Citrix SD-WAN 11

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Novedades

June 8, 2022

Mejoras centradas en las aplicaciones

Personalización de archivos de configuración automática de proxy dinámico (PAC):

Con el aumento en la adopción empresarial de aplicaciones SaaS de misión crítica y de personal distribuido, resulta sumamente crítico reducir la latencia y la congestión inherentes a los métodos tradicionales de backhaul del tráfico a través del Data Center.

Citrix SD-WAN permite una salida directa a Internet de aplicaciones SaaS como Office 365.

Sin embargo, si hay proxies web explícitos configurados en la implementación empresarial, todo el tráfico, incluido el tráfico de aplicaciones SaaS, 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) de empresa.

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.

Grupos de agregación de enlaces

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.

En Citrix SD-WAN versión 11.0, se admite un LAG simple (ACTIVE-BACKUP). Las negociaciones basadas en el protocolo 802.3ad LACP no se admiten en la versión actual.

Enlace en espera y medido

Inhabilitar si la opción Data Cap alcanzada se introduce en la versión 11.0.

- Si la casilla **Inhabilitar si se alcanza el límite de datos** está activada, el vínculo medido y todas sus rutas relacionadas se inhabilitarán hasta el siguiente ciclo de facturación, si el uso de datos alcanza el límite de datos.
- De forma predeterminada, la casilla de verificación **Desactivar si se alcanza el límite de datos** se desactivará, donde conserva el modo o estado actual establecido para que el enlace medido continúe después de alcanzar el límite de datos hasta el siguiente ciclo de facturación.

Autenticación LTE 210-SE

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Se introduce un nuevo campo de entrada de autenticación en el formulario de configuración de **APN**. Hay 4 valores posibles para este nuevo campo: Ninguno, PAP, CHAP, PAPCHAP.

El campo de autenticación se ha agregado para la configuración de APN en:

- IU central SD-WAN
- IU del dispositivo SD-WAN
- API de REST

Captura de paquetes

Utilice la opción **Captura de paquetes** para interceptar el paquete de datos que atraviesa las interfaces activas seleccionadas presentes en el sitio seleccionado.

Las interfaces activas están disponibles para la captura de paquetes en el sitio seleccionado. 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 captura de paquetes en todas las interfaces a la vez ayuda a acelerar la tarea de solución de problemas.

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 de fuera de banda permite crear una dirección IP de administración mediante un puerto reservado para la administración, que transporta tráfico de administración.

La administración en banda le permite utilizar los puertos de datos SD-WAN para la administración, que transporta tanto datos como tráfico de administración, sin tener que configurar una ruta de administración adicional.

Habilitar RED para el tráfico ICA

A partir de la versión 11.0, la detección temprana aleatoria (RED) se establece **en ON** de forma predeterminada para el tráfico ICA.

Servicios en la nube

Servicio Cloud Direct

El servicio **Cloud Direct** ofrece funcionalidades SD-WAN como servicio en la nube a través de una entrega confiable y segura para todo el tráfico vinculado a Internet independientemente del entorno de host (centro de datos, nube e Internet).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El servicio **Cloud Direct** mejora la visibilidad y la gestión de la red. Permite a los socios ofrecer servicios gestionados de SD-WAN para aplicaciones SaaS críticas para el negocio a sus clientes finales.

Integración de la red Palo Alto con SD-WAN

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.

Para conectar sus ubicaciones de red remotas al servicio Prisma Access, utilice el firewall de última generación de Palo Alto Networks. También puede utilizar un dispositivo compatible con IPsec de terceros, incluido SD-WAN, que puede establecer un túnel IPSec para el servicio.

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. El dispositivo puede conectarse desde ubicaciones de dispositivos SD-WAN con una configuración mínima.

Informes

Informes basados en el nombre de usuario HDX

En la página de informes de HDX, puede ver los siguientes tipos de informes:

- Estadísticas del sitio HDX
- Resumen de HDX (aplicable tanto para el canal de información HDX disponible como para las sesiones no disponibles)
- Sesiones de usuario HDX (aplicable para sesiones disponibles del canal de información HDX)
- Aplicaciones HDX (solo aplicable para sesiones disponibles del canal de información HDX)

La opción**Habilitar informes de usuario HDX** se agrega recientemente en el editor de configuración de SD-WAN. Al habilitar esta opción, se generan informes basados en usuarios recién agregados (resumen de HDX, sesiones de usuario de HDX y aplicaciones de HDX) y estos informes están disponibles en SD-WAN Center. Esto no es aplicable al informe **Estadísticas del sitio HDX**.

La opción**Habilitar informes de usuario de HDX** está disponible a nivel global y a nivel de sitio similar para **habilitar la opción DPI**.

Mejoras de redirección

Etiquetas de redistribución OSPF

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede utilizar etiquetas OSPF para evitar bucles de redirección durante la redistribución mutua entre OSPF y otros protocolos.

La especificación de etiquetas diferentes para rutas aprendidas SD-WAN y BGP permite que estas rutas se instalen en la tabla de redirección OSPF.

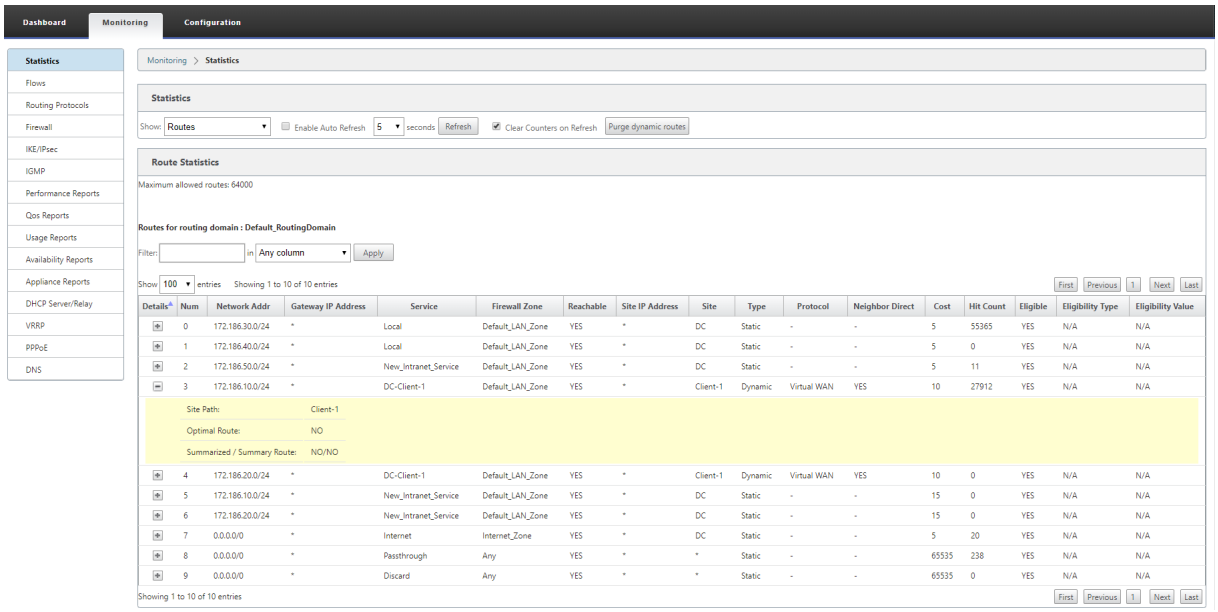
Preferencia de protocolo

Cuando Citrix SD-WAN aprende un prefijo de ruta a través de rutas virtuales, protocolo OSPF o protocolo BGP, se introduce al mismo tiempo el siguiente orden de preferencia predeterminado:

- OSPF -150
- BGP: 100
- SD-WAN: 250

Estadísticas de rutas

Otros detalles como Ruta del sitio, Ruta óptima, Ruta resumida o Ruta resumen se incluyen en el informe **Estadísticas de ruta**.



Longitud de ruta AS

El protocolo BGP utiliza el atributo de **longitud de ruta AS** para determinar la mejor ruta. La longitud de ruta AS indica el número de sistemas autónomos atravesados en una ruta. Citrix SD-WAN utiliza el atributo de **longitud de ruta BGP AS** para filtrar e importar rutas.

Citrix SD-WAN Center

Certificado de dispositivo SD-WAN Center

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anteriormente, se utilizaba un certificado de dispositivo predefinido que ya estaba instalado en el SD-WAN Center.

Con la versión 11.0 de Citrix SD-WAN, puede regenerar el certificado del dispositivo en el MCN que reemplaza el certificado predefinido e instalarlo en SD-WAN Center.

Función de administrador de seguridad en SD-WAN Center

La función de administrador de seguridad se agrega al Centro de SD-WAN. Un administrador de seguridad tiene acceso de lectura y escritura para el Firewall y la configuración relacionada con la seguridad en el **Editor de configuración**, mientras que tiene acceso de lectura a las otras secciones.

Implementar SD-WAN en Azure desde SD-WAN Center

Puede implementar Citrix SD-WAN en Azure desde Citrix SD-WAN Center.

Citrix SD-WAN para Azure permite a las organizaciones tener una conexión segura directa desde cada sucursal a las aplicaciones alojadas en Azure, lo que elimina la necesidad de realizar backhaul tráfico vinculado a la nube a través de un centro de datos.

Plataformas, escalabilidad e implementaciones

Escala de nodos de 6K para red

Citrix SD-WAN 11.0 admite una red de hasta 6000 sitios con un máximo de 128 regiones en una arquitectura de red interconectada.

Citrix SD-WAN SE en Google Cloud Platform

La implementación de Citrix SD-WAN SE VPX en Google Cloud Platform (GCP) permite a las organizaciones establecer una conexión directa y altamente segura desde cada sucursal a las aplicaciones alojadas en GCP. Esto elimina la necesidad de backhaul tráfico vinculado a la nube a través del centro de datos.

Las principales ventajas del uso de Citrix SD-WAN en GCP son:

- Cree conexiones directas desde cada sitio de sucursal a GCP.
- Asegúrese de que una conexión siempre activa a GCP.
- Extiende su perímetro seguro a la nube.
- Evolucionar a una red de sucursales simple y fácil de administrar.

Citrix SD-WAN 1100: Mejora de Small Form Factor Pluggable (SFP) para admitir HA con cable Y

Los puertos enchufables de factor de forma pequeño (SFP) disponibles en los dispositivos 1100 se pueden utilizar con cables en Y de fibra óptica para permitir una alta disponibilidad para la implementación del modo perimetral.

En el equipo 1100 SE y PE, el extremo dividido del cable divisor se conecta a los puertos de fibra de dos dispositivos 1100. Los puertos de fibra se configuran en un par de alta disponibilidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

API de REST

Se introducen las siguientes API:

- API de supervisión del estado de alta disponibilidad del dispositivo.
- API de banda ancha móvil para resumen de pin sim y operaciones de pin sim.
- API del editor de configuración para la configuración del archivo de configuración automática del proxy y la configuración del archivo de configuración automática del proxy del sitio.
- SD-WAN Center informa de API para aplicaciones HDX y sesiones HDX.
- SD-WAN Center informa de las API para el resumen HDX.

Notas de la versión

September 26, 2023

Esta nota de la versión describe los problemas conocidos y los problemas corregidos aplicables a la versión 11.0 del software Citrix NetScaler SD-WAN para los dispositivos SD-WAN Standard Edition, WANOP y Premium Edition.

En Citrix SD-WAN versión 11.0.0, el sistema operativo subyacente para el software SD-WAN se actualiza a una versión más reciente, lo que requiere un reinicio automático 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.

Para obtener información sobre las versiones anteriores de la versión, consulte la documentación.Citrix SD-WAN

Problemas resueltos

SDWANHELP-590: Mejoras de seguridad de Citrix SD-WAN Center.

SDWANHELP-594: Las rutas virtuales se marcan como **DESCONECTADA**para todos los sitios cuando se procesa el paquete de control dañado. Si el paquete de control está mal formado, se elimina y las rutas se vuelven inactivas.

SDWANHELP-600: Después de una actualización de software de la versión 9.3.2 a la 9.3.5, el nombre del sistema SNMP posterior a la actualización se muestra como la WAN virtual predeterminada y no utiliza el nombre del host del dispositivo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDWANHELP-617: La **ruta virtual dinámica**no se asigna con el ancho de banda necesario cuando la función **Detección de ancho de banda adaptable**está habilitada en cualquiera de los enlaces WAN que forman la ruta virtual dinámica.

SDWANHELP-626: No se puede acceder a Citrix SD-WAN Center debido a una interrupción de la memoria.

SDWANHELP-649: Las retransmisiones **excesivas de paquetes de ruta virtual**pueden experimentar con una utilización de ancho de banda bajo, una alta pérdida o congestión y menos de 20 ms de tiempo RTT.

SDWANHELP-650: El proceso de configuración, como agregar, modificar, clonar un sitio o realizar auditorías, hace que la GUI de MCN deje de responder.

SDWANHELP-654: El dispositivo SD-WAN WANOP 4000 podría interrumpirse al analizar las conexiones ICA.

SDWANHELP-666: PPTP o GRE túnel a través de Internet servicio no se puede establecer cuando el acceso a Internet para todos los dominios de enrutamiento función está habilitado.

El dispositivo SD-WAN actúa como paso a través y no como punto final.

SDWANHELP-671: Los archivos de registro de licencias consumen una gran cantidad de espacio en disco mientras se utiliza el servidor de licencias remoto.

SDWANHELP-674: En el dispositivo SD-WAN EE y PE, debe cambiar el nombre de host para la comunicación WANOP.

SDWANHELP-676: El servicio de dominio se reinicia automáticamente incluso cuando el servicio de dominio falla ocasionalmente.

SDWANHELP-680: Error en la configuración de auditoría al eliminar el servicio de Intranet en un sitio, si existía un servicio de Intranet con el mismo nombre en otro sitio.

SDWANHELP-682: El campo Ubicación del sitio no se guarda, al crear un sitio mediante el editor de configuración básico.

SDWANHELP-698: La conmutación por error de alta disponibilidad no ocurre si el puerto LAN se ha caído, si:

- Un dispositivo Citrix SD-WAN se implementa en modo de alta disponibilidad serie (FTW).
- Un puerto LAN (en FTB) se define en interfaces de alta disponibilidad para el seguimiento.

SDWANHELP-703: El tráfico IPsec a Zscaler se ve afectado cuando se observan picos de uso de memoria.

SDWANHELP-712: La ruta virtual conectada a LTE se informa como DOWN incluso cuando el módem está operativo en el dispositivo SD-WAN de la sucursal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDWANHELP-725: El dispositivo SD-WAN envía la información de ruta virtual de alta disponibilidad al SD-WAN Center. En los resultados, arroja un error de estadísticas ya que no puede reconocerlo.

SDWANHELP-734: El nombre de clase predeterminado no se actualiza después de cambiarlo.

SDWANHELP-735: La **partición Active OS es completamente alerta completa**se observa en la edición de la plataforma 1100 configurada como PE en 10.2.0 y 10.2.1 versiones.

Debe reiniciar manualmente el dispositivo 1100 después de actualizar a la versión 10.2.2.

SDWANHELP-736: El servicio SD-WAN podría interrumpirse durante el cambio de configuración en un modo de implementación de dos cajas.

SDWANHELP-742: El servicio SD-WAN podría interrumpirse durante la recopilación de paquetes STS cuando el número de reglas de **QoS de aplicación**excede las reglas de QoS basadas en IP.

SDWANHELP-746: Al crear dos reglas de firewall diferentes, puede producirse un error de auditoría si una dirección IP y un número de puerto son iguales incluso si los protocolos son diferentes.

SDWANHELP-748: La licencia no se aplica en varios sitios.

SDWANHELP-754: Al eliminar la configuración DHCP, los subobjetos como los relés DHCP y los conjuntos de opciones DHCP permanecen como entradas obsoletas.

Todos los objetos secundarios deben eliminarse cuando se elimina el elemento DHCP primario.

SDWANHELP-768: El servicio WAN virtual 5100 Premium Edition (PE) se reinicia al establecer el canal de señalización. Esto ocurre debido al conflicto de puertos efímeros entre varios motores de paquetes WANOP.

SDWANHELP-795: La prueba de ancho de banda de ruta se interrumpe, si:

- La prueba de ancho de banda de ruta se ejecuta en sucursales que están aisladas de MCN debido a que la ruta virtual está inactiva o inhabilitada.
- El MCN realiza el cambio de propiedad de enlace WAN de sucursal, cuando las sucursales surgen.

SDWANHELP-799: Los prefijos OSPF de aprendizaje de SD-WAN con coste "AS IS"de enrutadores vecinos y permiten la exportación de estos a dispositivos SD-WAN del mismo nivel. Si el coste de redistribución se cambia externamente en el enrutador vecino (como, por ejemplo, la redistribución de BGP y RIP en el cambio de coste métrico OSPF), el coste recién modificado se actualiza en el dispositivo SD-WAN conectado inmediatamente, pero no se actualiza a los dispositivos SD-WAN del mismo nivel.

SDWANHELP-801: El servicio SD-WAN podría interrumpirse al procesar paquetes ICMP a su IP virtual a alta velocidad y la actualización de la configuración se activa simultáneamente.

SDWANHELP-808: Debido a razones heredadas, SD-WAN no permite pocos patrones en la configuración del sitio. Este sitio en particular contiene APN en su nombre. Es engañoso solo en la GUI de SD-WAN y no afecta a ninguna operación en el nivel del sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDWANHELP-812: El aprovisionamiento 10.2.x falla en la plataforma 1100 Premium Edition (PE), ya que no creó el disco DBC.

SDWANHELP-818: Una vez que las rutas dinámicas han aprendido y convergido, si ocurre una actualización de configuración que tiene un cambio de coste realizado, después de la activación, el ID de ruta de las rutas aprendidas dinámicamente se restablece a '0'en lugar de permanecer enumerado causando incluso rutas óptimas para ser eliminadas en una actualización de ruta al vecino.

SDWANHELP-819: SD-WAN WANOP Premium Edition (PE) no puede establecer el emparejamiento seguro correctamente.

SDWANHELP-830: Los certificados de CA utilizados para el emparejamiento de seguridad automática en SD-WAN WANOP se eliminan al actualizar. Esto afecta a la formación de emparejamiento seguro para cualquier dispositivo nuevo agregado a la implementación. En este caso, es necesario volver a generar certificados de CA, eliminar certificados y pares de clave de certificado de todos los sitios y restablecer el emparejamiento de seguridad automática una vez más después de actualizar a 10.2.3.

SDWANHELP-831: Al encender los dispositivos 210, el Controller de relé FTW podría fallar al inicializarse, lo que puede llevar a que el relé permanezca en estado cerrado si está configurado en modo de alta disponibilidad en serie (FTW).

SDWANHELP-846: El servicio SD-WAN podría interrumpirse al recibir paquetes ICMP destinados a IP virtual en una implementación de dominio de enrutamiento múltiple.

SDWANHELP-854: En raras circunstancias, si se reciben paquetes no válidos, el sistema podría reiniciarse. Este problema puede producirse si el cifrado de ruta se inhabilitó desde su estado habilitado predeterminado.

SDWANHELP-866: SD-WAN descarta paquetes grandes debido a LR0/TSO habilitado.

SDWANHELP-914: No se puede aplicar la configuración al agregar una ruta para programar pruebas de ancho de banda para ella.

NSSDW-16165: La subred agregada como parte de la definición de región no se rellena en la tabla de rutas.

NSSDW-16825: El agente DHCP no pudo analizar paquetes DHCP OFERTA con relleno adicional como en el módem Satélite.

NSSDW-17108: Al seleccionar el primer grupo de rutas automáticas al configurar plantillas de vínculos WAN, se muestra como "ningún grupo seleccionado. "

NSSDW-18012: A veces, las rutas virtuales se desconectan después de la actualización de configuración en dispositivos PPPoE.

NSSDW-19233: El agente de Windows Azure se está llenando con la partición raíz debido a que pocas extensiones se están instalando por el portal de Azure.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas conocidos

NSSDW-17238: VPXL no muestra más de 4 interfaces cuando se crea en XenServer.

- **Solución alternativa**: Establezca el parámetro del kernel para XenServer como se muestra a continuación y reinicie XenServer.
  /opt/xensource/libexec/xen-cmdline –set-xen gnttab_max_frames=256

NSSDW-19132: En las sesiones MSI de HDX, el estado de conexión se muestra como **NO VÁLIDO** para algunas de las secuencias IDLE en el **Informe de sesiones de usuario de HDX** en la ficha HDX.

NSSDW-20154: Al volver a conectarse a la misma sesión, XenApplication y XenDesktop Server no vuelven a enviar los detalles relacionados con la aplicación. Por lo tanto, es posible que los datos del informe de **aplicaciones de HDX** no se muestren para esa sesión en particular.

NSSDW-20371: Cuando se habilita la **licencia centralizada**, la actualización a versiones anteriores arroja un error - **ERROR: Error al analizar modelos de licencia**.

- **Solución alternativa**: Inhabilite la licencia centralizada y continúe con la rebaja. Los dispositivos tienen una licencia de gracia. Una vez finalizada la actualización, puede volver a habilitar las licencias centralizadas y aplicar la configuración a través de la administración de cambios.

NSSDW-20500: En 5100 PE, cuando se inicia la operación de unión de dominios por primera vez, es posible que aparezca un mensaje de advertencia que indica que WANOP se está inicializando.

- **Solución alternativa**: Vuelva a unirse al dominio después de dos minutos.

NSSDW-20527: La interfaz de usuario permite configurar PPPoE para la interfaz LTE, que no se espera ni se permite.

NSSDW-27727: Las redes con instancia VPX y VPXL que utilizan el controlador IXGBEVF, utilizadas para ciertas NIC Intel de 10 GB cuando SR-IOV está habilitado, no deben actualizarse a 11.0. Esto podría resultar en una pérdida de conectividad. Se sabe que este problema afecta a las instancias de AWS con SR-IOV habilitado.

Limitaciones

- Los informes**basados en el usuario de HDX** se muestran desde XenApp y XenDesktop Server versión 7.17 en adelante.
- Se informa de que las aplicaciones publicadas en una sesión HDX están cerradas, es decir, la hora de finalización de la aplicación se muestra en el informe de **aplicaciones HDX** si SD-WAN recibe el **Tiempo de finalización de la aplicación** de Xen Application/Xen Desktop Server.

  Se informa de que algunas de las aplicaciones están activas incluso si están cerradas en caso de que no se reciba la hora de finalización de la aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- En caso de errores no deseados debido a los cuales la información de sesión de HDX no está disponible en el dispositivo, los informes basados en el usuario de HDX no se muestran aunque los **informes de usuario de HDX** estén habilitados en el editor de configuración.

  A veces, pocos campos como nombre de usuario, nombre del servidor, versión del servidor, ICA RTT en los informes se muestran como **NA**.

Notas de la versión de Citrix SD-WAN 11.0.1

May 7, 2021

Introducción

Esta nota de la versión describe los problemas resueltos y los problemas conocidos aplicables al software 11.0 Citrix SD-WAN Standard Edition, versión 1, WANOP, dispositivos Premium Edition y SD-WAN Center.

Para obtener información sobre las versiones anteriores, consulte laCitrix SD-WANdocumentación de docs.citrix.com.

Problemas resueltos

SDWANHELP-981: La implementación **automatizada de Azure Virtual WAN**a través de SD-WAN Center no pudo descargar o aplicar la configuración VPN y las rutas asociadas.

NSSDW-17552: En la versión 11.0, si el dispositivo se reiniciaba ya sea activado por el usuario o en una actualización de software, la **administración de cambios**ocasionalmente se congelaba en la preparación de paquetes que impedían al usuario realizar actualizaciones de configuración posteriores.

NSSDW-20755: Los dispositivos SD-WAN entraron en modo de licencia **Grace**, después de actualizar a la versión 11.0.

NSSDW-20901: La autenticación de usuario TACACS y RADIUS para SD-WAN Standard y Premium Edition estaba fallando.

NSSDW-20905: La adición de rutas estáticas en una ruta virtual estaba fallando debido a una comprobación de límites incorrecta mediante el **Editor de configuración**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas conocidos

NSSDW-17238: VPXL no muestra más de 4 interfaces cuando se crea en XenServer.

- **Solución alternativa**: Establezca el parámetro del kernel para XenServer como se muestra a continuación y reinicie XenServer.
  /opt/xensource/libexec/xen-cmdline –set-xen gnttab_max_frames=256

NSSDW-19132: En las sesiones MSI de HDX, el estado de conexión se muestra como **NO VÁLIDO** para algunas de las secuencias IDLE en el **Informe de sesiones de usuario de HDX** en la ficha HDX.

NSSDW-20154: Al volver a conectarse a la misma sesión, XenApplication y XenDesktop Server no vuelven a enviar los detalles relacionados con la aplicación. Por lo tanto, es posible que los datos del informe de **aplicaciones de HDX** no se muestren para esa sesión en particular.

NSSDW-20371: Cuando se habilita la **licencia centralizada**, la actualización a versiones anteriores arroja un error - **ERROR: Error al analizar modelos de licencia**.

- **Solución alternativa**: Inhabilite la licencia centralizada y continúe con la rebaja. Los dispositivos tienen una licencia de gracia. Una vez finalizada la actualización, puede volver a habilitar las licencias centralizadas y aplicar la configuración a través de la administración de cambios.

NSSDW-20500: En 5100 PE, cuando se inicia la operación de unión de dominios por primera vez, es posible que aparezca un mensaje de advertencia que indica que WANOP se está inicializando.

- **Solución alternativa**: Vuelva a unirse al dominio después de 2 minutos.

NSSDW-20527: La interfaz de usuario permite configurar PPPoE para la interfaz LTE, que no se espera ni se permite.

NSSDW-27727: Las redes con instancia VPX y VPXL que utilizan el controlador IXGBEVF, utilizadas para ciertas NIC Intel de 10 GB cuando SR-IOV está habilitado, no deben actualizarse a 11.0.1. Esto podría resultar en una pérdida de conectividad. Se sabe que este problema afecta a las instancias de AWS con SR-IOV habilitado.

Notas de la versión de Citrix SD-WAN 11.0.2

May 7, 2021

Introducción

Esta nota de la versión describe las novedades, los problemas corregidos y los problemas conocidos aplicables a la versión 11.0 del software Citrix SD-WAN versión 2 para los dispositivos SD-WAN Stan-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dard Edition, WANOP, Premium Edition y SD-WAN Center.

Para obtener información sobre las versiones anteriores de la versión, consulte la documentación.Citrix SD-WAN

Novedades

Integración de Palo Alto en la plataforma 1100

Se admite el firewall de última generación de Palo Alto Networks serie VM-Series (VM 50 y VM 100) alojado en la plataforma SD-WAN 1100.

Cuentas de usuario: Administrador de red

Se introduce un nuevo nivel de privilegios de cuenta de usuario, **Network Admin**. El administrador de red tiene acceso de lectura y escritura a la configuración de red.

Dominio de redirección

Se admiten los siguientes casos de uso del dominio de redirección:

- Permitir que los dominios de redirección transiten un sitio, pero no tengan ningún punto de salida en el sitio.
- Permitir que exista un dominio de redirección sin IP enrutable.

Clasificación de aplicaciones basada en nombres de dominio

El motor de clasificación de DPI se ha mejorado para clasificar las aplicaciones en función del nombre de dominio y los patrones. Las aplicaciones basadas en nombres de dominio clasificados se utilizan para configurar lo siguiente:

- Proxy DNS
- Reenviador transparente DNS
- Objetos de aplicación
- Rutas de aplicación
- Directiva de firewall
- Reglas de QoS de la aplicación
- QoE de aplicaciones

Autenticación de certificado

La autenticación basada en certificados se introduce en Citrix SD-WAN 11.0.2. Permite a las organizaciones utilizar certificados emitidos por su entidad de certificación privada para autenticar dispositivos antes de establecer las rutas virtuales entre sitios.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problemas resueltos

SDWANHELP-779: El tráfico de actualización de paquetes SD-WAN es lento y no maneja los paquetes fuera de servicio en la red de manera óptima.

SDWANHELP-896: En algunas implementaciones con **rutas virtuales dinámicas**o ciclos de vida cortos de **Security Association (SA)**en los que se crean y destruyen las SA con frecuencia, puede producirse un error de interrupción del servicio.

SDWANHELP-899: Una posible condición de carrera se aborda en la actualización de configuración de reglas que a veces puede causar la interrupción de la ruta de datos.

SDWANHELP-901: Si el sistema tiene alta disponibilidad y tiene mucha ruta virtual, es posible que no sincronice las rutas con los pares, siempre que haya muchos eventos de actualización de ruta disponibles de los otros pares.

SDWANHELP-919: Bajo carga pesada y una alta tasa de llegada de paquetes de caducidad de tiempo de vida (TTL), el servicio podría bloquearse si se aplica un filtro en **Supervisión > > Flujos**. Esto provocaría una conmutación de alta disponibilidad (HA) en la implementación de alta disponibilidad.

SDWANHELP-934: Enviamos la solicitud de protocolo de resolución de direcciones (ARP) (que no debe enviarse) si:

- La instancia de Virtual Router Redundancy Protocol (VRRP) está en estado inhabilitado.
- La solicitud de protocolo de resolución de direcciones (ARP) de ARP gratuito (GARP) recibida del router del mismo nivel.

Este problema se produce cuando se configura el VRRP y la instancia está inhabilitada.

SDWANHELP-945: En el Editor de configuración, si hace clic en **Auditoría**para la sección **BGP**, le llevará a la sección **OSPF**aunque OSPF no esté configurado.

SDWANHELP-947: El uso reportado para un enlace medido es anormalmente alto.

SDWANHELP-950: Los OID escalares expuestos en la MIB no devuelven la respuesta válida.

SDWANHELP-978: El módem LTE puede desaparecer al reiniciar los dispositivos SD-WAN 210. Este es un problema intermitente en el que un ciclo de alimentación debe poner el módem en línea de nuevo.

SDWANHELP-981: La implementación automatizada de **Azure Virtual WAN**a través de SD-WAN Center no pudo descargar y aplicar la configuración de VPN y las rutas asociadas.

SDWANHELP-999: No se pueden eliminar los archivos de licencia que tienen más de un '.'en el nombre del archivo.

SDWANHELP-1004: Los servicios Intranet/Internet no obtienen el recurso compartido de ancho de banda asignado en la dirección WAN a LAN, cuando el servicio VP estático, DVP, Intranet/Internet está habilitado en el enlace WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDWANHELP-1009: En raras condiciones, algunos paquetes IPSec de intranet o LAN pueden transmitirse con direcciones MAC de destino no válidas, lo que hace que los paquetes se pierdan o se eliminen en la red.

NSSDW-17552: Si el dispositivo se reiniciaba ya sea activado por el usuario o en una actualización de software, la **administración de cambios**ocasionalmente se congelaba en la preparación de paquetes que impedían al usuario realizar actualizaciones de configuración posteriores.

NSSDW-17238: Build root VPXL no muestra más de 4 interfaces cuando se crea en XenServer.

Problemas conocidos

NSSDW-21802: En una implementación de dos cajas, si el modo de dos cajas está inhabilitado en WANOP y se realiza una administración de cambios en WAN Virtual, al volver a habilitar el modo de dos cajas en WANOP, las IP de caché de WCCP no se rellenan intermitentemente.

Solución alternativa: Inhabilite y vuelva a habilitar el modo de dos cajas desde la GUI de WANOP.

NSSDW-21808: La información del dispositivo aprovisionado en SD-WAN Center se borra antes de que se complete la operación de desaprovisionamiento real en el dispositivo SD-WAN.

Solución alternativa: En la GUI de SD-WAN Center, vaya a Configuración > Firewall hospedado > Sitios de Firewall hospedados > Provisión, seleccione los sitios con errores desaprovisionados e inicie la provisión para restaurar la información del sitio.

NSSDW-21806: Para un grupo de interfaces PPPoE, al configurar el nombre de CA, el nombre de servicio y el nombre de usuario en mayúsculas, las entradas cambian a minúsculas. Esto podría causar problemas en el aprendizaje de IP desde el concentrador de acceso (ISP).

Solución alternativa: No configure ningún valor para el nombre de CA y el nombre de servicio o utilice minúsculas.

NSSDW-21873: Las aplicaciones personalizadas no se notifican en SD-WAN Center.

Solución alternativa: Agregue las aplicaciones personalizadas a un objeto de aplicación y habilite los informes sobre el objeto de aplicación.

NSSDW-20371: aparece el mensaje de error “Error al analizar modelos de licencia”cuando se descalifica a Citrix SD-WAN 10.2.3 o versiones anteriores, con licencias centralizadas habilitadas y la tasa de licencias establecida en automático.

Solución alternativa: Desactualización a Citrix SD-WAN 10.2.4.

NSSDW-27727: Las redes con instancia VPX y VPXL que utilizan el controlador IXGBEVF, que se utilizan para ciertas NIC Intel de 10 GB cuando SR-IOV está habilitado, no deben actualizarse a 11.0.2. Esto podría resultar en una pérdida de conectividad. Se sabe que este problema afecta a las instancias de AWS con SR-IOV habilitado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Notas de la versión de Citrix SD-WAN 11.0.3

May 7, 2021

Introducción

En esta nota de la versión se describen las novedades, los problemas resueltos y los problemas conocidos aplicables a la versión 11.0 del software de Citrix SD-WAN, versión 3, para SD-WAN Standard Edition, dispositivos WANOP, Premium Edition y SD-WAN Center.

Para obtener información sobre las versiones anteriores de la versión, consulte la documentación.Citrix SD-WAN

> **Nota**
>
> - CVE-2019-19781: una vulnerabilidad en los dispositivos Citrix SD-WAN WANOP (aplicable SOLAMENTE para modelos 4000-WO, 4100-WO, 5000-WO, 5100-WO Platform) que conduce a la ejecución de código arbitrario se corrige en la versión 10.2.6b. Para obtener más información, consulte CVE KB.
> - La versión 11.0.3.1018 contiene correcciones de seguridad y Citrix recomienda que todos los clientes apliquen el parche en Amazon Web Services.

Novedades

Compatibilidad con varios concentradores para Microsoft Virtual WAN

Con la versión 11.0.3, una rama se puede conectar a varios concentradores dentro de un recurso de Azure Virtual WAN. Un recurso WAN virtual de Azure se puede conectar con varios sitios de sucursales locales. Un sitio de sucursal debe estar asociado a recursos de Azure WAN para establecer túneles IPSec.

Cambio de contraseña de SD-WAN Standard Edition (SE) VPX

A partir de la versión 11.0.3, es obligatorio cambiar la contraseña predeterminada de la cuenta de usuario de administrador durante el aprovisionamiento de cualquier dispositivo SD-WAN o implementación de un nuevo dispositivo VPX con SD-WAN SE. Este cambio se aplica mediante la CLI y la interfaz de usuario.

Existe una cuenta de mantenimiento del sistema - CBVWSSH, para el desarrollo y la depuración y no tiene permisos de inicio de sesión externos. Solo se puede acceder a la cuenta a través de la sesión de CLI de un usuario administrativo normal.

Actualización del firmware de SD-WAN 210-LTE

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Con la versión 11.0.3, el firmware activo LTE se actualiza como parte del paquete de actualización de un solo paso. Para actualizar, debe actualizar la ventana de programación mediante la página **Configuración de administración de cambios** o esperar la hora programada predeterminada para actualizar el firmware LTE (diariamente a las 21:20:00).

Problemas resueltos

SDWANHELP-941: Durante la actualización de configuración podríamos perder el restablecimiento del evento de cambio de ruta virtual y podría dar lugar a este error en el que no bajaremos las rutas incluso cuando la ruta virtual correspondiente desaparezca.

SDWANHELP-961: Este problema afecta potencialmente a los dispositivos WANOP SD-WAN 4000 y 5000. Después de que el dispositivo ejecute 10.1.0 a 10.2.5 durante más de un año, existe la posibilidad de que se mantengan demasiados datos en los registros.

SDWANHELP-988: Los usuarios de **RADIUS** y **TACACS+** no pueden generar paquetes de diagnóstico desde la interfaz de usuario de SD-WAN Center. La creación de paquetes de diagnóstico a través de terminal está fallando para todos los usuarios. La opción **Configuración > Licencias** no está disponible en la interfaz de usuario de SD-WAN Center.

SDWANHELP-1000: Siempre que NetFlow está habilitado con la configuración de alta disponibilidad (HA), se produce un fallo de alta disponibilidad debido a la falta de recursos.

SDWANHELP-1023: los reinicios del servicio SD-WAN pueden producirse cuando los paquetes se enrutan incorrectamente después de la traducción de NAT.

SDWANHELP-1035: Las rutas no se propagan correctamente a sitios remotos a través de MCN y RCN.

SDWANHELP-1042: SD-WAN se bloquea cuando el usuario relanza una aplicación publicada que se desconectó en una sesión HDX existente y la cierra.

SDWANHELP-1049: La máquina virtual WAN virtual (VM) en plataformas basadas en XenServer puede tener un gran desplazamiento de tiempo con el tiempo. En este caso, la hora de la VM WAN virtual muestra inexacta después del reinicio.

SDWANHELP-1051: Con versiones de servidor de licencias inferiores a v11.16.3, podrían provocar ataques de denegación de servicio (DOS) que afecten a todos los servidores de licencias heredados inferiores a 11.16.3.

SDWANHELP-1070: La hora no se sincroniza con el reloj de hardware después de haber sido cambiado. Por ejemplo, actualización manual de tiempo o actualización de tiempo NTP.

SDWANHELP-1088: Algunas de las páginas GUI del dispositivo SD-WAN podrían dejar de responder si se reinicia un dispositivo después de habilitar la función de archivo PAC.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDWANHELP-1095: Es posible que la puerta de enlace de capa de aplicaciones (ALG) de FTP no analice correctamente las sesiones FTP si se utilizan los modos EPSV o EPRT causando un error en la sesión FTP.

SDWANHELP-1112: El número del sistema autónomo (AS) BGP admite un número de 32 bits.

SDWANHELP-1113: Intermitentemente no se puede acceder a la GUI de administración en plataformas WANOP solo después de actualizar a 11.0.2.

SDWANHELP-1116: Durante la actualización de configuración, es posible que perdamos el procesamiento de eventos de sincronización debido a la falla de alta disponibilidad (HA), que podría provocar que el dispositivo se encuentre en un estado problemático, donde la sincronización de rutas no ocurre con otras sucursales y ocasiona una interrupción de la red.

SDWANHELP-1123: Al configurar un dominio de enrutamiento con solo una interfaz DHCP, se muestra un error de auditoría.

SDWANHELP-1160: Citrix SD-WAN Center muestra direcciones IP duplicadas en vínculos WAN de un sitio en el Editor de configuración. El problema se produce cuando el cuarto número de dos direcciones IP de enlace WAN comienza con el mismo dígito y varía según el número de dígitos como 4, 45, 486.

SDWANHELP-1164: Al transferir la configuración del dispositivo desde SD-WAN Center, si la contraseña, en la configuración del dispositivo, contiene un símbolo de dólar seguido de algún carácter, la transferencia falla. Por ejemplo, las contraseñas test$1, test$1$d fallarán. Pero test1$ funcionará.

SDWANHELP-1169: El servicio se aborta cuando se programó la transmisión de un paquete para un DVP pendiente de eliminación. El software intenta eliminarlo erróneamente de una lista de paquetes vacía. El software ha sido actualizado.

SDWANHELP-1176: Debido a algunas entradas huérfanas en la base de datos de configuración, la API GET para config_editor/virtual_paths arroja algunas excepciones junto con la respuesta. Se ha corregido la eliminación en cascada para evitar las entradas de la base de datos huérfanas.

SDWANHELP-1189: Durante la actualización del dispositivo de software, el proceso de instalación puede fallar en los dispositivos SD-WAN 210 Standard Edition (SE). En la detección de errores, el dispositivo se reinicia automáticamente para evitar el problema, de modo que la actualización pueda continuar.

SDWANHELP-1201: El módem LTE se puede reiniciar por sí solo esporádicamente. Al iniciar una sesión de datos, el módem sigue informando de un error; el **servicio no es compatible**. La solución es inhabilitar y volver a habilitar automáticamente el módem para recuperar la falla.

SDWANHELP-1385: La información del número de serie del dispositivo SD-WAN podría perderse y restablecerse a la cadena predeterminada debido a un problema en el firmware del BIOS v1.0b en la plataforma SD-WAN 210.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDWANHELP-1365: En una configuración de MCN GEO de alta disponibilidad con reenvío WAN a WAN habilitado, un evento inactivo del **servicio de Internet** podría desencadenar un escenario erróneo en el que las rutas aprendidas de MCN GEO secundario tienen mayor prioridad que el MCN GEO primario.

NSSDW-22847: La casilla de verificación **Multi-salto** en BGP se mostró marcada en la interfaz de usuario de SD-WAN de forma predeterminada cuando BGP está habilitado. Pero la configuración no se habilitó a menos que el usuario inhabilite y vuelva a activarla.

NSSDW-25032: El discriminador de salida múltiple (MED) no se anunció al vecino cuando una directiva BGP se configura con métricas MED y enlazada a un vecino. Este problema era el prefijo de red incorrecto (32) establecido por el compilador.

NSSDW-25067: Se muestra un mensaje de advertencia o un mensaje ocupado cuando el módem LTE está deshabilitado y vuelve a activarlo antes de que el modo de funcionamiento haya cambiado a **Baja potencia**. La solución es advertir al usuario y mostrar el modo de funcionamiento actual antes de realizar la operación de activación/desactivación.

NSSDW-25135: A veces, durante la implementación de Zscaler, se usaron configuraciones incorrectas para crear la asignación. El problema se produce debido a entradas duplicadas erróneas en la base de datos. La corrección garantiza que no hay entradas duplicadas en la base de datos.

NSSDW-25147: Cuando la característica PPPoE se configura en dispositivos SD-WAN, el demonio de protocolo punto a punto (PPPD) se ejecuta para establecer las sesiones PPPoE. Esta configuración es vulnerable a CVE-2020-8597, una vulnerabilidad de desbordamiento de búfer. Este problema se corrige a partir de la versión 11.1.0.

NSSDW-25440: Es posible que se observen pérdidas significativas de paquetes o retrasos de red en Azure en instancias con aceleración de red habilitada.

NSSDW-28971: Una vez que inicie sesión en los dispositivos SD-WAN y las máquinas virtuales, puede obtener acceso al shell raíz con la imagen basada en 11.x utilizando una contraseña codificada. Las plataformas SD-WAN afectadas son 110 y VPX aprovisionadas con imágenes 11.x. Este es un problema relacionado con CLI y no se aplica a la GUI.

Problemas conocidos

NSSDW-23264: La obtención de una licencia remota falla si la compilación de SD-WAN Center está en 11.x, mientras que la compilación del dispositivo está en 10.x.

Solución alternativa: Downgrade SD-WAN Center se construye con la misma versión 10.x con la que está configurado el dispositivo SD-WAN.

NSSDW-23132: Después de actualizar a 11.x, el tiempo real de interrupción del tráfico podría tener un valor muy grande en segundos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solución alternativa: La administración de cambios subsecuente muestra el valor correcto, esto es solo un problema de visualización.

NSSDW-23134: Una inserción de software consistente podría ocurrir al intentar agregar un sitio a la red cuando la red se acaba de actualizar a 11.x.

Solución alternativa: Realice una vez más la administración de cambios.

NSSDW-23485: Cloud Direct no permite el funcionamiento si una configuración activa en MCN tiene un carácter de punto en el nombre.

Solución alternativa: Actualice el nombre del archivo de configuración sin incluir DOT.

SDWANHELP-1110: En un caso raro, se puede observar una interrupción en el servicio de rutas de datos en los dispositivos de gama baja (210/410) cuando se crean continuamente rutas virtuales dinámicas de corta duración.

Solución alternativa: Desactive la ruta virtual dinámica (DVP) o ajuste la configuración para evitar DVP de corta duración.

SDWANHELP-1159: Citrix SD-WAN no anuncia las rutas hacia el vecino OSPF. Esto sucede cuando las rutas se cambian en SD-WAN o se produce una solapa de rutas virtuales que hace que las rutas WAN virtuales se vuelvan a sincronizar a través de los sitios. En este caso, si el vínculo al par OSPF tiene pérdida de información, SD-WAN podría entrar en un estado en el que nunca anuncia las rutas SD-WAN al vecino OSPF.

Solución alternativa: Detenga y reinicie el servicio WAN virtual.

NSSDW-27727: Las redes con instancia VPX y VPXL que utilizan el controlador IXGBEVF, que se utilizan para ciertas NIC Intel de 10 GB cuando SR-IOV está habilitado, no deben actualizarse a 11.0.3. Esto podría resultar en una pérdida de conectividad. Se sabe que este problema afecta a las instancias de AWS con SR-IOV habilitado.

Requisitos del sistema

May 7, 2021

Requisitos de hardware

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 con versiones de software anteriores no pueden establecer una conexión de Ruta virtual con el dispositivo con la versión 11.0 de SD-WAN. Para obtener más información, póngase en contacto con el equipo de soporte técnico de Citrix.

Requisitos de software

Para obtener información detallada sobre los requisitos de licencia, consulte Licencias.

Requisitos del explorador

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

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

- Mozilla Firefox 49+
- Google Chrome 51+
- Microsoft Internet Explorer 11+
- Microsoft Edge 13+ adaptador de cable
- Safari 9+

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 superior.
- Citrix Hypervisor 6.5 o superior.
- Microsoft Hyper-V 2012 R2 o superior.
- Linux KVM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 y paquetes de software

September 26, 2023

En esta sección se proporciona información acerca de la descarga de los paquetes de software de Citrix SD-WAN.

> **Nota**
>
> Antes de descargar el software, debe obtener y registrar una licencia de software Citrix SD-WAN. Para más información, consulte Licencias.

Un paquete de dispositivo SD-WAN contiene el paquete de software SD-WAN para un modelo de dispositivo concreto incluido con un paquete de configuración SD-WAN específico. Los dos paquetes se agrupan y se distribuyen a los clientes mediante el Asistente para **administración de cambios** de la Interfaz Web de administración que se ejecuta en el nodo principal de control (MCN).

Si se trata de una instalación inicial, debe cargar, organizar y activar manualmente el paquete de dispositivo adecuado en cada uno de los dispositivos cliente que residen en la red SD-WAN. Si está actualizando la configuración de una implementación SD-WAN existente, el MCN distribuye y activa automáticamente el paquete de dispositivo adecuado en cada uno de los clientes existentes, cuando las rutas virtuales a los clientes entren en funcionamiento.

Descargar los paquetes de software

Existe un paquete de software de Citrix SD-WAN diferente para cada modelo de dispositivo. Debe descargar el paquete de software adecuado para cada modelo de dispositivo que quiera incluir en la red.

Para descargar los paquetes de software Citrix SD-WAN, vaya a la URL; descargas de productos.
En este sitio se proporcionan instrucciones para descargar el software.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paquetes de software de Citrix SD-WAN

Hay un paquete de software Citrix SD-WAN diferente para cada modelo de dispositivo SD-WAN compatible. Debe adquirir el paquete adecuado para cada modelo de dispositivo que tenga previsto incorporar a la red.

Modelos de dispositivos SD-WAN compatibles

Existen tres categorías principales de dispositivos Citrix SD-WAN:

- Modelos de hardware de dispositivos SD-WAN
  - WANOP, Standard Edition y Premium Edition
- Dispositivos virtuales VPX SD-WAN (VPX SD-WAN)
  - Standard Edition y WANOP Edition

> **Nota**
>
> Todos los modelos de dispositivos SD-WAN en un entorno SD-WAN deben ejecutar la misma versión de firmware de SD-WAN. Para obtener más información, póngase en contacto con el servicio de asistencia al cliente de Citrix SD-WAN.

Para obtener una descripción completa de los dispositivos SD-WAN, consulte la edición de la plataforma de productos SD-WAN hoja de datos en el sitio de descarga de productos.

Dispositivos de hardware de edición estándar SD-WAN

Citrix SD-WAN versión 11.0 admite los siguientes modelos de dispositivos de hardware de edición estándar SD-WAN:

MODELO DE PLATAFORMA SD-WAN SE	ROL
210-SE/210-SE LTE	Dispositivo de sucursal pequeña
410-SE	Dispositivo de sucursal pequeña
1000-SE	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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

MODELO DE PLATAFORMA SD-WAN SE	ROL
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 de hardware de optimización de WAN SD-WAN (WANOP SD-WAN)

Citrix SD-WAN 11.0 admite los siguientes modelos de dispositivos de optimización de WAN (WANOP) de SD-WAN:

MODELOS DE PLATAFORMA SD-WAN WANOP	ROL
WANOP 800	Dispositivo de sucursal pequeña
WANOP 1000	Dispositivo de sucursal grande
WANOP 2000	Dispositivo de sucursal grande
WANOP 3000	Dispositivo de sucursal grande
WANOP 4100	Dispositivo del centro de datos
WANOP 5100 adaptador de…	Dispositivo del centro de datos

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

Citrix SD-WAN 11.0 admite los siguientes modelos de dispositivo virtual de SD-WAN VPX (VPX-SE):

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 100SE	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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Citrix SD-WAN 11.0 admite los siguientes modelos SD-WAN WANOP Virtual Appliance (VPX-WANOP):

MODELOS DE PLATAFORMA SD-WAN VPX WANOP	ROL
WANOP VPX-2	Dispositivo de sucursal pequeña
WANOP VPX-6	Dispositivo de sucursal pequeña
WANOP VPX-10	Dispositivo de sucursal pequeña
WANOP VPX-20	Dispositivo de sucursal pequeña
WANOP VPX-50	Dispositivo de sucursal grande
WANOP VPX-100	Dispositivo de sucursal grande
WANOP VPX-200	Dispositivo de sucursal grande

> **Importante**
>
> En la versión 10.1, la edición de la plataforma Enterprise se cambia a “Premium Edition.”

Dispositivos de hardware de edición premium SD-WAN (SD-WAN PE)

Citrix SD-WAN 11.0 admite los siguientes modelos de dispositivo de SD-WAN Premium (Enterprise) Edition (SD-WAN PE):

MODELOS DE PLATAFORMA SD-WAN EE	ROL
1000-PE	Dispositivo de centro de datos y sucursal grande
1100-PE	Dispositivo de centro de datos y sucursal grande
2100-PE	Dispositivo de centro de datos y sucursal grande
5100-PE	Dispositivo de centro de datos y sucursal grande
6100-PE	Dispositivo de centro de datos y sucursal grande

Rutas de actualización

October 27, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

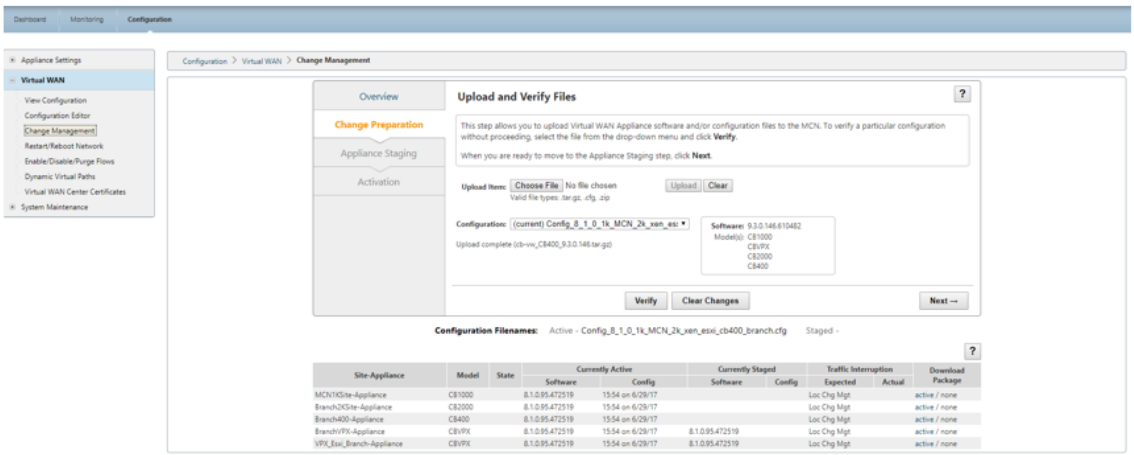
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualización del software WAN virtual a 9.3.5 con implementación WAN virtual en funcionamiento

May 7, 2021

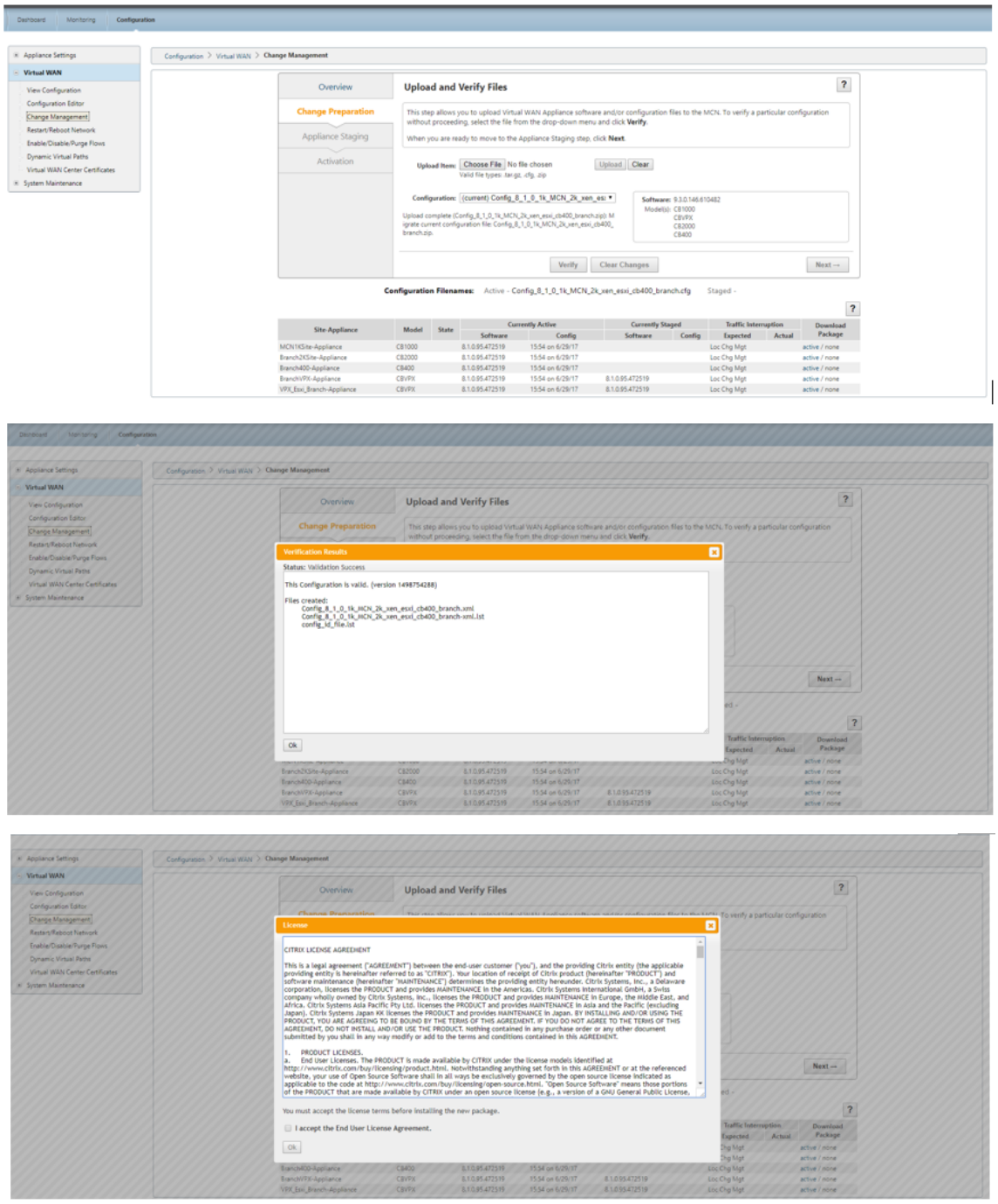
> **Nota:**
>
> Tener una configuración WAN virtual en funcionamiento que ejecute la versión 9.3.4 o inferior, con rutas virtuales establecidas desde MCN a los sitios de sucursal.

1. En el dispositivo MCN, vaya a **Configuración** > **WAN virtual** > **Administración de cambios**.
2. Obtenga el archivo *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* aplicable para todos los sitios de la red WAN virtual desde página de descargas de Citrix
3. Cargue el archivo *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* para las sucursales definidas en el archivo de configuración para las que se debe realizar la actualización. Realice la administración de cambios en la interfaz web SD-WAN para el dispositivo MCN y complete el proceso de administración de cambios.



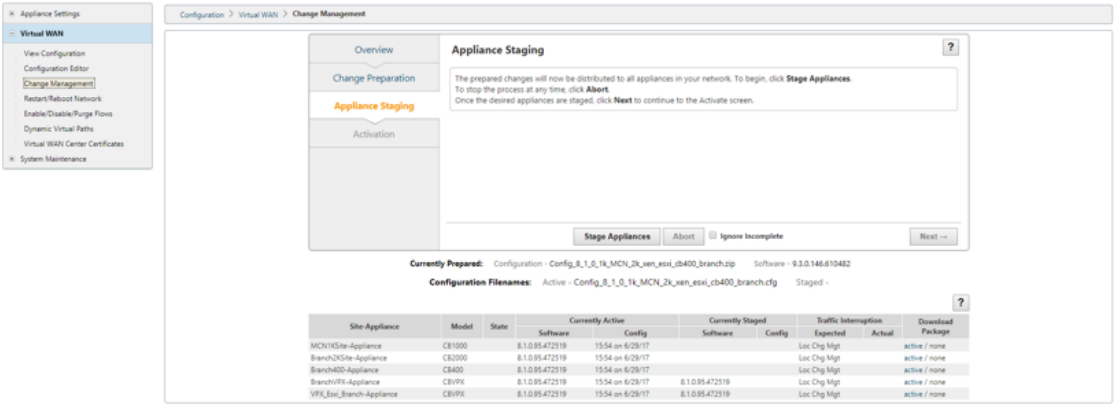
4. Haga clic en **Siguiente** para continuar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

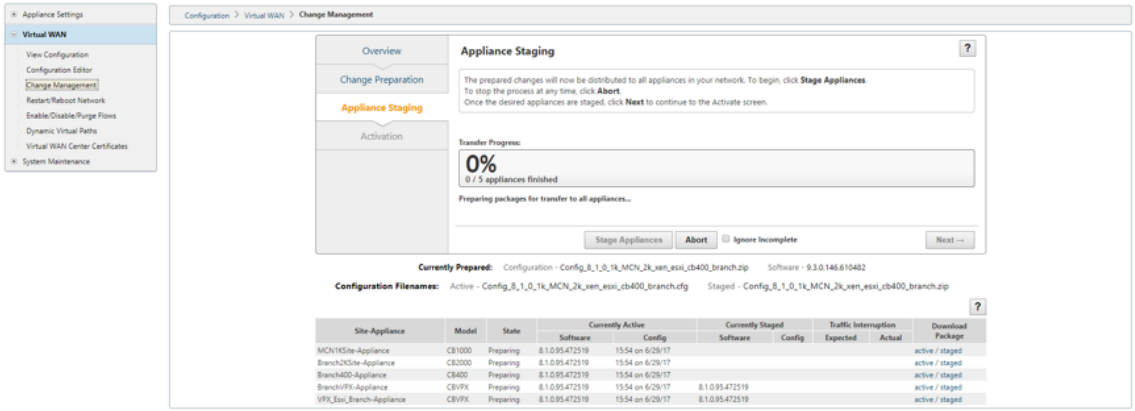


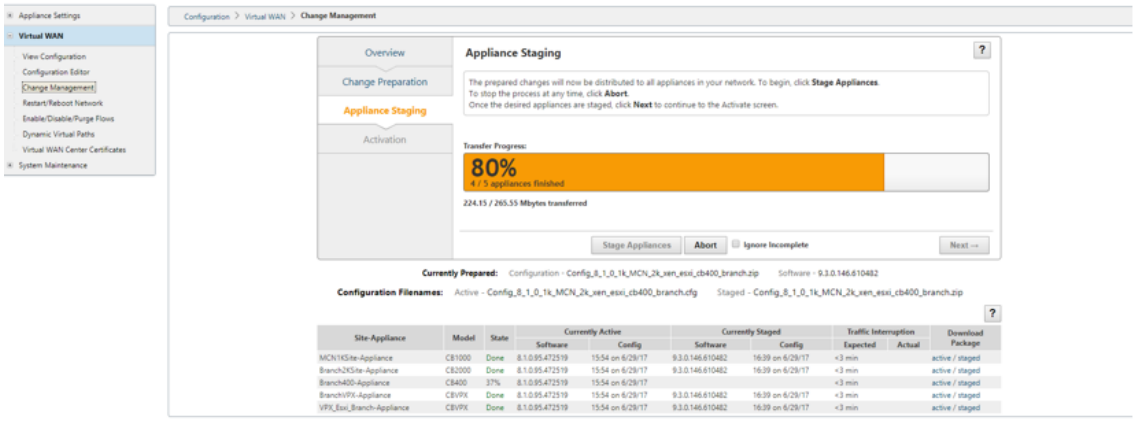
5. Después de aceptar el acuerdo de licencia, accederá a **Appliance Staging**, donde los dispositivos se pueden poner en escena haciendo clic en **Stage Appliances**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



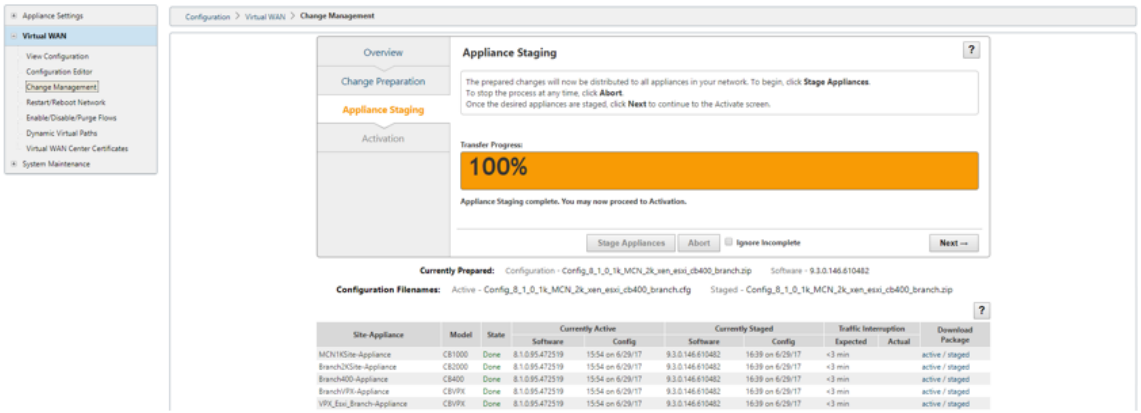
6. El estado Progreso de transferencia se muestra como parte de la preparación y puesta en escena de los paquetes de software en los dispositivos.



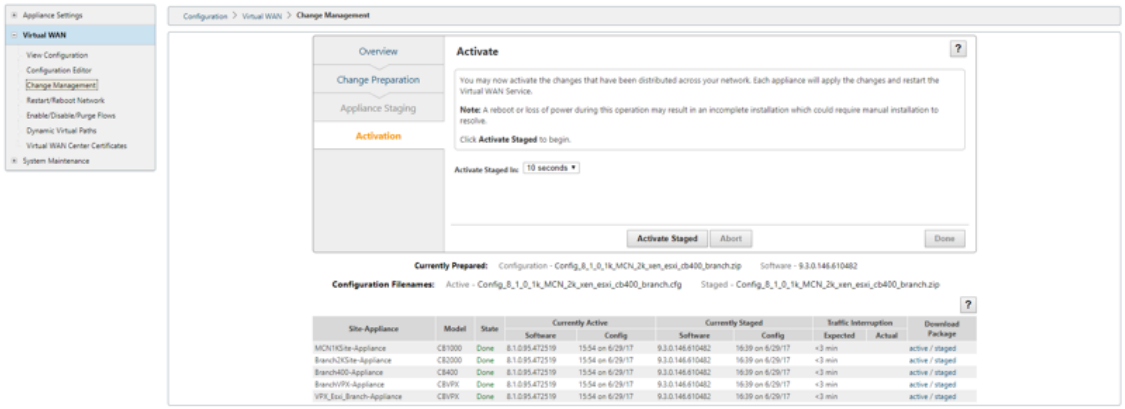


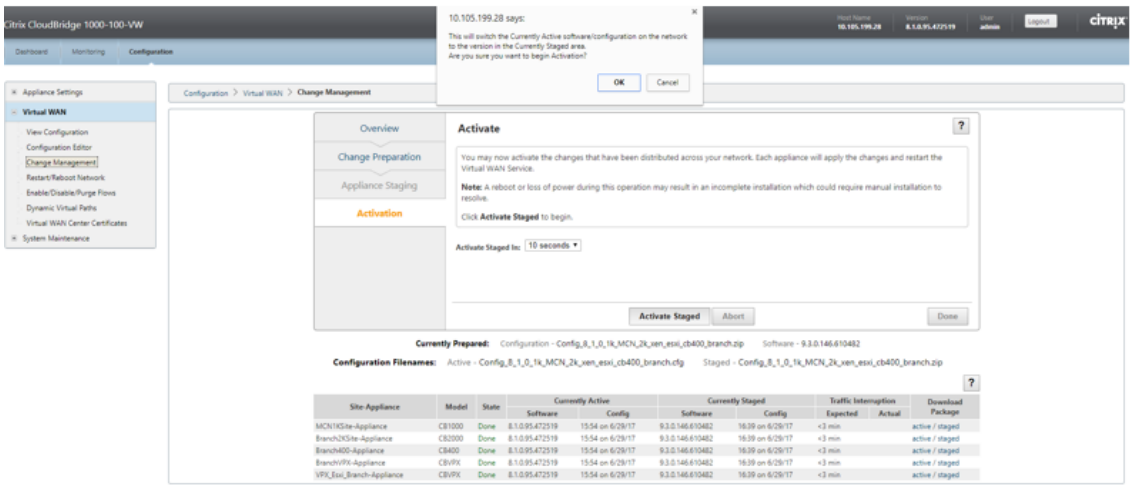
7. Haga clic en **Siguiente** cuando el progreso de transferencia muestre el 100% y el botón esté habilitado para continuar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



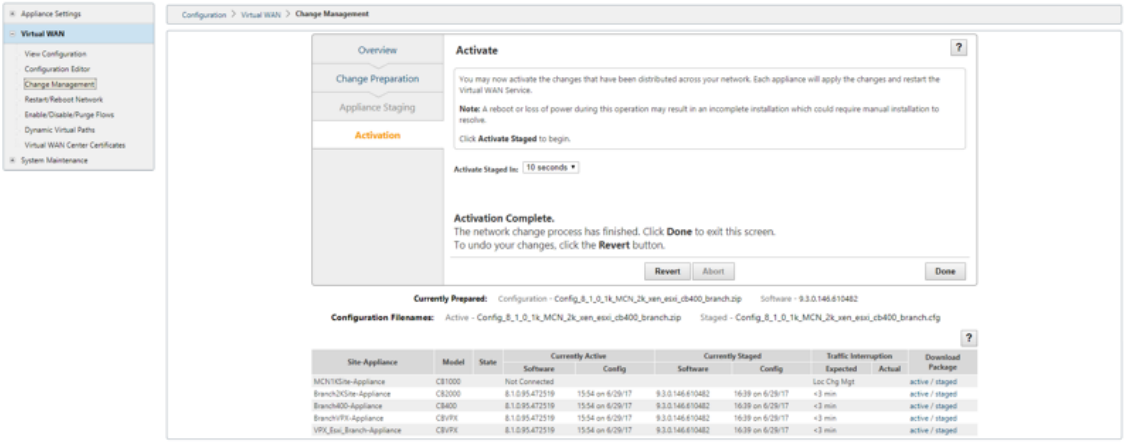
8. En la página **Activación**, haga clic en **Activar por etapas** para iniciar la activación.





9. Después de completar la cuenta atrás de activación de 180 s, haga clic en **Listo**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

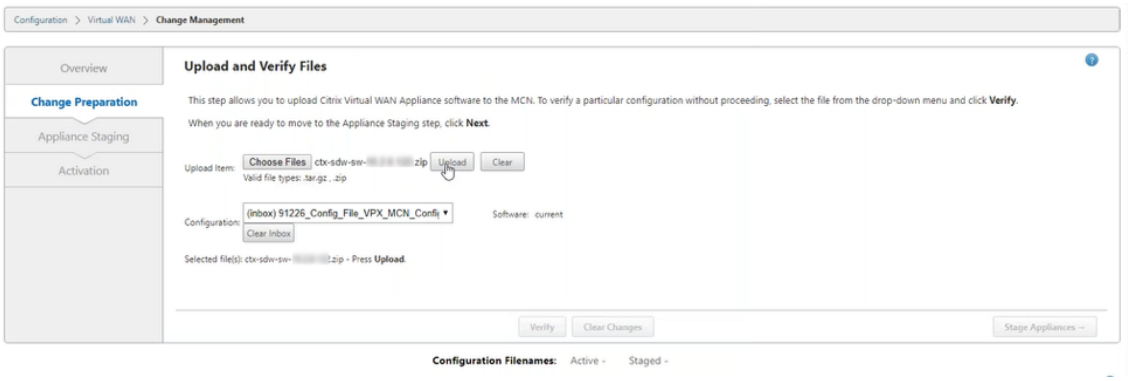


Actualizar la versión a 11.0 con implementación de WAN virtual en funcionamiento

January 10, 2022

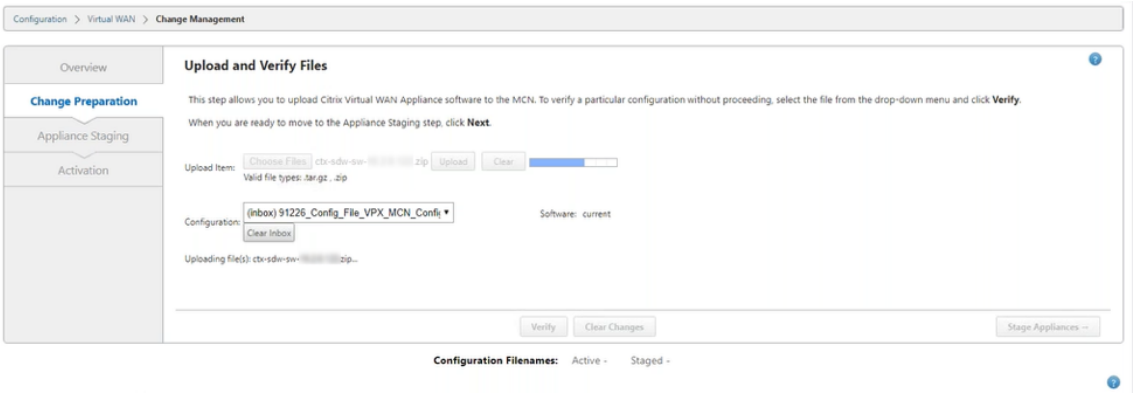
1. En la página **Administración de cambios > Preparación** de cambios, haga clic en **Elegir archivos** y seleccione el archivo de paquete de software *ctx-sdw-sw-11.0.0.x.zip*. Haga clic en **Cargar**.

   > **Nota:**
   >
   > Puede descargar el paquete de software Citrix SD-WAN versión 11 desde la página Descargas.

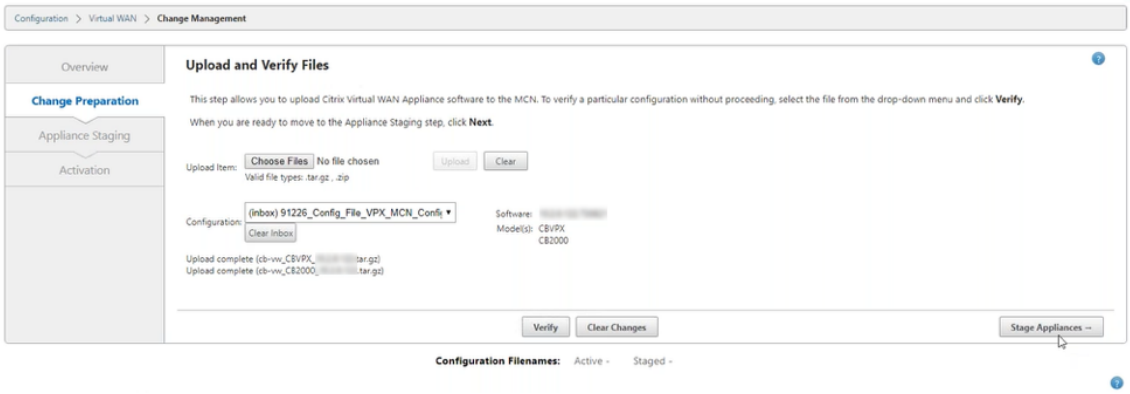


   Aparece una barra de progreso para mostrar el progreso de carga actual.

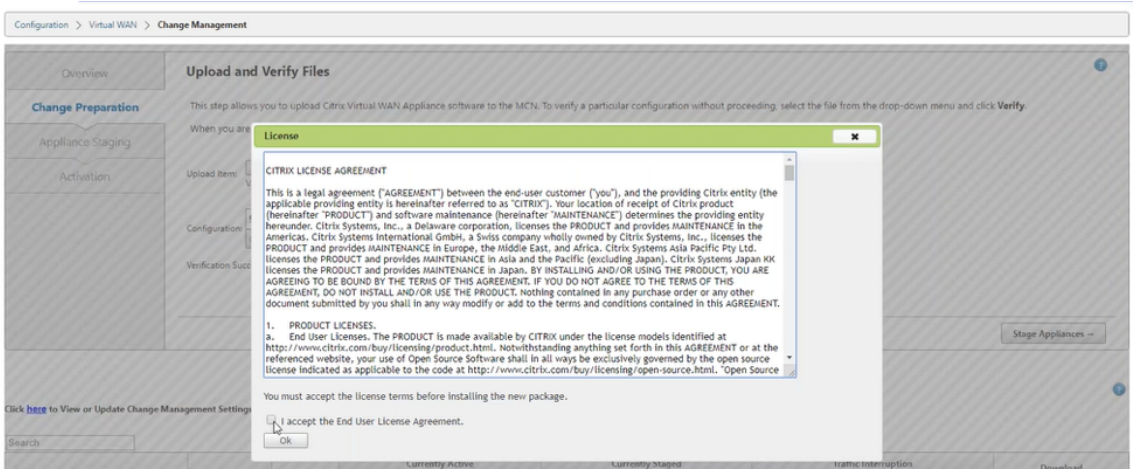
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Una vez que el proceso de carga se haya realizado correctamente, se mostrarán los modelos de dispositivo pertinentes. Los dispositivos se actualizarían en función del archivo de configuración.



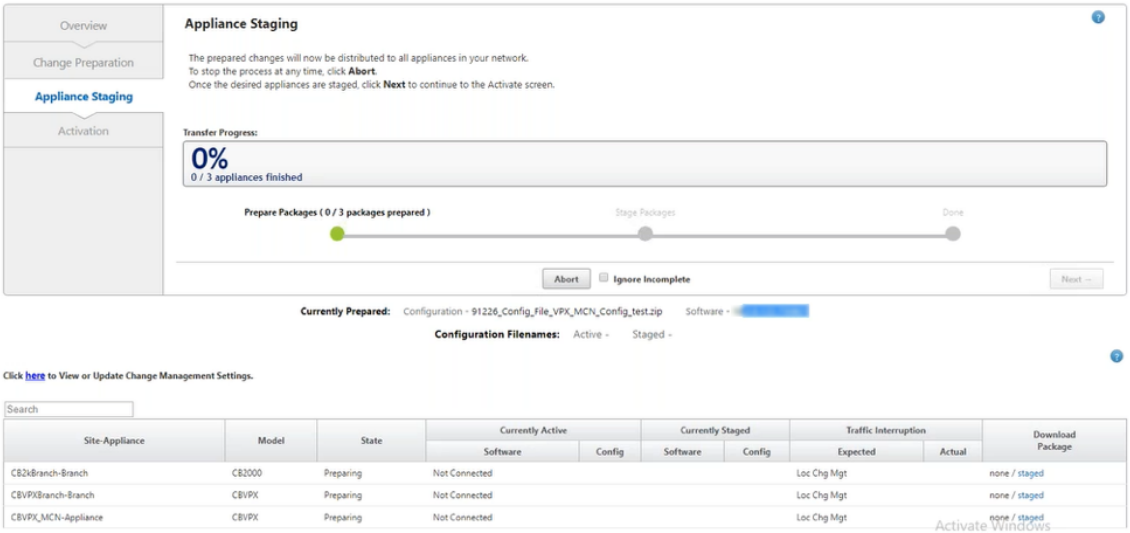
3. Haga clic en **Stage Appliance** para continuar con la validación del archivo de configuración. Aparecerá la página Contrato de licencia para la aceptación del usuario. Haga clic en **Acepto el Contrato de licencia de usuario final** y haga clic en **Aceptar**.



4. Se inicia el proceso de **ensayo del dispositivo**. Los cambios se distribuyen a todos los dispositivos de la red. Aparece la barra de progreso de transferencia y se actualiza la tabla de detalles

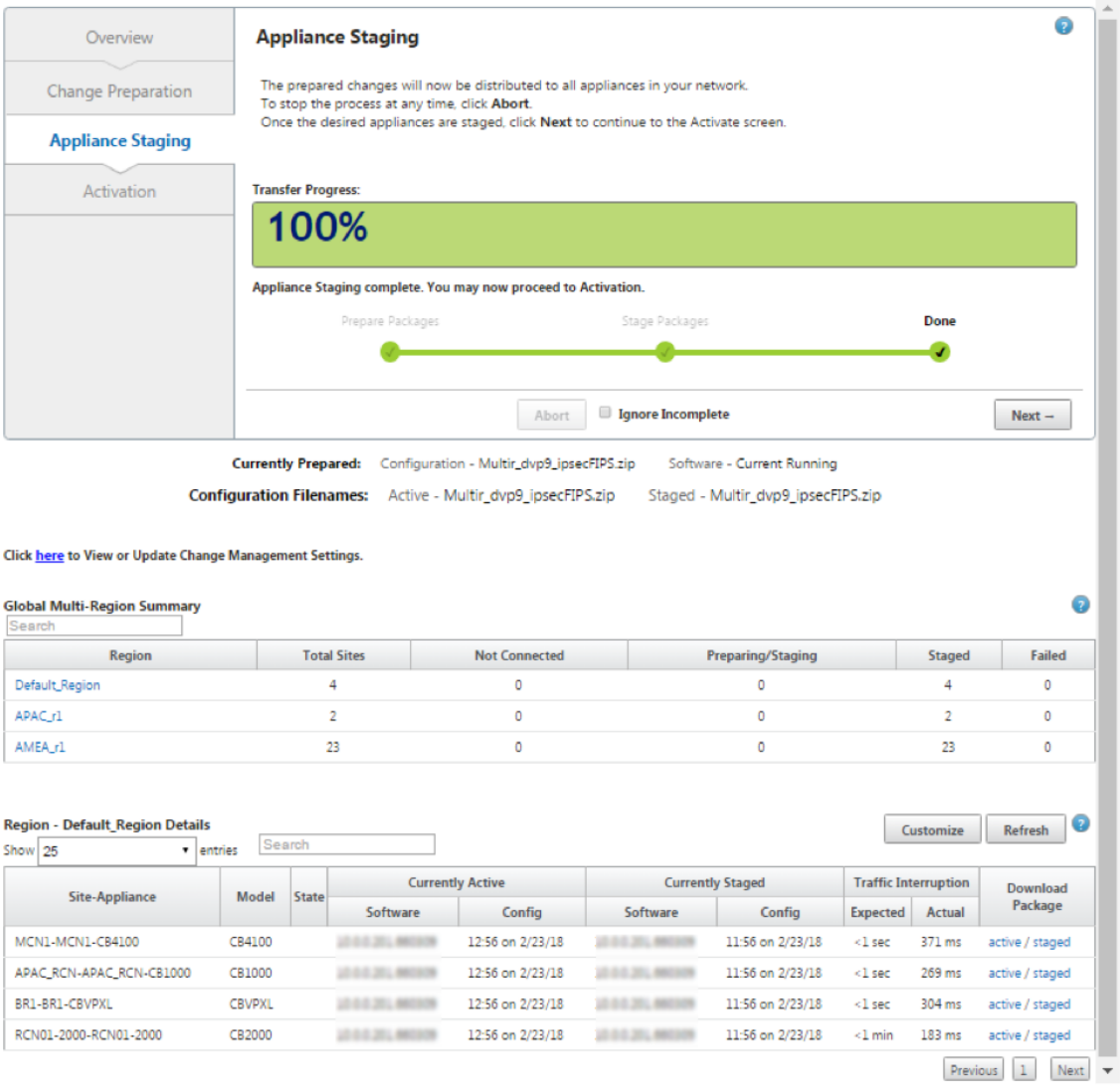
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

del sitio.



5. Una vez que el progreso de la transferencia haya finalizado al 100%, haga clic en **Siguiente** para continuar con la activación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Los diversos estados de configuración de paquetes de software mostrados en la tabla de resumen indican lo siguiente:

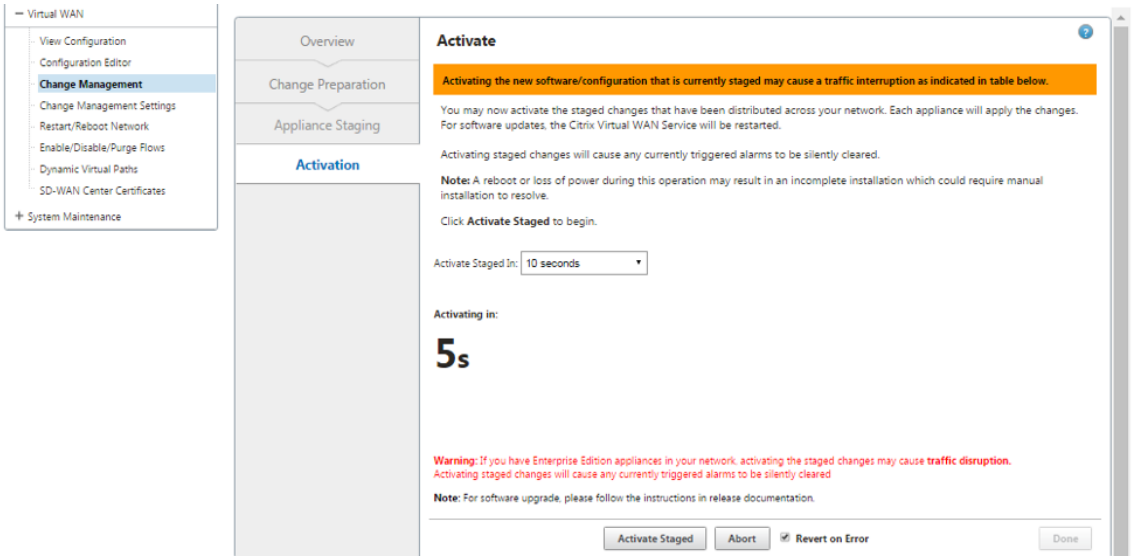
- **Preparación**: Procesamiento local para preparar el paquete de actualización para su transferencia al dispositivo.
- **Preparación de paquetes de región**: Procesamiento local para preparar el paquete de actualización para su transferencia a RCN. (Aplicable si RCN forma parte de la red).
- **Porcentaje: Porcentaje** del paquete transferido al dispositivo.
- **Desempaquetado**: Procesamiento remoto del dispositivo para aplicar el paquete de actualización.
- **Región de transferencia**: El paquete se está transfiriendo a RCN. (Aplicable si RCN forma parte de la red).
- **Error**: Se detectó una transferencia incompleta remota.
- **Cancelado** - Cancelado por el usuario cuando se comprobó 'Ignorar incompleto'durante

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stage Appliances

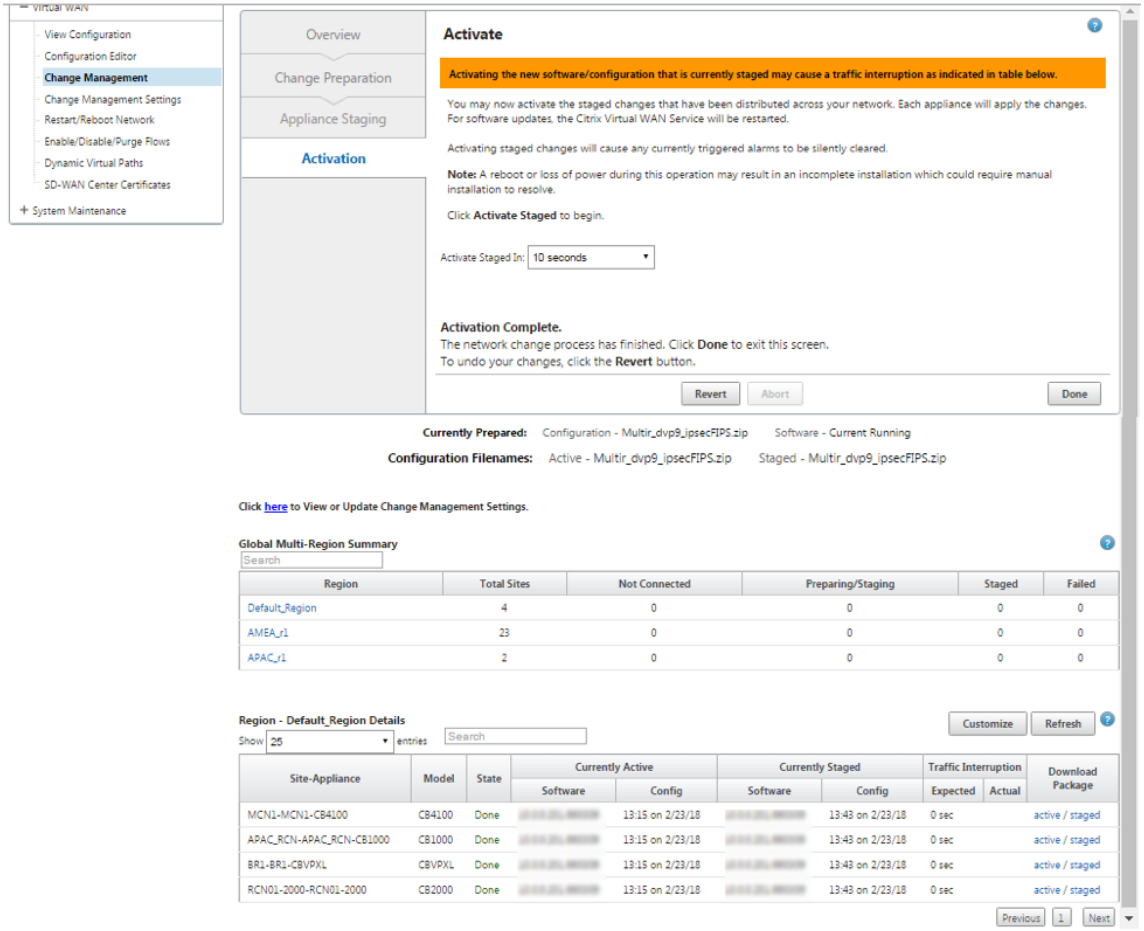
- **No es necesario**: El paquete preparado por etapas no incluye este nombre del dispositivo de sitio.
- **No conectado**: Local no puede ver la información del paquete activo del mando a distancia.

6. Haga clic en **Activar por etapas** para activar el software por etapas.



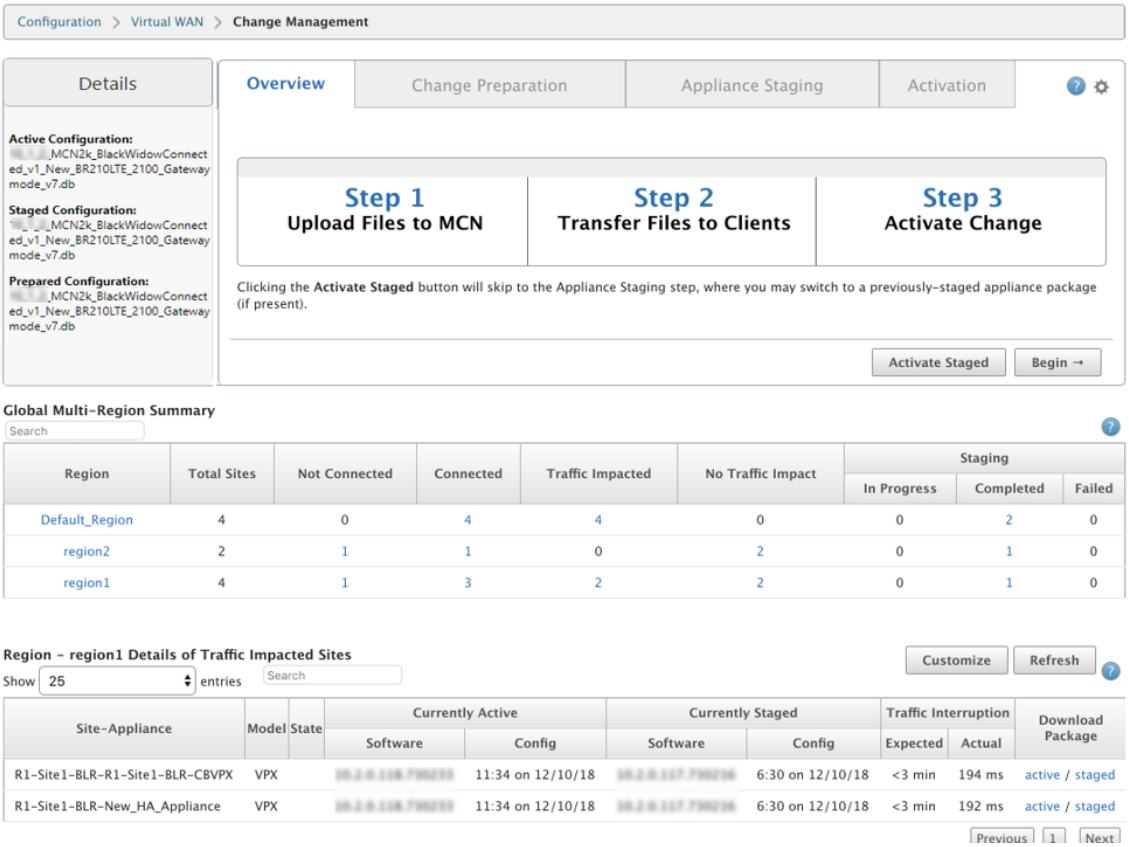
7. Después de la cuenta atrás, un mensaje indica que se ha completado la activación. Haga clic en **Done**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Acceda a la página **Gestión de cambios** para ver el estado de la transferencia.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La tabla de resumen de varias regiones proporciona los siguientes detalles:

- **Región**: Nombre de la región.
- **Sitio total**: Número total de sitios de la región.
- **No conectado**: Número total de sitios no conectados en la región.
- **Conectado**: Número total de sitios conectados en la región.
- **Tráfico impactado**: Número total de sitios donde el tráfico se ve afectado en la región.
- **Sin impacto en el tráfico**: Número total de sitios en los que el tráfico no se ve afectado en la región.
- **En fase intermedia**: Número total de sitios para los que el procesamiento local intenta preparar el paquete de actualización para su transferencia en la región.
- **Etapas completadas**: Número total de sitios para los que se ha completado la fase intermedia en la región.
- **Error de ensayo**: Número total de sitios para los que se ha eliminado una transferencia incompleta en la región.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Connected	Traffic Impacted	No Traffic Impact	Staging		
						In Progress	Completed	Failed
Default_Region	4	0	4	4	0	0	2	0
region2	2	1	1	0	2	0	1	0
region1	4	1	3	2	2	0	1	0

Haga clic en el enlace de entrada de la tabla **Resumen global de varias regiones** para filtrar los informes de configuración específicos de la región.

Region - Default_Region Details of Connected Sites

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-NY-MCN-NY-CB2000	2000		[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	82 s	active / staged
Def-Site1-SC-Def-Site1-SC-CBVPX	VPX		[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	209 s	active / staged
R1-RCN-MUM-R1-RCN-MUM-CBVPX	VPX	Done(auto)	[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	195 s	active / staged
R2-RCN-SA-R2-RCN-SA-CBVPX	VPX	Done(auto)	[illegible]	11:34 on 12/10/18	[illegible]	6:30 on 12/10/18	<3 min	199 s	active / staged

Previous 1 Next

Para la implementación en varias regiones, en cada RCN vaya a la página **Configuración de administración de cambios** y programe la instalación de componentes dependientes. De forma predeterminada, MCN/RCN asigna programas de instalación para que se intente todos los días a las 21:20:00 en función de la disponibilidad de software en las ramas. Para obtener más información, consulte Configuración de administración de cambios.

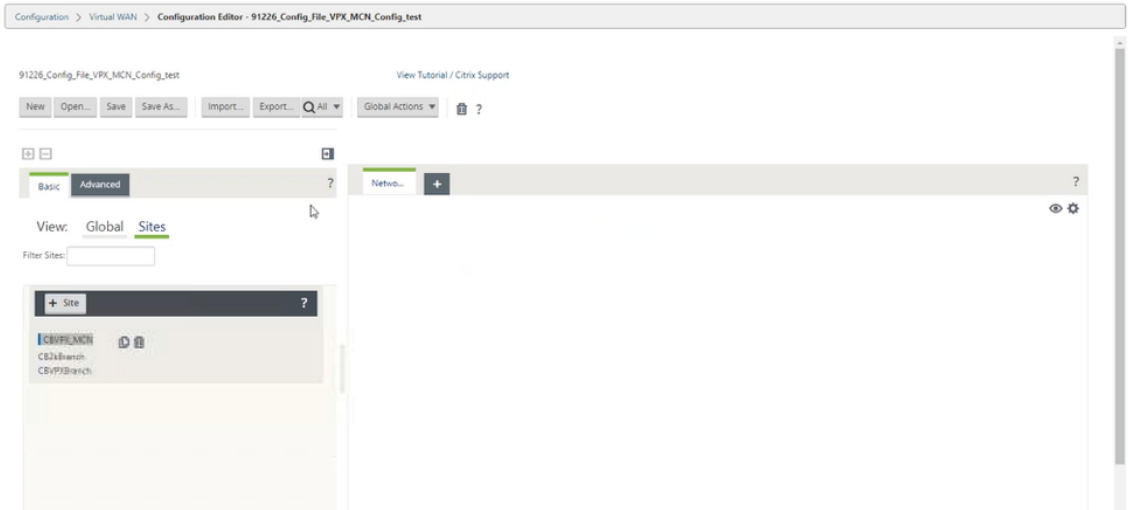
Actualizar la versión a 11.0 sin implementación de WAN virtual en funcionamiento

May 7, 2021

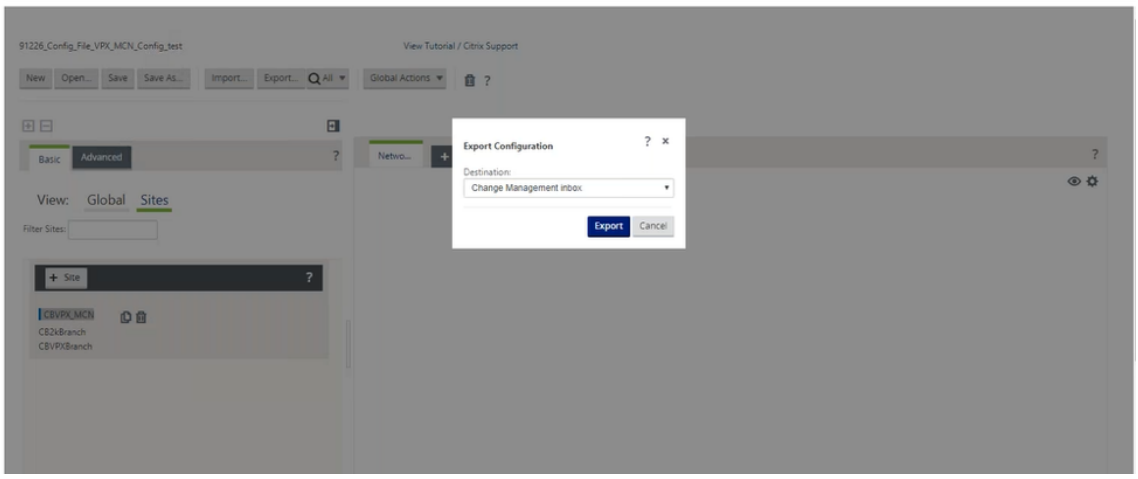
> Nota: Para configurar las funciones 11.0 más recientes, vuelva a instalar el dispositivo MCN al software 11.0. Para obtener más información, consulte Reimagen del software del dispositivo Citrix SD-WAN

1. Prepare la configuración con el **Editor de configuración** y guarde la configuración con un nombre válido. Para obtener más información, consulte el tema Configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



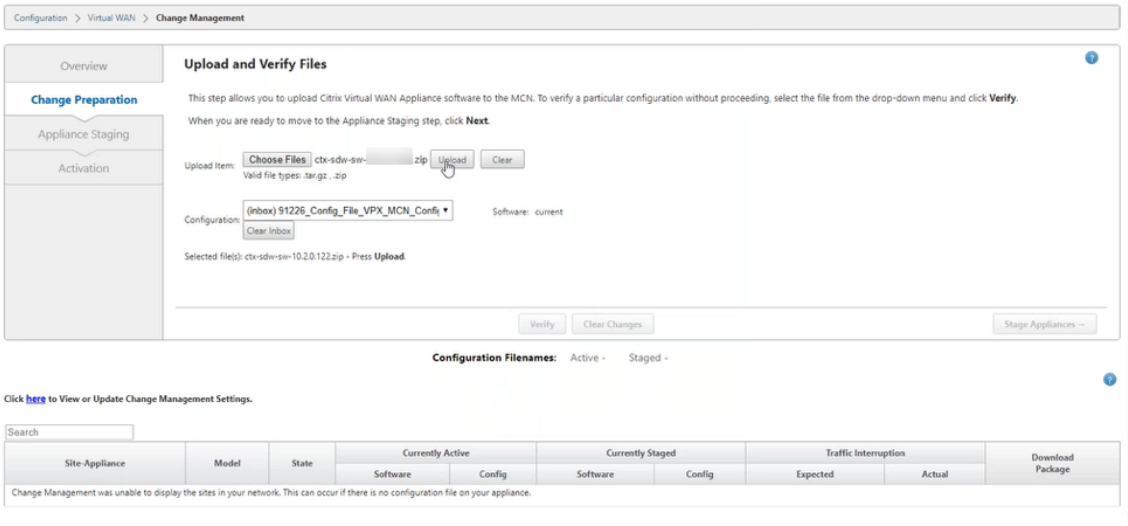
2. Exporte la configuración guardada a Administración de cambios. Haga clic en **Exportar** y seleccione **Bandeja de entrada de administración de cambios** como destino. Haga clic en **Export**.



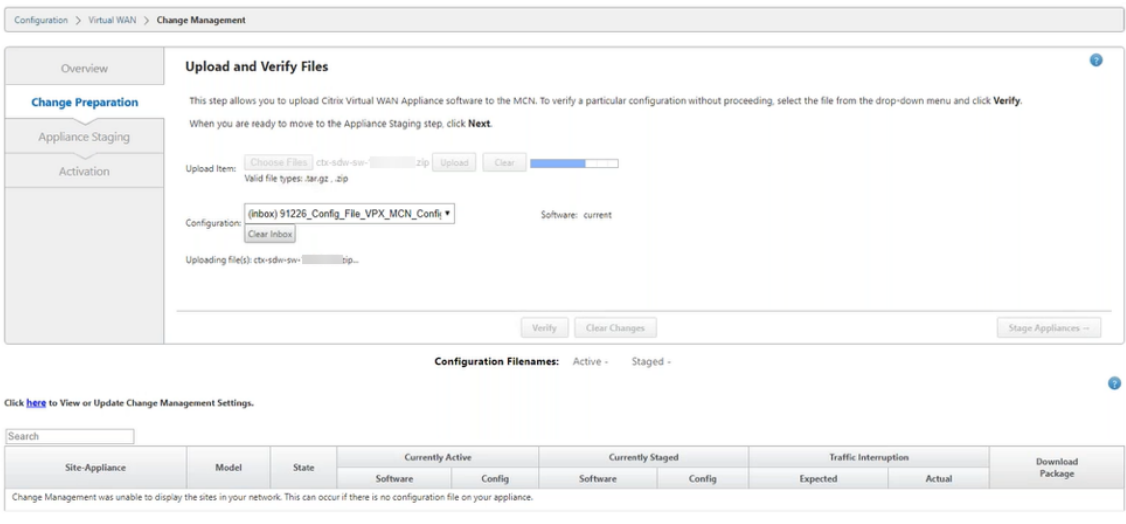
3. En la página **Administración de cambios > Preparación** de cambios, haga clic en **Elegir archivos** y seleccione el archivo de paquete de software *ctx-sdw-sw-11.0.0.x.zip*. Haga clic en **Cargar**.

> **Nota:**
>
> Puede descargar el paquete de software Citrix SD-WAN versión 11 desde la Descargas página.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

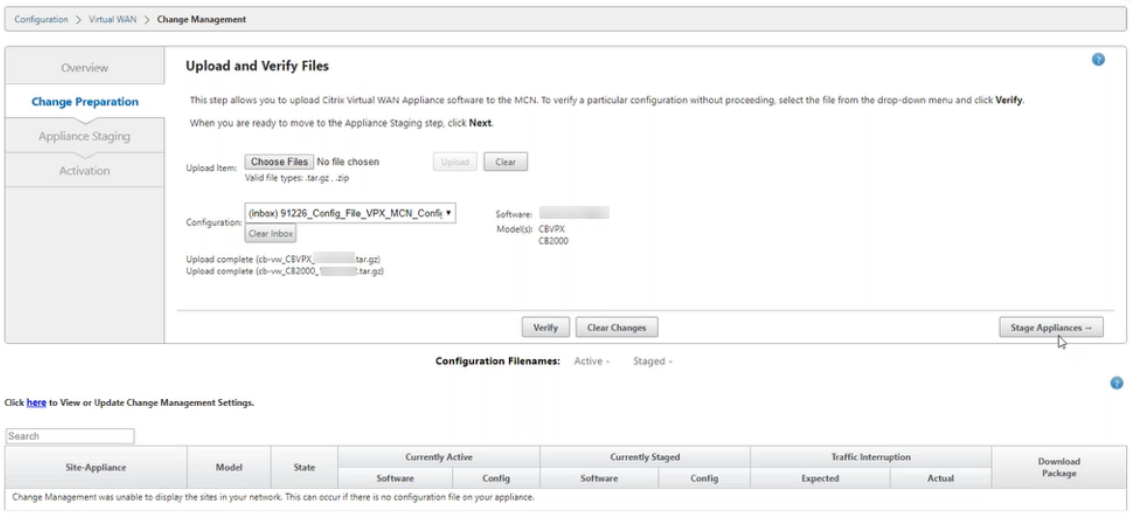


Aparece una barra de progreso para mostrar el progreso de carga actual.

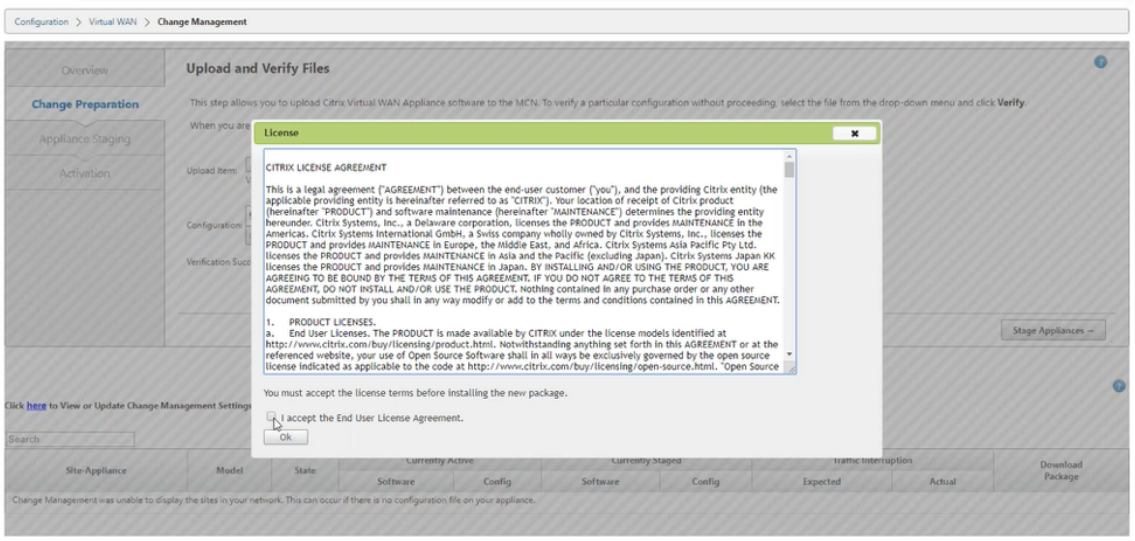


4. Después de que el proceso de carga sea correcto, se muestran modelos relevantes que se actualizarían en función del archivo de configuración que tiene información sobre cada modelo de plataforma de sucursal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

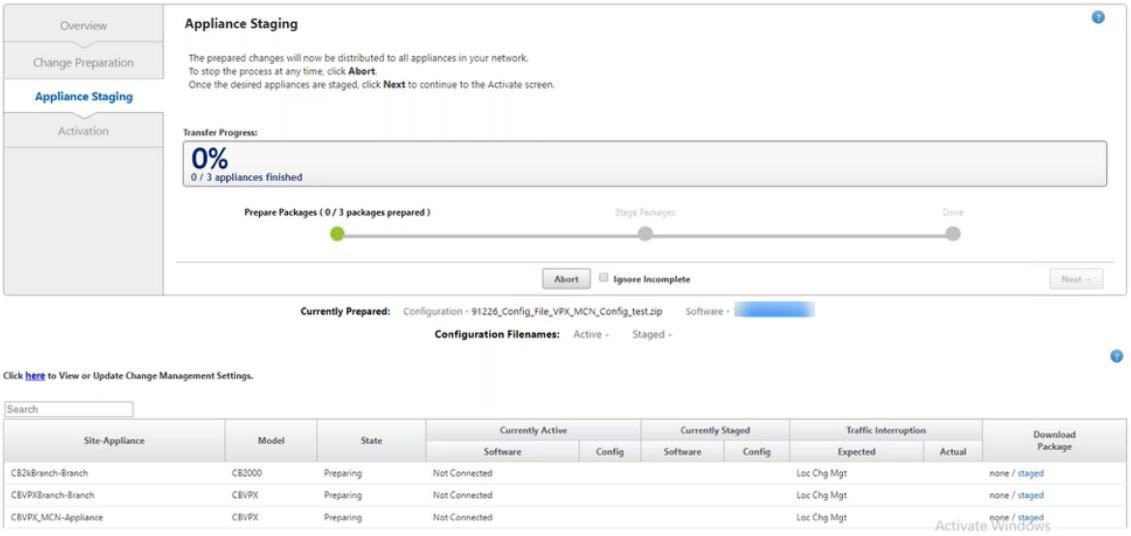


5. Haga clic en **Stage Appliance** para continuar con la validación del archivo de configuración. Aparecerá la página Contrato de licencia para la aceptación del usuario. Haga clic en **Acepto el Contrato de licencia de usuario final** y haga clic en **Aceptar**.

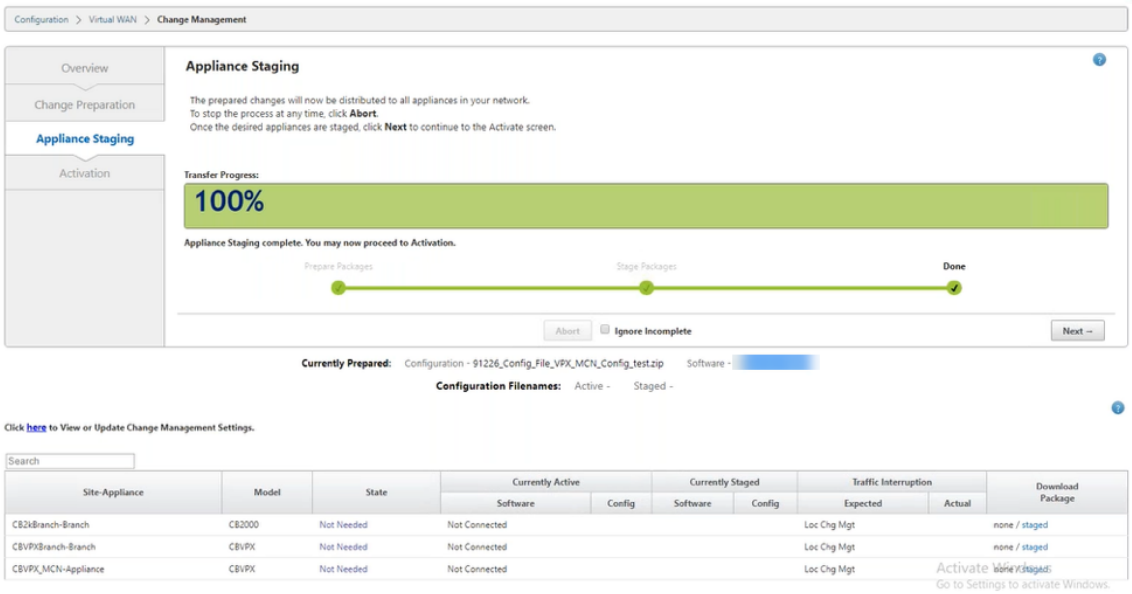


6. Se inicia el proceso de **ensayo del dispositivo**, los cambios se distribuirán a todos los dispositivos de la red. Aparece la barra de progreso de transferencia y se actualiza la tabla de detalles del sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



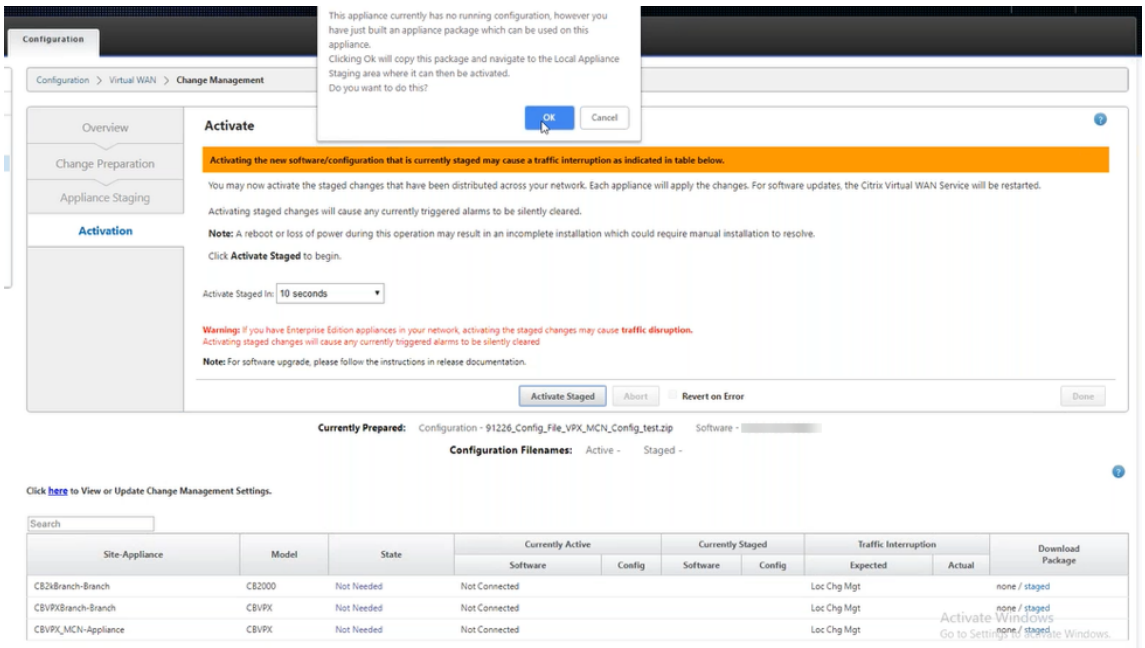
7. Una vez que el progreso de la transferencia haya finalizado al 100%, haga clic en **Siguiente** para continuar con la activación.



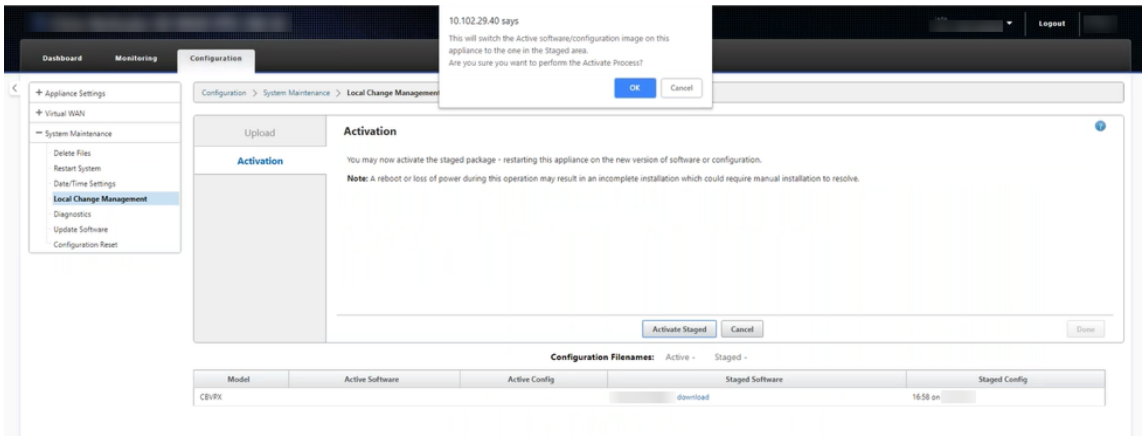
8. Haga clic en **Activar por etapas**. Aparece un mensaje emergente de aceptación del usuario, ya que es la primera vez que se realiza una puesta en escena del dispositivo.

   Se le redirigirá a la página **Administración de cambios locales** para activar el dispositivo local. Haga clic en **Aceptar** para continuar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

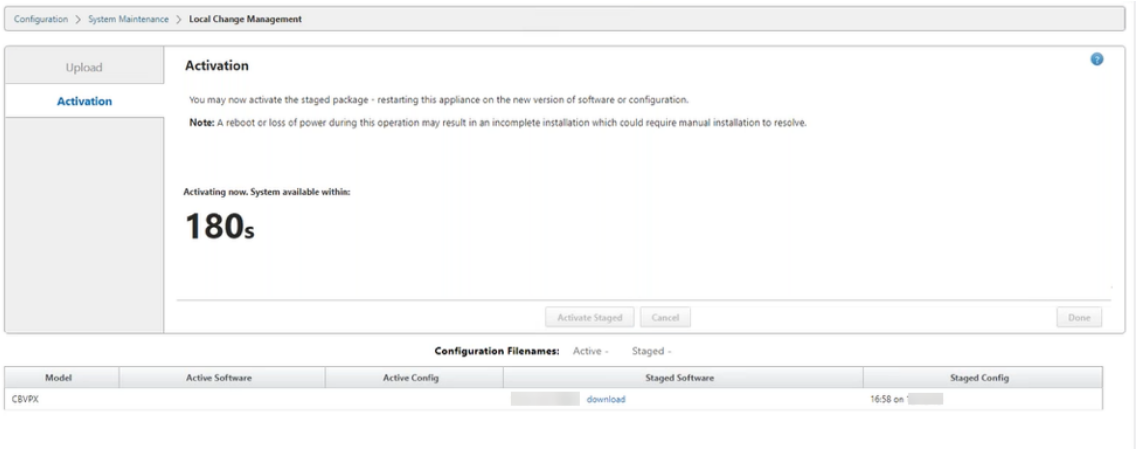


9. Haga clic en **Activar por etapas** en Administración de cambios locales. Aparecerá un mensaje de confirmación de activación. Haga clic en **OK**.

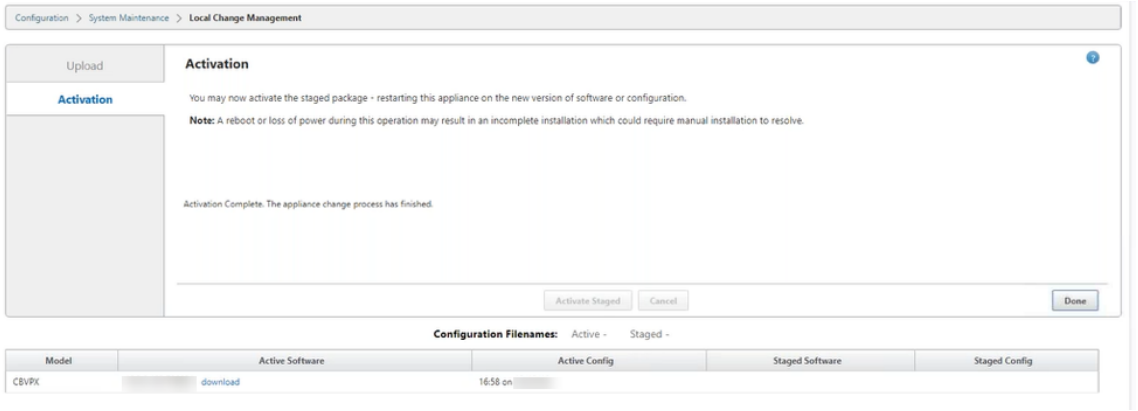


La activación comienza con un temporizador de cuenta atrás de 180 segundos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

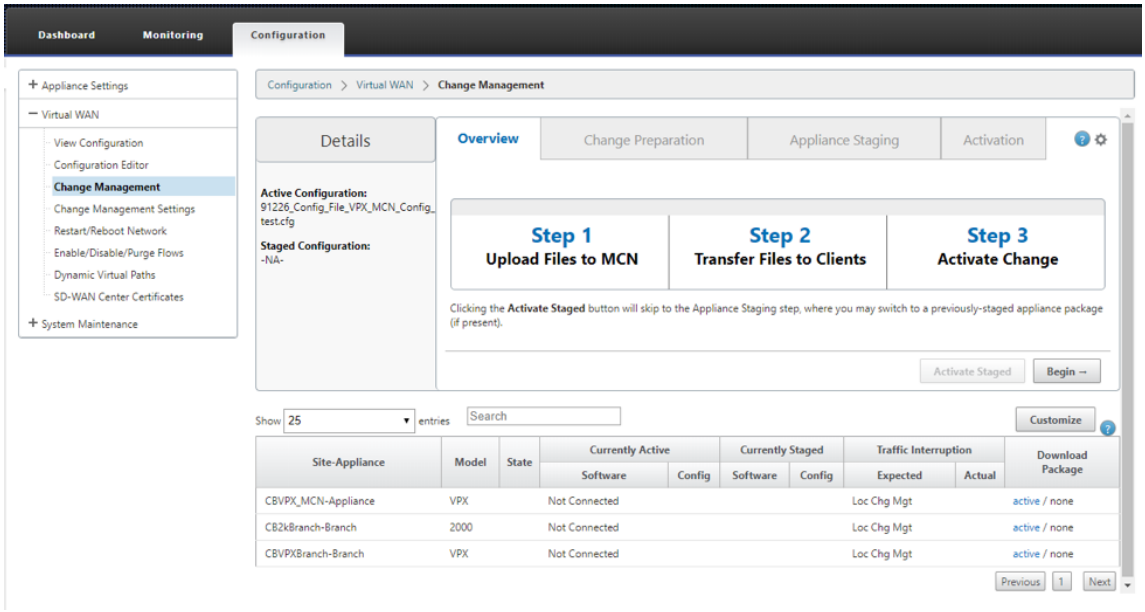


10. Después de la cuenta atrás, un mensaje indica que se ha completado la activación. Haga clic en **Listo**, el dispositivo se reiniciará.

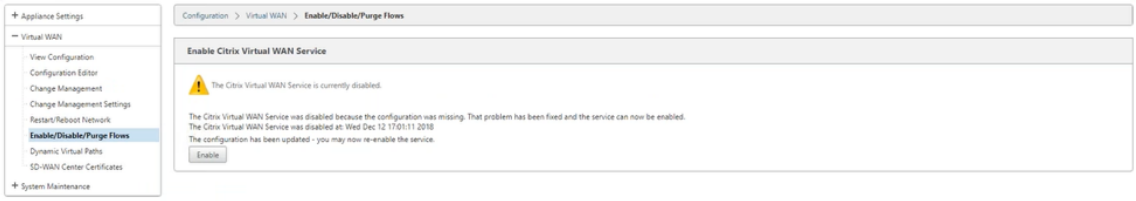


11. Una vez reiniciado el dispositivo, vaya a la página **Administración de cambios** para descargar los paquetes locales de administración de cambios para las respectivas sucursales que necesita para iniciar en la red con la actualización del software WAN virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



12. Habilite el servicio SD-WAN en el dispositivo. Vaya a **WAN virtual > Activar/Desactivar/depurar flujos** y haga clic en **Habilitar**.



Para configurar y agregar nuevos sitios a la red, siga el procedimiento en elConfigurar nodo de sucursaltema.

Reimagen del software del dispositivo Citrix SD-WAN

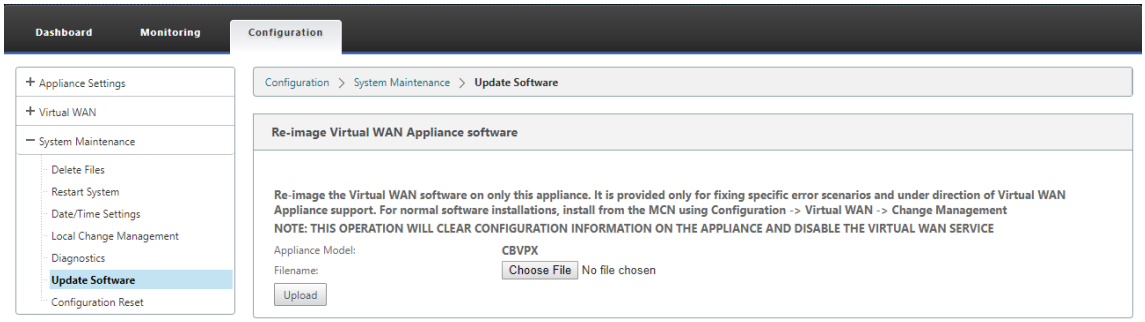
May 7, 2021

Descargue el *archivo.tar.gz* de la versión y plataforma del software Citrix SD-WAN requeridas desde el Descargas de Citrix portal.

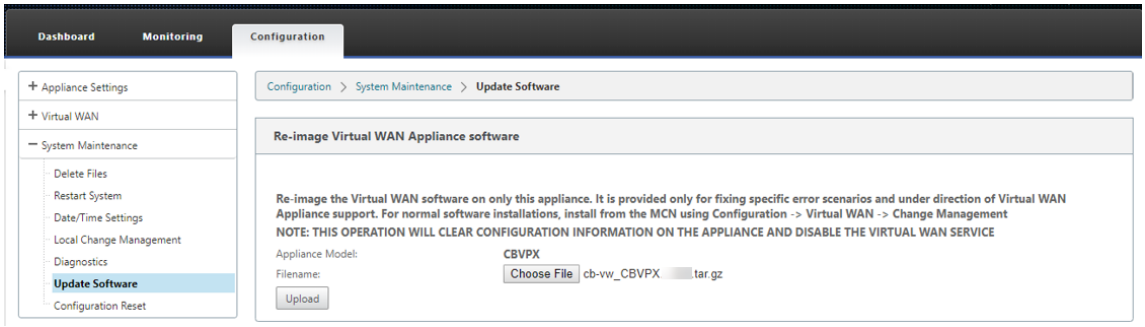
Para volver a crear imágenes del software del dispositivo Citrix SD-WAN:

1. En la GUI del dispositivo SD-WAN, vaya a **Configuración** > **Mantenimiento del sistema** > **Actualizar software**.

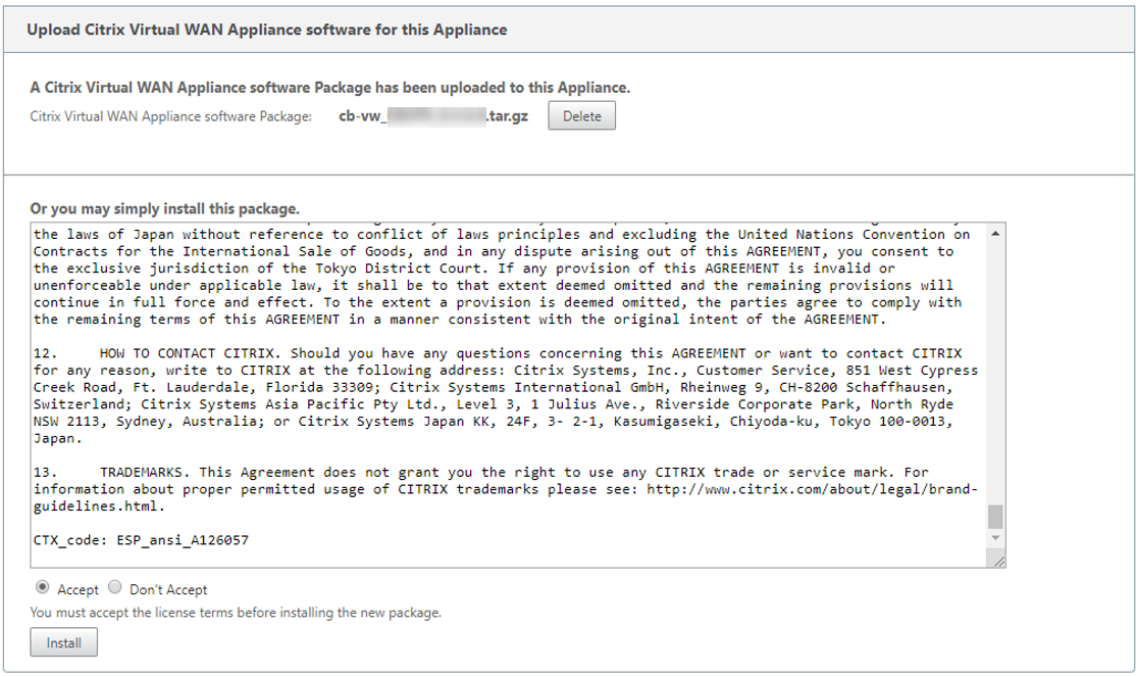
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Haga clic en **Elegir archivo** y seleccione el software del dispositivo Citrix SD-WAN descargado. Haga clic en **Cargar**.

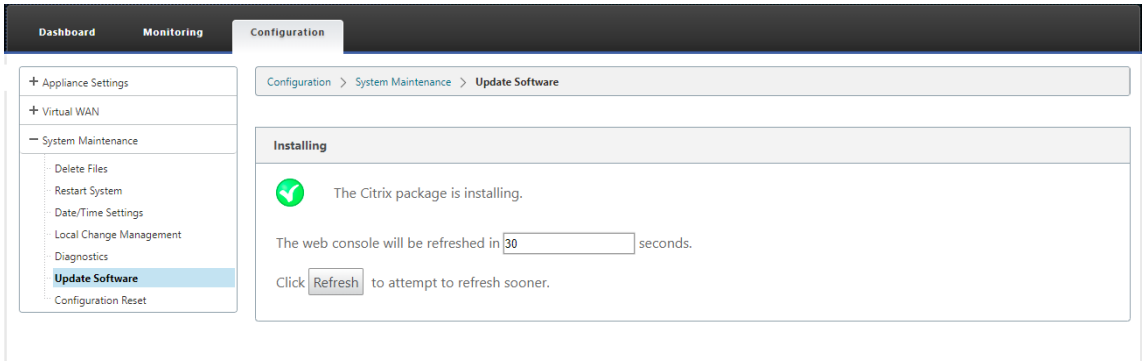


3. Lea y acepte los términos de la licencia. Haga clic en **Aceptar** y, a continuación, haga clic en **Instalar**.



La actualización de software tarda unos 35 segundos, después de lo cual el dispositivo se reinicia.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Actualización parcial del software mediante la administración de cambios local

May 7, 2021

> **Importante**
>
> De forma predeterminada, la opción **Actualización parcial de software** está inhabilitada.

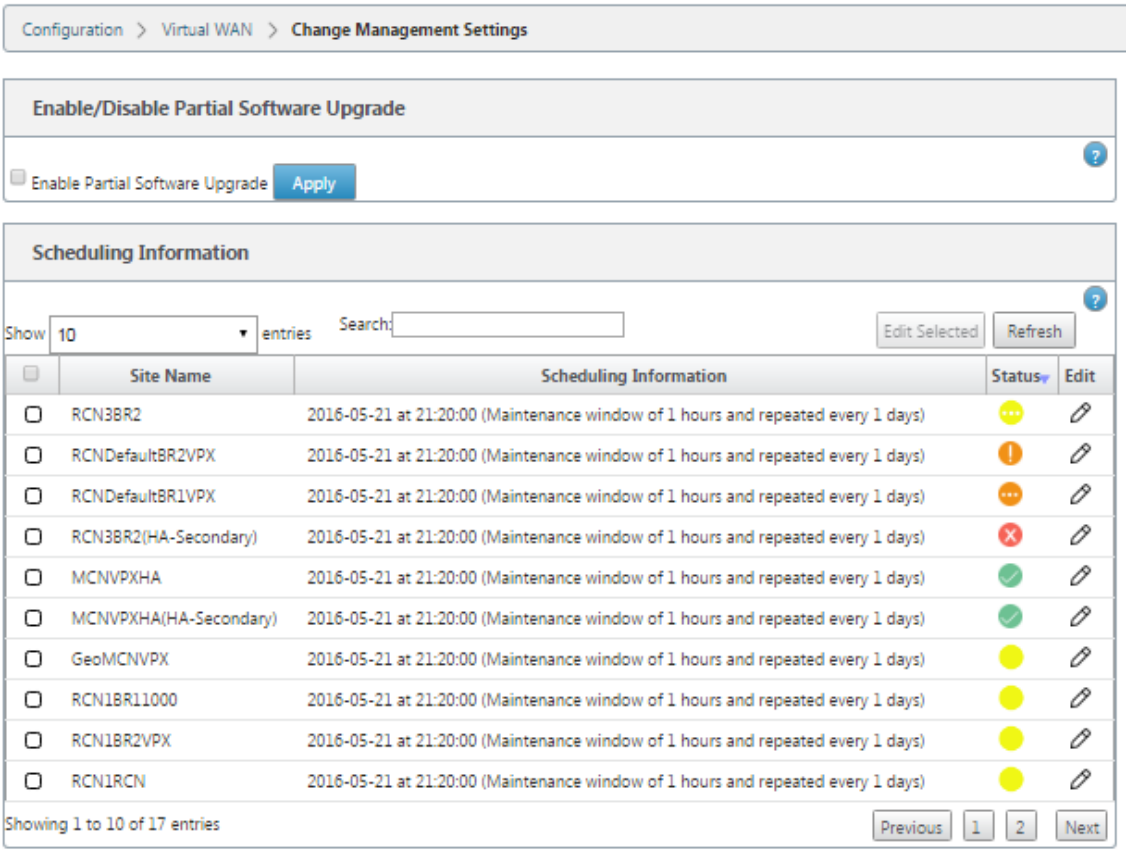
Puede instalar una versión de versión de software SD-WAN más reciente en un subconjunto de sitios cliente mediante la opción **Administración de cambios locales**. Esto se logra a través de la función de actualización parcial del software que permite al administrador de la red actualizar selectivamente el software en los sitios de la red sin necesidad de actualizar todos los sitios simultáneamente. Un caso de uso específico de esta función es que un administrador pruebe el nuevo software en algunos sitios de sucursales antes de instalarlo en todos los sitios de la red.

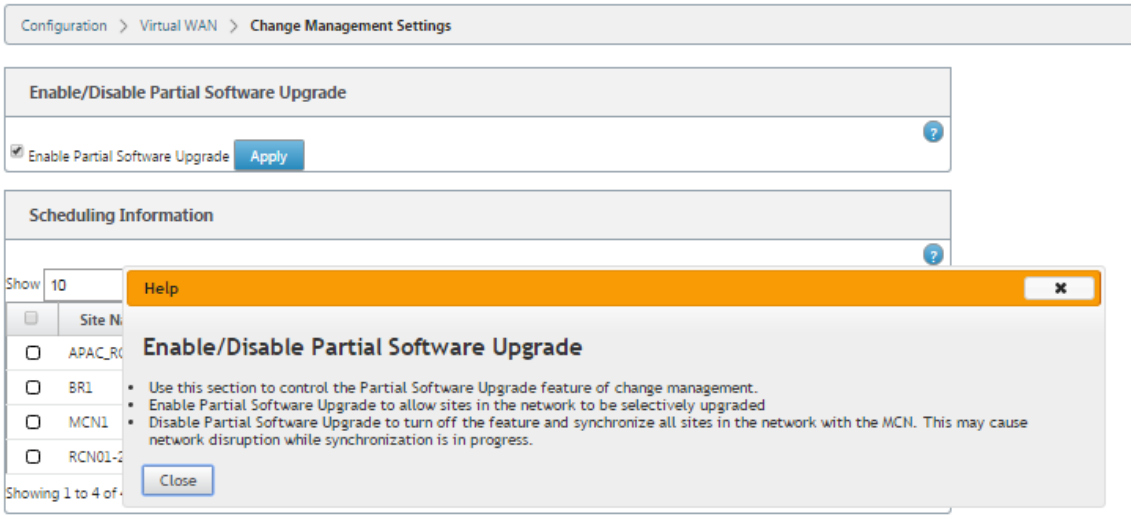
Requisitos previos y requisitos

Antes de continuar con la actualización parcial del software, revise los siguientes requisitos:

1. Tener un software SD-WAN activo versión 10.0 o posterior. Haga clic en la casilla de verificación **Habilitar actualización parcial de software**. Si desmarca la casilla, el software que se está ejecutando actualmente en el dispositivo MCN se aplica a las sucursales que tienen rutas virtuales activas en ejecución.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





2. Preconfigure una nueva versión del software mediante el proceso de **administración de cambios** de MCN con el mismo número de versión principal que el software activo y la misma configuración que la configuración activa.
3. El nuevo software debe ser la misma versión principal del software que el software activo. La versión secundaria puede ser diferente versión de software.
4. El nuevo software primero debe ser puesto en escena en todos los sitios del MCN. Deténgase en

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

el paso **Activar en etapas** de administración de cambios.

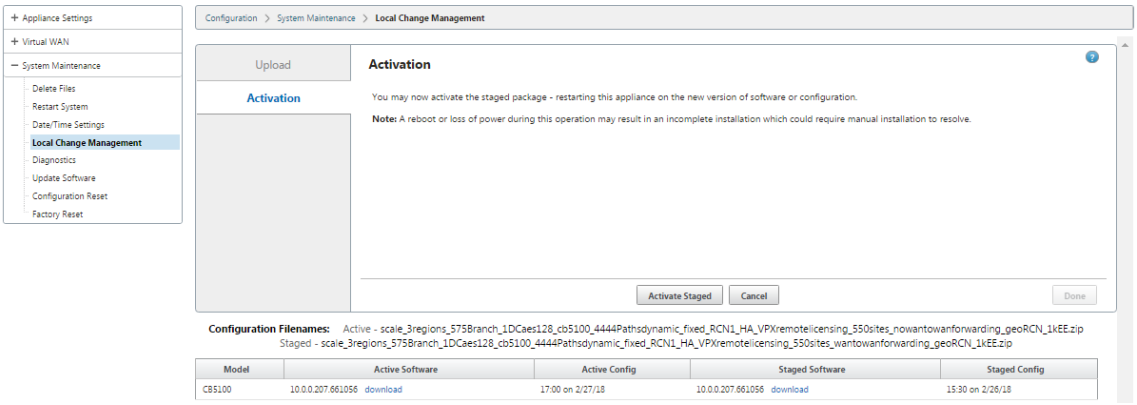
Para la configuración del sitio Activo y Parcial, el software debe ser idéntico en los sitios de MCN y Branch. No es posible tener un conjunto de funciones diferente habilitado en sitios parcialmente actualizados. Continúe con sitios individuales para realizar la **administración de cambios locales**. Consulte las instrucciones que se indican a continuación para la implementación de alta disponibilidad.

Para realizar una actualización parcial del software SD-WAN:

Hay dos casos en los que puede realizar una actualización parcial del software SD-WAN en un nodo de sucursal: El modo de alta disponibilidad y el modo de no alta disponibilidad.

Actualizar nodo de sucursal sin modo de alta disponibilidad

1. En la interfaz de administración web de Citrix SD-WAN, desplácese hasta el sitio de la sucursal, que debe actualizarse mediante el proceso de actualización parcial del sitio.
2. Abra **Administración de cambios locales**. Haga clic en **Siguiente**.
3. Haga clic en **Activar por etapas**. Cada sitio de sucursal se instalará ahora con una nueva versión de software.



Actualizar nodo de sucursal en modo de alta disponibilidad

1. En la interfaz de administración web de SD-WAN, navegue hasta el sitio de sucursal, que debe actualizarse mediante la actualización parcial del sitio.
2. Inhabilite el servicio en el dispositivo en espera.
3. En el dispositivo principal, abra **Administración de cambios locales**.
4. Haga clic en **Activar por etapas**. Este dispositivo se instalará ahora con una nueva versión de software.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. En el dispositivo en espera, abra **Administración de cambios locales**.
6. Haga clic en **Activar por etapas**. El dispositivo en espera se instalará ahora con una nueva versión de software.
7. Una vez que los dispositivos principal y en espera hayan completado el proceso de activación, habilite el servicio en el dispositivo en espera.

Actualizar red

Cuando esté listo para sincronizar la red, vaya a la pantalla de administración de cambios de red MCN y haga clic en **Activar en etapas**.

Conversión WANOP a Premium Edition con USB

May 7, 2021

> **Nota**
>
> Solo los dispositivos SD-WAN 1000 y 2000 WANOP se pueden convertir en dispositivos SD-WAN Premium Edition.

Antes de comenzar

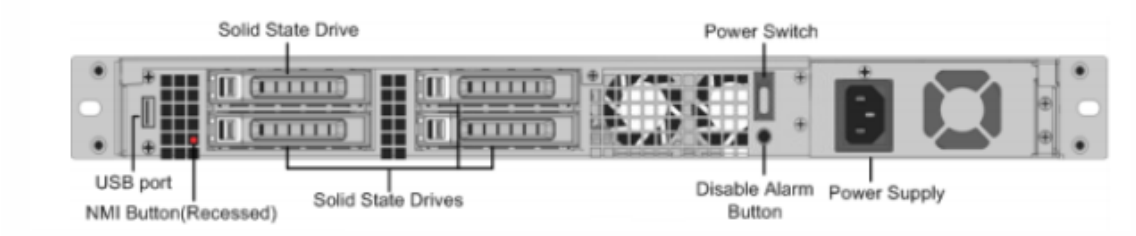
- Asegúrese de que está convirtiendo el dispositivo 1000 y no el 1000 WS. El dispositivo 1000 WS no admite la conversión al dispositivo SD-WAN Premium (Enterprise) Edition.
- Asegúrese de tener las credenciales predeterminadas para iniciar sesión en el *Dom-0 - root/ns-root*existente.

Procedimiento de actualización

El procedimiento de conversión es un proceso de dos pasos que implica los siguientes pasos:

- Inserte una memoria USB incluida en el dispositivo Citrix SD-WAN.
- Compruebe que la consola serie está conectada y continúe con el proceso de conversión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



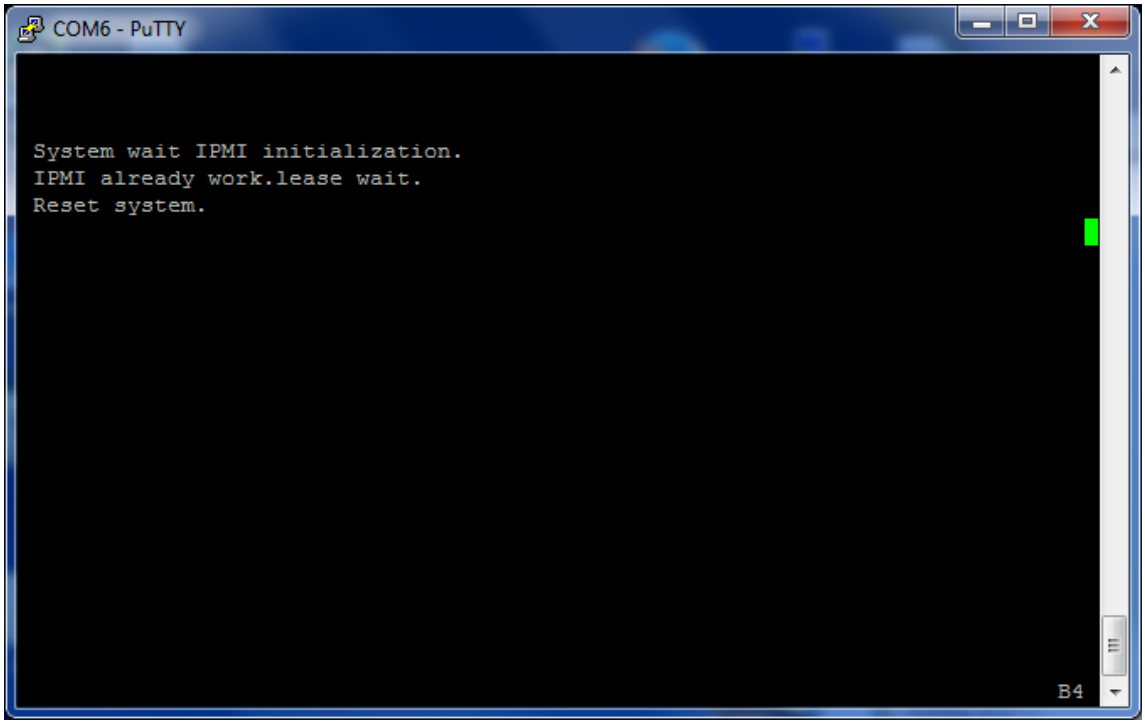
Cómo convertir con memoria USB

Para actualizar el dispositivo con una memoria USB:

1. Inserte la memoria USB incluida en el dispositivo Citrix SD-WAN.
2. Conéctese a la consola serie del dispositivo.
3. Reinicie el dispositivo.
4. Durante el proceso de arranque, cuando vea que el cursor se mueve por la pantalla, haga lo siguiente:
   a) Mantenga presionada la tecla **ESC**.
   b) Mantenga pulsada la tecla **MAYÚS**.
   c) Presione la tecla número **1** (MAYÚS +1 =!) y suelte todas las teclas.
   d) Repita los pasos a, b y c hasta que el cursor deje de moverse.

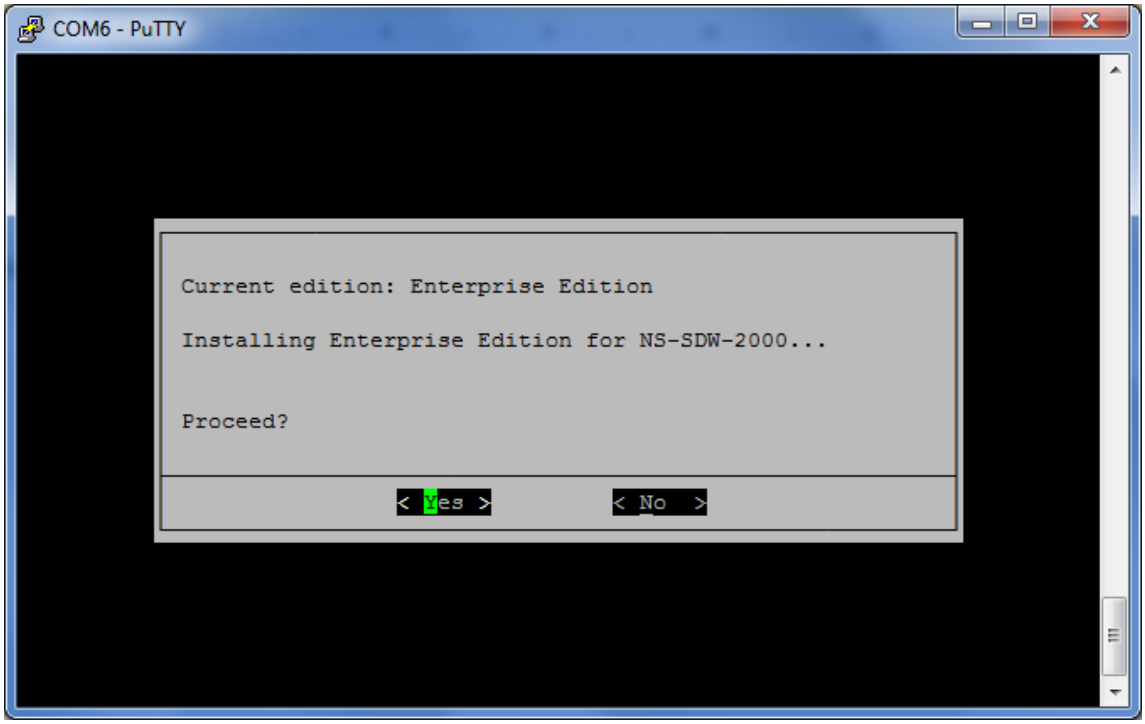
> **Nota**
>
> Los pasos anteriores deben ejecutarse durante el proceso de reinicio del dispositivo. Las pulsaciones de teclas deben ocurrir durante la etapa posterior del BIOS como se describe en el paso 4.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

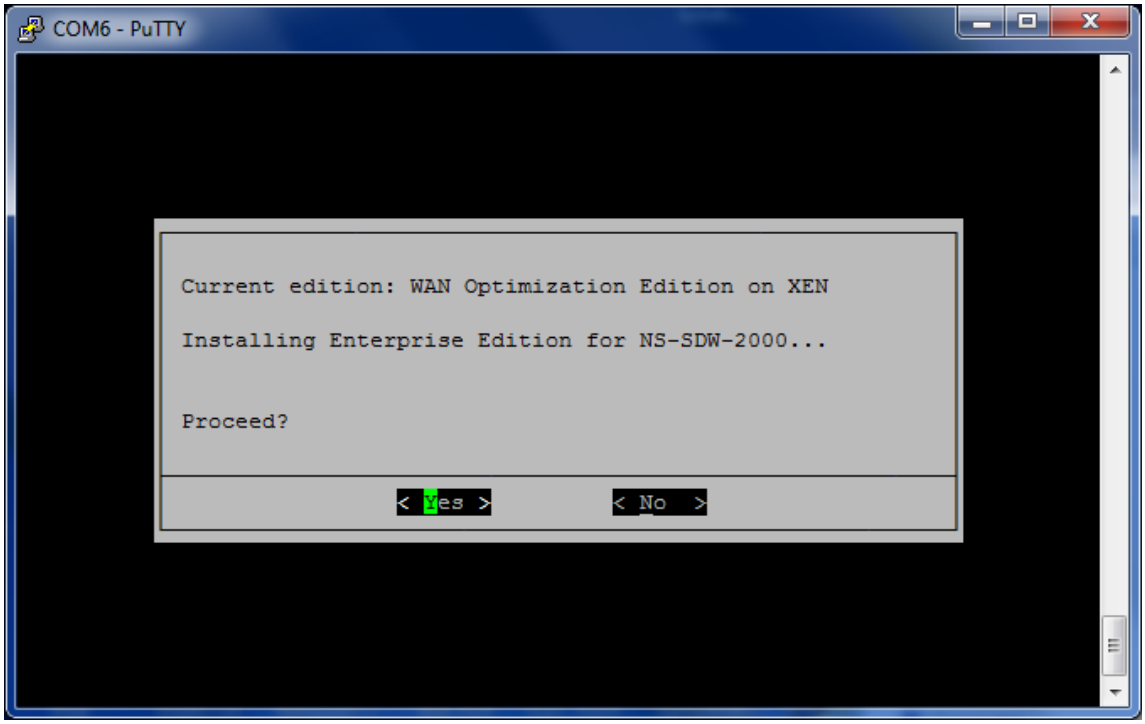


5. Cuando se cargue el BIOS, elija la unidad USB externa, por ejemplo, PNY USB 2.0 FD 1100 para arrancar el dispositivo. Citrix envía la unidad USB externa si lo ha pedido.

   Debe elegir la edición de plataforma que quiere utilizar, si la plataforma admite más de una edición, como 1000 y 2000. Por lo tanto, elija Premium (Enterprise) Edition primero antes de confirmar.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Seleccione la opción de actualización de software **Enterprise Edition** cuando se le solicite.
7. El proceso de actualización se completa en 20-30 minutos. El sistema se reinicia después de 1-2 minutos y se muestra el mensaje de inicio de sesión. Para la edición de la plataforma 1000, el proceso de actualización es de aproximadamente una hora, ya que la actualización de la unidad USB interna dura aproximadamente media hora.
8. Desenchufe la memoria USB una vez completado el procedimiento.

Referencias

- Para obtener licencias sobre los productos Citrix SD-WAN, consulte el vínculo de soporte en: http://support.citrix.com/article/ctx131110
- Para obtener información sobre documentación y notas de versión acerca de Citrix SD-WAN, consulte Documentación de SD-WAN.

Convertir Edición Estándar a Edición Premium

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Importante**
>
> En la versión 10.1, la edición de la plataforma “Enterprise”se cambia de nombre al término “Premium”.

Para realizar la conversión de plataforma de Standard Edition a Premium (Enterprise) Edition:

1. Exporte la configuración localmente.
2. Descargue el **paquete activo** desde la página **Gestión de cambios**.
3. Actualice el dispositivo mediante el paquete descargado desde **Mantenimiento del sistema** > **Actualizar software** > **Volver a crear imágenes del software Virtual WAN Appliance**.
4. Haga clic en **Elegir archivo** para proporcionar el archivo *CB-vw_cb1000_x.x.x.x.tar.gz*. Donde x.x.x.x es la versión del software SD-WAN.
5. Haga clic en **Cargar**. Seleccione **Aceptar** y haga clic en **Instalar** para continuar.
6. Instale la licencia Premium (Enterprise) Edition.
7. Realice la **administración de cambios locales** en el dispositivo mediante el paquete activo descargado en el paso 2 anterior.

Las siguientes son las condiciones para el aprovisionamiento de Optimización de WAN:

1. Si el rol de sitio es MCN, el aprovisionamiento de Optimización de WAN solo ocurre:
   - La actualización de software se realiza utilizando el paquete.zip (SSUP)
   - La licencia es PE
   - El servicio Virtual WAN está habilitado
2. Si el rol de sitio es Cliente, el aprovisionamiento de Optimización de WAN sólo ocurre:
   - La actualización de software se realiza utilizando el paquete.zip (SSUP)
   - El servicio Virtual WAN está habilitado
   - La licencia es PE
   - Ruta virtual se forma con MCN
3. Para el aprovisionamiento inmediato de Optimización de WAN, establezca el valor de la ventana de mantenimiento en 0 desde la página Cambiar configuración de administración para el sitio correspondiente.

Utilidad de reimagen USB

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La utilidad de reimagen USB de SD-WAN permite reutilizar el hardware mediante la instalación de una imagen limpia de fábrica desde una memoria USB de arranque. Citrix proporciona una unidad reemplazable en campo (FRU) de memoria USB con una imagen de software SD-WAN precargada. Utilice la FRU USB para volver a crear la imagen del dispositivo en las ediciones compatibles necesarias (SE/PE/AE). La licencia o configuración del dispositivo utilizada determina la edición del dispositivo.

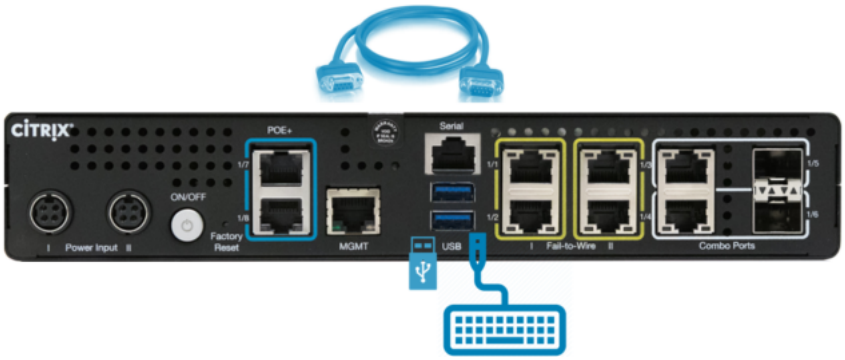
La siguiente tabla proporciona detalles sobre las imágenes FRU USB disponibles y las ediciones compatibles con los dispositivos SD-WAN.

Dispositivo	Imagen USB FRU	Ediciones admitidas
Citrix SD-WAN 110	11.1.1.39	SE
Citrix SD-WAN 210	10.2.7.17	SE, AE
Citrix SD-WAN 410	10.2.3.32	SE
Citrix SD-WAN 1100	10.2.7.17	SE, PE, AE
Citrix SD-WAN 2100	10.2.7.17	SE, PE
Citrix SD-WAN 4100	10.2.7.17	SE
Citrix SD-WAN 5100	10.2.7.17	SE, PE
Citrix SD-WAN 6100	10.2.7.17	SE, PE

Para realizar una reimagen USB:

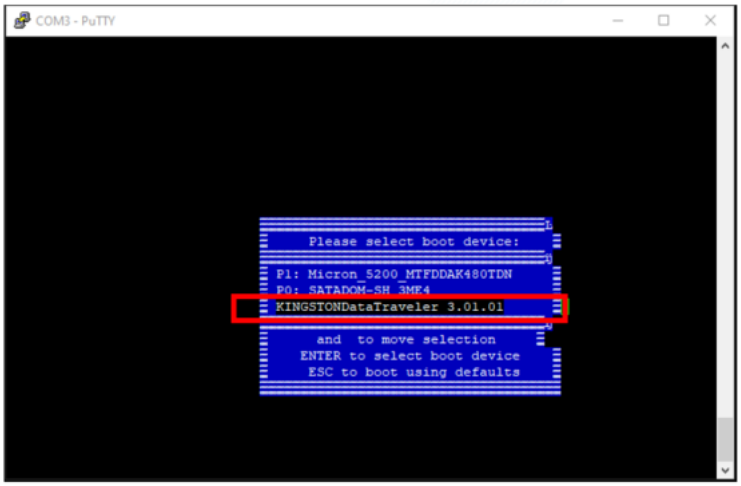
1. Inserte la memoria USB proporcionada por Citrix en uno de los puertos USB del dispositivo.
2. Conecte un teclado USB a otro puerto USB.

> **Sugerencia**
>
> Si hay un único puerto USB en el dispositivo, utilice un divisor USB para conectar la memoria USB y el teclado USB.

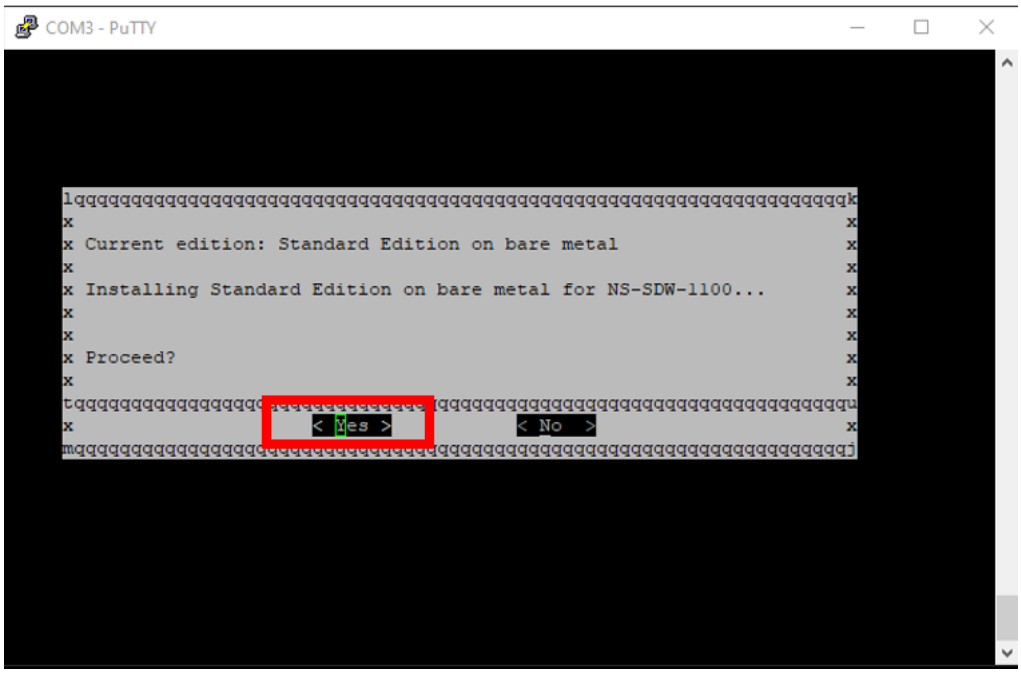


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Inicie sesión en la consola serie como administrador y ejecute el comando reboot appliance a través de la CLI.
4. Al arrancar, presione continuamente la tecla **F11** del teclado conectado por USB o **SHFT+ESC+1** a través de la conexión de consola serie.
5. Seleccione la unidad USB en el menú del dispositivo de arranque y presione Entrar.



6. Dependiendo de la edición soportada para la plataforma aparece una pantalla solicitando permiso para continuar con la instalación. Seleccione **Sí**.



> **Nota**
>
> Para la reimagen de PE y AE, el dispositivo puede aparecer en la GUI como Standard Edition

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> hasta que finalice la instalación adecuada de la licencia de SO y PE/AE.

La instalación tarda 30 minutos en completarse. No apague el dispositivo durante el proceso de reimagen. Puede reiniciarse varias veces.

7. La imagen de fábrica tiene DHCP habilitado de forma predeterminada. La dirección IP de administración predeterminada en todas las plataformas es 192.168.100.1. Úsalo para acceder a la GUI de SD-WAN.

   También puede configurar manualmente la IP de administración desde la consola serie ejecutando los siguientes comandos:

   Ejecute el comando '*management_ip*'

   Ejecute el comando '*set interface 192.168.100.1 255.255.255.0 192.168.100.254*'

   Ejecute el comando '*apply*'

8. El software, de forma predeterminada, se actualiza a SE. Instale la licencia PE o AE según sea necesario, dependiendo de las ediciones admitidas por el dispositivo.

   > **Nota**
   >
   > Solo puede configurar y administrar las capacidades de AE a través de SD-WAN Orchestrator. Para obtener más información, consulte Seguridad perimetral.

Opciones de licencia de Citrix SD-WAN

May 7, 2021

Hay tres ediciones Citrix SD-WAN cada una con un conjunto o subconjunto diferente de funciones SD-WAN. El tipo de licencia que instala determina la edición de la plataforma: Los dispositivos Standard Edition, WANOP y Premium Edition.

> **Nota**
>
> Al instalar y aplicar una licencia, asegúrese de que su dispositivo específico es compatible con la edición del dispositivo SD-WAN que quiere habilitar y de que dispone de la versión de software correcta disponible.

Compatibilidad con el software de la plataforma Citrix SD-WAN

En la siguiente tabla se muestran las plataformas Citrix SD-WAN compatibles con cada una de las versiones de software SD-WAN disponibles.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> En la versión 10.2, la edición de la plataforma Enterprise se cambia de nombre a la edición Premium.

Versión	Edición de optimización de WAN	Standard Edition	Premium Edition
Versión 7.x	Sí	No	No
Versión 8.x	No	Sí	No
Versión 9.0, 9.1, 9.2, 9.3	Sí	Sí	Sí
Versión 10.0, 10.1, 10.2	Sí	Sí	Sí
Versión 11.0	Sí	Sí	Sí

Para ver todos los modelos de dispositivos compatibles con Citrix SD-WAN versión 11.0, consulte Hoja de datos de Citrix SD-WAN.

Los modelos VPX-WANOP permiten licencias de ancho de banda de 2, 6, 10, 20, 50, 100 y 200 Mbps. Se requieren al menos dos CPU de 2,1 GHz para admitir las instancias VPX.

Antes de poder descargar el software, debe obtener y registrar una licencia de software de Citrix SD-WAN. Para obtener instrucciones sobre cómo obtener una licencia de software SD-WAN, póngase en contacto con el servicio de atención al cliente de Citrix. Las instrucciones para cargar e instalar el archivo de licencia en sus dispositivos se proporcionan en la sección,Carga e instalación del archivo de licencia del software SD-WAN. Antes de instalar la licencia, primero debe configurar el hardware del dispositivo y establecer la fecha y hora del dispositivo.

El procedimiento de licencia para el Provisioning de licencias para las ediciones de la plataforma SD-WAN abarca los siguientes temas:

- Modelo de licencia SD-WAN compatible: Local, Remoto y Centralizado.
- Compatibilidad con el servidor de licencias remoto para dispositivos SD-WAN.
- Requisitos previos para usar el Servidor de licencias remoto.

> **Nota**
>
> A partir del 4 de noviembre de 2020, hay un cambio en el proceso «Devolución y modificación de licencias de Citrix». Con este nuevo proceso, no puede devolver ni modificar sus licencias a través del portal Administrar licencias de Citrix.com y Mis herramientas de licencia en Partner Central.
> Para obtener más información y lista de casos de uso, consulte Artículo KB CTX285157.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Licencias locales

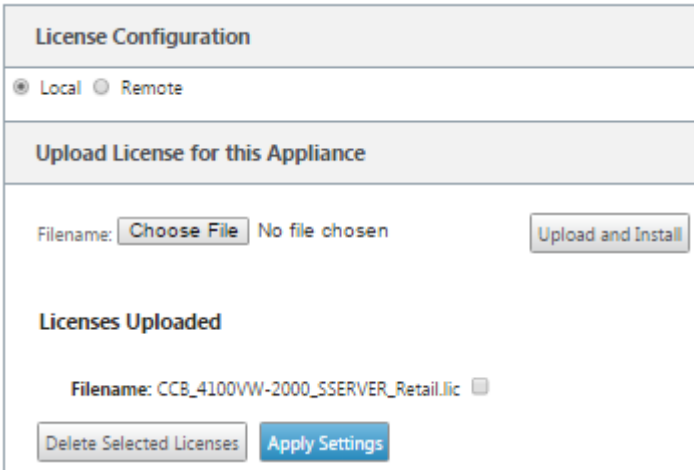
May 7, 2021

Con la licencia local, debe iniciar sesión en cada dispositivo de la red y cargar el archivo de licencia. Incluso con el servicio ZTD, el dispositivo solo estará disponible con una licencia de gracia. Tendrá que cargar un archivo de licencia para la conexión de red activa. Los archivos de licencia se generan en función de los ID de host de los dispositivos individuales.

Puede instalar y configurar licencias para dispositivos SD-WAN mediante la interfaz de administración web de SD-WAN.

Importación de licencias para dispositivos SD-WAN implementados en plataformas XenServer/ESXI/Hyper-V:

1. En la interfaz de administración web de SD-WAN, vaya a **Configuración > Configuración del dispositivo > Licencias**.
2. Seleccione **Local** y cargue la licencia. Haga clic en **Upload and Install** (Cargar e instalar).
3. Guarde los cambios haciendo clic en **Aplicar configuración**.



Licencias remotas

May 7, 2021

Requisitos previos para utilizar el servidor de licencias remoto para dispositivos SD-WAN.

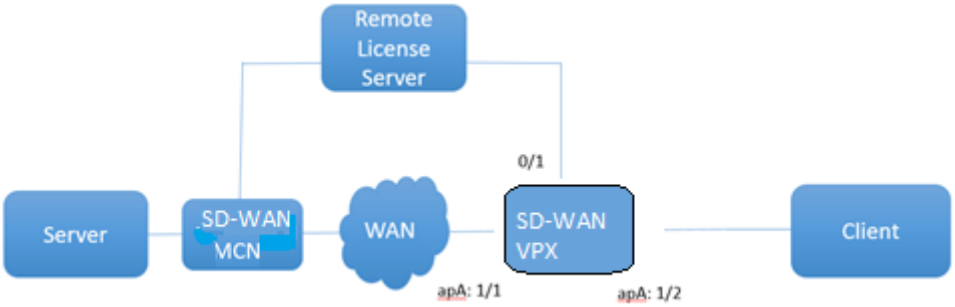
- NTP debe configurarse tanto para el servidor de licencias como para SD-WAN (la fecha y la hora deben estar sincronizados)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

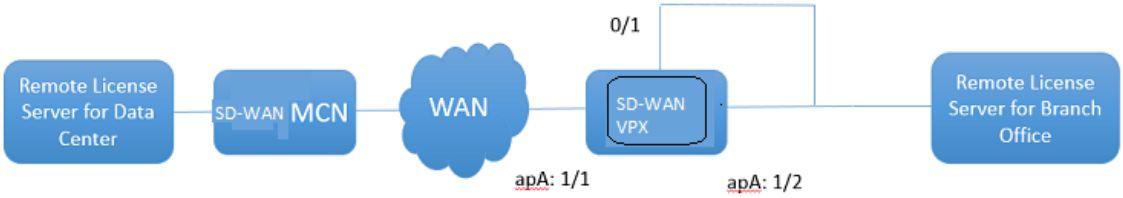
- Se recomienda utilizar la versión más reciente del servidor de licencias:
  - Versión 9.1, 9.2:11.13.1 L.S
  - Versión 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2:11.14.1 L.S
  - Versión 11.0.3:11.16.3 L.S

Casos de uso:

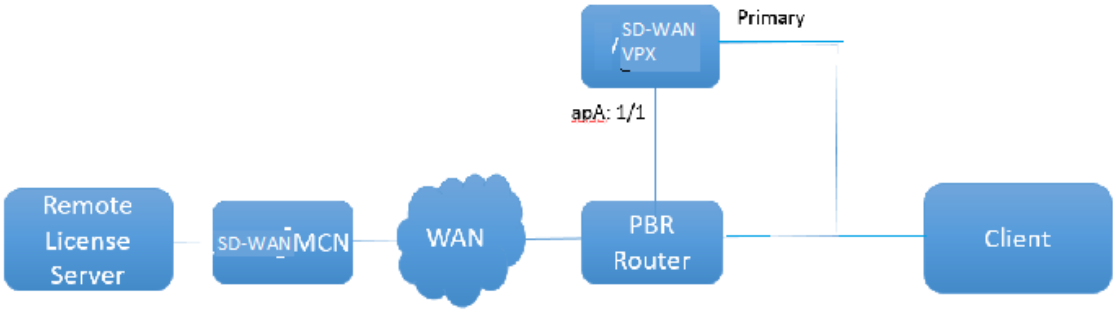
1. Servidor de licencias remoto accesible a través de la red de administración sin utilizar puertos de datos/APA.



2. Servidor de licencias remoto en la red de sucursales.



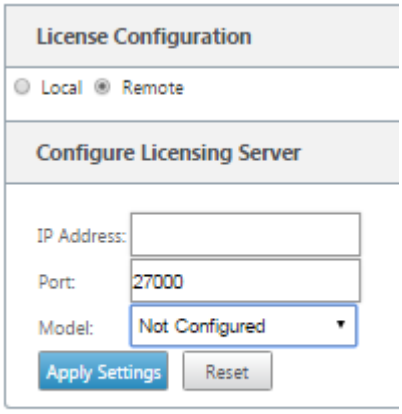
3. SD-WAN VPX-SE: Implementación de PBR en la sucursal.



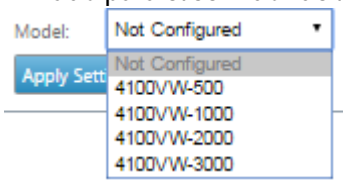
Licencia remota:

1. En la interfaz de administración web de SD-WAN, vaya a **Configuración > Configuración del dispositivo > Licencias**.
2. Seleccione **Remoto** e introduzca los detalles de la dirección IP del servidor remoto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Seleccione el **modelo** de dispositivo deseado en el menú implementable. El puerto predeterminado para el servidor de licencias remoto es 27000.



> **Importante**
>
> Si quiere instalar licencias remotas para el dispositivo SD-WAN mediante SD-WAN Center, asegúrese de habilitar las licencias centralizadas en el dispositivo SD-WAN MCN en la configuración global del Editor de configuración de la interfaz de administración web de SD-WAN.

Licencias centralizadas

May 7, 2021

A medida que las implementaciones de red crecen con un gran número de nodos de red, la administración y la concesión de licencias de dispositivos se vuelven engorrosos. Para simplificar este proceso de incorporación eficiente de los dispositivos SD-WAN y operaciones de red sencillas, se ha introducido un modelo centralizado de licencias para la red SD-WAN.

En el nuevo modelo de licencia centralizado, la interfaz de administración web dSD-WAN Center (portal de administración y generación de informes de dispositivos SD-WAN) proporciona servicios de licencias a dispositivos SD-WAN individuales de la red sin tener que iniciar sesión en el dispositivo.

La dirección IP dSD-WAN Center se proporciona en la interfaz gráfica de usuario del dispositivo SD-WAN en **Global > Centralizada Licencias**. Esta dirección IP se propaga a dispositivos individuales

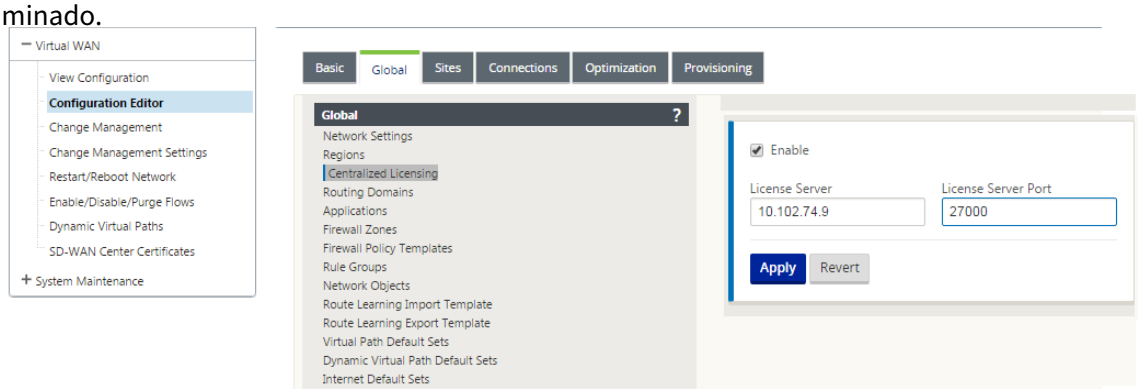
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a través de paquetes de configuración o actualizaciones. Cuando se cambia la dirección IP, debe pasar por el proceso de administración de cambios para insertar dispositivos. La configuración global puede ser anulada por la configuración local del sitio.

El ancho de banda de licencia se puede seleccionar con el modelo de dispositivo para la configuración del sitio. El ancho de banda de enlaces WAN se audita con la licencia seleccionada.

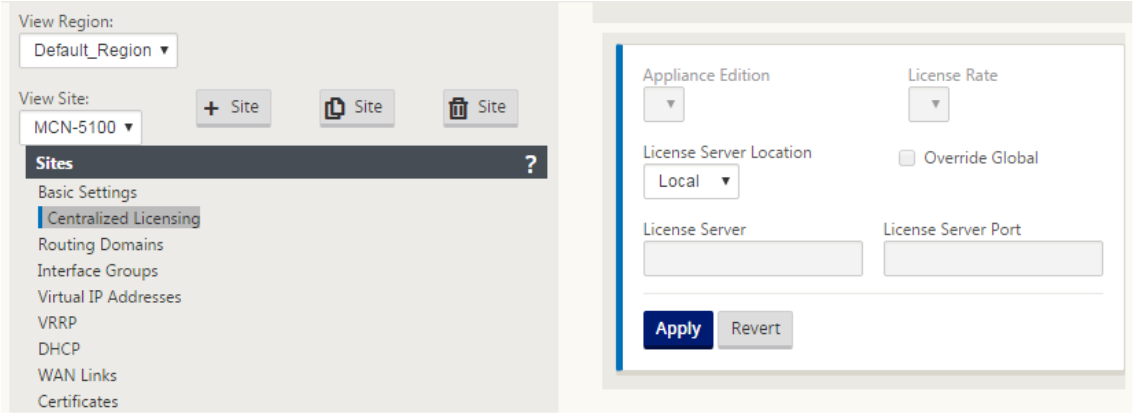
Para habilitar las licencias centralizadas en la GUI del dispositivo SD-WAN:

1. Vaya a **Configuración** > **WAN virtual** > **Editor de configuración**. Abra un paquete de configuración WAN virtual existente o cree uno nuevo. Se abrirá el paquete de configuración.
2. Acceda a la ficha **Global**. Seleccione **Licencias centralizadas**. Haga clic en **Habilitar**.
3. Introduzca la dirección IP del servidor de licencias desde la que puede descargar y administrar licencias SD-WAN. Proporcione la dirección IP de administración de SD-WAN Center, de modo que el paquete de configuración para el MCN de SD-WAN o los dispositivos de sucursal pueda descargar la licencia desde SD-WAN Center.
4. Escriba **27000** para el **puerto del servidor de licencias**, que es un número de puerto predeterminado.

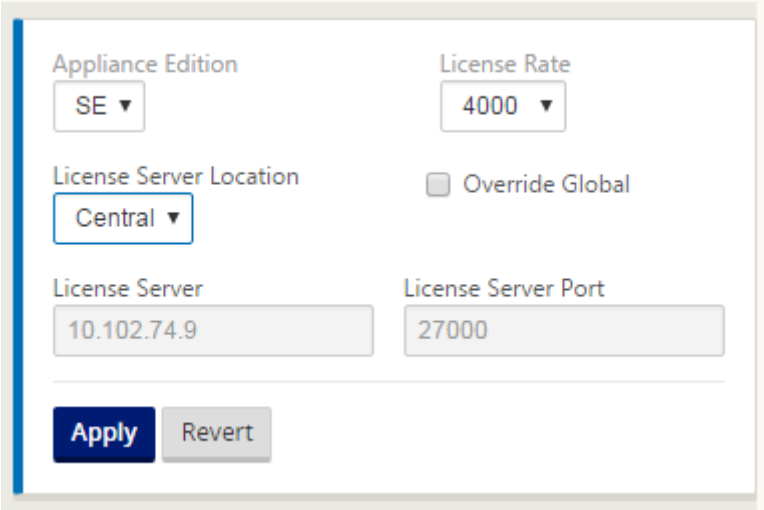


5. Haga clic en **Aplicar**.
6. Acceda a la ficha **Sitios**. Seleccione MCN o sitio de sucursal en **Ver sitio**, dependiendo de la región y el sitio para el que quiera administrar las licencias centrales.
7. Seleccione **Licencias centralizadas**. Aparecerá la vista central de opciones de licencia. De forma predeterminada, la opción **Local** está seleccionada para la **Ubicación del servidor de licencias**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

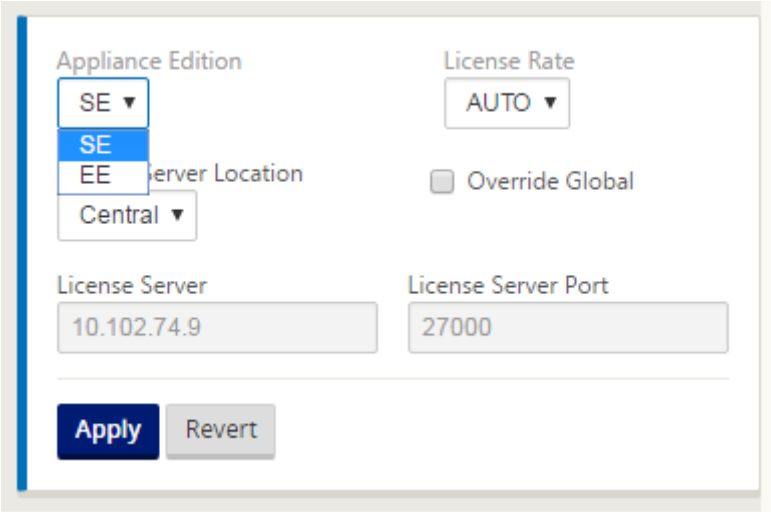


8. Haga clic en el menú implementable y seleccione **Central** para cambiar la ubicación predeterminada del servidor de licencias. Muestra la dirección IP y la información de puerto que proporcionó para el servidor de licencias cuando habilita la licencia central en la configuración Global. Por ejemplo,; el servidor de licencias podría ser la dirección IP dSD-WAN Center que administra los dispositivos de la red.



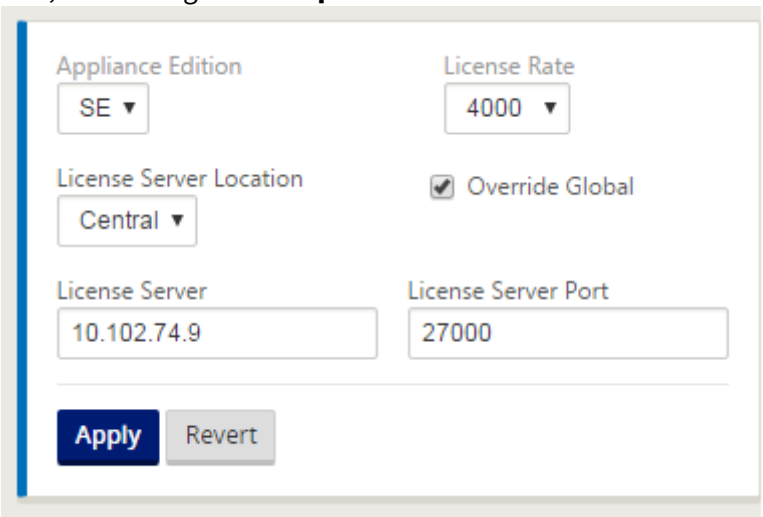
9. Elija la **edición del dispositivo** y la **tasa de licencia** en función de los dispositivos que se instalarán. Haga clic en **Aplicar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nota: Puede optar por anular la información del servidor de licencias proporcionada en la configuración Global de la configuración.

10. Seleccione **Anular global** para anular la configuración global. Configure la nueva dirección IP del servidor de licencias. Conservar el número de puerto predeterminado del servidor de licencias; 27000. Haga clic en **Aplicar**.



Ahora puede administrar licencias para todos los nodos de los sitios de sucursal y MCN configurados para un paquete de configuración de dispositivo SD-WAN específico desde el servidor de licencias que haya configurado.

El servidor de licencias puede ser un portal de administración de SD-WAN Center que adquiere licencias obtenidas de la configuración de red a los sitios a través del proceso de administración de cambios.

Licencia basada en la asignación de ancho de banda:

Cada dispositivo puede elegir una licencia con un nivel de ancho de banda superior o igual al ancho

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de banda configurado. Si la licencia de ancho de banda configurada no está disponible, se agrega la capacidad de un dispositivo para elegir la siguiente licencia de ancho de banda superior. Esta capacidad es válida tanto para la funcionalidad del servidor de licencias centralizado como remoto. Por ejemplo:

- Si tiene tres licencias de 410-200 Mbps. Utilizaría las mismas licencias para todas las asignaciones de ancho de banda asociadas con el dispositivo 410. El sitio A (20 Mbps), el sitio B (50 Mbps) y el sitio C (200 Mbps) deberían poder usar licencias de 410 a 200 Mbps.
- Si tiene una licencia de 410-20 Mbps y una licencia de 410-200 Mbps. El sitio A está configurado para consumir 50 Mbps, entonces el sitio A puede usar una licencia de 410 a 200 Mbps.

Período de gracia de licencia:

El período de gracia permitido es de 30 días cuando se quita el archivo de licencia o la configuración de licencia del dispositivo. Las alertas Grace son compatibles con Syslog y correos electrónicos.

> **Nota**
>
> Cuando la tasa de licencia seleccionada no coincide con la velocidad de enlace WAN configurada, se muestra el siguiente mensaje en la interfaz gráfica de usuario del dispositivo para eventos de licencia.
>
> Mensaje: La velocidad total configurada permitida (LAN a WAN) NNN (Kbps) no debe exceder el doble de la velocidad de licencia que es NNNN (Kbps)
>
> Gravedad: ADVERTENCIA
>
> Eventos: Syslog, Email

Administración de licencias

May 7, 2021

Las licencias de los dispositivos Citrix SD-WAN se administran mediante la comunicación con el servicio de licencias remoto para comprobar si existen licencias. Si el dispositivo tiene licencia, las operaciones de red continúan sin interrupción. Si el dispositivo no tiene licencia, se inicia el modo de licencia de gracia.

Proceso de administración de licencias del dispositivo SD-WAN:

1. Cada sitio se comunica con el servidor remoto o SD-WAN Center mediante la interfaz de administración web. Esta comunicación se produce a través de un mecanismo de latido para supervisar la conectividad y un mecanismo de retirada que verifica el estado de la licencia.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Los latidos del corazón se envían a través de una conexión TCP al servidor de licencias cada 10 a 20 minutos para comprobar la conectividad.
3. Después de una pérdida de dos latidos cardíacos consecutivos, el dispositivo entra en un modo de gracia. El método de retirada determina el estado de la licencia. Este estado puede ser "Real" , "Gracia"o "Denegado"que se envía al dispositivo desde SD-WAN Center. Cada vez que un dispositivo se pone en contacto con el SD-WAN Center para obtener el estado de la licencia, se desconecta y desconecta la nueva licencia. Si SD-WAN Center no recibe dos latidos cardíacos, SD-WAN Center libera la licencia asignada al sitio en el grupo. El período de gracia es de 30 días, por lo que después de la pérdida de 2 latidos cardíacos, el dispositivo entra en el período de gracia. Durante estos 30 días, la comunicación tiene que ser restaurada. Una vez restaurado, el dispositivo vuelve al modo de funcionamiento normal. Si NO se restablece la comunicación, el dispositivo se pone en estado sin licencia y sigue el procedimiento de caducidad sin licencia/licencia.

Licencias listas para usar (OOB) para dispositivos MCN:

- El dispositivo MCN no tendrá un período de gracia inicial. Necesita tener licencia para salir.

Licencias listas para usar (OOB) para el dispositivo cliente:

- El nodo cliente presenta un período de gracia de 30 días con o sin funcionalidad ZTD.
- El dispositivo está habilitado con un archivo de licencia OOB válido durante 30 días.
- Tiene 30 días para cargar un archivo de licencia o obtener una licencia a través del servidor de licencias centralizadas.
- Si el dispositivo tiene licencia, funciona normalmente y forma parte de la red.
- Si el dispositivo no tiene licencia en un plazo de 30 días, se sigue el procedimiento de caducidad de la licencia.

La única forma de restablecer el dispositivo para que vuelva a aparecer con la licencia OOB es realizar un "restablecimiento de fábrica. "

Caducidad de la licencia

May 7, 2021

El dispositivo SD-WAN entra en un período de gracia de 30 días y debe cargar la licencia después de que caduque la licencia.

Durante el período de gracia, todas las operaciones funcionan normalmente. Si la licencia no se carga a tiempo (30 días después de la expiración), Virtual WAN Service está inhabilitado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las licencias centralizadas tienen un archivo de registro para realizar un seguimiento del funcionamiento del período de gracia, sin licencia, con licencia, estado de comunicación y fallos.

En la GUI del dispositivo SD-WAN, en diagnóstico, está disponible la funcionalidad de prueba de conectividad MCN en SD-WAN Center a otros sitios. Esto se puede utilizar para comprobar si cada dispositivo puede llegar al servidor de licencias. Los sitios, el estado de la licencia y la tabla de estado están disponibles para administrar y realizar el seguimiento de las licencias.

Período de gracia:

1. Se proporciona un período de gracia de 30 días para los nodos cliente listos para usar. La notificación indica que el dispositivo está en modo listo para usar y necesita una licencia válida. Esta opción utiliza un archivo de licencia de gracia.
2. Caducidad de la licencia: Una vez que caduca la licencia, se proporciona un período de gracia de 30 días. La notificación indica que el motivo del período de gracia es la expiración de la licencia y necesita una renovación.
3. Pérdida de comunicación con SD-WAN Center: Después de 2 latidos cardíacos, el dispositivo pasa al modo gracia durante 30 días. La notificación indica que el motivo del período de gracia es un error de comunicación.

Configuración

May 7, 2021

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

La configuración del dispositivo SD-WAN incluye lo siguiente:

Configurar MCN: El MCN sirve como punto de distribución para la configuración inicial del sistema y cualquier cambio posterior de configuración. La mayoría de los procedimientos de actualización se realizan a través de la Interfaz Web de administración en el MCN. Solo puede haber un MCN activo en una WAN virtual.
De forma predeterminada, los dispositivos tienen el rol preasignado de cliente. 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.

Configurar sucursal: El procedimiento para agregar un sitio de sucursal es muy similar a crear y configurar el sitio de MCN. Sin embargo, algunos de los pasos y opciones de configuración varían ligeramente para un sitio de sucursal. Además, una vez que haya agregado un sitio de sucursal inicial, para los sitios que tengan el mismo modelo de dispositivo, puede utilizar la función **Clone** (duplicado) para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

optimizar el proceso de agregar y configurar esos sitios. Al igual que con la creación del sitio de MCN, para configurar un sitio de sucursal debe utilizar el **Editor de configuración** de la Interfaz Web de administración del dispositivo MCN. El **Editor de configuración** está disponible cuando la interfaz está configurada en el modo **Consola de MCN**.

Configurar ruta virtual entre MCN y sitios de sucursal: Configure el servicio de ruta virtual entre el MCN y cada uno de los sitios cliente (sucursal). Para ello, utilizará los formularios de configuración y los parámetros disponibles en el árbol de configuración de la sección **Conexiones** del **Editor de configuración**.

Habilitar y configurar la optimización de WAN: La sección proporciona instrucciones paso a paso para habilitar y configurar las funciones de optimización de WAN de SD-WAN Premium (Enterprise) Edition para su WAN virtual. Para ello, utilizará los formularios de la sección **Optimización** en el **Editor de configuración** de la interfaz de administración web en el MCN.

Configuración inicial

September 26, 2023

Estos procedimientos deben completarse para cada dispositivo que quiera agregar a su SD-WAN. Por consiguiente, este proceso requerirá cierta coordinación con los administradores del sitio en toda la red, a fin de garantizar que los dispositivos estén preparados y listos para su implementación en el momento adecuado. Sin embargo, una vez configurado e implementado el nodo principal de control (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 los dispositivos virtuales SD-WAN VPX (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 alto o máximo.

> **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 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 que establezca el intervalo de tiempo de **espera** de la sesión de consola

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 SD-WAN en ESXi.

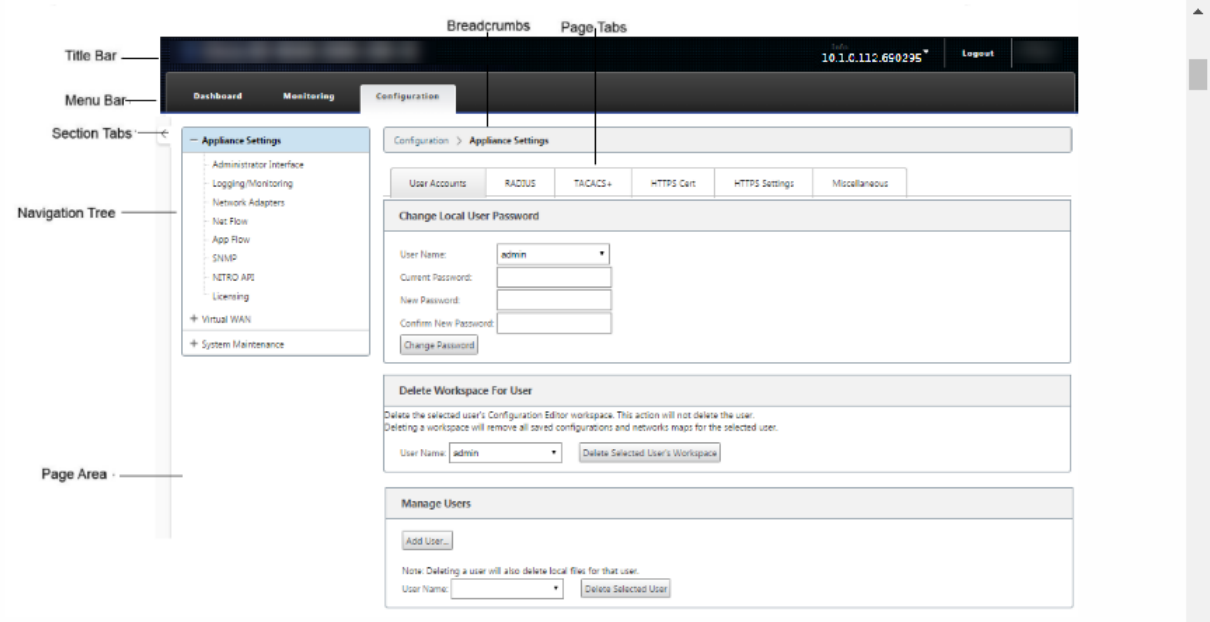
Introducción al diseño de la Interfaz Web (UI)

May 7, 2021

Esta sección proporciona 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. También se proporcionan instrucciones de navegación específicas para el **Editor de configuración** y el **Asistente para administración de cambios**.

Navegación básica

La siguiente figura describe los elementos básicos de navegación de la interfaz de administración web y la terminología utilizada para identificarlos.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 menú principal**: Esta es la barra que se muestra debajo de la barra de título en cada pantalla de 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 para las páginas y formularios de la Interfaz de administración web. Cada sección tiene su propio árbol de navegación para navegar por la jerarquía de páginas en 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 sucursal del árbol para mostrar las páginas disponibles para ese tema de sucursal.
  - Haga clic en un nombre de página para mostrar esa página en el área de página.
  - Haga clic en: (signo menos) junto a un elemento de sucursal para cerrar la sucursal.
- **Rutas de navegación**: 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 de menú principal. Los vínculos de navegación activos se muestran en fuente azul. El nombre de la página actual se muestra en negrita negra.
- **Área de página**: Se trata de la visualización de la página y el área de trabajo de la página seleccionada. Seleccione un elemento en el árbol de navegación para mostrar la página predeterminada para 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 página, justo debajo de la pantalla de pan rallado. A veces (como en el caso del 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Cambio de tamaño del área de página**: Para algunas páginas, puede aumentar o reducir el ancho del área de página (o secciones del mismo) para mostrar más campos en una tabla o formulario. En este caso, hay una barra de cambio de tamaño vertical gris en el borde derecho de un panel de área de página, formulario o tabla. Desplace 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.

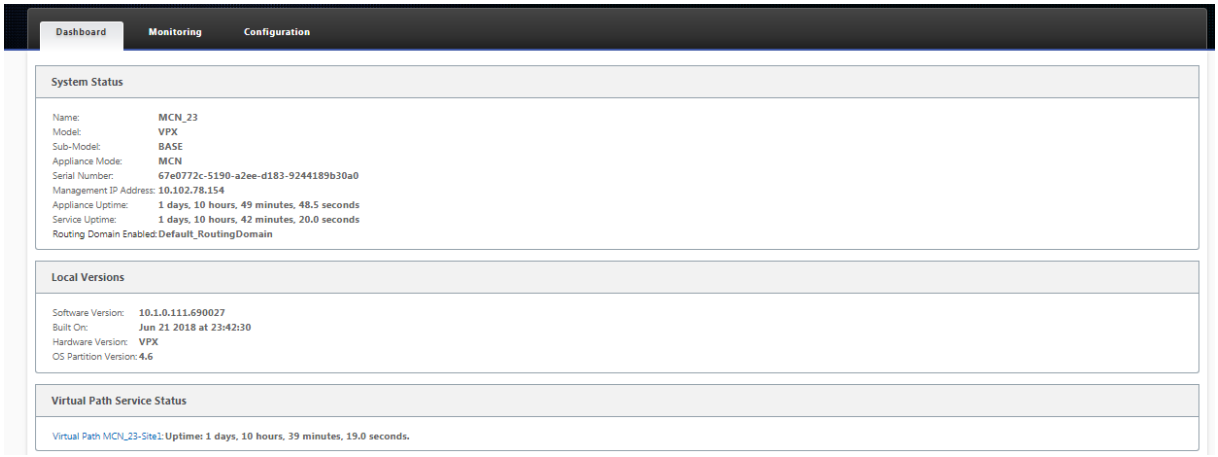
Panel de interfaz de administración web

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

La página **Panel** muestra la siguiente información básica para el dispositivo:

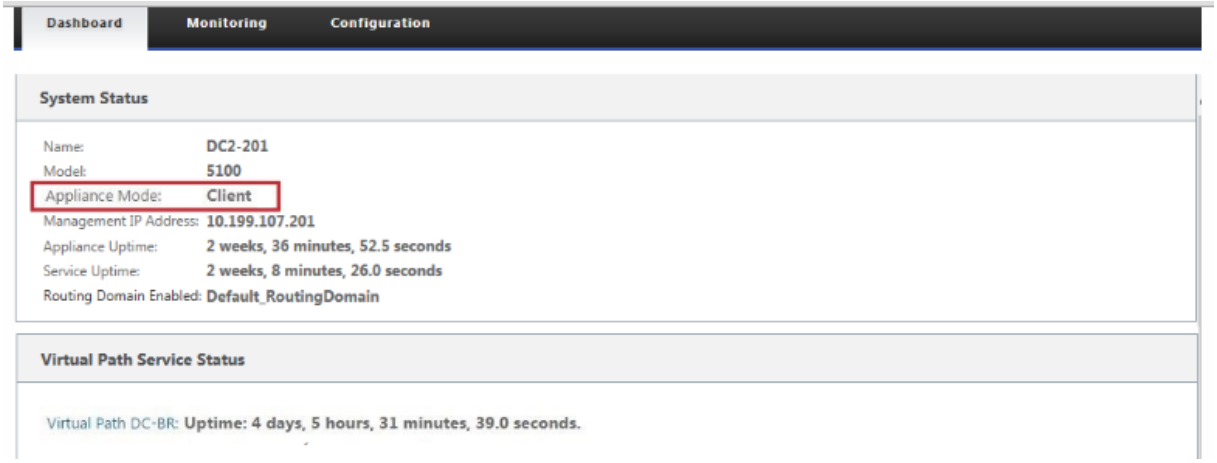
- Estado del sistema
- Estado del servicio Ruta virtual
- Información de la versión del paquete de software del dispositivo local

En la siguiente figura se muestra una muestra de ejemplo del **panel** del dispositivo de nodo de control maestro (MCN).



En la siguiente figura se muestra una muestra del panel del dispositivo cliente de ejemplo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Editor de configuración

El editor de configuración permite agregar y configurar sitios de dispositivos WAN virtuales, conexiones, optimización y Provisioning, así como crear y definir la configuración de WAN virtual.

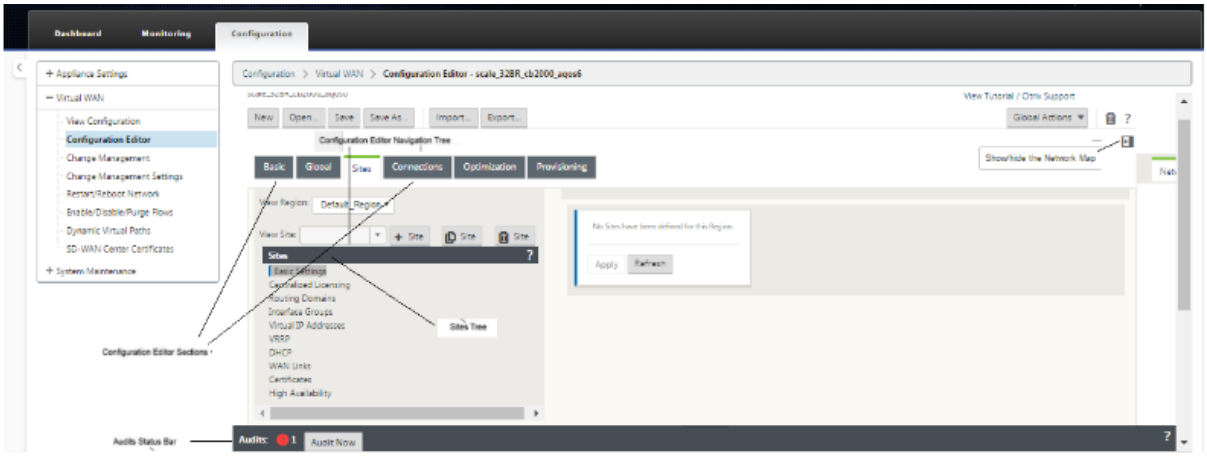
El Editor de configuración está disponible solo cuando la interfaz de administración web está en el modo de consola de MCN. De forma predeterminada, la interfaz web de un dispositivo nuevo se establece en modo cliente. Debe cambiar la configuración del modo a la consola MCN antes de poder acceder al editor de configuración. Para obtener instrucciones, consulte la sección Cambiar la interfaz web de administración al modo de consola de MCN.

Para desplazarse al **Editor de configuración**, haga lo siguiente:

1. Inicie sesión en la interfaz de administración web en el dispositivo MCN.1. Seleccione la ficha **Configuración.1**. En el árbol de navegación, haga clic en **+** junto a la sucursal **WAN virtual** del árbol. Muestra las páginas disponibles para la categoría **WAN virtual.1**. En la sucursal WAN virtual del árbol, seleccione **Editor de configuración**.

   En la siguiente figura se describen los elementos básicos de navegación y página del **Editor de configuración**, así como la terminología utilizada para identificarlos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



A continuación se describen los elementos de navegación principales del **Editor de configuración** a los que se hace referencia en esta guía:

- **Barra de menús del Editor de configuración**: Se encuentra en la parte superior del área de página, justo debajo de los enlaces de pan rallado. La barra de menús contiene los botones de actividad principales para las operaciones **del Editor de configuración**. Además, en el extremo derecho de la barra de menús se encuentra el botón de enlace **Ver tutorial** para iniciar el tutorial del **Editor de configuración**. El aprendizaje le guiará por una serie de descripciones de burbujas para cada elemento de la pantalla del **Editor de configuración**.
- **Árbol de secciones del Editor de configuración**: Se trata de la pila de barras de color gris oscuro que se encuentra en el panel izquierdo del área de página del **Editor de configuración**. Cada barra gris representa una sección de nivel superior. Haga clic en un nombre de sección para mostrar las subramas de esa sección.
- **Sucursales de árbol de secciones**: Haga clic en un nombre de sección en el árbol de secciones para abrir una sucursal de sección. Cada sucursal de sección contiene una o más subramas de categorías y formularios de configuración, que a su vez pueden contener más sucursales y formularios secundarios.
- **Árbol de sitios**: Muestra los nodos del sitio que se han agregado a la configuración abierta actualmente en el **Editor de configuración**. En el árbol de sección. Haga clic en un nombre de sitio para abrir la sucursal de ese sitio. Haga clic en el sitio para cerrar una sucursal. Para obtener instrucciones detalladas sobre cómo navegar y utilizar el árbol de **sitios** y los formularios de configuración, consulte las siguientes secciones:
  - Configuración del sitio del nodo principal de control (MCN)
  - Adición y configuración de los sitios de sucursal
- **Barra de estado de auditorías**: Es la barra gris oscuro situada en la parte inferior de la página **Editor de configuración** y que abarca todo el ancho de la pantalla Interfaz Web de administración. La barra de estado **Auditorías** solo está disponible cuando el **Editor de configuración**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

está abierto. Un icono de alerta de auditoría (punto rojo o delta de vara dorada) en el extremo izquierdo de la barra de estado indica uno o más errores presentes en la configuración abierta actualmente. Haga clic en la barra de estado para mostrar una lista completa de todas las alertas de auditoría no resueltas para esa configuración.

Asistentes de administración de cambios

Los asistentes de **administración de cambios** le guiarán a través del proceso de carga, descarga, almacenamiento en almacenamiento y activación del software y la configuración de WAN virtual en el dispositivo del nodo de control maestro (MCN) y los dispositivos cliente. Hay dos versiones del Asistente para administración de **cambios, una para administración** de cambios en todo el sistema ("global") de la WAN virtual y otra para administración de cambios local, como se indica a continuación:

- **Asistente de administración de cambios de MCN (Global): El asistente de administración de cambios globales** de MCN es la versión principal (principal) y solo está disponible en la interfaz de administración web del dispositivo MCN. Utilice esta opción para generar los paquetes del dispositivo WAN virtual que se implementarán para cada tipo de dispositivo WAN virtual de la red. También puede utilizar el asistente para propagar automáticamente los cambios de configuración a los dispositivos ya implementados en la WAN virtual. Las instrucciones básicas de navegación se proporcionan en la sección "Uso del Asistente de administración de cambios globales de MCN"que aparece a continuación. En la sección se proporcionan instrucciones para utilizar el Asistente **de administración de cambios** global de MCN para crear los paquetes del dispositivoPreparación de los paquetes de Virtual WAN Appliance en el MCN.
- **Asistente para administración de cambios locales: El Asistente para administración de cambios locales** está disponible en la interfaz de administración web que se ejecuta tanto en el MCN como en todos los dispositivos de nodo cliente. Utilice esta opción para cargar, organizar y activar el paquete de dispositivo WAN virtual apropiado en un dispositivo local que se agregará a su WAN virtual. También puede utilizar este asistente para cargar un paquete de dispositivo actualizado específicamente al MCN local o a un dispositivo WAN virtual local individual ya implementado en la red.

Uso del asistente de administración de cambios globales de MCN

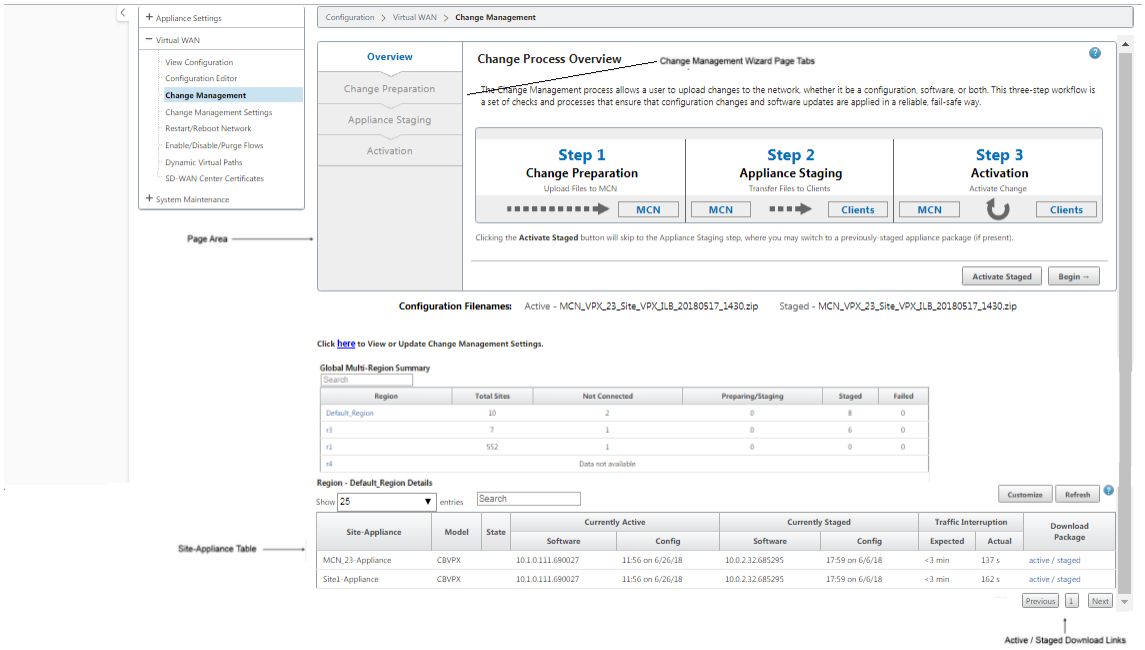
Para abrir el Asistente de **administración de cambios** globales de MCN, haga lo siguiente:

1. Inicie sesión en la interfaz de administración web del dispositivo MCN.
2. Seleccione la ficha **Configuración**. En el árbol de navegación, haga clic en **+** junto a la sucursal **WAN virtual** del árbol.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. En la sucursal **WAN virtual**. Seleccione **Gestión de cambios**.

   Muestra la primera página del asistente de **administración de cambios**, la página **Resumen del proceso de los cambios**, tal como se muestra en la siguiente imagen.



4. Para iniciar el asistente, haga clic en **Iniciar**.

   Para obtener instrucciones completas sobre el uso del asistente para cargar, organizar y activar el software SD-WAN y la configuración en los dispositivos, consulte las siguientes secciones:

- Preparación de los paquetes de Virtual WAN Appliance en el MCN
- Instalación de los paquetes de Virtual WAN Appliance en los clientes

El Asistente para **administración de cambios** contiene los siguientes elementos de navegación:

- **Área de página**: Muestra los formularios, tablas y botones de actividad de cada página del Asistente para **administración de cambios**.
- **Fichas de página del asistente Administración de cambios**: Las fichas de página se encuentran en el panel izquierdo del área de página de cada página del asistente. Las fichas aparecen en el orden en que se producen los pasos correspondientes en el proceso del asistente. Cuando una ficha está activa, puede hacer clic en ella para volver a una página anterior del asistente. Si hay una ficha activa, el nombre se muestra en fuente azul. La fuente gris indica una ficha inactiva. Las fichas están inactivas hasta que todas las dependencias (pasos anteriores) se han completado sin error.
- **Tabla de sitio de** dispositivos: Se encuentra en la parte inferior del área de página del asistente, en la mayoría de las páginas del asistente. La tabla contiene información sobre cada sitio de dispositivo configurado y vínculos para descargar los paquetes de dispositivo activos o por etapas

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

para ese modelo y sitio de dispositivo. Un paquete en este contexto es un paquete de archivos Zip que contiene el paquete de software SD-WAN adecuado para ese modelo de dispositivo y el paquete de configuración especificado. La sección **Nombres de archivo de configuración** que aparece encima de la tabla muestra el nombre del paquete de los paquetes activos y en etapas actuales del dispositivo local.

- **Enlaces de descarga activo/por etapas**: Se encuentran en el campo **Paquete de descarga** (columna derecha) de cada entrada de **la tabla Sitio de** dispositivo. Haga clic en un vínculo de una entrada para descargar el paquete activo o por etapas del sitio del dispositivo.
- **Iniciar**: Haga clic en Iniciar para **iniciar** el proceso del asistente **de administración de cambios** y continúe con la página de separador **Preparación de cambios**.
- **Activar por etapas**: Si no se trata de una implementación inicial y quiere activar la configuración por etapas actualmente, tiene la opción de continuar directamente con el paso **Activación**. Haga clic en **Activar por etapas** para pasar directamente a la página Activación e iniciar la activación de la configuración en fase interactiva.

Configuración del hardware del dispositivo

May 7, 2021

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

1. Configure 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 mínimo de 2 pulgadas de espacio libre en los lados y en la parte posterior del dispositivo, para una ventilación adecuada.

2. Conecta la alimentación.

   a) Asegúrese de que el interruptor de alimentación está desactivado.
   b) Conecte el cable de alimentación al dispositivo y a una toma de CA.
   c) Pulse el botón de encendido en la parte frontal del dispositivo.

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> Antes de conectar el dispositivo, asegúrese de que el puerto Ethernet está habilitado en el equipo. Utilice un cable Ethernet para conectar el puerto de administración del dispositivo 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 al crear la máquina virtual VPX, debe 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 al crear la máquina virtual VPX, debe 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

September 26, 2023

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

1. Si está configurando un dispositivo SD-WAN de hardware, conecte físicamente el dispositivo a un equipo.

   - Si aún no lo ha hecho, conecte un extremo de un cable Ethernet al puerto de administración del dispositivo y el otro extremo al puerto Ethernet predeterminado del PC.

   > **Nota**
   >
   > Asegúrese de que el puerto Ethernet está habilitado en el equipo que está utilizando 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. Cambie la dirección IP de la PC.

   En el equipo, abra la configuración de la interfaz de red y cambie la dirección IP del equipo a la siguiente:

   - 192.168.100.50

4. Cambie la configuración **Máscara de subred** del equipo a la siguiente:

   - 255.255.0.0

5. En el equipo, 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.
   >
   > Ignorar cualquier advertencia de certificado del explorador para la Interfaz Web de administración.

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

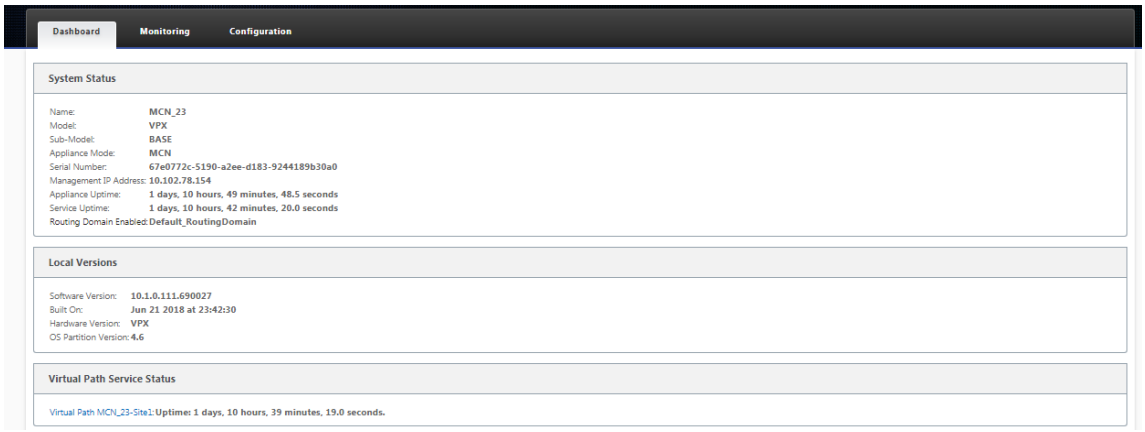
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 podría 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 después de haber instalado la licencia y completado el proceso de configuración e implementación del dispositivo.

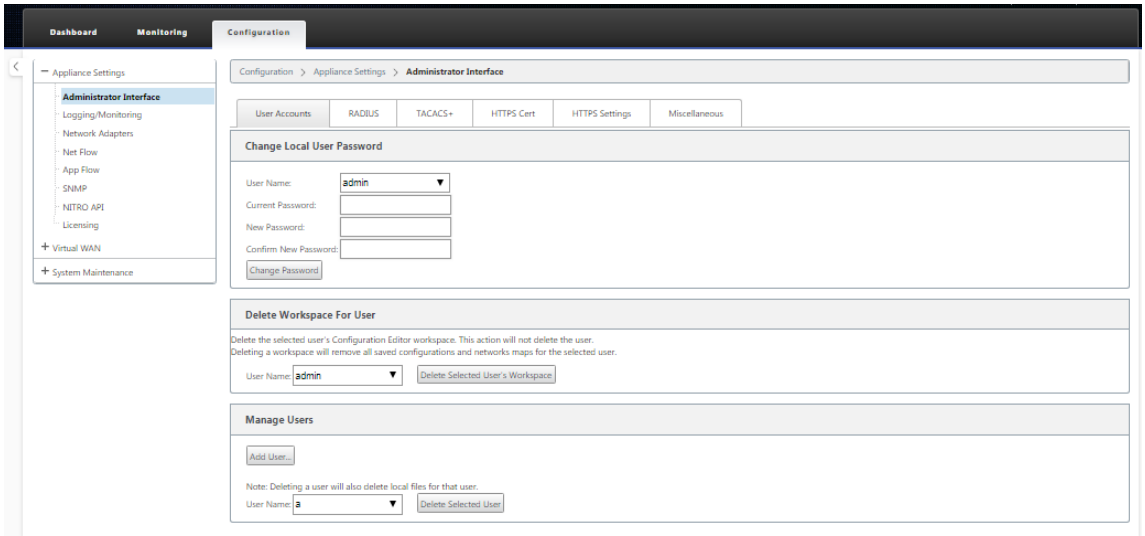
7. En la barra de menús principal, seleccione la ficha **Configuración de** la sección.

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

   - Configuración del dispositivo
   - WAN virtual
   - Mantenimiento del sistema

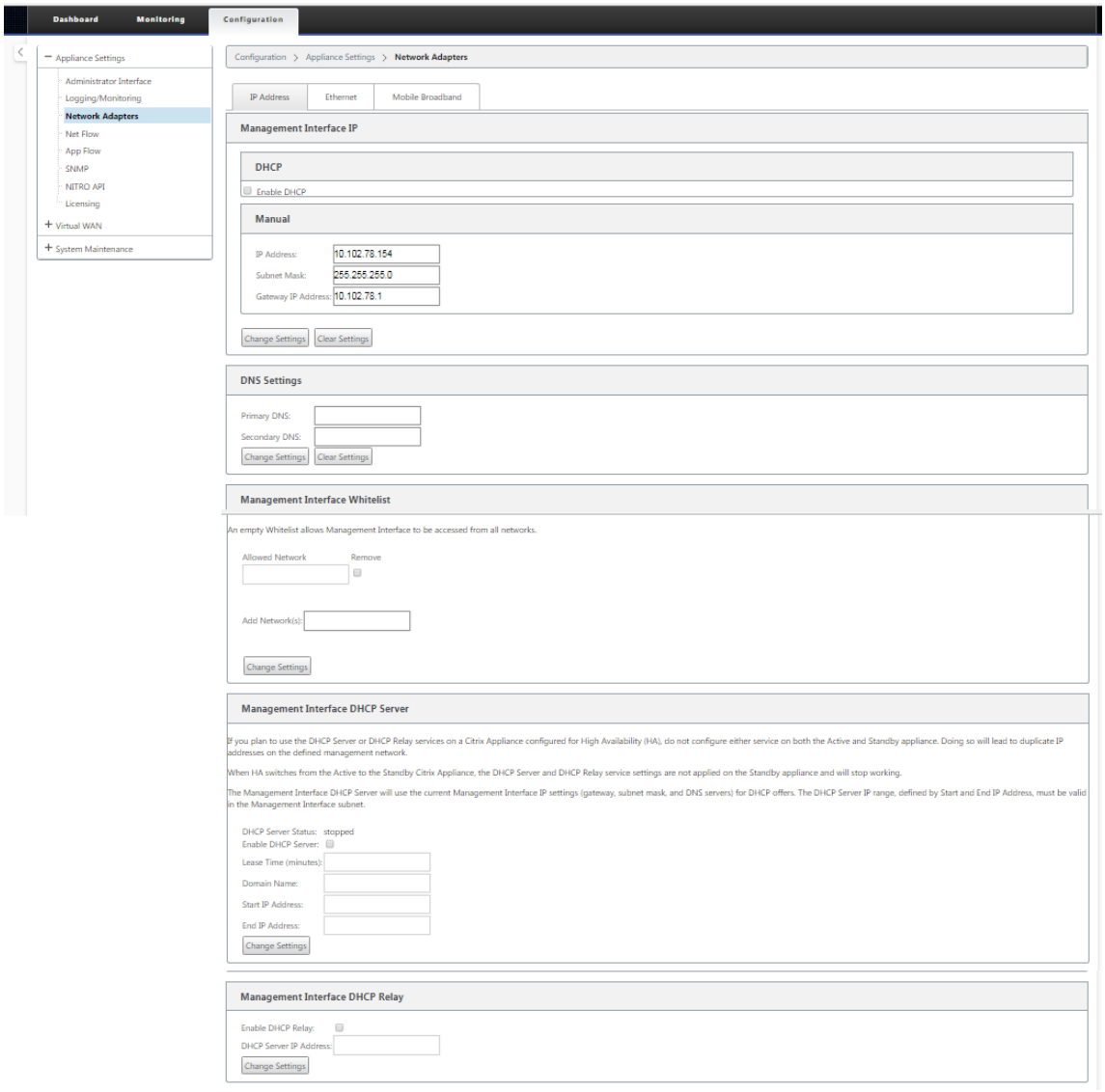
   Al seleccionar la ficha **Configuración**, se abre automáticamente la sucursal **Configuración del equipo**, con la página **Interfaz de administrador** preseleccionada de forma predeterminada, como se muestra en la figura siguiente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. En la rama **Configuración del equipo** 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 figura siguiente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



9. En la página **de ficha Dirección IP**, introduzca la siguiente información para el dispositivo SD-WAN que quiere configurar.

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

   > **Nota**
   >
   > La dirección IP de administración debe ser única para cada dispositivo.

10. Haga clic en **Change Settings**. Aparece un cuadro de diálogo de confirmación en el que se le pide que compruebe que quiere cambiar esta configuración.
11. Haga clic en **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

12. Cambie la configuración de la interfaz de red de su PC a la configuración original.

    > **Nota**
    >
    > Al cambiar la dirección IP del equipo, se cierra automáticamente la conexión al dispositivo y finaliza la sesión de inicio de sesión en la interfaz web de administración.

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

    El dispositivo SD-WAN ahora está conectado a la red y 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.

    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 está utilizando 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.

Establecer fecha y hora

May 7, 2021

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

> **Nota**
>
> Debe repetir este proceso para cada dispositivo que quiera agregar a la red.

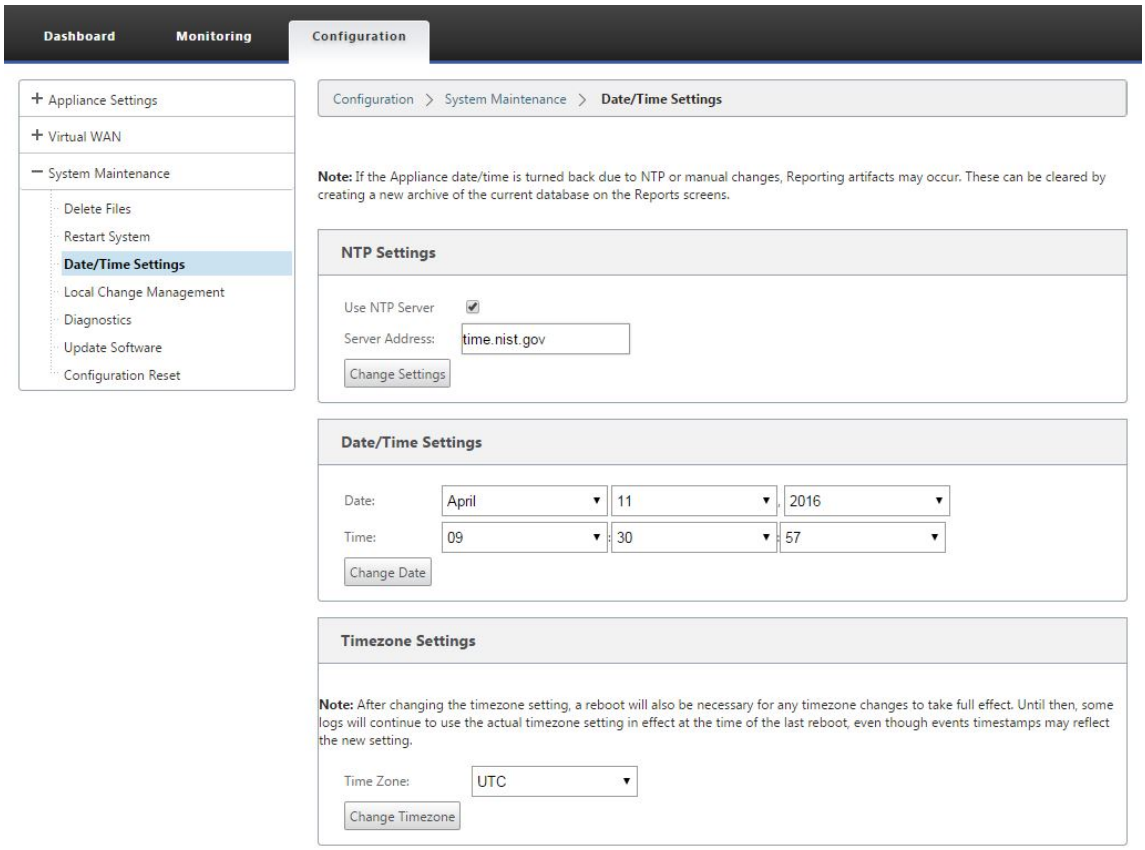
Para establecer la fecha y la hora, haga lo siguiente:

1. Inicie sesión en la Interfaz Web de administración del dispositivo que está configurando.
2. En la barra de menús principal, seleccione la **ficha Configuración.**

   Muestra el árbol de navegación **Configuración** en el panel izquierdo de la pantalla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Abra la **sucursal Mantenimiento del sistema** en el árbol de navegación.
4. En la **sucursal Mantenimiento del sistema, seleccione Configuración de fecha/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 zona horaria, debe hacerlo antes de establecer la fecha y la hora, de lo contrario, la configuración no se mantiene como se ha introducido.

6. Haga clic en **Cambiar zona horaria**. Esto actualiza la zona horaria y vuelve a calcular la configuración de fecha y hora actual, en consecuencia. Si establece la fecha y la hora correctas antes de este paso, la configuración ya no es correcta. Cuando se complete la actualización de la zona horaria, se muestra un icono de alerta de éxito (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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) Haga clic en **Change Settings**.Aparece
un icono de alerta de éxito (marca de verificación verde) y un mensaje de estado cuando se complete la actualización.

8. Seleccione el mes, el día y el año en los menús implementables del campo **Fecha**.
9. Seleccione la hora, los minutos y los segundos en los menús implementables 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 de éxito o un mensaje de estado.

El siguiente paso es 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 podría 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 pasar directamente a la sección,Carga e instalación del archivo de licencia del software 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

May 7, 2021

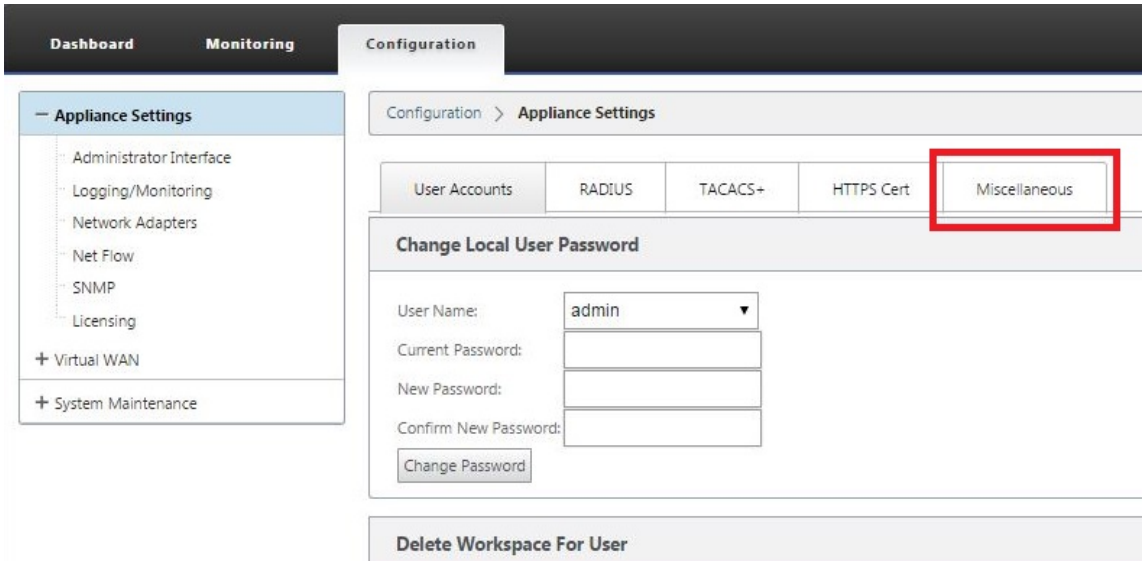
Si el tiempo de espera de la sesión de consola o cierra sesión en Management Web Interface antes de guardar la configuración, se perderán los cambios de configuración no guardados. A continuación, debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por ese motivo, se recomienda establecer el intervalo de tiempo de **espera** de sesión de la consola en un valor alto al crear o modificar un paquete de configuración o 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

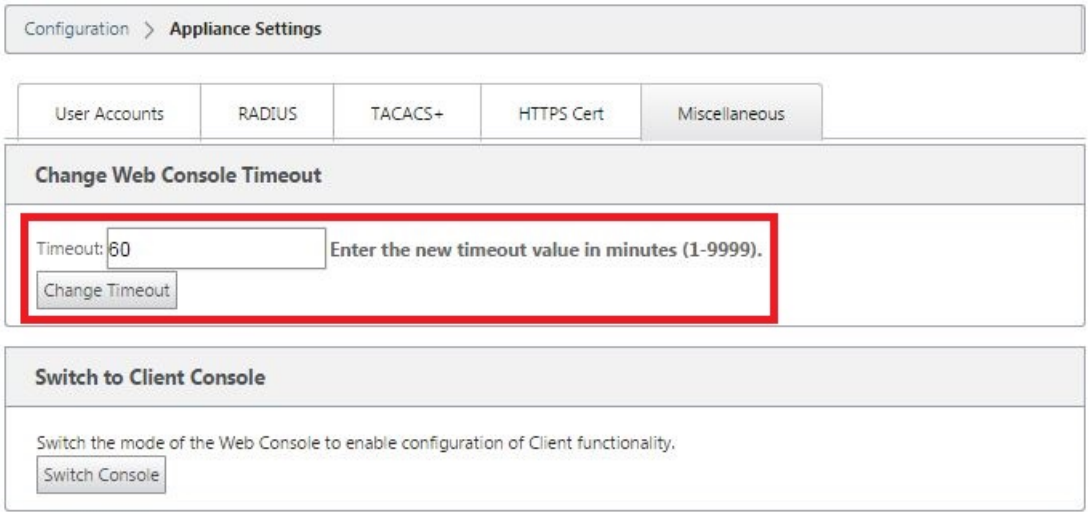
1. Seleccione la ficha **Configuración** y, a continuación, seleccione la sucursal **Configuración del equipo** en el árbol de navegación.

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



2. Seleccione la ficha **Varios** (esquina derecha).

   Muestra la ficha **Varios**.



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

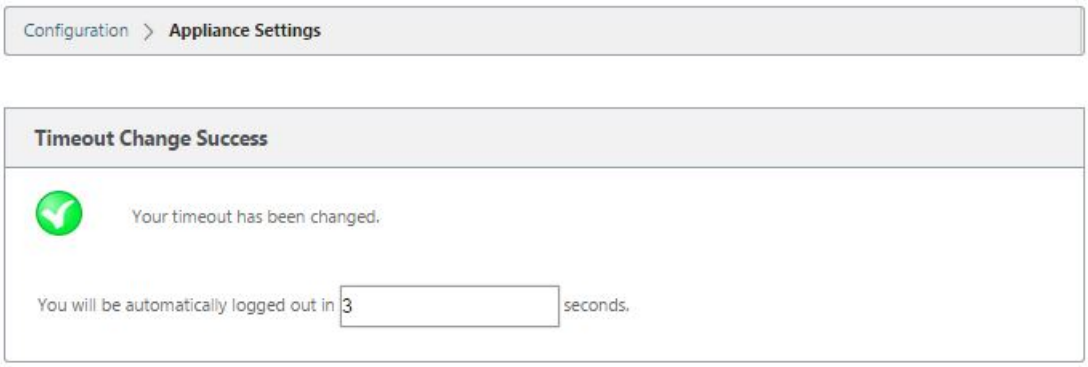
   En el campo **Tiempo de espera** de la sección **Cambiar tiempo de espera de la consola Web**, introduzca un valor superior (en minutos) hasta el valor máximo de 9999. El valor predeterminado es 60, que es demasiado breve para una sesión de configuración inicial.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

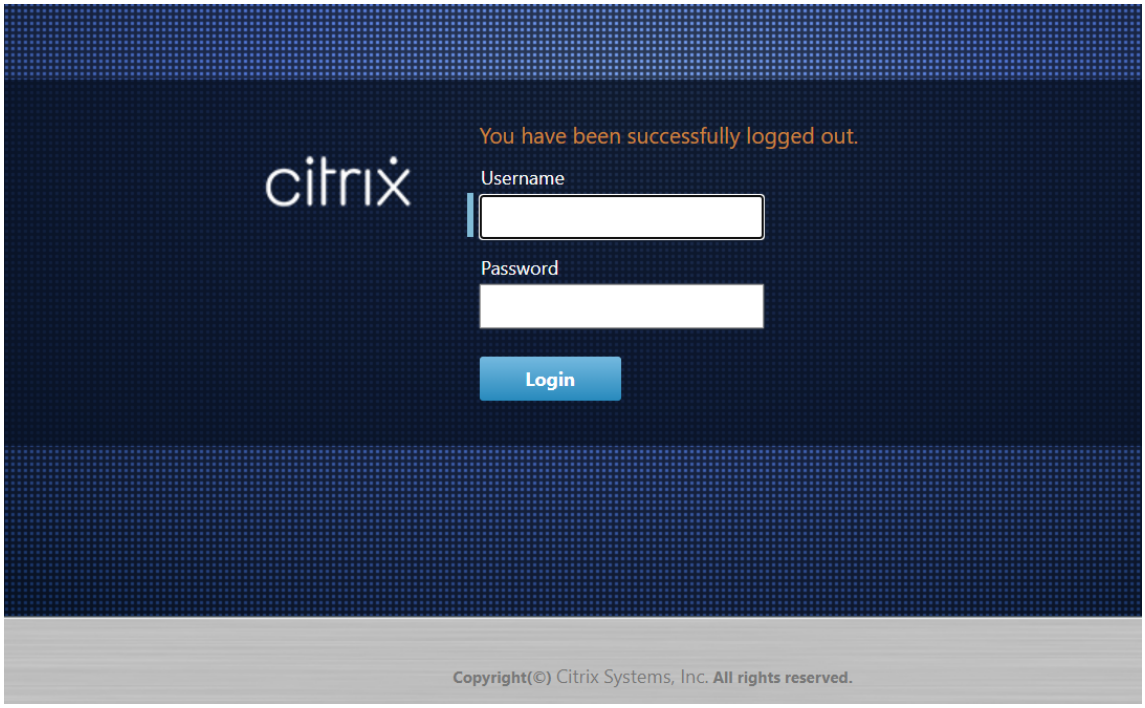
> **Nota**
>
> Por razones de seguridad, asegúrese de restablecer este valor a un intervalo inferior después de completar la configuración y la implementación.

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.



   Después de un breve intervalo (unos segundos), la sesión finaliza y se cierra automáticamente la sesión de la Interfaz Web de administración. Aparecerá la página Inicio de sesión.



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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurar alarmas

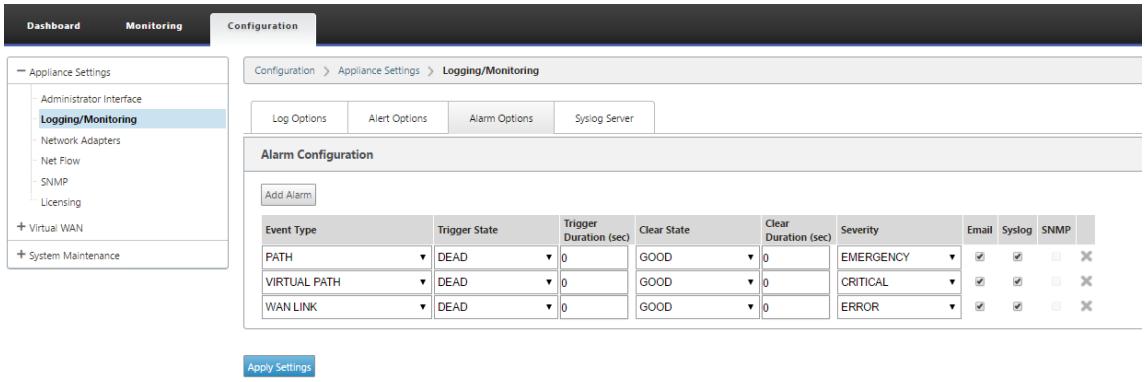
May 7, 2021

Ahora puede configurar su dispositivo SD-WAN para identificar las condiciones de alarma en función de su red y 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 de borrado y una gravedad.

Para configurar las opciones de alarma:

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



3. Seleccione o introduzca valores para los siguientes campos:

   - **Tipo de evento**: El dispositivo SD-WAN puede activar alarmas para determinados subsistemas u objetos de la red, estos se denominan tipos de eventos. Los tipos de evento 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 e IPSEC_TUNNEL.
   - **Estado del desencadenador**: Estado del evento que activa una alarma para un tipo de evento. Las opciones de estado de activación disponibles dependen del tipo de evento elegido.
   - **Duración del desencadenador**: La duración en segundos determina la rapidez con que el dispositivo desencadena 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 dentro del período Duración del desencadenador. Solo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

se activan más alarmas si un evento persiste más tiempo que el período de duración del desencadenador.

- **Borrar estado: Estado**del 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 de activación elegido.
- **Duración clara:** 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 15-7200 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**: El activador de alarma y las alertas claras para el tipo de evento se envían por correo electrónico.
- **Syslog**: El activador de alarma y las alertas claras 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**.

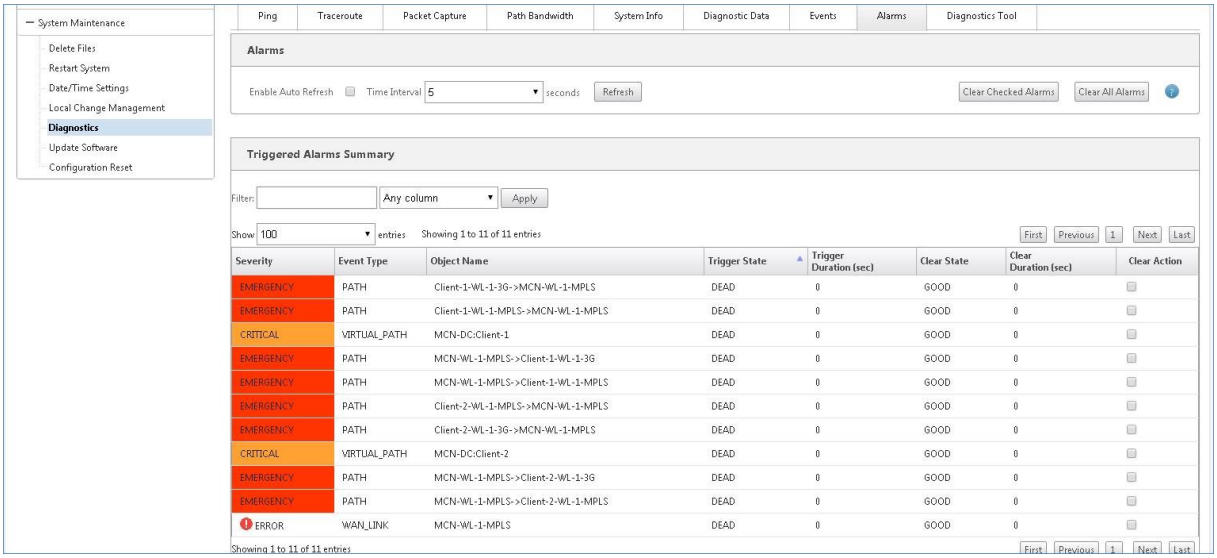
Visualización de alarmas activadas

Para ver un resumen de todas las alarmas activadas:

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

Se muestra una lista de todas las alarmas activadas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Borrar alarmas activadas

Para borrar manualmente las alarmas activadas:

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

Configurar la reversión

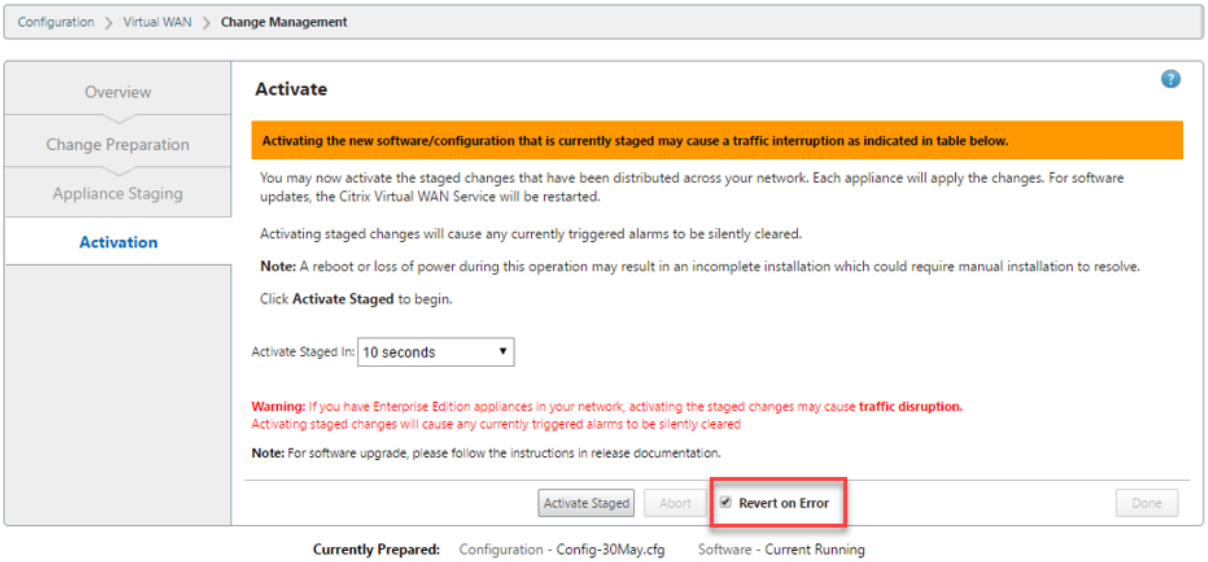
May 7, 2021

La función de reversión de configuración permite que el sistema de administración de cambios detecte y recupere los siguientes errores de software/configuración volviendo al software/configuración previamente activo:

- Después de una actualización de software, Virtual Path está muerto y el servicio se desactiva si se produce el bloqueo del software.
- Después de realizar los cambios de configuración, Virtual Path está muerto sin ningún bloqueo de software.
- Si la configuración del propio dispositivo MCN causa un problema de red en el sitio de MCN, no detecta la interrupción y no se deshacen. Sin embargo, todos los demás clientes de la red se deshacen porque no pudieron conectarse al MCN.

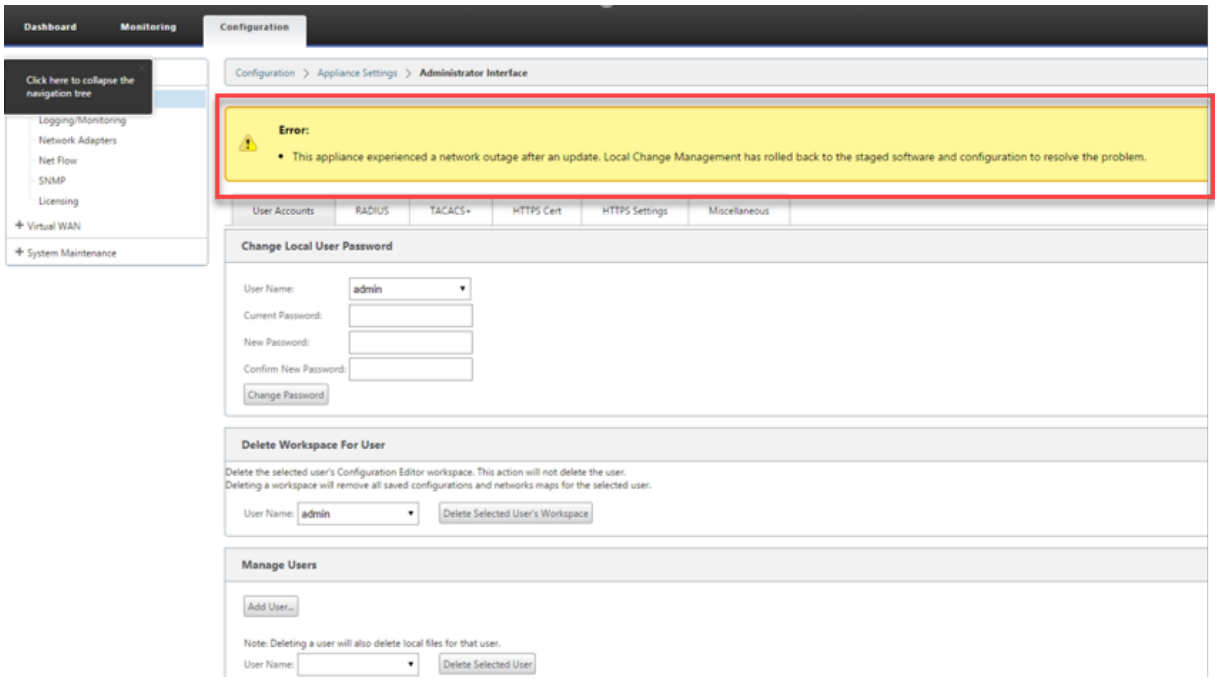
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La función de reversión de configuración está habilitada de forma predeterminada, para deshabilitar esta función, desactive la opción **Revertir en caso de error** en la ficha **Activación** del asistente Administración de cambios.



Si se produce un error de configuración del sistema en un cliente al activar el paquete en etapas desde un MCN, el cliente vuelve a la configuración de software anterior y aparece un mensaje de error como se muestra en la siguiente captura de pantalla.

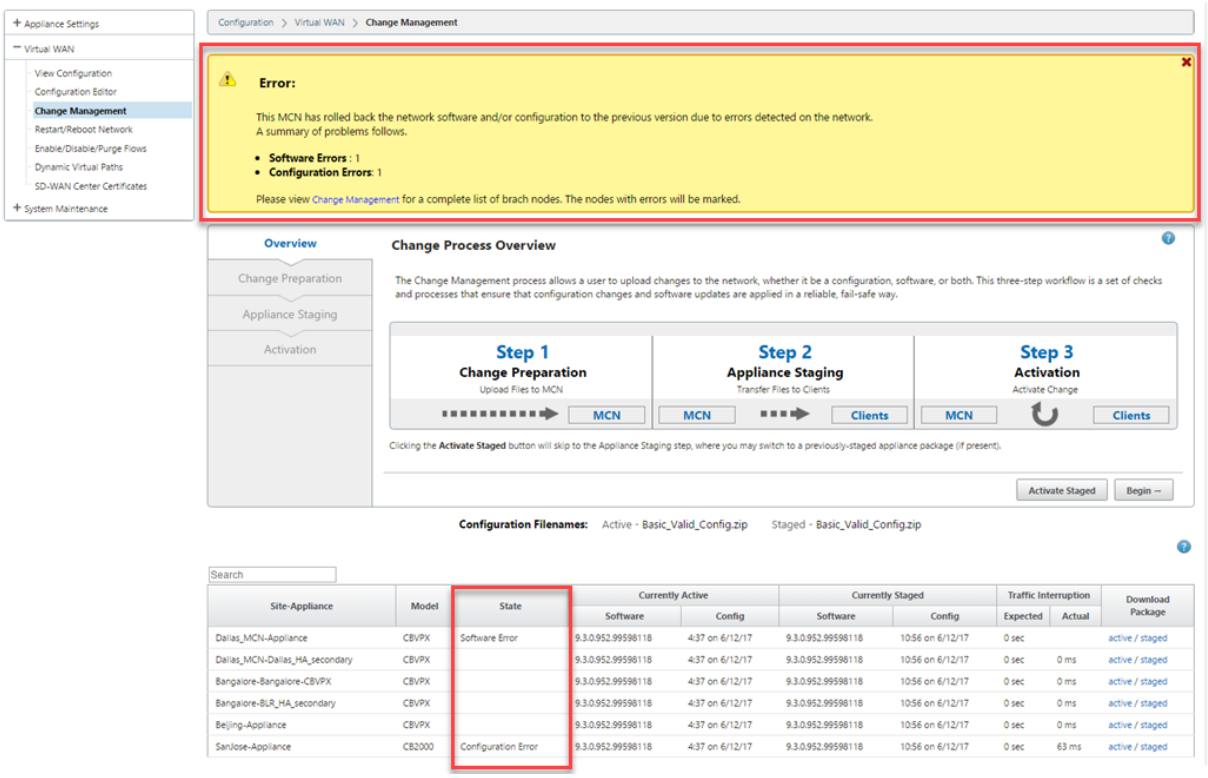
El cliente genera un evento de gravedad crítica para el objeto SOFTWARE_UPDATE si se detecta un bloqueo del dispositivo o genera un evento de gravedad crítico para el objeto CONFIG_UPDATE si se detecta una interrupción de la red.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si **Revert on Error** está habilitado, los dispositivos cliente se supervisan durante unos 30 minutos. Si el software se cierra de manera inesperada en menos de 30 minutos o si la red está desconectada (no se puede establecer una ruta virtual al MCN) durante 30 minutos, se desencadena una reversión.

En el MCN, aparece un mensaje de error como se muestra en la siguiente captura de pantalla. A medida que los clientes se vuelven a unir a la red, informa del tipo de error encontrado. En el mensaje de error se muestra un recuento resumido del número de errores.



En la ventana **Administración de cambios** del MCN, puede ver el estado de los dispositivos del sitio que indica si ese sitio ha encontrado un error de software o un error de configuración.

Configuración del nodo de control maestro

May 7, 2021

El **nodo de control maestro (MCN) de SD-WAN** es el dispositivo de cabecera de la WAN virtual. Normalmente, se trata de un dispositivo WAN virtual 4000 o 5100 implementado en el centro de datos de la empresa. El MCN sirve como punto de distribución para la configuración inicial del sistema y cualquier cambio posterior de configuración. Además, realiza la mayoría de los procedimientos de actualización a través de la Interfaz Web de administración en el MCN. Solo puede haber un MCN activo en una WAN virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

De forma predeterminada, los dispositivos tienen el rol preasignado de cliente. 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.

Información complementaria sobre la implementación del sitio de MCN

Se recomiendan los siguientes artículos de soporte de Knowledge Base:

- Pasos de implementación del modo PBR de WAN virtual (CTX201577)

  http://support.citrix.com/article/CTX201577
- Pasos de implementación del modo de puerta de enlace WAN virtual (CTX201576)

  http://support.citrix.com/article/CTX201576

Introducción a los procedimientos de configuración del sitio de MCN

Los pasos para agregar y configurar el sitio de MCN son los siguientes:

1. Cambie la Interfaz Web de administración al modo **Consola de MCN**.
2. Agregue el sitio de MCN.
3. Configure los grupos de interfaz virtual para el sitio de MCN.
4. Configure las direcciones IP virtuales para el sitio de MCN.
5. (Opcional) Configure los túneles LAN GRE para el sitio.
6. Configure los enlaces WAN para el sitio de MCN.
7. Configure las interfaces de acceso para el sitio de MCN.
8. Configure las rutas para el sitio de MCN.
9. (Opcional) Configurar alta disponibilidad para el sitio de MCN.
10. (Opcional) Configure la seguridad y el cifrado de la WAN virtual.
11. Asigne un nombre y guarde la configuración del sitio de MCN.

En las siguientes secciones se proporcionan instrucciones para cada una de estas tareas.

Descripción general de MCN

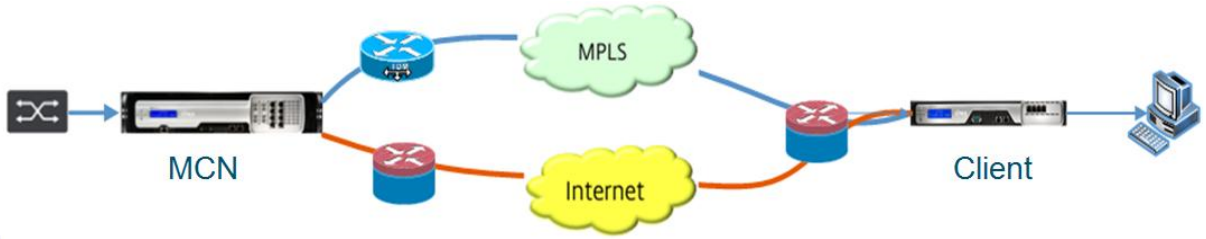
May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El **nodo de control maestro (MCN)** es el dispositivo WAN virtual central que actúa como Controller maestro de la WAN virtual y punto de administración central de los nodos cliente. Todas las actividades de configuración, así como la preparación de los paquetes del dispositivo y su distribución a los clientes, se realizan en el MCN. Además, cierta información de supervisión de WAN virtual solo está disponible en el MCN. El MCN puede supervisar toda la WAN
virtual, mientras que los nodos de cliente solo pueden supervisar sus intranets locales, junto con cierta información para los clientes con los que están conectados.

El objetivo principal del MCN es establecer y utilizar rutas virtuales con uno o más nodos de cliente ubicados a través de la WAN virtual, para las comunicaciones de sitio a sitio de la empresa. Un MCN puede administrar y tener rutas virtuales a varios nodos de cliente. Puede haber más de un MCN, pero solo uno puede estar activo en un momento dado.

La siguiente figura ilustra las funciones básicas y el contexto de los dispositivos MCN (centro de datos) y cliente (nodo de sucursal) para una implementación Virtual WAN Edition.



Cambiar a la consola de MCN

May 7, 2021

Para agregar y configurar el sitio de MCN, primero debe iniciar sesión en la Interfaz Web de administración del dispositivo que está promoviendo a la función de MCN y cambiar la Interfaz Web de administración al modo **Consola de MCN**. El modo**Consola MCN** permite el acceso al Editor de configuración en la Interfaz Web de administración a la que está conectado actualmente. A continuación, puede utilizar el **Editor de configuración** para agregar y configurar el sitio MCN.

> **Nota**
>
> Al cambiar al modo **Consola de MCN** solo se cambia el modo de funcionamiento del modo Interfaz Web de administración, y no el rol activo del propio dispositivo. Para promover un dispositivo a la función de MCN, primero debe agregar y configurar el sitio de MCN y activar la configuración y el paquete de software en el dispositivo MCN designado.

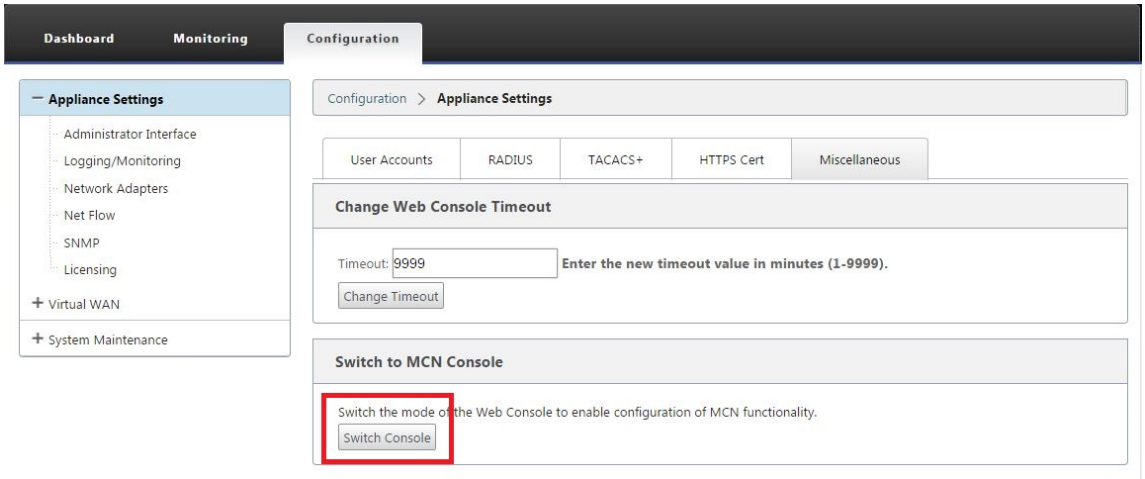
Para cambiar la Interfaz Web de administración al modo **Consola MCN**, haga lo siguiente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Inicie sesión en la Interfaz Web de administración del dispositivo que quiere configurar como MCN.
2. Haga clic en **Configuración** en la barra de menú principal de la pantalla principal de Management Web Interface (barra azul en la parte superior de la página).
3. En el árbol de navegación (panel izquierdo), abra la rama **Configuración del equipo** y haga clic en **Interfaz de administrador**.

   Muestra la página Interfaz de administrador en el panel central.
4. Seleccione la ficha **Varios**.

   Muestra la página **Otras configuraciones administrativas**.



En la parte inferior de la ficha **Varios** se encuentra la sección **Cambiar a cliente > Consola de MCN**. Esta sección contiene el botón **Conmutador de consola** para alternar entre los modos de consola del dispositivo.

El encabezado de sección indica el modo de consola actual, como se indica a continuación:

- En el modo de **consola de cliente** (predeterminado), el encabezado de sección es **Cambiar a consola de MCN**.
- En el modo **Consola de MCN**, el encabezado de sección es **Cambiar a Consola de cliente.**

De forma predeterminada, un nuevo dispositivo está configurado en modo de **consola de cliente**.

El modo**Consola de MCN** habilita la sucursal **Editor de configuración** en el árbol de navegación. El **Editor de configuración** sólo está disponible en el dispositivo MCN.

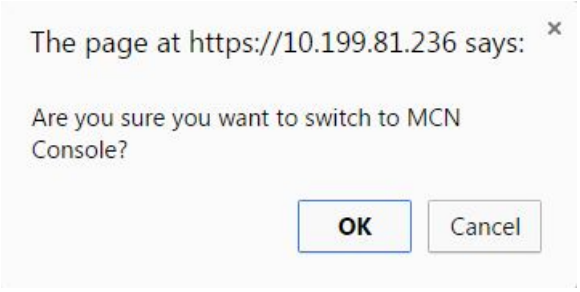
> **Nota**
>
> Antes de continuar con el paso siguiente, asegúrese de que el dispositivo sigue configurado como predeterminado (modo de **consola de cliente**). El encabezado de la sección debe

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ser: **Cambiar a la consola MCN**.

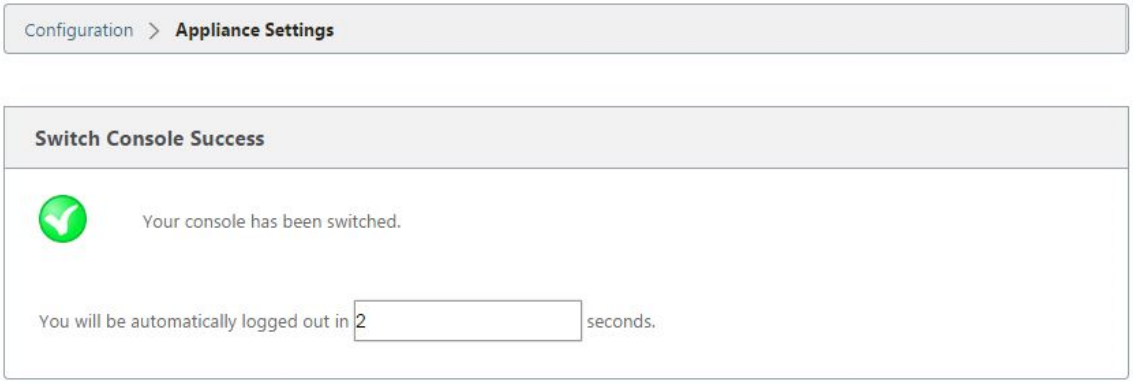
5. Haga clic en **Modo de conmutación** para configurar el modo del dispositivo en el modo de **consola de MCN**.

   Aparece un cuadro de diálogo en el que se le pide que confirme que quiere cambiar al modo MCN.



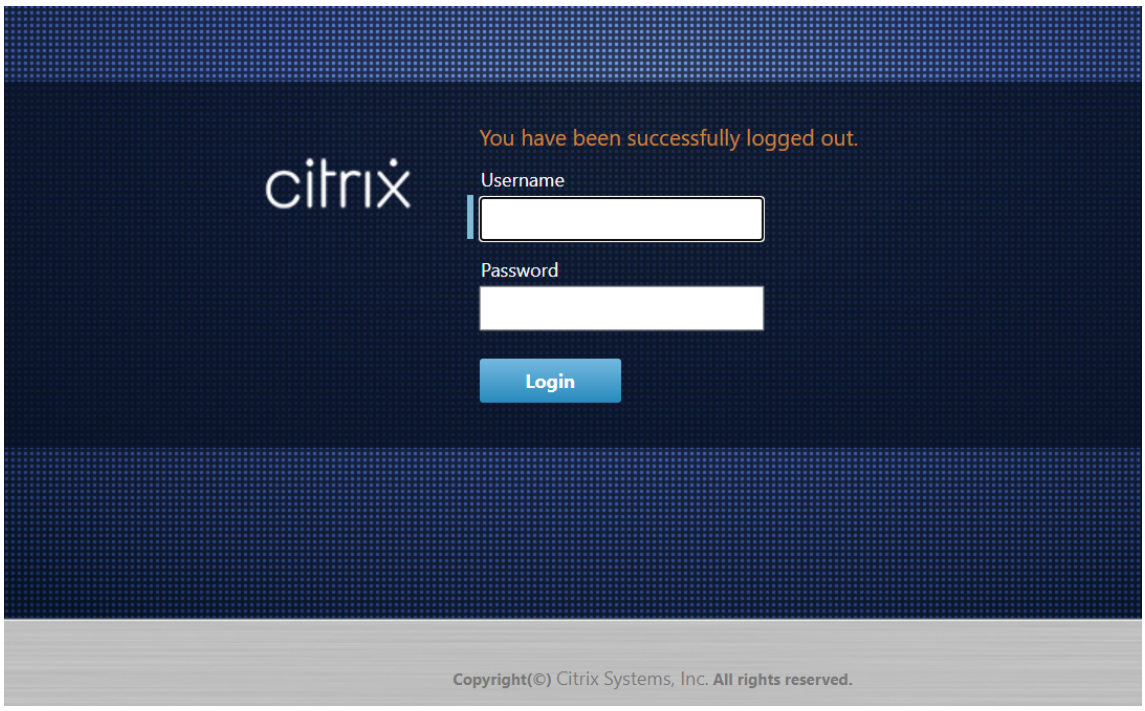
6. Haga clic en **OK**.

   Esto cambia el modo de consola al modo de **consola MCN** y finaliza la sesión actual. Aparece un mensaje de éxito, junto con un estado de cuenta atrás que indica el número de segundos que quedan antes de que finalice la sesión.



   Una vez completada la cuenta atrás, la sesión finaliza y aparece la página de inicio de sesión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

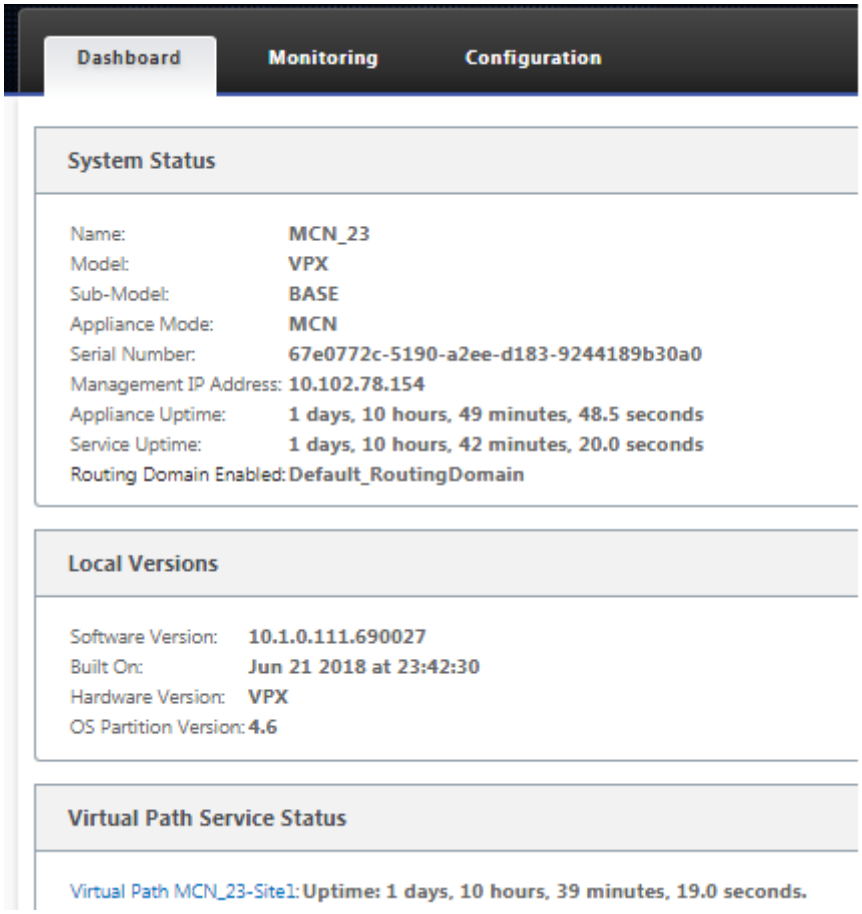


7. Introduzca el nombre de usuario y la contraseña del administrador y haga clic en **Iniciar sesión**.

   - Nombre de usuario predeterminado del administrador: *admin*
   - Contraseña de administrador predeterminada: *password*

   Después de iniciar sesión, aparece el **Panel de mandos**, que indica que el dispositivo está en modo MCN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



El siguiente paso es abrir una nueva configuración y agregar el sitio MCN a la tabla Sitios y comenzar a configurar el nuevo sitio MCN.

Configurar MCN

May 7, 2021

El primer paso es abrir un nuevo paquete de configuración y agregar el sitio de MCN a la nueva configuración.

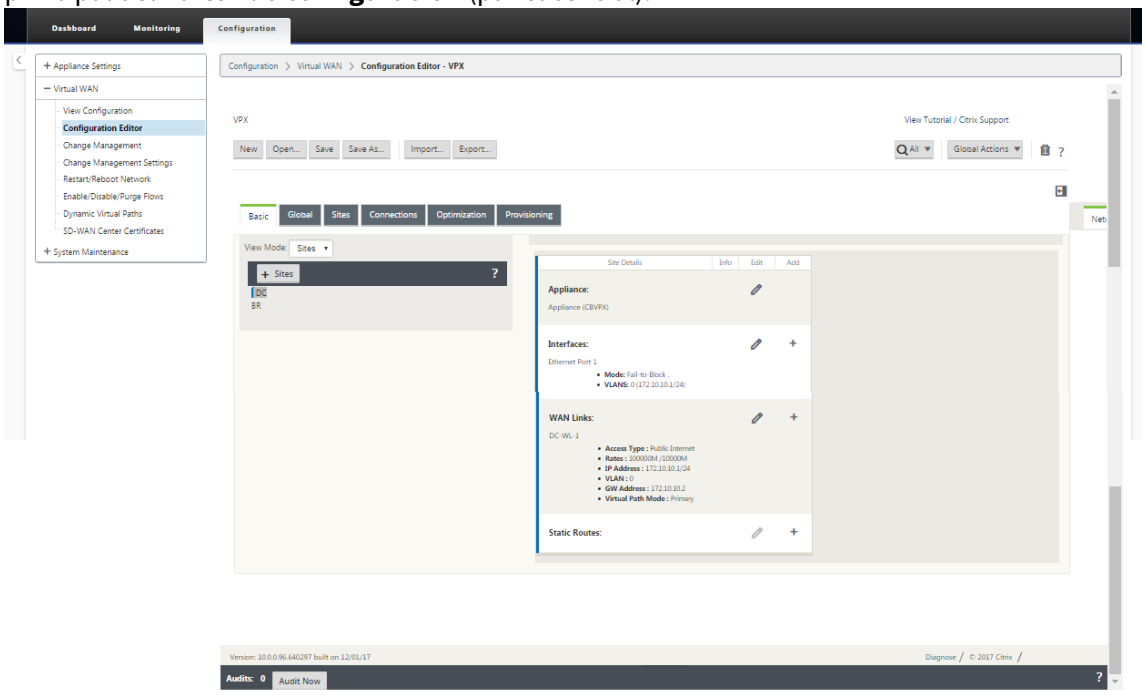
> **Nota**
>
> El **Editor de configuración** está disponible en el modo **Consola de MCN**. Si la opción **Editor de configuración** no está disponible en la sucursal WAN virtual del árbol de navegación, consulte la sección Cambio de la interfaz web de administración al modo de consola de MCN, para obtener instrucciones sobre cómo cambiar el modo de consola.
>
> Se recomienda guardar el paquete de configuración con frecuencia o en puntos clave de la con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> figuración. Las instrucciones se proporcionan en la sección.Asignación de nombres, almacenamiento y copia de seguridad de la configuración del sitio de MCN
>
> **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. A continuación, debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por este motivo, se recomienda que establezca 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. 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 obtener instrucciones, consulte la secciónConfiguración del intervalo de tiempo de espera de la sesión de consola (opcional)

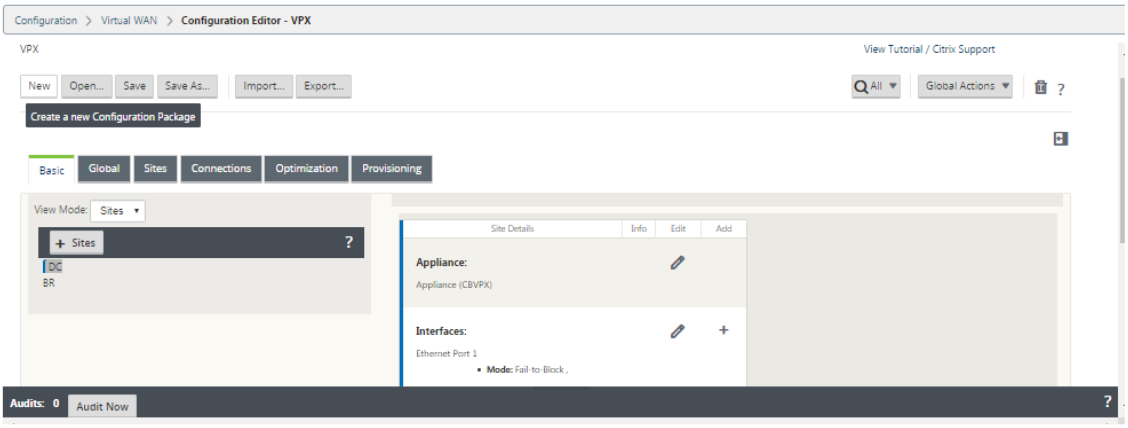
Para agregar y comenzar a configurar el sitio del dispositivo MCN, haga lo siguiente:

1. En el árbol de navegación, vaya a **Virtual WAN** > **Editor de configuración**. Muestra la página principal del **Editor de configuración** (panel central).

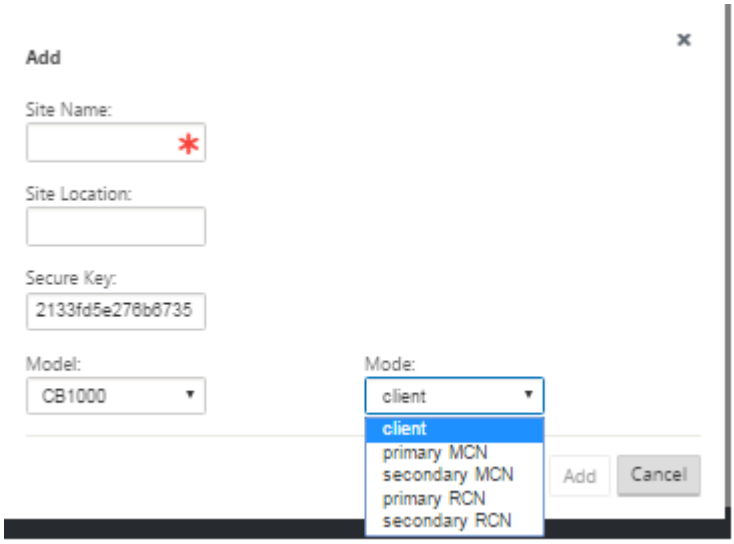


2. Haga clic en **Nuevo** para empezar a definir una nueva configuración. Aparecerá la página **Nuevos** valores de configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Haga clic en**+ Sitiosen la barra Sitios**para comenzar a agregar y configurar el sitio MCN. Muestra el cuadro de diálogo**Agregar sitio**.



4. Introduzca la información del sitio.

Haga lo siguiente:

1. Introduzca el **nombre del sitio** y la **clave segura**.
2. Seleccione el **modelo**del dispositivo.
3. Seleccione el **Modo**.
4. Seleccione **MCN principal** como modo.

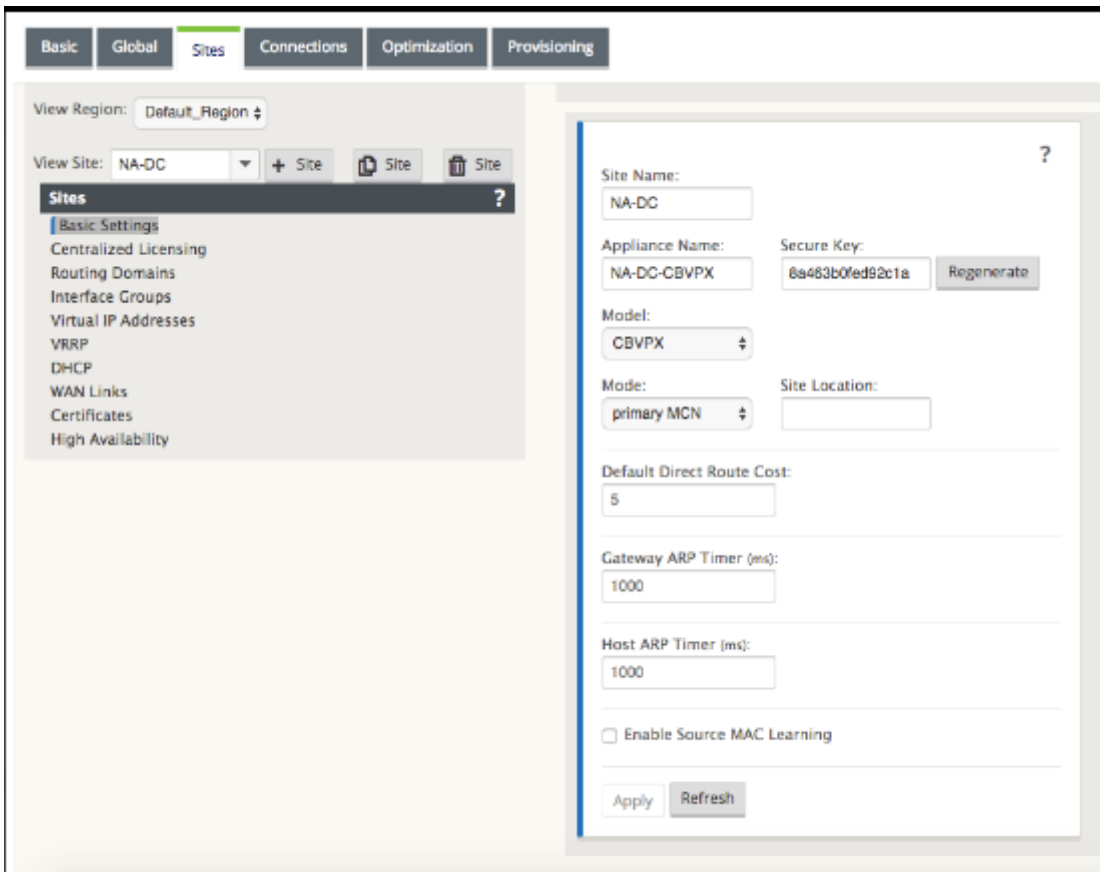
> **Nota**
>
> El menú Opciones del **modelo** muestra los nombres genéricos de los modelos de dispositivo compatibles. Los nombres genéricos no incluyen el sufijo de modelo Standard Edition, pero sí corresponden a los modelos equivalentes del dispositivo SD-WAN. Seleccione el número de modelo correspondiente para este modelo de dispositivo SD-WAN. (Por ejemplo, seleccione 4000 si

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> se trata de un dispositivo SD-WAN 4000-SE).
>
> Las entradas no pueden contener espacios y deben estar en formato Linux.

Para agregar sitio:

1. Haga clic en **Agregar** para agregar el sitio. Esto agrega el nuevo sitio al árbol **Sitios** y muestra el formulario de configuración de **Configuración básica** para el nuevo sitio.



   Después de hacer clic en **Aplicar**, aparecen advertencias de auditoría que indican que es necesario realizar más acciones. Un punto rojo o un icono delta de vara dorada indica un error en la sección donde aparece. Puede utilizar estas advertencias para identificar errores o falta información de configuración. Pase el cursor sobre un icono de advertencia de auditoría para mostrar una breve descripción de los errores en esa sección. También puede hacer clic en la barra de estado **Auditorías** de color gris oscuro (parte inferior de la página) para mostrar una lista completa de todas las advertencias de auditoría no resueltas. El temporizador ARP de host configurable (ms) se agrega a nivel de sitio durante la configuración. El valor predeterminado actual es 1.000 ms. El rango configurable es de 1.000 ms a 180.000 ms. La configuración del temporizador ARP del host no es aplicable al puerto de administración.

2. Introduzca la configuración básica del nuevo sitio o acepte los valores predeterminados. En implementaciones de Citrix SD-WAN como Gateway y One-arm, cuando las solicitudes ARP se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

reciben con frecuencia, los puntos de acceso se sobrecargan afectando al flujo de tráfico. Ahora puede configurar los temporizadores ARP para enviar las solicitudes ARP con intervalos específicos. El intervalo de tiempo se configura en segundos. Puede configurar los intervalos de tiempo de ARP al configurar el sitio del centro de datos en la ficha **Configuración básica** de la GUI del dispositivo Citrix SD-WAN.

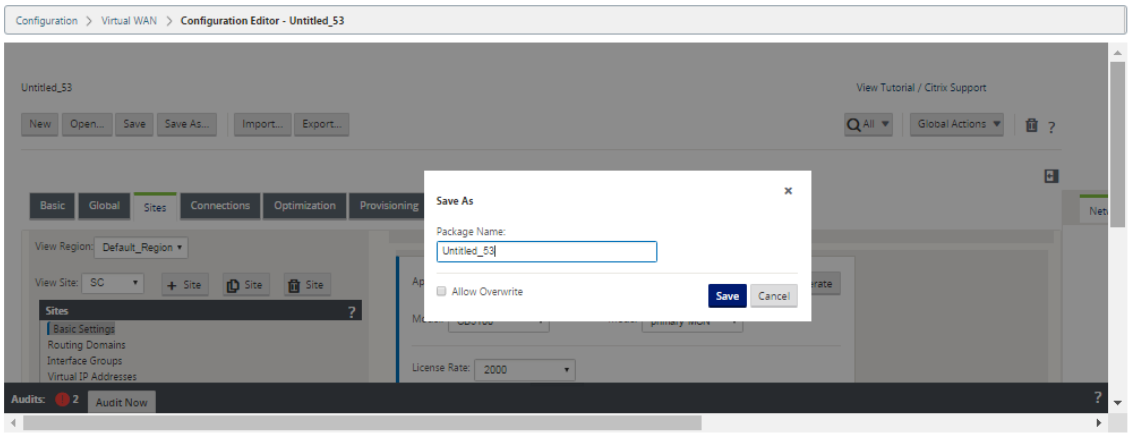
3. (Opcional, recomendado) Guarde la configuración en curso.

Si no puede completar la configuración en una sesión, puede guardarla en cualquier momento, de modo que pueda volver a completarla más tarde. La configuración se guarda en el Workspace en el dispositivo local. Para reanudar el trabajo en una configuración guardada, haga clic en **Abrir** en la barra de menús del **Editor de configuración** (parte superior del área de página). Esto muestra un cuadro de diálogo para seleccionar la configuración que quiere modificar.

> **Nota**
>
> Como precaución adicional, se recomienda utilizar **Guardar como, en lugar de**Guardar**, para evitar sobrescribir el paquete de configuración incorrecto.

Para guardar el paquete de configuración actual, haga lo siguiente:

1. Haga clic en **Guardar como** (en la parte superior del panel central del **Editor de configuración**). Se abre el cuadro de diálogo **Guardar como**.



2. Introduzca el nombre del paquete de configuración. Si está guardando la configuración en un paquete existente, asegúrese de seleccionar **Permitir sobrescritura** antes de guardar.
3. Haga clic en **Guardar**.

Cómo configurar grupos de interfaz para el MCN

Después de agregar el nuevo sitio de MCN, el siguiente paso es crear y configurar los grupos de interfaz virtual para el sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

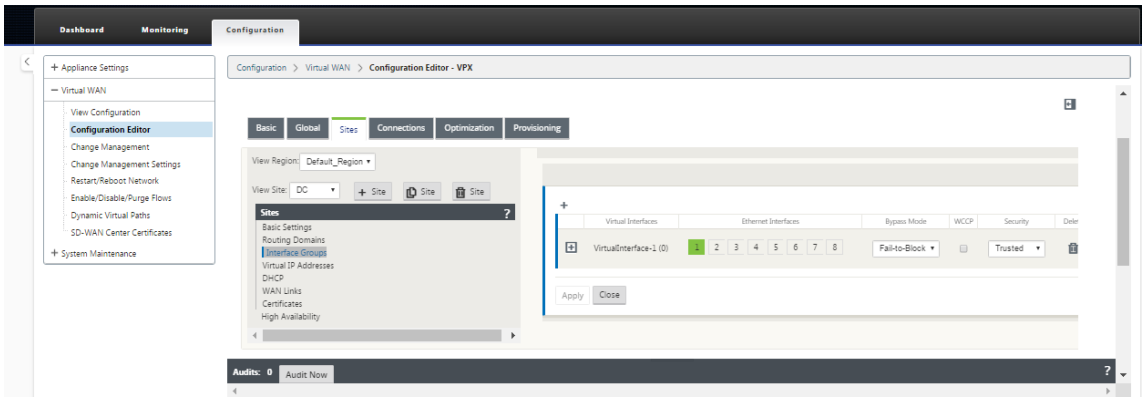
A continuación se indican algunas pautas para configurar grupos de interfaz virtual:

- Utilice nombres lógicos que describan mejor el grupo.
- Las redes de confianza son redes que están protegidas detrás de un firewall.
- Las interfaces virtuales asocian interfaces a pares Fail to Wire (FTW).
- Las interfaces WAN individuales no pueden estar en un par FTW.

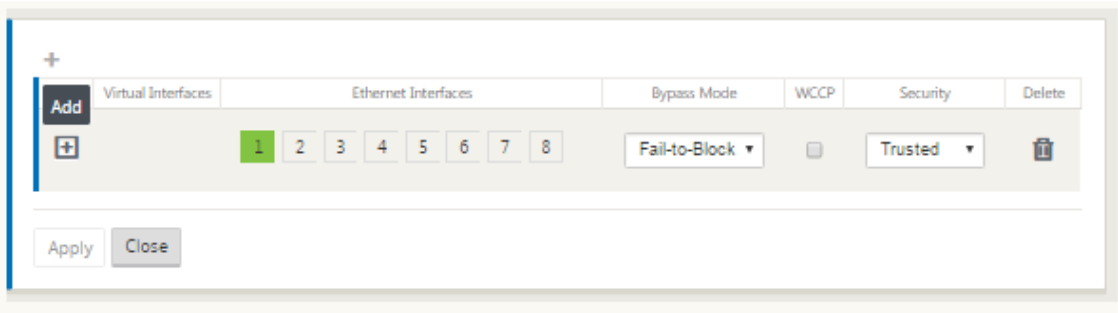
> **Nota**
>
> Para obtener más instrucciones e información sobre la configuración de grupos de interfaz virtual, consulte la sección Redirección y reenvío virtuales.

Para agregar un grupo de interfaz virtual al nuevo sitio de MCN, haga lo siguiente:

1. Continuando en la vista **Sitios** del **Editor de configuración**, seleccione el sitio en el menú implementable **Ver sitio**. Esto abre la vista de configuración del sitio seleccionado.

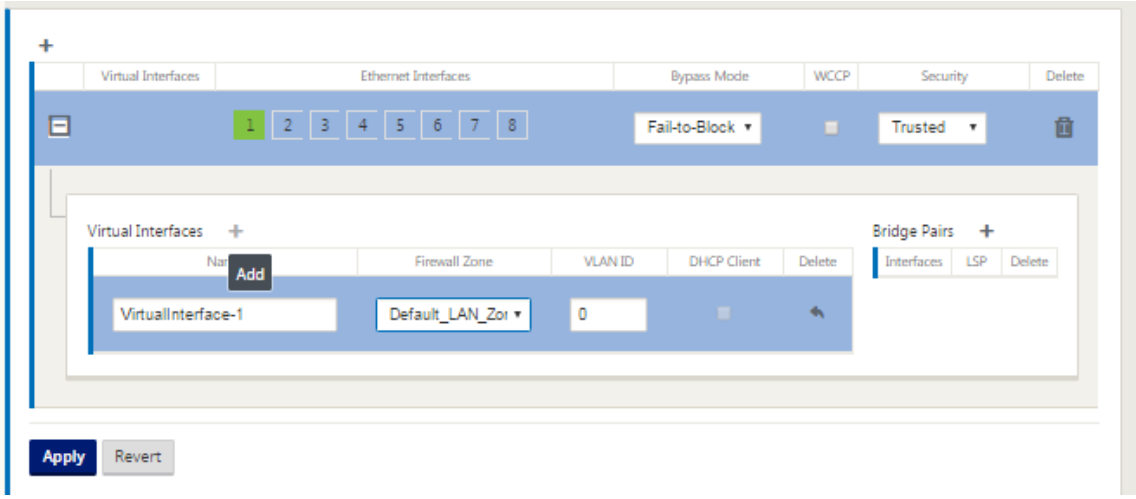


2. Haga clic en **+** para agregar el **grupo de interfaz virtual**. Esto agrega una nueva entrada de grupo de interfaz virtual en blanco a la tabla y la abre para su edición.



3. Haga clic en **+** a la derecha de **Interfaces virtuales**. Esto agrega una nueva entrada de grupo en blanco a la tabla y la abre para su edición.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



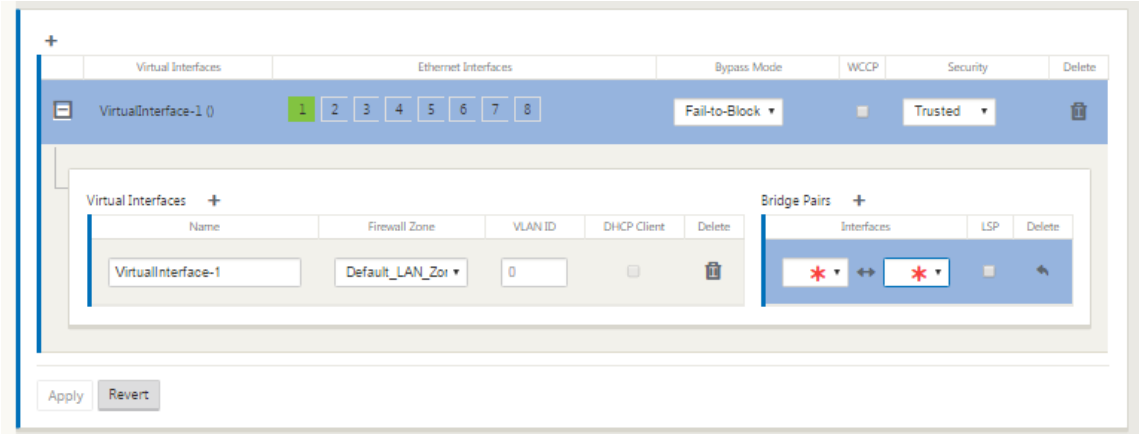
4. Seleccione las **interfaces Ethernet** que quiere incluir en el grupo. En **Interfaces Ethernet**, haga clic en una interfaz para incluir/excluir esa interfaz. Puede seleccionar cualquier número de interfaces que quiera incluir en el grupo.

5. Seleccione el **Modo de omisión** en el menú implementable (sin valor predeterminado). El **modo de omisión** especifica el comportamiento de las interfaces emparejadas en puente en el grupo de interfaz virtual, en caso de que un dispositivo o servicio falle o se reinicie. Las opciones son: **Fail-to-Wire** o **Fail-to-Block**.

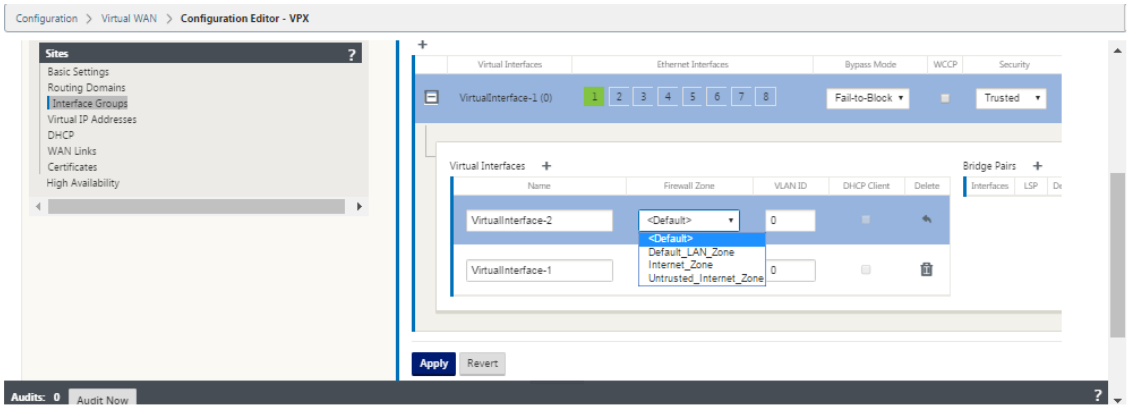
6. Seleccione el **Nivel de seguridad** en el menú implementable. Especifica el nivel de seguridad para el segmento de red del grupo de interfaz virtual. Las opciones son: De **confianza** o de **no confianza**. Los segmentos de confianza están protegidos por un firewall (el valor predeterminado es Trusted).

7. Haga clic en **+** en el borde izquierdo de la interfaz virtual que ha agregado. Muestra la tabla **Interfaces Virtuales**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Haga clic en **+** a la derecha de **Interfaces virtuales**. Esto revela los identificadores de **nombre, zona de cortafuegos** e **ID de VLAN**.



9. Introduzca el **nombre** y el **ID de VLAN** para este grupo de interfaz virtual.
   - **Nombre** : es el nombre por el que se hace referencia a esta Interfaz Virtual.
   - **Zona de cortafuegos** - Seleccione una zona de cortafuegos en el menú implementable.
   - **ID de VLAN**: Este es el ID para identificar y marcar el tráfico hacia y desde la interfaz virtual. Use un ID de 0 (cero) para el tráfico nativo/no etiquetado.

10. Haga clic en **+** a la derecha de los **pares de puentes**. Esto agrega una nueva entrada de **Bridge Pairs** y la abre para su edición.

11. Seleccione las interfaces Ethernet que se van a emparejar en los menús desplegables. Para agregar más pares, haga clic en **+** junto a **Pairs de puente** de nuevo.

12. Haga clic en **Aplicar**. Esto aplica la configuración y agrega el nuevo grupo de interfaz virtual a la tabla. En esta etapa, verá un icono amarillo de alerta de auditoría delta, a la derecha de la nueva entrada del grupo de interfaz virtual. Esto se debe a que aún no ha configurado ninguna dirección IP virtual (VIP) para el sitio. Por ahora, puede ignorar esta alerta, ya que se resuelve automáticamente cuando haya configurado correctamente las IP virtuales para el sitio.

13. Para agregar más grupos de interfaz virtual, haga clic en **+** a la derecha de la sucursal **Grupos**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de interfaz y continúe como se muestra arriba.

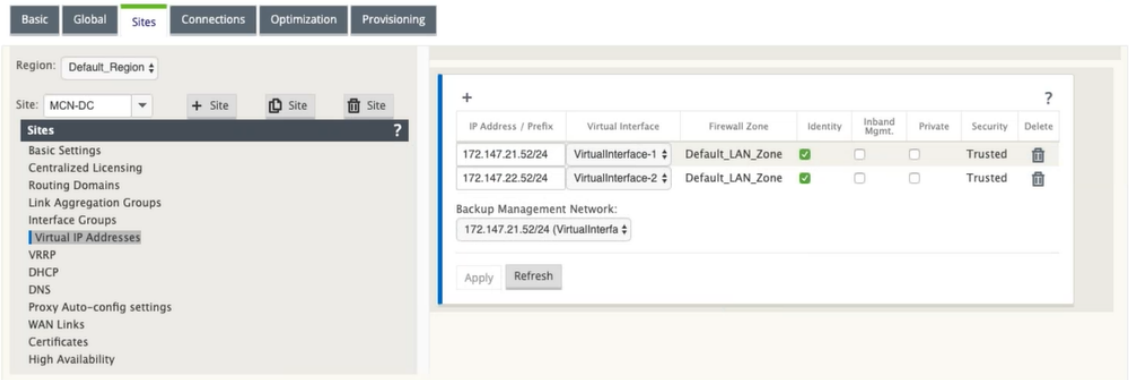
Cómo configurar la dirección IP virtual para el MCN

El siguiente paso es configurar las direcciones IP virtuales para el sitio y asignarlas al grupo apropiado.

1. Continuando en la vista **Sitios** del nuevo sitio MCN, haga clic en **+** a la izquierda de **Direcciones IP virtuales**. Muestra la tabla **Direcciones IP virtuales** para el nuevo sitio.
2. Haga clic en **+** a la derecha de **Direcciones IP virtuales** para agregar una dirección. Esto abre el formulario para agregar y configurar una nueva dirección IP virtual.
3. Introduzca la información **Dirección IP/Prefijo**y seleccione la**Interfaz Virtual** con la que está asociada la dirección. La dirección IP virtual debe incluir la dirección de host completa y la máscara de red.
4. Seleccione la configuración quiereda para la dirección IP virtual, como Zona de firewall, Identidad, Privado y Seguridad.
5. Seleccione **Administración en banda para permitir** que la dirección IP virtual se conecte a servicios de administración como la interfaz de usuario web y SSH.

   > **Nota:**
   >
   > La interfaz debe ser del tipo de seguridad **Confiable** e **Identidad** habilitada.

6. Seleccione una IP virtual como una **red de administración de copias de seguridad**. Esto le permite utilizar la dirección IP virtual para la administración si el puerto de administración no está configurado con una Gateway predeterminada.



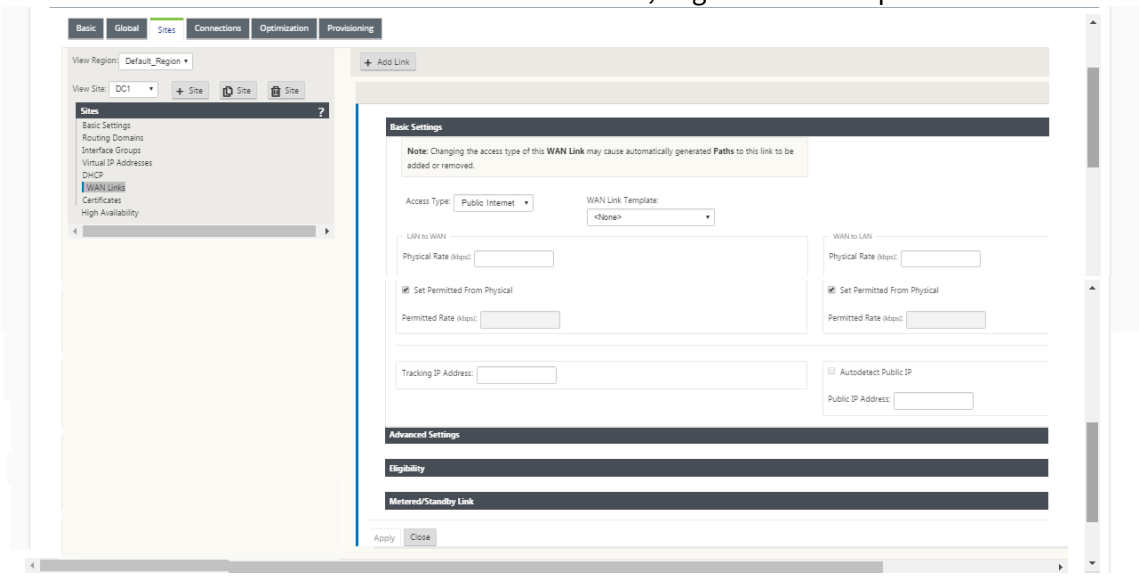
7. Haga clic en **Aplicar**. Esto agrega la información de dirección al sitio y la incluye en la tabla **Direcciones IP virtuales** del sitio.
8. Para agregar más direcciones IP virtuales, haga clic en **+** a la derecha de las **Direcciones IP virtuales**y continúe como se indica anteriormente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

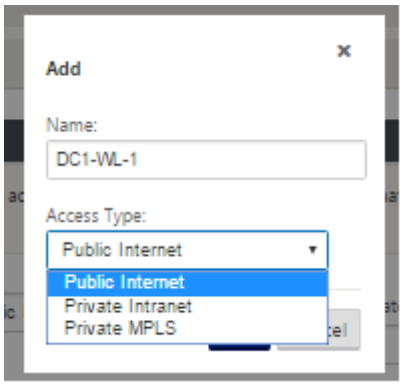
Cómo configurar enlaces WAN para el MCN

El siguiente paso es configurar los enlaces WAN para el sitio.

1. Continuando en la vista **Sitios** del nuevo sitio de MCN, haga clic en la etiqueta **Enlaces WAN**.



2. Haga clic en **Agregar vínculo** a la derecha de los **enlaces WAN** para agregar un nuevo enlace WAN. Esto abre el cuadro de diálogo **Agregar**.

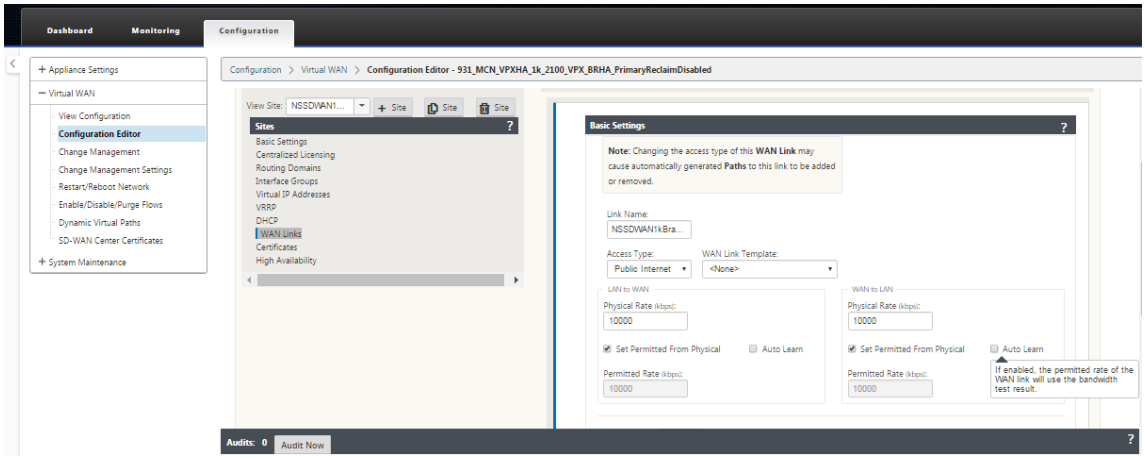


3. (Opcional) Escriba un nombre para el enlace WAN si no quiere utilizar el valor predeterminado. El valor predeterminado es el nombre del sitio, anexado con el siguiente sufijo: WL- <number>, donde <number> es el número de enlaces WAN para este sitio, incrementado en uno.

4. Seleccione **Tipo de acceso** en el menú implementable. Las opciones son **Internet público, Intranet privadao MPLS privado.**

5. Haga clic en **Agregar**. Esto muestra la página de configuración básica de **enlaces WAN** y agrega el nuevo enlace WAN no configurado a la página.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

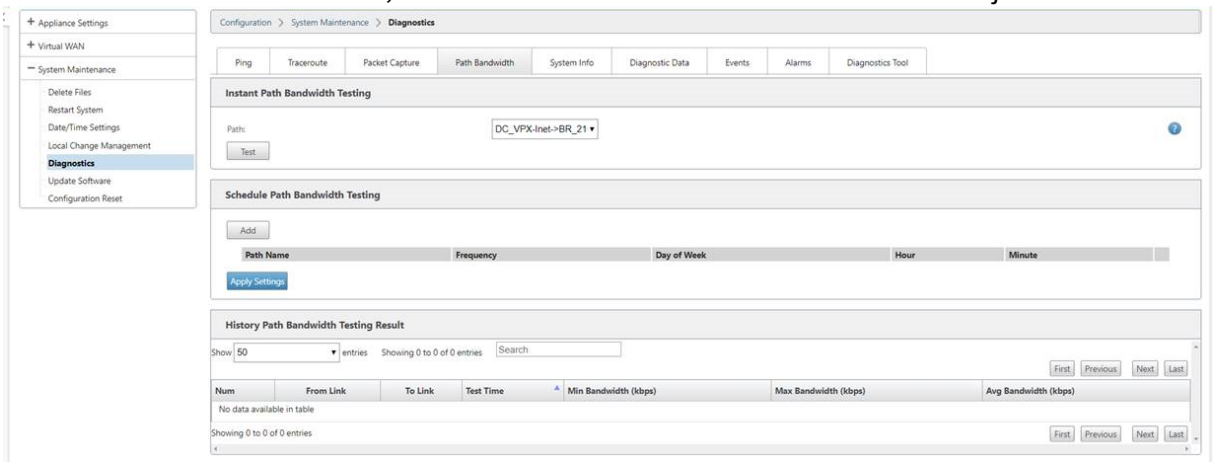


Aprendizaje automático del consumo de ancho de banda

El aprendizaje automático se ejecuta en el inicio del sistema y se repite cada cinco minutos hasta que se observa un resultado correcto. El aprendizaje automático también se ejecuta después de que se realicen cambios en la configuración del enlace WAN desde el editor de configuración.

Puede ejecutar pruebas manualmente o programar pruebas en la GUI de SD-WAN. Los resultados de estas pruebas también deben aplicarse a la tasa permitida cuando la prueba tenga éxito y el aprendizaje automático esté habilitado.

Cuando se utiliza el aprendizaje automático en redes grandes, si el cambio de configuración se reinicia, todos los sitios ejecutan pruebas simultáneamente en el MCN, causando un alto uso de ancho de banda que conduce a resultados inexactos. Se recomienda programar pruebas de ancho de banda una o dos veces al día, normalmente cuando el volumen de tráfico es bajo.



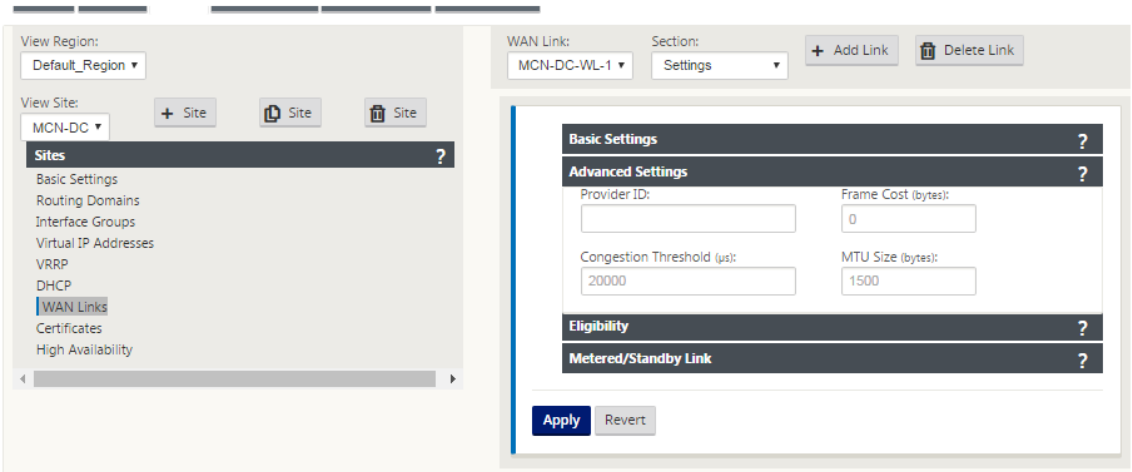
1. Introduzca los detalles del vínculo para el nuevo enlace WAN. Configure la configuración de LAN a WAN, WAN a **LAN**. Algunas directrices son las siguientes:

    - Algunos enlaces a Internet pueden ser asimétricos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La configuración incorrecta de la velocidad permitida puede afectar negativamente al rendimiento de ese enlace
- Evite utilizar velocidades de ráfaga que superen la velocidad comprometida.
- Para los enlaces WAN de Internet, asegúrese de agregar la Dirección IP pública.

2. Haga clic en la barra de sección **Configuración avanzada** gris. Esto abre el formulario **Configuración avanzada** del vínculo.



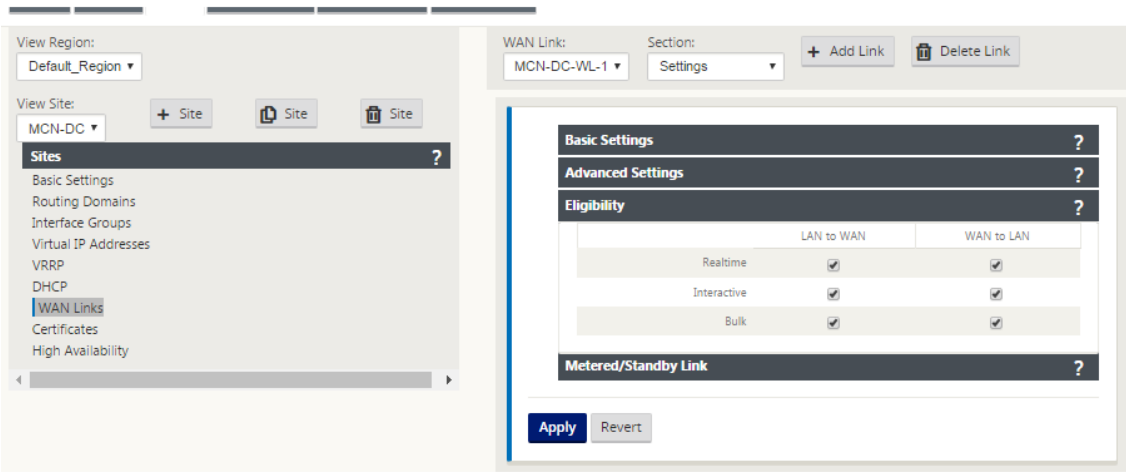
3. Introduzca la **Configuración avanzada** para el enlace:

   - **ID** de proveedor: (Opcional) Introduzca un número de ID único 1 a 100 para designar enlaces WAN conectados al mismo proveedor de servicios. La WAN virtual utiliza el Id. de proveedor para diferenciar rutas al enviar paquetes duplicados.
   - **Coste de trama (bytes)**: Introduzca el tamaño (en bytes) del encabezado/remolque agregado a cada paquete. Por ejemplo, el tamaño en bytes de los remolques Ethernet IPG o AAL5 agregados.
   - **Umbral** de congestión: Introduzca el umbral de congestión (en microsegundos) después del cual el enlace WAN limita la transmisión de paquetes para evitar una mayor congestión.
   - **Tamaño de MTU (bytes)**: Introduzca el tamaño de paquete sin procesar más grande (en bytes), sin incluir el coste de trama.

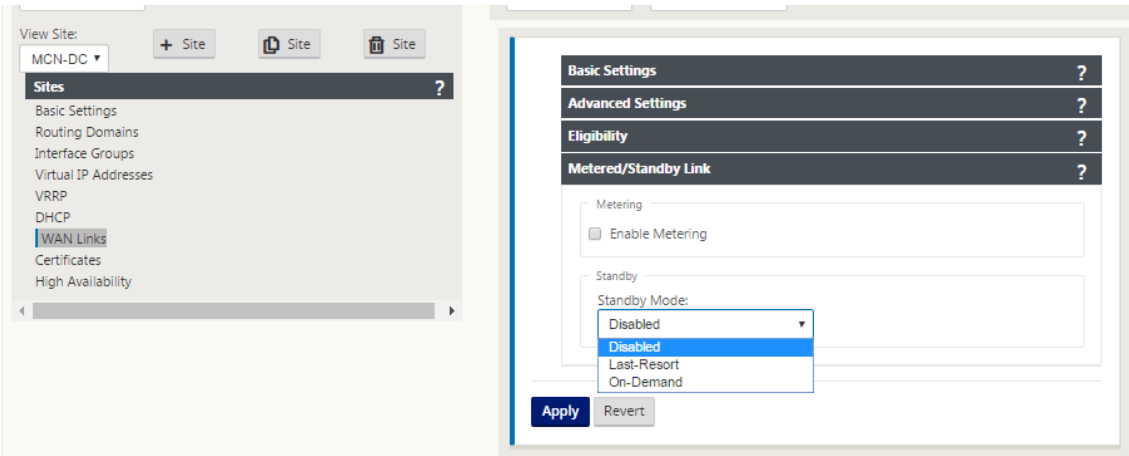
4. Haga clic en la barra de sección de **elegibilidad** gris. Esto abre el formulario Configuración de **elegibilidad** para el vínculo.

5. Seleccione la configuración de **elegibilidad** para el enlace.

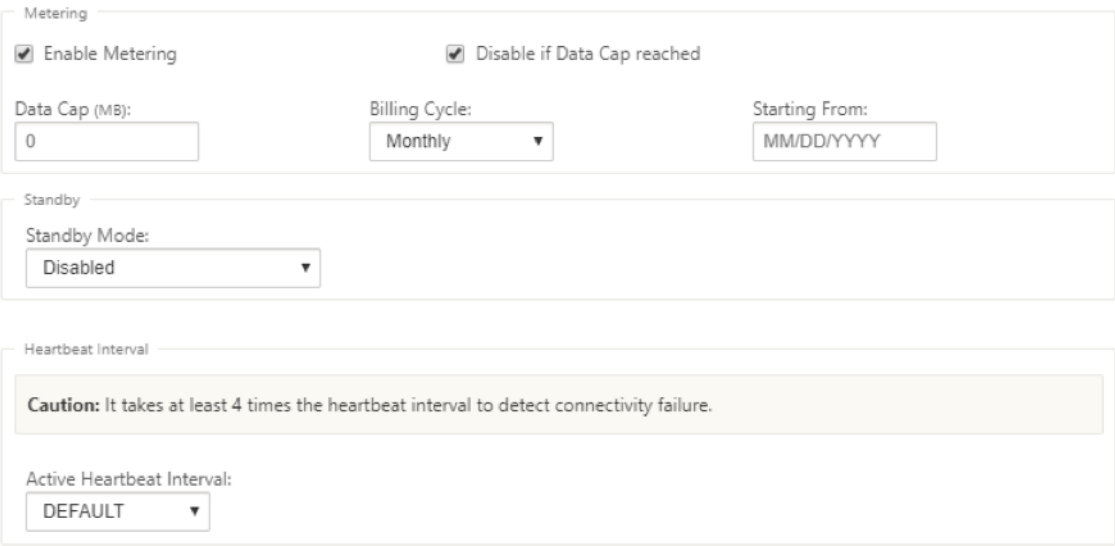
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Haga clic en la barra de sección **Vínculo medido** gris. Esto abre el formulario de configuración de **Vínculo medido** para el vínculo.
7. (Opcional) Seleccione **Activar medición** para habilitar la medición para este vínculo. Muestra los campos **Habilitar configuración de medición**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Configure los parámetros de medición para el enlace. Escriba lo siguiente:

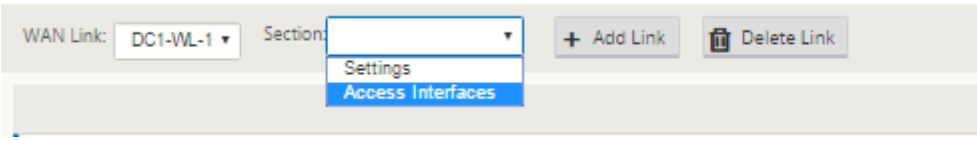
- **Límite de datos (MB)**: Introduzca la asignación de límite de datos para el vínculo, en megabytes.
- **Ciclo** de facturación: seleccione **Mensual o Semanal** en el menú desplegable.
- Empezar **desde**: Introduzca la fecha de inicio del ciclo de facturación.
- Establecer **último recurso** : seleccione esta opción para habilitar este enlace como enlace de último recurso en caso de que se produzcan errores en todos los demás enlaces disponibles. En condiciones WAN normales, la WAN virtual envía solo un tráfico mínimo a través de enlaces medidos, para comprobar el estado del vínculo. Sin embargo, en caso de fallo, SD-WAN puede utilizar vínculos medidos activos como último recurso para reenviar el tráfico de producción.

Haga clic en **Aplicar**. Esto aplica la configuración especificada al nuevo enlace WAN.

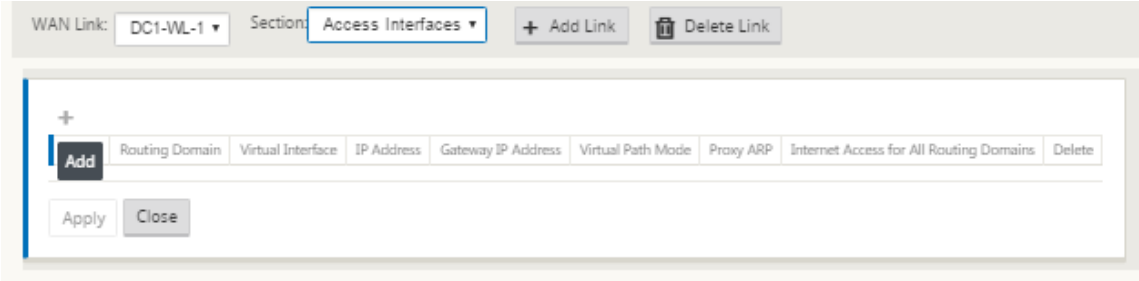
El siguiente paso es configurar las interfaces de acceso para el nuevo enlace WAN. Una interfaz de acceso consta de una interfaz virtual, una dirección IP de punto final WAN, una dirección IP de puerta de enlace y un modo de ruta virtual definido colectivamente como una interfaz para un enlace WAN específico. Cada enlace WAN debe tener al menos una interfaz de acceso.

Cómo configurar la interfaz de acceso:

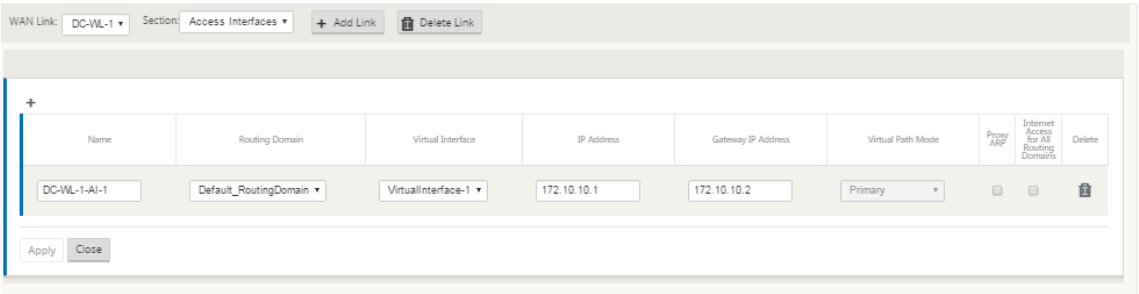
1. Seleccione **Interfaces de Acceso** en la página de configuración de Enlace WAN para el vínculo. Esto abre la vista **Interfaces de acceso** para el sitio.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Haga clic en **+** para agregar una interfaz. Esto agrega una entrada en blanco a la tabla y la abre para su edición. Introduzca la configuración de **las interfaces de acceso** para el vínculo. Cada enlace WAN debe tener al menos una interfaz de acceso.



3. Escriba lo siguiente:

- Nombre: Este es el nombre por el que se hace referencia a esta interfaz de acceso. Escriba un nombre para la nueva interfaz de acceso o acepte el valor predeterminado. El valor predeterminado utiliza la siguiente convención de nomenclatura:
  WAN_LINK_NOMBRE-AI-Number: Donde *WAN_LINK_NAME* es el nombre del vínculo WAN que está asociando a esta interfaz y número es el número de interfaces de acceso configuradas actualmente para este vínculo, incrementado en 1.

> **Nota**
>
> Si el nombre aparece truncado, puede colocar el cursor en el campo y, a continuación, mantener pulsado el ratón y mover el ratón hacia la derecha o hacia la izquierda para ver la parte truncada.

- **Interfaz virtual**: Esta es la interfaz virtual que utiliza esta interfaz de acceso. Seleccione una entrada del menú desplegable de Interfaces virtuales configuradas para este sitio de sucursal.
- **Dominio de enrutamiento**: El dominio de enrutamiento que quiere elegir para la interfaz de acceso.
- **Dirección IP**: Dirección IP del extremo de la interfaz de acceso desde el dispositivo a la WAN.
- **Dirección IP de la puerta de enlace**: Esta es la dirección IP del enrutador de la puerta de enlace.
- **Modo de ruta virtual**: Especifica la prioridad del tráfico de ruta virtual en este enlace WAN. Las opciones son: **Principal**, **Secundario**o **Excluir**. Si se establece en **Excluir**, esta interfaz de acceso se utiliza solo para el tráfico de Internet e Intranet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Proxy ARP**: Seleccione la casilla de verificación que desea activar. Si está habilitada, Virtual WAN Appliance responde a las solicitudes ARP para la dirección IP de la Gateway, cuando la puerta de enlace es inalcanzable.

1. Haga clic en **Aplicar**.

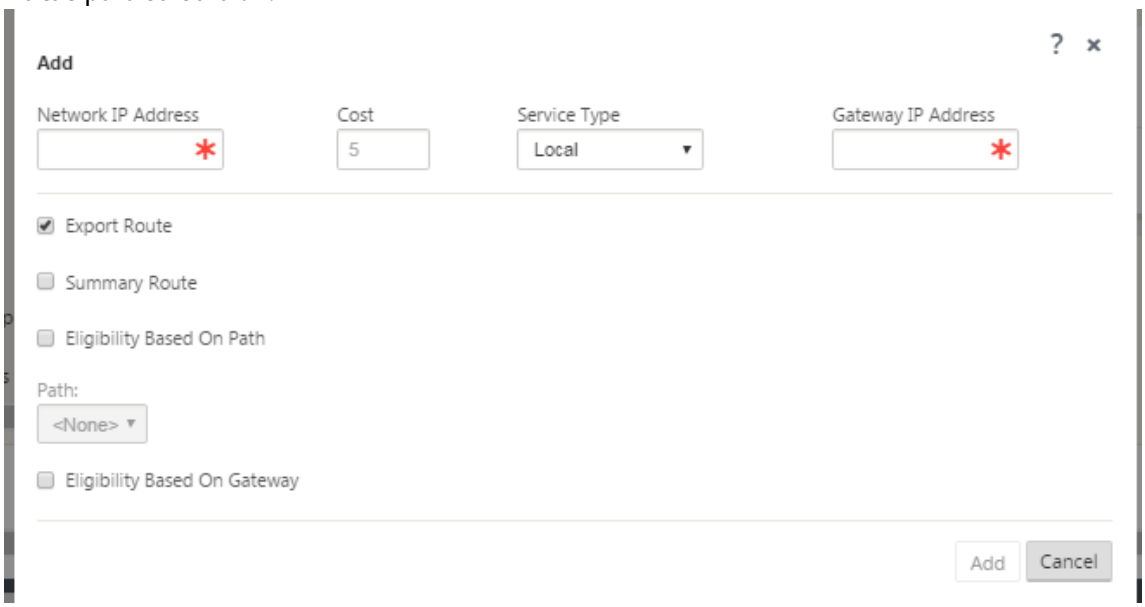
Ya ha terminado de configurar el nuevo enlace WAN. Repita estos pasos para agregar y configurar más enlaces WAN para el sitio.

El siguiente paso es agregar y configurar las rutas para el sitio.

Cómo configurar rutas para el MCN

Para agregar y configurar las rutas para el sitio, haga lo siguiente:

1. Haga clic en la vista **Conexiones** para el nuevo sitio de MCN y seleccione **Rutas**. Muestra la vista **Rutas** del emplazamiento.
2. Haga clic en **+** a la derecha de **Rutas** para agregar una ruta. Esto abre el cuadro de diálogo **Rutas** para su edición.



3. Introduzca la información de configuración de ruta para la nueva ruta. Escriba lo siguiente:

- **Dirección IP de red**: Introduzca la **dirección IP de red**.
- **Coste**: Introduzca un peso de 1 a 15 para determinar la prioridad de ruta para esta ruta. Las rutas de menor coste tienen prioridad sobre las rutas de mayor coste. El valor predeterminado es 5.
- **Tipo de servicio**: Seleccione el tipo de servicio para la ruta en el menú implementable de este campo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Opciones disponibles:

- **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. Esto se logra midiendo y adaptándose constantemente a la demanda cambiante de las aplicaciones y a las condiciones WAN. Los dispositivos SD-WAN miden la red por trayecto. 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 sitios de Internet público. El tráfico de este tipo no está encapsulado. Durante los tiempos de 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 Intranet de acuerdo con la configuración de SD-WAN establecida por el Administrador.
- **Intranet**: Este servicio administra el tráfico de Intranet de empresa que no se ha definido para su transmisión a través de una ruta de acceso virtual. Al igual que con el tráfico de Internet, permanece sin encapsular y la SD-WAN administra el ancho de banda limitando la velocidad de este tráfico en relación con otros tipos de servicios durante los tiempos de congestión. En determinadas condiciones, y si se configura para la repliegue de intranet en la ruta de acceso virtual, el tráfico que normalmente viaja por una ruta de acceso virtual se puede tratar como tráfico de intranet, para mantener la fiabilidad de la red.
- **PassThrough**: Este servicio administra el tráfico que se va a pasar a través de la WAN virtual. El tráfico dirigido al Servicio de paso incluye difusiones, ARP y otro tráfico no IPv4, así como el tráfico en la subred local del Dispositivo WAN virtual, subredes configuradas o Reglas aplicadas por el Administrador de red. El SD-WAN no retrasa, da forma ni modifica este tráfico. Por lo tanto, debe asegurarse de que el tráfico PassThrough no consume recursos sustanciales en los enlaces WAN que el dispositivo SD-WAN está configurado para utilizar para otros servicios.
- **Local**: Este servicio administra el tráfico IP local en el 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 GRE LAN configurado en el sitio. La función Túnel GRE le permite configurar los dispositivos SD-WAN para terminar los túneles GRE en la LAN. Para una ruta con el tipo de servicio GRE Tunnel, la Gateway debe residir en una de las subredes de túnel del túnel GRE local.
- **Túnel IPSec LAN**: Este servicio administra el tráfico IP destinado al túnel IPSec.
- **Dirección IP de la puerta** de enlace: Introduzca la **dirección IP de la puerta** de enlace para esta ruta.
- **Elegibilidad** - Basado en ruta (casilla de verificación) - (Opcional) Si está activada, la ruta no recibe tráfico cuando la ruta seleccionada está desactivada.
- **Ruta**: Especifica la ruta que se utilizará para determinar la elegibilidad de la ruta.

Dependiendo del Tipo de servicio, se muestran los siguientes ajustes:

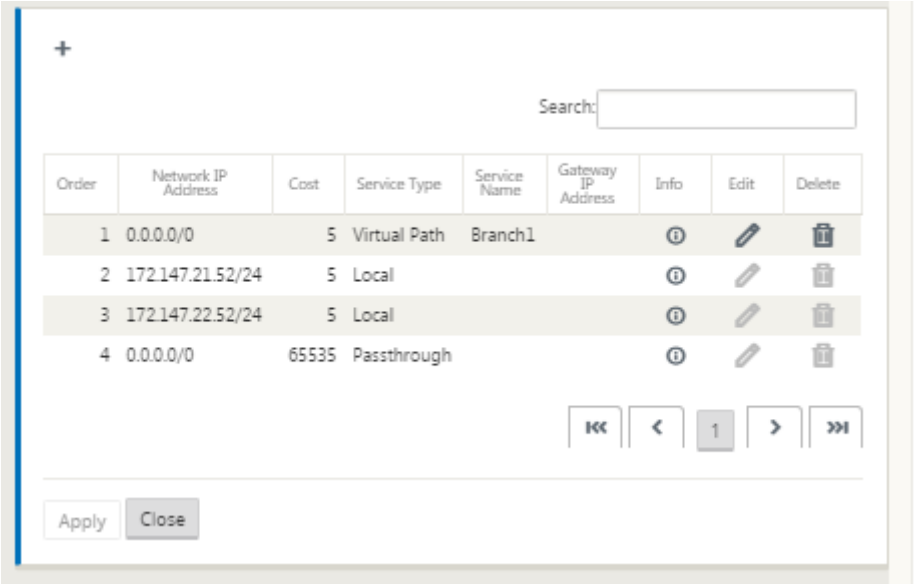
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tipo de servicio	Configuración del tipo de servicio
Ruta virtual	Sitio de salto siguiente: Indica el sitio remoto al que se dirigen los paquetes de ruta virtual.
Internet	Exportar ruta: Activar/Inhabilitar para exportar rutas a otros sitios conectados, Elegibilidad basada en la ruta
Intranet	Ruta de exportación, servicio de intranet, Elegibilidad basada en la ruta, Elegibilidad basada en el túnel
Paso a través	Elegibilidad basada en la ruta
Locales	Ruta de exportación, Ruta de resumen, Elegibilidad basada en ruta
Túnel GRE	Ruta de exportación, Elegibilidad basada en la ruta, Elegibilidad basada en la puerta de enlace
Túnel IPSec	Ruta de exportación, Elegibilidad basada en ruta, Túnel IPSec, Elegibilidad basada en túnel
Descartar	Ruta de exportación, Ruta de resumen

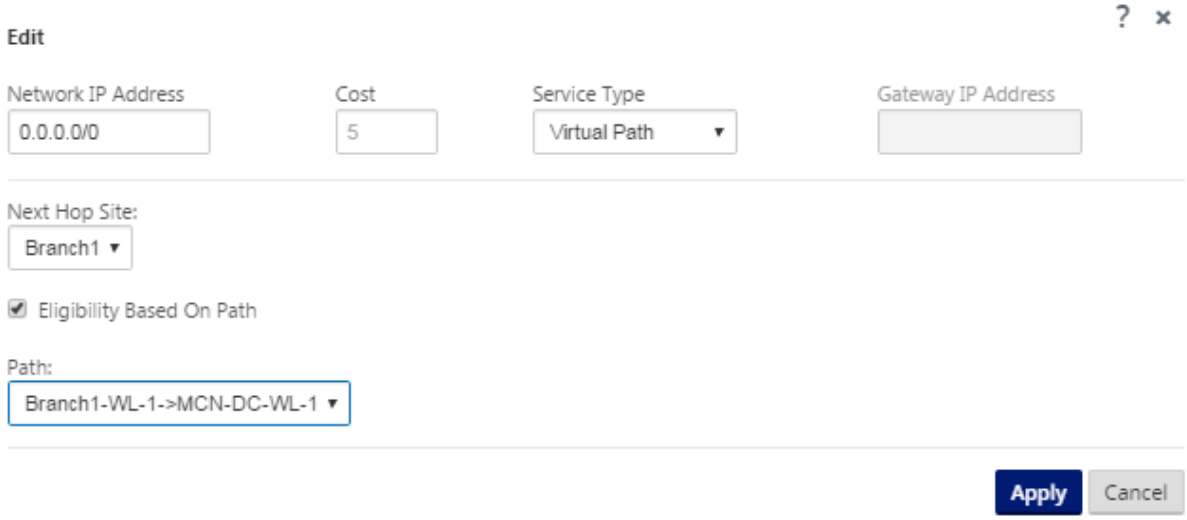
1. Haga clic en **Aplicar**.

> **Nota**
>
> Después de hacer clic en **Aplicar**, es posible que aparezcan advertencias de auditoría que indiquen que es necesario realizar más acciones. Un punto rojo o un icono delta de vara dorada indica un error en la sección donde aparece. Puede utilizar estas advertencias para identificar errores o falta información de configuración. Pase el cursor sobre un icono de advertencia de auditoría para mostrar una breve descripción de los errores en esa sección. También puede hacer clic en la barra de estado **Auditorías** de color gris oscuro (parte inferior de la página) para mostrar una lista completa de todas las advertencias de auditoría.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



También puede modificar las rutas configuradas de la siguiente manera.



Para agregar más rutas para el sitio, haga clic en **+** a la derecha de la sucursal **Rutas** y proceda como se indica anteriormente.

Ya ha terminado de introducir la información de configuración principal para el nuevo sitio de MCN. Las dos secciones siguientes proporcionan instrucciones para más pasos opcionales:

- Configuración de alta disponibilidad (HA) para el sitio de MCN (opcional).
- Habilitación y configuración de la seguridad y el cifrado de la WAN virtual (opcional).

Si no quiere configurar estas funciones ahora, puede pasar directamente a la sección Asignación de nombres, almacenamiento y copia de seguridad de la configuración del sitio de MCN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

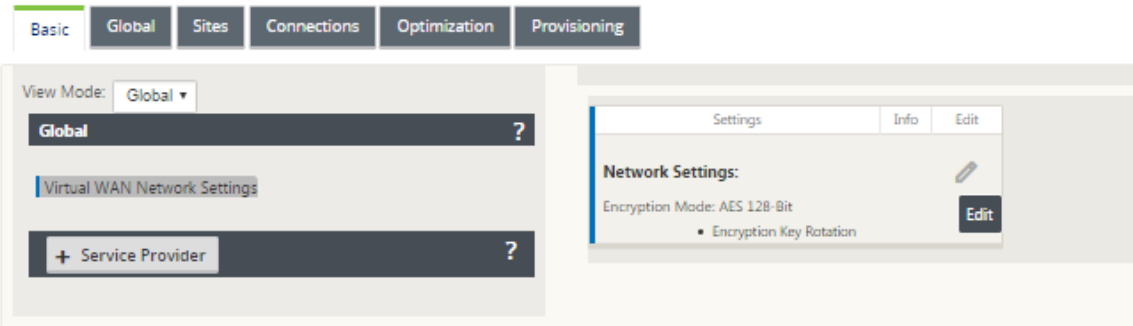
Habilitar y configurar la seguridad y el cifrado de la WAN virtual (opcional)

May 7, 2021

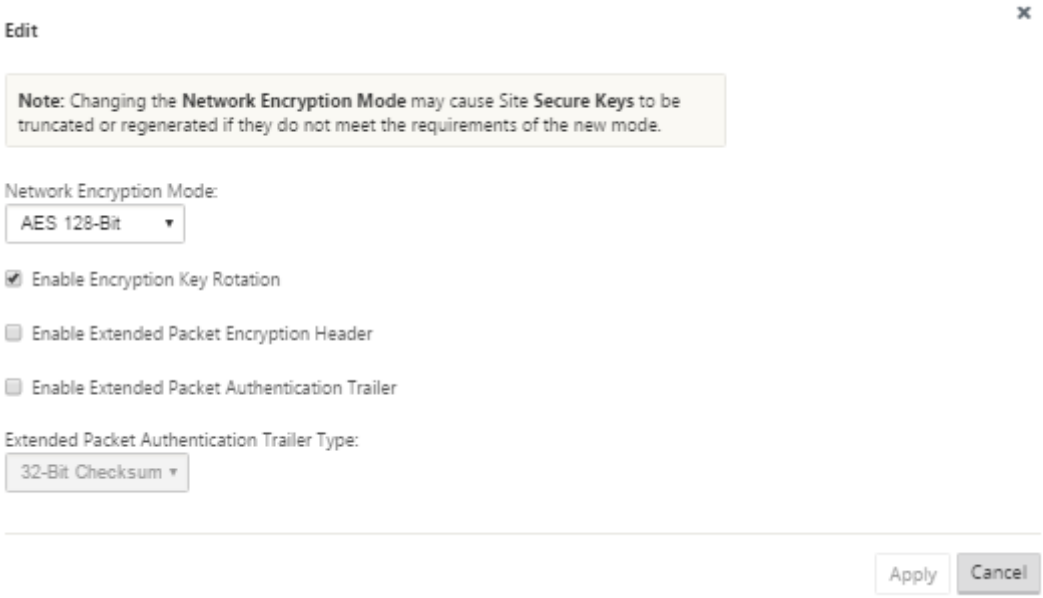
Para habilitar y configurar la seguridad y el cifrado de la WAN virtual, haga lo siguiente:

> **Nota**
>
> Habilitar la seguridad y el cifrado de la WAN virtual es opcional.

1. Acceda a la ficha **Básico** del **Editor de configuración**, Seleccionar **global** en el modo **Vista**. Se muestra el formulario de configuración de la red virtual.



2. Haga clic en **Modificar** (icono de lápiz) para habilitar la edición del formulario.



3. Introduzca la configuración de seguridad global. Opciones disponibles:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Modo de cifrado de red**: Es el algoritmo de cifrado utilizado para las rutas cifradas. Seleccione una de las siguientes opciones en el menú implementable: **AES 128 Bits** o **AES 256 Bits**.
- **Habilitar rotación de claves de cifrado**: Cuando está activada, las claves de cifrado se giran a intervalos de 10 a 15 minutos.
- **Habilitar encabezado de cifrado de paquetes extendido**: Cuando está habilitado, un contador cifrado de 16 bytes se antepone al tráfico cifrado para que sirva como vector de inicialización y aleatorice el cifrado de paquetes.
- **Habilitar Trailer de autenticación de paquetes extendida**: Cuando está habilitado, se agrega un código de autenticación al contenido del tráfico cifrado para verificar que el mensaje se entrega sin cambios.
- **Tipo de remolque de autenticación de paquetes extendida**: Este es el tipo de remolque utilizado para validar el contenido del paquete. Seleccione una de las siguientes opciones en el menú implementable: **Suma de comprobación de 32 bits** o **SHA-256**.

4. Haga clic en **Aplicar** para aplicar los ajustes a la configuración.

Esto completa la configuración del sitio de MCN. El siguiente paso consiste en nombrar y guardar la nueva configuración del sitio de MCN (opcional, pero recomendado), tal y como se describe en la siguiente sección.

> **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. A continuación, debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por esta razón, se recomienda guardar el paquete de configuración con frecuencia, o en puntos clave de la configuración.

Configurar MCN secundario

October 27, 2021

Puede configurar un sitio como MCN secundario para admitir la redundancia de MCN. El MCN secundario supervisa continuamente el estado del MCN primario. Si el MCN principal falla, el MCN secundario asume la función del MCN. Para crear un MCN secundario, mientras agrega un nuevo sitio en la opción **Modo**, seleccione MCN secundario. Puede configurar manualmente la interfaz virtual, la IP virtual, el enlace WAN y otros parámetros. Del mismo modo, también puede configurar un RCN secundario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> No confunda la configuración MCN secundaria con la configuración de alta disponibilidad. En la configuración de MCN secundaria, un sitio de sucursal o cliente en una ubicación geográfica diferente se configura como MCN secundario para permitir la recuperación ante desastres. En la configuración de alta disponibilidad, se configuran dos dispositivos con la misma subred o ubicación geográfica para garantizar la tolerancia a fallos. Para obtener información sobre cómo configurar la configuración de alta disponibilidad, consulte Implementación de alta disponibilidad.

Puede elegir un modelo de dispositivo para MCN secundario según el uso, los requisitos de ancho de banda y el número de sitios admitidos.

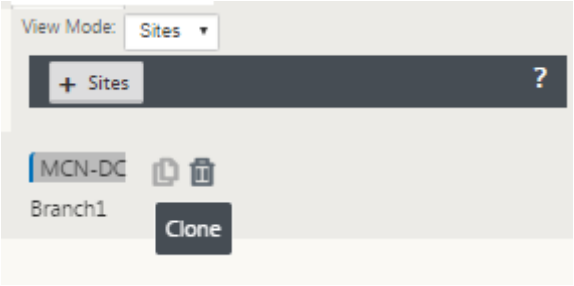
El cambio de MCN primario a MCN secundario se produce después de 15 segundos de que el MCN primario está inactivo. No se puede configurar la recuperación principal para el MCN secundario; la recuperación principal se produce automáticamente después de que el dispositivo principal vuelve a encenderlo y caduca el temporizador de espera.

La mejor manera de configurar un MCN secundario sería clonar el MCN existente, ya que conserva la mayor parte de la configuración de MCN. Cuando se clona un sitio, se copia todo el conjunto de opciones de configuración del sitio y se muestra en una única pantalla de formulario. A continuación, puede modificar la configuración de acuerdo con los requisitos de forma rápida y sencilla.

> **Nota**
>
> Puede clonar un MCN para crear un MCN secundario o sitios de sucursales. Solo puede configurar un MCN secundario.

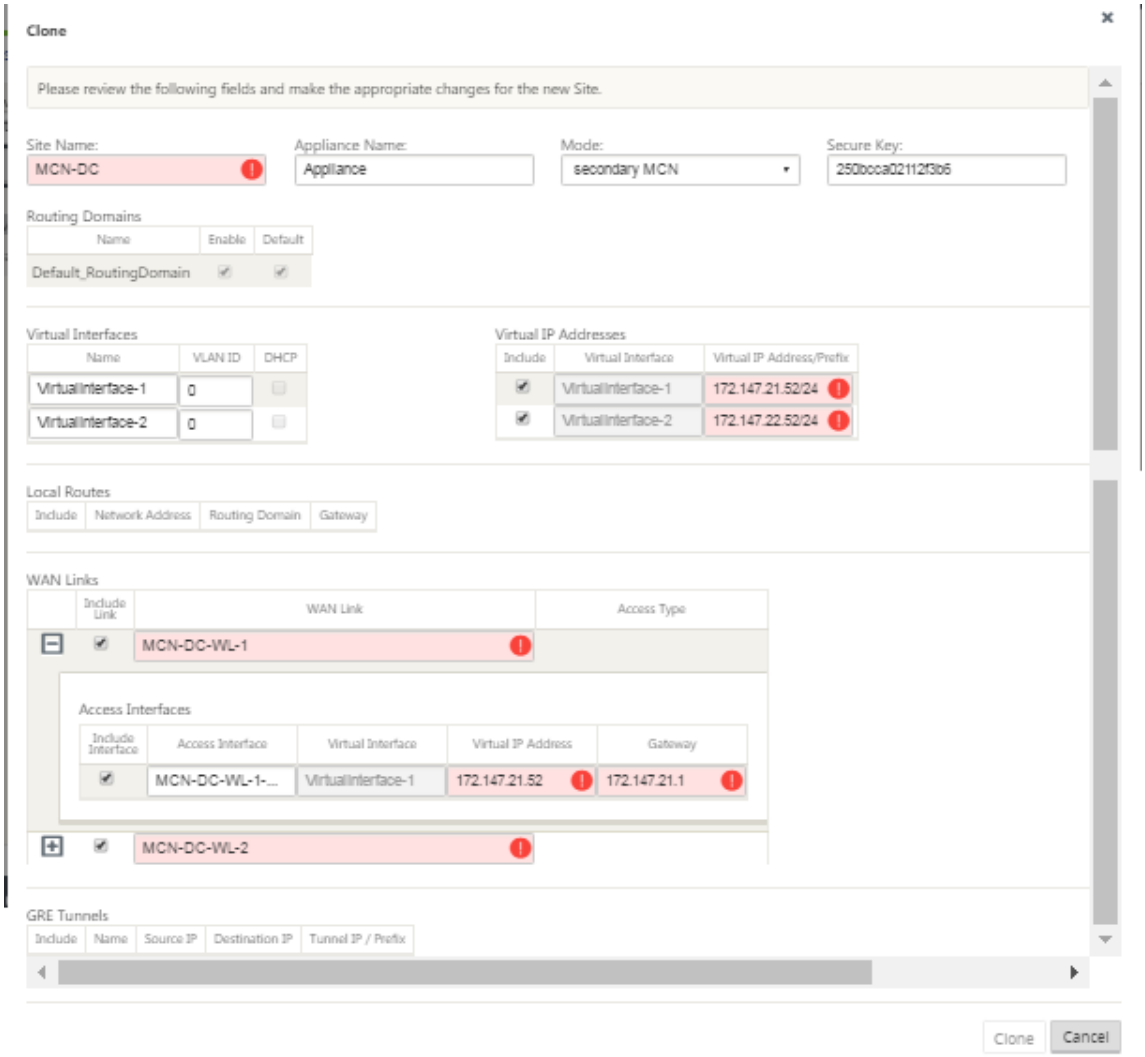
Para clonar un sitio de MCN y crear un MCN secundario:

1. En el Editor de configuración, vaya a **Básico** > **Sitios** y haga clic en el icono de clon del sitio MCN.



2. Introduzca los parámetros de configuración para el nuevo emplazamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**:
>
> Un campo resaltado con un icono de alerta de auditoría (punto rojo) indica un parámetro obligatorio que debe tener un valor distinto del valor actual.

3. En el campo **Modo**, seleccione **MCN secundario**. Resolver todas las alertas de auditoría
4. Haga clic en **Clonar** para crear el sitio de MCN secundario.

Administrar configuración de MCN

May 7, 2021

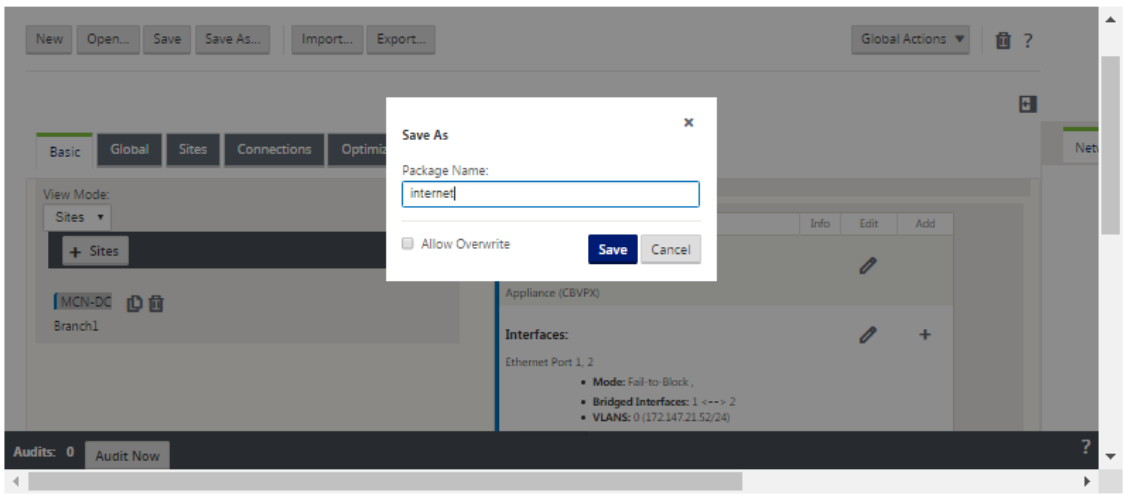
El siguiente paso es nombrar y guardar la nueva configuración, vista también como un paquete de configuración. Este paso es opcional en este punto de la configuración, pero se recomienda. El paquete

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de configuración se guarda en el Workspace del dispositivo local. A continuación, cierre la sesión de la Interfaz Web de administración y continúe el proceso de configuración más tarde. Sin embargo, si cierra la sesión, debe volver a abrir la configuración guardada cuando reanude. A continuación se proporcionan instrucciones para abrir una configuración guardada.

> **Advertencia**
>
> Si el tiempo de espera de la sesión de consola o se cierra la sesión de Management Web Interface antes de guardar la configuración, se perderán los cambios de configuración no guardados. Debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por esta razón, se recomienda guardar el paquete de configuración con frecuencia, o en puntos clave de la configuración.
> Sugerencia:
>
> Como precaución adicional, se recomienda que utilice Guardar como, en lugar de Guardar, para evitar sobrescribir el paquete de configuración incorrecto.

1. Haga clic en **Guardar como** (en la parte superior del panel central del **Editor de configuración**). Se abrirá el cuadro de diálogo **Guardar como**.



2. Escriba el nombre del paquete de configuración.

> **Nota**
>
> Si está guardando la configuración en un paquete de configuración existente, asegúrese de seleccionar **Permitir sobrescritura** antes de guardarla.

3. Haga clic en **Guardar**.

> **Nota**
>
> Después de guardar el archivo de configuración, puede cerrar la sesión de Management Web Interface y continuar el proceso de configuración más adelante. Sin embargo, si cierra

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> la sesión, debe volver a abrir la configuración guardada cuando reanude. Las instrucciones se proporcionan en la sección.Cargar un paquete de configuración guardado en el Editor de configuración

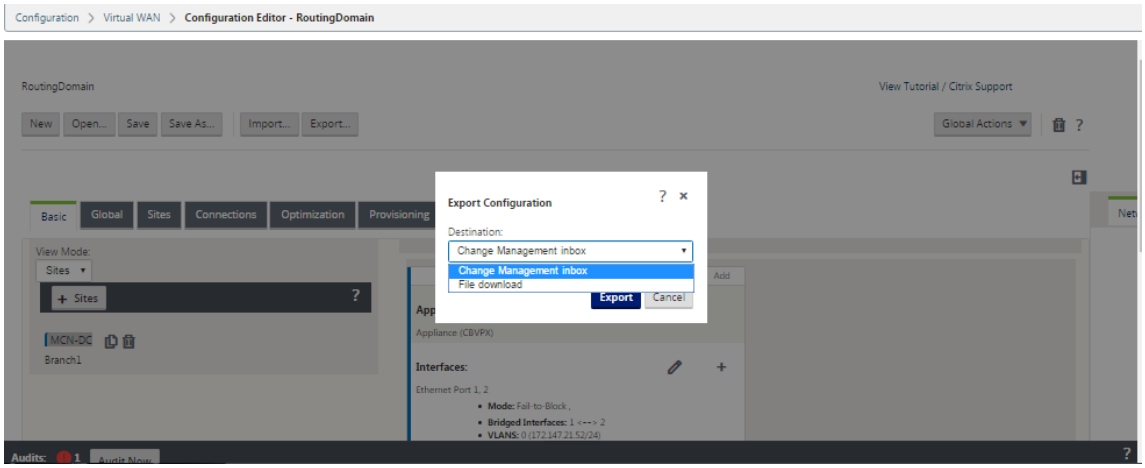
Ahora ha completado la configuración del sitio de MCN y ha creado un nuevo paquete de configuración de SD-WAN. Ahora está listo para agregar y configurar los sitios de sucursal. Las instrucciones se proporcionan en setup Branch Sites](/es-es/citrix-sd-wan/11/configuration/setup-branch-nodes.html).

Exportar copia de seguridad del paquete de configuración

Además de guardar la configuración en curso en el Workspace del dispositivo, se recomienda que también realice periódicamente una copia de seguridad de la configuración en el equipo local.

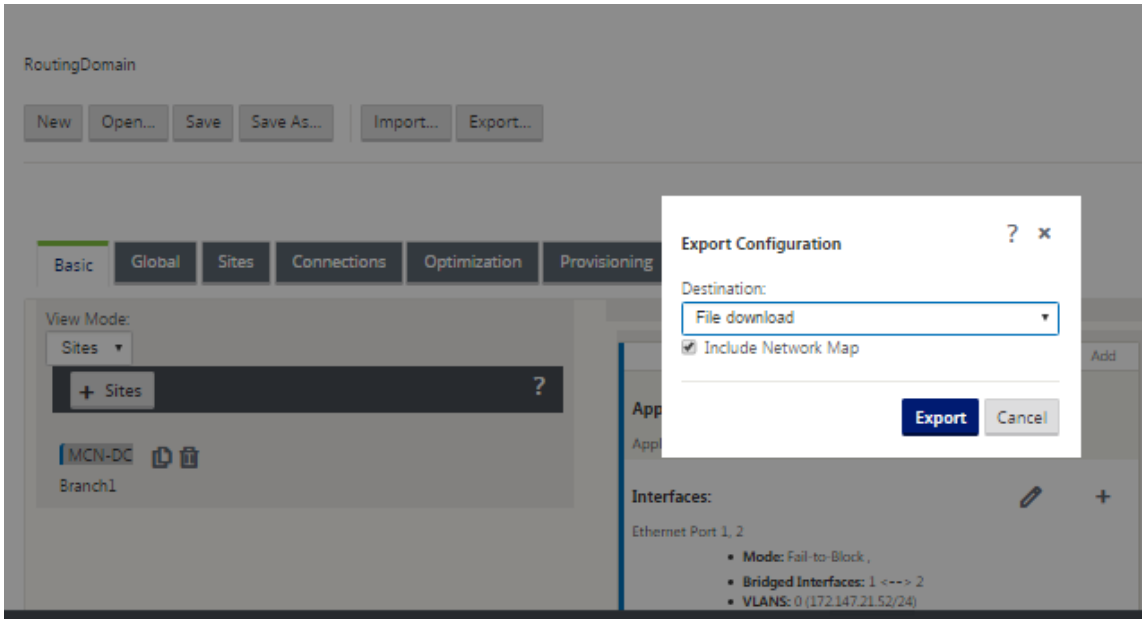
Para exportar el paquete de configuración actual a su PC, haga lo siguiente:

1. Haga clic en **Export**. Muestra el cuadro de diálogo **Configuración de exportación**.



2. Seleccione **Descarga de archivos** en el menú implementable **Destino:**. Esto revela la opción **Incluir mapa de red**, que está seleccionada de forma predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Acepte el valor predeterminado y haga clic en **Exportar**. Esto incluye la información de **mapa de red** en el paquete de configuración y abre un explorador de archivos para especificar el nombre y la ubicación para guardar la configuración.
4. Desplácese hasta la ubicación de guardado en su PC y haga clic en **Guardar**. Esto guarda el paquete de configuración en su PC.

> **Nota**
>
> Para recuperar un paquete de configuración de copia de seguridad, puede utilizar una operación de **importación** para importar el paquete desde su PC y cargarlo en el **Editor de configuración**. A continuación, puede guardar el paquete importado en el Workspace de la Interfaz Web de administración para utilizarlo en el futuro.

Importar paquete de configuración de copia de seguridad

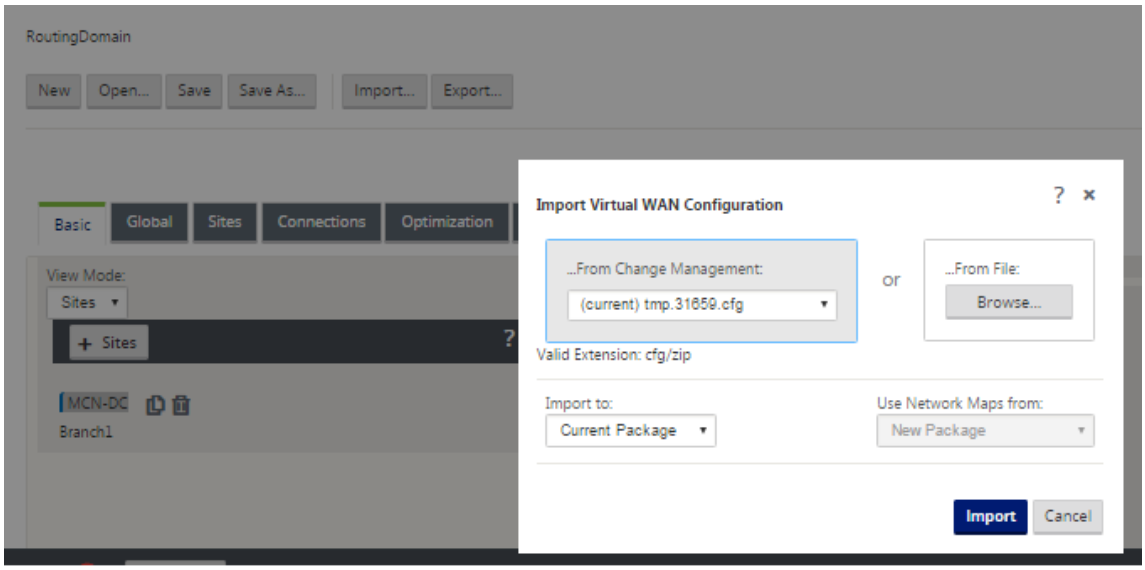
A veces, es posible que quiera volver a una versión anterior de un paquete de configuración. Si ha guardado una copia de la versión anterior en su PC local, puede volver a importarla en el Editor de configuración y, a continuación, abrirla para modificarla. Si no se trata de una implementación inicial, también puede importar un paquete de configuración existente desde la bandeja de entrada de Administración de cambios global en el MCN actual. A continuación se proporcionan instrucciones para ambos procedimientos.

Para importar un paquete de configuración, haga lo siguiente:

1. Abra el **Editor de configuración**.
2. En la barra de menús del **Editor de configuración**, haga clic en **Importar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

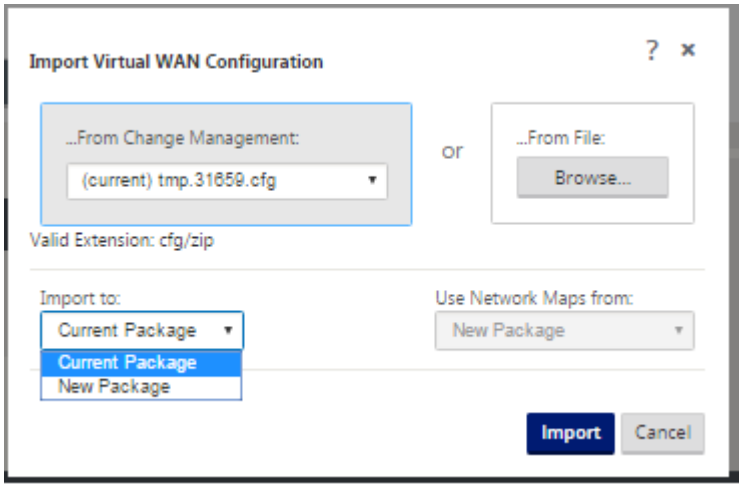
Aparece el cuadro de diálogo **Importar configuración WAN virtual**.



3. Seleccione la ubicación desde la que quiere importar el paquete.

   - Para importar un paquete de configuración desde Change Management: Seleccione el paquete en el menú implementable **From Change Management** (esquina superior izquierda).
   - Para importar un paquete de configuración desde su PC local: Haga clic en **Examinar** para abrir un explorador de archivos en su PC local. Seleccione el archivo y haga clic en **Aceptar**.

4. Seleccione el destino de importación (si procede). Si un paquete de configuración ya está abierto en el **Editor de configuración,** estará disponible el menú implementable **Importar a:**.



Seleccione una de estas opciones:

Paquete actual: Seleccione esta opción para reemplazar el contenido del paquete de configuración abierto por el contenido del paquete importado y conservar el nombre del paquete

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

abierto. Sin embargo, el contenido de la versión guardada del paquete actual no se sobrescribe hasta que guarde explícitamente el paquete modificado. Si utiliza **Guardar como** para guardar el paquete, seleccione **Permitir sobrescritura** para habilitar la sobrescritura de la versión anterior.

- **Nuevo paquete**: Seleccione esta opción para abrir un nuevo paquete de configuración en blanco y rellenarlo con el contenido del paquete importado. El nuevo paquete toma automáticamente el mismo nombre que el paquete importado.

5. Especifique los mapas de red que quiere incluir (si procede). Si un paquete de configuración ya está abierto en el **Editor de configuración**, estará disponible el menú implementable **Usar mapas de red desde:**.

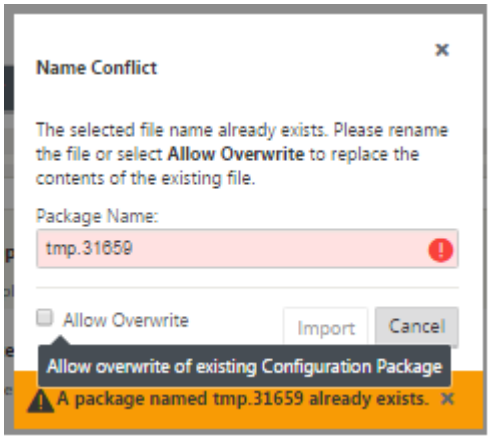
Seleccione una de estas opciones:

- Paquete actual: Conserva los mapas de red configurados actualmente en el paquete ahora disponibles en el Editor de configuración y descarta los mapas de red del paquete importado.
- Nuevo paquete: Reemplaza los mapas de red configurados actualmente en el paquete abierto con los mapas de red (si los hay) del paquete importado.
- Ambos **paquetes**: Incluye todos los mapas de red tanto del paquete actual como del importado.

6. Haga clic en **Importar**. El archivo importado se carga en el **Editor de configuración**, de acuerdo con sus especificaciones.

> **Nota**
>
> Si existe un paquete con el mismo nombre en el Workspace, aparecerá el cuadro de diálogo **Conflicto de nombres**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para especificar el nombre que se va a utilizar para el paquete importado, siga uno de estos procedimientos:

- Escriba un nombre diferente en el campo **Nombre del paquete** para cambiar el nombre del paquete nuevo y active el botón **Importar**. El paquete importado se carga en el **Editor de configuración** con el nombre especificado. El nombre del paquete se guarda ahora en el Workspace, pero el contenido del paquete se guarda en el Workspace hasta que se guarde explícitamente el paquete.
- Seleccione **Permitir sobrescritura** para confirmar que quiere conservar el nombre existente y habilitar la sobrescritura del contenido del paquete guardado. Sin embargo, el contenido de la versión guardada del paquete actual no se sobrescribe hasta que guarde explícitamente el paquete modificado.

Esto también activa el botón **Importar** del cuadro de diálogo **Conflicto de nombres**. Haga clic en **Importar** para completar la operación de importación.

Cargar paquete de configuración guardado

Para reanudar el trabajo en un paquete de configuración guardado, primero debe abrirlo y cargarlo en el **Editor de configuración.**

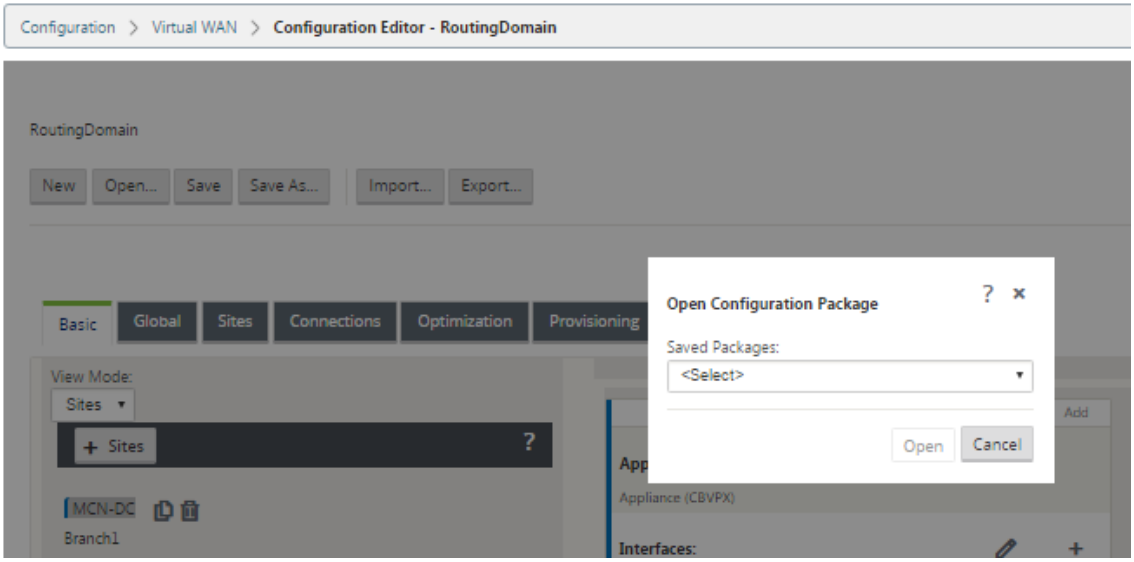
Para cargar un paquete de configuración guardado, haga lo siguiente:

1. Vuelva a iniciar sesión en la Interfaz Web de administración y desplácese hasta el **Editor de configuración**. Esto abre la página principal del **Editor de configuración** para una nueva sesión.

   Si ha vuelto a iniciar sesión en la Interfaz Web de administración, el **Editor de configuración** se abre inicialmente para una nueva sesión, sin ningún paquete de configuración cargado. Puede iniciar una nueva configuración (**Nueva**), abrir una configuración guardada existente (**Abrir**) o importar (**Importar)**y, a continuación, abrir **(Abrir**) una configuración previamente respaldada en su PC local.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Haga clic en **Abrir**. Aparece el cuadro de diálogo **Abrir paquete de configuración**.



3. Seleccione el paquete que quiere abrir en el menú implementable **Paquetes guardados**.

> **Nota**
>
> Si ha abierto el **Editor de configuración**, el menú **Paquetes guardados**puede tardar unos segundos o un minuto o dos en completarse, dependiendo del número de configuraciones que haya guardado en el Workspace. Si es así, mientras tanto, el campo de menú **Paquetes guardados** podría mostrar el mensaje **No hay paquetes guardados**. Si esto ocurre, haga clic en **Cancelar** para cerrar el cuadro de diálogo, espere unos momentos y vuelva a hacer clic en **Abrir** para volver a abrir el cuadro de diálogo.

4. Haga clic en **Abrir**.

> **Nota**
>
> Esto abre el paquete de configuración especificado y lo carga en el **Editor de configuración** solo para modificarlo. Esto no pone en escena ni activa la configuración seleccionada en el dispositivo local.

Cambiar nombre de sitios

Si cambia el nombre del sitio MCN en el editor de configuración, debe aplicar la configuración con el sitio renombrado a la red MCN y SD-WAN. Según el rol de MCN y si la alta disponibilidad está habilitada o inhabilitada, los siguientes casos son aplicables para la configuración de red SD-WAN al cambiar el nombre de sitios.

- MCN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- MCN con alta disponibilidad
- GEO
- GEO con alta disponibilidad
- RCN
- RCN con alta disponibilidad

Cambiar el nombre del sitio de MCN

Después de cambiar el nombre del MCN, debe cargar la nueva configuración con el sitio renombrado.

Para cargar nueva configuración para el sitio renombrado:

1. Desde el MCN, la red de caso con la nueva configuración.
2. Descargue el paquete de configuración provisional para el MCN renombrado.
3. Acceda a la página **Gestión de cambios Locales** del MCN.
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** una vez finalizado el procesamiento.
   c) Haga clic en **Activar**.

> **Nota**
>
> Una vez completado el paso 3 (c), el proceso de administración de cambios activa automáticamente el software por etapas para dispositivos (nodos) en la red.

Cambiar el nombre del sitio de MCN con alta disponibilidad

Después de cambiar el nombre del MCN para el que está habilitada la alta disponibilidad, debe cargar la nueva configuración.

1. Desde el MCN, red de caso con nueva configuración.
2. Descargue el paquete de configuración provisional para los dispositivos MCN activos y de alta disponibilidad con nuevo nombre.
3. Inhabilite el servicio en el dispositivo MCN en espera.
4. Acceda a la página **Gestión de cambios Locales** del MCN activo.
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** cuando finalice el procesamiento.
   c) Haga clic en **Activar**.
   d) Repita los pasos i, ii, iii, iv para el dispositivo MCN en espera inhabilitado de alta disponibilidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) Habilite el servicio en el dispositivo MCN en espera.

> **Nota**
>
> Una vez completado el paso 4 (c), el proceso de administración de cambios activa automáticamente el software por etapas para los dispositivos de la red.

Cambio de nombre del sitio GEO

Para cargar nueva configuración para un sitio GEO renombrado:

1. Desde el MCN, red de casos con nueva configuración que contiene el sitio GEO renombrado.
2. Desde el MCN, descargue el paquete de configuración provisional para el sitio GEO renombrado.
3. En el **MCN**, seleccione **Activar en etapas** para la red. Esto desactiva el sitio renombrado y el sitio deja de estar disponible.
4. Acceda a la página **Gestión de cambios Locales** en el sitio GEO.
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** cuando finalice el procesamiento del paquete.
   c) Haga clic en **Activar**.

Cambiar el nombre del sitio GEO con alta disponibilidad

Para cargar nueva configuración con un sitio GEO renombrado habilitado con alta disponibilidad:

1. Desde el MCN, red de caso con nueva configuración que contiene el renombrado sitio GEO.
2. Desde el MCN, descargue el paquete de configuración provisional para los dispositivos activos y de alta disponibilidad con el sitio GEO renombrado.
3. En el **MCN**, seleccione **Activar en etapas**para la red. Esto inhabilita el sitio renombrado y el sitio deja de estar disponible.
4. Desplácese hasta el dispositivo GEO activo.
   a) Vaya a la página Administración de cambios locales.
   b) Cargue el paquete descargado anteriormente.
   c) Haga clic en **Siguiente** cuando finalice el procesamiento del paquete.
   d) Haga clic en **Activar**.
   e) Repita los pasos a, b, c y d para el dispositivo en espera.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cambiar el nombre del sitio de RCN

Para cargar nueva configuración con el sitio RCN renombrado:

1. Desde el MCN, red de caso con nueva configuración que contiene el sitio RCN renombrado.
2. Desde el MCN, descargue el paquete provisional para el sitio RCN renombrado.
3. En el **MCN**, seleccione **Activar en etapas** para la red. Esto inhabilita el sitio RCN renombrado y el sitio de la región deja de estar disponible en el MCN. El sitio de RCN y las sucursales de la región se comunican entre sí, sin embargo, hasta que se complete el paso 4, la región no podrá comunicarse con el MCN (a menos que haya un RCN de GEO que no se cambie el nombre).
4. Acceda a la página Gestión de cambios Locales de RCN:
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** cuando finalice el procesamiento del paquete.
   c) Haga clic en **Activar**.

> **Nota**
>
> Las sucursales de la región tardan algún tiempo en llegar a estar disponibles, ya que la etapa de la región no se produce hasta que se haya completado el paso 4 (c). El proceso de administración de cambios del RCN administra la puesta en escena de la región.

Cambiar el nombre del sitio de RCN con alta disponibilidad

Para cargar nueva configuración con el sitio RCN renombrado habilitado con alta disponibilidad.

1. Desde el MCN, red de caso con nueva configuración que contiene el sitio RCN renombrado.
2. Desde el MCN, descargue el paquete provisional para los dispositivos activos y de alta disponibilidad con el sitio RCN renombrado. Esto inhabilita el sitio RCN renombrado y el sitio de la región deja de estar disponible en el MCN. El sitio de RCN y las sucursales de la región se comunican entre sí, sin embargo, hasta que se complete el paso 4, la región no podrá comunicarse con el MCN (a menos que haya un RCN de GEO que no se cambie el nombre).
3. En el **MCN**, seleccione **Activar en etapas para la red**.
4. Inhabilite el servicio en el dispositivo RCN en espera.
5. Acceda a la página **Gestión de cambios Locales** de RCN activa:
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** cuando finalice el procesamiento del paquete.
   c) Haga clic en **Activar**.
   d) Repita los pasos a, b y c para el dispositivo RCN en espera inhabilitado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Habilite el servicio en el dispositivo RCN en espera.

Cambio de nombre del sitio GEO RCN

Para cargar nueva configuración con el sitio GEO RCN renombrado:

1. Desde el MCN, red escénica con nueva configuración con sitio GEO RCN renombrado.
2. Desde el MCN, descargue el paquete provisional para el sitio GEO RCN renombrado.
3. En el **MCN**, seleccione **Activar en etapas** para la red. Esto inhabilita el sitio renombrado y el sitio deja de estar disponible. Si el RCN principal está en línea, la región permanece conectada a la red al cambiar el nombre del sitio GEO RCN.
4. Acceda a la página **Gestión de cambios Locales** de GEO RCN:
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** cuando finalice el procesamiento del paquete.
   c) Haga clic en **Activar**.

Cambiar el nombre del sitio GEO RCN con alta disponibilidad

1. Desde el MCN, red escénica con nueva configuración con sitio GEO RCN renombrado.
2. Desde el MCN, descargue el paquete provisional para el dispositivo activo y de alta disponibilidad para el sitio GEO RCN renombrado.
3. En el **MCN**, seleccione **Activar en etapas** para la red. Esto inhabilita el sitio renombrado y el sitio deja de estar disponible. Si el RCN principal está en línea, la región permanece conectada a la red al cambiar el nombre del sitio GEO RCN.
4. Acceda a la página **Gestión de cambios Locales** de GEO RCN activa:
   a) Cargue el paquete descargado anteriormente.
   b) Haga clic en **Siguiente** cuando finalice el procesamiento del paquete.
   c) Haga clic en **Activar**.
   d) Repita los pasos a, banda c para el dispositivo en espera.

Configuración de nodos de sucursal

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Este capítulo proporciona instrucciones para agregar y configurar los sitios de sucursales. El procedimiento para agregar un sitio de sucursal es muy similar a crear y configurar el sitio de MCN. Sin embargo, algunos de los pasos y opciones de configuración varían ligeramente para un sitio de sucursal. Además, una vez que haya agregado un sitio de sucursal inicial, para los sitios que tengan el mismo modelo de dispositivo, puede utilizar la función **Clone** (duplicado) para optimizar el proceso de agregar y configurar esos sitios.

Al igual que con la creación del sitio de MCN para configurar un sitio de sucursal, debe utilizar el **Editor de configuración** de la Interfaz Web de administración del dispositivo MCN. El **Editor de configuración** está disponible cuando la interfaz está configurada en el modo **Consola de MCN**.

Información complementaria sobre la implementación del sitio de sucursal

Además de esta guía, también se recomiendan los siguientes artículos de soporte de Knowledge Base:

- Pasos de implementación del modo PBR de WAN virtual (CTX201577)

  http://support.citrix.com/article/CTX201577
- Pasos de implementación del modo de puerta de enlace WAN virtual (CTX201576)

  http://support.citrix.com/article/CTX201576

Introducción a los procedimientos de configuración del sitio de sucursal

Los pasos para completar este proceso son los siguientes:

1. Agregue el sitio de sucursal.
2. Configure los grupos de interfaz virtual para el sitio de sucursal.
3. Configure las direcciones IP virtuales para el sitio de la sucursal.
4. (Opcional) Configure los túneles LAN GRE para el sitio de sucursal.
5. Configure los enlaces WAN para el sitio de la sucursal.
6. Configure las rutas para el sitio de la sucursal.
7. (Opcional) Configure High Availability para el sitio de sucursal.
8. (Opcional) Clonar el nuevo sitio de sucursal para crear y configurar sitios adicionales.

   > **Nota**
   >
   > Clonar el sitio es opcional. Los modelos del dispositivo WAN virtual deben ser los mismos para los sitios originales y clonados. No se puede cambiar el modelo de dispositivo especi-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ficado para un clon. Si el modelo de dispositivo es diferente para un sitio, debe agregarlo manualmente.

9. Resuelva las alertas de auditoría de configuración.
10. Guarde la configuración completada.

Configurar nodo de sucursal

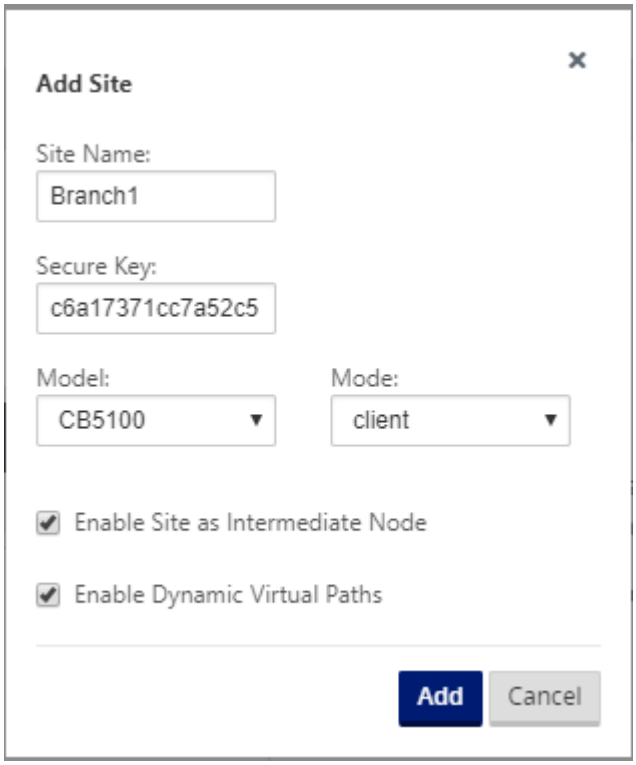
May 7, 2021

Para agregar un nuevo sitio de sucursal a la tabla **Sitios** y comenzar a configurar el sitio, haga lo siguiente:

> **Nota**
>
> Si ha cerrado la sesión del MCN después de crear y guardar el nuevo paquete de configuración, deberá volver a iniciar sesión y volver a abrir la configuración antes de poder continuar. Para ello, haga clic en **Abrir** en la barra de menús del **Editor de configuración** (parte superior del área de página). Esto muestra un cuadro de diálogo para seleccionar la configuración que quiere cambiar.

1. Continuando con el **Editor de configuración**, haga clic en **Agregar**en la barra **Sitios**para comenzar a agregar y configurar el nuevo sitio de sucursal. Aparecerá el cuadro de diálogo **Agregar sitio**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



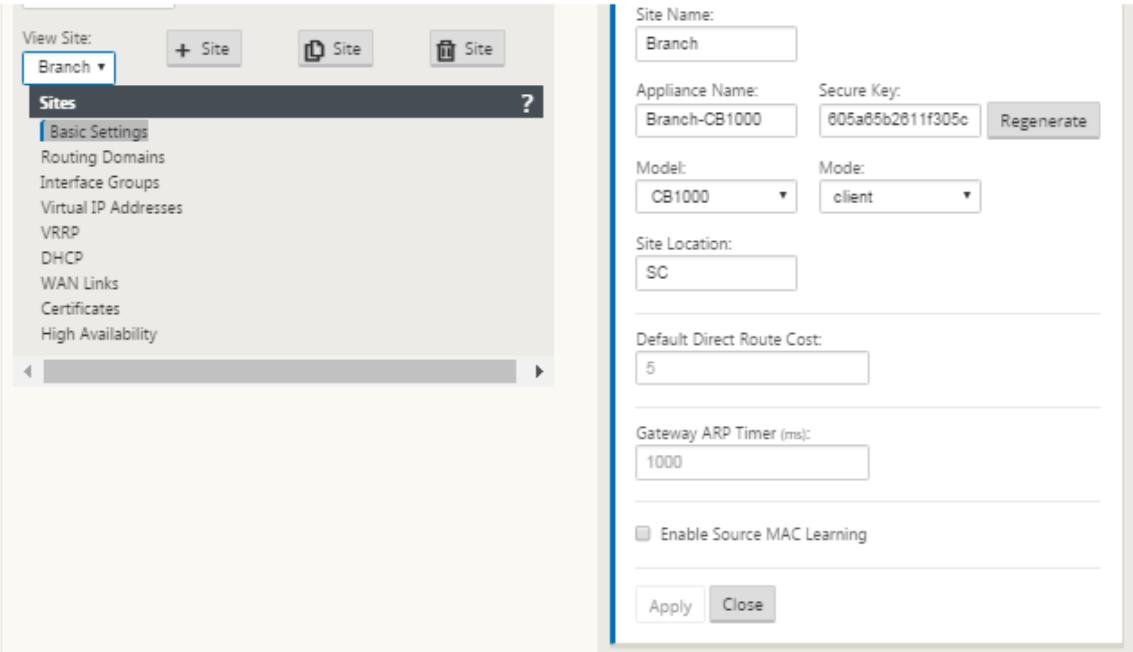
2. Escriba la siguiente información del sitio.

> **Nota**
>
> Las entradas no pueden contener espacios y deben estar en formato Linux.

   - **Nombre del sitio**: Escriba un nombre para el sitio.
   - **Nombre del dispositivo**: Escriba el nombre que quiere asignar al dispositivo.
   - **Clave segura**: Se trata de una clave hexadecimal de 8 a 32 dígitos que se utiliza para el cifrado y la verificación de pertenencia en el dispositivo SD-WAN. De forma predeterminada, este campo se rellena previamente con una clave de seguridad generada automáticamente. Acepte el valor predeterminado o escriba un formato hexadecimal de clave personalizada.
   - **Modelo**: Seleccione el modelo de dispositivo en el menú implementable.
   - **Modo**: Seleccione el cliente como modo.

3. Haga clic en **Agregar** para agregar el sitio. El nuevo sitio se agrega al árbol de **sitios** y abre el formulario de **configuración de configuración básica** del sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



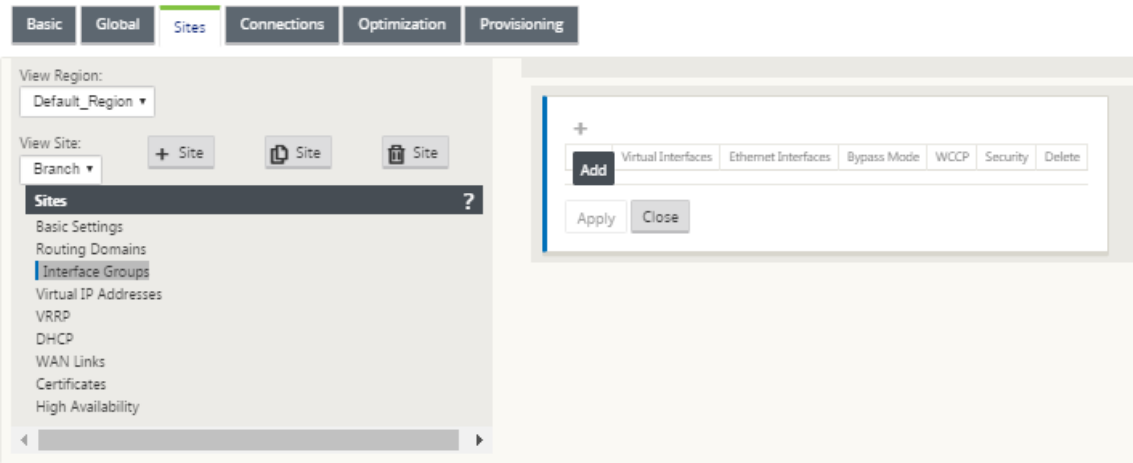
4. Escriba la configuración básica del sitio y haga clic en **Aplicar**.

   El siguiente paso es agregar y configurar los grupos de interfaz para el nuevo sitio de sucursal.

Cómo configurar grupos de interfaz para la sucursal

Para agregar Grupo de interfaz al nuevo sitio de sucursal, haga lo siguiente:

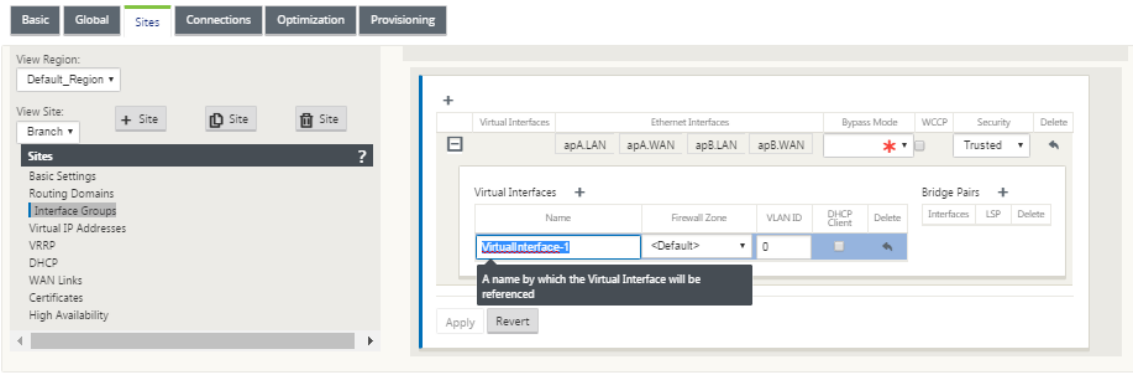
1. Continuando en la vista **Sitios** del **Editor de configuración**, seleccione el sitio de sucursal en el menú implementable **Ver sitio**. Esto abre la vista de configuración para el sitio seleccionado.



2. Haga clic en **+** para agregar el **grupo de interfaz virtual**. Se agrega una nueva entrada de grupo de interfaz virtual en blanco a la tabla y se abre para modificarla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Haga clic en **+** a la derecha de **Interfaces virtuales**. Se agrega una nueva entrada de grupo en blanco a la tabla y se abre para modificarla.



4. Seleccione las **interfaces Ethernet** que quiere incluir en el grupo.

   En **Interfaces Ethernet**, haga clic en una interfaz para incluir/excluir esa interfaz. Puede seleccionar cualquier número de interfaces que quiera incluir en el grupo.

5. Seleccione el **Modo de omisión** en el menú implementable (sin valor predeterminado).

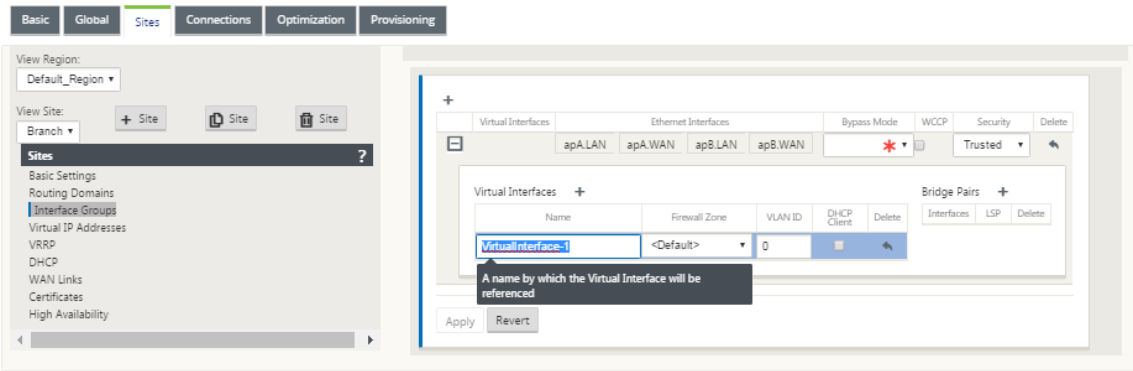
   El **modo de omisión** especifica el comportamiento de las interfaces emparejadas en puente en el grupo de interfaz virtual, en caso de que un dispositivo o servicio falle o se reinicie. Las opciones son: **Fail-to-Wire** o **Fail-to-Block**.

6. Seleccione el **Nivel de seguridad** en el menú implementable.

   Especifica el nivel de seguridad para el segmento de red del grupo de interfaz virtual. Las opciones son: De **confianza** o de **no confianza**. Los segmentos de confianza están protegidos por un firewall (el valor predeterminado es Trusted).

7. Haga clic en **+** en el borde izquierdo de la interfaz virtual que ha agregado. Muestra la tabla **Interfaces Virtuales**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Haga clic en **+** a la derecha de **Interfaces virtuales**. Aparecen los identificadores de **nombre, zona de cortafuegos** e **ID de VLAN**.
9. Escriba el **nombre** y el **ID de VLAN** para este grupo de interfaz virtual.
   - **Nombre**: Nombre por el que se hace referencia a estas interfaces virtuales.
   - **Zona de firewall**: Seleccione una zona de firewall en el menú implementable.
   - **ID de VLAN**: ID para identificar y marcar el tráfico hacia y desde la interfaz virtual. Use un ID de 0 (cero) para el tráfico nativo/no etiquetado.
10. Haga clic en **+** a la derecha de los **pares de puentes**. Se agrega una nueva entrada de **Bridge Pairs** y se abre para modificarla.
11. Seleccione las interfaces Ethernet que se van a emparejar en los menús desplegables. Para agregar más pares, haga clic en **+** junto a **Pairs de puente** de nuevo.
12. Haga clic en **Aplicar**. La configuración se aplica y agrega al nuevo grupo de interfaz virtual de la tabla.

    > **Nota**
    >
    > En esta etapa, verá un icono amarillo de alerta de auditoría delta, a la derecha de la nueva entrada del grupo de interfaz virtual. Esto se debe a que aún no ha configurado ninguna dirección IP virtual (VIP) para el sitio. Por ahora, puede ignorar esta alerta, ya que se resuelve automáticamente cuando haya configurado correctamente las IP virtuales para el sitio.

13. Para agregar más grupos de interfaz virtual, haga clic en **+** a la derecha de la sucursal **Grupos de interfaz** y proceda como se indica anteriormente.

Cómo configurar la dirección IP virtual para el sitio de sucursal

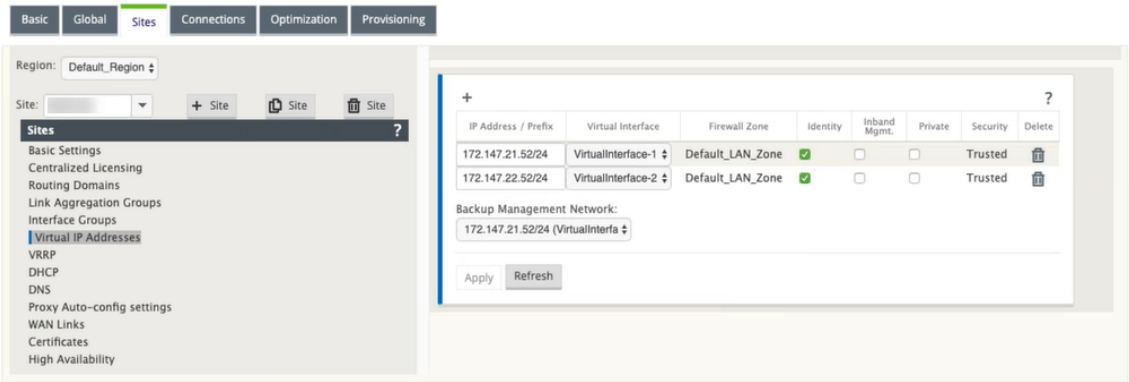
El siguiente paso es configurar las direcciones IP virtuales para el sitio y asignarlas al grupo apropiado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Continuando en la vista **Sitios** para el nuevo sitio de sucursal, haga clic en **+** a la izquierda de **Direcciones IP virtuales**. Muestra la tabla **Direcciones IP virtuales** para el nuevo sitio.
2. Haga clic en **+** a la derecha de **Direcciones IP virtuales** para agregar una dirección. Aparecerá el formulario para agregar y configurar una nueva dirección IP virtual.
3. Escriba la información **de dirección IP** / **prefijo** y seleccione la **interfaz virtual** con la que está asociada la dirección. La dirección IP virtual debe incluir la dirección de host completa y la máscara de red.
4. Seleccione la configuración quiereda para la dirección IP virtual, como Zona de firewall, Identidad, Privado y Seguridad.
5. Seleccione **Administración en banda para permitir** que la dirección IP virtual se conecte a servicios de administración como la interfaz de usuario web y SSH.

   > **Nota:**
   >
   > La interfaz debe ser del tipo de seguridad **Confiable** e **Identidad** habilitada.

6. Seleccione una IP virtual como una **red de administración de copias de seguridad**. Esto le permite utilizar la dirección IP virtual para la administración si el puerto de administración no está configurado con una Gateway predeterminada.



7. Haga clic en **Aplicar**. La información de dirección al sitio se agrega e incluye en la tabla **Direcciones IP virtuales** del sitio.
8. Para agregar más direcciones IP virtuales, haga clic en **+** a la derecha de las **Direcciones IP virtuales**y continúe como se indica anteriormente.

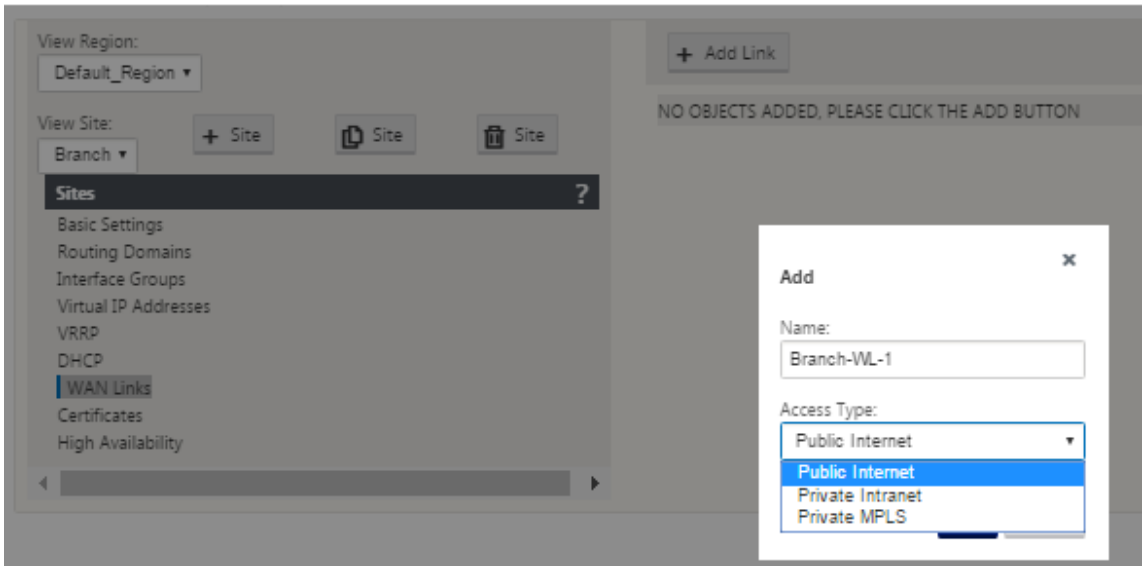
Cómo configurar enlaces WAN para la sucursal

El siguiente paso es configurar los enlaces WAN para el sitio.

1. Continuando en la vista **Sitios** del nuevo sitio de sucursal, haga clic en la etiqueta **Enlaces WAN**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Haga clic en **Agregar vínculo** a la derecha de los **enlaces WAN** para agregar un nuevo enlace WAN. Aparecerá el cuadro de diálogo **Agregar**.



3. (Opcional) escriba un nombre para el enlace WAN si no quiere utilizar el valor predeterminado.

   El valor predeterminado es el nombre del sitio, anexado con el siguiente sufijo:

   <number>- WL-

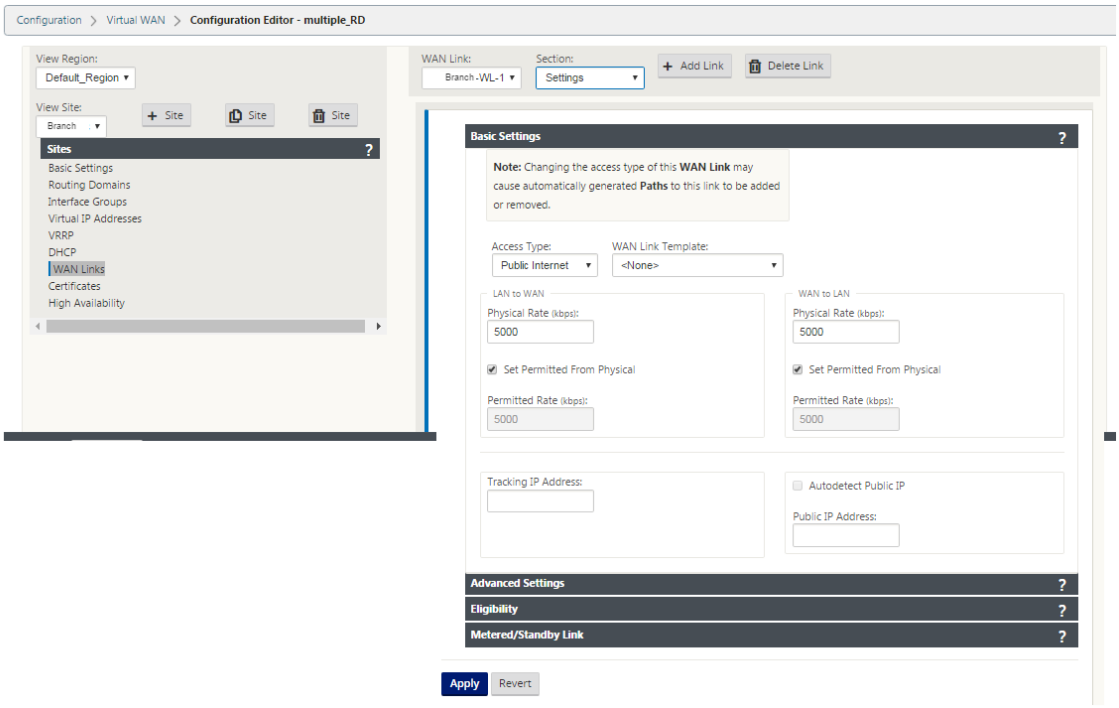
   Dónde <number> es el número de enlaces WAN para este sitio, incrementados en uno.

4. Seleccione **Tipo de acceso** en el menú implementable.

   Las opciones son **Internet público, Intranet privada**o **Cambio de etiquetas multiprotocolo privado.**

5. Haga clic en **Agregar**. Aparece la página de configuración básica de **enlaces WAN** y agrega el nuevo enlace WAN no configurado a la página.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

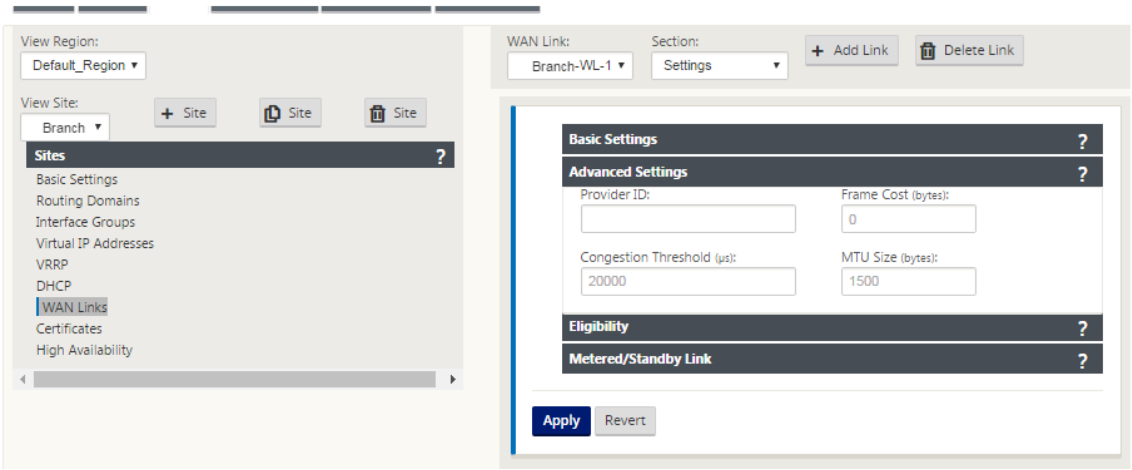


6. Escriba los detalles del vínculo para el nuevo enlace WAN. Configure la configuración de LAN a WAN, WAN a **LAN**.

   Algunas directrices son las siguientes:

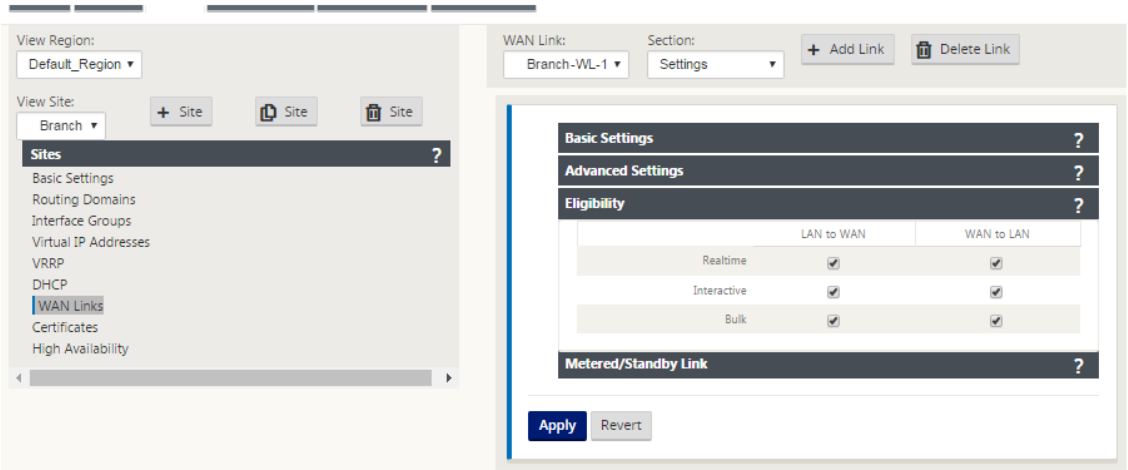
   - Algunos enlaces a Internet pueden ser asimétricos. La configuración incorrecta de la velocidad permitida puede afectar negativamente al rendimiento de ese enlace.
   - Evite utilizar velocidades de ráfaga que superen la velocidad comprometida.
   - Para los enlaces WAN de Internet, asegúrese de agregar la Dirección IP pública.

7. Haga clic en la barra de sección **Configuración avanzada** gris. Esto abre el formulario **Configuración avanzada** del vínculo.



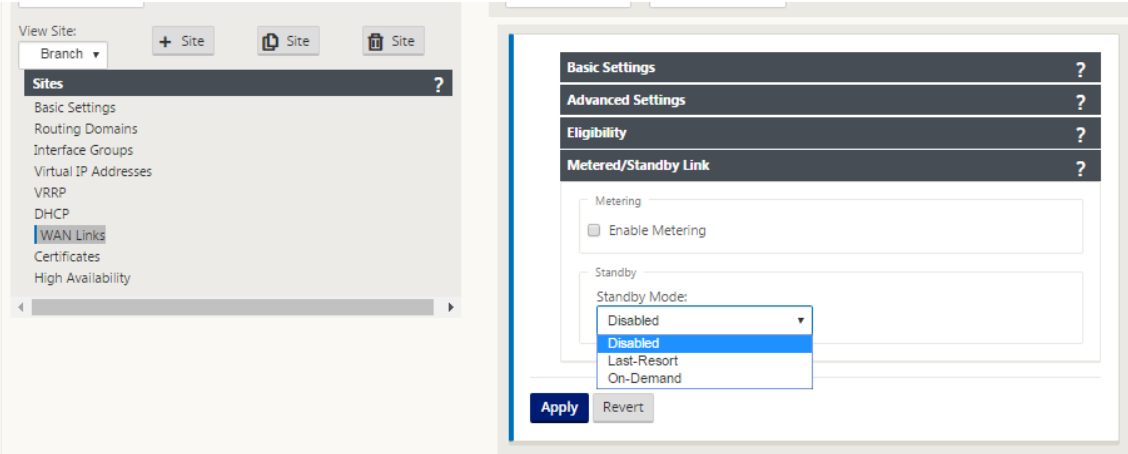
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

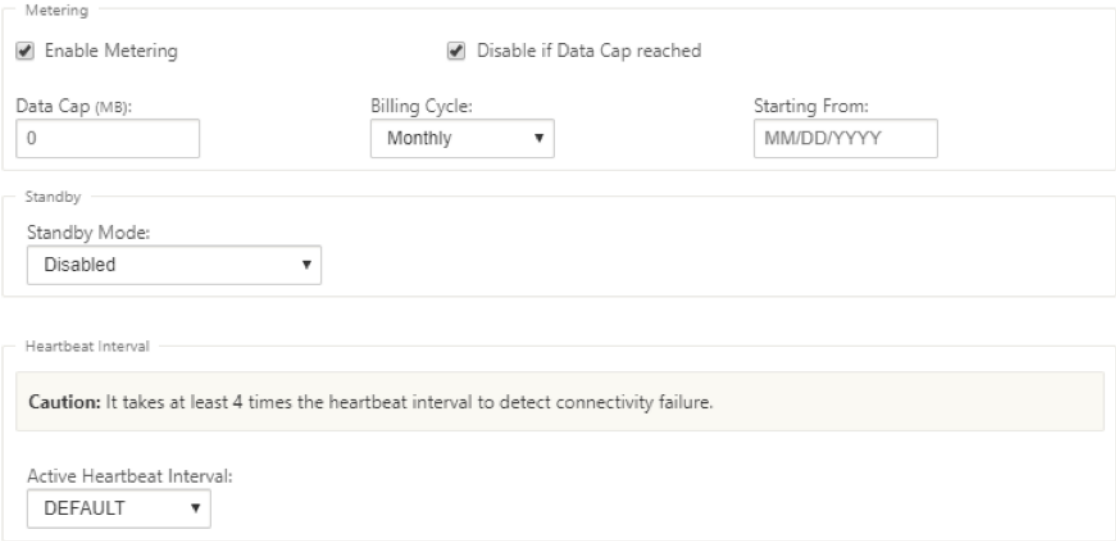
8. Escriba la **Configuración avanzada** del vínculo.
   - **ID de proveedor**: Escriba un número de ID único 1 a 100 para designar enlaces WAN conectados al mismo proveedor de servicios. La WAN virtual utiliza el Id. de proveedor para diferenciar rutas al enviar paquetes duplicados.
   - **Coste de trama (bytes)**: Escriba el tamaño (en bytes) del encabezado/remolque agregado a cada paquete. Por ejemplo, el tamaño en bytes de los remolques Ethernet IPG o AAL5 agregados.
   - **Umbral** de congestión: Escriba el umbral de congestión (en microsegundos) después del cual el enlace WAN limita la transmisión de paquetes para evitar una mayor congestión.
   - **Tamaño de MTU (bytes)**: Escriba el tamaño de paquete sin procesar más grande (en bytes), sin incluir el coste de trama.
9. Haga clic en la barra de sección de **elegibilidad** gris. Esto abre el formulario Configuración de **elegibilidad** para el vínculo.
10. Seleccione la configuración de **elegibilidad** para el enlace.



11. Haga clic en la barra de sección **Vínculo medido** gris. Esto abre el formulario de configuración de **Vínculo medido** para el vínculo.
12. (Opcional) Seleccione **Activar medición** para habilitar la medición para este vínculo. Muestra los campos **Habilitar configuración de medición**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





13. Configure los parámetros de medición para el enlace. Escriba lo siguiente:

    - **Límite de datos (MB)**: Escriba la asignación de límite de datos para el vínculo, en MB.
    - **Ciclo de facturación**: Seleccione **Mensual o Semanal** en el menú implementable.
    - **Desde Inicio**: Escriba la fecha de inicio del ciclo de facturación.
    - **Establecer último recurso**: Seleccione esta opción para habilitar este enlace como enlace de último recurso en caso de fallo de todos los demás enlaces disponibles. En condiciones WAN normales, la WAN virtual envía solo un tráfico mínimo a través de enlaces medidos, para comprobar el estado del vínculo. Sin embargo, en caso de fallo, SD-WAN puede utilizar vínculos medidos activos como último recurso para reenviar el tráfico de producción.

14. Haga clic en **Aplicar**. Esto aplica la configuración especificada al nuevo enlace WAN.

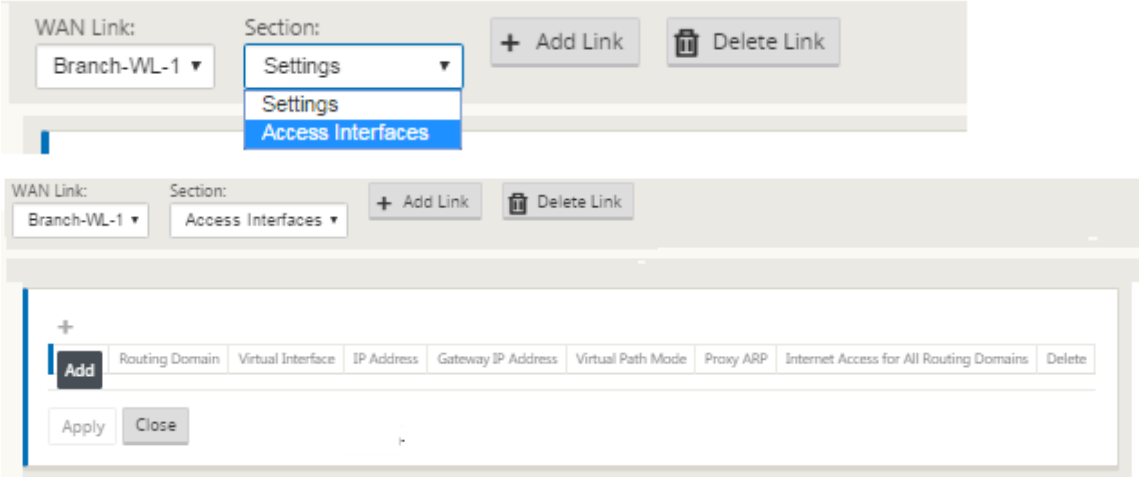
    El siguiente paso es configurar las interfaces de acceso para el nuevo enlace WAN. Una interfaz de acceso consta de una interfaz virtual, una dirección IP de punto final WAN, una dirección IP de puerta de enlace y un modo de ruta virtual definido colectivamente como una interfaz para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

un enlace WAN específico. Cada enlace WAN debe tener al menos una interfaz de acceso.

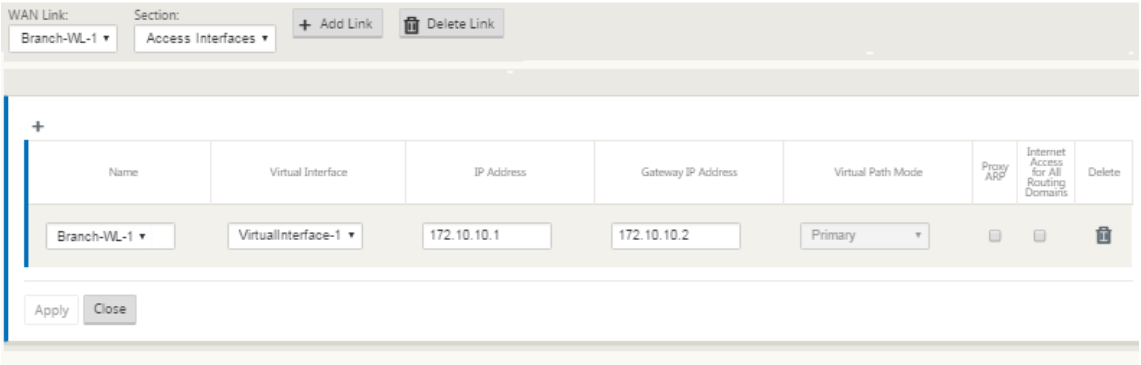
> **Nota**
>
> Se agrega una opción para aprovisionar recursos compartidos automáticamente teniendo en cuenta el ancho de banda remoto para configurar enlaces WAN. La opción Establecer Provisioning mediante ancho de banda remoto permite a los usuarios con redes grandes y diversas configuraciones de ancho de banda administrar el aprovisionamiento de ancho de banda para sitios de centro de datos de forma dinámica.

15. Seleccione **Interfaces de Acceso** en la página de configuración de Enlace WAN para el vínculo. Esto abre la vista **Interfaces de acceso** para el sitio.



16. Haga clic en **+** para agregar una interfaz. Se agrega una entrada en blanco a la tabla y se abre para modificarla. Escriba la configuración de **las interfaces de acceso** para el vínculo.

> **Nota**
>
> Cada enlace WAN debe tener al menos una interfaz de acceso.



17. Escriba lo siguiente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nombre: Nombre**por el que se hace referencia a esta Interfaz de Acceso. Escriba un nombre para la nueva interfaz de acceso o acepte el valor predeterminado. El valor predeterminado utiliza la siguiente convención de nomenclatura:

  WAN_LINK_Nombre-AI-Number

  Donde *WAN_LINK_NAME* es el nombre del enlace WAN que está asociando a esta interfaz, y el número es el número de interfaces de acceso configuradas actualmente para este vínculo, incrementado en 1.

> **Nota**
>
> Si el nombre aparece truncado, puede colocar el cursor en el campo y, a continuación, mantener pulsado el ratón y mover el ratón hacia la derecha o hacia la izquierda para ver la parte truncada.

- **Interfaz virtual**: La interfaz virtual que utiliza esta interfaz de acceso. Seleccione una entrada del menú desplegable de Interfaces virtuales configuradas para este sitio de sucursal.
- **Dirección IP: Dirección** IP del extremo de la interfaz de acceso desde el dispositivo a la WAN.
- **Dirección IP de la Gateway**: Esta es la dirección IP del enrutador de la puerta de enlace.
- **Modo de ruta virtual**: Prioridad para el tráfico de ruta virtual en este enlace WAN. Las opciones son: **Principal**, **Secundario**o **Excluir**. Si se establece en **Excluir**, esta interfaz de acceso se utiliza solo para el tráfico de Internet e Intranet.
- **Proxy ARP**: Seleccione la casilla de verificación que desea activar. Si está habilitada, Virtual WAN Appliance responde a las solicitudes ARP para la dirección IP de la Gateway, cuando la puerta de enlace es inalcanzable.

18. Haga clic en **Aplicar**.

    Ya ha terminado de configurar el nuevo enlace WAN. Repita estos pasos para agregar y configurar enlaces WAN adicionales para el sitio.

    El siguiente paso es agregar y configurar las rutas para el sitio.

Cómo configurar rutas para la sucursal

Para agregar y configurar las rutas para el sitio, haga lo siguiente:

1. Haga clic en la vista **Conexiones** para el nuevo sitio de sucursal y seleccione **Rutas**. Muestra la vista **Rutas** del emplazamiento.
2. Haga clic en **+** a la derecha de **Rutas** para agregar una ruta. Esto abre el cuadro de diálogo **Rutas** para su edición.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Escriba la información de configuración de ruta para la nueva ruta.

   - **Dirección IP de red**: Escriba la Dirección IP de red.
   - **Coste**: Escriba un peso de 1 a 15 para determinar la prioridad de ruta para esta ruta. Las rutas de menor coste tienen prioridad sobre las rutas de mayor coste. El valor predeterminado es 5.
   - **Tipo de servicio**: Seleccione el tipo de servicio para la ruta en el menú implementable de este campo. Opciones disponibles:
   - **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. Esto se hace midiendo y adaptándose constantemente a la demanda cambiante de las aplicaciones y a las condiciones WAN. Los dispositivos SD-WAN miden la red por trayecto. 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 sitios de Internet público. El tráfico de este tipo no está encapsulado. Durante los tiempos de 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 Intranet de acuerdo con la configuración de SD-WAN establecida por el Administrador.
   - **Intranet**: Este servicio administra el tráfico de Intranet de empresa que no se ha definido para su transmisión a través de una ruta de acceso virtual. Al igual que con el tráfico de Internet, permanece sin encapsular y la SD-WAN administra el ancho de banda limitando la velocidad de este tráfico en relación con otros tipos de servicios durante los tiempos de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

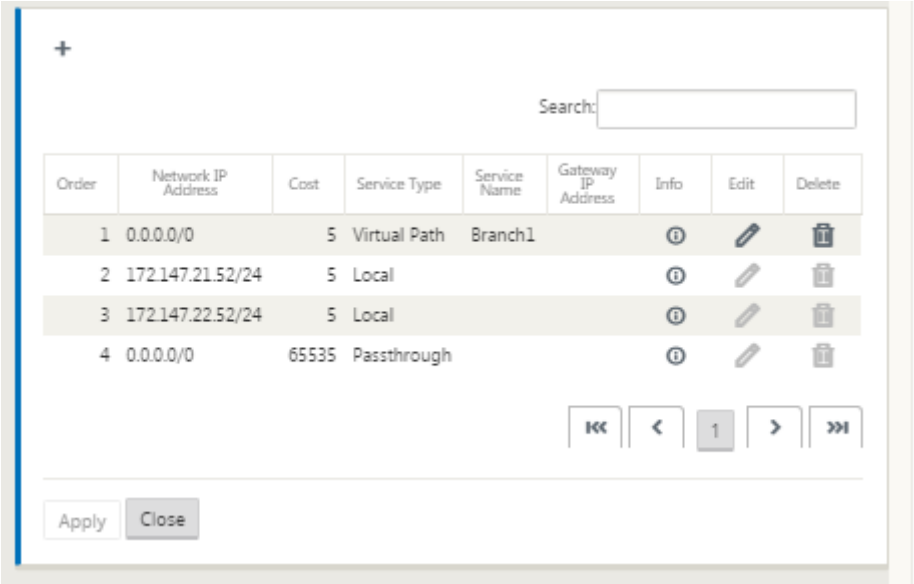
congestión. En determinadas condiciones, y si se configura para la repliegue de intranet en la ruta de acceso virtual, el tráfico que normalmente viaja con una ruta de acceso virtual se puede tratar como tráfico de intranet, para mantener la fiabilidad de la red.

- **PassThrough**: Este servicio administra el tráfico que se va a pasar a través de la WAN virtual. El tráfico dirigido al Servicio de paso incluye difusiones, ARP y otro tráfico no IPv4, así como el tráfico en la subred local del dispositivo WAN virtual, subredes configuradas o Reglas aplicadas por el Administrador de red. El SD-WAN no retrasa, da forma ni cambia este tráfico. Por lo tanto, debe asegurarse de que el tráfico PassThrough no consume recursos sustanciales en los enlaces WAN que el dispositivo SD-WAN está configurado para utilizar para otros servicios.
- **Local**: Este servicio administra el tráfico IP local en el 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 GRE LAN configurado en el sitio. La función Túnel GRE le permite configurar los dispositivos SD-WAN para finalizar los túneles GRE en la LAN. Para una ruta con el tipo de servicio GRE Tunnel, la Gateway debe residir en una de las subredes de túnel del túnel GRE local.
- **Túnel IPSec LAN**: Este servicio administra el tráfico IP destinado al túnel IPSec.
- **Direcciones IP de puerta de**enlace: Escriba la dirección IP de puerta de enlace para esta ruta.
- **Elegibilidad basada en la ruta** (casilla de verificación): (Opcional) Si está activada, la ruta no recibe tráfico cuando la ruta seleccionada está desactivada.
- **Ruta**: Especifica la ruta que se utilizará para determinar la elegibilidad de la ruta.

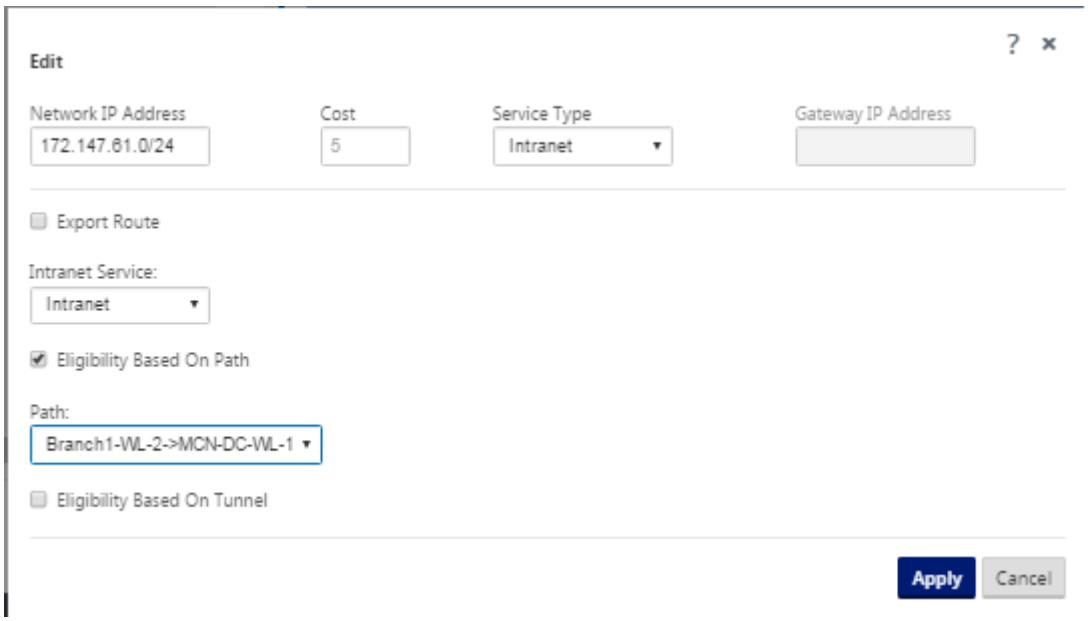
4. Haga clic en **Aplicar**.

> **Nota**
>
> Después de hacer clic en **Aplicar**, es posible que aparezcan advertencias de auditoría que indiquen que es necesario realizar más acciones. Un punto rojo o un icono delta de vara dorada indica un error en la sección donde aparece. Puede utilizar estas advertencias para identificar errores o falta información de configuración. Pase el cursor sobre un icono de advertencia de auditoría para mostrar una breve descripción de los errores en esa sección. También puede hacer clic en la barra de estado **Auditorías** de color gris oscuro (parte inferior de la página) para mostrar una lista completa de todas las advertencias de auditoría.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



También puede modificar rutas configuradas como se muestra a continuación.



Ahora ha completado los pasos necesarios para configurar un sitio cliente. También hay algunos pasos opcionales adicionales que puede completar antes de continuar con la siguiente fase de la implementación. A continuación se proporciona una lista de estos pasos y enlaces a las instrucciones. Si no quiere configurar estas funciones ahora, puede proceder directamente aPreparación de los paquetes de dispositivos SD-WAN en el MCN.

Los pasos opcionales son los siguientes:

- **Configurar alta disponibilidad**: Alta disponibilidad es una configuración en la que dos dispositivos WAN virtuales en un sitio funcionan en una capacidad de asociación activo/en espera con

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

fines de redundancia. Si no está implementando Alta disponibilidad para este sitio, puede omitir este paso. Para obtener instrucciones, consulte Configuración de alta disponibilidad (alta disponibilidad) para el sitio de sucursal (opcional).

- **Clonar el nuevo sitio de sucursal**: Tiene la opción de clonar el sitio de sucursal que configuró y usarlo como plantilla para agregar otro sitio. Los modelos del dispositivo para el sitio original y el clon deben ser los mismos. Para obtener instrucciones, consulte Clonación del sitio de sucursal (opcional).
- **Configurar optimización de WAN: Si** la licencia de WAN virtual de Citrix SD-WAN incluye funciones de optimización de WAN, tiene la opción de habilitar y agregar estas funciones a su configuración. Para ello, debe completar la sección **Optimización** en el **Editor de configuración** y guardar la configuración modificada.

Guardar configuración

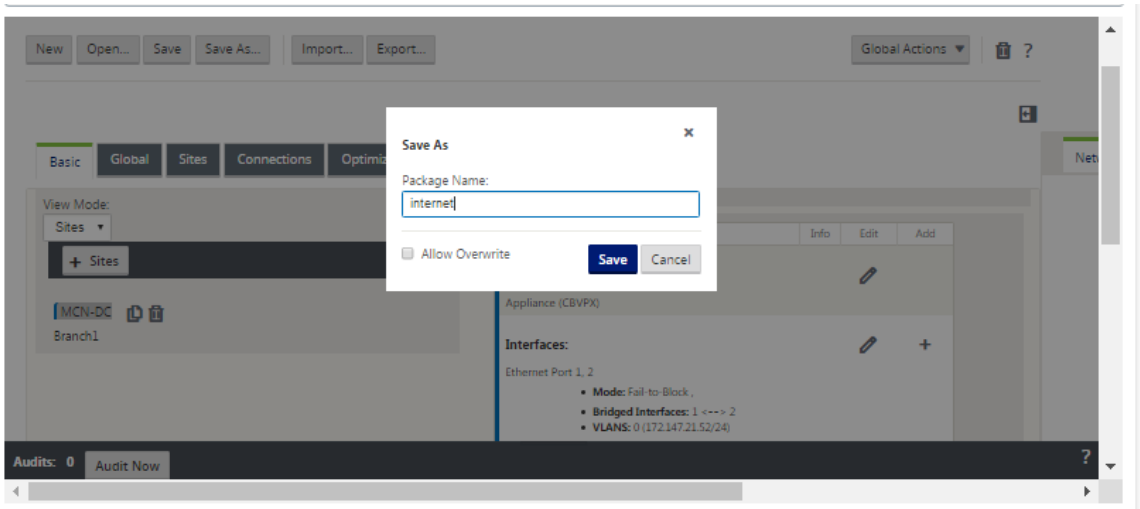
El siguiente paso es guardar la configuración de Sitios completada. La configuración se guarda en el Workspace en el dispositivo local.

> **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. A continuación, debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por esta razón, se recomienda guardar el paquete de configuración con frecuencia, o en puntos clave de la configuración.
>
> **Nota**
>
> Como precaución adicional, se recomienda utilizar **Guardar como, en lugar de**Guardar**, para evitar sobrescribir el paquete de configuración incorrecto.
>
> Después de guardar el archivo de configuración, tiene la opción de cerrar la sesión de Management Web Interface y continuar el proceso de configuración más adelante. Sin embargo, si cierra la sesión, deberá volver a abrir la configuración guardada cuando reanude. Las instrucciones se proporcionan en la sección **Configuración de MCN**;Cargar un paquete de configuración guardado en el Editor de configuración.

Para guardar el paquete de configuración actual, haga lo siguiente:

1. Haga clic en **Guardar como** (en la parte superior del panel central del **Editor de configuración**). Se abre el cuadro de diálogo **Guardar como**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Escriba el nombre del paquete de configuración. Haga clic en **Guardar.**

> **Nota**
>
> Si está guardando la configuración en un paquete de configuración existente, asegúrese de seleccionar **Permitir sobrescritura** antes de guardarla.

El siguiente paso es configurar las rutas virtuales y el servicio de rutas virtuales entre el MCN y los sitios cliente. Las instrucciones se proporcionan en elConfiguración del servicio de ruta virtual entre los sitios de MCN y cliente.

Cambiar el nombre del sitio de sucursal

Después de cambiar el nombre del sitio de la sucursal, debe cargar el nuevo paquete de configuración a la red.

1. Desde el MCN, red de caso con nueva configuración que contiene el sitio de sucursal renombrado.
2. Descargue el paquete provisional para el sitio de sucursal renombrado.
3. En el **MCN**, seleccione **Activar red en etapas**. Esto inhabilita el sitio renombrado y el sitio deja de estar disponible.
4. Acceda a la página **Gestión de cambios Locales** de la sucursal.
5. Cargue el paquete descargado anteriormente. Haga clic en **Siguiente** y, a continuación, en **Activar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cambiar el nombre del sitio de sucursal con alta disponibilidad

Para cargar nueva configuración después de cambiar el nombre de un sitio de sucursal habilitado con alta disponibilidad:

1. Desde el MCN, red de caso con nueva configuración que contiene el sitio de sucursal renombrado.
2. Descargue el paquete provisional para el dispositivo activo y de alta disponibilidad con el sitio de sucursal renombrado.
3. En el **MCN**, seleccione **Activar en etapas** para la red. Esto inhabilita el sitio renombrado y el sitio deja de estar disponible.
4. Desplácese hasta el dispositivo activo en la sucursal. Vaya a la página **Administración de cambios locales**.
5. Cargue el paquete descargado anteriormente. Haga clic en **Siguiente** y, a continuación, en **Activar**.
6. Repita los pasos 4 (a) y 4 (b) para el dispositivo en espera.

Clonar el sitio de una sucursal (opcional)

May 7, 2021

Esta sección proporciona instrucciones para clonar el nuevo sitio de sucursal para usarlo como plantilla parcial para agregar más sitios de sucursal.

> **Nota**
>
> Clonar el sitio es opcional. Los modelos del dispositivo WAN virtual deben ser los mismos para los sitios originales y clonados. No se puede cambiar el modelo de dispositivo especificado para un clon. Si el modelo de dispositivo es diferente para un sitio, debe agregarlo manualmente, como se indica en las secciones anteriores.

La clonación de un sitio optimiza el proceso de agregar y configurar más nodos de sucursal. Cuando se clona un sitio, todo el conjunto de opciones de configuración del sitio se copia y se muestra en una sola página de formulario. A continuación, puede modificar la configuración de acuerdo con los requisitos del nuevo sitio. Algunos de los ajustes originales se pueden conservar, cuando corresponda. Sin embargo, la mayoría de la configuración debe ser única para cada sitio.

Para clonar un sitio, haga lo siguiente:

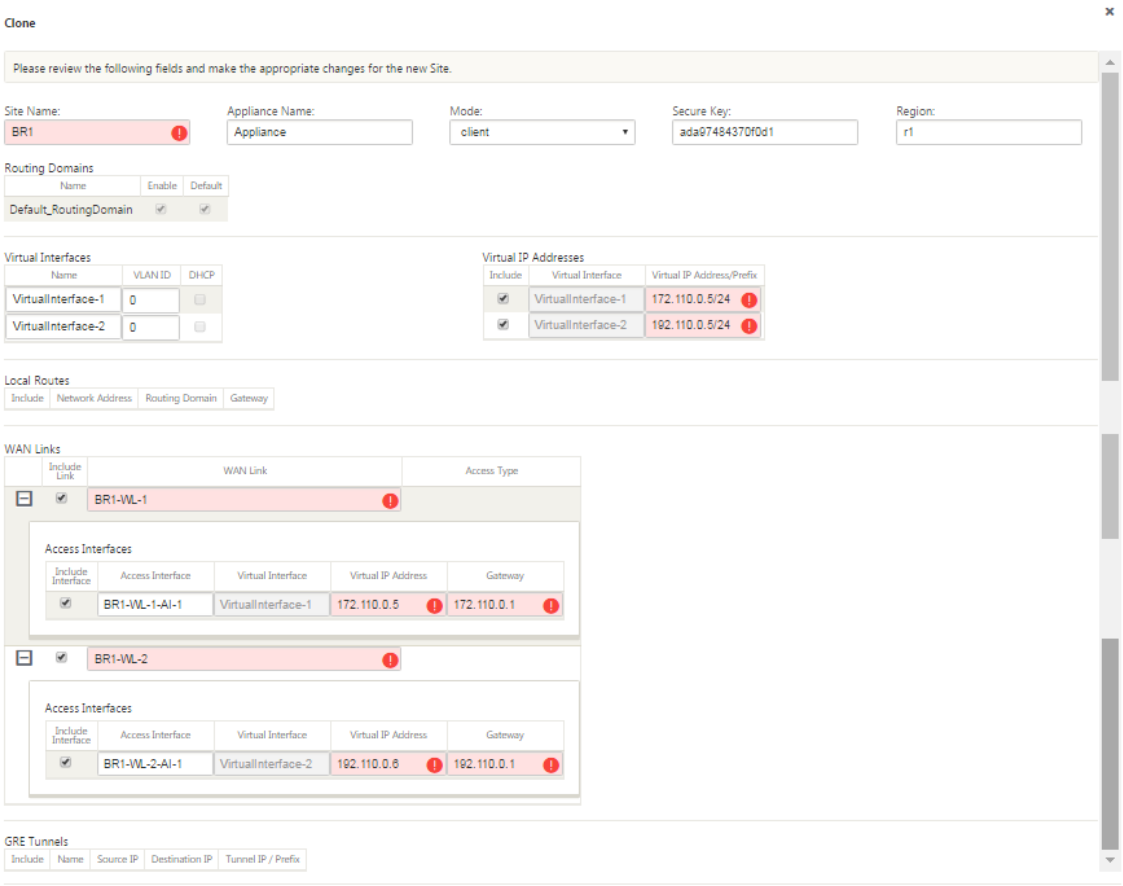
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el árbol **Sitios** (panel central) del **Editor de configuración**, haga clic en el sitio de sucursal que quiere duplicar.

   Esto abre esa sucursal del sitio en el árbol **Sitios** y muestra el botón **Clonar** (icono de página doble) y el botón Eliminar (icono de papelera).

2. Haga clic en el icono **Clonar** situado a la derecha del nombre del sitio de la sucursal en el árbol.

   Esto abre la página de configuración de **Clonar sitio**.



3. Introduzca los parámetros de configuración para el nuevo emplazamiento.

   Un campo rosa con un icono de alerta de auditoría (punto rojo) indica una configuración de parámetro necesaria que debe tener un valor diferente al de la configuración del sitio clonado original. Por lo general, este valor debe ser único.

   > **Sugerencia**
   >
   > Para optimizar aún más el proceso de clonación, utilice una convención de nomenclatura consistente predefinida al nombrar los clones.

4. Resuelva las alertas de auditoría.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para diagnosticar un error, pase el cursor sobre el icono **Alerta de auditoría** (punto rojo o delta de vara dorada) para revelar la ayuda de burbujas para esa alerta específica.

5. Haga clic en **Clonar** (esquina derecha) para crear el sitio y agregarlo a la tabla **Sitios**.

> **Nota**
>
> El botón **Clonar** no estará disponible hasta que haya introducido todos los valores necesarios y la nueva configuración del sitio no haya errores.

6. (Opcional.) Guarde los cambios en la configuración.

> **Nota**
>
> Como precaución adicional, se recomienda utilizar **Guardar como, en lugar de**Guardar****, para evitar sobrescribir el paquete de configuración incorrecto. Asegúrese de seleccionar **Permitir sobrescritura** antes de guardar en una configuración existente o los cambios no se guardarán.

Repita los pasos hasta este punto para cada sitio de sucursal que quiera agregar.

Después de haber terminado de agregar todos los sitios, el siguiente paso es comprobar la configuración de las alertas de auditoría y realizar las correcciones o adiciones necesarias.

Realizar auditorías de la configuración de sucursales

May 7, 2021

Un icono de alerta de auditoría (un punto rojo o un delta de vara dorada) junto a un elemento indica un error de configuración o falta información de parámetros para ese elemento. Un número junto al icono indica el número de errores asociados para esa alerta. Para ver la ayuda de burbujas para una alerta concreta, pase el cursor sobre el icono de alerta. Muestra una breve descripción de los errores específicos marcados por esa alerta. Debe resolver todas las alertas de auditoría de la configuración o no podrá verificar, organizar y activar el paquete de configuración más adelante en el proceso de implementación.

La resolución de todas las alertas de auditoría (si las hay) completa la fase **Sitios** de la configuración. El siguiente paso es guardar la configuración de **Sitios** completada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

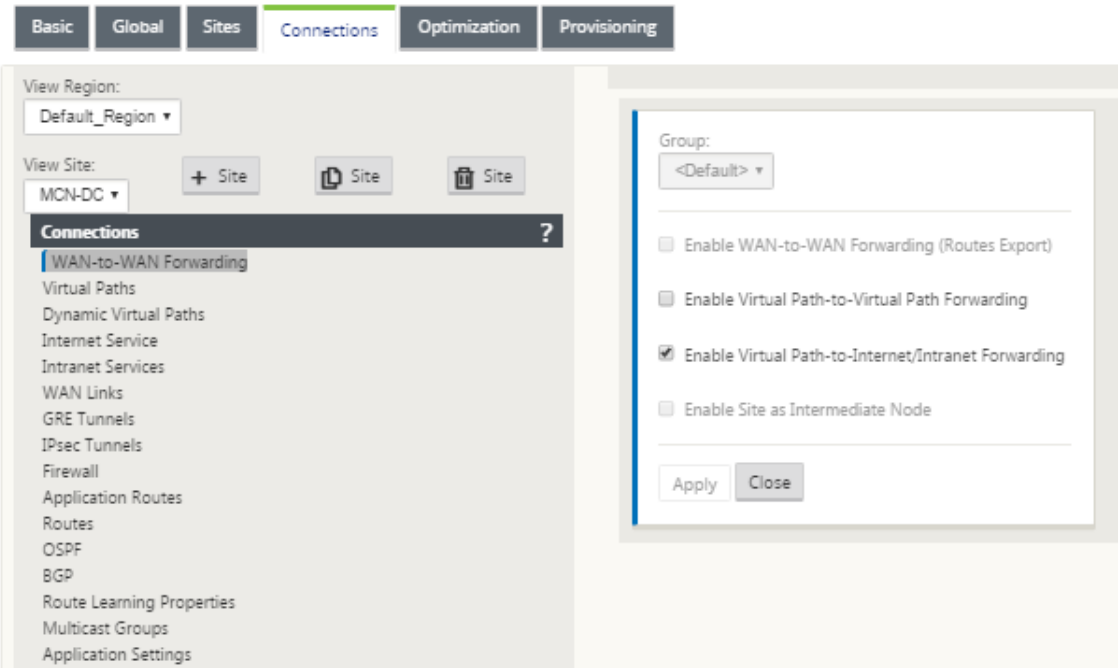
Configuración del servicio de rutas virtuales entre los sitios de MCN y cliente

May 7, 2021

El siguiente paso es configurar Virtual Path Service entre el MCN y cada uno de los sitios cliente (sucursal). Para ello, utilice los formularios de configuración y los parámetros disponibles en el árbol de configuración de la sección **Conexiones** del **Editor de configuración**.

Para configurar el servicio de rutas virtuales entre el MCN y un sitio cliente, haga lo siguiente:

1. Continuando en el **Editor de configuración**, haga clic en la ficha **Conexiones**. Muestra el árbol de configuración de la sección **Conexiones**.
2. Seleccione el **MCN** en el menú implementable **Ver sitio** en la página de la sección **Conexiones**. Esto abre el sitio de MCN en la configuración de **Conexiones**.

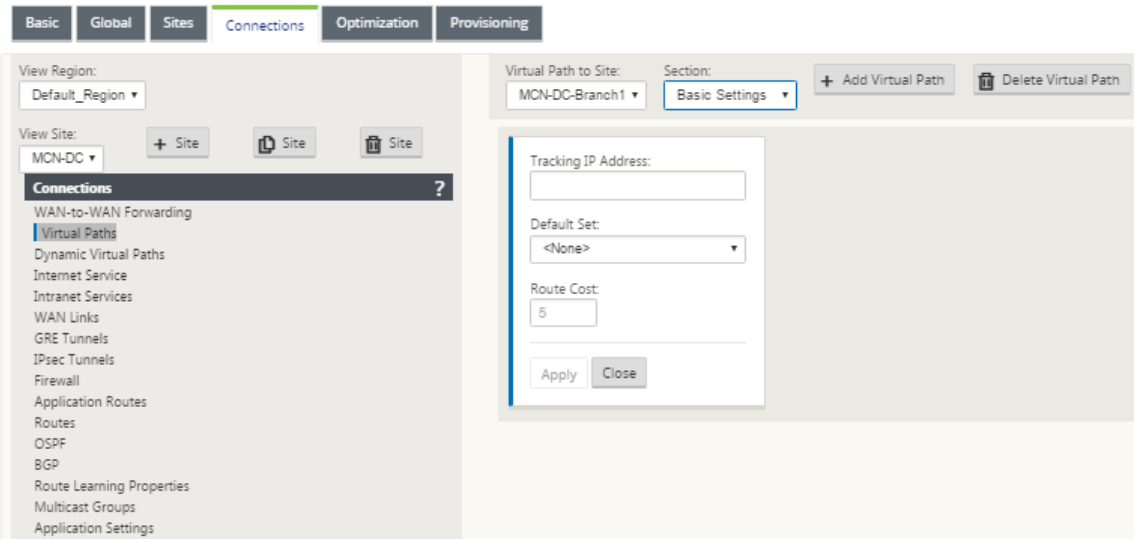


> **Nota**
>
> Los grupos de reenvío de WAN a WAN solo se admiten dentro de una región y no entre regiones. Puede utilizar Regiones para segregar redes en lugar de depender de grupos de reenvío WAN a WAN.

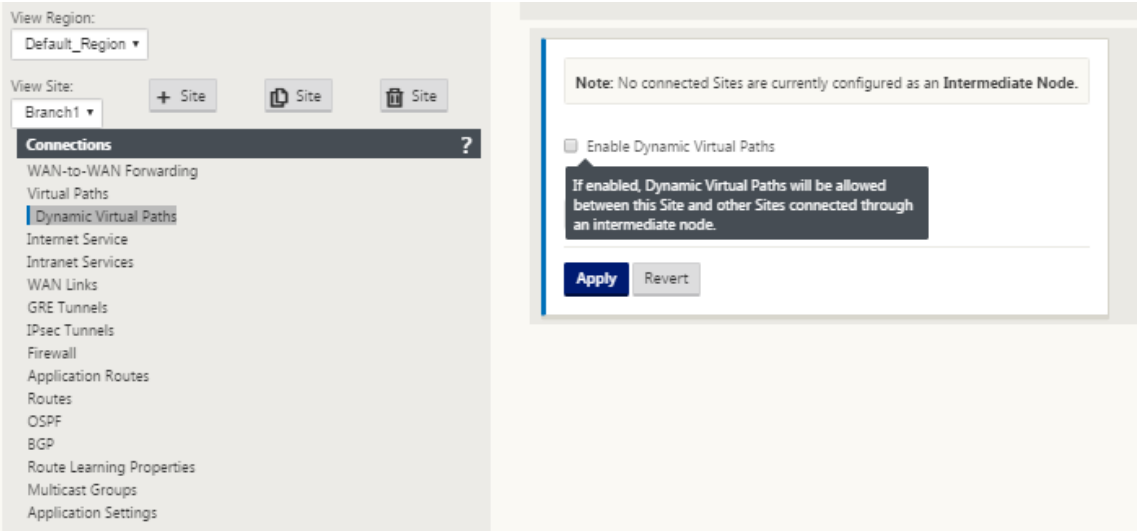
3. Haga clic en **Rutas virtuales**. Esto abre la sección **Configuración de rutas virtuales** (sucursal secundaria) para el sitio de MCN. En esta sección se proporcionan configuraciones y formularios para configurar el servicio de rutas virtuales entre el MCN y cada uno de los sitios cliente de WAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

virtual. La siguiente figura muestra una sección de rutas virtuales de ejemplo para un sitio de MCN.



En la siguiente figura se muestra una sección de **rutas virtuales dinámicas** de ejemplo para un sitio de sucursal.



La sección **Rutas Virtuales Dinámicas** permite configurar lo siguiente:

- **Rutas virtuales dinámicas** (opcional): La configuración de esta sección le permite habilitar y inhabilitar Rutas virtuales dinámicas y establecer las rutas virtuales dinámicas máximas permitidas para el sitio. Las rutas virtuales dinámicas son rutas virtuales que se establecen directamente entre sitios, en función de un umbral configurado. El umbral suele basarse en la cantidad de tráfico que se produce entre esos sitios. Las rutas virtuales dinámicas solo funcionan después de alcanzar el umbral especificado. Las rutas virtuales dinámicas no son necesarias para el funcionamiento normal, por lo que la configuración de esta sección es opcional.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **<MCN_Site_Name>**_<**Branch_Site_Name**>: El sistema inicialmente agrega automáticamente una ruta virtual estática entre el MCN y un sitio cliente, ya que esta ruta virtual es necesaria. El nombre de la ruta de acceso utiliza el siguiente formulario:

  <MCN_Site_Name>_<Branch_Site_Name>

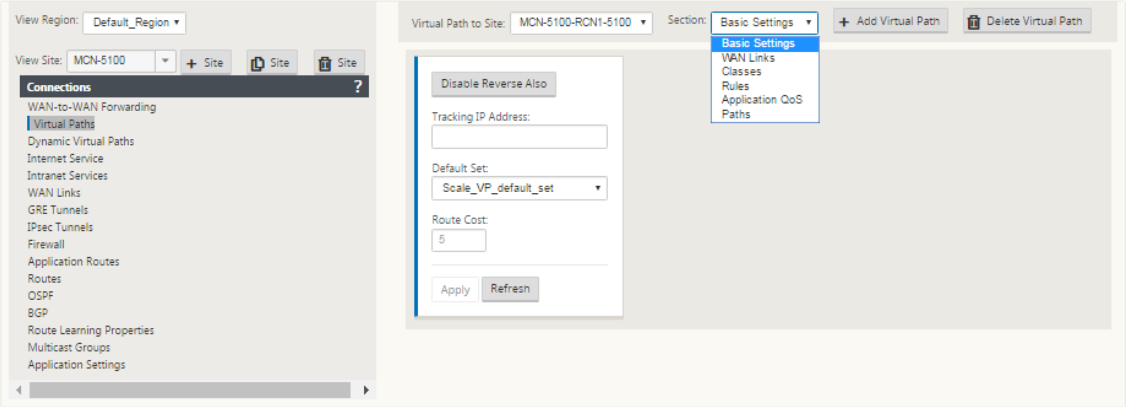
  Donde:

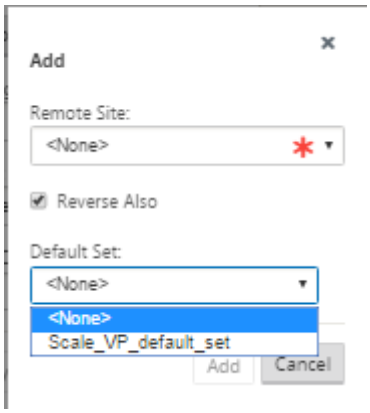
  MCN_Site_Name es el nombre del MCN para esta WAN virtual.

  Branch_Site_Name es el nombre de un sitio de cliente identificado en el paquete de configuración actual.

La configuración predeterminada configurable por el usuario se aplica inicialmente a la ruta virtual estática, tal como se define en la sección **Ruta virtual > Conjuntos predeterminados** del árbol de configuración de **Conexiones**. Sin embargo, puede personalizar o agregar a los **conjuntos predeterminados**definidos, así como personalizar la configuración de un sitio específico y una ruta virtual.

> **Nota**
>
> Para agregar más rutas virtuales estáticas para un sitio, debe hacerlo manualmente. Las instrucciones para agregar manualmente una ruta virtual estática se incluyen en los pasos que se indican a continuación.





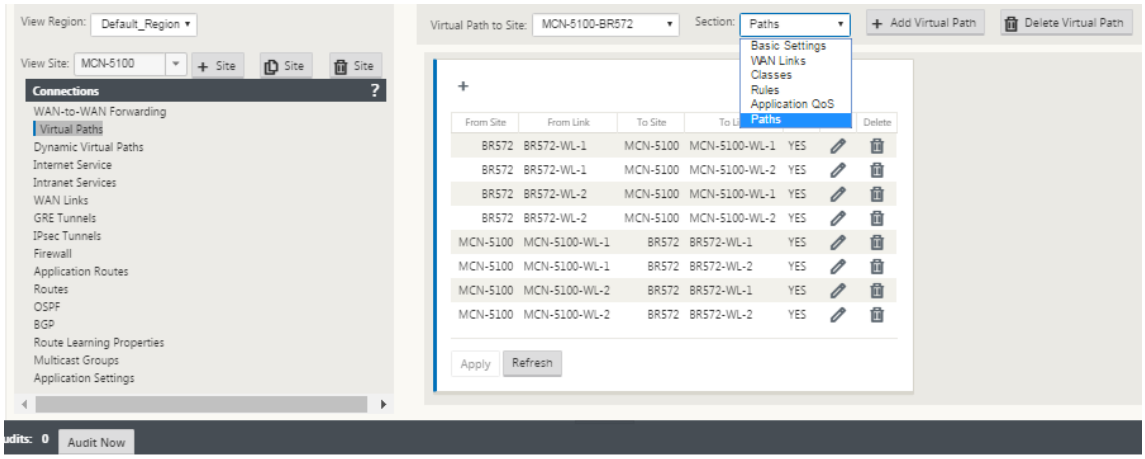
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Haga clic en **+ Agregar ruta virtual** junto al nombre de la ruta virtual estática en la sección **Rutas virtuales**. Esto revela más configuración para la ruta virtual estática:

   a) **Sitio remoto**: Esta sección le permite ver y configurar los valores de **ruta virtual** desde la perspectiva de un sitio remoto. Puede ver, personalizar y agregar **clases** o **reglas** según sea necesario para esta ruta virtual específica. También puede agregar rutas virtuales al sitio remoto, según sea necesario.
   b) **Invertir también**: Cuando está habilitado, las clases y las reglas se reflejan en ambos sitios la ruta virtual.
   c) **Conjunto predeterminado**: Nombre del conjunto predeterminado de ruta virtual que se utiliza para rellenar reglas y clases para la ruta virtual en el sitio.

   En la siguiente figura se muestra un ejemplo de sucursal de ruta virtual estática de MCN y sucursales secundarias.

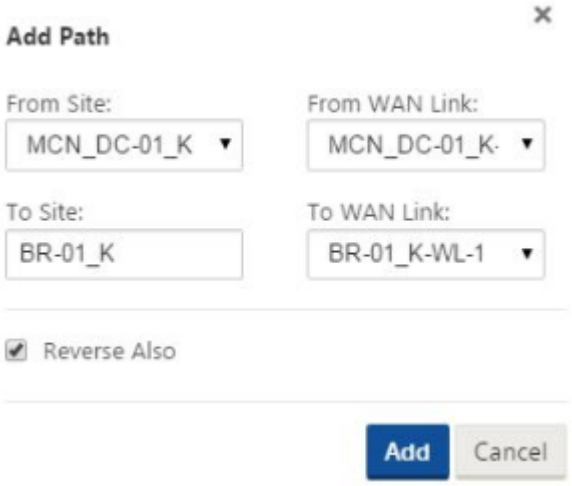
5. Seleccione **Rutas** en el menú implementable **Sección**.



6. Haga clic en **+** (Agregar) encima de la tabla **Rutas**.

   Muestra el cuadro de diálogo **Agregar ruta** (formulario de configuración).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



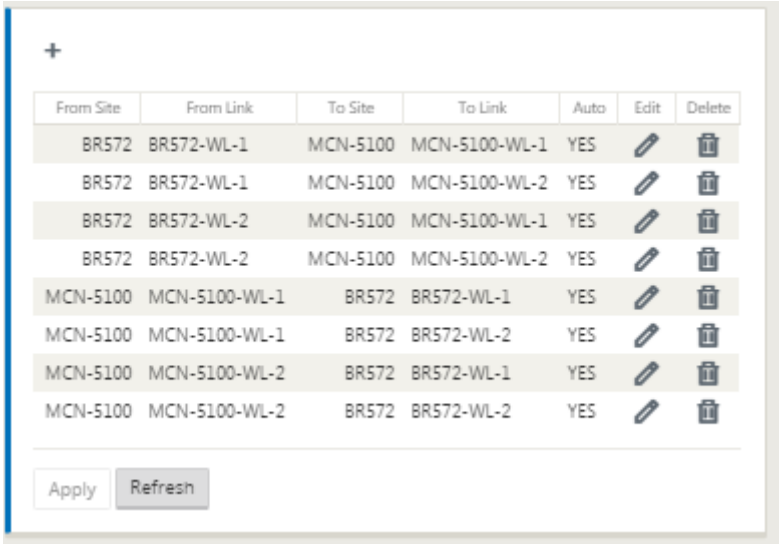
7. Especifique la información del sitio de origen y destino para la nueva ruta virtual.
8. Especifique lo siguiente en los menús desplegables disponibles:

> **Nota**
>
> Dependiendo de cómo se configuran los enlaces WAN para los sitios, algunos campos son de solo lectura. Los campos configurables proporcionan un menú desplegable con las selecciones disponibles.

   - **Desde el sitio**: Este es el sitio de origen de la ruta de acceso virtual. Para la ruta virtual estática requerida, se configura como el sitio de MCN de forma predeterminada.
   - **Desde el enlace WAN**: Este es el enlace WAN de origen para la ruta virtual.
   - **Al sitio**: Este es el sitio de destino de la ruta de acceso virtual.
   - **Enlace a WAN**: Este es el enlace WAN de destino para la ruta de acceso virtual.
9. Haga clic en **Agregar**.

   Esto agrega la ruta virtual configurada tanto al MCN como al sitio cliente asociado en el árbol **Conexiones > Rutas virtuales**. Esto también abre automáticamente el formulario de configuración de **rutas** para el **sitio de origen** para la ruta virtual (en este caso, el MCN).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



From Site	From Link	To Site	To Link	Auto	Edit	Delete
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-2	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-2	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-2	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-2	YES		

Apply Refresh

10. Haga clic en Modificar (icono de lápiz), a la derecha de la etiqueta Ruta virtual de McN-to-Client. Esto abre el formulario de configuración de Virtual Path Service para su edición.
11. Configure los valores de la ruta de acceso virtual o acepte los valores predeterminados.

    El formulario de configuración de **rutas** contiene los siguientes valores:

    - **Desde la sección Sitio** :
      - **Sitio**: Este es el sitio de origen de la ruta de acceso virtual. Para la ruta virtual estática requerida, se configura como el sitio de MCN de forma predeterminada.
      - **Enlace WAN**: Este es el enlace WAN de origen para la ruta virtual.
    - Sección**To Site** :
      - **Sitio**: Este es el sitio de destino de la ruta virtual.
      - **Enlace WAN**: Este es el enlace WAN de destino para la ruta de acceso virtual.
    - **Invertir también**: Active esta casilla de verificación para habilitar Invertir también para esta ruta virtual. Si está habilitado, el sistema crea automáticamente una ruta virtual en la dirección opuesta a la ruta configurada, mediante los mismos enlaces WAN configurados para la ruta original.
    - **Etiquetado DSCP IP**: Seleccione una etiqueta en el menú implementable. Especifica la etiqueta DSCP que se va a establecer en el encabezado IP para el tráfico que viaja a través de esta ruta virtual.
    - **Habilitar cifrado**: Active esta casilla de verificación para habilitar el cifrado de los paquetes enviados a lo largo de esta ruta virtual.
    - **Sensible a pérdidas incorrectas**: Seleccione una configuración en el menú implementable. Las opciones son:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

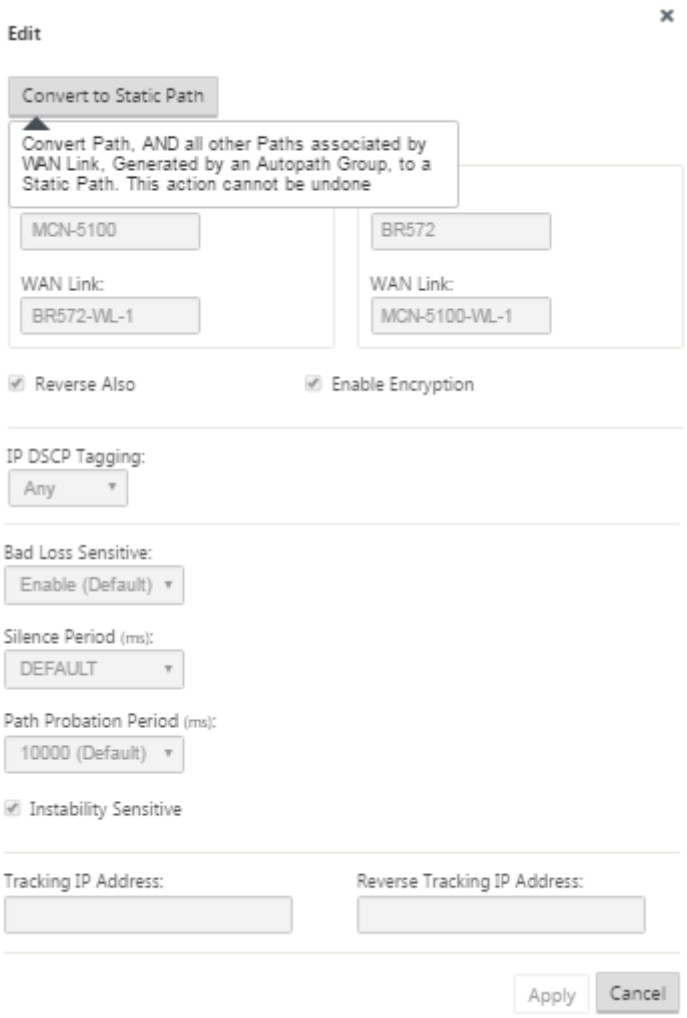
- **Habilitar**: (Predeterminado) Si está activado, las rutas se marcan como **MAL**debido a la pérdida, y incurrirán en una penalización de puntuación de ruta.
- **Desactivar**: Inhabilitar la función **Sensible a pérdidas incorrectas** puede ser útil cuando la pérdida de ancho de banda es intolerable.
- **Personalizado**: Seleccione Personalizado para especificar el porcentaje de pérdida a lo largo del tiempo necesario para marcar una ruta como INCORRECTA. Al seleccionar esta opción, se muestran los siguientes ajustes adicionales:
  * **Porcentaje de pérdida (%)**: Especifica el porcentaje del umbral de pérdida antes de que una ruta se marque como mala, medido durante el tiempo especificado. De forma predeterminada, el porcentaje se basa en los últimos 200 paquetes recibidos.
  * **Durante el tiempo (ms)**: Especifique el período de tiempo (en milisegundos) durante el cual se mide la pérdida de paquetes. Seleccione una opción entre 100 y 2000 en el menú desplegable de este campo.
- **Período de silencio (ms)**: Especifica la duración (en milisegundos) antes de que el estado de ruta pase de **BIEN** a **MAL**.

El valor predeterminado es 150 milisegundos. Seleccione una opción entre 150 y 1000 en el menú desplegable de este campo.

- **Período de prueba de ruta (ms)**: Especifica el tiempo de espera (en milisegundos) antes de que una ruta pase de MAL a BIEN. Seleccione una opción entre 500 y 60000 en el menú desplegable de este campo. El valor predeterminado es 10.000 milisegundos.
- **Sensible a la inestabilidad**: Active esta casilla de verificación para activarla. Si se habilita, las penalizaciones de latencia debidas a un estado de ruta de acceso de **MAL** y otros picos de latencia se consideran en el algoritmo de puntuación de ruta.
- **Dirección IP de seguimiento**: Introduzca una dirección IP virtual en la ruta de acceso virtual que se puede hacer ping para determinar el estado de la ruta.
- **Dirección IP de seguimiento inverso**: Si está activada la opción **Invertir también** para la ruta de acceso virtual, introduzca una dirección IP virtual en la ruta de acceso que se puede hacer ping para determinar el estado de la ruta de acceso inversa.

12. Haga clic en **Aplicar**. Esto revela que las dos nuevas rutas virtuales **desde el sitio**y **hacia el sitio** entre el MCN y el sitio cliente se han agregado a la tabla Rutas de acceso.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

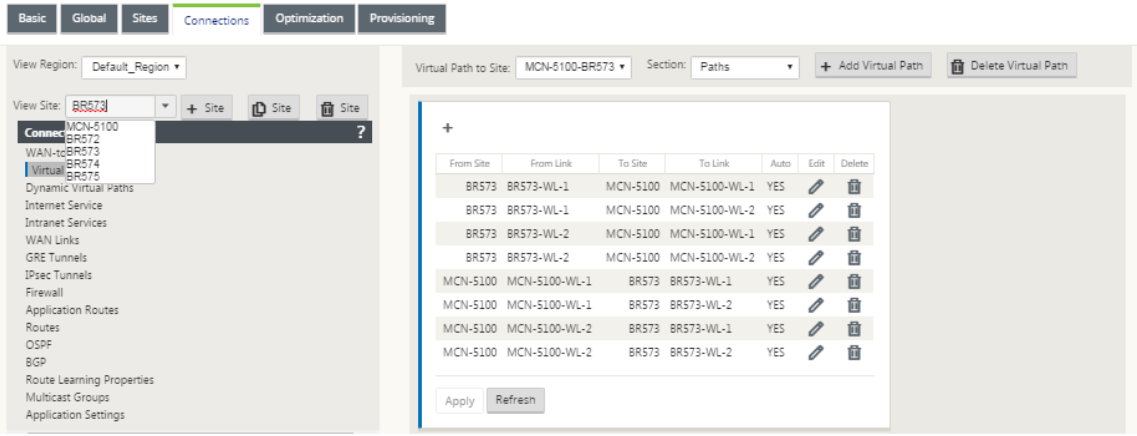


13. Repita los pasos anteriores para cada sucursal que quiera conectar al MCN.

    A continuación, tiene la opción de personalizar las configuraciones de rutas virtuales para los sitios cliente, así como agregar y configurar más rutas entre clientes. Las instrucciones se proporcionan en los pasos restantes, a continuación.

14. Seleccione una sucursal de sitio cliente en el menú implementable **Ver sitio**. Se abre la configuración de la sucursal del sitio del cliente en el árbol de **Conexiones**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

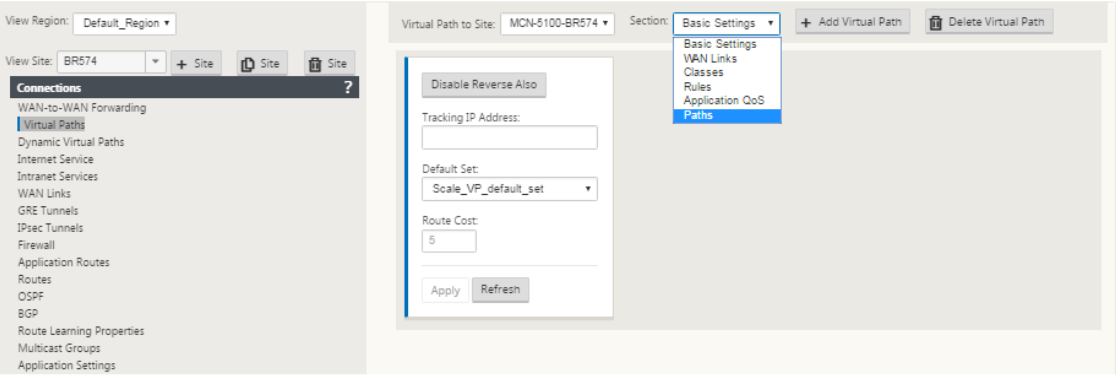


15. Desplácese hasta el formulario de configuración de **rutas** de acceso para cualquier ruta de acceso virtual del sitio cliente que quiera configurar.

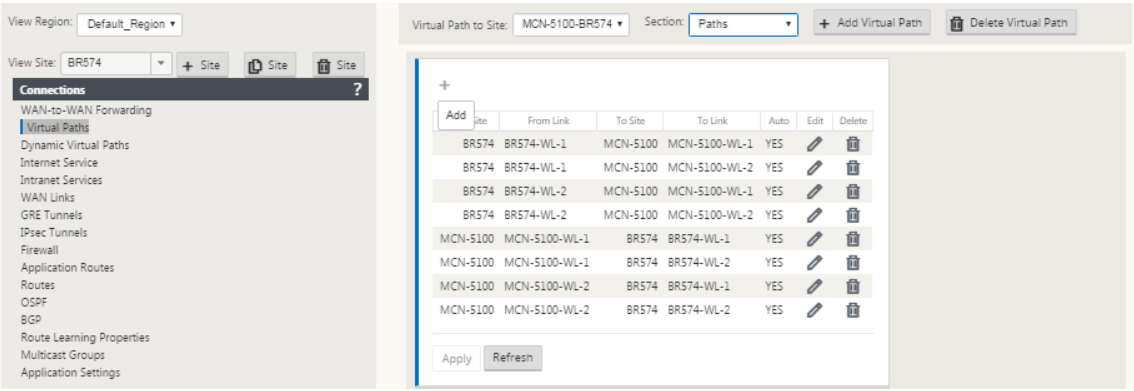
    Para desplazarse al formulario configuración de **Rutas** para el sitio cliente, haga lo siguiente:

16. Seleccione **Rutas de acceso** en la ficha **Sección** de la página de sucursal para el sitio cliente.

    En la siguiente figura se muestra un formulario de configuración de **Rutas** de la nueva ruta **desde el sitio** agregada en los pasos anteriores.



17. Configure los parámetros para cada ruta que quiera personalizar. Siga los mismos pasos que hizo para configurar las rutas virtuales para el sitio de MCN.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Esto completa la configuración básica de las rutas virtuales entre los sitios cliente y el MCN.

> **Nota**
>
> Para obtener información sobre la configuración de más opciones en las secciones **Conexiones** o **Aprovisionamiento** del **Editor de configuración**, consulte la ayuda en línea de la Interfaz Web de administración para esas secciones. Si no quiere configurar estos parámetros actualmente, puede continuar con el paso apropiado que se indica a continuación.

El siguiente paso depende de la licencia SD-WAN Edition que haya activado para su implementación, como se indica a continuación:

- **SD-WAN Premium (Enterprise) Edition:** la edición Premium (Enterprise) incluye el conjunto completo de funciones de optimización de WAN. Si quiere configurar la optimización WAN para sus sitios, continúe con el tema.Habilitación y configuración de la optimización WAN De lo contrario, puede proceder directamente a Instalación de los paquetes de dispositivos SD-WAN en los clientes.
- **Edición SD-WAN**: Esta edición no incluye las funciones de optimización WAN. Ahora puede proceder directamente a Instalación de los paquetes de dispositivos SD-WAN en los clientes.

Implementar configuración de MCN

May 7, 2021

El siguiente paso es preparar los paquetes del dispositivo SD-WAN para su distribución a los nodos cliente. Esto implica los dos procedimientos siguientes:

1. Exporte el paquete de configuración a Administración de cambios.

   Antes de poder generar los paquetes del equipo, primero debe exportar el paquete de configuración completado desde el **Editor de configuración** a la bandeja de entrada provisional de **administración de cambios** global en el MCN. Las instrucciones se proporcionan en la sección.Realizar administración de cambios

2. Generar y organizar los paquetes del equipo.

   Después de agregar el nuevo paquete de configuración a la bandeja de entrada **de Administración de cambios**, puede generar y organizar los paquetes del equipo. Para ello, utilizará el Asistente para **administración de cambios** en la Interfaz Web de administración del MCN. Las instrucciones se proporcionan en la secciónImplementar configuración en sucursales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

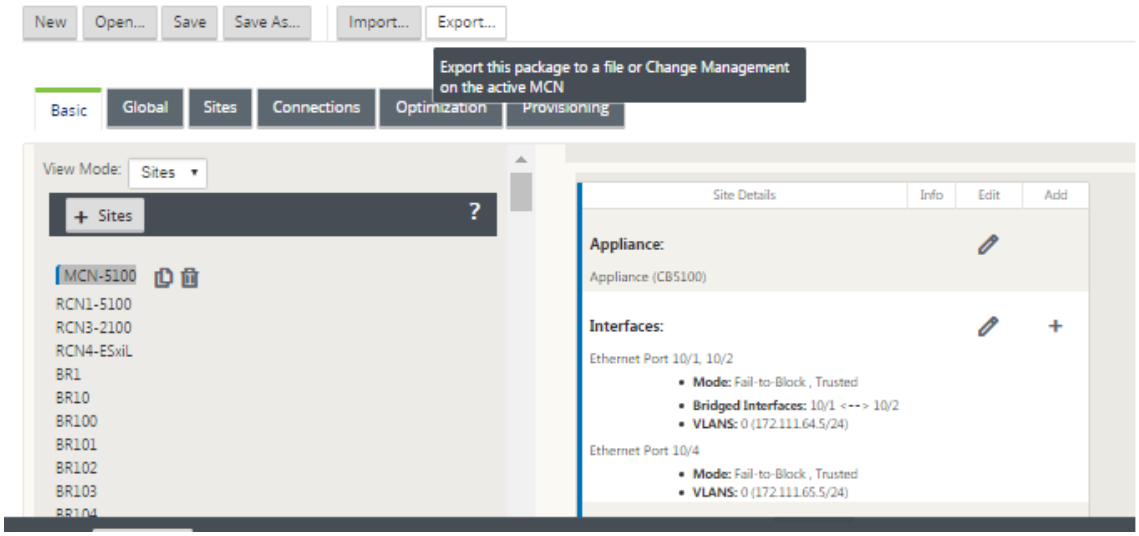
Realizar administración de cambios de MCN

May 7, 2021

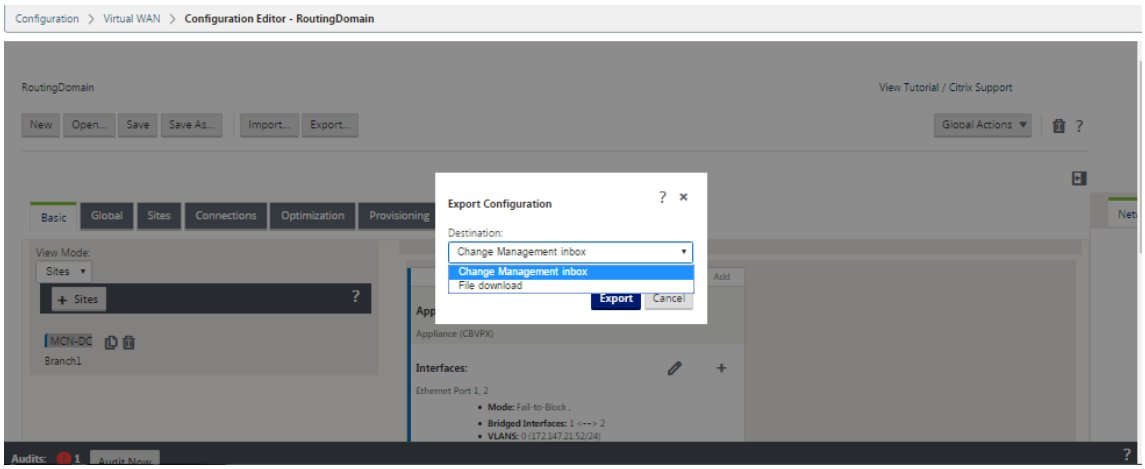
Antes de poder generar los paquetes del dispositivo, primero debe exportar el paquete de configuración completado al sistema Management Web Interface **Change Management**.

Para exportar el paquete de configuración a **Administración de cambios**, haga lo siguiente:

1. En la página **Editor de configuración**, haga clic en **Exportar** (en la parte superior de la página).



Se abre el cuadro de diálogo **Configuración de exportación**.



2. Seleccione Bandeja **de entrada de administración de cambios** como destino de exportación. Utilice el menú implementable del campo **Destino** para realizar la selección.
3. Pulse **Exportar.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cuando finaliza la operación de exportación, aparece un mensaje de estado de éxito verde en la parte superior de la página.

> **Sugerencia**
>
> Puede hacer clic en el vínculo azul **Administración de cambios** en el mensaje de éxito para ir directamente a la página **Preparación de cambios**: **Cargar y verificar archivos** (segunda página) del Asistente para **administración de cambios**. Tendrá que navegar a esta página para realizar el siguiente paso en el proceso de configuración. Sin embargo, el mensaje de éxito se muestra solo durante unos segundos, después de lo cual debe utilizar el árbol de navegación para abrir el asistente y, a continuación, pasar a esta página. Las instrucciones se proporcionan en la siguiente sección.

Ahora está listo para cargar los paquetes de software SD-WAN al dispositivo MCN y preparar los paquetes del dispositivo para distribuirlos a los nodos cliente.

Implementar configuración en sucursales

May 7, 2021

Después de haber preparado la configuración mediante el editor de configuración y exportado el paquete de configuración a la bandeja de entrada de administración de cambios, el siguiente paso es preparar los paquetes de dispositivo SD-WAN para su distribución a los nodos cliente. Utilice el Asistente para **administración de cambios** en la Interfaz Web de administración en el MCN.

Hay un paquete de software SD-WAN diferente para cada modelo de dispositivo SD-WAN. Un paquete de dispositivo consiste en el paquete de software para un modelo específico, incluido con el paquete de configuración que quiere implementar. Por lo tanto, se debe preparar y generar un paquete de dispositivo diferente para cada modelo de dispositivo de la red.

> **Nota**
>
> Si aún no ha descargado los paquetes de software SD-WAN necesarios a un PC conectado a su red, puede hacerlo ahora. Para obtener información sobre cómo adquirir y descargar el software, consulte la sección Adquirir los paquetes de software SD-WAN

Para cargar e instalar el paquete y la configuración en el MCN, haga lo siguiente:

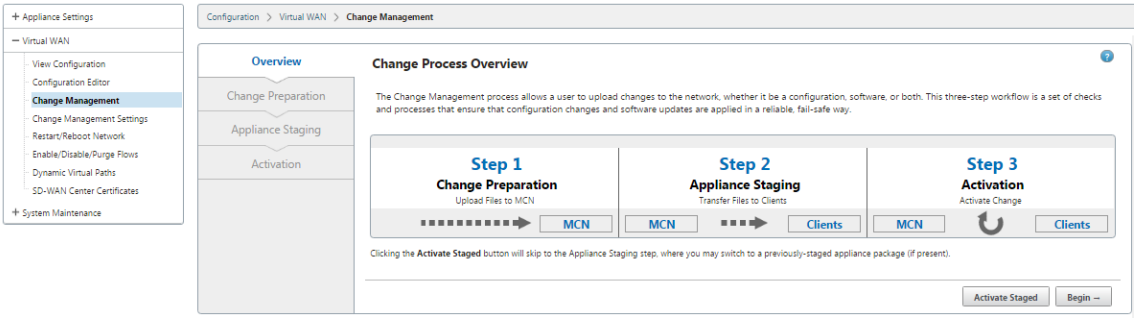
1. Inicie sesión en la Interfaz Web de administración en el dispositivo MCN.

   > **Nota**
   >
   > Está cargando los paquetes de software que descargó previamente en el PC conectado.

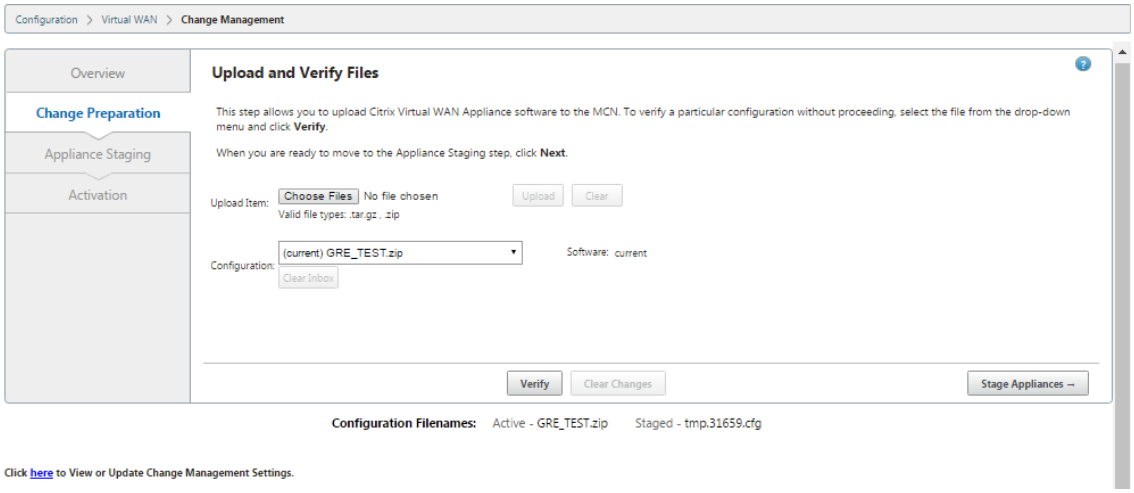
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Para mayor comodidad, es posible que quiera utilizar este mismo equipo para conectarse de nuevo al MCN.

2. Seleccione la ficha **Configuración**.
3. En el panel izquierdo, abra la sección **WAN virtual** y seleccione **Administración de cambios**. Aparece la primera página del asistente de **administración de cambios**, la página **Resumen del proceso de los cambios**.



4. Haga clic en **Iniciar**. La página **Preparación de Cambios** para cargar y comprobar que se muestran los paquetes de software y configuración especificados.



5. Cargue cada uno de los paquetes de software SD-WAN necesarios para su red.
   Para cada paquete de software SD-WAN que quiera implementar, haga lo siguiente:

   a) Haga clic en **Elegir archivo** junto al campo **Subir elemento**. Esto abre un explorador de archivos para seleccionar un paquete de software SD-WAN para cargar.

   b) Seleccione un paquete de software SD-WAN y haga clic en **Aceptar**.

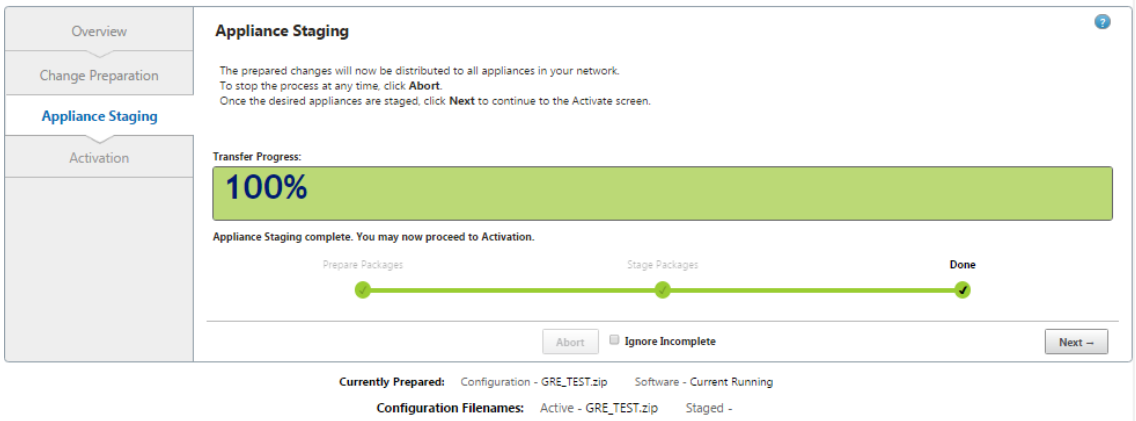
   c) Desplácese hasta los paquetes de software SD-WAN que descargó anteriormente en el PC local y seleccione el paquete que quiere cargar.

   d) Haz clic en **Cargar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) Repita los pasos (i) a (iii) para cada uno de los paquetes de software SD-WAN necesarios para su red.

6. En el menú implementable del campo **Configuración**, seleccione el nuevo paquete de configuración que acaba de exportar a **Administración de cambios**.
7. Haga clic en **Stage Appliance**. La puesta en escena del dispositivo inicia las siguientes acciones:
   - Transfiere el paquete de software seleccionado y la configuración al MCN.
   - Genera un paquete de equipo para cada modelo de dispositivo identificado en la configuración seleccionada.
   - Agrega los nuevos paquetes del equipo a la lista de paquetes disponibles en la tabla Site-Appliance.
   - Etapas la nueva configuración y el paquete de software apropiado en el MCN.
8. Haga clic en **Siguiente**. Esto pasa a la página de **ensayo del dispositivo**.



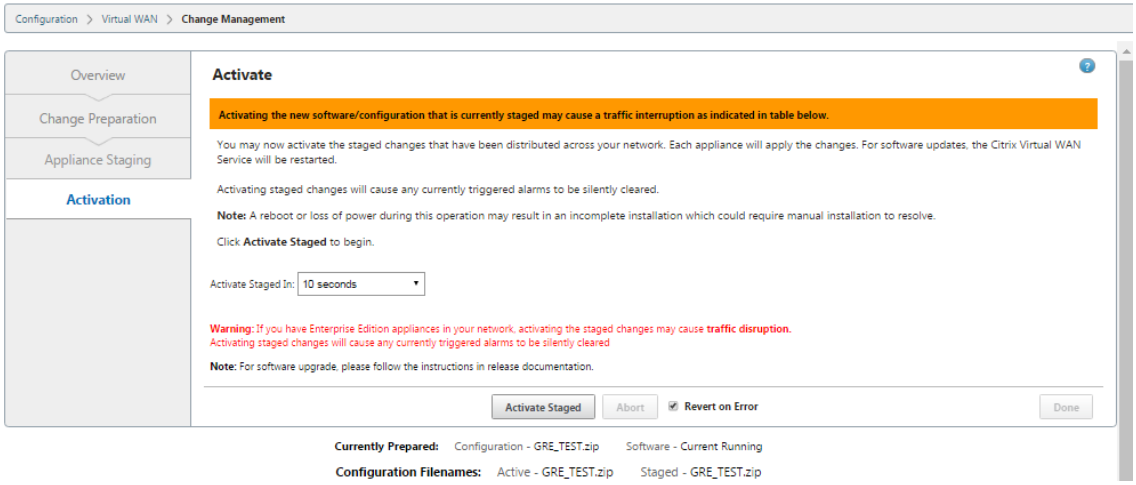
Una vez finalizada la operación provisional, la tabla Site-Appliance** se rellena con la información de los paquetes de dispositivos que se han instalado recientemente.

> **Nota**
>
> Si se trata de una implementación inicial, solo el MCN se actualiza y se pone en escena ahora. Si está actualizando una implementación existente y las rutas virtuales ya están funcionando entre los sitios implementados, esto también distribuye los paquetes de dispositivo adecuados a los nodos de cliente implementados e inicia la puesta en escena en esos nodos. Sin embargo, si va a agregar nuevos nodos de cliente a una implementación de WAN virtual existente, deberá cargar, organizar y activar manualmente el paquete de dispositivo adecuado en cada cliente nuevo, como se describe en los pasos restantes de este procedimiento.
>
> Seleccione **Omitir incompleto**, cuando agregue más sitios a la red o si el sitio **no está**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **conectado** . Esto indica que sólo los sitios conectados y el MCN se actualizan y se organizan en etapas. Una vez que los sitios que **no estaban conectados** vuelven a estar conectados, MCN los actualiza automáticamente como parte de la corrección automática.

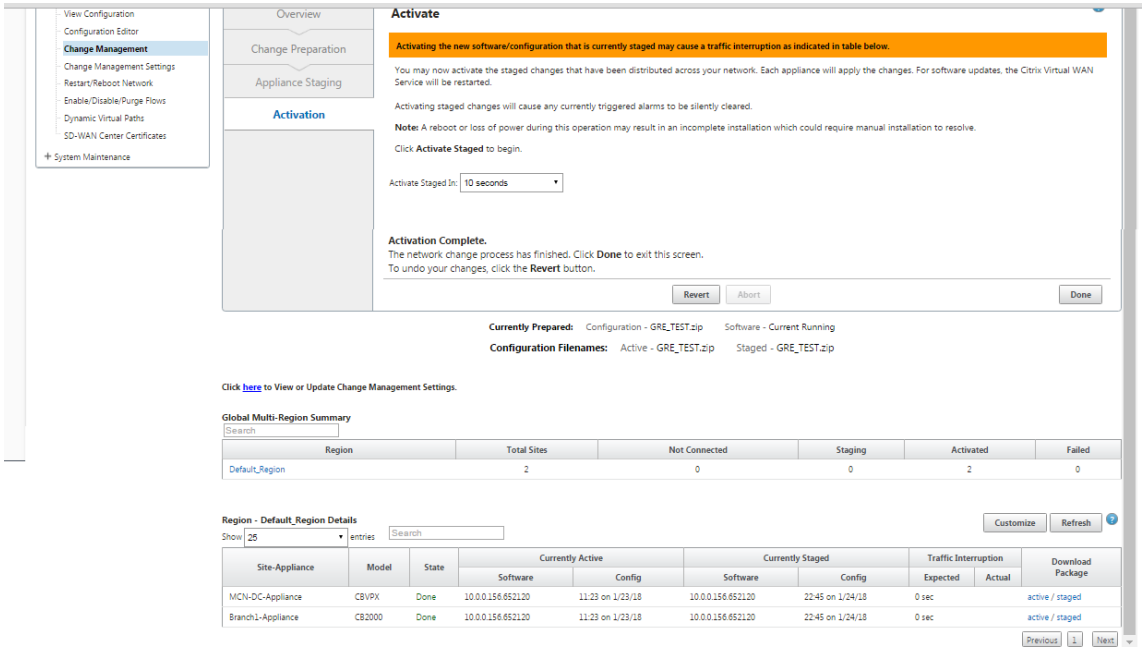
9. Seleccione **Revertir en Error** para volver al paquete de aplicación anterior al encontrar algún error. Para obtener más información, consulte Configuración Rollback.
10. Haga clic en **Activar por etapas**.



Los resultados y los pasos siguientes difieren en este punto, dependiendo de si se trata de una configuración inicial o si está actualizando o reemplazando una configuración existente, como se indica a continuación:

- Si está actualizando o cambiando la configuración en una implementación existente.
  - Si no se trata de una configuración inicial, se activarán la nueva configuración y el paquete del dispositivo apropiado en el dispositivo MCN. A continuación, el paquete del dispositivo apropiado se distribuye y se activa automáticamente en cada cliente de la SD-WAN. Esto puede tardar varios segundos en completarse.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cuando se complete la activación, aparece un mensaje de estado **Activación completada** y se habilita el botón **Listo**. Además, la línea de estado **Nombres de archivo de configuración** (encima de la tabla) ahora muestra el nombre del paquete recién activado en el campo **Activo**.

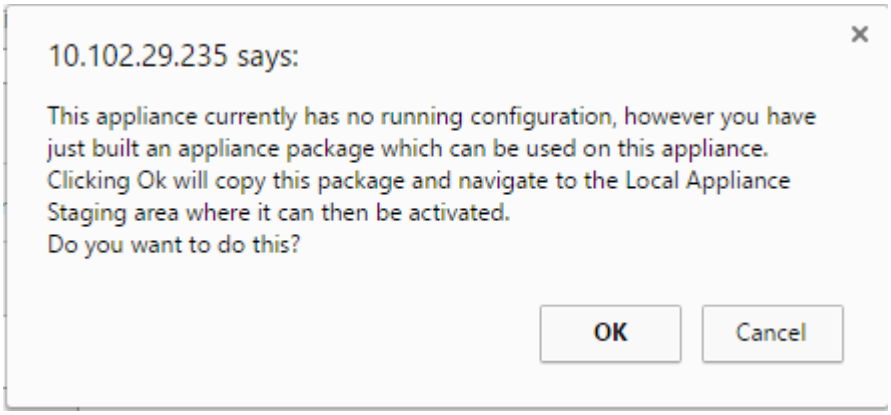
11. Haga clic en **Listo** y continúe con una de las siguientes opciones:

    - Si no va a agregar nodos nuevos a su SD-WAN, esto completa la preparación, distribución y activación de los nuevos paquetes de dispositivos en su SD-WAN. Puede proceder directamente a.Habilitación del servicio WAN virtual
    - Si quiere agregar nuevos nodos de cliente a su SD-WAN, vaya a Conexión de los dispositivos cliente a la red.
    - Si está activando una configuración inicial, el nuevo paquete de configuración no se activa en este momento, y hay más pasos que debe realizar. El siguiente paso es copiar el paquete de configuración en el área Local Appliance Staging, como preparación para la puesta en escena y la activación del paquete de configuración en el MCN.

    Haga lo siguiente:

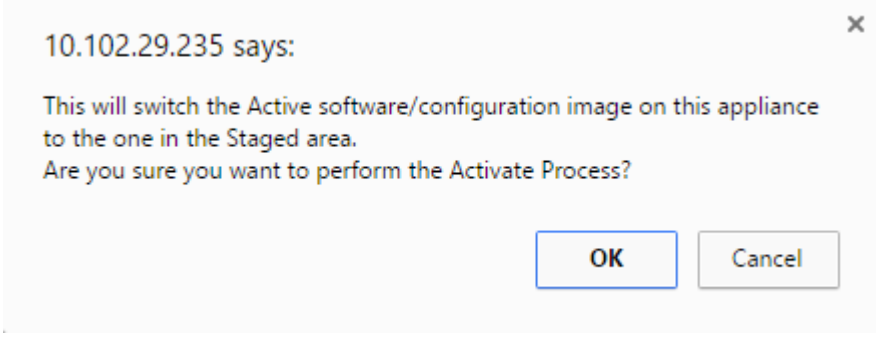
12. Una vez que haga clic en **Activar por etapas**, aparecerá el siguiente mensaje.

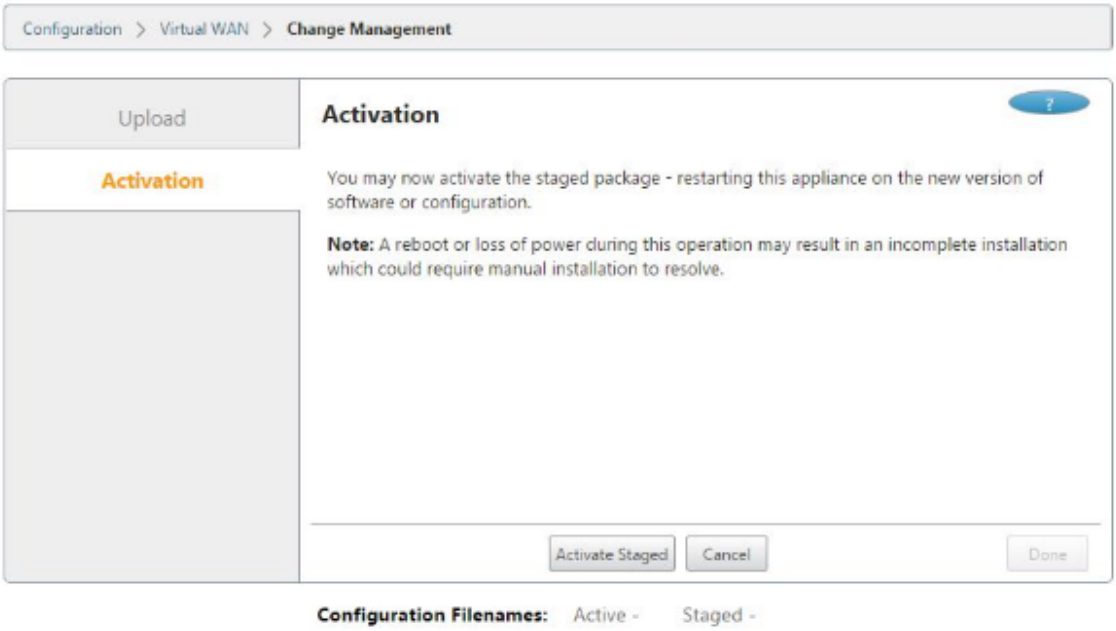
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



13. Haga clic en **OK**.
14. Haga clic en **Activar por etapas**.

    Aparece un cuadro de diálogo en el que se le pide que confirme la operación de activación.





15. Haga clic en **OK**.

    Esto inicia la activación del paquete de configuración por etapas. Este proceso tarda varios se-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

gundos, durante los cuales se muestra un mensaje de estado de progreso.

Cuando se complete la activación, aparece un mensaje de estado indicando la activación completada y el botón **Listo** está habilitado.

16. Haga clic en **Done**. Esto pasa a la página **Panel** de Control de Interfaz Web de Gestión, donde puede ver los resultados de activación.

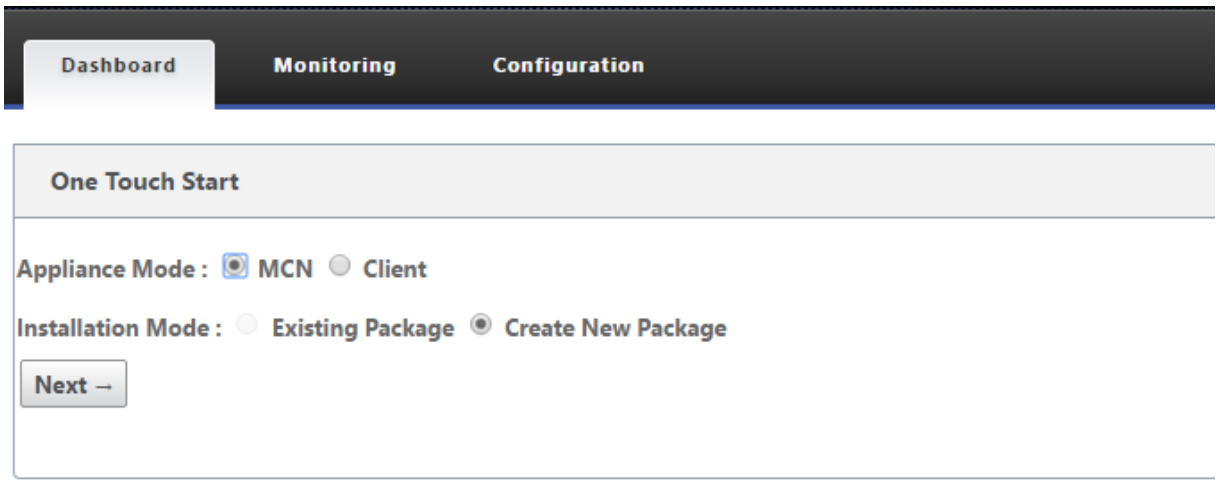
Ya ha completado la preparación de los paquetes de dispositivos SD-WAN en el MCN. Proceda a Conexión de los dispositivos cliente a la red.

> **Sugerencia**
>
> El Asistente **de administración de cambios** permite buscar en la tabla del sitio-dispositivo. Esto le permite buscar sitios en una red grande con varios sitios y descargar la configuración por etapas requerida. También puede buscar estados de error, por ejemplo: 'Fail'o 'Not connected'. Esto le da una lista de todos los sitios en ese estado.

Inicio con un solo toque

May 7, 2021

Una vez que toque, el inicio le permite configurar fácil y rápidamente su dispositivo SD-WAN como cliente en el inicio por primera vez.
La opción de inicio con un solo toque aparece cuando el dispositivo se inicia por primera vez.



> **Nota**
>
> Para configurar el dispositivo SD-WAN como un MCN, cree una configuración o importe una configuración existente mediante el **Editor de configuración**. Para obtener más información, con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

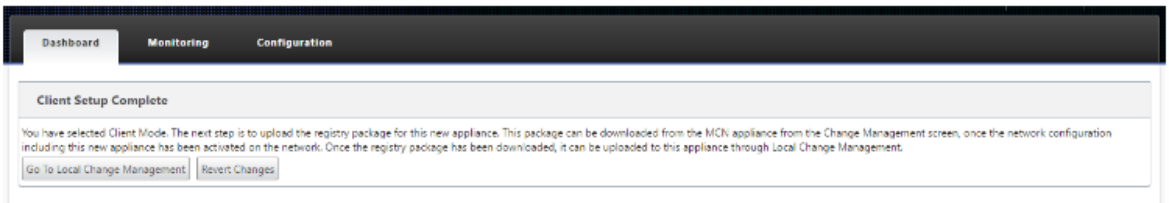
> sulte:Preparación de los paquetes de dispositivos SD-WAN en el MCN

Para configurar el dispositivo SD-WAN como cliente mediante un archivo de configuración existente:

1. Seleccione **Cliente** como modo de dispositivo.
2. Seleccione el modo de instalación **del paquete existente**. El administrador debe guardar periódicamente la configuración del MCN para hacer uso de un paquete existente del MCN.
3. Haga clic en **Elegir archivo** para seleccionar el paquete de configuración del equipo local.
4. Haga clic en **Upload and Install** (Cargar e instalar).

Para configurar el dispositivo SD-WAN como cliente mediante la administración de cambios locales:

1. Seleccione **Cliente** como modo de dispositivo.
2. Seleccione **Crear nuevo paquete** para cargar el paquete de configuración de este dispositivo mediante la administración de cambios locales. El paquete se puede descargar desde el dispositivo MCN desde la pantalla Administración de cambios.
3. Haga clic en **Siguiente**.
4. Haga clic en **Ir a Administración de cambios locales.**



Siga el procedimiento en el temaInstalación de los paquetes de dispositivos SD-WAN en los clientes.

Conexión de los dispositivos cliente a la red

May 7, 2021

Para una implementación inicial, o si va a agregar nodos de cliente a una SD-WAN existente, el siguiente paso es que los administradores del sitio de sucursal conecten los dispositivos cliente a la red en sus respectivos sitios de sucursal. Esto se prepara para cargar y activar los paquetes de dispositivos SD-WAN adecuados a 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

   a) Configure el hardware del dispositivo SD-WAN y los dispositivos virtuales SD-WAN VPX (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 alto o máximo.
   d) Cargue e instale el archivo de licencia de software en el dispositivo.

2. Conecte el dispositivo a la LAN del sitio de la sucursal. Conecte un extremo de un cable Ethernet a un puerto configurado para LAN en el 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.

Instalación de los paquetes de dispositivos SD-WAN en los clientes

May 7, 2021

Después de haber preparado los paquetes del dispositivo y conectado el MCN, y los administradores del sitio de sucursal han conectado sus respectivos dispositivos cliente a la LAN y WAN, el siguiente paso es cargar y activar el paquete de dispositivos SD-WAN adecuado en cada cliente. El Asistente de administración de cambios le guía a través de este proceso.

Para instalar y activar el software y la configuración en un dispositivo cliente, haga lo siguiente:

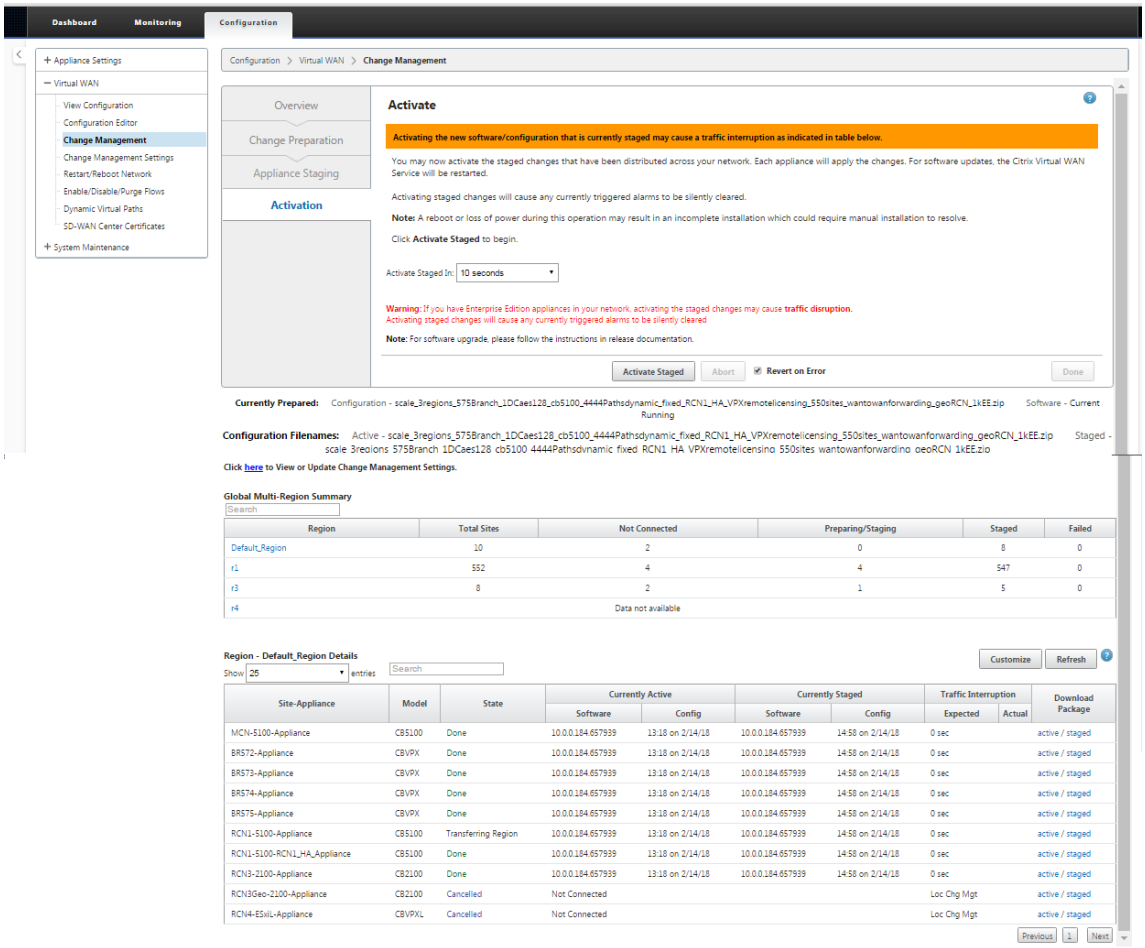
1. En un equipo conectado, abra un explorador e inicie sesión en la Interfaz Web de administración del dispositivo MCN.

   Introduzca la dirección IP de administración del MCN en el campo de dirección del explorador. Muestra la página **Panel** de Interfaz Web de Gestión para el dispositivo MCN.

2. Seleccione la ficha **Configuración**. En el panel de navegación de la izquierda, seleccione **WAN virtual** y, a continuación, seleccione **Administración de cambios**.

   Muestra la página **Resumen del proceso de los cambios** (la primera página del asistente **Gestión de cambios**).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



En la parte inferior de esta página, puede ver una tabla con los sitios y dispositivos individuales. En el extremo derecho de la tabla en la columna **Descargar paquete**, hay vínculos para los paquetes de dispositivo **activos** (si los hay) y **preconfigurados**.

> **Nota**
>
> Si se trata de una instalación inicial, los vínculos **activos** aún no están disponibles y se reemplazan por un marcador de texto sin formato **ninguno**.

3. Haga clic en el enlace en **etapas** del paquete que quiere descargar.

   En la tabla **Site-Appliance**, busque la entrada del dispositivo del sitio y haga clic en el vínculo En **etapas** de la columna **Descargar paquete** de dicha entrada. Aparece un explorador de archivos para seleccionar la ubicación de descarga (en el PC local).

4. Seleccione la ubicación de descarga y haga clic en **Aceptar.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. (Opcional.) Una vez completada la descarga, cierre la sesión de la interfaz web de administración de MCN.
6. Abra un explorador e introduzca la dirección IP del cliente al que quiere cargar el archivo.zip del paquete del dispositivo.

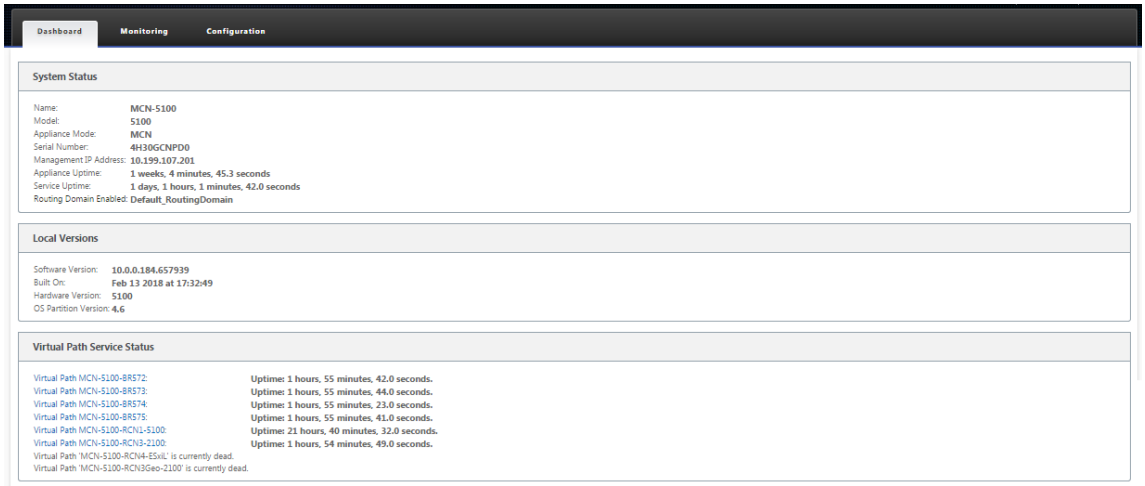
   > **Nota**
   >
   > Ignore cualquier advertencia de certificado de explorador para la Interfaz Web de administración.

   Esto abre la pantalla de inicio de sesión de Citrix SD-WAN Management Web Interface en el dispositivo cliente.

7. Introduzca el nombre de usuario y la contraseña del administrador y haga clic en **Iniciar sesión**. El nombre de usuario Administrador predeterminado es *admin*. La contraseña predeterminada es *contraseña*.

   Muestra la página **Panel** de Interfaz Web de administración para el dispositivo cliente.

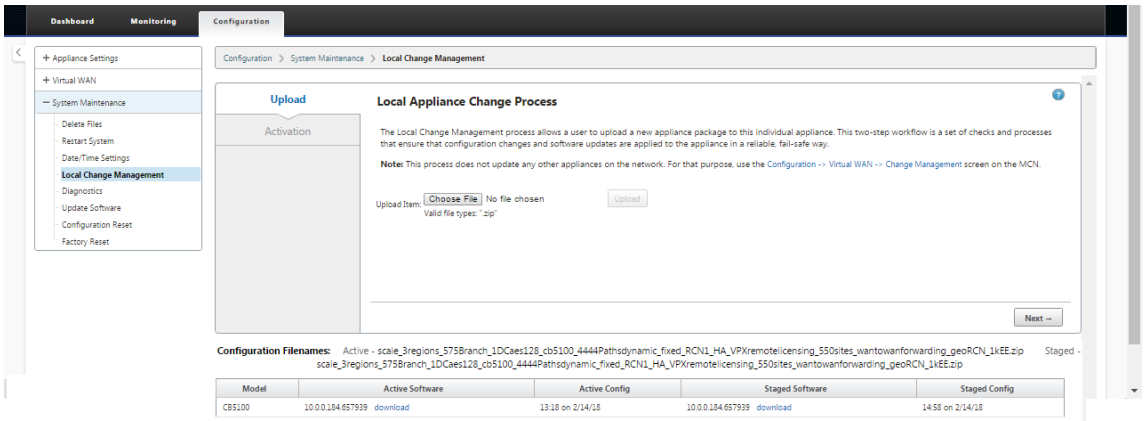
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Si se trata de una instalación inicial o si ha desactivado temporalmente el servicio WAN virtual en este dispositivo, puede ver un icono de alerta de auditoría de vara dorada con un mensaje de estado que indica que el servicio WAN virtual está inactivo o inhabilitado. Puede ignorar esta alerta por ahora. La alerta permanecerá en la página **Panel** de control hasta que inicie manualmente el servicio, después de completar la instalación.

8. Seleccione la ficha **Configuración**.
9. Abra la sucursal Mantenimiento del sistema en el árbol de navegación (panel izquierdo) y seleccione **Administración de cambios locales**.

   Aparecerá la página **Carga del proceso de cambio de dispositivo local** para cargar un paquete de dispositivo.



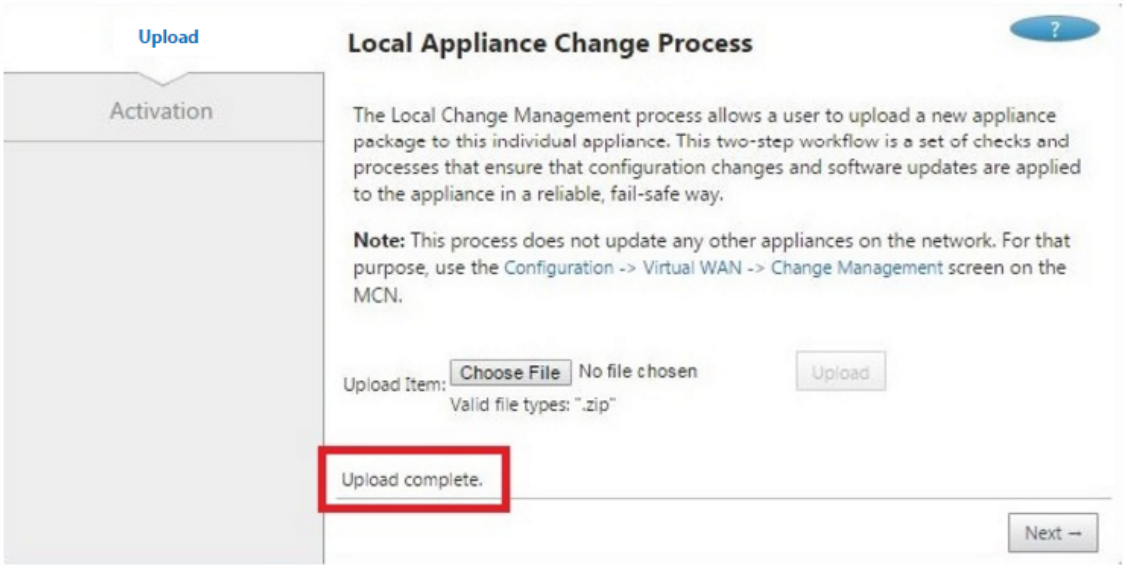
10. Haz clic en **Elegir archivo** junto a la etiqueta **Subir artículo**.

    Esto abre un explorador de archivos para seleccionar el paquete del dispositivo que quiere cargar al cliente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

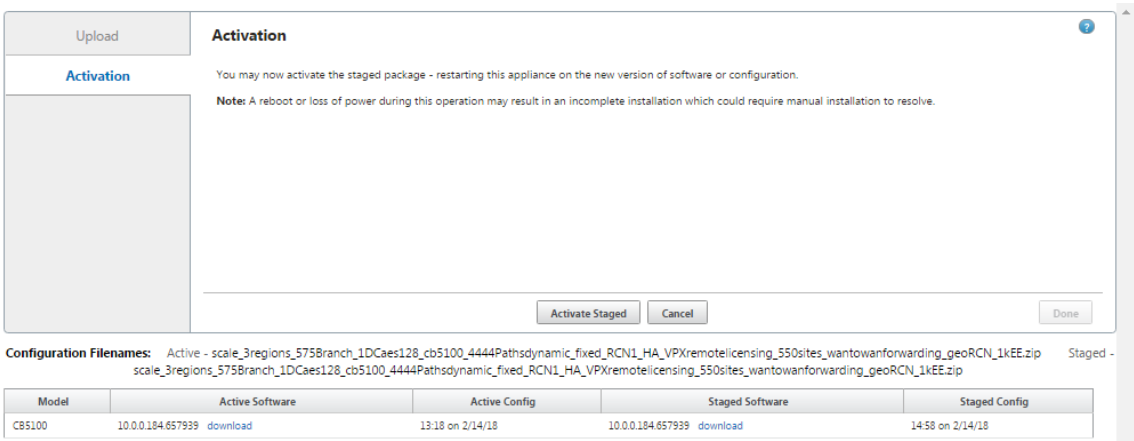
11. Desplácese hasta el archivo zip del paquete del dispositivo SD-WAN que acaba de descargar del MCN, selecciónelo y haga clic en **Aceptar**.
12. Haga clic en **Cargar**.

    El proceso de carga tarda unos segundos en completarse. Cuando se haya completado, aparece un mensaje de estado (en el centro izquierdo de la página) que indica **Subir completado.**



13. Haga clic en **Siguiente**.

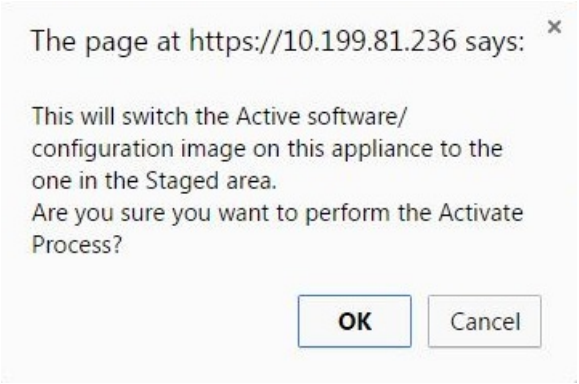
    Esto carga el paquete de software especificado y muestra la página **Activación** de administración de cambios locales.



14. Haga clic en **Activar por etapas**.

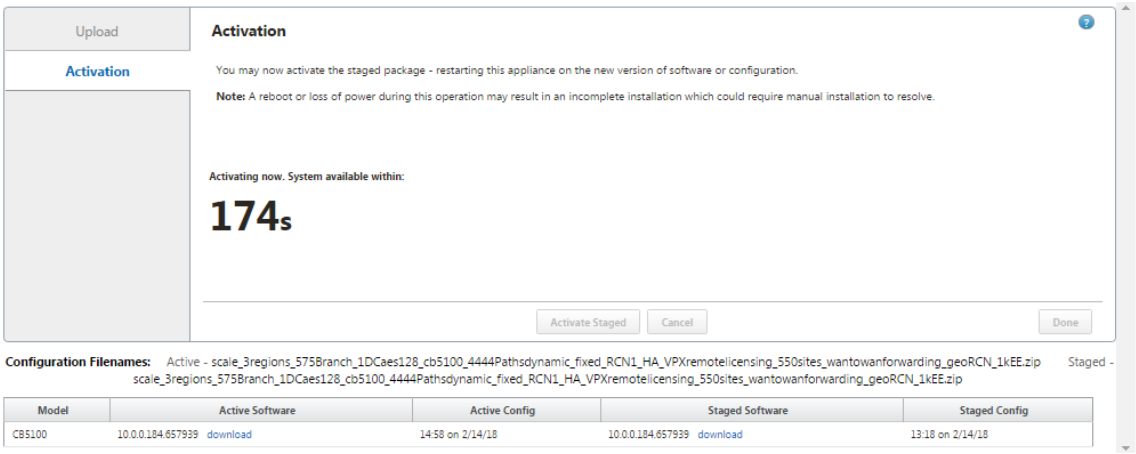
    Aparecerá un cuadro de diálogo en el que se le pedirá que confirme la operación de activación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

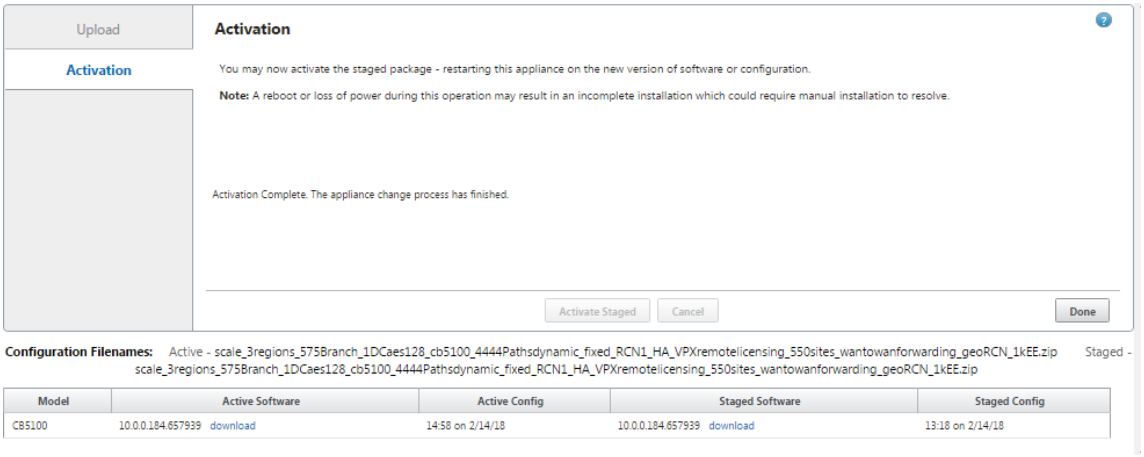


15. Haga clic en **OK**.

    Esto activa el paquete recién instalado y, si no se trata de una implementación inicial, inicia el servicio WAN virtual en el dispositivo cliente. Este proceso tarda varios segundos, durante los cuales se muestra un mensaje de estado de progreso.



    Cuando se complete la activación, aparece un mensaje de estado que indica **Activación completada**y el botón **Listo**estará disponible.



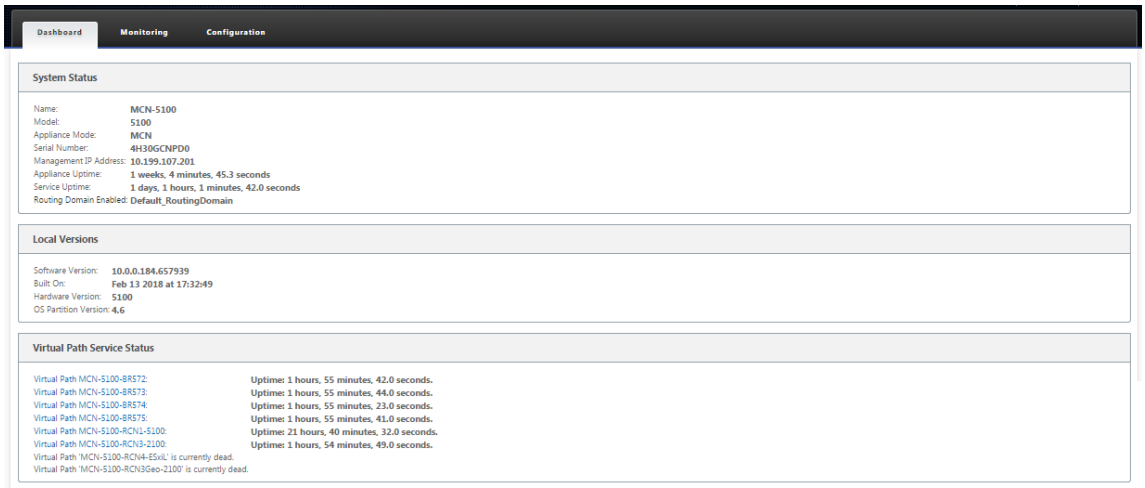
16. Haga clic en **Listo** para salir del asistente y ver los resultados de la activación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Una vez finalizada la activación, haga clic en **Listo** en la página **Activación** para volver a la página **Panel** de Interfaz Web de administración.

Si no se trata de una implementación inicial, esta página debería mostrar información actualizada para la versión activa del paquete de software, la partición del sistema operativo y el estado de la ruta virtual. Si se trata de una instalación inicial, aparecerá un icono de alerta de auditoría de vara dorada junto con un mensaje de estado que indica que el servicio WAN virtual está inactivo o inhabilitado. En este caso, debe habilitar manualmente el servicio, como se describe enHabilitación del servicio WAN virtual.

La siguiente figura muestra una página de **panel** de cliente de ejemplo que muestra el icono de alerta y el mensaje de estado.



El paso final para completar una implementación inicial de SD-WAN es habilitar el servicio WAN virtual. Las instrucciones se proporcionan en la sección.Habilitación del servicio WAN virtual

Implementaciones

May 7, 2021

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Creación de una red SD-WAN
- Redirección para segmentación LAN
- Utilización del dispositivo Premium (Enterprise) Edition para proporcionar únicamente servicios de optimización de WAN
- Modo de dos cajas
- Implementación de Zero Touch
- Implementación de una sola región
- Implementación en varias regiones
- Alta disponibilidad

Lista de comprobación y cómo llevas a cabo implementaciones

May 7, 2021

Para obtener información sobre los conceptos y directrices de Virtual WAN para planificar la implementación, consulte Guía de planificación de la implementación de Citrix Virtual WAN.

Prepararse para la implementación

En la siguiente lista se describen los pasos y procedimientos necesarios para implementar las ediciones SD-WAN Standard y Premium (Enterprise).

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 del túnel GRE
  - Rutas
  - VLAN
  - Ancho de banda en cada sitio para cada circuito

Prácticas recomendadas

January 10, 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 del enrutamiento 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 enrutamiento dinámico 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 sólo 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 enrutar, 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 el enrutamiento se gestiona en el perímetro, las posturas de seguridad como el cortafuegos, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 enrutamiento dinámico 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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** :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 el enrutamiento 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. Enrutamiento dinámico 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 inquierebles 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 inquierebles.
  - 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 el enrutamiento se ve influenciado hacia SD-WAN, los paquetes de superposición comienzan a bucle y provocan resultados no quieredos.
- 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 el enrutamiento dinámico, debe haber cuidado adecuadamente al administrar todas las subredes LAN, lo que de no ser así, podría causar problemas de redirección no quieredos.
- 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 enrutamiento 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).

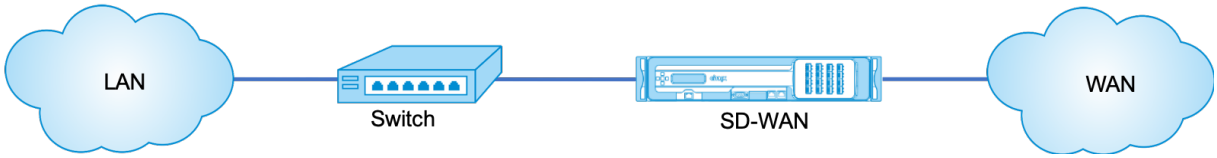
Modo de puerta de enlace

May 7, 2021

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:

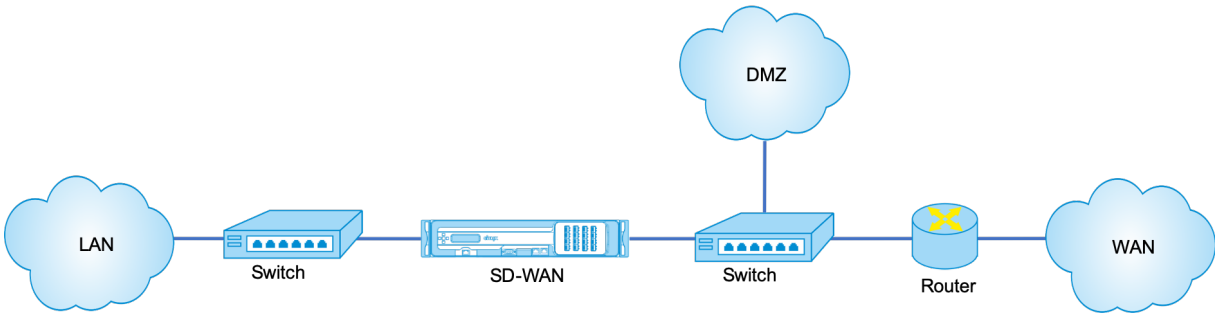
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



> **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.



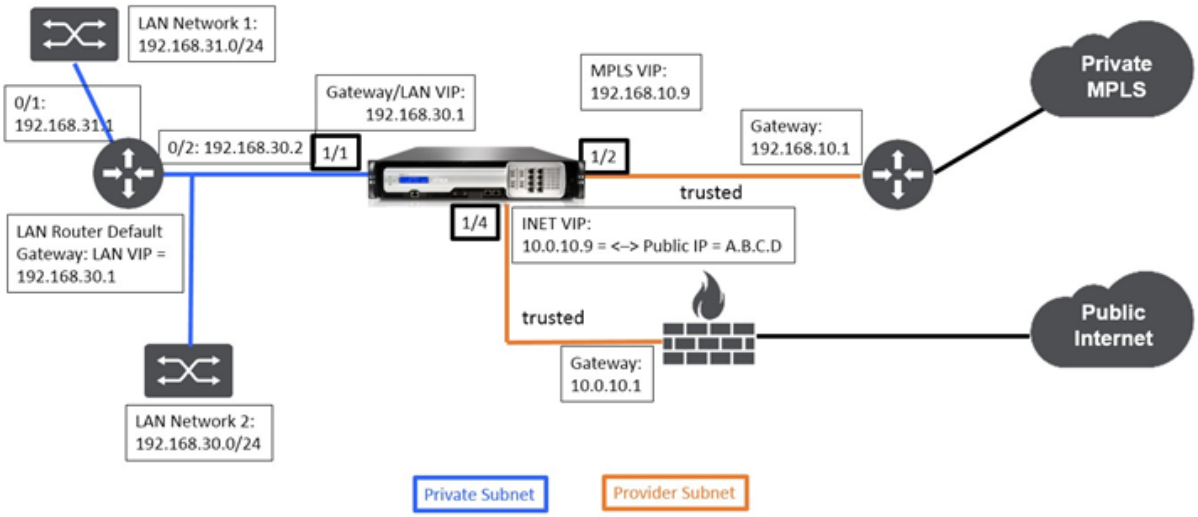
En este artículo se proporciona un procedimiento paso a paso para configurar un dispositivo SD-WAN en modo de puerta de enlace en una configuración de red de ejemplo. La implementación en línea también se describe para que el lado de la sucursal complete la configuración. Una red puede seguir funcionando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

Topología

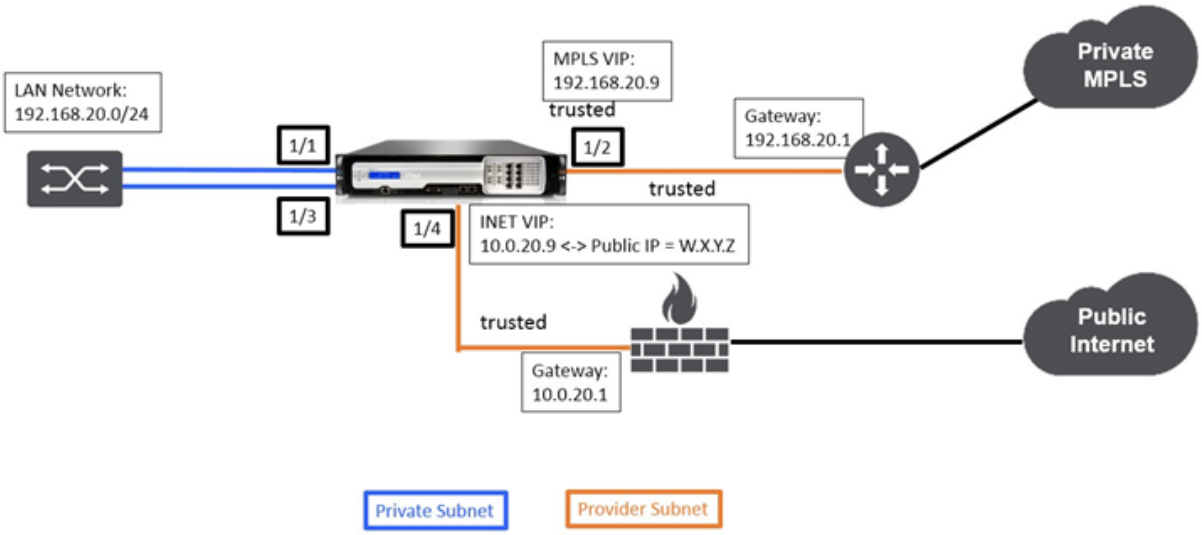
En las siguientes ilustraciones se describen las topologías admitidas en una red SD-WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Centro de datos en implementación de Gateway



Sucursal en implementación en línea



Requisitos de implementación

Los requisitos de implementación y la información relacionada se describen a continuación para ayudarle a crear la configuración.

Nombre del sitio	Sitio del centro de datos	Sitio de sucursal
Nombre del dispositivo	A_DC1	A_BR1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del sitio	Sitio del centro de datos	Sitio de sucursal
Gestión IP	172.30.2.10/24	172.30.2.20/24
Clave de seguridad	En caso de que haya	En caso de que haya
Modelo/Edición	4000	2000
Modo	Puerta de enlace	En línea
Topología	2 x Ruta WAN	2 x Ruta WAN
Dirección VIP	192.168.10.9/24 –MPLS, 10.0.10.9/24 –Internet (IP pública –A.B.C.D), 192.168.30.1/24 - LAN	192.168.20.9/24 - MPLS, 10.0.20.9/24 –Internet (IP pública –W.X.Y.Z)
MPLS de puerta de enlace	192.168.10.1	192.168.20.1
Puerta de enlace a Internet	10.0.10.1	10.0.20.1
Velocidad de enlace	MPLS: 100 Mbps, Internet: 20 Mbps	MPLS: 10 Mbps, Internet: 2 Mbps
Ruta	Dirección IP de red - 192.168.31.0/24, Tipo de servicio - Local, Dirección IP de puerta de enlace - 192.168.30.2	En caso de que haya
VLAN	En caso de que haya	En caso de que haya

Requisitos previos de configuración

- Habilite el dispositivo SD-WAN como nodo de control maestro.
- La configuración se realiza en el nodo principal de control (MCN) del dispositivo SD-WAN.

Para habilitar un dispositivo como nodo de control maestro:

1. En la interfaz de administración web de SD-WAN, vaya a **Configuración** > **Configuración del equipo** > **Interfaz de administrador** > **ficha Varios** > **Consola del conmutador**.

   > **Nota**
   >
   > Si aparece Switch to Client Console, el dispositivo ya está en modo MCN. Solo debe haber un MCN activo en una red SD-WAN.

2. Inicie Configuración navegando a **Configuración** > **Virtual WAN** > **Editor de configuración**. Haga clic en **Nuevo** para iniciar la configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

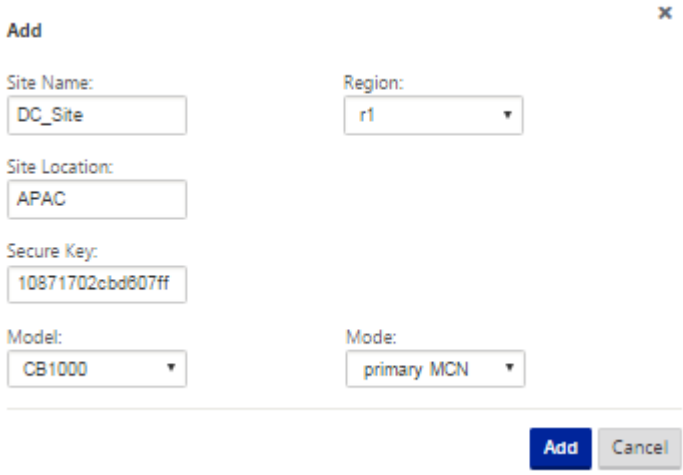
Configuración del modo de Gateway del sitio de

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

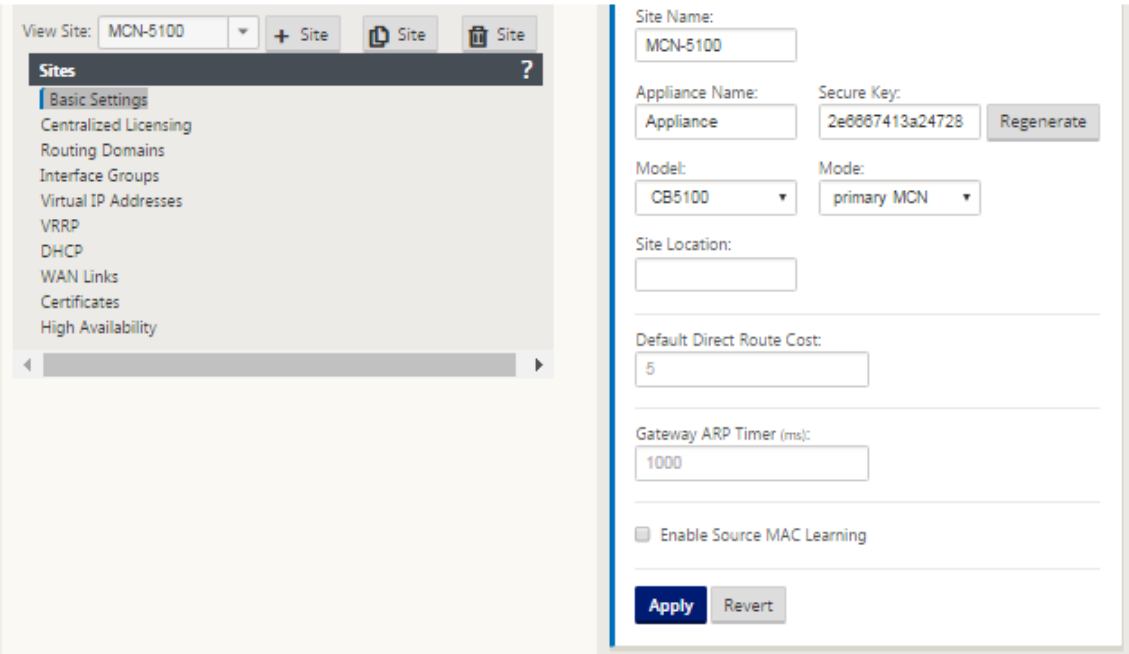
1. Cree un sitio de DC.
2. Rellene grupos de interfaces basados en interfaces Ethernet conectadas.
3. Crear dirección IP virtual para cada interfaz virtual.
4. Rellene los enlaces WAN en función de la velocidad física y no de las velocidades de ráfaga mediante Internet y MPLS Links.
5. Rellene rutas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

Para crear un sitio de DC

1. Desplácese hasta **Editor de configuración** - > **Sitios**y haga clic en el botón **+ Agregar**.
2. Rellene los campos como se muestra a continuación.
3. Mantenga la configuración predeterminada a menos que se le indique que cambie.



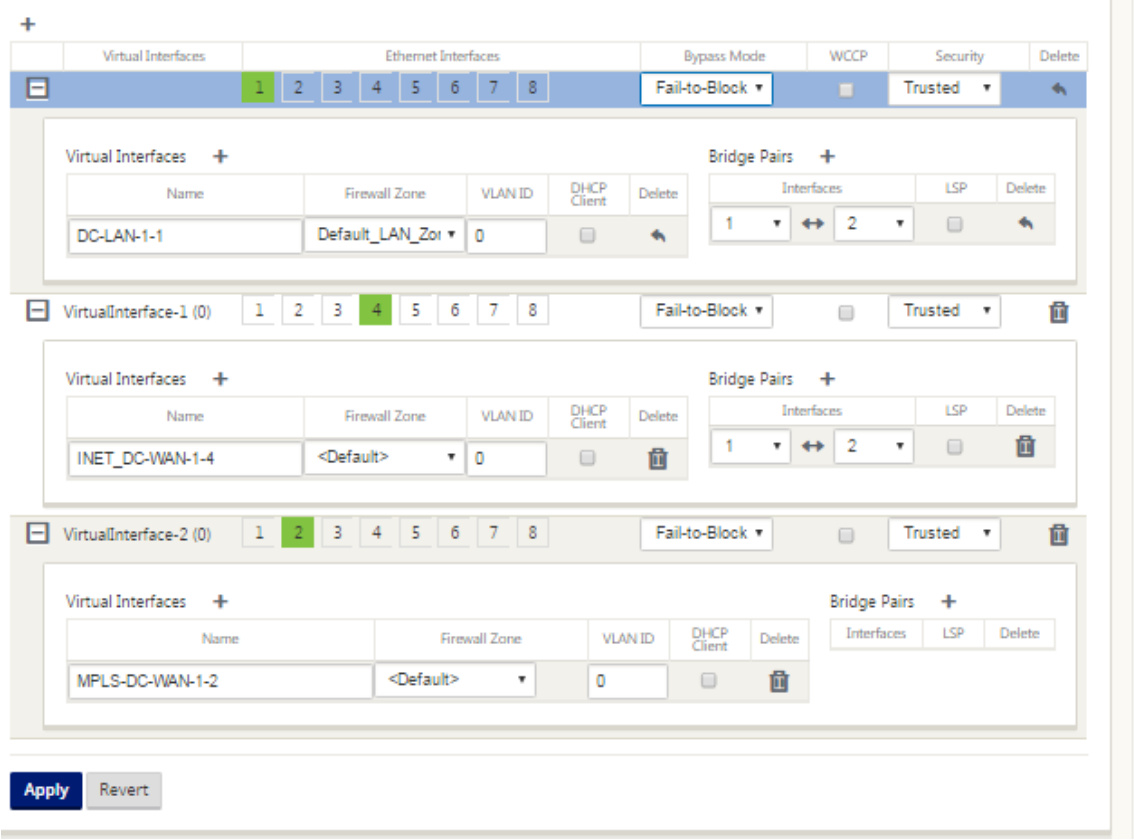
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para configurar grupos de interfaces basados en interfaces Ethernet conectadas

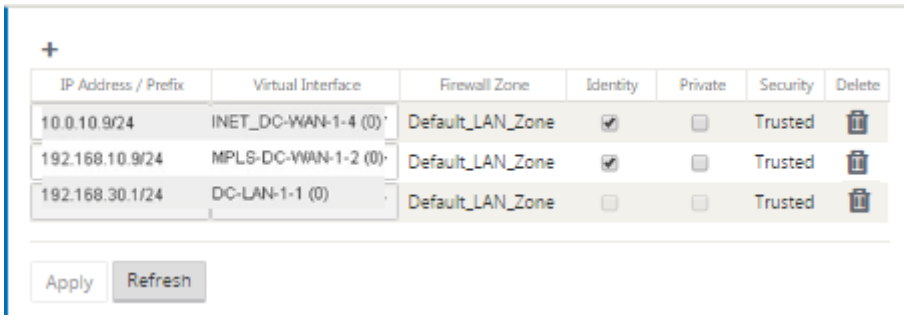
1. En el **Editor de configuración**, vaya a **Sitios** > **Ver sitio** > **[Nombre del sitio]** > **Grupos de interfaz**. Haga clic en **"+"** para agregar las interfaces que se van a utilizar. Para el modo de puerta de enlace, a cada grupo de interfaz se le asigna una única interfaz Ethernet.
2. El modo de omisión se establece en **error de bloqueo**, ya que sólo se utiliza una interfaz Ethernet/física por interfaz virtual. Tampoco hay pares de puentes.
3. En este ejemplo se crean tres grupos de interfaces, uno frente a la LAN y otros dos frente a cada enlace WAN respectivo. Consulte la topología de ejemplo "Modo de puerta de enlace de CC" anterior y rellene los campos Grupos de interfaz como se muestra a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

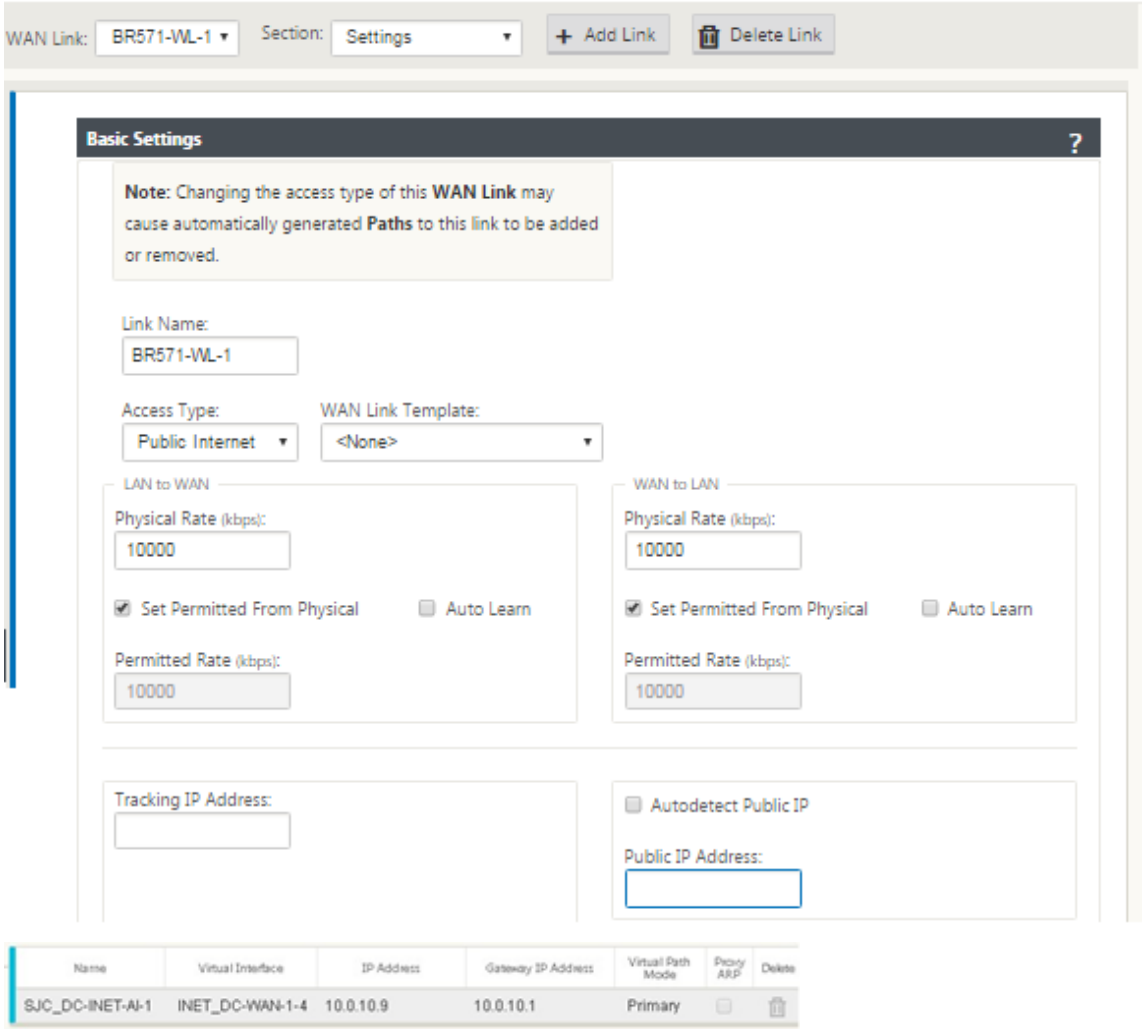


Para rellenar los vínculos WAN en función de la velocidad física y no de las velocidades de ráfaga mediante el enlace de Internet:

1. Navegue hasta **Vínculos WAN**, haga clic en **+ Botón Agregar Vínculo** para agregar un vínculo WAN para el vínculo de Internet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

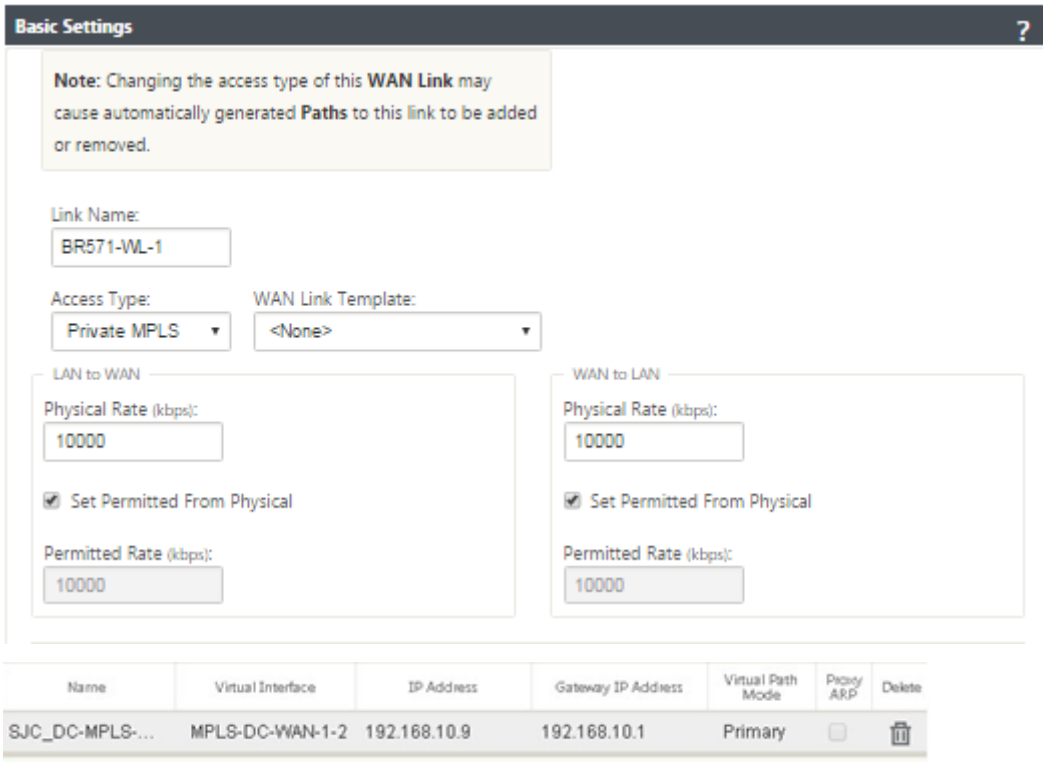


Para crear un vínculo MPLS

1. Vaya a **Vínculos WAN**, haga clic en el botón **+** para agregar un vínculo WAN para el vínculo 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 vínculo MPLS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

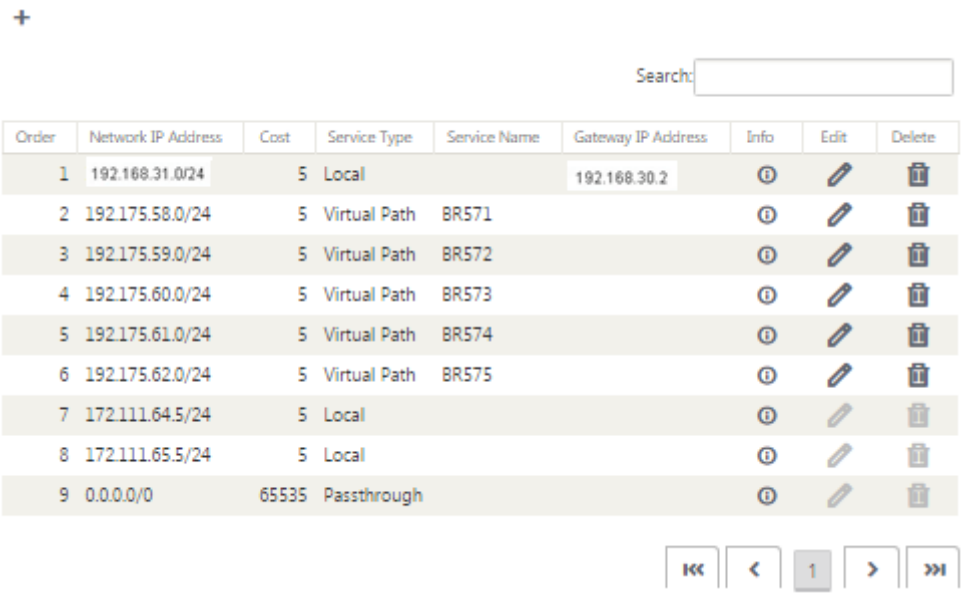
4. Rellene la interfaz de acceso para direcciones IP y Gateway como se muestra a continuación.



Para rellenar rutas

Las rutas se crean automáticamente en función de la configuración anterior. La topología de ejemplo LAN de CC 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración de implementación en línea del sitio de sucursal

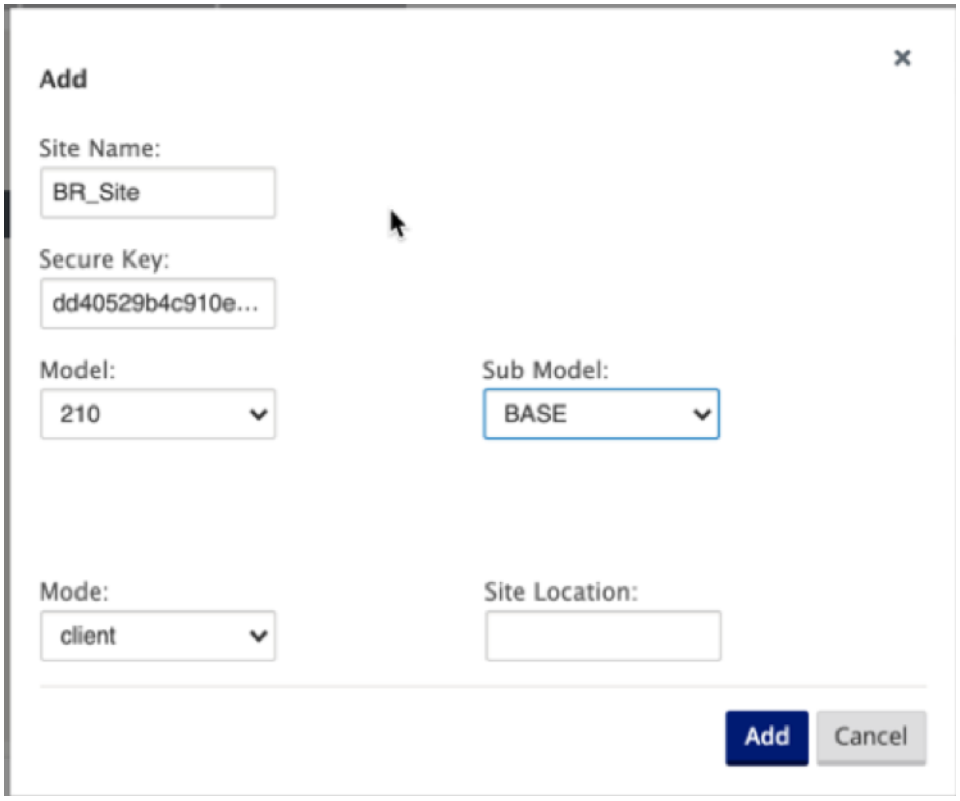
A continuación se presentan los pasos de configuración de alto nivel para configurar el sitio de sucursal para la implementación en línea:

1. Crear un sitio de sucursal.
2. Rellene grupos de interfaces basados en interfaces Ethernet conectadas.
3. Crear 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.

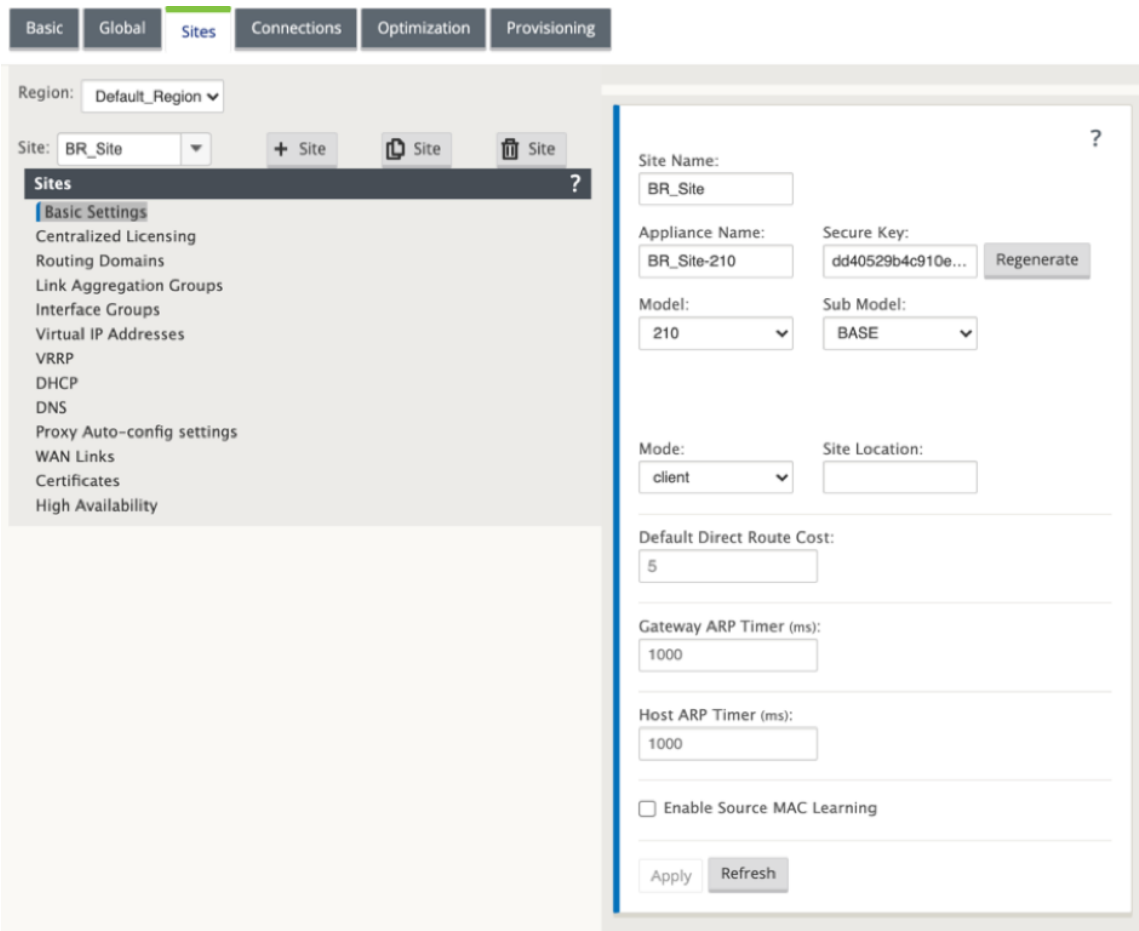
Para crear un sitio de sucursal

1. Desplácese hasta el **Editor de configuración** > **Sitios**y haga clic en el botón **+ Agregar**.
2. Rellene los campos como se muestra a continuación.
3. Mantenga la configuración predeterminada a menos que se le indique que cambie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



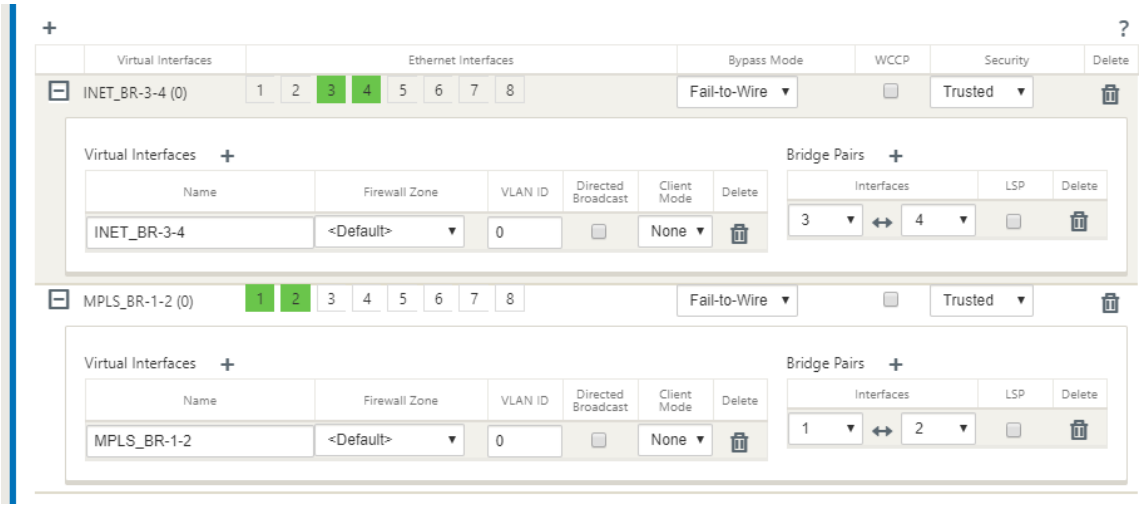
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para rellenar grupos de interfaces basados en interfaces Ethernet conectadas

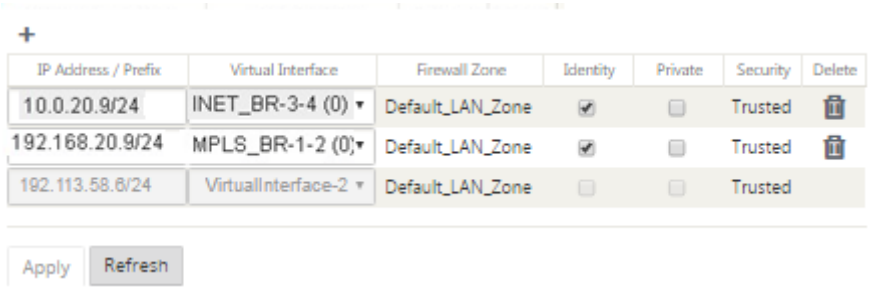
1. En el **Editor de configuración**, vaya a **Sitios** > **Ver sitio** > **[Nombre del sitio del cliente]** > **Grupos de interfaz**. Haga clic en **+** para agregar las interfaces que se van a utilizar. Para el modo en línea, a cada grupo de interfaz se le asignan dos interfaces Ethernet.
2. El modo de derivación se establece en **fallo a cable** y Bridge Pair se crea mediante las dos interfaces Ethernet.
3. Consulte la topología de ejemplo Modo en línea de sitio remoto anterior y rellene los campos Grupos de interfaz como se muestra a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

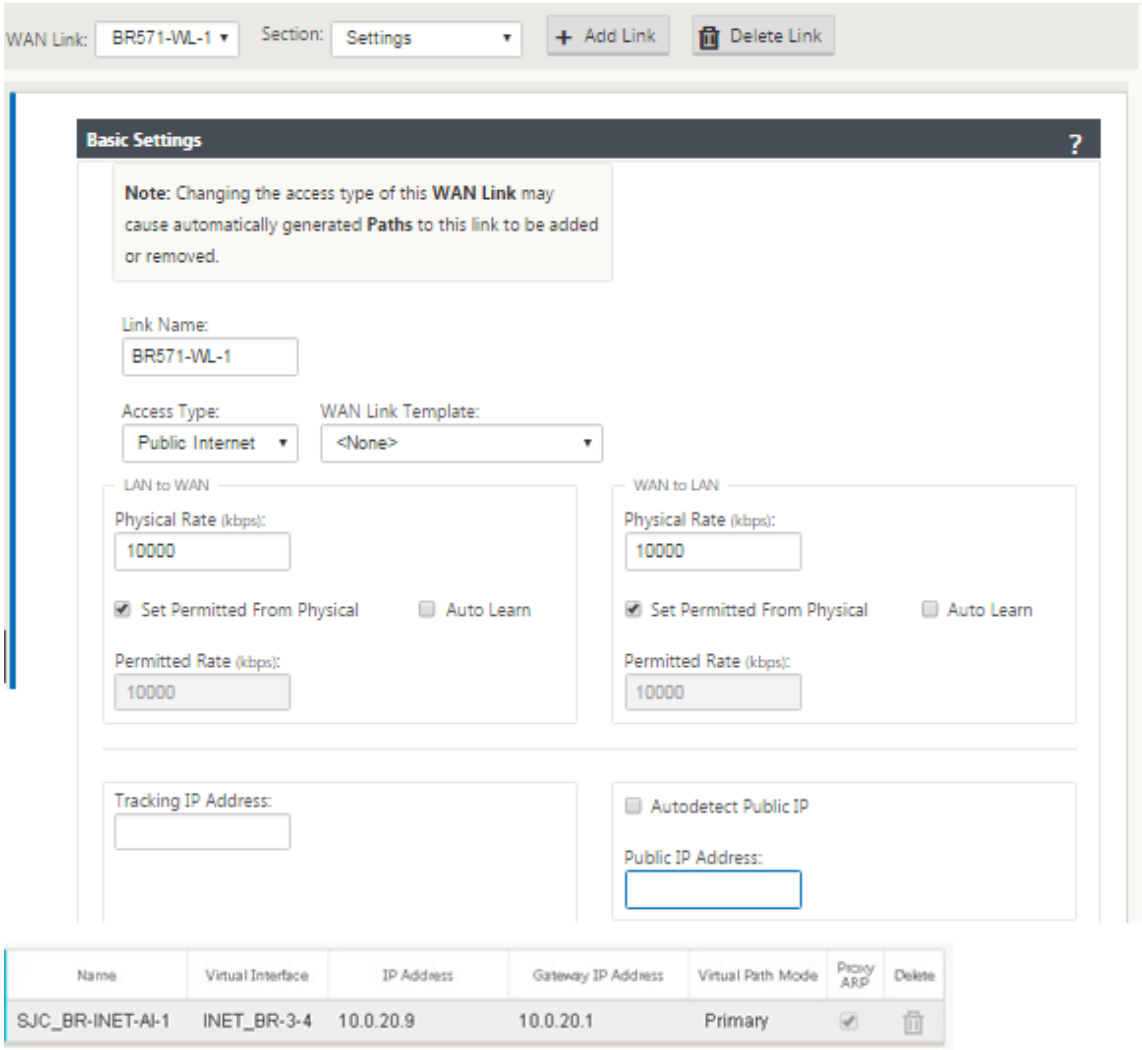
1. Cree una dirección IP virtual en la subred adecuada para cada enlace WAN. Los VIP se utilizan para la comunicación entre dos dispositivos SD-WAN en el entorno WAN virtual.



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 **Vínculos WAN**, haga clic en el botón **+** para agregar un vínculo 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.

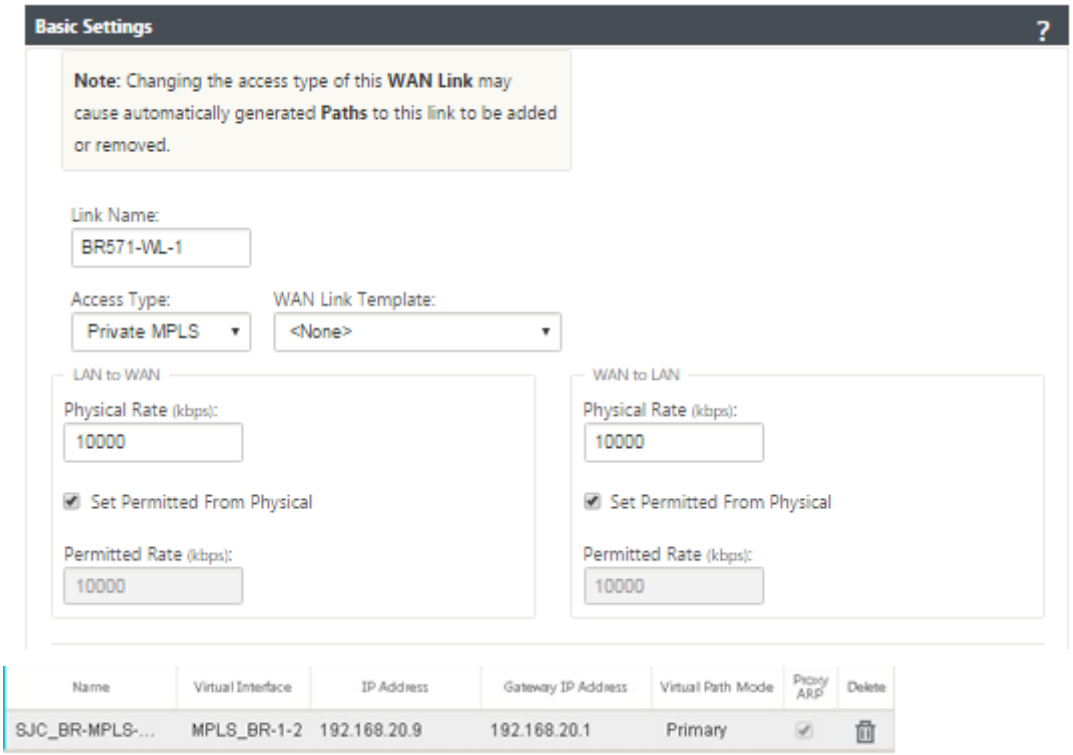
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para crear un vínculo MPLS

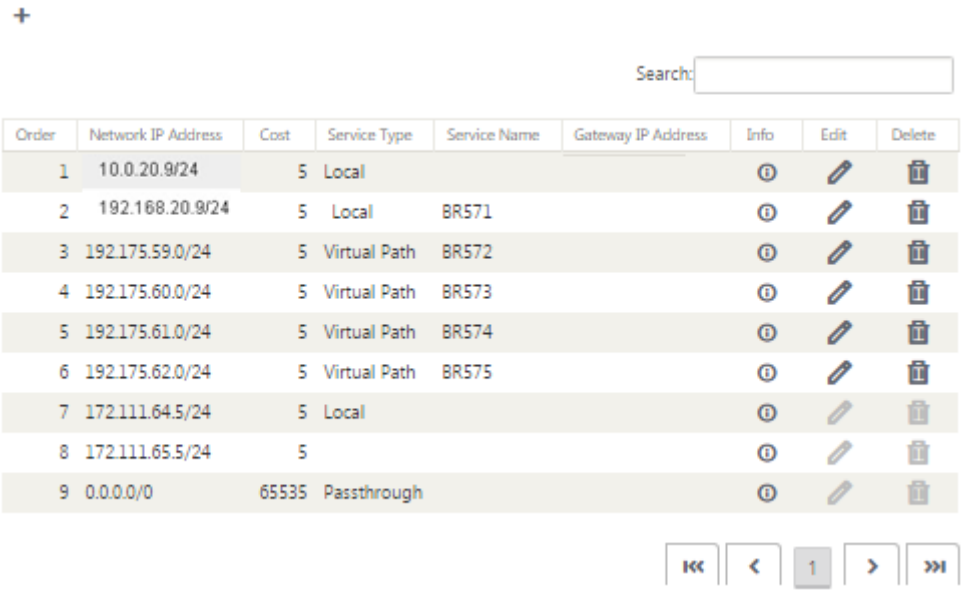
1. Vaya a Vínculos WAN, haga clic en el botón **+** para agregar un vínculo WAN para el vínculo MPLS.
2. Rellene los detalles del enlace MPLS como se muestra a continuación.
3. Vaya a Interfaces de Acceso, haga clic en el botón **+** para agregar detalles de interfaz específicos para el vínculo MPLS.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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

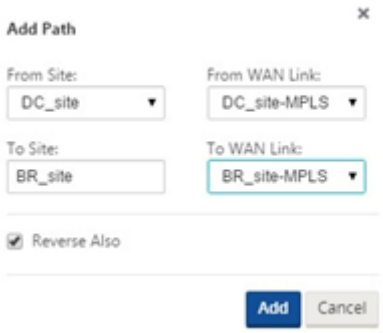


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Enlaces WAN definidos como el 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, proceda aPreparación de los paquetes del dispositivo SD-WAN.

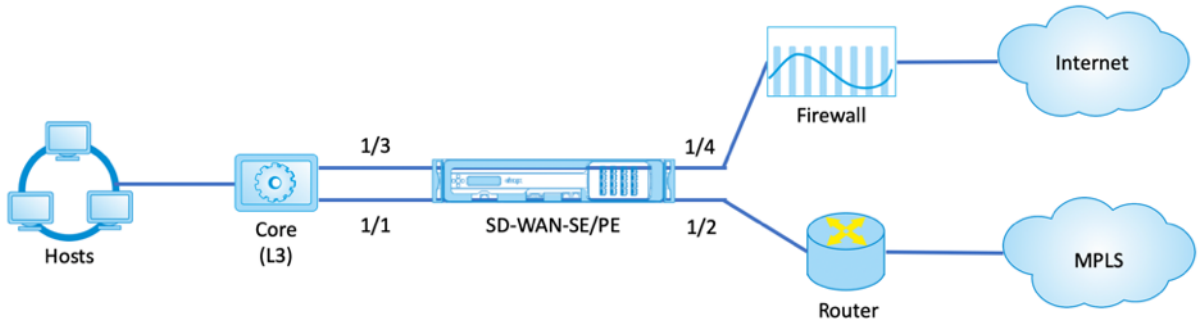
Modo en línea

May 7, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



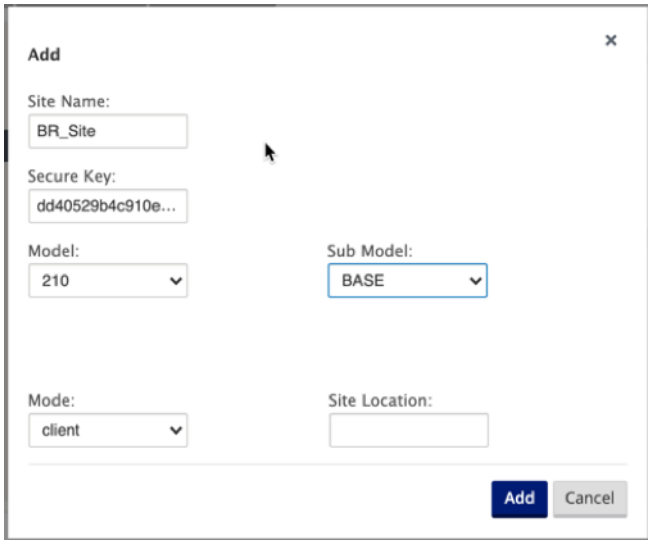
Configuración de implementación en línea del sitio de sucursal

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

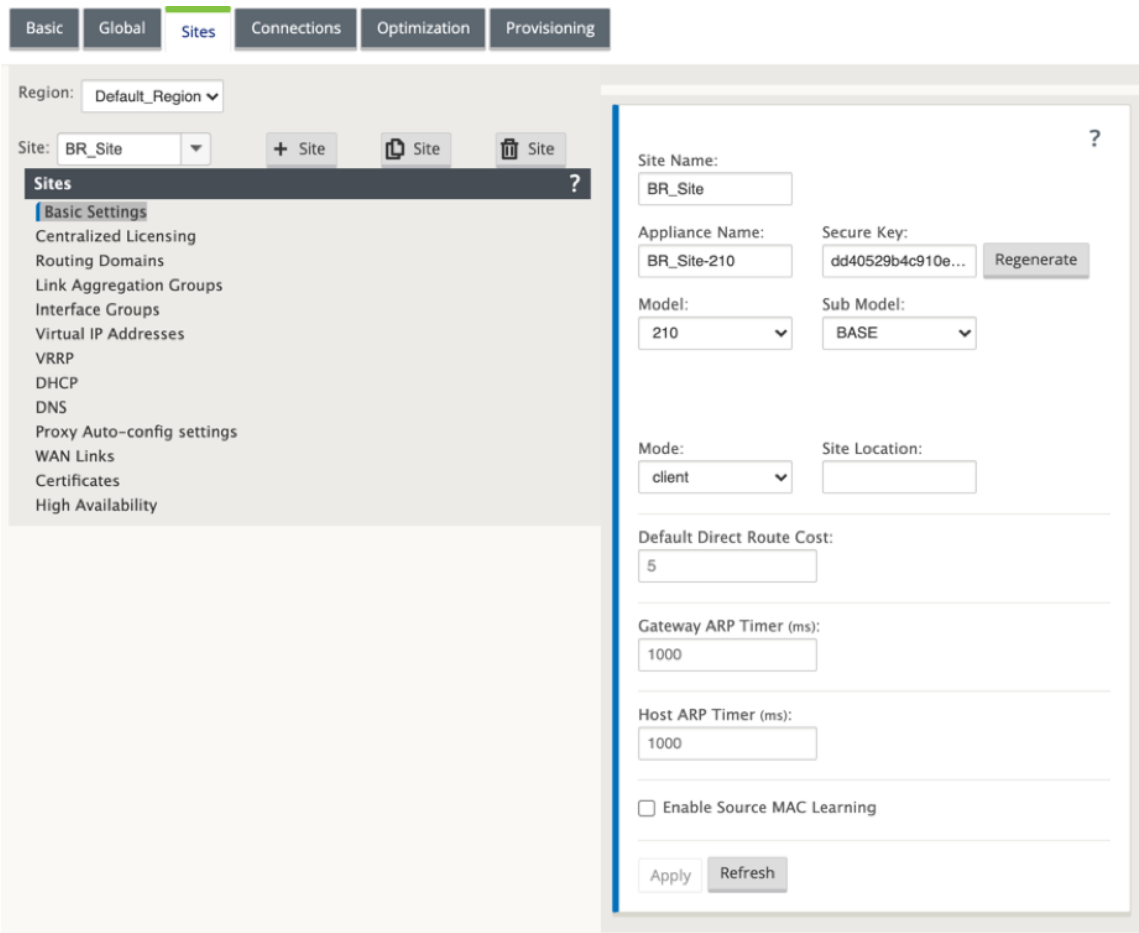
1. Crear un sitio de sucursal.
2. Rellene grupos de interfaces basados en interfaces Ethernet conectadas.
3. Crear dirección IP virtual para cada interfaz virtual.
4. Rellene los enlaces WAN en función de la velocidad física y no de las velocidades de ráfaga mediante Internet y MPLS Links.
5. Rellene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

Para crear un sitio de sucursal

1. Desplácese hasta el **Editor de configuración > Sitios**y haga clic en el botón **+ Agregar** .
2. Mantenga la configuración predeterminada a menos que se le indique que cambie.



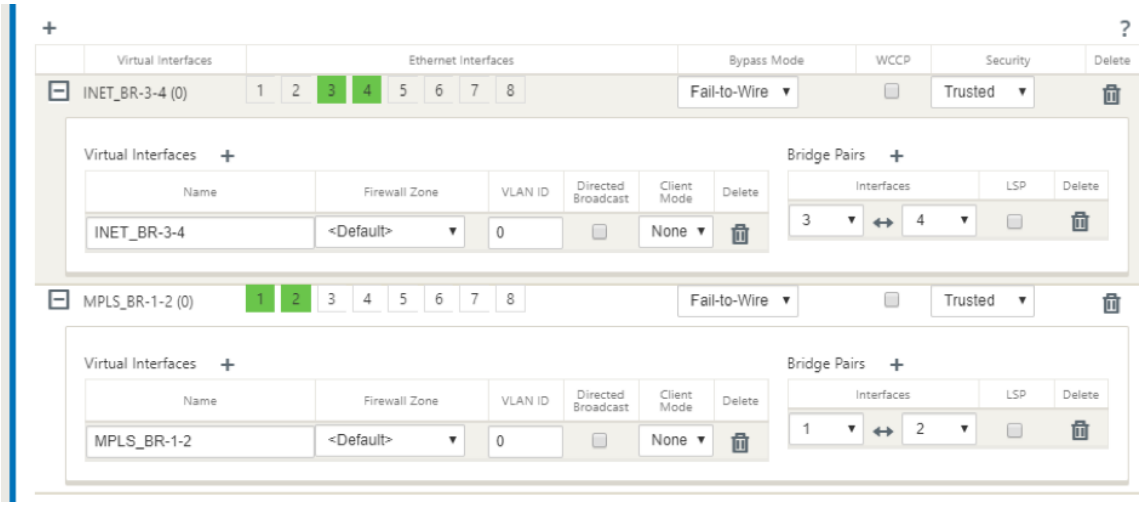
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para rellenar grupos de interfaces basados en interfaces Ethernet conectadas

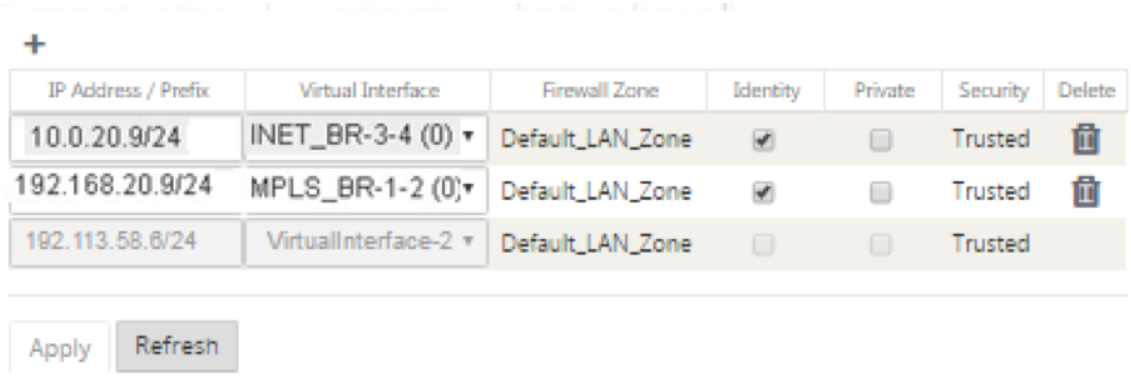
1. En el Editor de configuración, vaya a **Sitios > Ver sitio > [Nombre del sitio del cliente] > Grupos de interfaz**. Haga clic en **+** para agregar las interfaces que se van a utilizar. Para el modo en línea, a cada grupo de interfaz se le asignan dos interfaces Ethernet.
2. El modo de derivación se establece en **fallo a cable** y Bridge Pair se crea mediante las dos interfaces Ethernet.
3. Consulte la topología de ejemplo anterior y rellene los campos Grupos de interfaz como se muestra a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

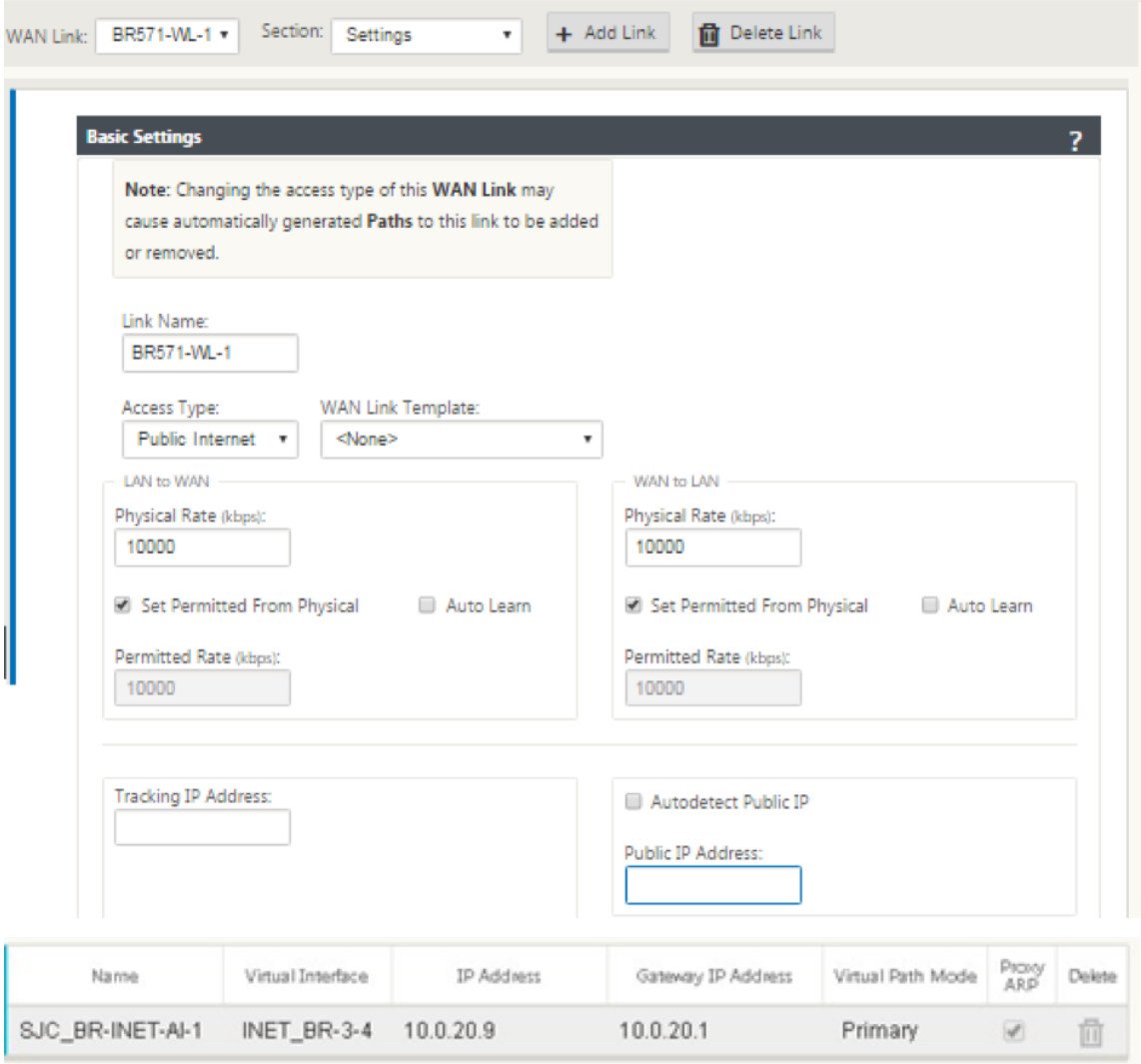
1. Cree una dirección IP virtual en la subred adecuada para cada enlace WAN. Los VIP se utilizan para la comunicación entre dos dispositivos SD-WAN en el entorno WAN virtual.



Para rellenar enlaces WAN basados en la velocidad física y no en las velocidades de ráfaga mediante vínculo de Internet

1. Vaya a **Vínculos WAN**, haga clic en el botón **+** para agregar un vínculo 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.

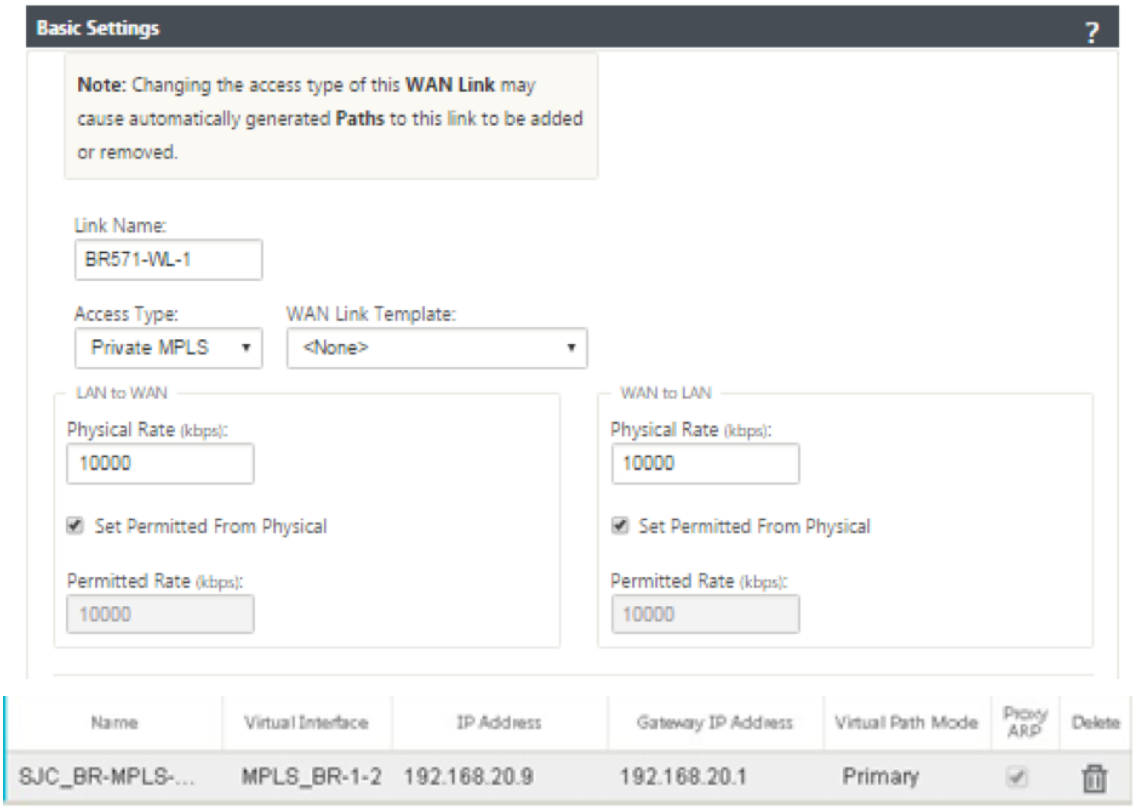
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para crear un vínculo MPLS

1. Vaya a **Vínculos WAN**, haga clic en el botón **+** para agregar un vínculo WAN para el vínculo 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 vínculo MPLS.
4. Rellene la interfaz de acceso para la dirección IP y la Gateway como se muestra a continuación.

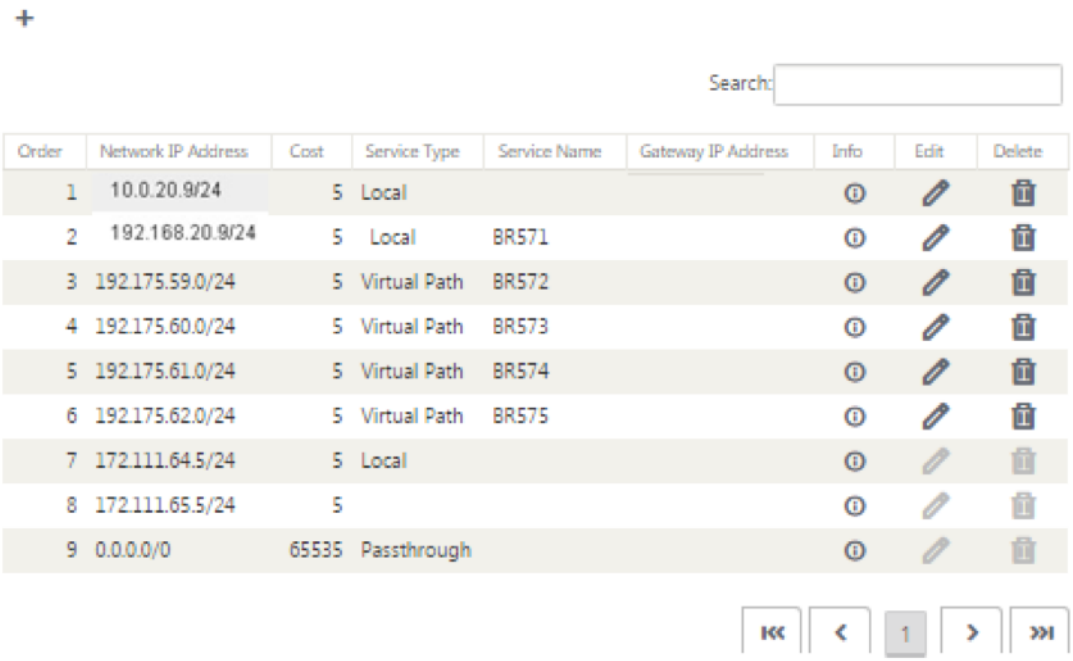
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Modo virtual en línea

October 27, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

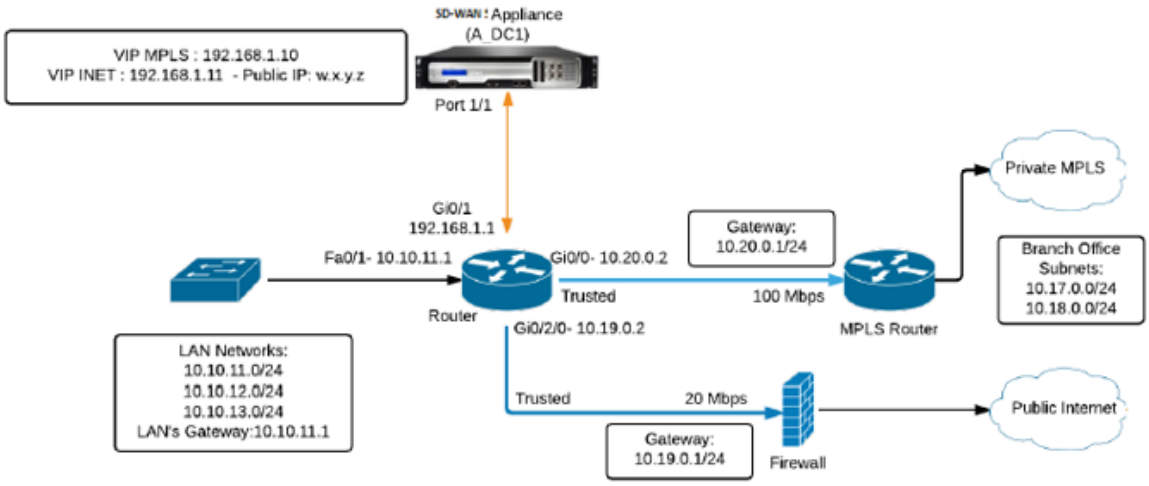
Recopilar información

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

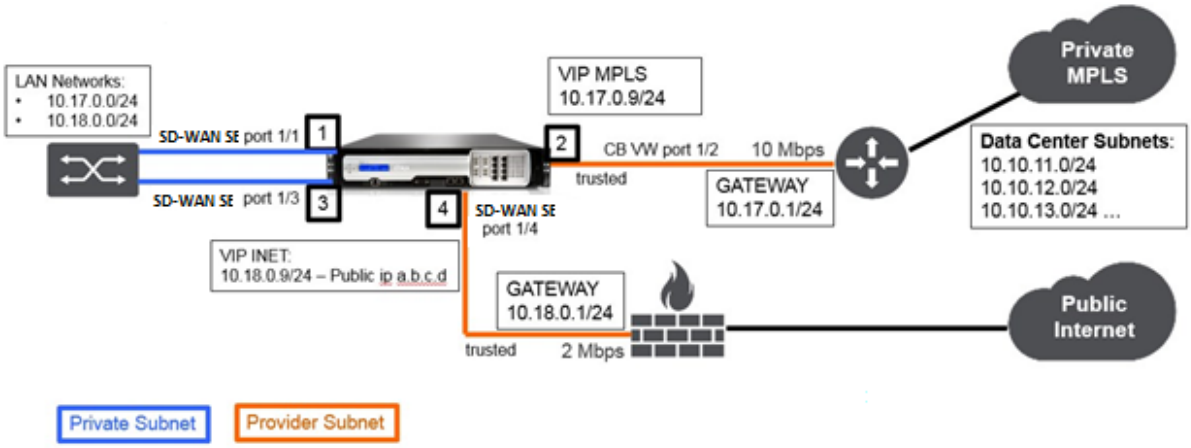
A continuación se muestra un diagrama de red y una tabla de implementación de ejemplo:

Topología del centro de datos: Modo en línea virtual



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Topología de bifurcación: Modo en línea



Nombre del sitio	Sitio del centro de datos	Sitio de sucursal
Nombre del dispositivo	SJC-DC	SJC-BR
Gestión IP	172.30.2.10/24	172.30.2.2.0/24
Llave de seguridad	En caso de que haya	En caso de que haya
Modelo/Modificación	4000	2000
Modo	Modo virtual en línea	En línea
Topología	2 x Ruta WAN	2 x Ruta WAN
Dirección VIP	192.168.1.10/24 —MPLS, 192.168.2.10/24 —Internet, IP pública w.x.y.z	10.17.0.9/24 - MPLS, 10.18.0.9/24: Internet, dirección IP pública a.b.c.d
MPLS de puerta de enlace	10.20.0.1	10.17.0.1
Puerta de enlace a Internet	10.19.0.1	10.18.0.1
Velocidad de enlace	MPLS: 100 Mbps, Internet: 20 Mbps	MPLS —10 Mbps, Internet —2 Mbps

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nombre del sitio	Sitio del centro de datos	Sitio de sucursal
Ruta	Necesita agregar una ruta en el dispositivo SD-WAN SE sobre cómo llegar a las subredes LAN (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc.) a través de cualquiera de las interfaces físicas: Gi0/1 - 192.168.1.1, **Configuration > Virtual WAN > Editor de configuración > SJC_DC\ > Rutas**. En este ejemplo se utilizó la interfaz 192.168.1.1: - n/w dirección: 10.10.13.0/24, 10.10.12.0/24, 10.10.11.0/24, - Tipo de servicio: Local, - Dirección IP de puerta de enlace: 192.168.1.1	No se agregaron rutas adicionales
VLAN	MPLS - VLAN 10, Internet - VLAN 20	Ninguno (valor predeterminado 0)

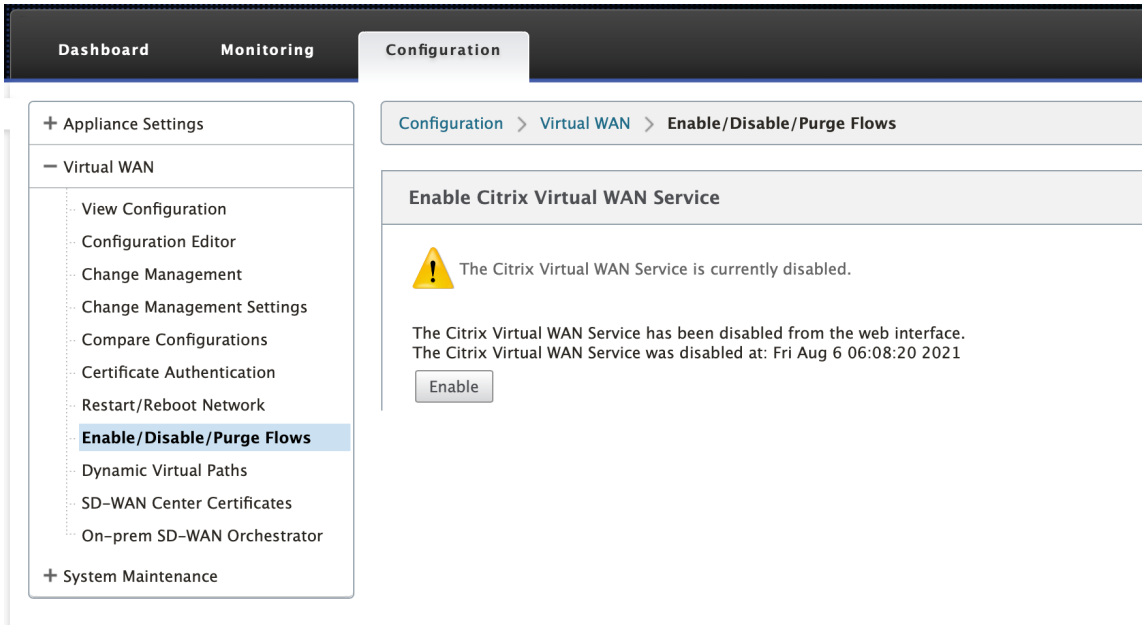
Requisitos previos

1. En la interfaz de administración web del dispositivo SD-WAN, vaya a **Configuración > Configuración del dispositivo > Interfaz de administrador > ficha Varios** y haga clic en **Consola del conmutador**.

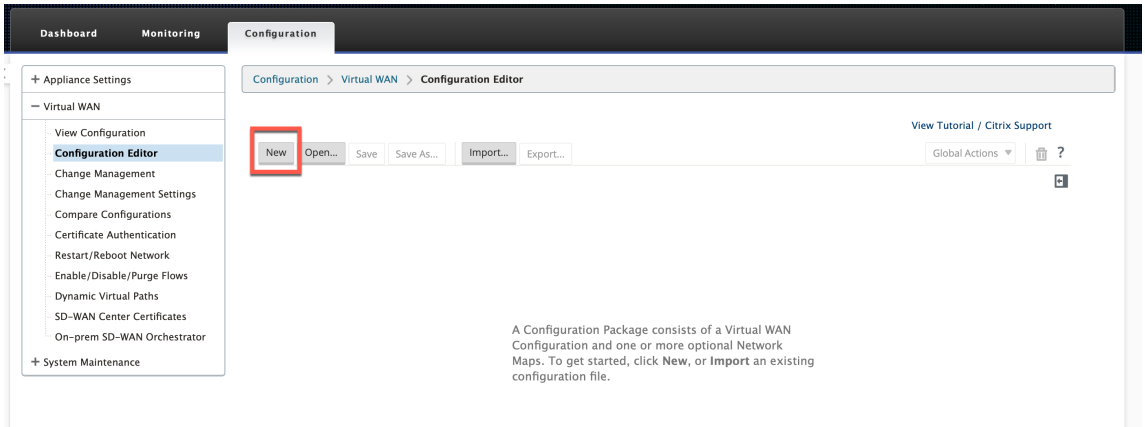
   > **Nota**
   >
   > Si aparece **Cambiar a consola cliente**, el dispositivo ya está en modo MCN. Solo debe tener un MCN activo en una red SD-WAN.

2. Vaya a **Configuración > WAN virtual > Habilitar/inhabilitar/purgar flujos** y haga clic en **Habilitar** en la sección **Habilitar servicio WAN virtual de Citrix**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Para iniciar la configuración, vaya a **Configuración > WAN virtual > Editor de configuración**. Haga clic en **Nuevo** para iniciar la configuración. Al hacer clic en **Nuevo** se crea un archivo de configuración inicial con **Untitled_1** como nombre de archivo. Puede cambiar el nombre [opcional] del archivo más adelante mediante el botón **Guardar como**.

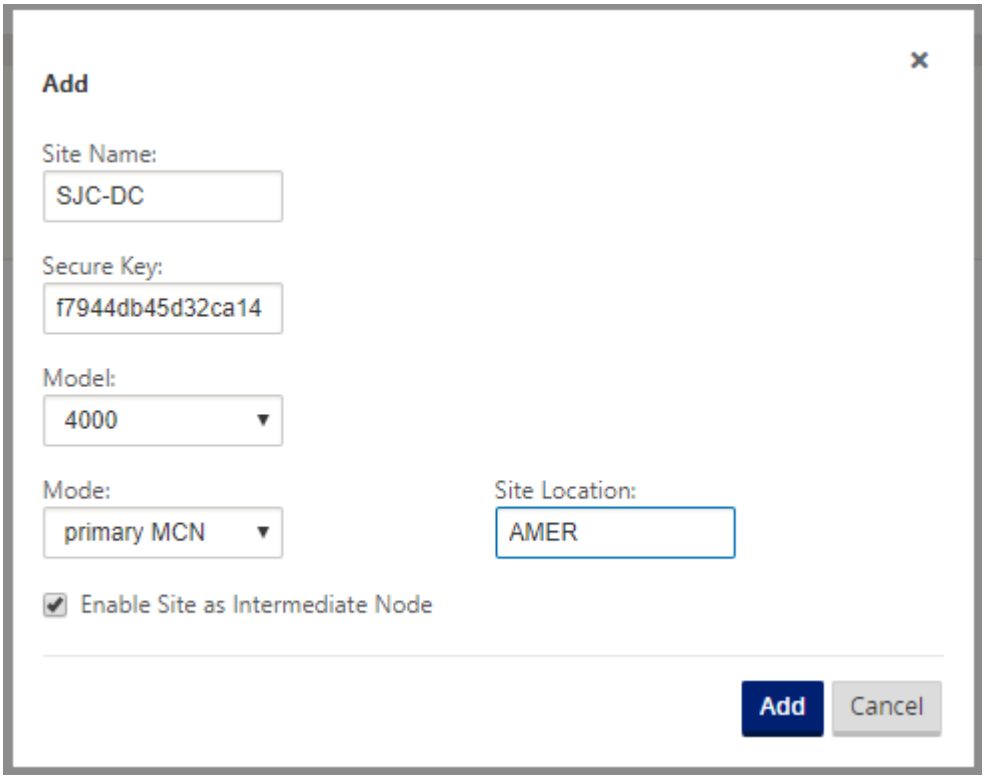


Sitio del centro de datos: configuración en modo virtual en línea

Creación de un sitio de centro de datos

1. Vaya a **Configuración > WAN virtual > Editor de configuración > Sitios** y haga clic en **+ Sitio**.
2. Introduzca el nombre y la ubicación del sitio. Elija el **modelo del equipo en la lista desplegable Modelo** y **MCN principal** en la lista desplegable **Modo**.
3. Haga clic en **Agregar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

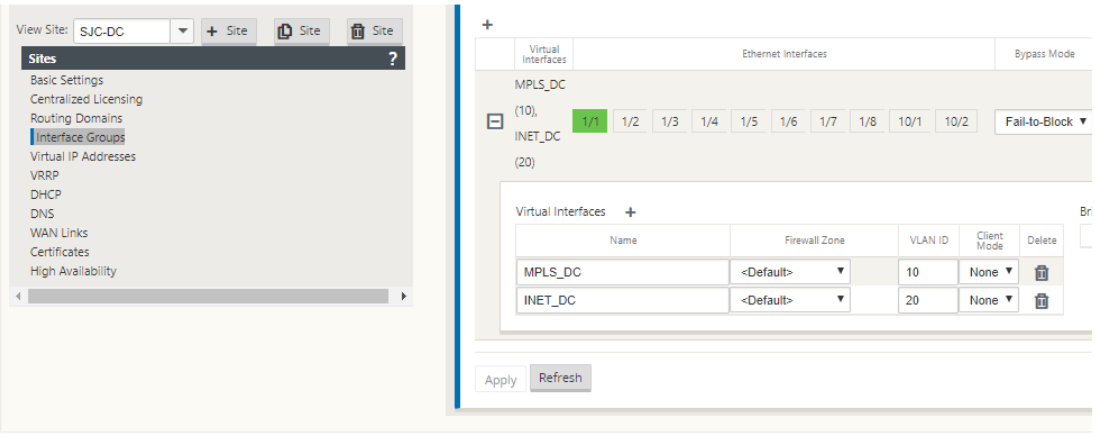


Configurar grupos de interfaces basados en interfaces Ethernet conectadas

En la configuración del modo virtual en línea, solo se utiliza una interfaz Ethernet, es decir, la interfaz que conecta el enrutador ascendente que proporciona implicaciones de directiva de redirección (Interfaz de ejemplo 1/5). El modo de derivación está configurado en Fail-to-Block (FTB), ya que solo se utiliza una interfaz Ethernet/física por interfaz virtual. Además, no hay pares de puentes.

1. En el **Editor de configuración**, vaya a **Sitios > [Nombre del sitio] > Grupos de interfaz**. Haga clic en **+** para agregar las interfaces que se van a utilizar.
2. Seleccione la interfaz Ethernet que se conecta al enrutador ascendente y haga clic en **+** junto a Interfaces virtuales. Agregue las interfaces virtuales para los vínculos MPLS e INTERNET. Según la topología de ejemplo, agregue lo siguiente:
   - Interfaz virtual **MPLS** configurada en **VLAN 10**
   - Interfaz virtual **INTERNET** configurada en **VLAN 20**
3. Seleccione **Fallo al bloquear** en **la lista desplegable Modo de omisión**. Haga clic en **Aplicar**.

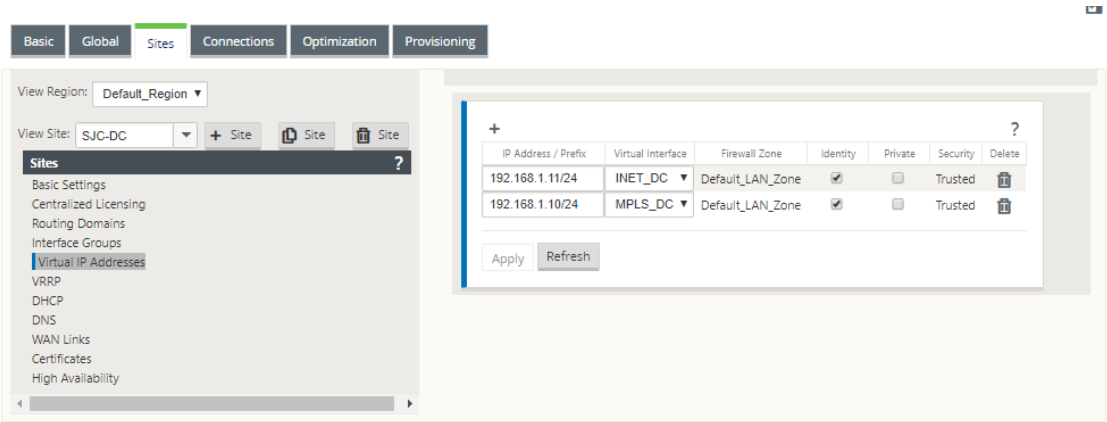
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Crear una dirección IP virtual para cada interfaz virtual

Cree una dirección IP virtual (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.

1. En el **Editor de configuración**, vaya a **Sitios >[Nombre del sitio] > Direcciones IP virtuales**. Haga clic en **+** para crear VIP.
2. Introduzca la dirección IP/prefijo y seleccione la interfaz virtual correspondiente para MPLS e Internet.
3. Haga clic en **Aplicar**.



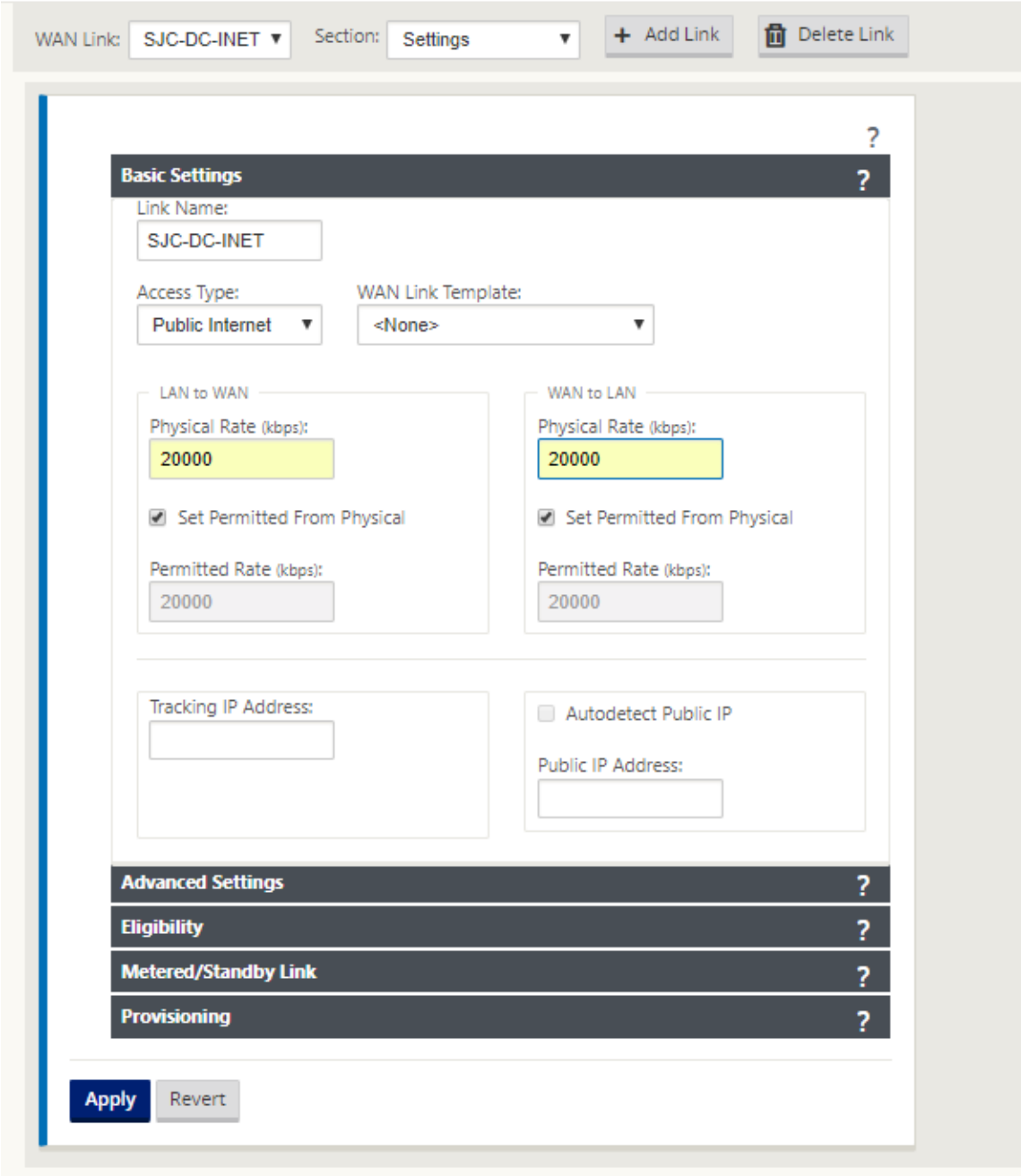
Crear enlace WAN de Internet

Cree un enlace WAN de Internet basado en la velocidad física y no en las velocidades de ráfaga.

1. En el **Editor de configuración**, vaya a **Sitios >[Nombre del sitio] > Vínculos WAN** y haga clic en **+ Enlace**. Introduzca un nombre y seleccione **Tipo de acceso** como **Internet público**. Haga clic en **Agregar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Introduzca la tarifa física. No marque la casilla **Detectar IP pública automáticamente**. Para el dispositivo SD-WAN configurado como MCN, no se puede seleccionar la casilla de verificación **Detectar IP pública automáticamente**.

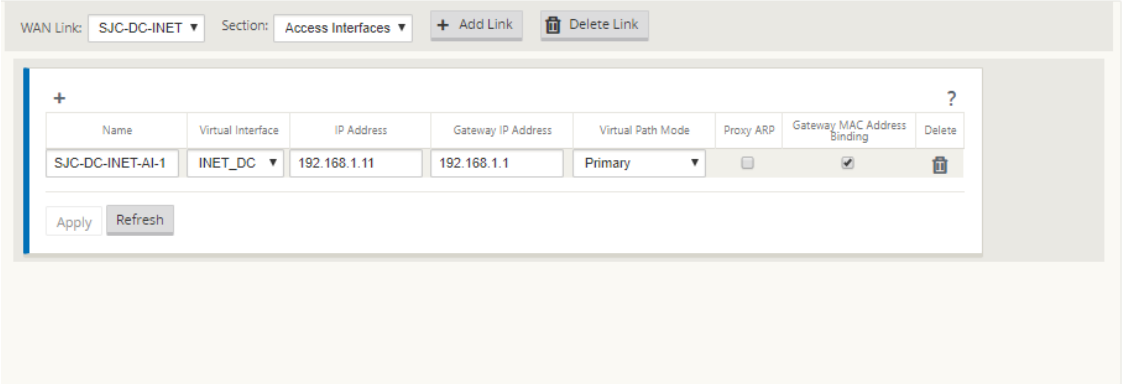


3. Seleccione **Interfaces de acceso** en la lista desplegable **Sección** y haga clic en el botón **+** para agregar detalles de interfaz específicos para el enlace de Internet.

4. Introduzca la dirección IP virtual y la dirección de puerta de enlace de Internet WAN. El ARP proxy no está comprobado para menos de dos interfaces Ethernet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

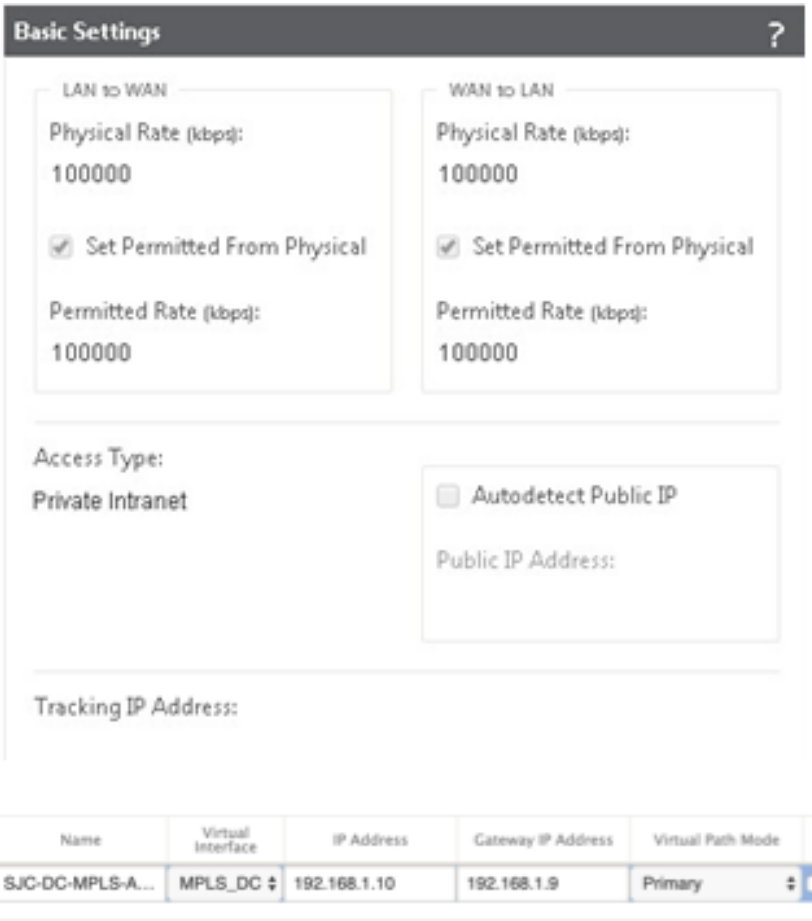
5. Haga clic en **Aplicar**.



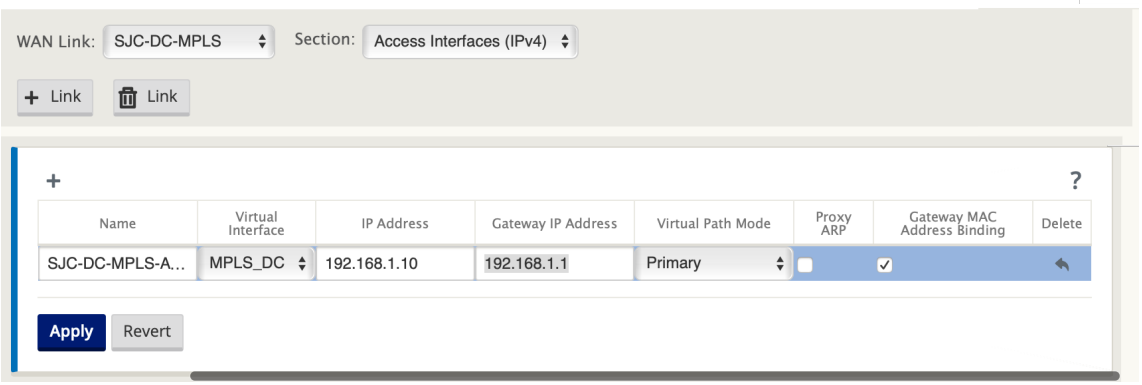
Crear enlace MPLS

1. En la página **Sitios > [Nombre del sitio] > Vínculos WAN**, seleccione **Configuración** en la lista desplegable **Sección**. Haga clic en el botón **+ Enlace** para agregar un enlace WAN para MPLS.
2. Introduzca el nombre del enlace WAN MPLS y seleccione **Tipo de acceso** como **intranet privada**. Haga clic en **Agregar**.
3. Introduzca la tarifa física y otros detalles. Haga clic en **Aplicar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Seleccione **Interfaces de acceso** en la lista desplegable **Sección** y haga clic en el botón **+** para agregar detalles de interfaz específicos del enlace MPLS.
5. Introduzca la dirección IP virtual de MPLS y la dirección de puerta de enlace. El ARP proxy no está comprobado para menos de dos interfaces Ethernet.
6. Haga clic en **Aplicar**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Rellenar rutas

En el lado del centro de datos, agregue una ruta en el dispositivo SD-WAN sobre cómo llegar a las subredes LAN (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc.) a través de cualquiera de las interfaces físicas.

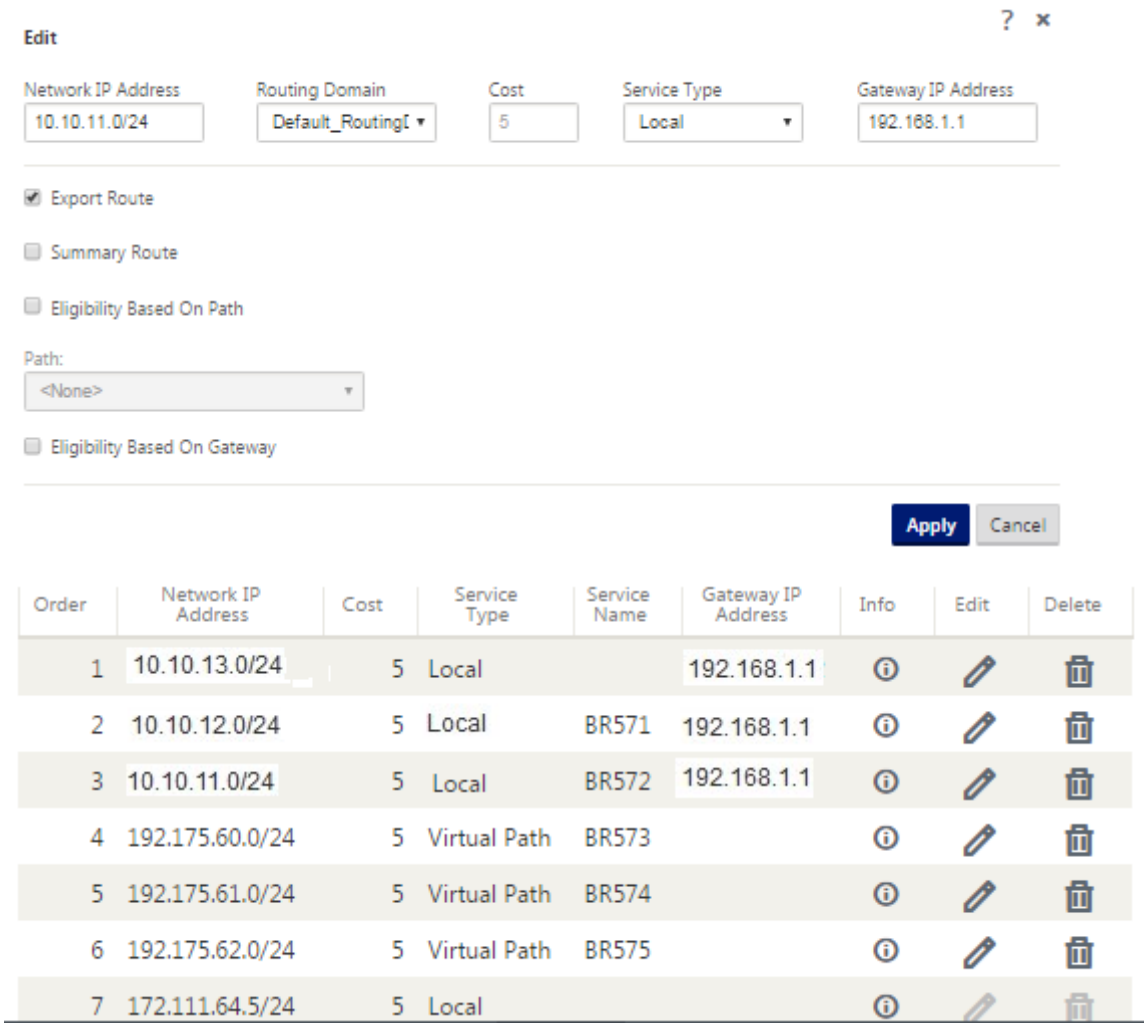
0/1/0.1: 192.168.1.1 en VLAN 10

0/1/0.2: 192.168.2.1 en VLAN 20

En este ejemplo, se utiliza la interfaz 192.168.1.1.

En el **Editor de configuración**, vaya a **Conexiones > Rutas** y haga clic en **+** para agregar las rutas.

Introduzca la **dirección IP de la red**, el **coste** y la **dirección de puerta de enlace**. Haga clic en **Agregar**.

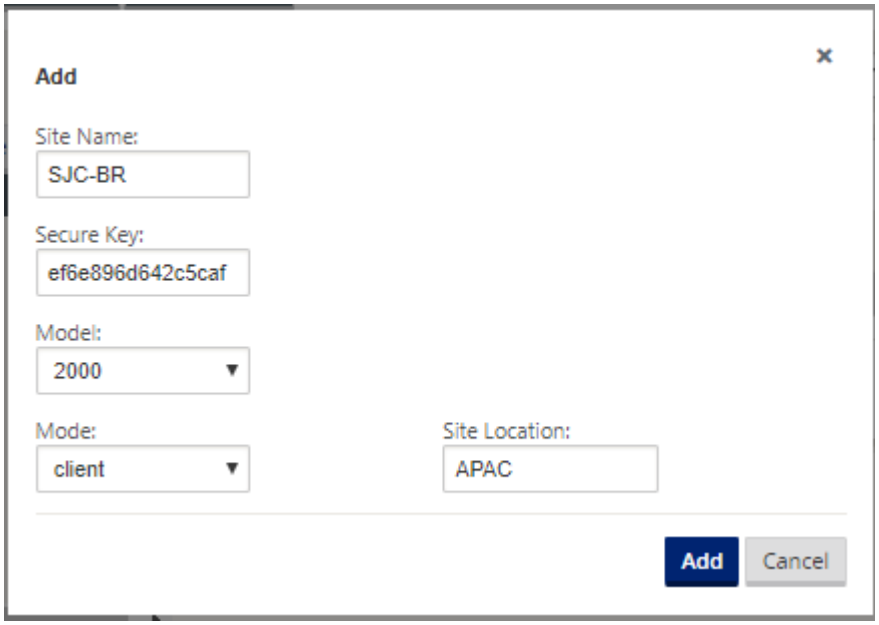


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración de implementación en línea del sitio de sucursal

Crear un sitio de sucursal

1. Vaya al **Editor de configuración > Sitios** y haga clic en **+ Sitio**.
2. Introduzca el nombre y la ubicación del sitio. Elija el modelo de dispositivo en la lista desplegable **Modelo** y **Cliente** en la lista desplegable **Modo**.
3. Haga clic en **Agregar**.



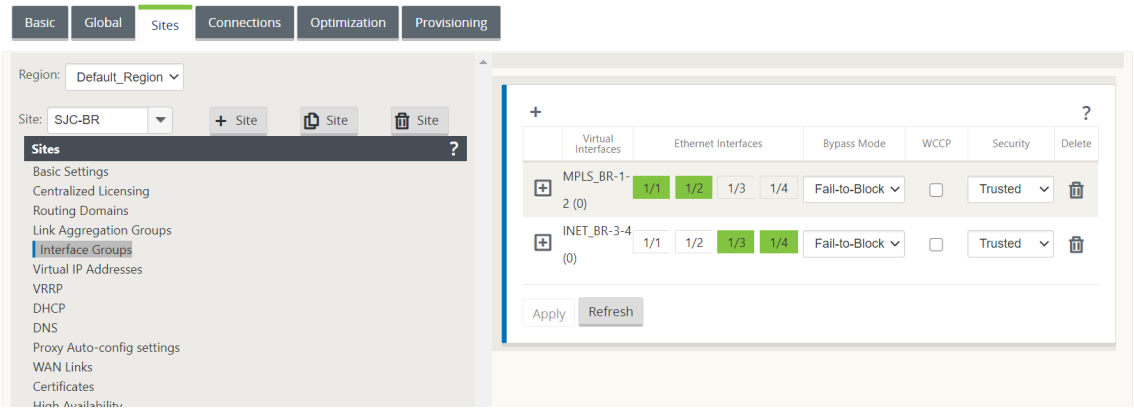
Configurar grupos de interfaces basados en interfaces Ethernet conectadas

1. En el **Editor de configuración**, vaya a **Sitios > [Nombre del sitio del cliente] > Grupos de interfaz**. Haga clic en **+** para agregar las interfaces que se van a utilizar. Para la configuración del modo en línea, se utilizan cuatro interfaces de Ethernet; par de interfaces 1/3, 1/4 y par de interfaces 1/1 y 1/2.
2. Establezca el **modo Bypass** en fail-to-wire, ya que se utilizan dos interfaces Ethernet/físicas por interfaz virtual. Hay dos pares de puentes.
3. Haga clic en **+** junto a **Interfaces virtuales** y rellene los vínculos WAN en función de la velocidad física y no de las velocidades de ráfaga mediante vínculos de Internet y MPLS.
   - Interfaz virtual **INTERNET** configurada en el par Bridge 1/3 y 1/4
   - Interfaz virtual **MPLS** configurada en Bridge Pair 1/1 y 1/2.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Haga clic en **+** junto a **Pares de puentes** y cree el par de puentes seleccionando las interfaces adecuadas.

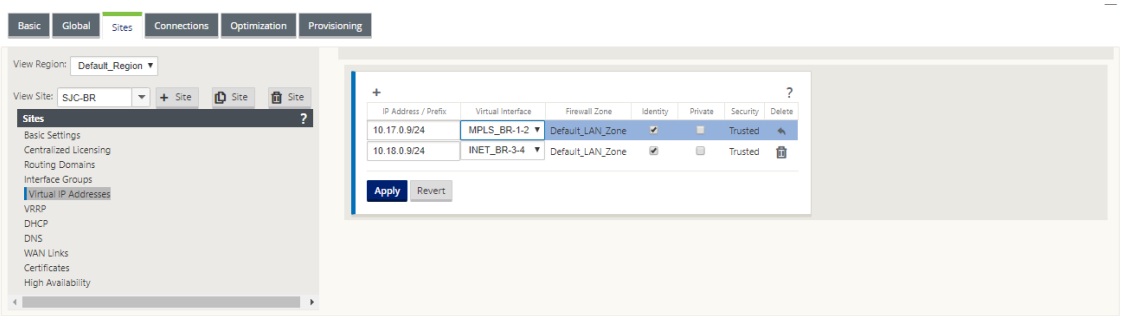
   Consulte el diagrama **topología de bifurcación: topología en modo en línea** en la sección Requisitos previos y rellene los Grupos de interfaces.



Crear dirección IP virtual (VIP) para cada interfaz virtual

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.

1. En el **Editor de configuración**, vaya a **Sitios >[Nombre del sitio] > Direcciones IP virtuales**. Haga clic en **+** para crear VIP.
2. Introduzca la dirección IP/prefijo y seleccione la interfaz virtual correspondiente para MPLS e Internet.
3. Haga clic en **Aplicar**.

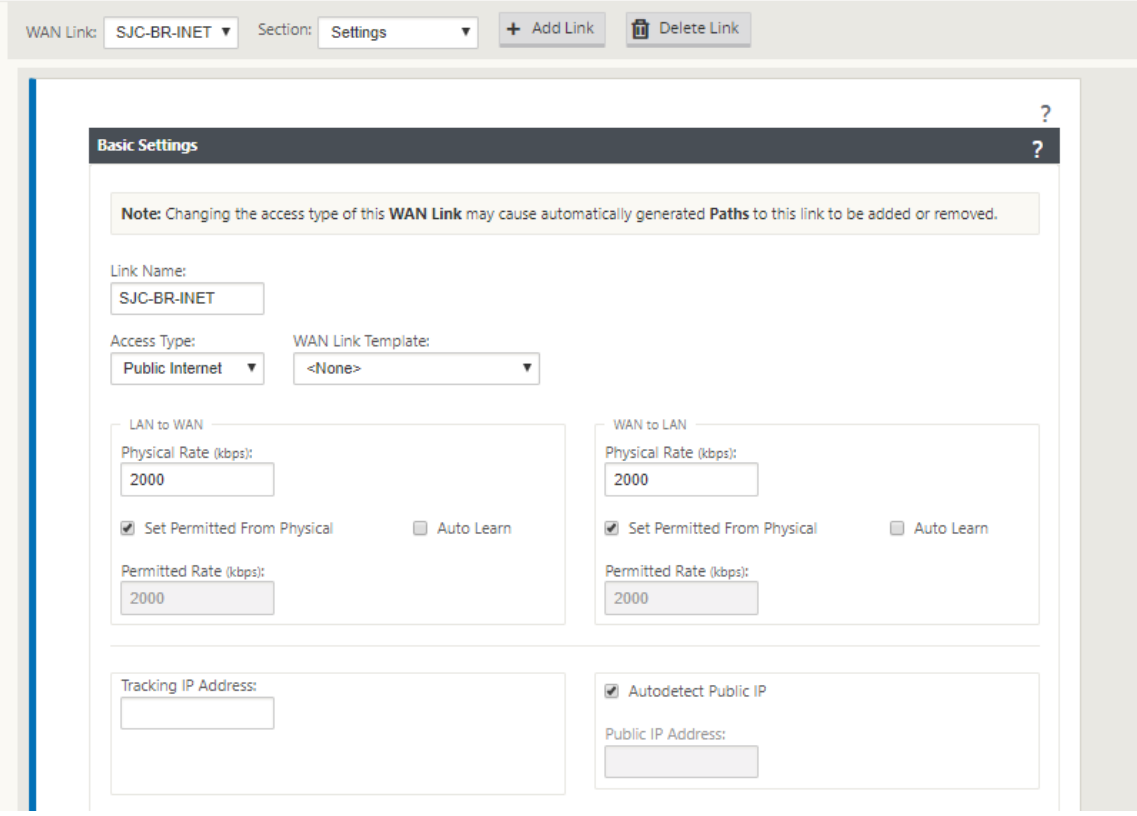


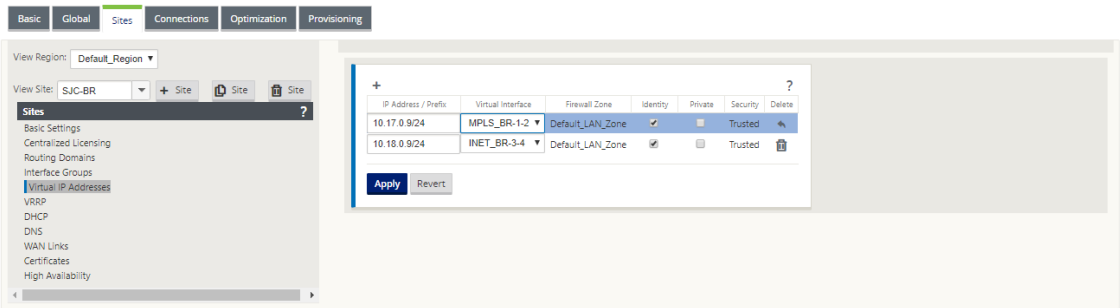
Crear enlace WAN de Internet

Para rellenar enlaces WAN basados en la velocidad física y no en las velocidades de ráfaga mediante vínculo de Internet

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Vaya a **Vínculos WAN**, haga clic en el botón **+ Enlace** para agregar un enlace WAN para el enlace de Internet. Introduzca un nombre y seleccione **Tipo de acceso** como **Internet público**. Haga clic en **Agregar**.
2. Rellene los detalles del vínculo de Internet y marque la casilla **Detectar automáticamente la dirección IP pública**.
3. Seleccione **Interfaces de acceso** en la lista desplegable **Sección** y haga clic en el signo **+** para agregar detalles de interfaz específicos para el enlace de Internet.
4. Introduzca la dirección IP virtual y la dirección de puerta de enlace de Internet WAN. El ARP proxy no está comprobado para menos de dos interfaces Ethernet.

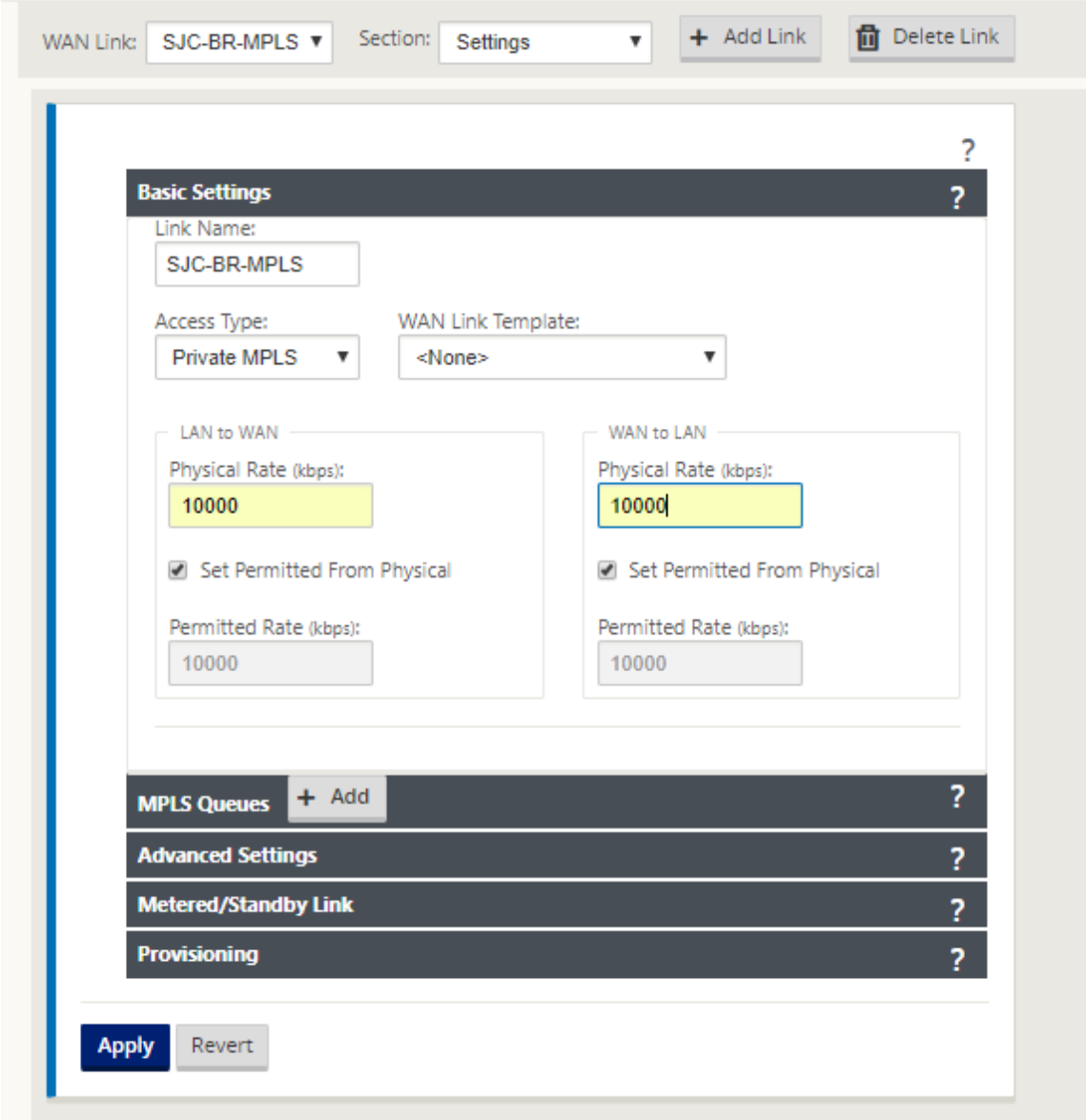




© 1999–2024 Cloud Software Group, Inc. All rights reserved.

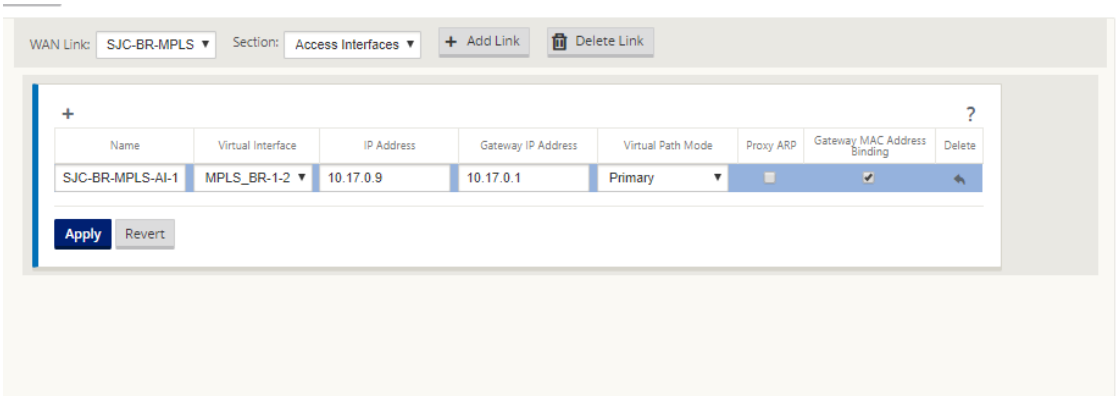
Crear enlace WAN MPLS

1. Vaya a **Vínculos WAN** y seleccione **Configuración** en la lista desplegable **Sección**. Haga clic en el botón **+ Enlace** para agregar un enlace WAN para el enlace MPLS.
2. Introduzca el nombre del enlace WAN MPLS y otros detalles. Seleccione **Tipo de acceso** como **intranet privada**.



3. Seleccione **Interfaces de acceso** en la lista desplegable **Sección** y haga clic en el botón **+** para agregar detalles de interfaz específicos para el enlace MPLS.
4. Introduzca la dirección IP virtual de MPLS y la dirección de puerta de enlace. El ARP proxy no está comprobado para menos de dos interfaces Ethernet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

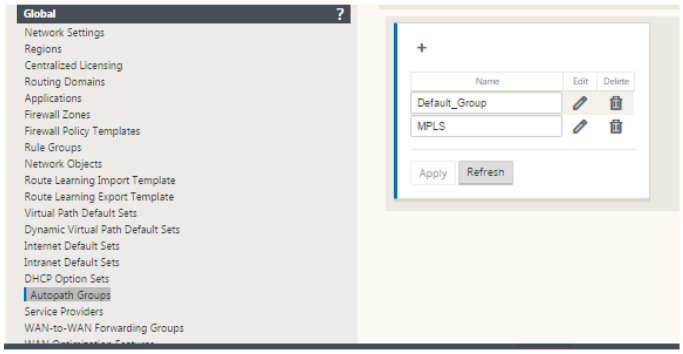


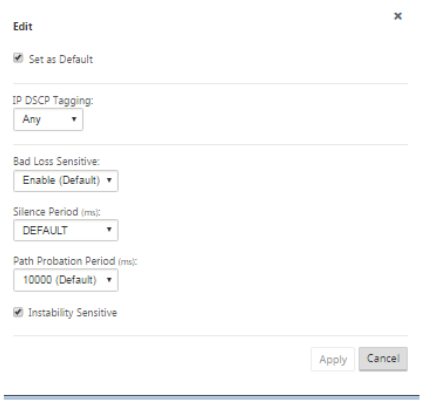
Rellenar rutas

Las rutas se crean automáticamente en función de la configuración anterior. Si hay más subredes específicas para esta sucursal remota, es necesario agregar rutas específicas que identifiquen qué puerta de enlace dirigir el tráfico para llegar a esas subredes back-end.

Crear grupos de rutas automáticas

1. En el **Editor de configuración**, vaya a **Global > Grupos de rutas automáticas**. Haga clic en **+**.
2. Introduce un nombre y haga clic en **Aplicar**.
3. Configure el grupo de rutas automáticas según sus necesidades y haga clic en **Aplicar**.





4. Vaya a **Conexiones > Vínculos WAN**. Seleccione el enlace WAN de Internet en la lista desplegable **Vínculos WAN** y **Rutas virtuales** en la lista desplegable **Sección**.
5. Seleccione la casilla de verificación **Usar** y elija el grupo de rutas automáticas recién creado en la casilla de verificación **Grupo de rutas automáticas** para los vínculos WAN de intranet en los sitios respectivos (tanto del centro de datos como de la sucursal).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

No se pueden marcar dos grupos de rutas automáticas como predeterminados. Si se marca, se produciría un error de auditoría.

Después de agregar manualmente las rutas virtuales para los vínculos WAN con el tipo de acceso como **Intranet privada**, las rutas virtuales se rellenan en **Rutas de acceso**.

Después de completar todos los pasos anteriores, proceda a Preparación de los paquetes de dispositivos SD-WAN.

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

May 7, 2021

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

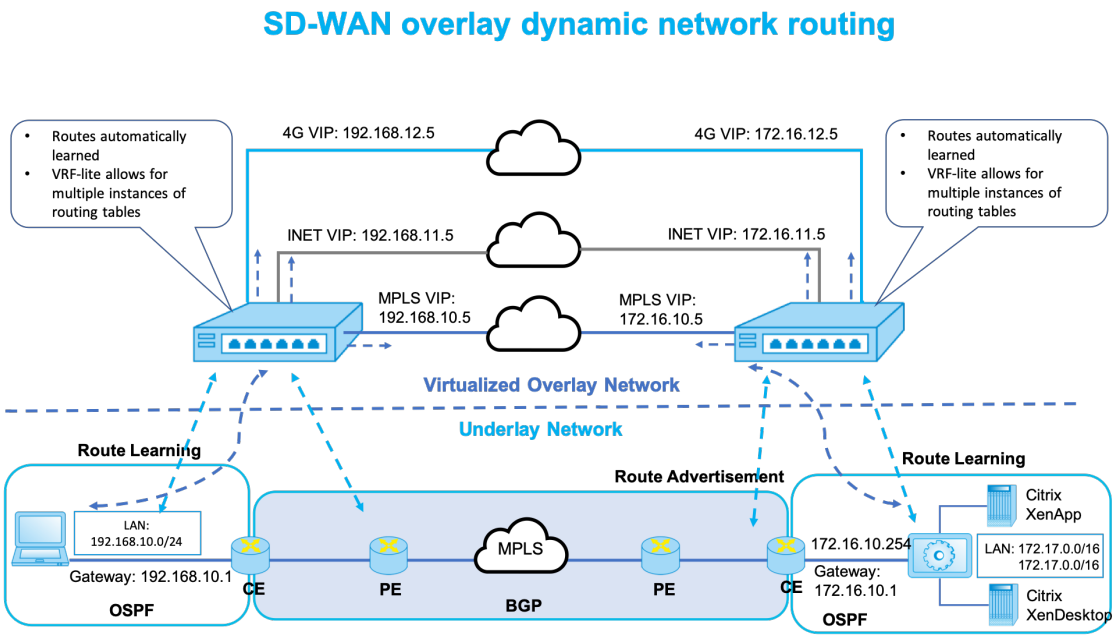
1. Cree un túnel de ruta WAN a través de cada enlace WAN entre dos dispositivos SD-WAN.
2. Configure la IP virtual para representar el punto final de cada enlace WAN. Puede establecer rutas WAN cifradas a través de la red L3 actual.
3. Agrega 2, 3 y 4 paths WAN (enlaces físicos) en una única ruta virtual que permite que los paquetes atraviesen la WAN mediante la red de superposición SD-WAN en lugar del subyacente existente, que es menos inteligente y rentable.

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 Ruta virtualizada al dispositivo de sitio seleccionado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Intranet: Sitios sin dispositivo SD-WAN
- Internet: tráfico vinculado a Internet
- Pass-through: tráfico intacto, en una interfaz de puente fuera de 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.



Optimización WAN con edición Premium (Enterprise)

May 7, 2021

Los dispositivos SD-WAN Premium (Enterprise) Edition contienen funcionalidad de optimización de WAN totalmente equipada, además de la virtualización de WAN. Algunos clientes prefieren implementar la funcionalidad de optimización WAN antes de migrar a servicios SD-WAN. Este caso de uso de implementación proporciona los pasos necesarios para utilizar los dispositivos Premium (Enterprise) Edition para utilizar los servicios de optimización de WAN.

Citrix SD-WAN Product Platform Edition incluye los siguientes dispositivos:

- SD-WAN: Dispositivo SD-WAN Standard Edition
- Premium (Enterprise): dispositivo SD-WAN Premium (Enterprise) Edition
- WANOP: Dispositivo SD-WAN WANOP Edition

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para integrar dispositivos Premium (Enterprise) Edition en una red WANOP distribuida existente, puede configurar el dispositivo SD-WAN (físico o virtual) en el sitio de DC como MCN. El dispositivo SD-WAN administra toda la configuración de la red. Se establece una ruta de acceso virtual entre el sitio de sucursal y MCN en el sitio de DC. Esta ruta virtual se utiliza para enviar tráfico de control entre los dispositivos. En el dispositivo de sucursal, el tráfico de datos se procesa como un servicio de intranet. El tráfico de intranet no está encapsulado y atraviesa el enlace WAN existente para llegar al sitio de DC. Un dispositivo WANOP en el sitio de DC debe estar en la ruta de tráfico para proporcionar una optimización de tráfico de extremo a extremo.

Para los sitios de clientes que no tienen un dispositivo de hardware SD-WAN en el extremo de la cabeza, los dispositivos VPX en un par de HA (dos VPX de WAN virtuales) se pueden utilizar como MCN en modo de un brazo. Para el modo de un brazo, se requieren reglas de PBR en el enrutador de terceros para redirigir el tráfico al dispositivo SD-WAN.

En este documento se supone que los dispositivos de sitio de DC se implementan en modo HA para redundancia. El modo HA no es obligatorio para esta implementación.

Requisitos previos

- Un par de dispositivos WANOP y un par de dispositivos SD-WAN implementados en modo HA en el sitio de DC.
- Un dispositivo Premium (Enterprise) Edition en el sitio de la sucursal.

Topología de red

SD-WAN Standard Edition y dispositivos WANOP en implementación PBR:

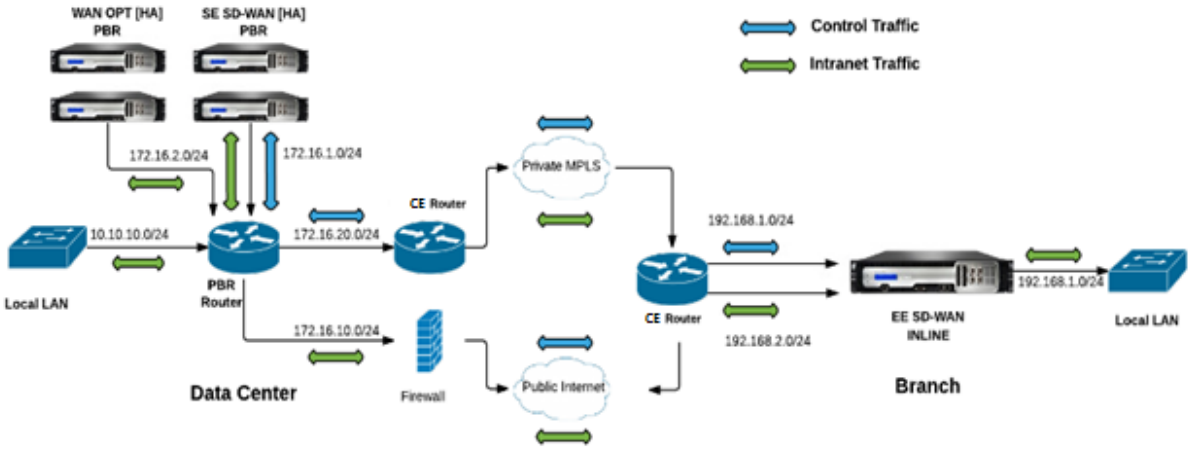
En la ilustración siguiente, tanto los dispositivos SD-WAN SE como WAN OP en el sitio de DC se implementan en modo de un brazo. El dispositivo SD-WAN admite la implementación de PBR, mientras que el dispositivo WANOP admite PBR y WCCP. El enrutador PBR redirige el tráfico de control (tráfico de ruta virtual) recibido de WAN en el sitio de DC al dispositivo SD-WAN. El enrutador PBR redirige el tráfico de datos al dispositivo de optimización WAN.

Flujo de tráfico para WAN a DC LAN:

- Enrutador CE (Cliente Edge) -> Enrutador PBR -> SD-WAN -> Enrutador PBR -> LAN
- Enrutador CE (Cliente Edge) -> Enrutador PBR - > OPT WAN - > Router- > LAN

El mismo flujo de tráfico se sigue en la dirección inversa.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



SD-WAN Standard Edition en modo PBR y WANOP en implementación en línea:

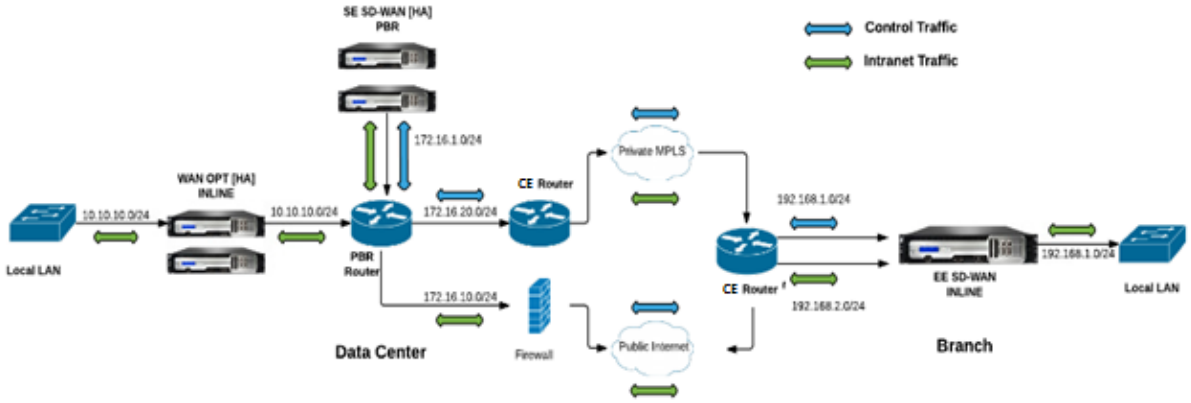
En la ilustración siguiente, el dispositivo SD-WAN en el sitio de DC se implementa en modo de un brazo mientras que el dispositivo WANOP se implementa en modo en línea.

El enrutador PBR redirige el tráfico de control (tráfico de ruta virtual) recibido de WAN en el sitio de DC al dispositivo SD-WAN. El enrutador PBR reenvía el tráfico de datos al dispositivo de optimización WAN (en línea).

Flujo de tráfico para WAN a DC LAN:

- Enrutador CE (Cliente Edge) -> Enrutador PBR -> SD-WAN -> Enrutador PBR -> LAN
- Enrutador CE (Customer Edge) - > Enrutador PBR -> WAN OPT - > LAN

El mismo flujo de tráfico se sigue en la dirección inversa.



Pasos de configuración

1. Configure el dispositivo SD-WAN en DC [MCN] para establecer rutas virtuales entre los sitios DC y Branch.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

¿VesConfigurar el servicio de rutas virtuales entre MCN y clientes?

2. Configurar el servicio de intranet en el sitio de DC.

   a) En el MCN (sitio DC), vaya a **Configuración > WAN virtual > Editor de configuración > Conexiones > Sitio (DC) > Servicios de Intranet**. Haga clic en el signo **[+]**para agregar un servicio de intranet.

   b) Seleccione uno o más enlaces WAN para el **servicio de intranet**y, a continuación, haga clic en **Aplicar**.

   c) Desplácese hasta Rutas en el mismo **sitio (DC)**, haga clic en **[+]** firmar para agregar la red remota con un coste inferior a 5 y seleccione **Agregar**.

      Por ejemplo, - Introduzca **192.168.1.0/24** en el campo **Dirección IP de red** con coste 4 y seleccione **Tipo de servicio** como **Intranet**.

      > **Nota**
      >
      > El coste en cada sitio debe ser inferior a 5 para que la ruta de intranet tenga prioridad.

3. Configurar el servicio de intranet en el sitio de la sucursal.

   a) Repita los subpasos de a a c del **paso 2** anterior en el sitio de la sucursal.

      Por ejemplo, - Introduzca **172.16.1.0/24** en el campo Dirección IP de red con coste 4 y seleccione **Tipo de servicio** como **Intranet**.

4. Realice **la administración de cambios** para cargar y distribuir la configuración en el sitio de la sucursal.

   Consulte Exportación de paquetes de configuración y administración de cambios.

   De forma predeterminada, el tráfico se envía de Branch a DC a través de la ruta virtual.

   > **Nota**
   >
   > El enrutador PBR debe configurarse para redirigir el tráfico según los pasos de implementación proporcionados.

   Para obtener más información acerca de la configuración de la Optimización de WAN, consulte: Activar-configurar-optimizar-WAN.

Modo de dos cajas

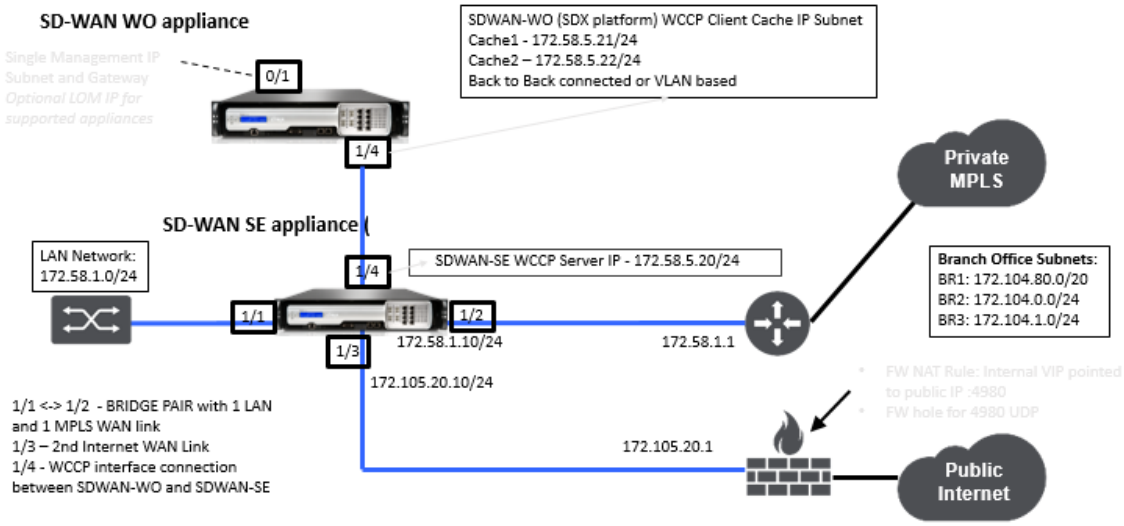
May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El modo de dos cajas es una implementación basada en un brazo WCCP donde el dispositivo SD-WAN SE actúa como un enrutador WCCP y los dispositivos SDWAN-WANOP (4000/5000) actúan como clientes WCCP y ayudan a establecer la convergencia WCCP. De esta forma, todos los paquetes TCP orientados al servicio de ruta virtual o intranet que llegan al dispositivo SD-WAN SE se redirigen al dispositivo SDWAN-WANOP para obtener beneficios de optimización al proporcionar beneficios tanto SD-WAN SE como WANOP para el tráfico del cliente.

El modo de dos cajas se admite en los siguientes modelos de dispositivos:

- Dispositivos SD-WAN SE: 4000, 4100 y 5100
- Dispositivos WANOP SD-WAN: 4000, 4100, 5000 y 5100



Nota

Los modos de implementación de alta disponibilidad y WCCP no son accesibles cuando el modo de dos cajas está habilitado. Sin embargo, estos modos de implementación están disponibles para que el usuario los administre.

Importante

- Aunque la implementación WCCP heredada está inhabilitada cuando se habilita el modo de dos cajas, la convergencia del grupo de servicios se puede verificar desde la página de supervisión de WCCP. No hay ninguna página de interfaz gráfica de usuario independiente en la sección de supervisión para el modo de dos cajas.
- Si el proceso WCCP que se ejecuta en el dispositivo Standard Edition se reinicia varias veces en un breve intervalo de tiempo, por ejemplo, 3 veces en un minuto, el grupo de servicios se apaga automáticamente. En tal caso, para obtener la convergencia WCCP en el dispositivo WANOP, vuelva a habilitar la función WCCP en la GUI web del dispositivo WANOP.
- Cuando se produce un cambio en la configuración de WCCP o en la optimización de WAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

relacionado con la configuración en el dispositivo Standard Edition, el dispositivo WANOP externo se reinicia. Por ejemplo, al activar/inhabilitar la casilla de verificación WCCP en el grupo de interfaz del editor de configuración seguido del proceso de administración de cambios, se reinicia también el dispositivo WANOP.

Nota

Además, tenga en cuenta los siguientes puntos a tener en cuenta al implementar el modo de dos cuadros:

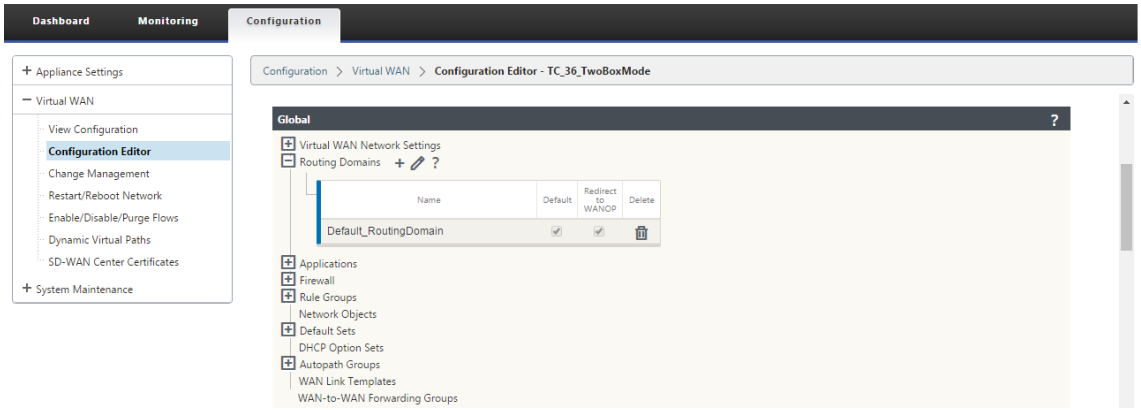
- Cuando se selecciona un dominio de redirección para ser redirigido al dispositivo WANOP desde el Editor de configuración, debe agregarse al grupo de interfaz para el que está habilitado WCCP.
- También se debe seleccionar el mismo tráfico del dominio de enrutamiento en el sitio asociado. Por ejemplo, **MCN** > **Branch01** para observar los beneficios de optimización WAN.
- Si se selecciona un dominio de enrutamiento en el grupo de interfaces en el que está habilitado WCCP, otro grupo de interfaces que contenga las interfaces en puente debe tener configurado el mismo dominio de enrutamiento. Solo si el grupo de interfaz habilitado WCCP tiene configurado el dominio de enrutamiento, no es suficiente transmitir el tráfico de extremo a extremo que fluye con beneficios de optimización WAN.

Edición estándar de Citrix SD-WAN

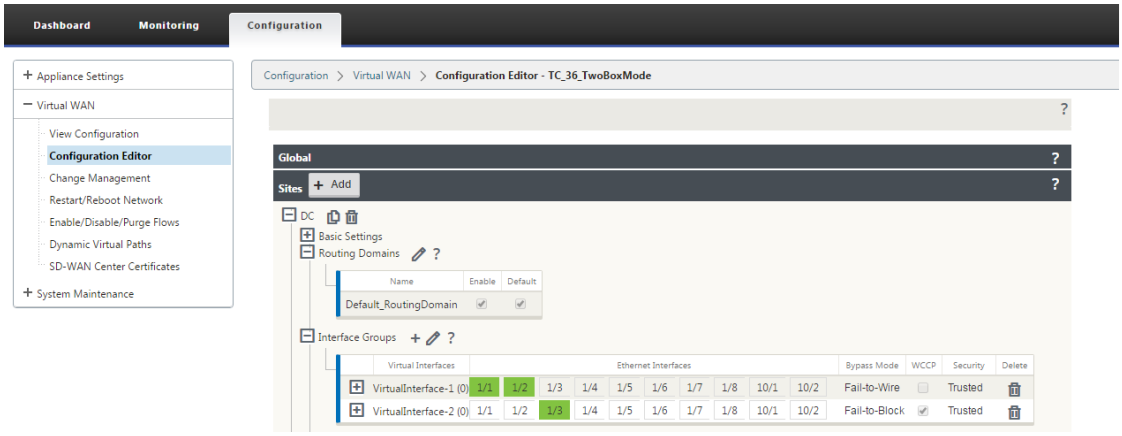
Para configurar la solución de modo de dos cajas en el dispositivo Standard Edition en el sitio de DC o sucursal:

1. En la interfaz de administración web de SD-WAN SE, vaya a **Configuración** > **Virtual WAN** > **Editor de configuración**. Abra un paquete de configuración existente o cree un paquete.
2. En el paquete de configuración elegido, vaya a la ficha **Avanzadas** para ver los detalles de configuración.
3. Abra Configuración **global** y expanda **Dominios de enrutamiento** para ver que la casilla de verificación **Redirigir a WANOP** está habilitada.

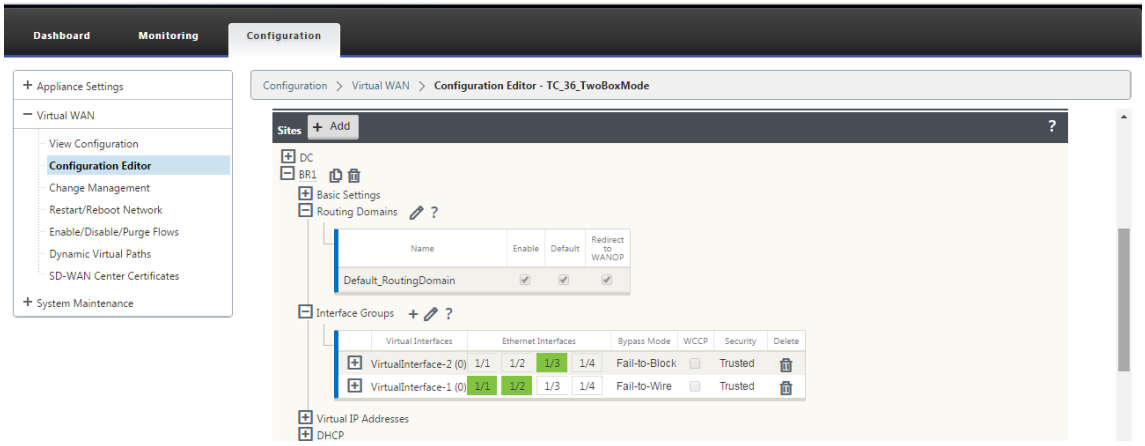
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Expanda DC para habilitar **WCCP** para la **interfaz virtual** en Configuración **del grupo de interfaz** que indica para qué interfaz de red virtual está habilitado el dispositivo.



5. Expanda **Sites+ Agregar** para ver la configuración del dominio de enrutamiento de sucursales y del grupo de interfaces. En el sitio de la sucursal, la casilla de verificación **Redirigir a WANOP** está habilitada para Redirección de dominios.



> **Nota**
>
> La escucha WCCP debe estar habilitada para aquellas interfaces de red virtual que tengan

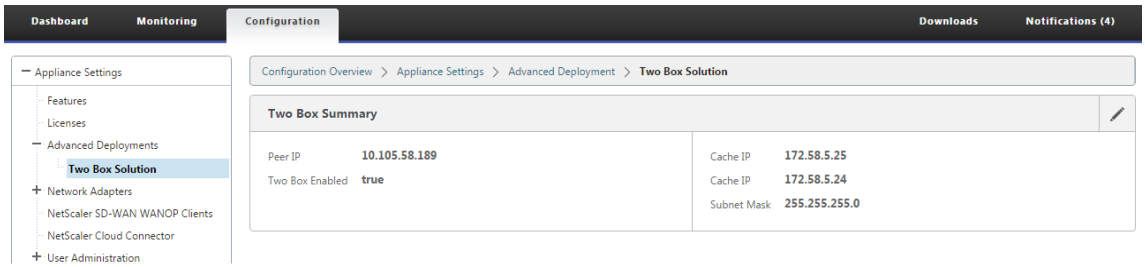
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> una sola interfaz Ethernet configurada. No habilite la escucha WCCP en un par BRIDGED. Está diseñada para habilitarse en la interfaz ONE-ARM entre los dispositivos SD-WAN SE y SD-WAN WANOP.

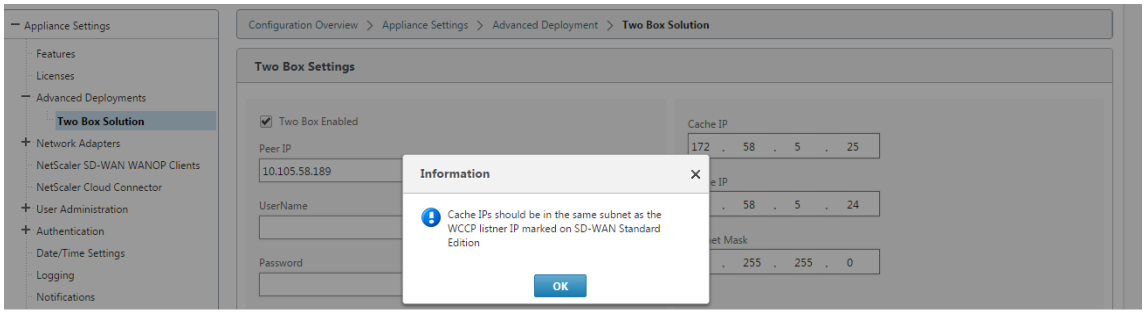
Configuración de Citrix SD-WAN WANOP

Para configurar el modo de implementación de dos cajas en la GUI web del dispositivo WANOP de SD-WAN:

1. En la interfaz de administración web SD-WAN WANOP, vaya a **Configuración** > **Configuración del equipo** > **Implementaciones avanzadas** > **Solución de dos cajas**.



2. Haga clic en el icono **Modificar** para modificar los dos ajustes del modo de cuadro. Aparece el cuadro de diálogo de información sobre las **direcciones IP de caché**. Haga clic en **OK**.



3. Active la casilla de verificación **Dos cajas habilitadas**.
4. Introduzca la **IP del mismo nivel**. La dirección IP del mismo nivel es la dirección IP del dispositivo SD-WAN Standard Edition.
5. Introduzca las credenciales de usuario y haga clic en **Aplicar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración y capacidad de administración de dos modos de caja

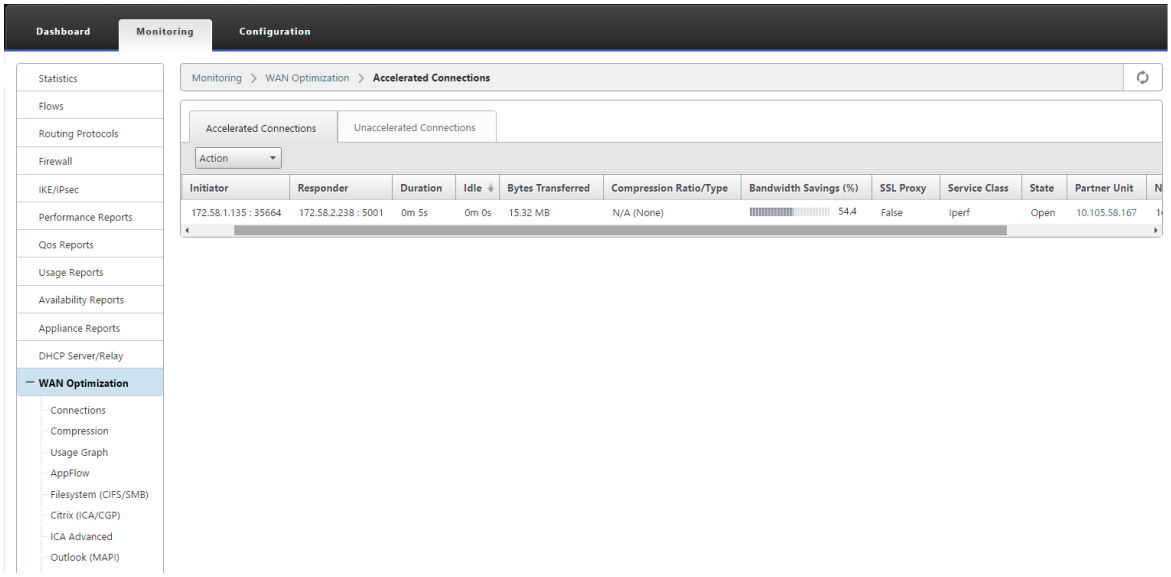
A continuación se presentan algunos de los dos puntos de configuración y capacidad de administración del modo de caja que se deben tener en cuenta para la implementación:

- Las configuraciones WANOP SD-WAN mencionadas a continuación se pueden configurar desde el editor de configuración SD-WAN SE como un panel unificado
  - CLASE DE SERVICIO
  - CLASIFICADOR DE APLICACIONES
  - FUNCIONES
  - AJUSTE DEL SISTEMA

Supervisión

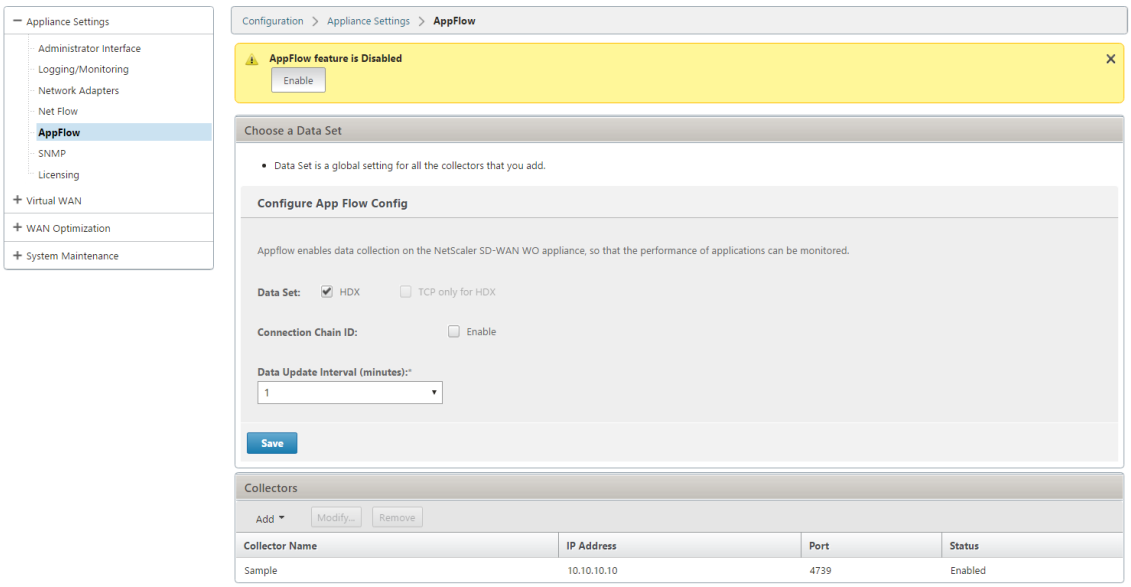
Puede supervisar el tráfico WANOP de SD-WAN directamente mediante la página Supervisión de la interfaz de usuario web del dispositivo SD-WAN SE. Esto permite la supervisión de un solo panel de los dispositivos SDWAN-SE y SDWAN-WO mientras se procesa el tráfico de datos. Puede ver los detalles de conexión, los detalles de los asociados seguros, etc., en el nodo Optimización de WAN en la interfaz de usuario de SDWAN-SE.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración

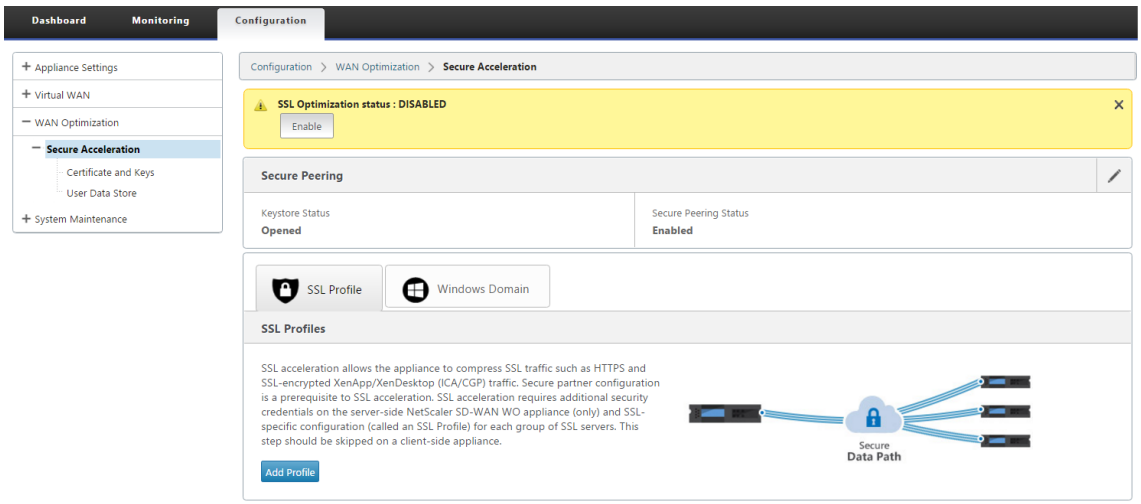
Puede configurar APPFLOW directamente desde la página **Configuración** de SDWAN-SE en el nodo **APPFLOW**. Esto permite a SDWAN-SE actuar como un único panel para la configuración de APPFLOW y otros atributos de configuración de procesamiento de datos, como Clase de servicio, Clasificadores de aplicaciones. La configuración realizada en el SDWAN-SE se refleja en la configuración de SDWAN-WO, manteniendo una compatibilidad perfecta con la funcionalidad APPFLOW.



El WANOP de SD-WAN ya descubierto por Citrix Application Delivery Management (ADM), si se utiliza en el modo de dos cajas, debe aislarse y no configurarse con Citrix ADM hasta que este modo se desactive. Esto se debe a que la configuración de WANOP para el procesamiento del tráfico es administrada por el dispositivo SD-WAN SE en el modo Two Box.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las optimizaciones avanzadas o la aceleración segura deben configurarse directamente en el dispositivo SDWAN-SE como lo haría en el dispositivo SDWAN-WO. Esto ayuda a mantener un único panel de configuración de configuraciones como Domain Join o Aceleración segura/SSL Profile Creation para optimizaciones avanzadas o SSL Proxy.



- Las licencias deben administrarse por separado para cada uno de los dispositivos SD-WAN SE y SD-WAN WANOP.
- La actualización de software debe administrarse por separado para cada uno de los dispositivos SD-WAN SE y SD-WAN WANOP con los respectivos paquetes de software. Por ejemplo, tar.gz para SD-WAN SE y upgrade upg para SD-WAN WANOP.
- La integración de rutas de datos debe configurarse entre SD-WAN SE y dispositivos WANOP externos a través del modo de implementación WCCP.
  - A nivel de ruta de datos, las funciones WCCP y WAN virtual se ofrecen a través de la integración de rutas de datos entre WANOP y SE externamente en modo de un brazo para obtener beneficios de optimización.

Configuración y supervisión unificadas

Cuando habilita el modo de dos cajas con dispositivos SD-WAN SE y SDWAN-WANOP, puede ver la configuración en el dispositivo SD-WAN SE de forma similar a la que puede ver la configuración de dos cajas con el dispositivo SD-WAN-EE.

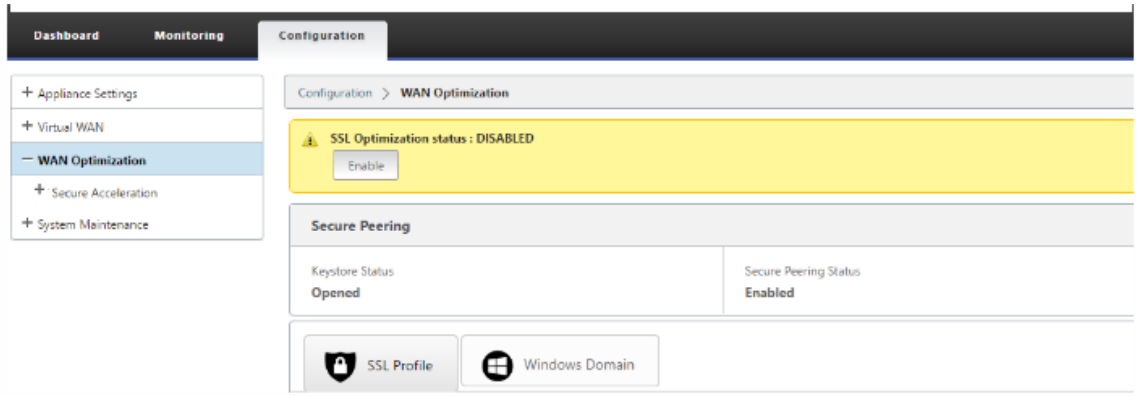
1. Vaya a **Configuración** > **WAN virtual** > **Optimización de WAN**
2. Nodo Appflow en **Configuración** > **Configuración del dispositivo**
3. Nodo de optimización WAN en Configuración.

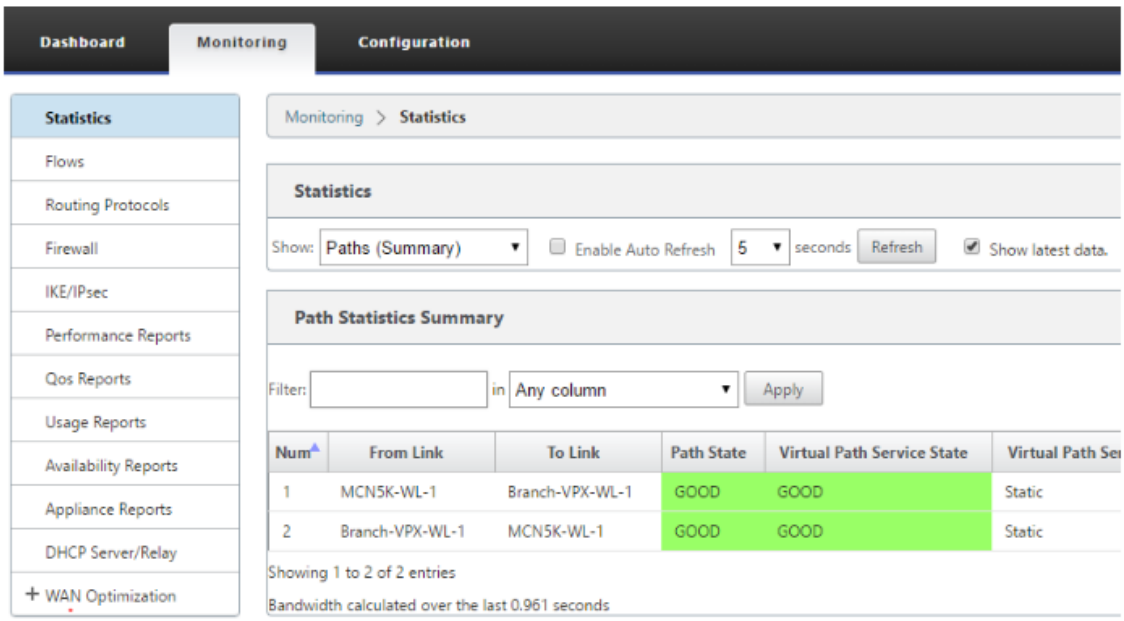
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Esta información se redirige desde el dispositivo WANOP SD-WAN que se encuentra en modo de caja de dos con el dispositivo SD-WAN SE.

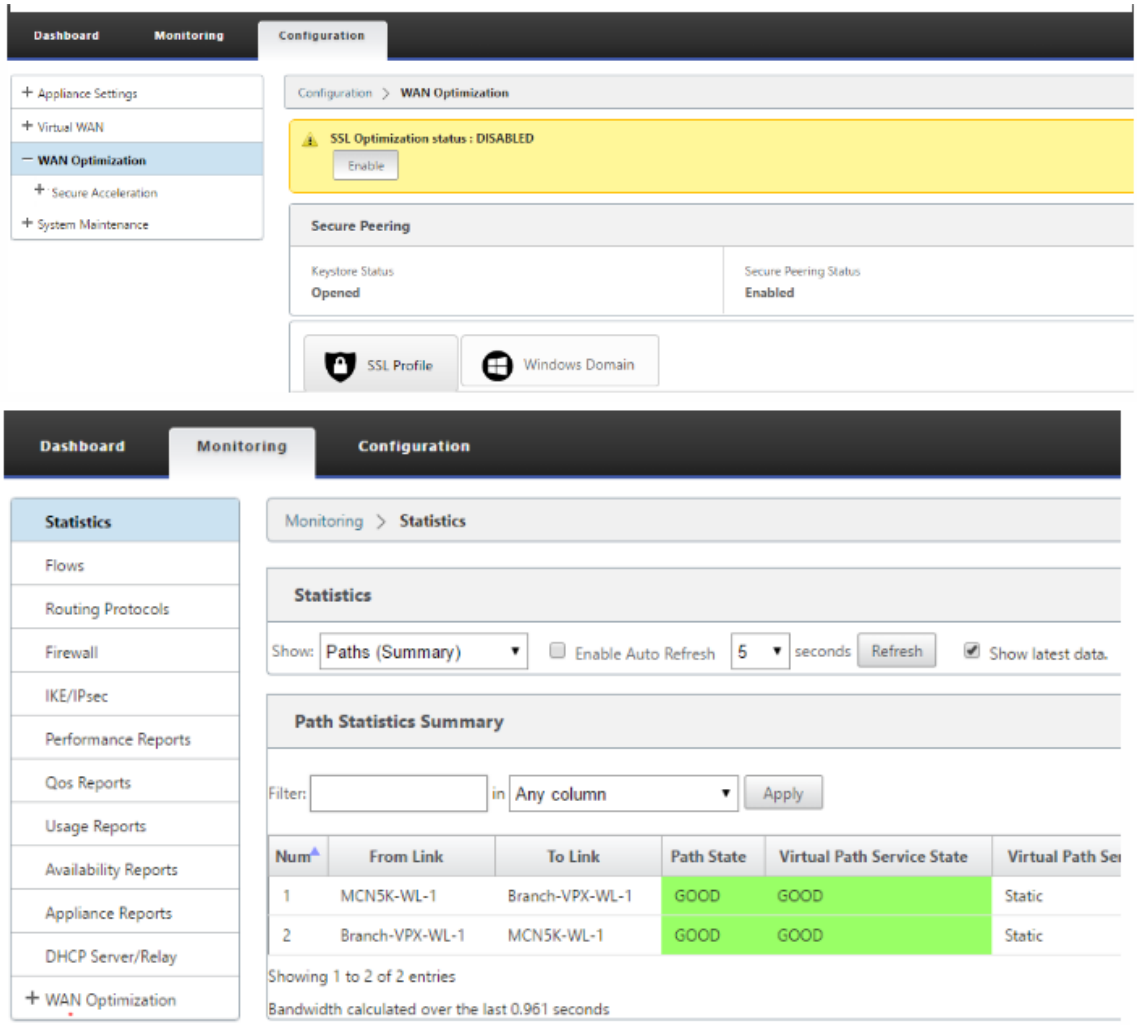
La configuración relacionada con WANOP, como SSL Acceleration y AppFlow ahora se puede realizar desde SD-WAN SE Web GUI.

Las estadísticas relacionadas con el tráfico, como Conexiones, Compresión, CIFS/SMB, ICA Advanced, MAPI y asociados de negocios ahora se pueden supervisar desde la GUI web de SD-WAN SE en **Supervisión** > **Optimización de WAN** similar al dispositivo de edición SD-WAN Premium (Enterprise).





© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cambio de dirección IP de administración para el dispositivo WANOP SD-WAN en modo de dos cajas

Para cambiar la dirección IP de administración del dispositivo SDWAN-WANOP en el modo de dos cuadros:

1. Ejecute el comando *clear_wo_sync* en el dispositivo SD-WAN SE. Garantiza que la información de la dirección IP WANOP de SD-WAN se borra para la redirección de GUI.
2. Desactive y active la configuración del modo de dos cajas en el dispositivo WANOP SD-WAN. La nueva dirección IP (IP modificada) del dispositivo SD-WAN WANOP se envía a SD-WAN SE. La nueva dirección IP modificada se muestra en las páginas de redirección de URL.

La dirección IP de administración se utiliza para la configuración de direcciones IP del mismo nivel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Inhabilitar el modo de dos cajas en el dispositivo WANOP SD-WAN

Para inhabilitar o desacoplar los dispositivos SD-WAN WANOP y SD-WAN SE del modo Dos cajas:

1. Inhabilite el modo de dos cajas desde el dispositivo WANOP SD-WAN.
2. Se espera ver el dispositivo SD-WAN WANOP dos páginas en modo de caja en la GUI web SD-WAN SE. Para borrar estas páginas, ejecute el comando: *clear_wo_sync*.

Alta disponibilidad

October 27, 2021

En este tema se tratan las implementaciones y configuraciones de alta disponibilidad (alta disponibilidad) compatibles con los dispositivos SD-WAN (Standard Edition y Premium (Enterprise) 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. Dependiendo del modo de implementación, la conmutación por error rápida tiene un impacto mínimo en el tráfico de aplicaciones que pasa a través de la red.

Modos de implementación de alta disponibilidad

Modo de un brazo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

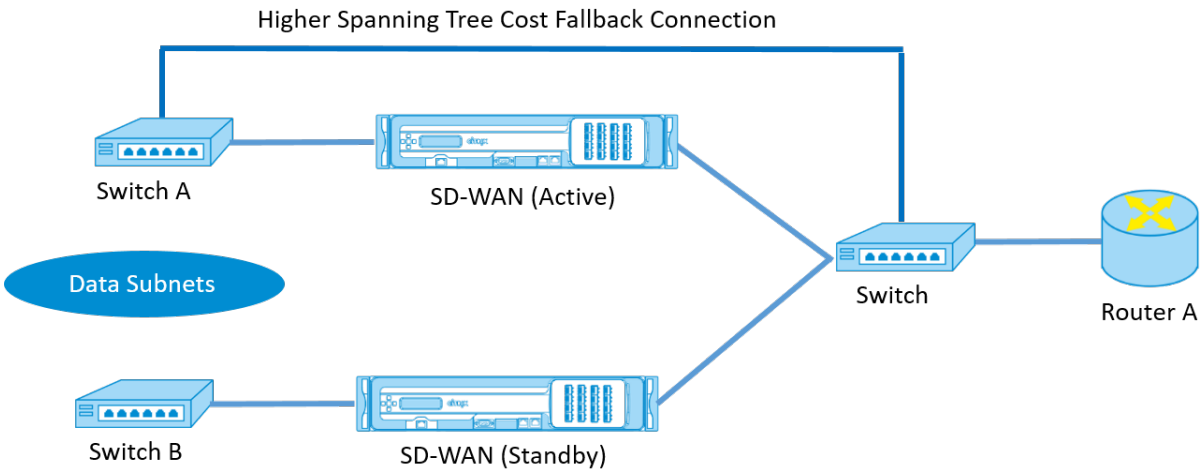
Modo paralelo de alta disponibilidad en línea:

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.

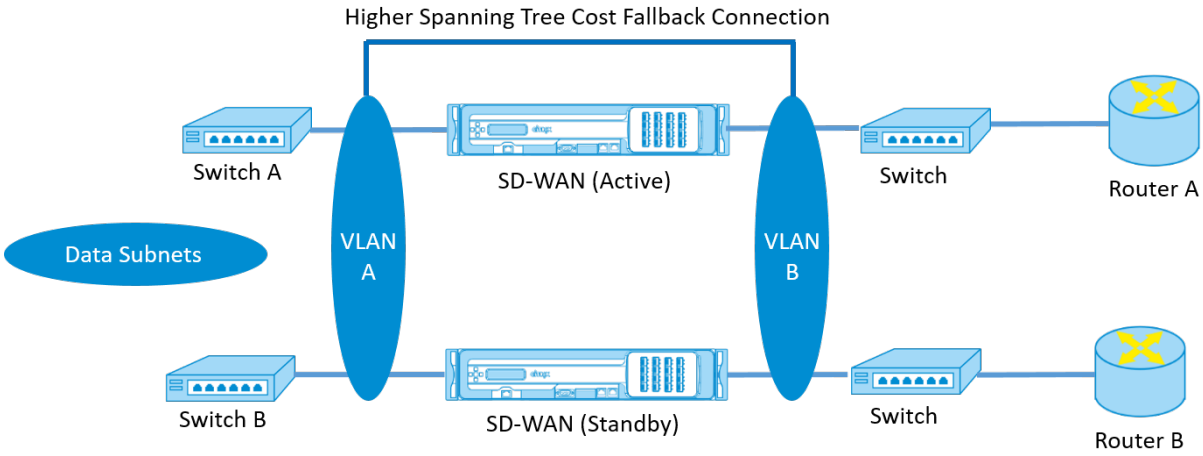
El estado de alta disponibilidad se puede supervisar a través de los grupos de interfaces en línea o a través de una conexión directa entre los dispositivos. El seguimiento externo se puede utilizar para supervisar la accesibilidad de la infraestructura de red ascendente o descendente. Por ejemplo, falla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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

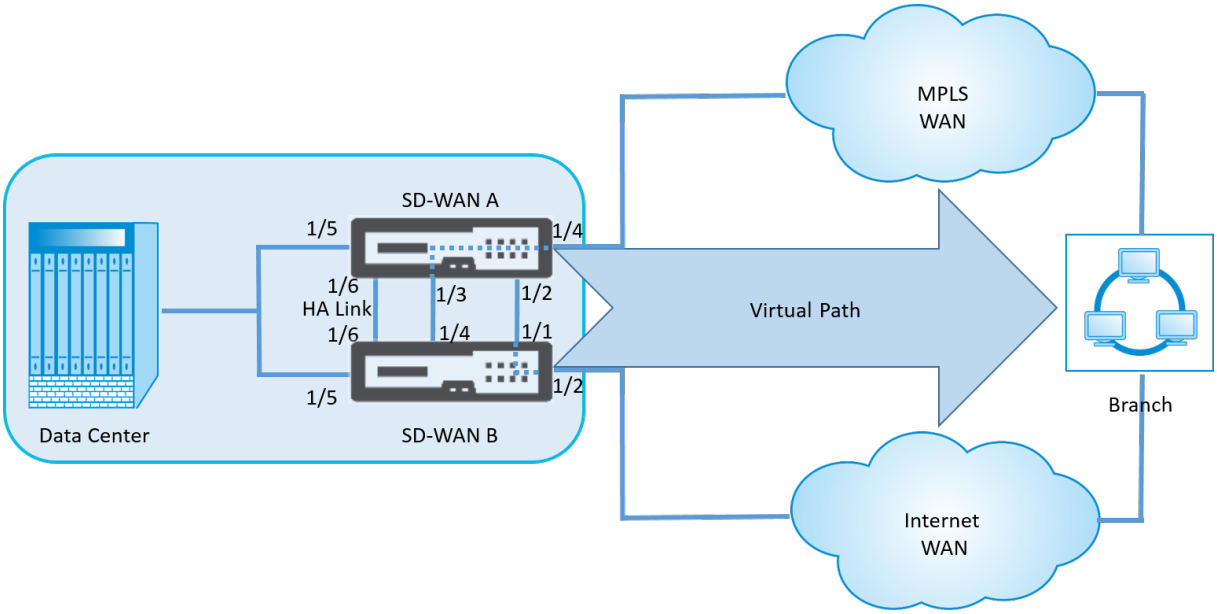
> **Nota**
>
> - La conmutación de alta disponibilidad en modo de error a cable tarda aproximadamente 10 a 12 segundos debido al retraso en la recuperación de los puertos del modo Fail-to-Wire.
> - Si falla la conexión de alta disponibilidad entre los dispositivos, ambos equipos pasan al estado Activo y provocan una interrupción del servicio. Para mitigar la interrupción del

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

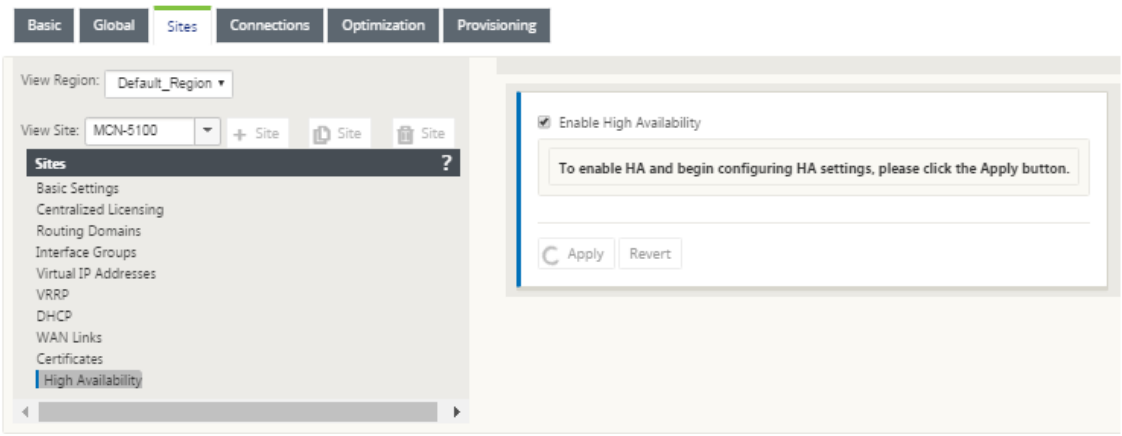
Si se acepta una pérdida mínima de servicio durante una conmutación por error, el modo de alta disponibilidad Fail-to-Wire es una mejor solución. El modo de alta disponibilidad Fail-to-Wire protege contra fallos del dispositivo y la alta disponibilidad en línea paralela protege contra todos los fallos.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

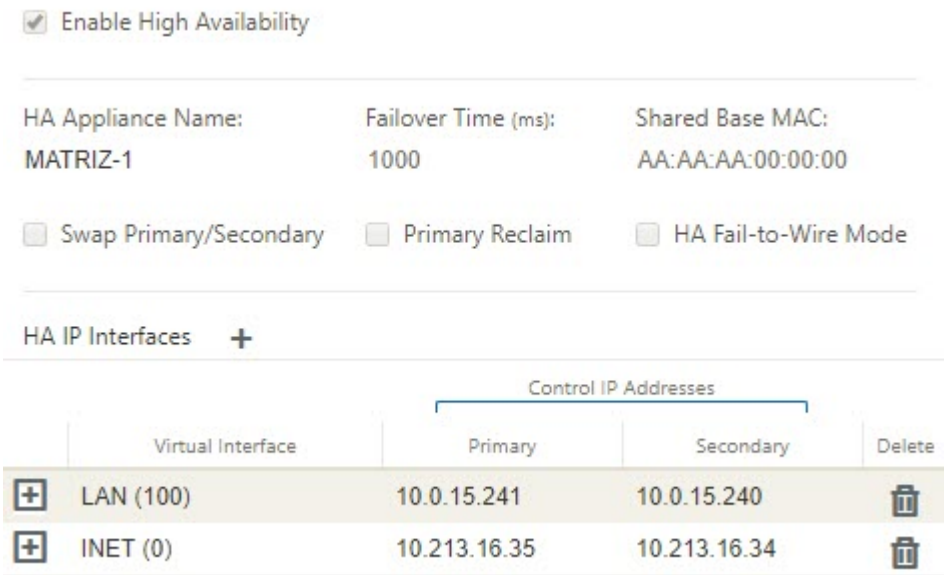
Configurar alta disponibilidad

Para configurar la alta disponibilidad:

1. En el Editor de configuración, vaya a **Sitios** > **nombre del sitio** > **Alta disponibilidad.** Seleccione **Activar alta disponibilidad y haga** clic en **Aplicar.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





2. Escriba los valores para el parámetro siguiente:

   - **Nombre del dispositivo de alta disponibilidad:** nombre del dispositivo de alta disponibilidad (secundario).
   - **Tiempo de conmutación por error:** el tiempo de espera (en milisegundos) después de perder el contacto con el dispositivo primario, antes de que el dispositivo en espera se active.
   - **MAC base compartida:** la dirección MAC compartida para los dispositivos de par de alta disponibilidad. Cuando se produce una conmutación por error, el dispositivo secundario tiene las mismas direcciones MAC virtuales que el dispositivo principal con error.
   - **Intercambiar primario/secundario:** si se selecciona, si ambos dispositivos del par de alta disponibilidad se presentan simultáneamente, el dispositivo secundario se convierte en el dispositivo principal y tiene prioridad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Reclamación principal:** cuando se selecciona, el dispositivo principal designado recupera el control al reiniciar después de un evento de conmutación por error.
- **Modo Fail-to-Wire de alta disponibilidad:** Seleccione esta opción para habilitar el modo de implementación de alta disponibilidad de fallos a cables.

> **Nota**
>
> Para plataformas basadas en hipervisor y en la nube, elija la opción **Inhabilitar MAC de base compartida** para inhabilitar la dirección MAC virtual compartida.
>
> Para plataformas basadas en Hypervisor, asegúrese de que el modo promiscuo esté habilitado en los hipervisores para permitir el abastecimiento de paquetes desde una dirección MAC compartida de alta disponibilidad. Si el modo promiscuo no está habilitado, puede habilitar la opción **Inhabilitar MAC de base compartida**.

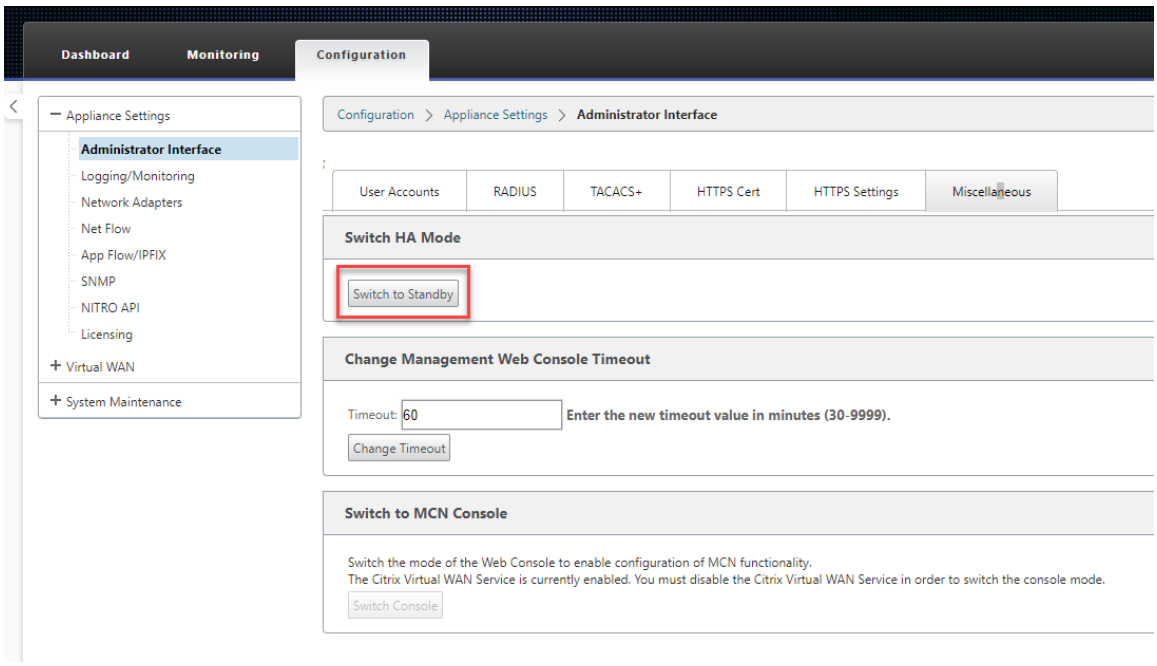
Haga clic en **+** junto a **Interfaces IP de alta disponibilidad para configurar grupos de interfaces**. Escriba Valores para los siguientes parámetros:

- **Interfaz virtual**: Interfaz virtual que se utilizará para la comunicación entre los dispositivos del par de alta disponibilidad. Supervisa el dispositivo Active para la accesibilidad. Para el modo de alta disponibilidad de un brazo, solo se requiere un grupo de interfaz.
- **Principal**: La dirección IP virtual única para el dispositivo principal. El dispositivo secundario utiliza la dirección IP virtual principal para comunicarse con el dispositivo principal.
- **Secundaria**: La dirección IP virtual única para el dispositivo secundario. El dispositivo principal utiliza la dirección IP virtual secundaria para comunicarse con el dispositivo secundario.

Haga clic en **+** a la izquierda de la nueva entrada de **interfaces IP de alta disponibilidad**. En el campo **Dirección IP de seguimiento** externo, escriba la dirección IP del dispositivo externo que responde a las solicitudes ARP para determinar el estado del dispositivo principal y, a continuación, haga clic en **Aplicar**.

> **Nota:**
>
> También puede activar manualmente una conmutación de alta disponibilidad desde el dispositivo. Vaya a **Configuración** > **Configuración del dispositivo** > **Interfaz de administrador** > **Varios**. En la sección Switch HA Mode, haga clic en **Cambiar a modo de espera** o **Cambiar a activo** según el dispositivo HA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

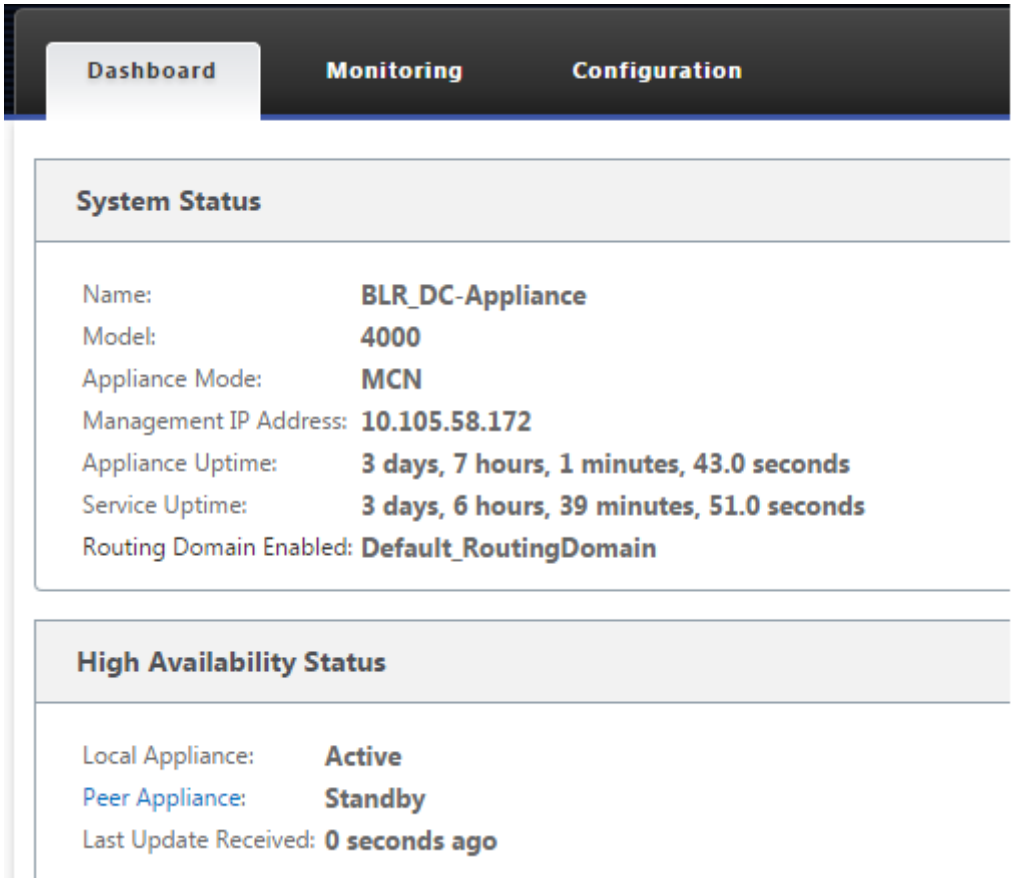


Supervisión

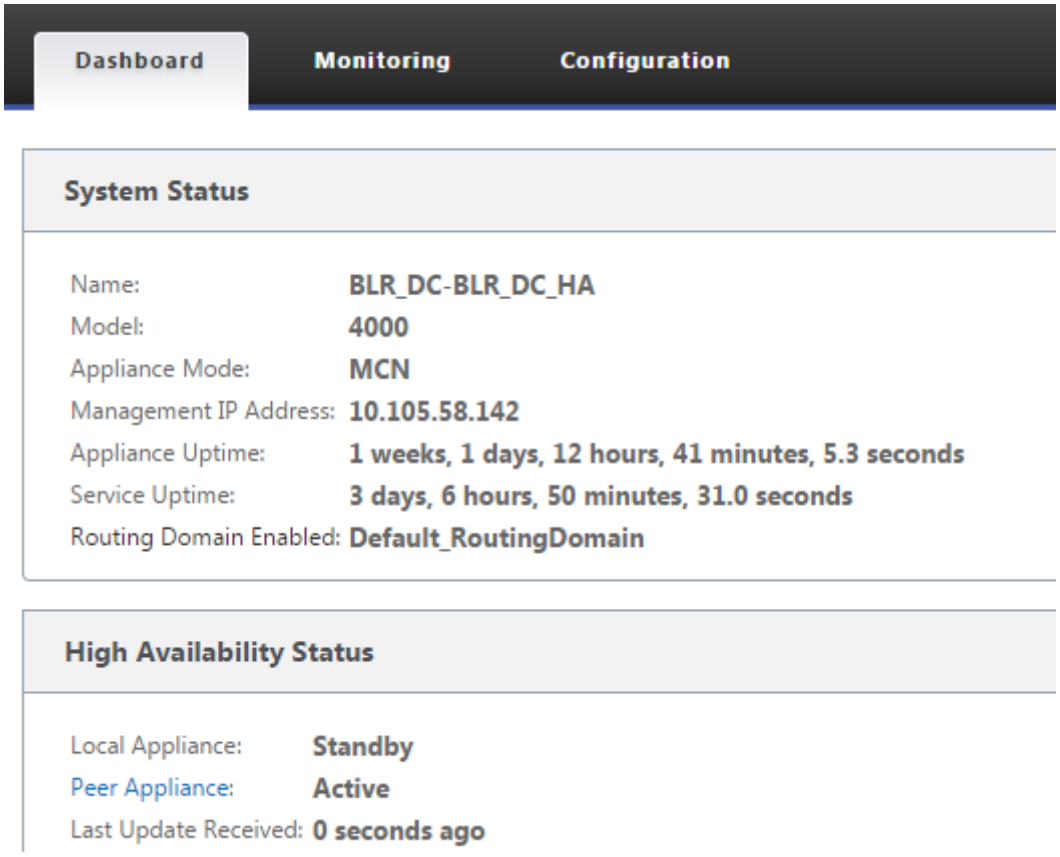
Para supervisar la configuración de alta disponibilidad:

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.

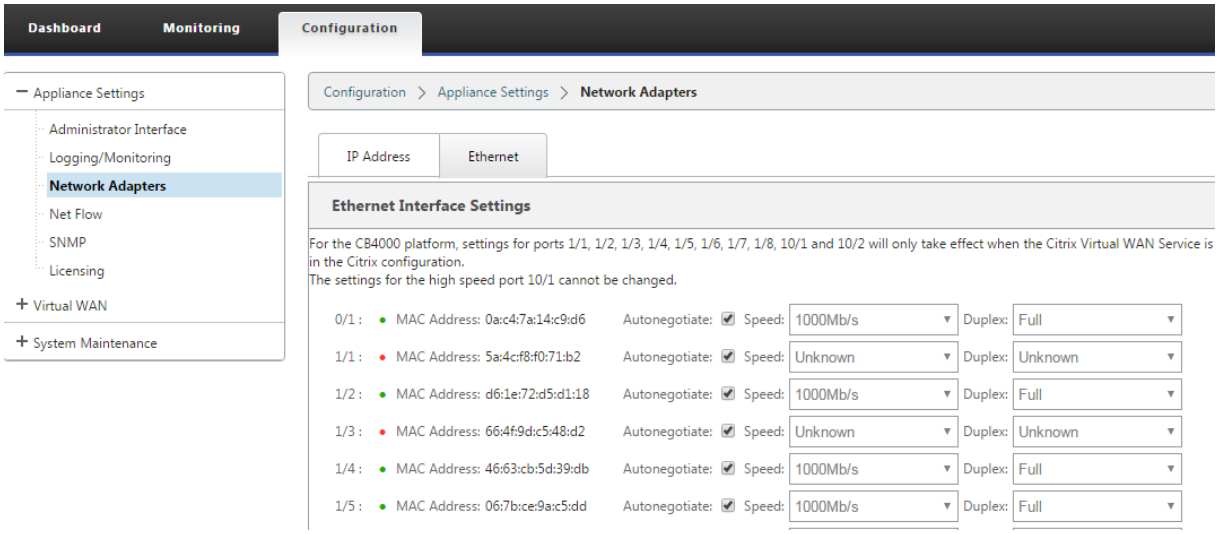
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



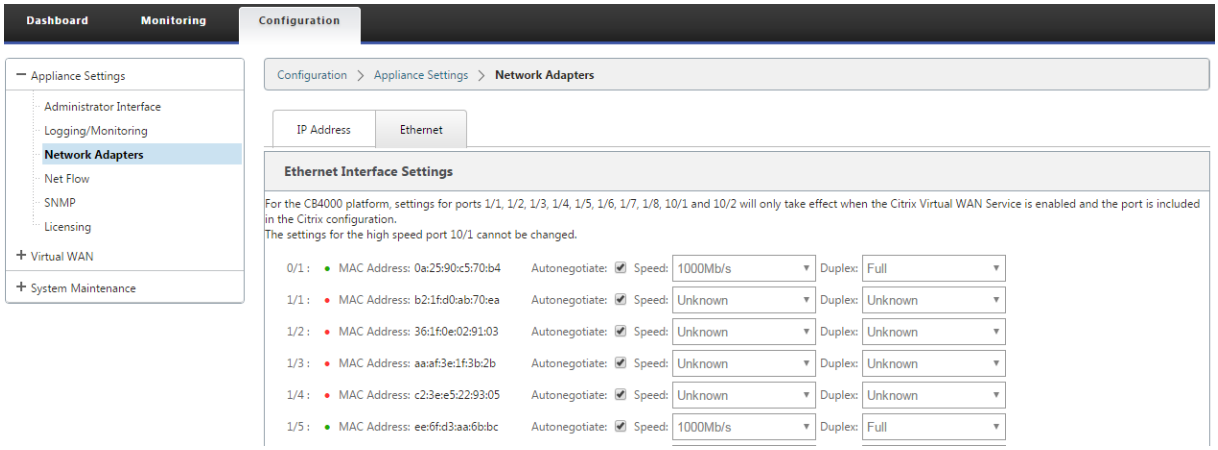
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

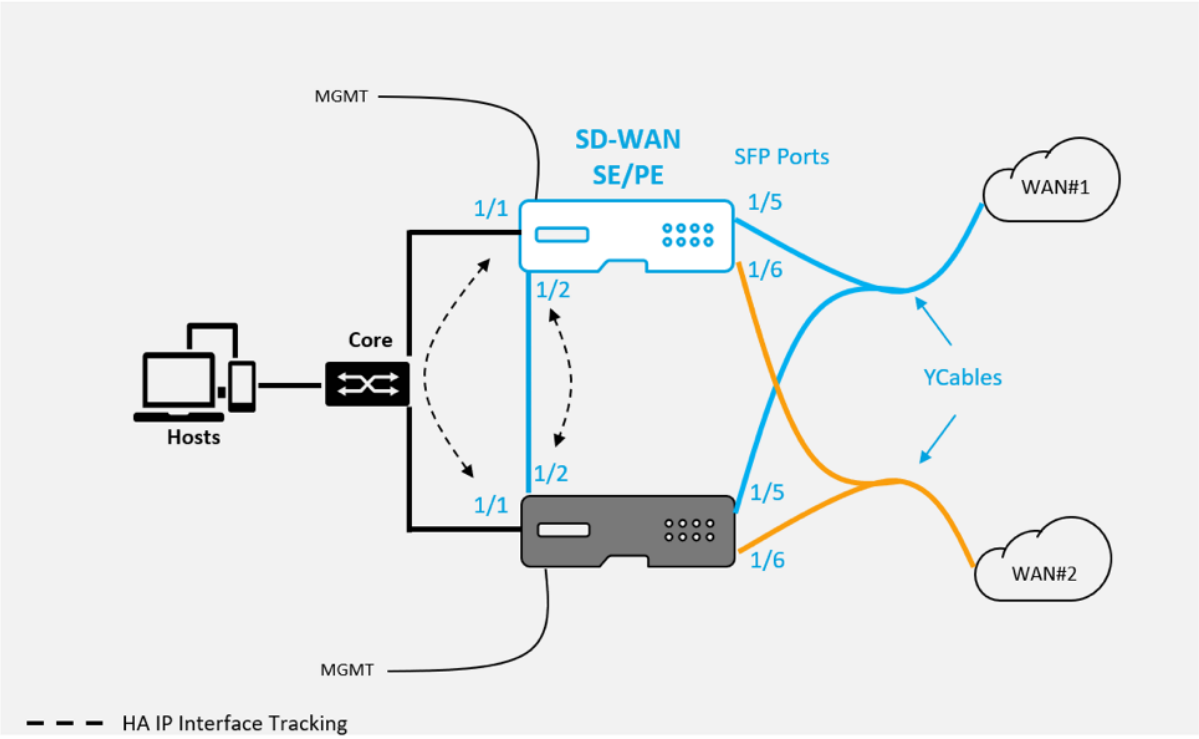
Habilitar alta disponibilidad en modo de borde mediante cable Y de fibra óptica

September 26, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

En el siguiente procedimiento se describen los pasos para habilitar la alta disponibilidad (HA) en 1100 dispositivos SE/PE implementados en modo perimetral, donde las entregas 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 en Y de fibra óptica para habilitar la función de alta disponibilidad para la implementación del modo perimetral.
En el dispositivo 1100 SE/PE, el extremo dividido del cable divisor se conecta a los puertos de fibra de dos dispositivos 1100 configurados en un par HA.
El cable en Y de fibra óptica tiene tres extremos. Un extremo se conecta al traspaso de fibra del proveedor y los otros dos extremos se conectan a puertos SFP configurados para ese enlace WAN en dos dispositivos SE/PE de 1100 implementados en un par de alta disponibilidad. El cable divisor se utiliza para dividir una señal entrante en varias señales.

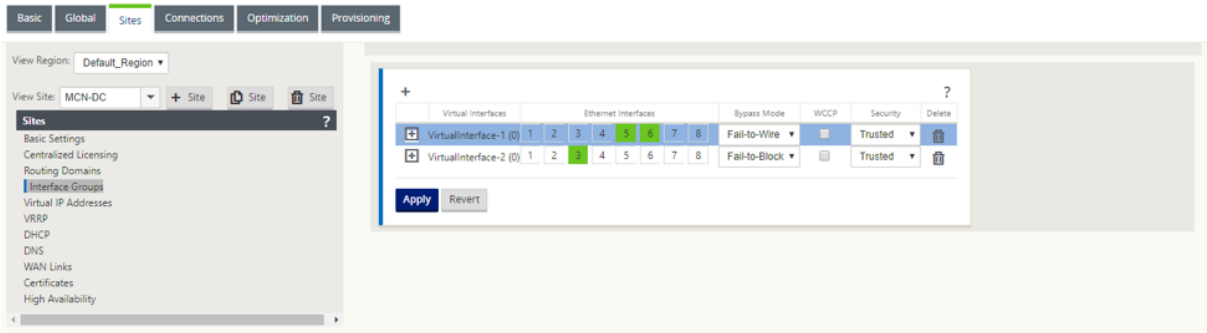


Requisitos previos:

1. En el dispositivo 1100 SE/PE, los puertos 1/5 y 1/6 son puertos SFP. Conecte los extremos del divisor del cable Y a cualquiera de estos puertos en ambos dispositivos en el par HA; consulte1100 SEpara obtener más información.
2. Agregue puertos SFP a la configuración del dispositivo SD-WAN. La configuración de los puertos SFP es lo mismo que la configuración de cualquier puerto de interfaz de red. Para obtener

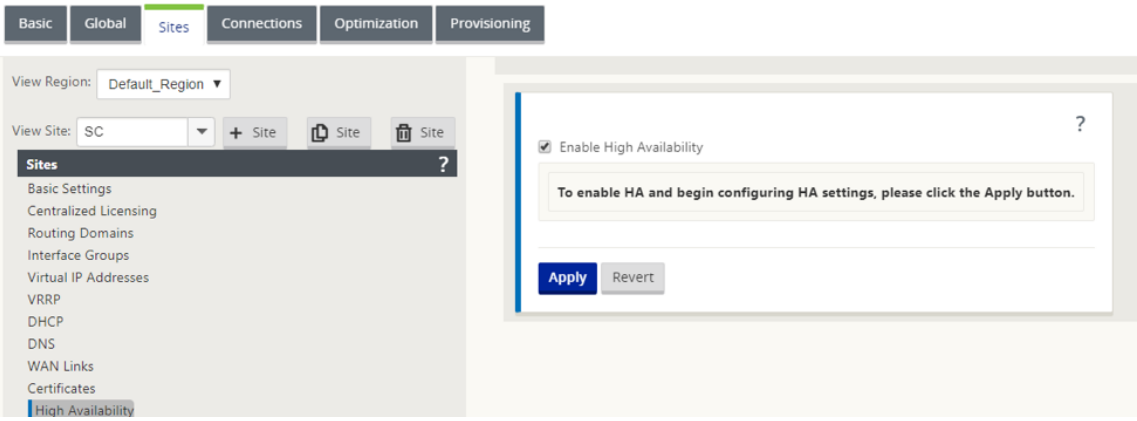
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

más información, consulte Cómo configurar grupos de interfaz. Agregar puertos 1/5 o 1/6 a la configuración le permite habilitar la función de soporte de cable Y.



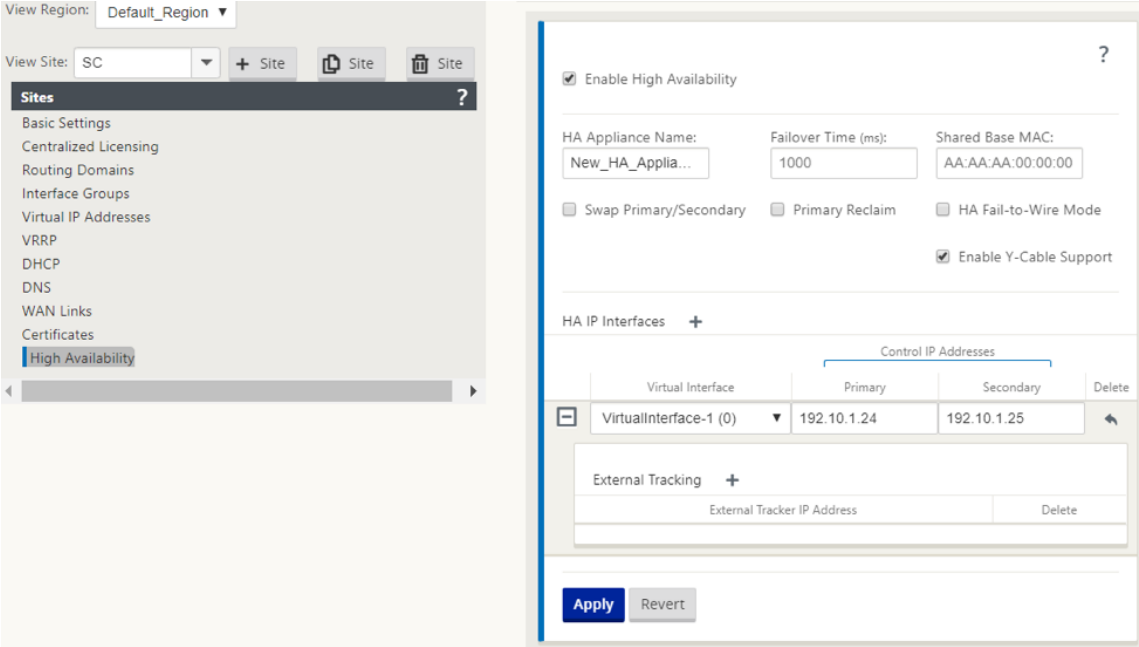
Para habilitar la alta disponibilidad mediante el cable Y:

1. En la GUI del dispositivo SE/PE 1100, vaya a **Configuración > WAN virtual > Editor de configuración > Sitios**. Haga clic en **Habilitar alta disponibilidad**.



2. Haga clic en **Habilitar compatibilidad con cable Y.**
3. Agregue interfaces IP de alta disponibilidad mediante cualquier otra interfaz además de las interfaces conectadas a los cables Y (por ejemplo, interfaz orientada a LAN 1/1 o interfaces 1/2 conectadas directamente). Cuando la función de cable Y está habilitada, los puertos SFP no se pueden utilizar para las interfaces IP de alta disponibilidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Aplicar, Stage y Activar la configuración.

Limitaciones:

- No se admite la configuración del modo de conmutación por error de alta disponibilidad 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 superior de software y 11.0 o superior para admitir esta implementación.

Tacto cero

June 8, 2022

> **Nota**
>
> El servicio Zero Touch Deployment se admite en determinados dispositivos Citrix SD-WAN:
>
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1100 Standard Edition
> - SD-WAN 1100 Modificación Premium
> - SD-WAN 1000 Standard Edition (se requiere reimagen)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - SD-WAN 1000 Enterprise Edition (Premium Edition)
> - SD-WAN 2000 Standard Edition
> - SD-WAN 2000 Enterprise Edition (Premium Edition)
> - SD-WAN 2100 Enterprise Edition (Premium 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 back-end que alojan la identificación almacenada de los clientes de Citrix que han adquirido dispositivos compatibles con Zero Touch (por ejemplo, SD-WAN 410-SE, 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.

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:

- Creación de configuraciones mediante la herramienta de configuración de red de Citrix SD-WAN Center o importación de configuración desde el dispositivo SD-WAN del nodo de control maestro (MCN)
- Citrix Cloud Login para iniciar el servicio Zero Touch Deployment Service para la implementación de nuevos nodos de sitio.

  > **Nota**
  >
  > Si su SD-WAN Center está conectado a Internet a través de un servidor proxy, debe configurar la configuración del servidor proxy en SD-WAN Center. Para obtener más información, consulteConfiguración del servidor proxy para la implementación Zero Touch.

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

- Si es necesario, configure firewalls para la comunicación saliente con FQDN ***sdwanzt.citrixnetworkapi.net*** desde SD-WAN Center.

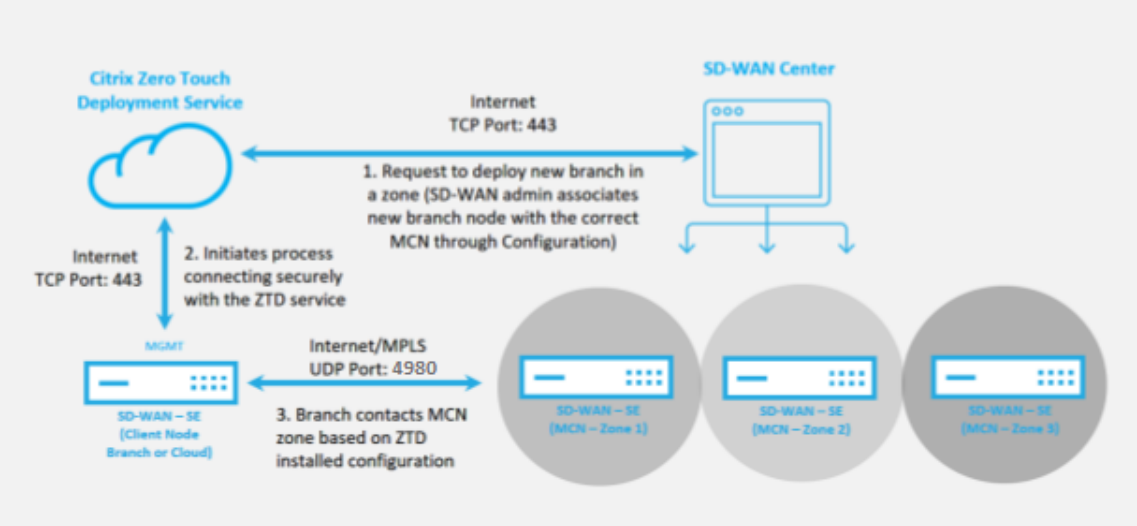
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 en cada modelo, así que consulte la documentación para identificar los datos y los puertos de administración.



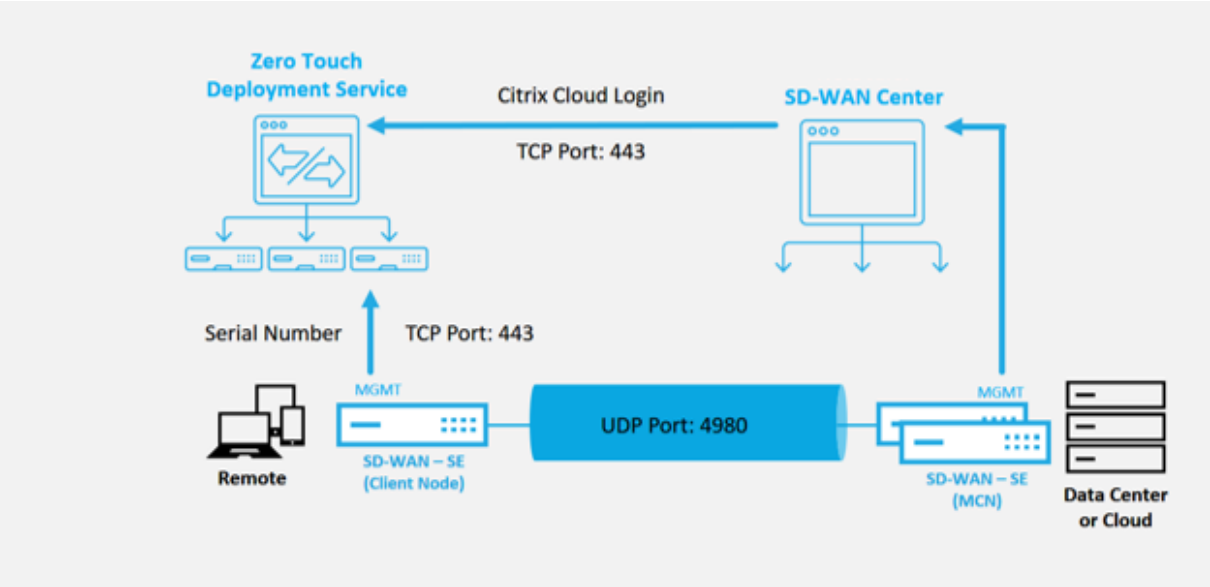
Se requieren los siguientes requisitos previos antes de iniciar cualquier servicio Zero Touch Deployment:

- Ejecución activa de SD-WAN promovida a Master Control Nodo (MCN).
- Ejecutar activamente SD-WAN Center con conectividad al MCN a través de Ruta Virtual.
- 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Conectividad de red de administración (SD-WAN Center y SD-WAN Appliance) a Internet en el puerto 443, ya sea directamente o a través de un servidor proxy.
- (opcional) Al menos un dispositivo SD-WAN que se ejecuta activamente en una sucursal en modo cliente con conectividad de ruta virtual válida a MCN para ayudar a validar el establecimiento de rutas correctas en la red subyacente existente.

El último requisito previo no es un requisito, pero permite al administrador de SD-WAN validar que la red de calcos subyacentes permite establecer rutas virtuales cuando se completa la implementación Zero Touch 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:

El servicio Zero Touch Deployment Service funciona en conjunto con el SD-WAN Center para facilitar la implementación de los dispositivos SD-WAN de sucursales. SD-WAN Center se configura y utiliza como herramienta de administración central para los dispositivos SD-WAN Standard y Enterprise (Premium) Edition. Para utilizar Zero Touch Deployment Service (o servicio en la nube de implementación sin intervención), un administrador debe comenzar por implementar el primer dispositivo SD-WAN en el entorno y, a continuación, configurar e implementar el SD-WAN Center como punto central de administración. Cuando el SD-WAN Center, versión 9.1 o posterior, se instala con conectividad a Internet pública en el puerto 443, SD-WAN Center inicia automáticamente el servicio en la nube e instala los componentes necesarios para desbloquear las funciones de implementación Zero Touch y hacer que la opción Zero Touch Deployment esté disponible en el GUI de SD-WAN Center. Zero Touch Deployment no está disponible de forma predeterminada en el software SD-WAN Center. Se ha diseñado específicamente para garantizar que los componentes preliminares adecuados de la red subyacente estén presentes antes de permitir que un administrador inicie cualquier actividad in situ que implique

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la implementación sin intervención.

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. Con SD-WAN Center capaz de comunicarse con el servicio de implementación sin contacto, la GUI expone las opciones de implementación Zero Touch en la ficha **Configuración**. Al iniciar sesión en Zero Touch Service, se autentica el ID de cliente asociado con el entorno SD-WAN concreto y se registra SD-WAN Center, además de desbloquear la cuenta para una mayor autenticación de las implementaciones de dispositivos de implementación sin contacto.

Con la herramienta Configuración de red de SD-WAN Center, el administrador de SD-WAN deberá utilizar las plantillas o la capacidad de clonar sitio para crear la configuración de SD-WAN y agregar nuevos sitios. SD-WAN Center utiliza la nueva configuración para iniciar la implementación de la implementación sin contacto para los sitios recién agregados. 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.

Zero Touch Deployment Cloud Service 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 sucursal validando el número de serie.
- Autenticar que el Administrador de SD-WAN aceptó el sitio para la implementación sin contacto mediante SD-WAN Center.
- Extraiga el archivo de configuración específico para el dispositivo de destino del SD-WAN Center.
- Inserte el archivo de configuración específico del dispositivo de destino en el dispositivo de sucursal.
- Instale el archivo de configuración en el dispositivo de sucursal.
- Inserte los componentes de software de SD-WAN que falten o las actualizaciones necesarias en el dispositivo de sucursal.

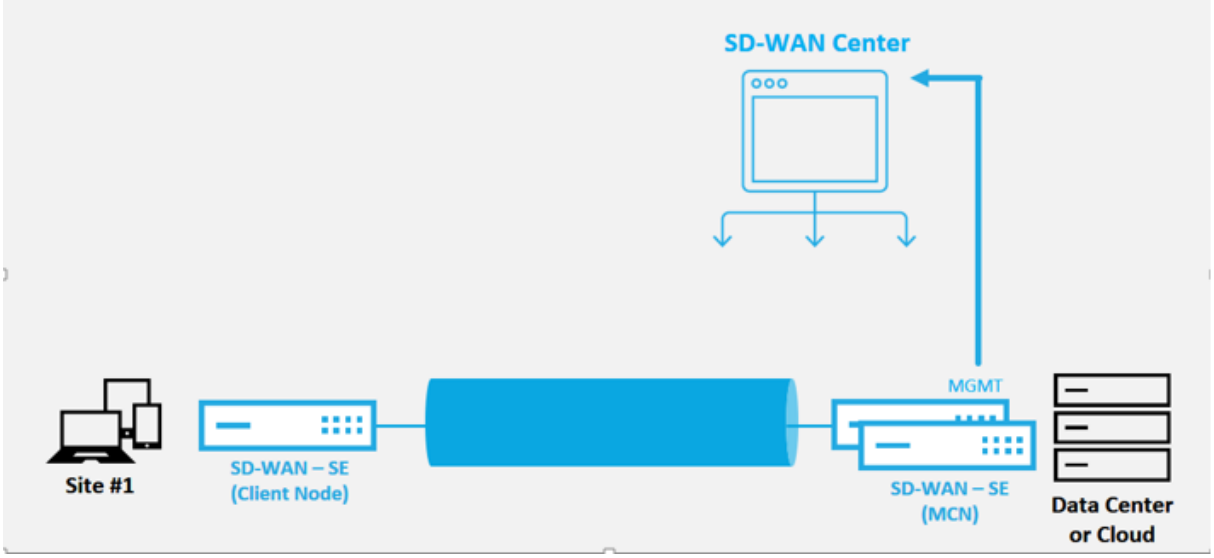
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Inserte un archivo de licencia temporal de 10 Mbps para confirmar el establecimiento de la ruta virtual en el dispositivo de sucursal.
- Habilite el servicio SD-WAN en el dispositivo de sucursal.

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

Procedimiento de dispositivo de implementación cero táctil

En el siguiente procedimiento se detallan los pasos necesarios para implementar un nuevo sitio mediante el servicio de implementación Zero Touch. Tener un MCN en ejecución y un nodo cliente ya funcionando con una comunicación adecuada con SD-WAN Center y establecieron rutas virtuales que confirmen la conectividad a través de la red subyacente. Se requieren los siguientes pasos del Administrador de SD-WAN para iniciar la implementación de Zero Touch:



Cómo configurar el servicio de implementación Zero Touch

El SD-WAN Center tiene la funcionalidad de aceptar solicitudes de dispositivos recién conectados para unirse a la red SD-WAN Enterprise. La solicitud se reenvía a la interfaz web a través del servicio de implementación sin contacto. Una vez que el dispositivo se conecta al servicio, se descargan los paquetes de configuración y actualización de software.

flujo de trabajo de configuración:

- Acceda a **SD-WAN Center** > **Crear nueva configuración de sitio** o Importe la configuración existente y guárdela.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Inicie sesión en Citrix Workspace para habilitar el servicio de implementación sin intervención. La opción de menú Implementación Zero Touch ahora se muestra en la interfaz de administración web de SD-WAN Center.
- En SD-WAN Center, vaya a **Configuración** > **Implementación sin intervención** > **Implementar nuevo sitio**.
- Seleccione un dispositivo, haga clic en **Habilitar**y haga clic en**Implementar**.
- El instalador recibe el correo electrónico de activación > Introduzca el número de serie > **Activar** > El dispositivo se ha implementado correctamente.

Para configurar el servicio Zero Touch Deployment:

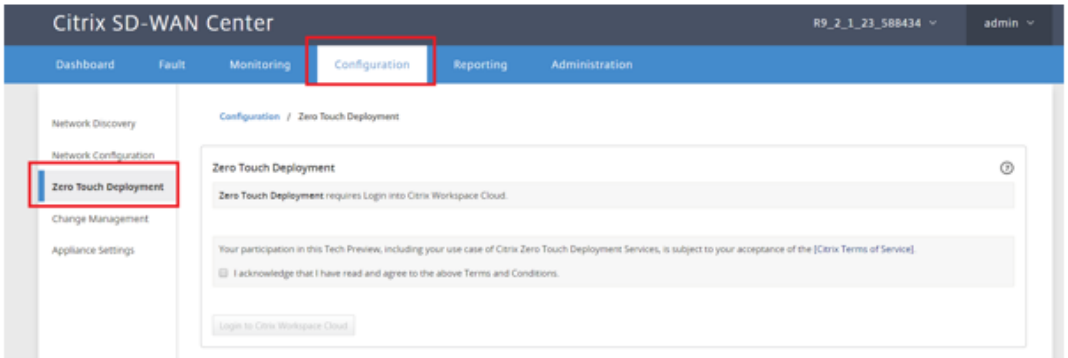
1. Instale SD-WAN Center con capacidades de implementación cero táctil habilitadas:

   a) Instale SD-WAN Center con la dirección IP asignada por DHCP.

   b) Verifique que SD-WAN Center asigne una dirección IP de administración adecuada y una dirección DNS de red con conectividad a Internet pública a través de la red de administración.

   c) Actualice el SD-WAN Center a la versión más reciente del software de SD-WAN.

   d) Con una conectividad a Internet adecuada, el SD-WAN Center inicia el servicio en la nube de implementación sin intervención y descarga e instala automáticamente cualquier actualización de firmware específica para la implementación sin intervención; si este procedimiento de Call Home falla, la siguiente opción de implementación sin contacto no estará disponible en la GUI.



   e) Lea los Términos y Condiciones y, a continuación, seleccione **Reconozco que he leído y acepto los Términos y Condiciones anteriores**.

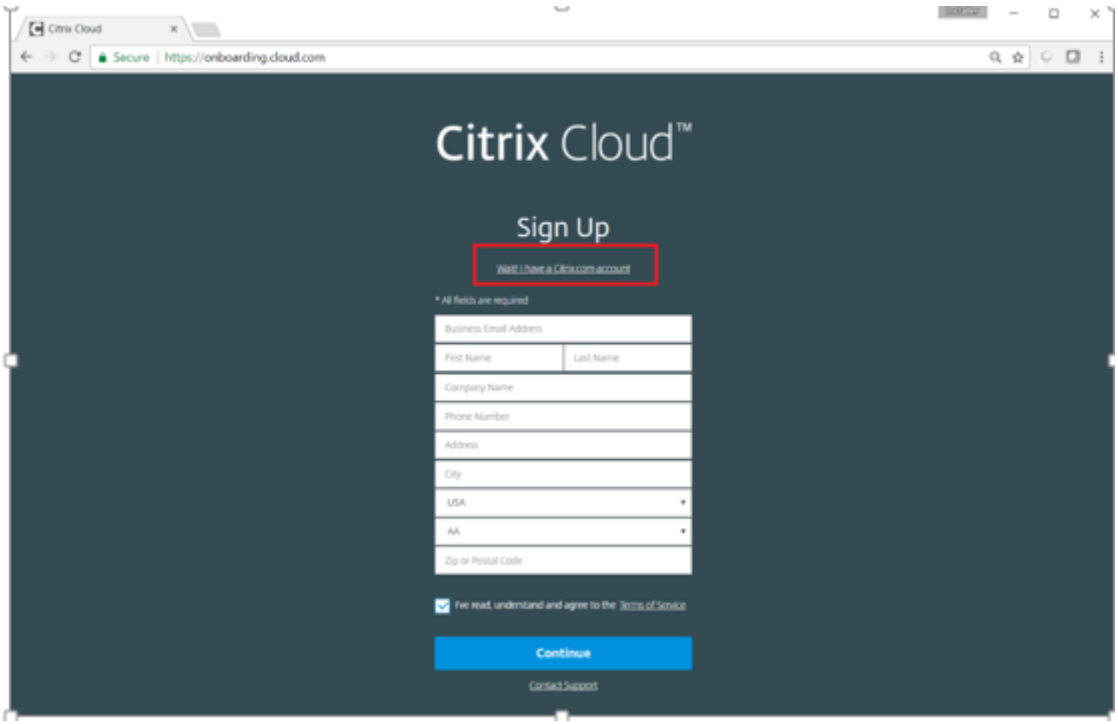
   f) Haga clic en el botón **Iniciar sesión en Citrix Workspace Cloud** si ya se ha creado una cuenta de Citrix Cloud.

   g) Inicie sesión en la cuenta de Citrix Cloud y, tras recibir el siguiente mensaje de inicio de sesión correcto, **NO CIERRE ESTA VENTANA, EL PROCESO REQUIERE UNOS 20 SEGUN-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

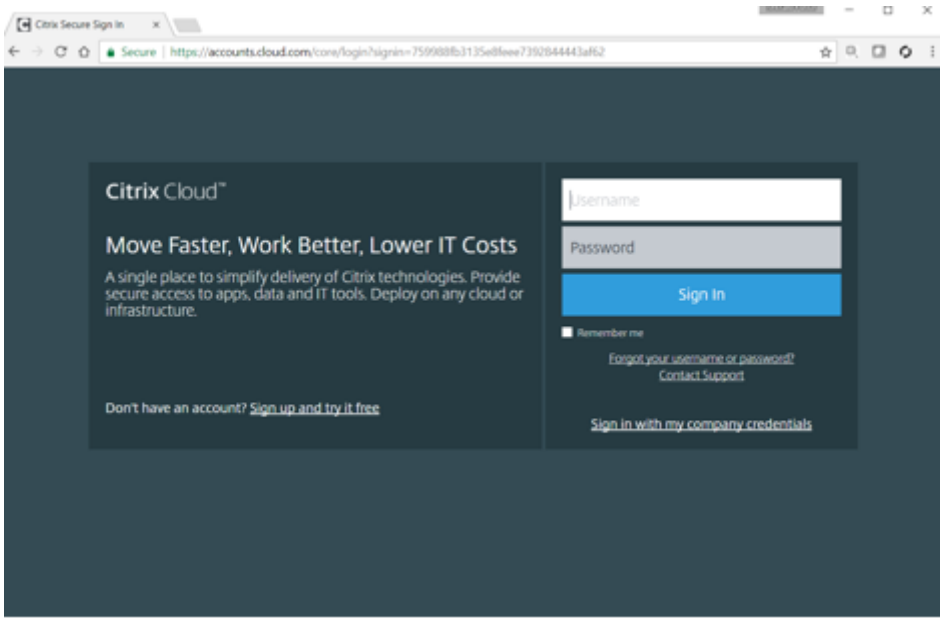
DOS MÁS PARA QUE SE ACTUALICE LA INTERFAZ GRÁFICA DE USUARIO DE SD-WAN CENTER. La ventana debe cerrarse por sí sola cuando esté completa.

2. Para crear una cuenta de inicio de sesión en Cloud, siga el procedimiento siguiente: Abra un explorador web en https://onboarding.cloud.com
3. Haga clic en el enlace de **Esperar, tengo una cuenta de Citrix.com**.



4. Inicie sesión con una cuenta Citrix existente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Una vez iniciado sesión en la página SD-WAN Center Zero Touch Deployment, es posible que observe que no hay sitios disponibles para la implementación sin contacto debido a las siguientes razones:

   - La configuración activa no se ha seleccionado en el menú desplegable Configuración
   - Todos los sitios de la configuración activa actual ya se han implementado
   - La configuración no se creó mediante SD-WAN Center, sino el Editor de configuración disponible en el MCN
   - Los sitios no se crearon en la configuración que hace referencia a dispositivos compatibles con cero contacto (por ejemplo, 410-SE, 2100-SE, Cloud VPX)

6. Actualice la configuración para agregar un **nuevo sitio remoto** con un **dispositivo SD-WAN compatible con ZTD** mediante SD-WAN Center Network Configuration.

   Si la configuración de SD-WAN no se creó mediante la configuración de red de SD-WAN Center, importe la configuración activa desde el MCN y comience a modificar la configuración mediante SD-WAN Center. Para la capacidad de implementación de Zero Touch, el administrador de SD-WAN debe crear la configuración mediante SD-WAN Center. Se debe utilizar el siguiente procedimiento para agregar un nuevo sitio destinado a la implementación sin contacto.

   a) Diseñe el nuevo sitio para la implementación del dispositivo SD-WAN describiendo primero los detalles del nuevo sitio (es decir, el modelo del dispositivo, el uso de grupos de interfaz, las direcciones IP virtuales, los enlaces WAN con ancho de banda y sus puertas de enlace respectivas).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

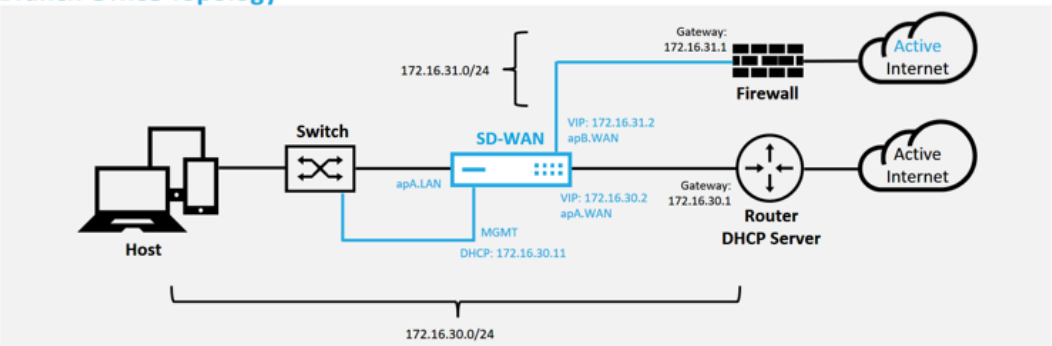
Importante

Es posible que observe también en la lista cualquier nodo de sitio que tenga VPX seleccionado como modelo, pero actualmente el soporte de implementación sin contacto solo está disponible para la instancia de AWS VPX.

Nota

- Asegúrese de utilizar un explorador web compatible con Citrix SD-WAN Center
- Asegúrese de que el explorador web no bloquea ninguna ventana emergente durante el inicio de sesión de Citrix Workspace

Branch Office Topology



Este es un ejemplo de implementación de un sitio de sucursal, el dispositivo SD-WAN se implementa físicamente en la ruta del enlace WAN MPLS existente a través de una red 172.16.30.0/24 y mediante un enlace de respaldo existente al habilitarlo en un estado activo y terminar ese segundo enlace WAN directamente en la SD-WAN dispositivo en una subred diferente 172.16.31.0/24.

Nota

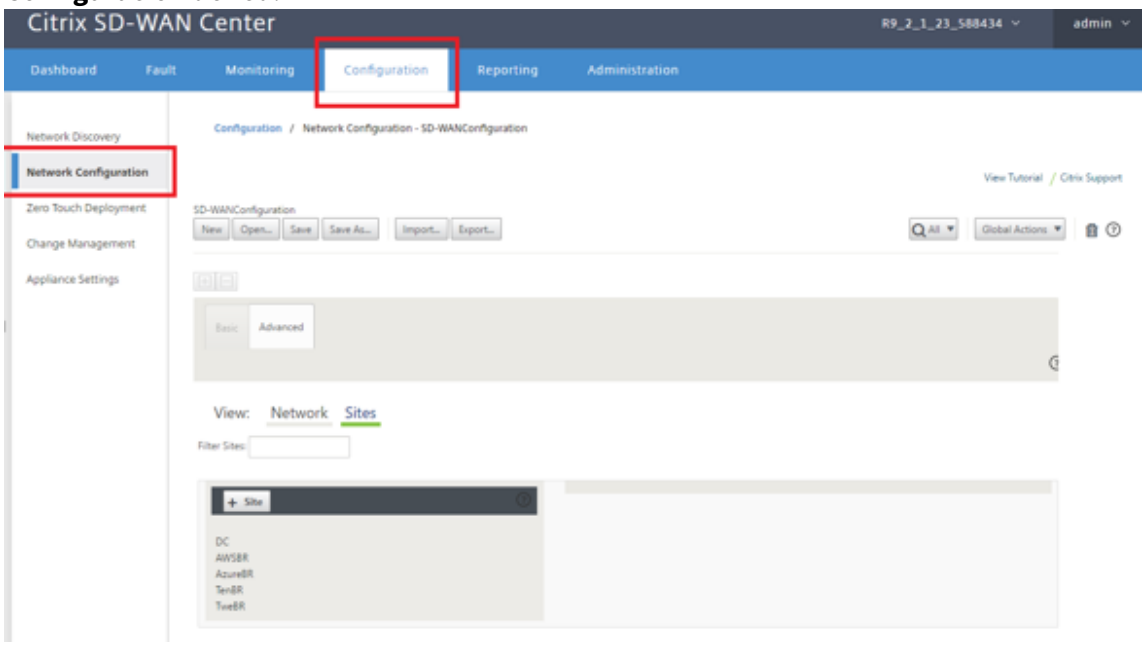
Los dispositivos SD-WAN asignan automáticamente una dirección IP predeterminada 192.168.100.1/16. Si DHCP está habilitado de forma predeterminada, el servidor DHCP de la red puede proporcionar al dispositivo una segunda dirección IP en una subred que se superponga a la predeterminada. Esto puede provocar un problema de redirección en el dispositivo en el que el dispositivo podría no conectarse al servicio en la nube de implementación sin contacto. Configure el servidor DHCP para asignar direcciones IP fuera del rango 192.168.0.0/16.

Hay varios modos de implementación diferentes disponibles para la colocación de productos SD-WAN en una red. En el ejemplo anterior, SD-WAN se está implementando como una superposición sobre la infraestructura de red existente. Para los nuevos sitios, los administradores de SD-WAN pueden optar por implementar la SD-WAN en modo Edge o Gateway, lo que elimina la necesidad de un enrutador perime-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> tral WAN y un firewall, y consolida las necesidades de red de la redirección perimetral y el firewall en la solución SD-WAN.

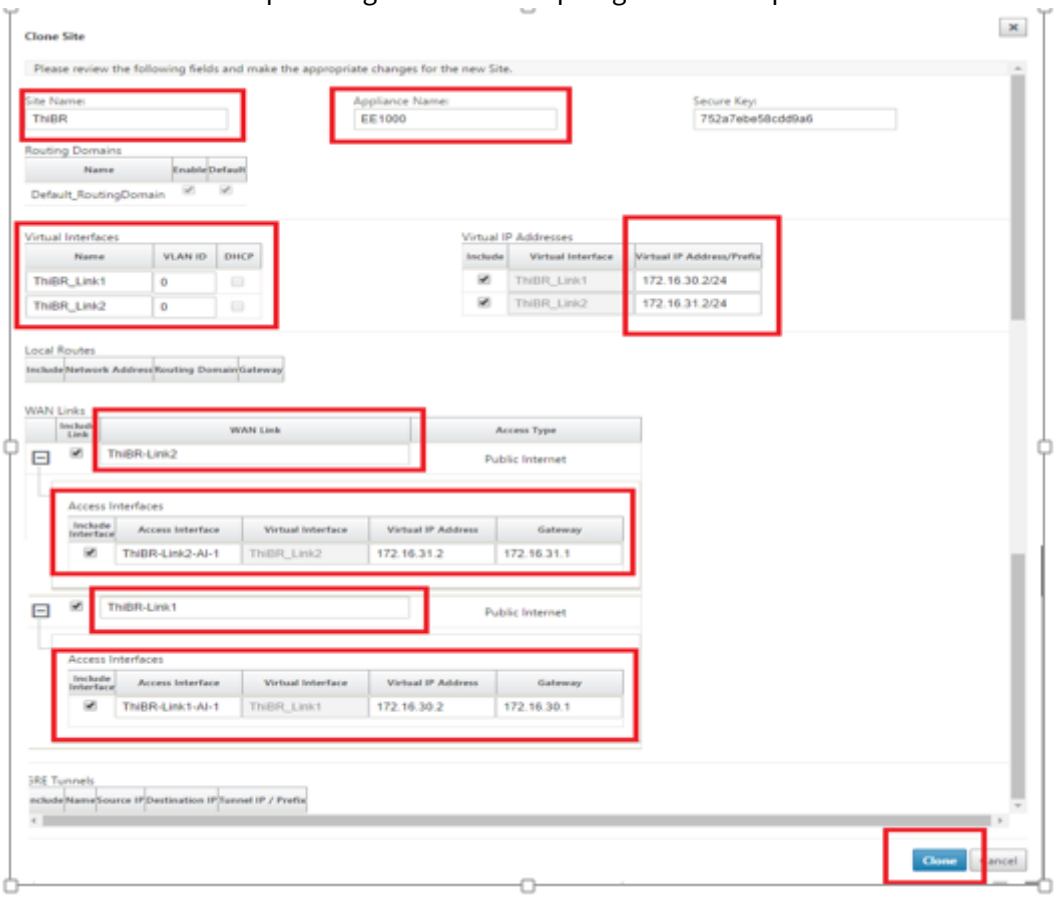
7. Abra la interfaz de administración web de SD-WAN Center y vaya a la página **Configuración** > **Configuración de red**.



8. Asegúrese de que ya existe una configuración en funcionamiento o importe la configuración desde el MCN.
9. Vaya a la ficha Avanzado para crear un sitio.
10. Abra el icono Sitios para mostrar los sitios configurados actualmente.
11. Construya rápidamente la configuración del nuevo sitio mediante la función de clonación de cualquier sitio existente.

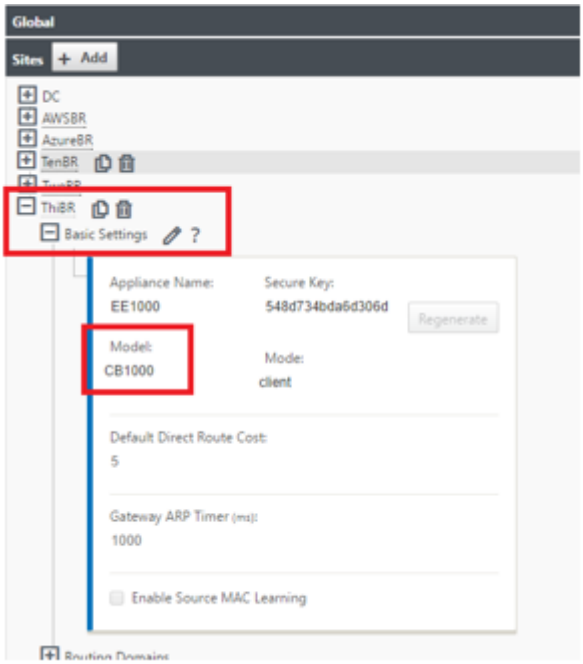
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

12. Rellene todos los campos obligatorios de la topología diseñada para esta nueva sucursal



13. Después de clonar un sitio nuevo, navegue hasta la **configuración básica**del sitio y verifique que el modelo de SD-WAN esté seleccionado correctamente, lo que admitiría el servicio de contacto cero.

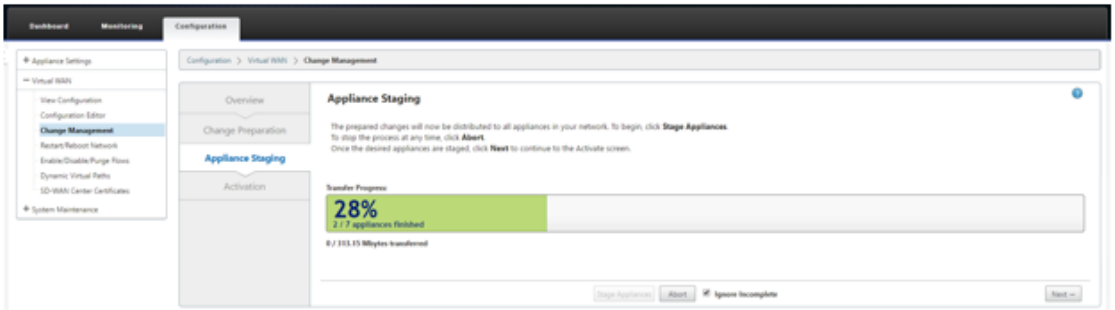
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



El modelo SD-WAN del sitio se puede actualizar, pero tenga en cuenta que los grupos de interfaces pueden tener que redefinirse, ya que el dispositivo actualizado puede tener un diseño de interfaz nuevo que el que se utilizó para clonar.

14. Guarde la nueva configuración en SD-WAN Center y utilice la opción Exportar a la **bandeja de entrada de Change Management** para insertar la configuración mediante Change Management.

15. Siga el procedimiento de administración de cambios para preparar correctamente la nueva configuración, lo que hace que los dispositivos SD-WAN existentes conozcan el nuevo sitio que se va a implementar sin tocar, debe usar la opción “Ignorar incompleto”para omitir el intento de enviar la configuración al nuevo sitio que aún debe pasar el flujo de trabajo de implementación sin intervención.



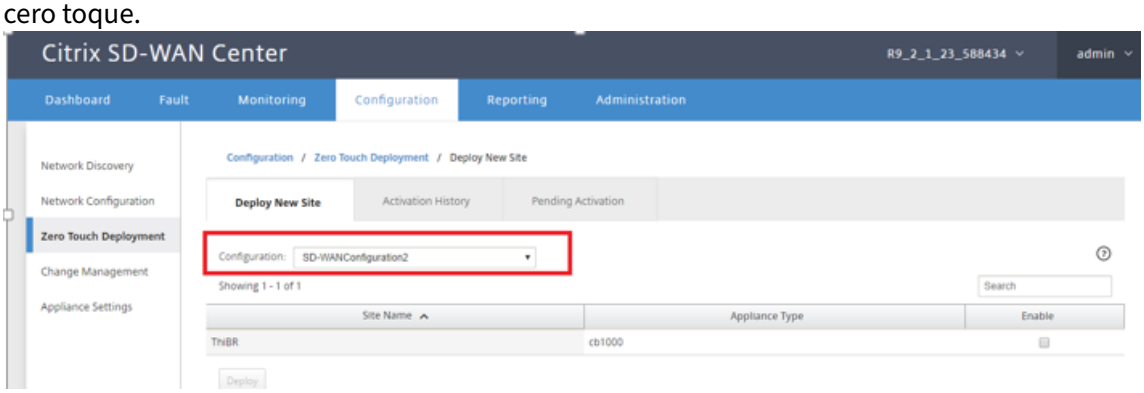
16. Vuelva a la página SD-WAN Center Zero Touch Deployment y, con la nueva configuración activa en ejecución, el nuevo sitio estará disponible para su implementación.

17. En la página Zero Touch Deployment, en la ficha **Implementar nuevo sitio**, seleccione el

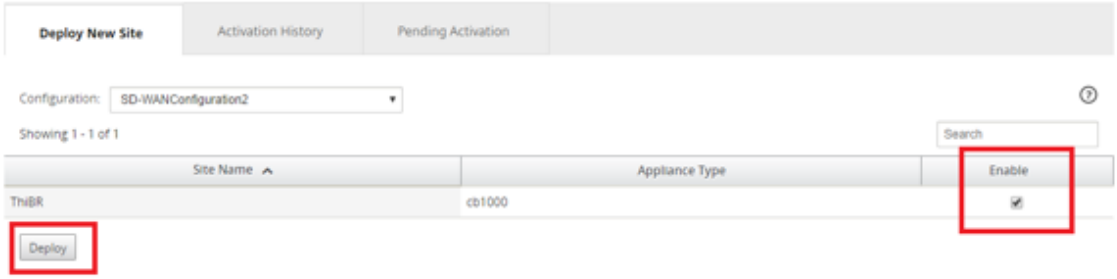
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

archivo de configuración de red en ejecución

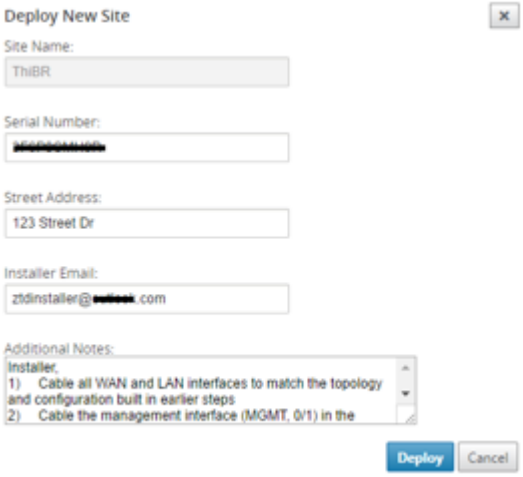
18. Después de seleccionar el archivo de configuración en ejecución, se mostrará la lista de todos los sitios de sucursales con dispositivos SD-WAN no implementados que son compatibles con cero toque.



19. Seleccione los sitios de sucursales que desee configurar para el servicio Zero Touch, haga clic en **Habilitar**y, a continuación, haga clic en **Implementar**.



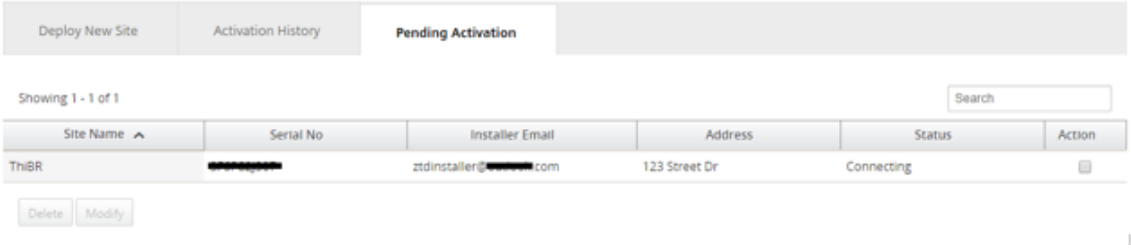
20. Aparece una ventana emergente Implementar nuevo sitio, en la que el administrador puede proporcionar el número de serie, la dirección de calle del sitio de la sucursal, la dirección de correo electrónico del instalador y más notas, si es necesario.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> El campo de entrada Número de serie es opcional y, dependiendo de si se rellena o no, dará lugar a un cambio en la actividad in situ de la que es responsable el instalador.
>
> ```
> >\-  Si se rellena el campo Número de serie — No es necesario que el instalador introduzca el número de serie en la URL de activación generada con el comando del sitio de implementación
> >
> >\-  Si el campo Número de serie se deja en negro — El instalador se encargará de introducir en el número de serie correcto del dispositivo en la URL de activación generada con el comando deploy site
> ```

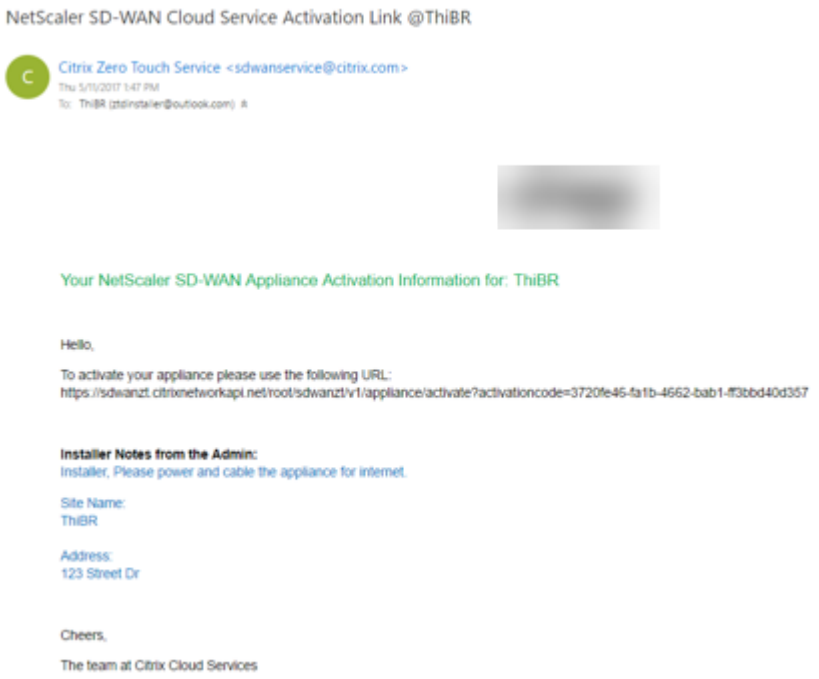
21. Después de hacer clic en el botón **Implementar**, aparecerá un mensaje indicando que “La configuración del sitio se ha implementado.”Esta acción desencadena SD-WAN Center, que anteriormente se registró con el servicio en la nube de implementación sin contacto, para compartir la configuración de este sitio en particular para que se almacene la temporalidad en el servicio en la nube de implementación sin contacto.
22. Acceda a la ficha Activación pendiente para confirmar que la información del sitio de la sucursal se rellenó correctamente y se puso en un estado de actividad del instalador pendiente.



> **Nota**
>
> Opcionalmente, se puede elegir una implementación de cero toque en el estado Pendiente de activación para Eliminar o Modificar, si la información es incorrecta. Si se elimina un sitio de la página de activación pendiente, estará disponible para su implementación en la página de ficha Implementar nuevo sitio. Una vez que elija eliminar el sitio de la sucursal de Activación pendiente, el enlace de activación enviado al instalador se convierte en inválido.
>
> Si el administrador de SD-WAN no ha rellenado el campo Número de serie, el campo Estado indica “Esperando al instalador”en lugar de “Conexión”. “

23. La siguiente serie de actividades la realiza el instalador in situ.
    a) El instalador comprueba el buzón de correo para la dirección de correo electrónico que el administrador de SD-WAN utilizó al implementar el sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) Abra la URL de activación de implementación sin intervención en una ventana del explorador de Internet.

c) Si el administrador de SD-WAN no rellenó previamente el número de serie en el paso del sitio de implementación, el instalador será responsable de localizar el número de serie en el dispositivo físico e introducir el número de serie manualmente en la URL de activación y, a continuación, haga clic en el botón **Activar**.

d) Si el administrador rellenando previamente la información del número de serie, la URL de activación ya habrá progresado al siguiente paso.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) El instalador debe estar físicamente in situ para realizar las siguientes acciones:

- Cable todas las interfaces WAN y LAN para que coincidan con la topología y la configuración incorporadas en los pasos anteriores.
- Conecte la interfaz de administración (MGMT, 0/1) en el segmento de la red que proporciona la dirección IP DHCP y la conectividad a Internet con DNS y FQDN a la resolución de direcciones IP.
- Cable de alimentación del dispositivo SD-WAN.
- Encienda el interruptor de encendido del dispositivo.

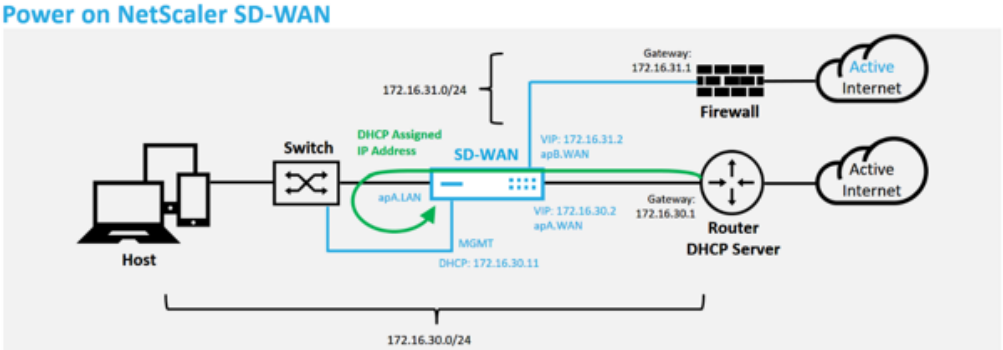
> **Nota**
>
> La mayoría de los dispositivos se encenderán automáticamente cuando el cable de alimentación esté conectado. Es posible que algunos dispositivos tengan que encenderse mediante el interruptor de encendido de la parte frontal del dispositivo, mientras que otros pueden tener el interruptor de encendido en la parte posterior del dispositivo. Algunos interruptores de encendido requieren mantener presionado el botón de encendido hasta que la unidad se encienda.

24. La siguiente serie de pasos se automatizan con la ayuda del servicio Zero Touch Deployment, pero requiere que estén disponibles los siguientes requisitos previos.

    - El dispositivo de sucursal debe estar encendido
    - DHCP debe estar disponible en la red existente para asignar la administración y la dirección IP DNS
    - Cualquier dirección IP asignada DHCP requiere conectividad a Internet con capacidad para resolver FQDN
    - La asignación de IP se puede configurar manualmente, siempre que se cumplan los demás requisitos previos

      a) El dispositivo obtiene una dirección IP del servidor DHCP de la red. En esta topología de ejemplo, esto se logra mediante las interfaces de datos omitidas de un dispositivo de estado predeterminado de fábrica.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

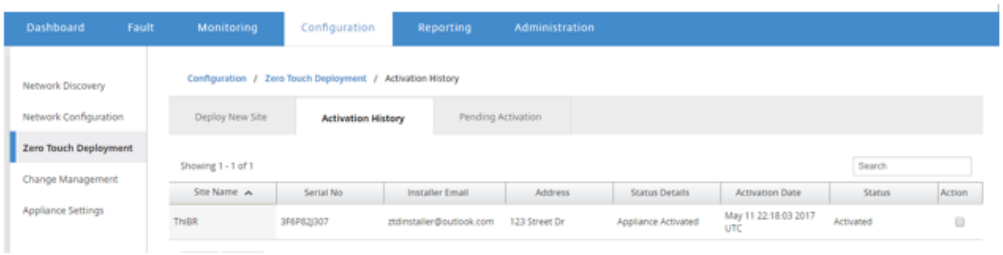


b) A medida que el dispositivo obtiene la administración web y las direcciones IP DNS del servidor DHCP de red de calco subyacente, el dispositivo inicia el servicio de implementación Zero Touch y descarga cualquier actualización de software relacionada con la implementación sin contacto.

c) Con una conectividad correcta con el servicio en la nube de implementación sin contacto, el proceso de implementación realiza automáticamente lo siguiente:

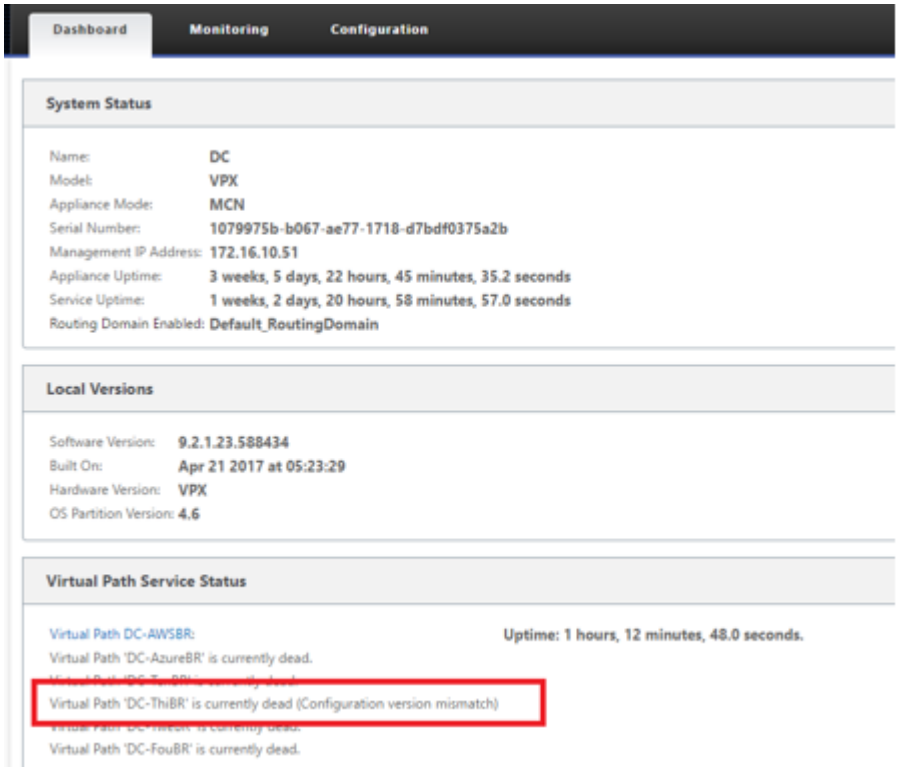
- Descargue el archivo de configuración almacenado anteriormente por el Centro de SD-WAN
- Aplicación de la configuración al dispositivo local
- Descargar e instalar un archivo de licencia temporal de 10 MB
- Descargue e instale las actualizaciones de software si es necesario
- Activar el servicio SD-WAN

d) Se puede realizar una confirmación adicional en la interfaz de administración web de SD-WAN Center; en el menú Implementación táctil se muestran los dispositivos activados correctamente en la ficha **Historial de activación**.

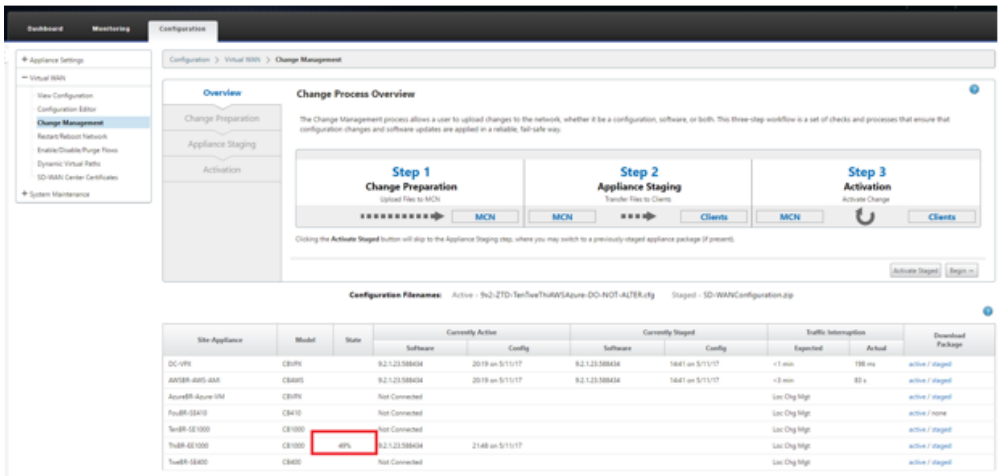


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) Es posible que las rutas virtuales no se muestren inmediatamente en un estado conectado porque es posible que el MCN no confíe en la configuración transmitida desde el Cloud Service de implementación sin intervención e informa de que la versión de configuración no coincide en el panel de control de MCN.

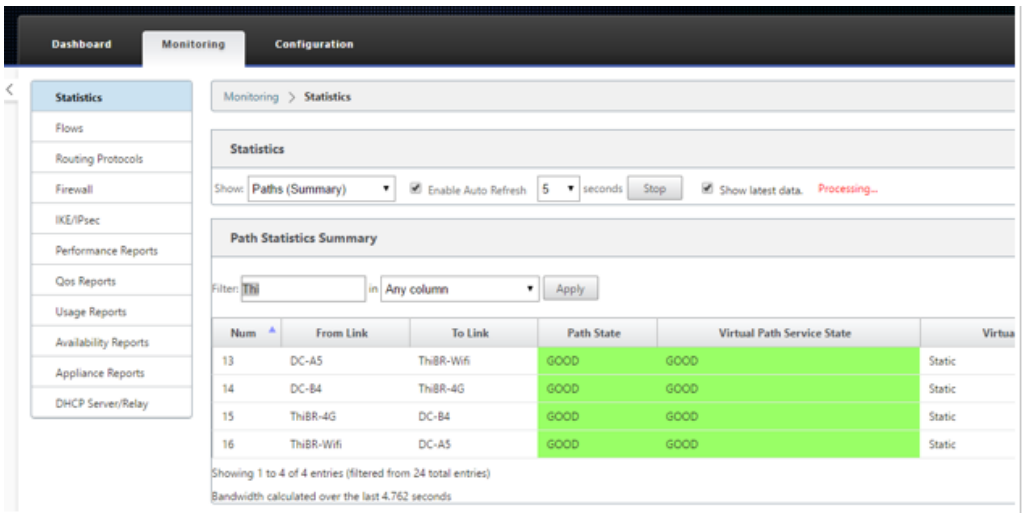


f) La configuración se vuelve a entregar al dispositivo de sucursal recién instalado y el estado se supervisa en la página **MCN** > **Configuración** > **WAN virtual** > **Administración de cambios** (este proceso puede tardar varios minutos en completarse).

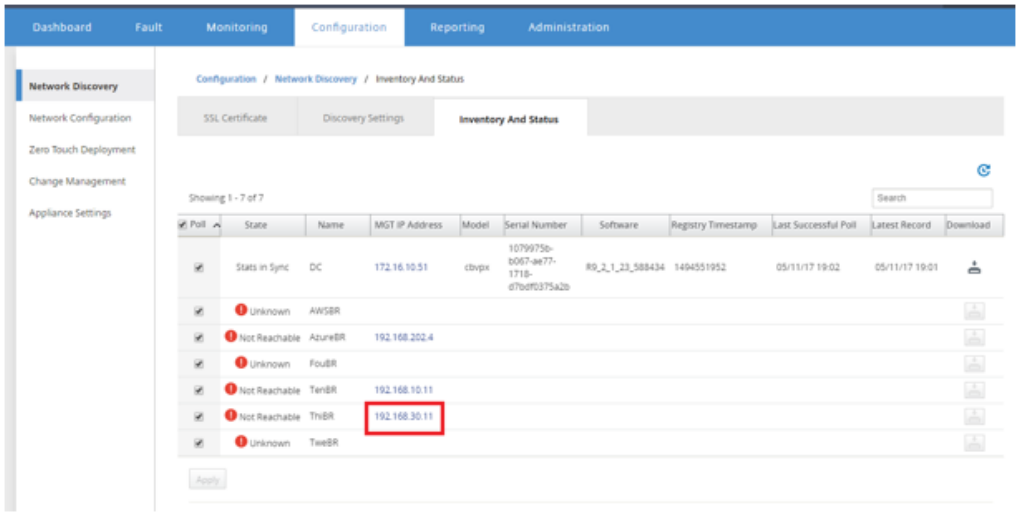


g) El Administrador de SD-WAN puede supervisar la página de administración web de MCN de cabecera para las rutas virtuales establecidas del sitio remoto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

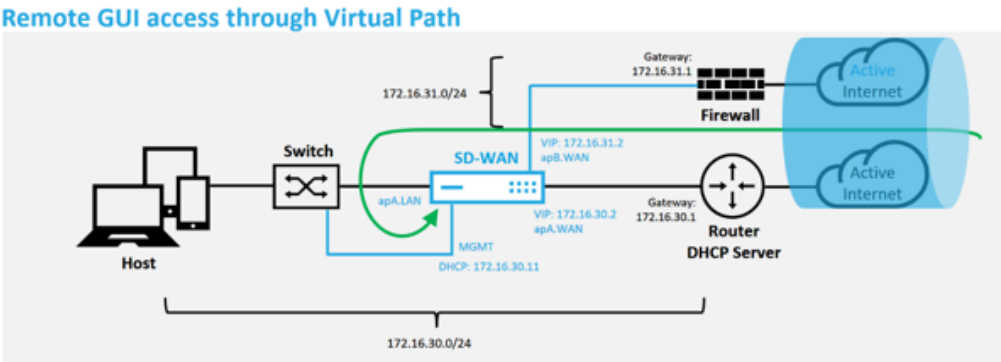


h) SD-WAN Center también se puede utilizar para identificar la dirección IP asignada por DHCP del dispositivo in situ en la página **Configuración** > **Detección de redes** > **Inventario y estado**.

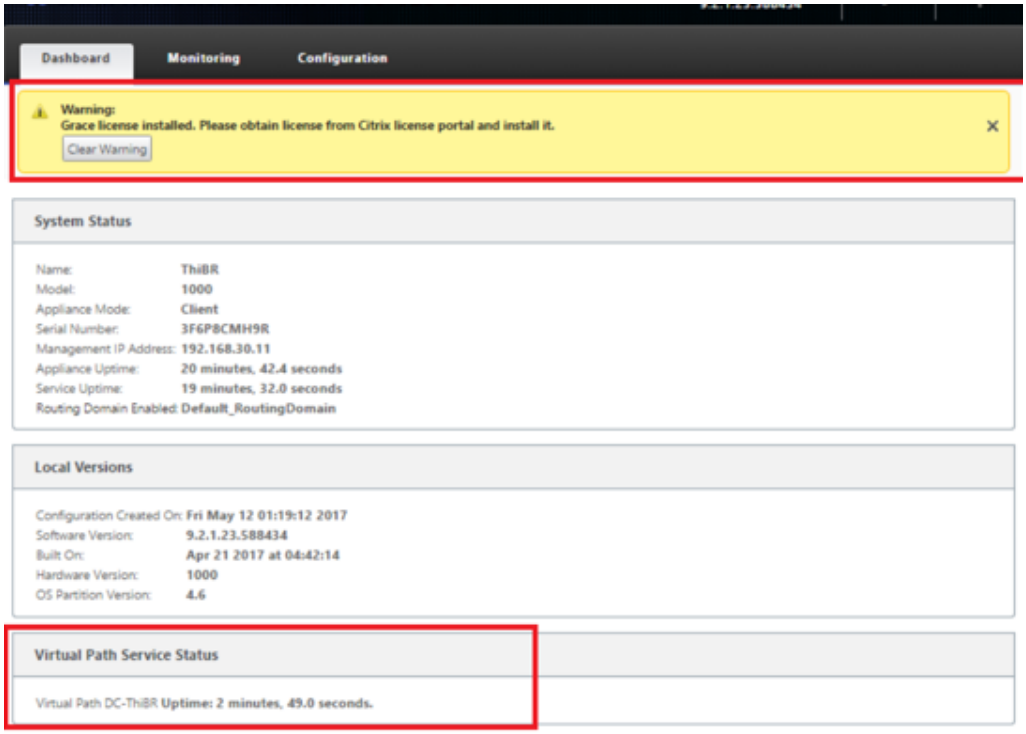


i) En este punto, el administrador de red de SD-WAN puede obtener acceso a la administración web del dispositivo in situ mediante la red superpuesta SD-WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

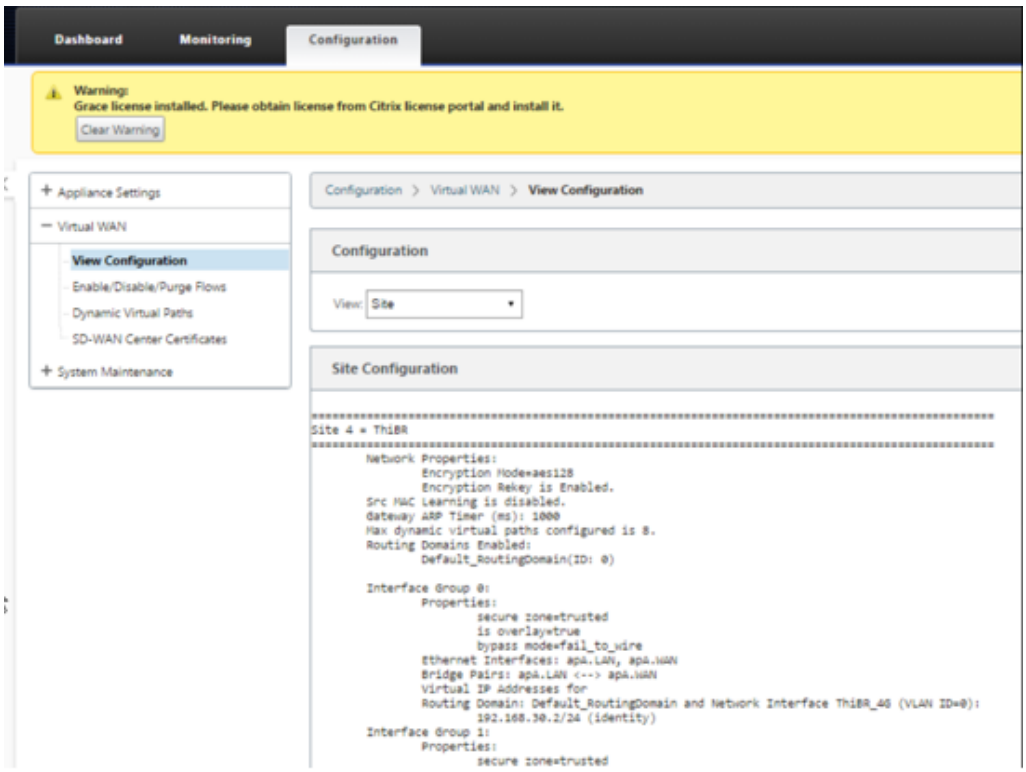


j) El acceso de administración web al dispositivo de sitio remoto indica que el dispositivo se ha instalado con una licencia Grace temporal a 10 Mbps, lo que permite que el estado del servicio de ruta virtual se informe como activo.

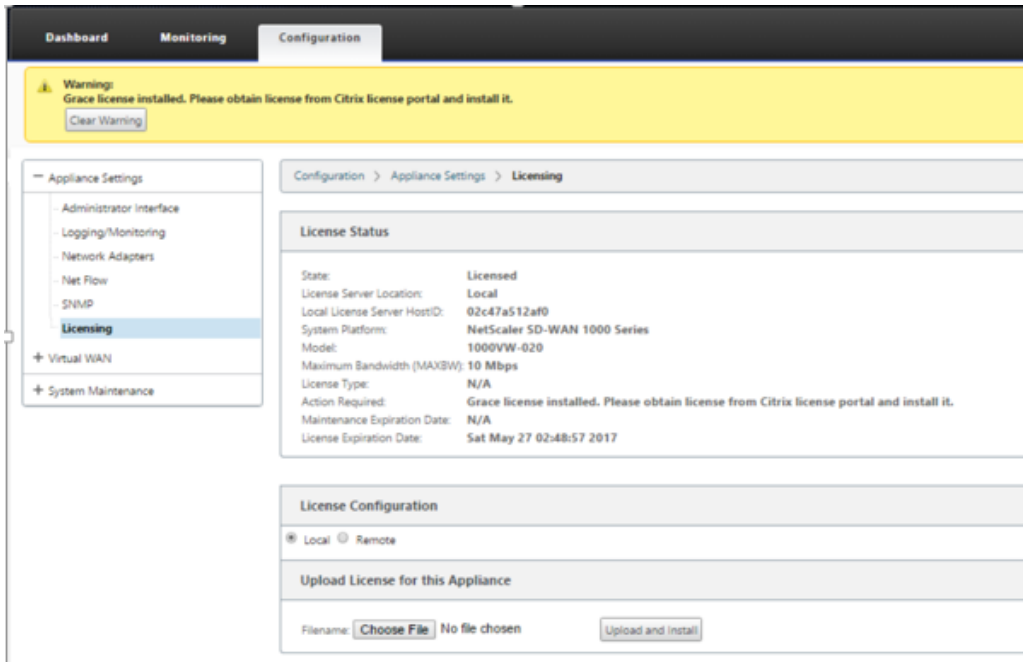


k) La configuración del dispositivo se puede validar mediante la página **Configuración** > **WAN virtual** > **Ver configuración**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



l) 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 banner de advertencia de licencia de Grace desaparece y durante el proceso de instalación de la licencia no se producirá pérdida de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

conectividad con el sitio remoto (cero pings se eliminan).

Zero Touch local

May 7, 2021

Para obtener instrucciones acerca de cómo implementar un dispositivo SD-WAN con servicio Zero Touch, consulte el tema Cómo configurar el servicio de implementación Zero Touch.

AWS

May 7, 2021

En las secciones siguientes se describe cómo implementar ZTD en un entorno de AWS.

Implementación en AWS:

Con la versión 9.3 de SD-WAN, las capacidades de implementación de Zero Touch se han extendido a las instancias de la nube. El procedimiento para implementar el proceso de implementación sin contacto cuatro instancias en la nube es ligeramente diferente de la implementación de dispositivos para el servicio sin contacto.

1. Actualice la configuración para agregar un nuevo sitio remoto con un dispositivo en la nube SD-WAN compatible con ZTD mediante SD-WAN Center Network Configuration.

   Si la configuración de SD-WAN no se creó mediante la configuración de red de SD-WAN Center, importe la configuración activa desde el MCN y comience a modificar la configuración mediante SD-WAN Center. Para la capacidad de implementación de Zero Touch, el administrador de SD-WAN debe crear la configuración mediante SD-WAN Center. Se debe utilizar el siguiente procedimiento para agregar un nuevo nodo en la nube destinado a la implementación de Zero Touch.

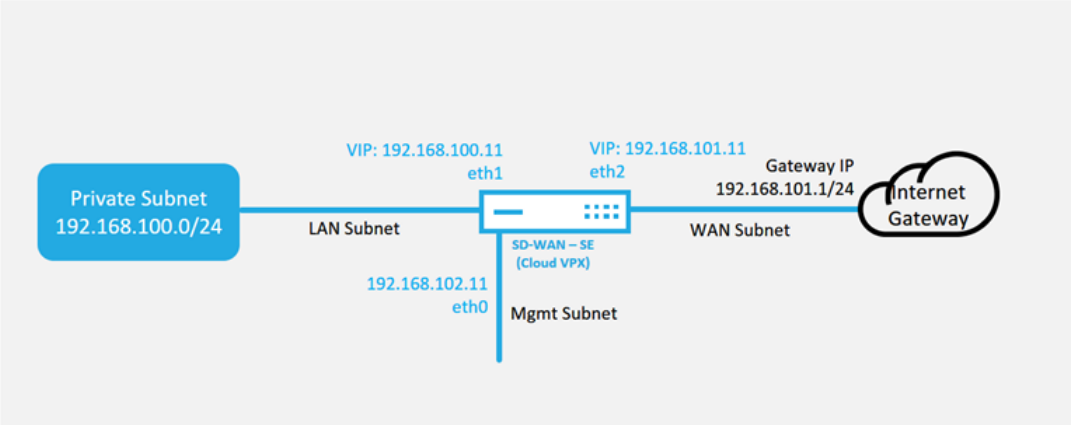
   a) Diseñar el nuevo sitio para la implementación en la nube SD-WAN esbozando primero los detalles del nuevo sitio (es decir, tamaño VPX, uso de grupos de interfaz, direcciones IP virtuales, enlaces WAN con ancho de banda y sus respectivas puertas de enlace).

      > **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: Adminis-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

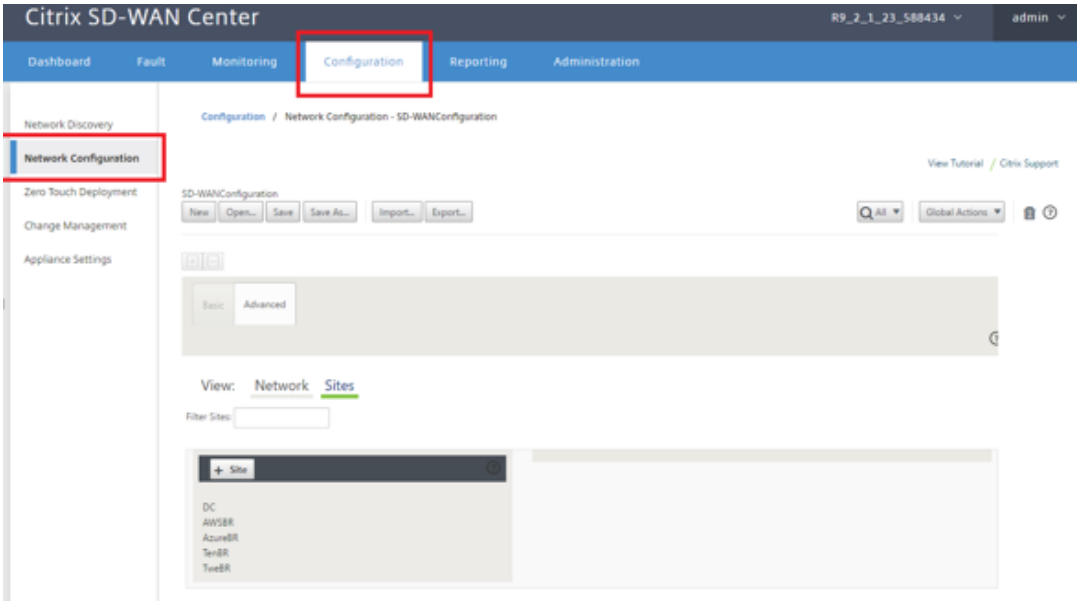
> tración, LAN y WAN (en ese orden).
> - Las plantillas de nube disponibles para SD-WAN VPX están actualmente configuradas para obtener la dirección IP #.#.#.11 de las subredes disponibles en la VPC.

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 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.

b) Abra la interfaz de administración web de SD-WAN Center y vaya a la página **Configuración** > **Configuración de red**.



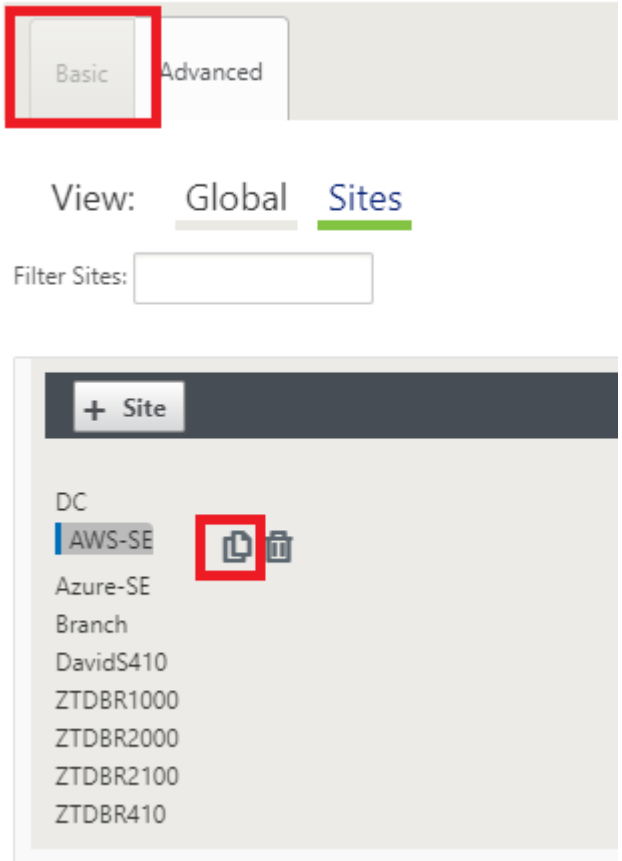
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) Asegúrese de que ya hay una configuración en funcionamiento o importe la configuración desde el MCN.

d) Acceda a la ficha Básico para crear un nuevo sitio.

e) Abra el icono Sitios para mostrar los sitios configurados actualmente.

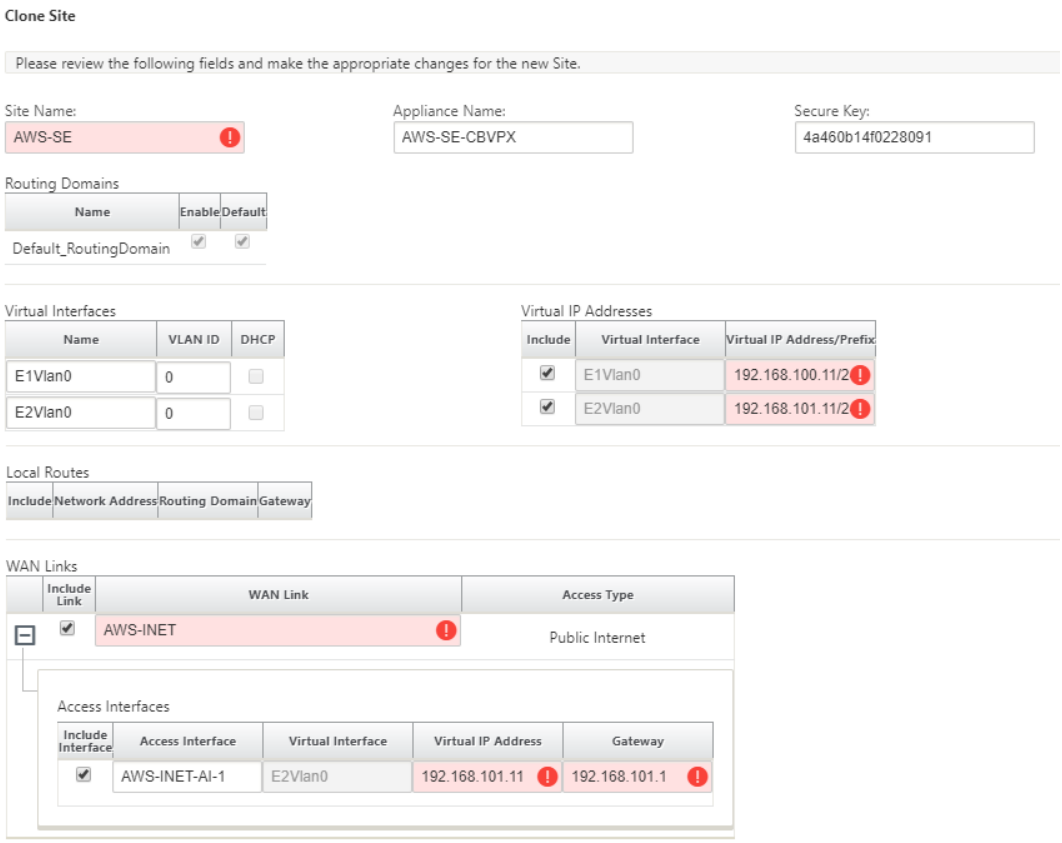
f) Cree rápidamente la configuración para el nuevo sitio en la nube mediante la función de clonación de cualquier sitio existente o cree manualmente un nuevo sitio.



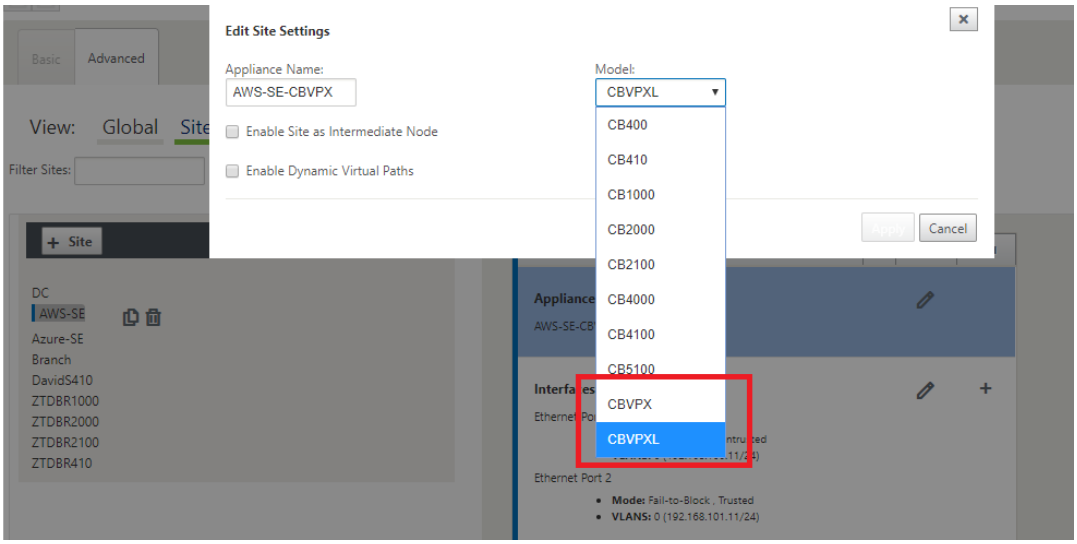
g) Rellene todos los campos requeridos de la topología diseñada anteriormente para este nuevo sitio en la nube

Tenga en cuenta que la plantilla disponible para implementaciones de ZTD en la nube es difícil utilizar la dirección IP #.#.#.11 para las subredes de administración, LAN y WAN. Si la configuración no está definida para que coincida con la dirección de host IP .11 esperada para cada interfaz, el dispositivo no podrá establecer correctamente ARP en las puertas de enlace del entorno de nube y conectividad IP con la ruta virtual del MCN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



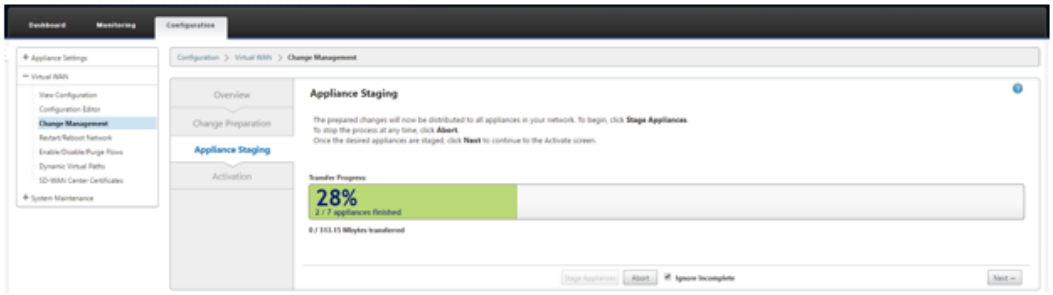
h) Después de clonar un sitio nuevo, desplácese hasta la **Configuración básica** del sitio y verifique que el Modelo de SD-WAN esté seleccionado correctamente, lo que soportaría el servicio Zero Touch.



i) Guarde la nueva configuración en SD-WAN Center y utilice la opción Exportar a la **bandeja de entrada de Change Management** para insertar la configuración mediante Change Management.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

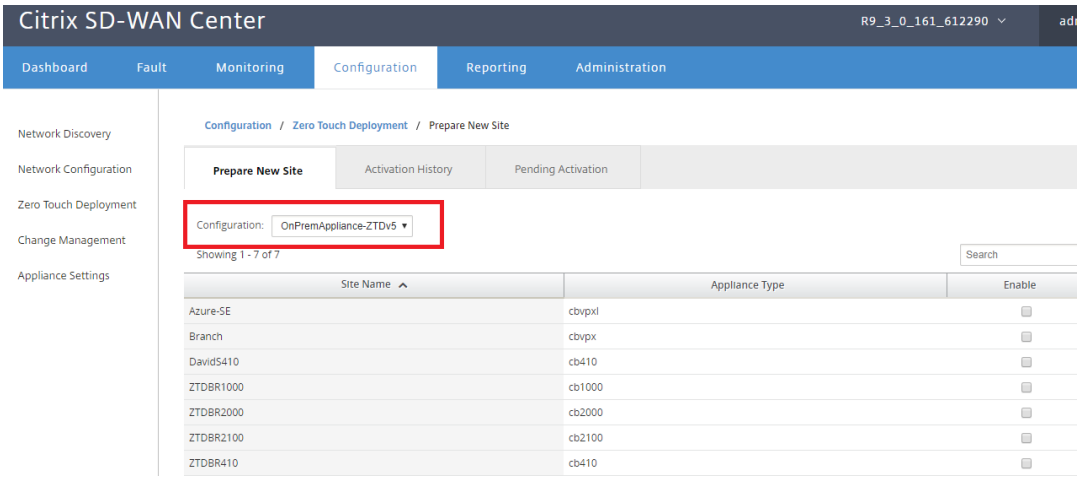
j) Siga el procedimiento de administración de cambios para organizar correctamente la nueva configuración, lo que hace que los dispositivos SD-WAN existentes conozcan el nuevo sitio que se va a implementar sin contacto, deberá utilizar la opción *Ignorar incompleto* para omitir el intento de insertar la configuración en el nuevo sitio que todavía necesita pasar por el flujo de trabajo ZTD.



2. Vuelva a la página SD-WAN Center Zero Touch Deployment y, con la nueva configuración activa ejecutándose, el nuevo sitio estará disponible para su implementación.

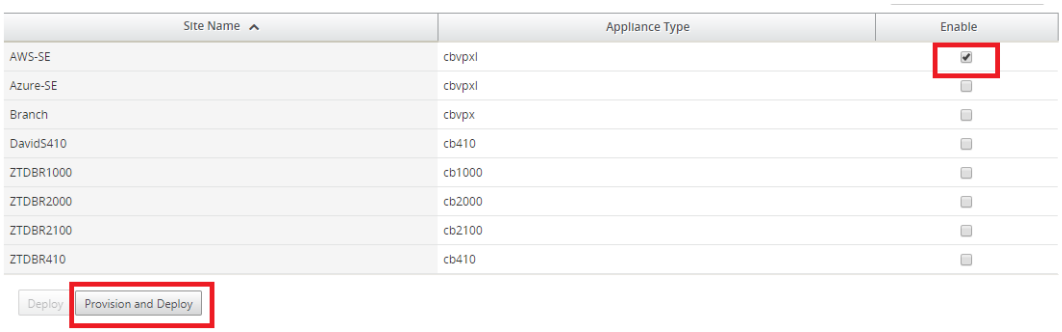
   a) En la página Deployment Zero Touch, en la ficha **Implementar nuevo sitio**, seleccione el archivo de configuración de red en ejecución.

   b) Después de seleccionar el archivo de configuración en ejecución, se mostrará la lista de todos los sitios de sucursales con dispositivos Citrix SD-WAN no implementados que admiten sin contacto.



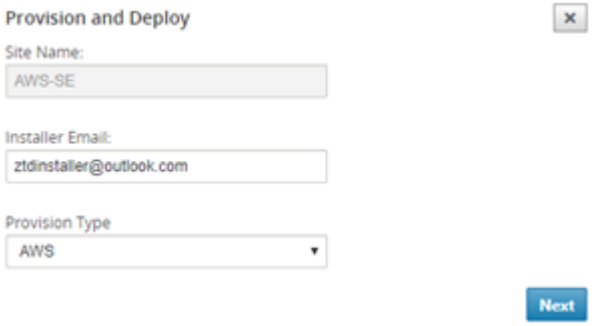
   c) Seleccione el sitio de nube de destino que desea implementar mediante el servicio Zero Touch, haga clic en **Habilitar**y, a continuación, **aprovisionar e implementar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

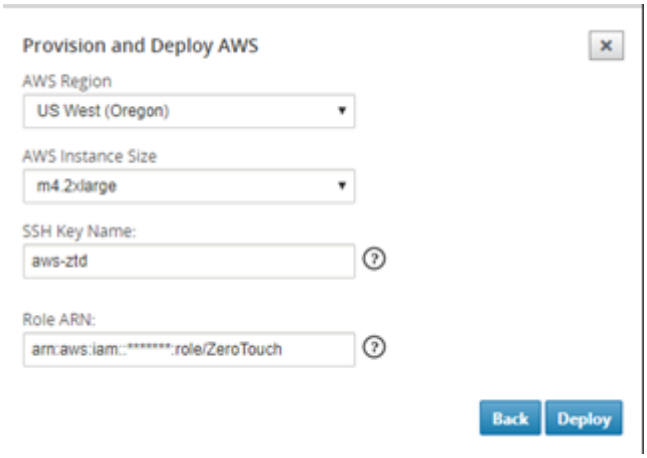


d) Aparecerá una ventana emergente en la que el administrador de Citrix SD-WAN puede iniciar la implementación de Zero Touch.

Rellene una dirección de correo electrónico donde se puede entregar la URL de activación y seleccione el **tipo de provisión** para la nube deseada.



e) Después de hacer clic en **Siguiente**, seleccione la región adecuada, tamaño de instancia, rellene correctamente los campos Nombre de clave SSH y ARN de rol.



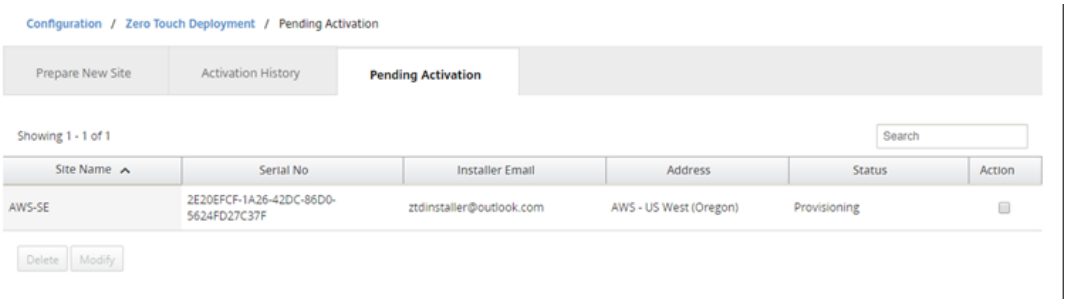
> **Nota**
>
> Utilice los enlaces de ayuda para obtener orientación sobre cómo configurar la clave SSH y el ARN de rol en la cuenta Cloud. Asegúrese también de que la región de selección coincida con lo que está disponible en la cuenta y de que el tamaño de instancia

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> seleccionado coincida con VPX o VPXL como el modelo seleccionado en la configuración de SD-WAN.

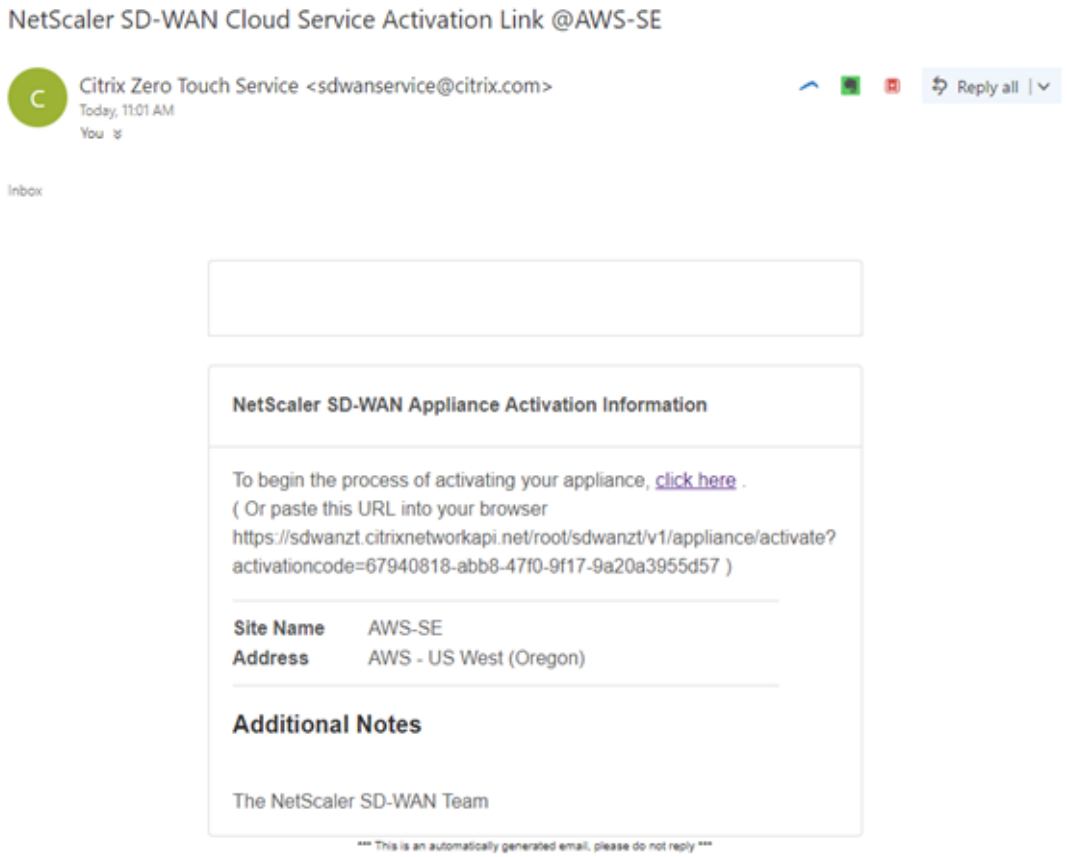
f) Haga clic en **Implementar**, activando el SD-WAN Center, que se había registrado previamente con ZTD Cloud Service, para compartir la configuración de este sitio para que sea temporal almacenada en ZTD Cloud Service.

g) Acceda a la ficha **Activación pendiente** para confirmar que la información del sitio se rellenó correctamente y se puso en un estado de Provisioning.



3. Inicie el proceso de implementación Zero Touch como administrador de la nube.

a) El instalador deberá comprobar el buzón de correo de la dirección de correo electrónico que el Administrador de SD-WAN utilizó al implementar el sitio.



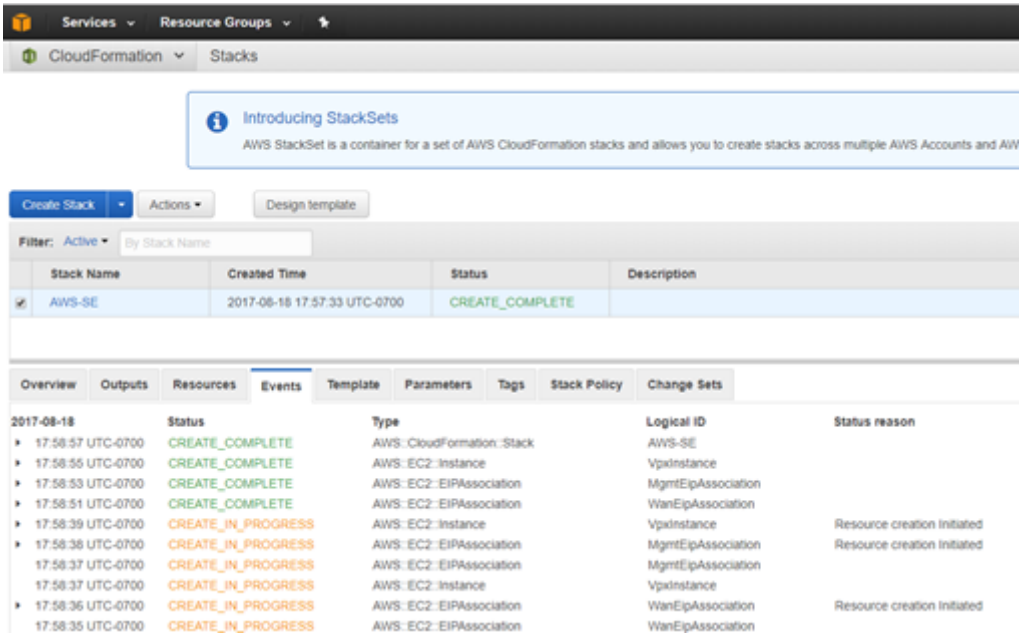
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Abra la URL de activación que se encuentra en el correo electrónico en una ventana del explorador de Internet (ejemplo: `https://sdwanzt.citrixnetworkapi.net`).

c) Si la clave SSH y el ARN de rol se introducen correctamente, el servicio de implementación Zero Touch comenzará inmediatamente a Provisioning la instancia SD-WAN; de lo contrario, los errores de conexión se mostrarán inmediatamente.

d) Para solucionar problemas adicionales en la consola de AWS, el servicio Cloud Formation se puede utilizar para detectar cualquier evento que se produzca durante el proceso de Provisioning.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

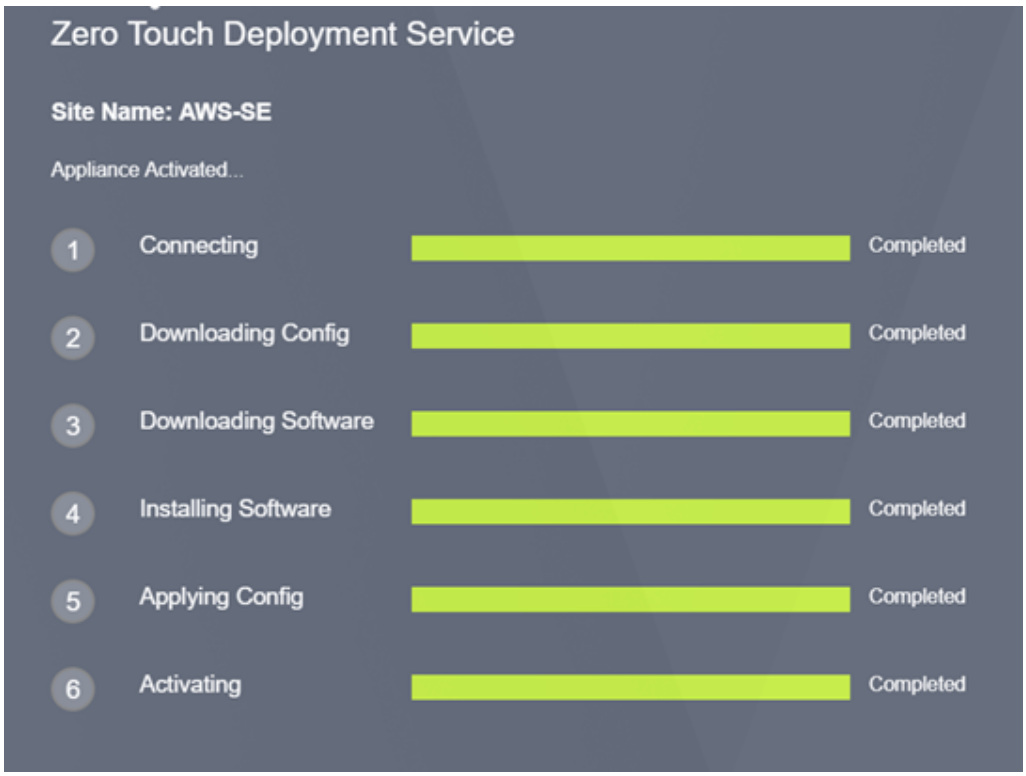


e) Permitir que el proceso de Provisioning entre 8 y 10 minutos y la activación entre 3 y 5 minutos se complete por completo.

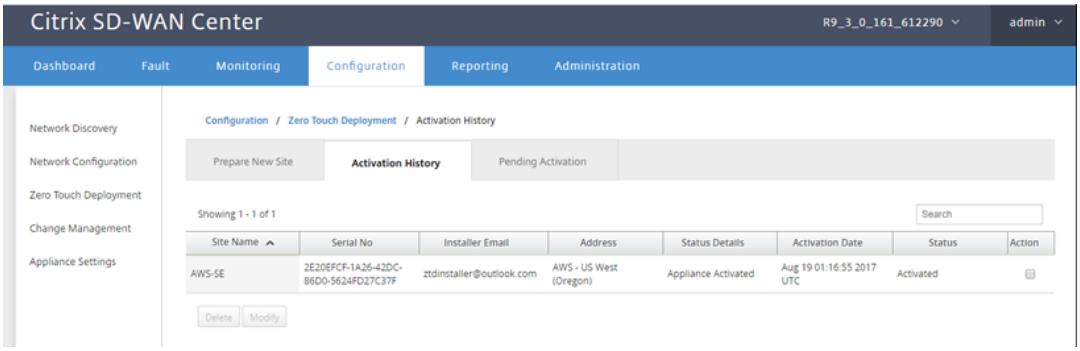
f) Con una conectividad correcta de la instancia de nube SD-WAN al servicio de nube ZTD, el servicio realizará automáticamente lo siguiente:

- Descargue el archivo de configuración específico del sitio almacenado anteriormente por SD-WAN Center
- Aplicación de la configuración a la instancia local
- Descargar e instalar un archivo de licencia temporal de 10 MB
- Descargar e instalar cualquier actualización de software si es necesario
- Activar el servicio SD-WAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

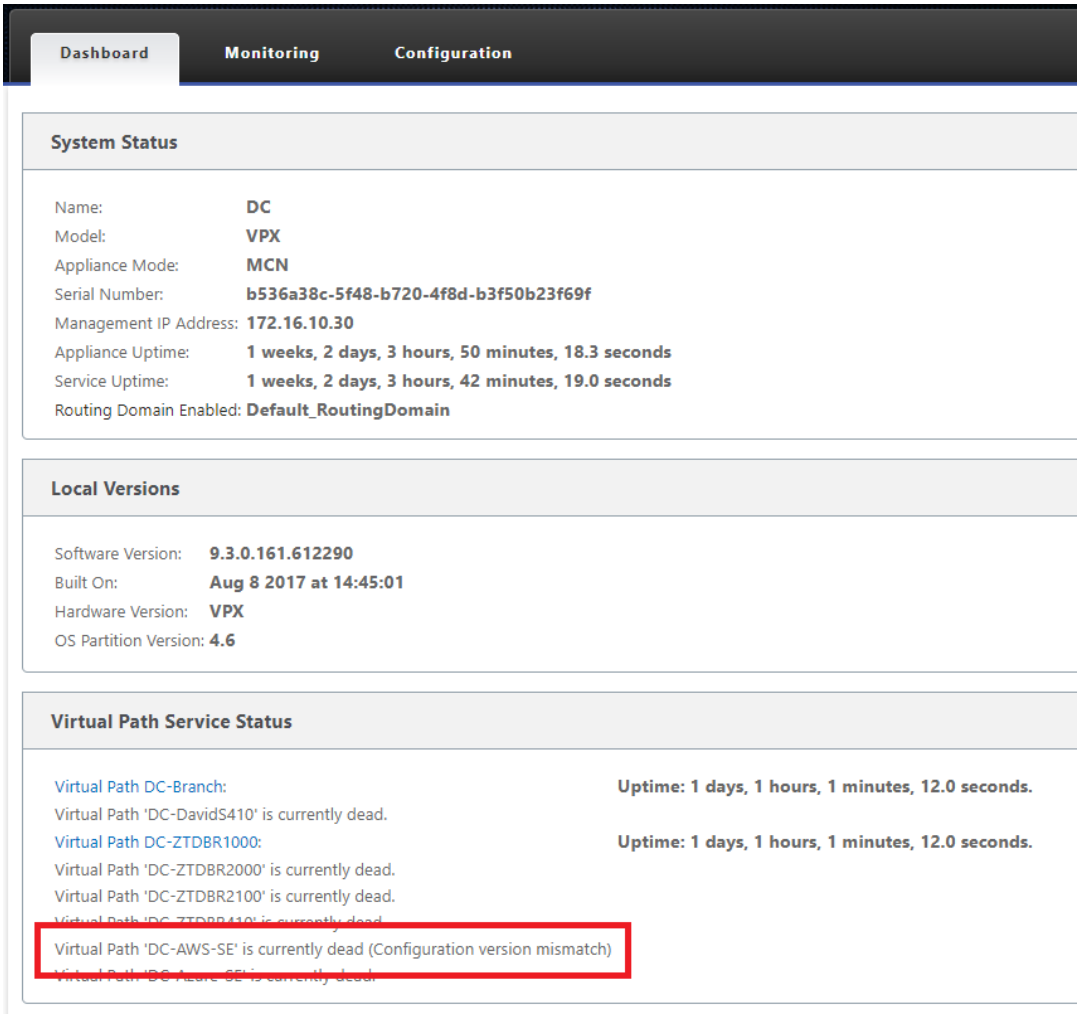


g) Se puede realizar una confirmación adicional en la interfaz de administración web de SD-WAN Center; el menú Deployment Zero Touch mostrará los dispositivos activados correctamente en la ficha **Historial de activación**.



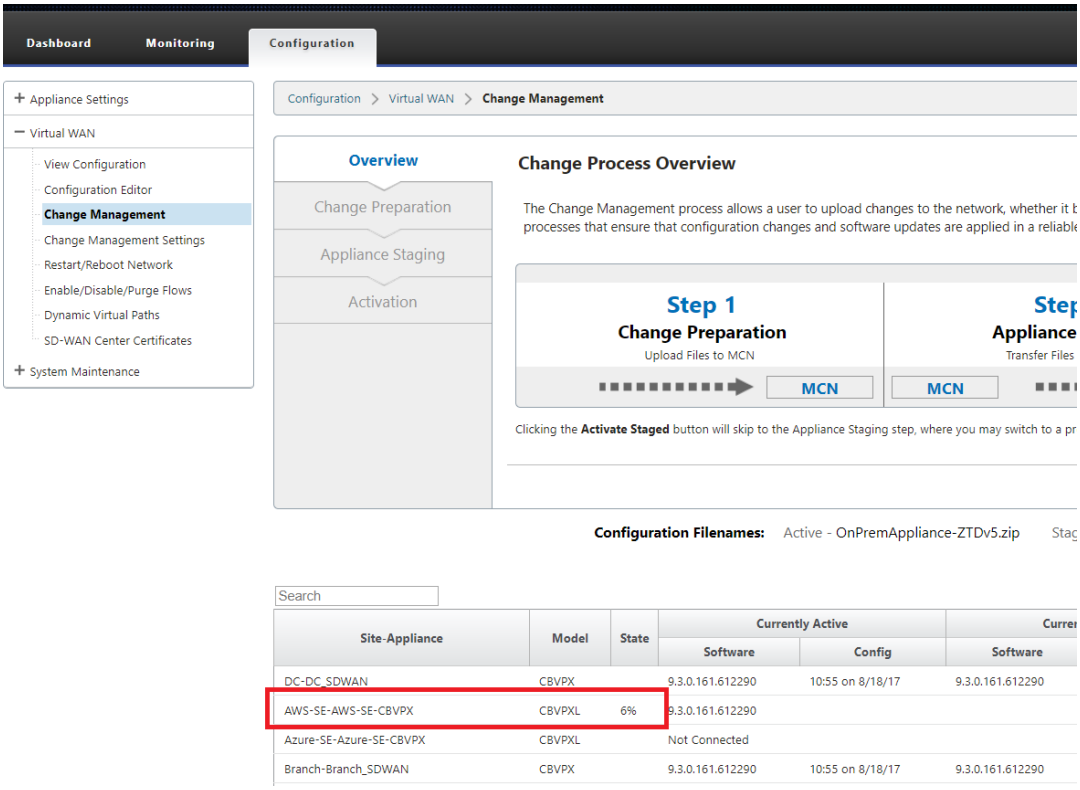
h) Es posible que las rutas virtuales no se muestren inmediatamente en un estado conectado, esto se debe a que el MCN puede no confiar en la configuración transmitida desde ZTD Cloud Service e informará que la *versión de configuración no coincide* en el Panel de MCN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

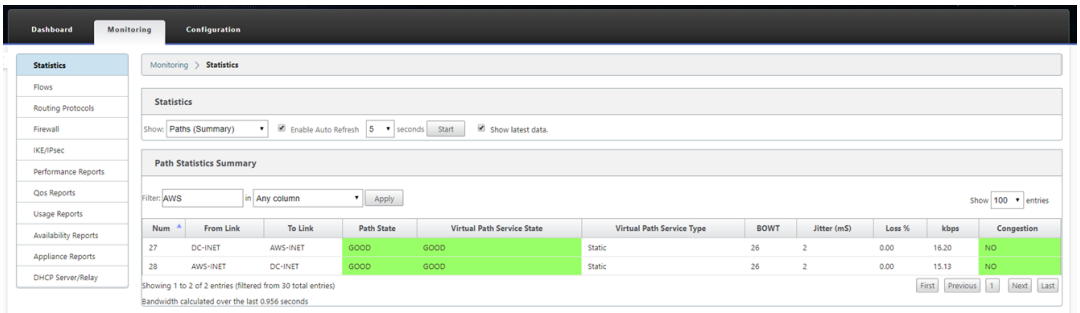


i) La configuración se volverá a entregar automáticamente al dispositivo de sucursal recién instalado, el estado de esta puede ser la supervisión en la página **MCN** > **Configuración** > **Virtual WAN** > **Administración de cambios** (dependiendo de la conectividad, este proceso puede tardan varios minutos en completarse).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

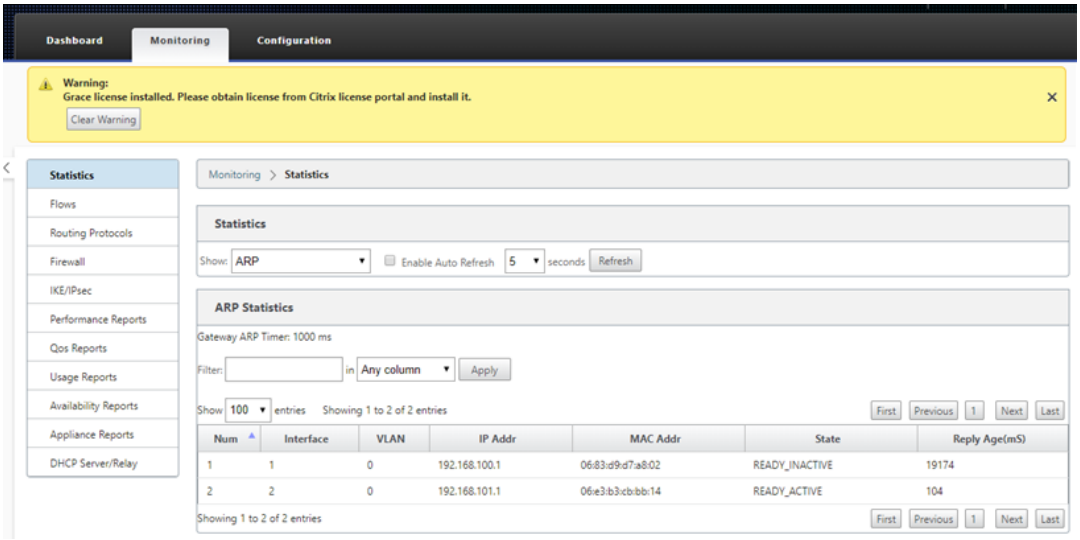


j) El Administrador de SD-WAN puede supervisar la página de administración web de MCN de cabecera para las rutas virtuales establecidas del sitio de nube recién agregado.



k) Si es necesario solucionar problemas, abra la interfaz de usuario de instancias SD-WAN mediante la IP pública asignada por el entorno de nube durante el Provisioning y utilice la tabla ARP de la página **Monitoring** > **Statistics** para identificar cualquier problema relacionado con las puertas de enlace previstas, o utilizan las opciones de ruta de seguimiento y captura de paquetes en diagnósticos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Azure

May 7, 2021

El procedimiento para implementar el proceso de implementación de Zero Touch para las instancias en la nube es ligeramente diferente al de la implementación del dispositivo para el servicio táctil cero.

Actualice la configuración para agregar un nuevo sitio remoto con un dispositivo en la nube SD-WAN compatible con ZTD mediante la configuración de red SD-WAN Center

Si la configuración de SD-WAN no se creó mediante la configuración de red de SD-WAN Center, importe la configuración activa desde el MCN y comience a modificar la configuración mediante SD-WAN Center. Para la capacidad de implementación de Zero Touch, el administrador de SD-WAN debe crear la configuración mediante SD-WAN Center. Se debe utilizar el siguiente procedimiento para agregar un nuevo nodo en la nube destinado a la implementación de Zero Touch.

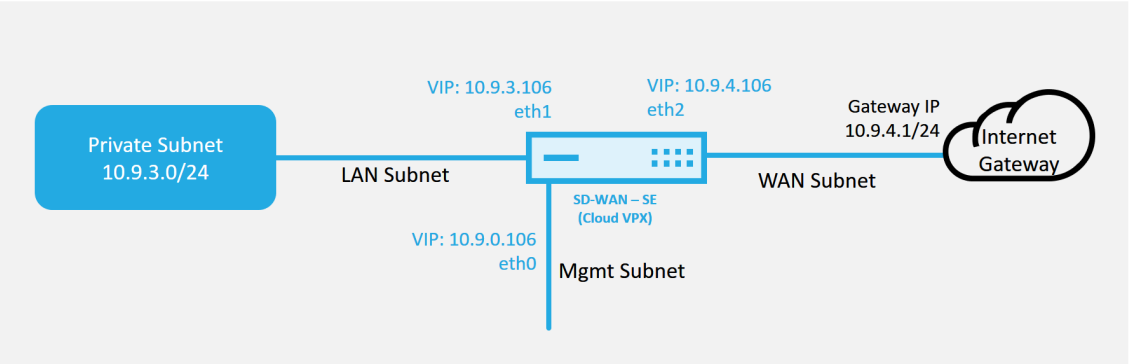
1. Diseñar el nuevo sitio para la implementación en la nube SD-WAN esbozando primero los detalles del nuevo sitio (es decir, tamaño VPX, uso de grupos de interfaz, direcciones IP virtuales, enlaces WAN con ancho de banda y sus respectivas puertas de enlace).

   > **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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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).

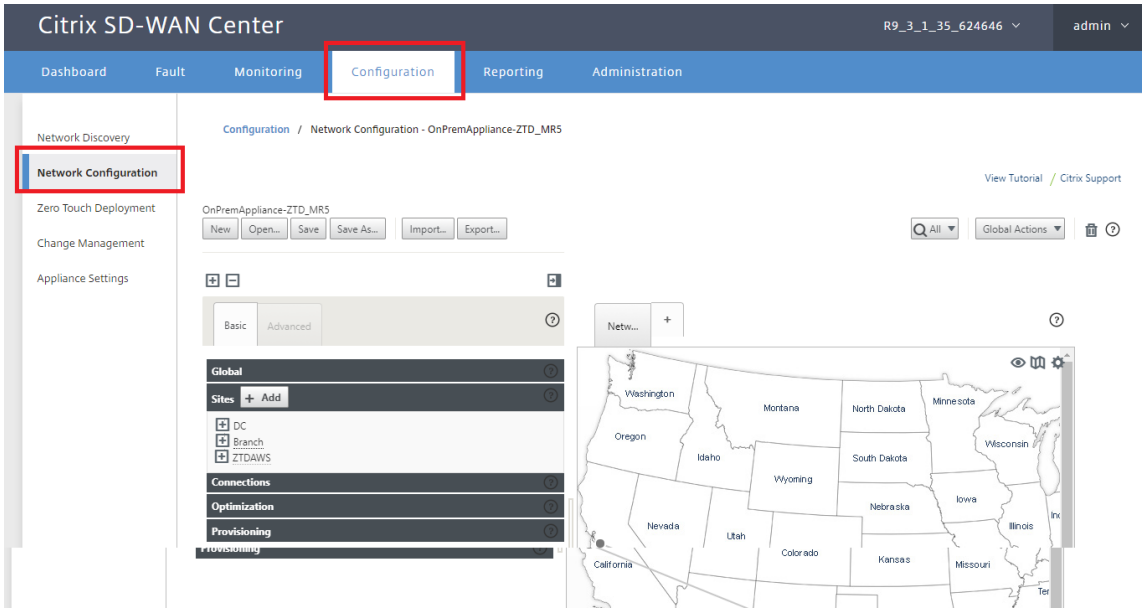
Azure Cloud Topology with NetScaler SD-WAN



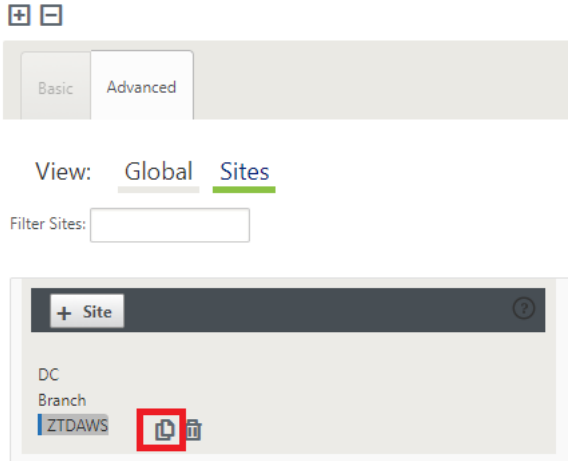
Este es un ejemplo de implementación de un sitio implementado en la nube SD-WAN, el dispositivo Citrix SD-WAN se implementa como el dispositivo perimetral que presta servicio a un único enlace WAN de Internet en esta red en la nube. Los sitios remotos podrán aprovechar varios enlaces WAN de Internet 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.

2. Abra la interfaz de administración web de SD-WAN Center y vaya a la página **Configuración** > **Configuración de red**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Asegúrese de que ya hay una configuración en funcionamiento o importe la configuración desde el MCN.
4. Acceda a la ficha Básico para crear un nuevo sitio.
5. Abra el icono Sitios para mostrar los sitios configurados actualmente.
6. Cree rápidamente la configuración para el nuevo sitio en la nube mediante la función de clonación de cualquier sitio existente o cree manualmente un nuevo sitio.



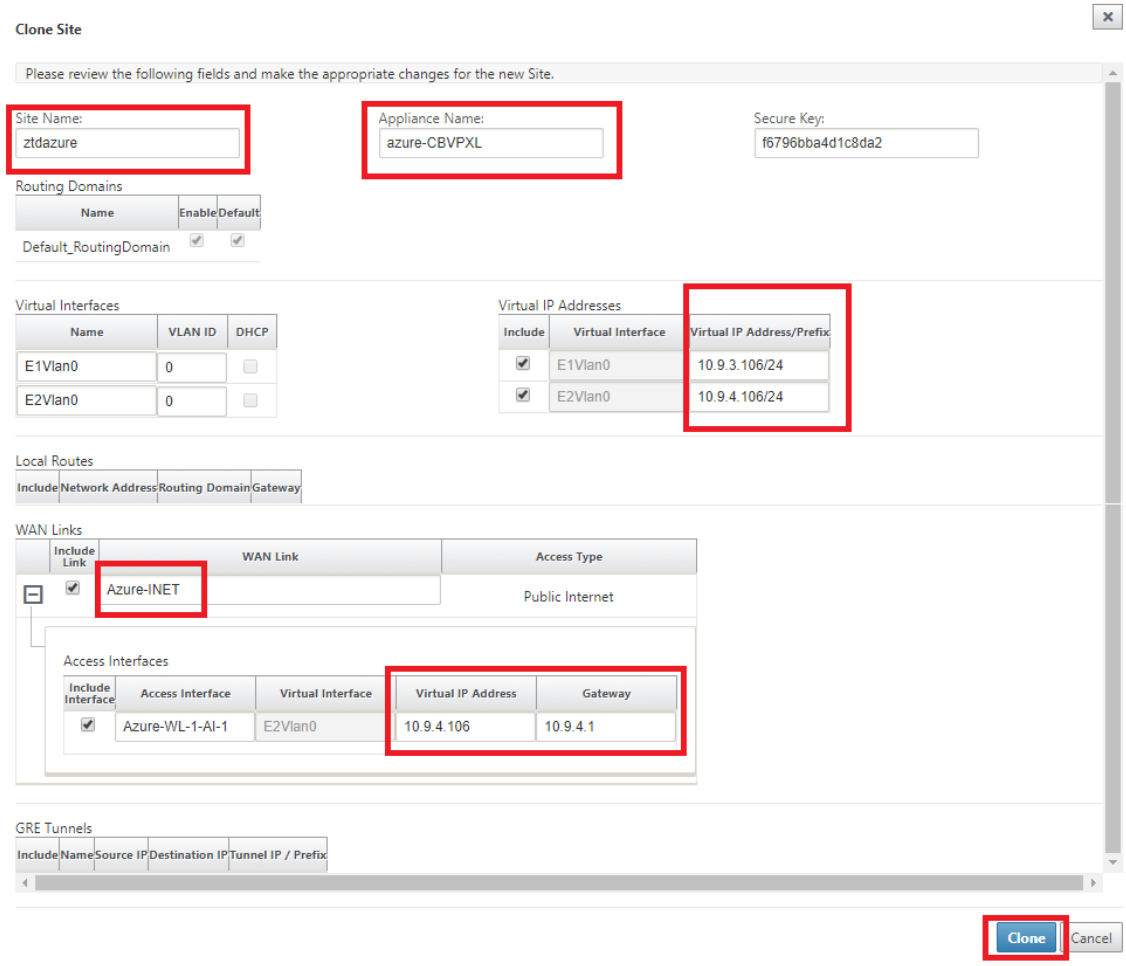
7. Rellene todos los campos necesarios de la topología diseñada anteriormente para este nuevo sitio en la nube.

   Tenga en cuenta que la plantilla disponible para las implementaciones de ZTD en la nube de Azure está actualmente configurada 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. Si la configuración no está definida para que coincida con la dirección VIP esperada para cada interfaz, el dispositivo no

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

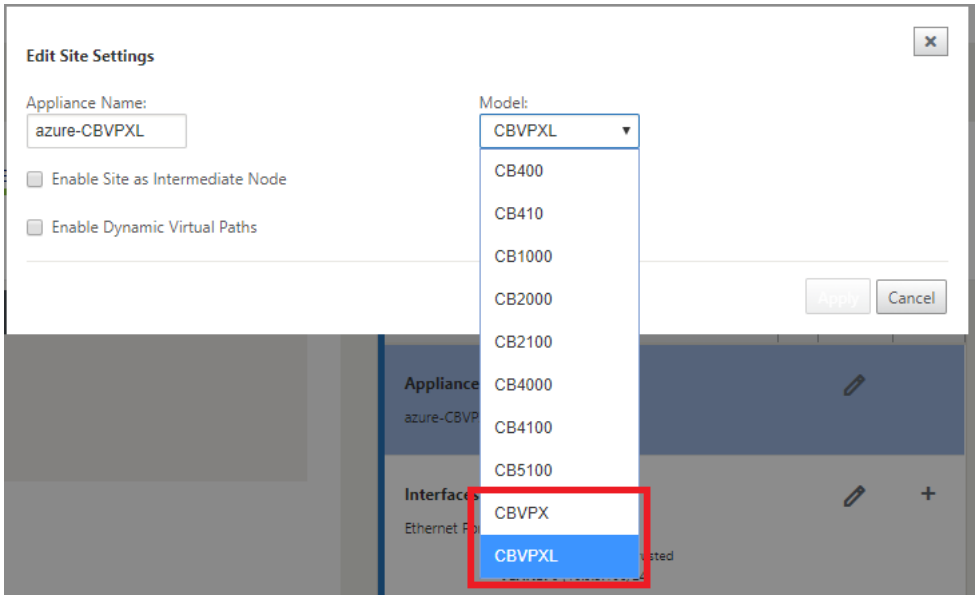
podrá establecer correctamente ARP en las puertas de enlace del entorno de nube y conectividad IP con la ruta virtual del MCN.

Es importar que el nombre del sitio sea compatible con lo que Azure espera. El nombre del sitio debe estar en minúsculas, al menos 6 caracteres, sin caracteres especiales, debe confirmar a la siguiente expresión regular **^ [a-z] [a-z0-9-] {1,61} [a-z0-9] $.**



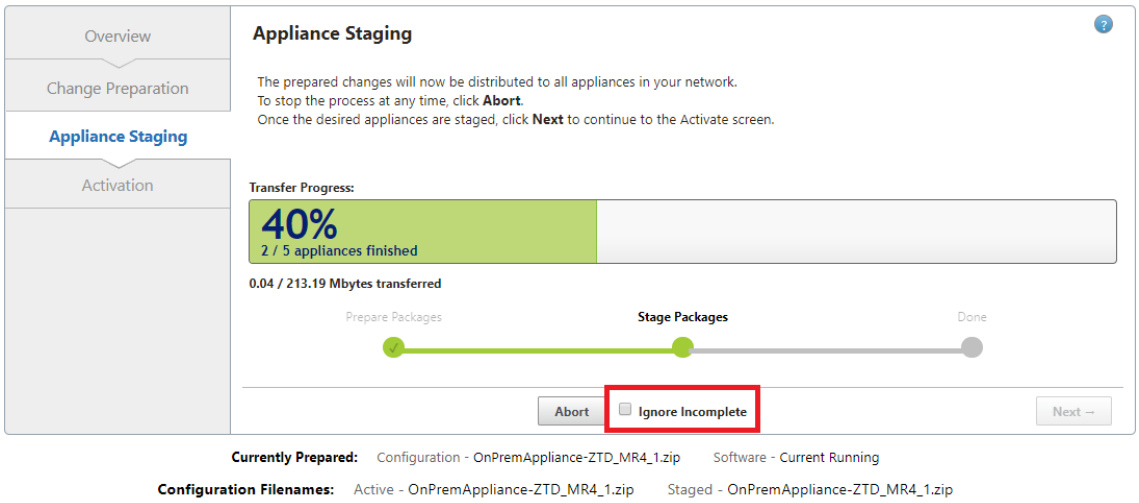
8. Después de clonar un sitio nuevo, desplácese hasta la **Configuración básica** del sitio y verifique que el Modelo de SD-WAN esté seleccionado correctamente, lo que soportaría el servicio Zero Touch.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



9. Guarde la nueva configuración en SD-WAN Center y utilice la opción Exportar a la **bandeja de entrada de Change Management** para insertar la configuración mediante Change Management.

10. Siga el procedimiento de administración de cambios para organizar correctamente la nueva configuración, lo que hace que los dispositivos SD-WAN existentes conozcan el nuevo sitio que se va a implementar sin contacto, deberá utilizar la opción *Ignorar incompleto* para omitir el intento de insertar la configuración en el nuevo sitio que todavía necesita pasar por el flujo de trabajo ZTD.

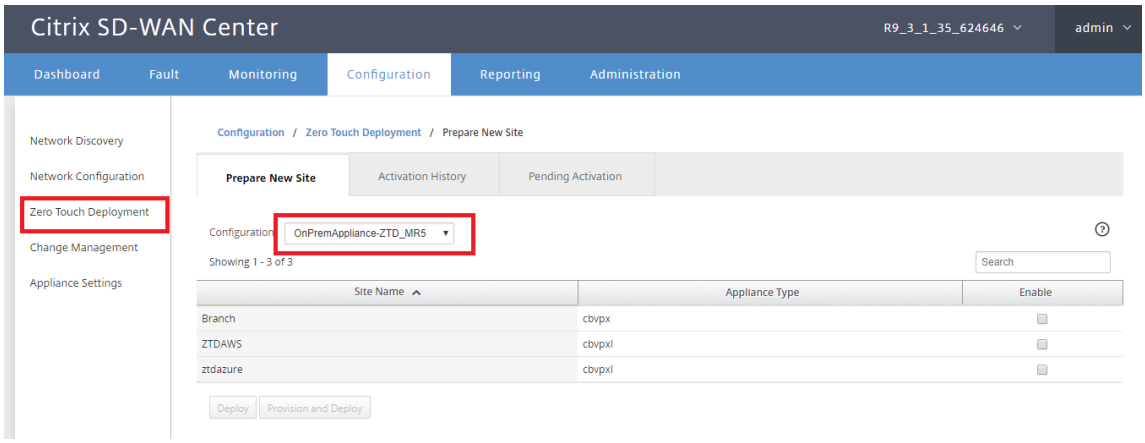


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

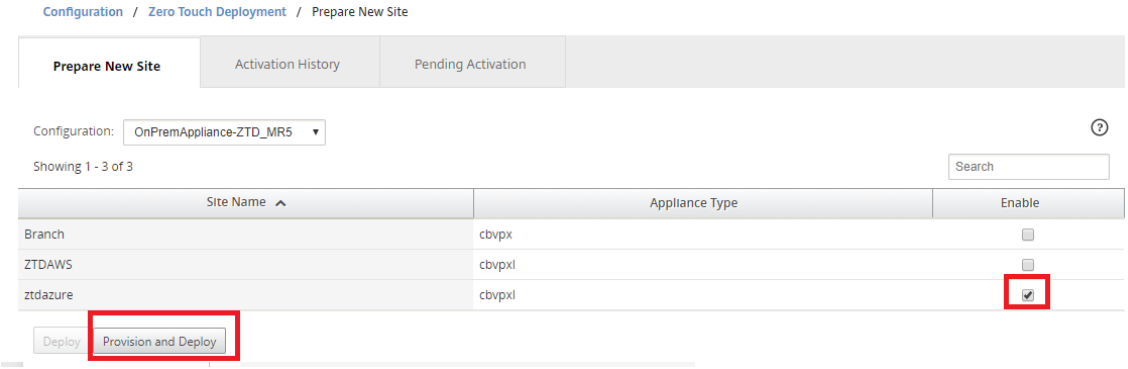
Vaya a la página de implementación de Zero Touch de SD-WAN Center y, con la nueva configuración activa en ejecución, el nuevo sitio estará disponible para SD-WAN Center Provision and Deploy Azure (paso 1 de 2)

1. En la página Deployment Zero Touch, inicie sesión con las credenciales de su cuenta de Citrix. En la ficha **Implementar nuevo sitio**, seleccione el archivo de configuración de red en ejecución.

2. Después de seleccionar el archivo de configuración en ejecución, se mostrará la lista de todos los sitios de sucursales con dispositivos Citrix SD-WAN compatibles con ZTD.

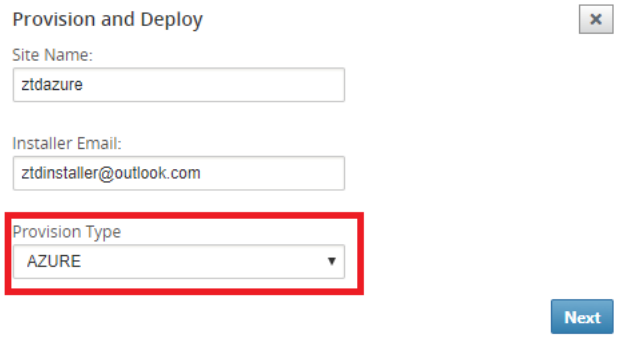


3. Seleccione el sitio de nube de destino que desea implementar mediante el servicio Zero Touch, haga clic en **Habilitar**y, a continuación, **aprovisionar e implementar**.



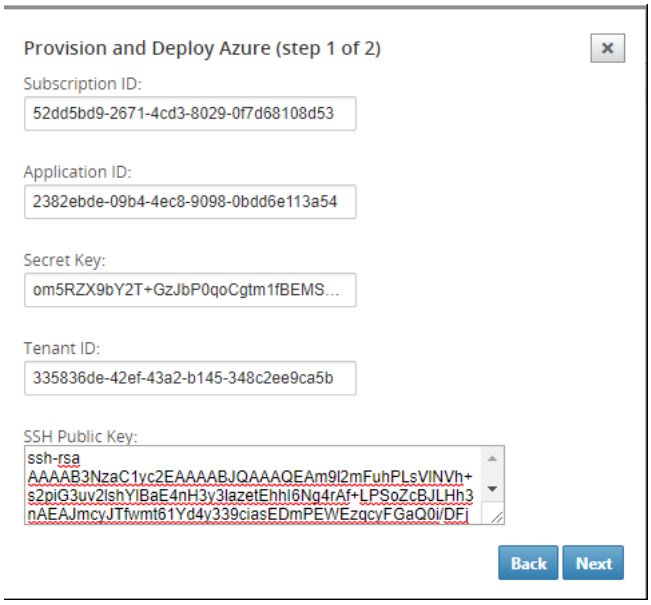
4. Aparecerá una ventana emergente en la que el administrador de Citrix SD-WAN puede iniciar la implementación de Zero Touch. Validar que el nombre del sitio cumpla con los requisitos de Azure (minúsculas sin caracteres especiales). Rellene una dirección de correo electrónico en la que se pueda entregar la URL de activación y seleccione Azure como **Tipo de aprovisionamiento** para la nube deseada, antes de hacer clic en **Siguiente**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



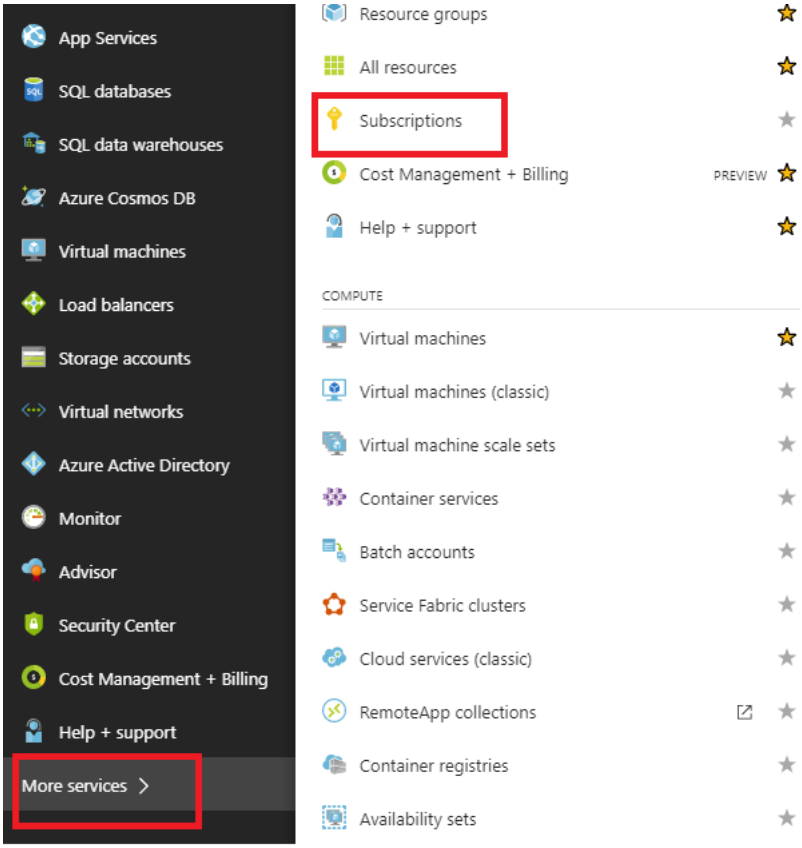
5. Después de hacer clic en **Siguiente**, la ventana Aprovisionar e implementar Azure (paso 1of 2) requerirá la entrada de obtenida de la cuenta de Azure.

   Copie y pegue cada campo requerido después de obtener la información de su cuenta de Azure. En los pasos siguientes se describe cómo obtener el ID de suscripción, el ID de aplicación, la clave secreta y el ID de arrendatario necesarios desde su cuenta de Azure y, a continuación, haga clic en **Siguiente**.



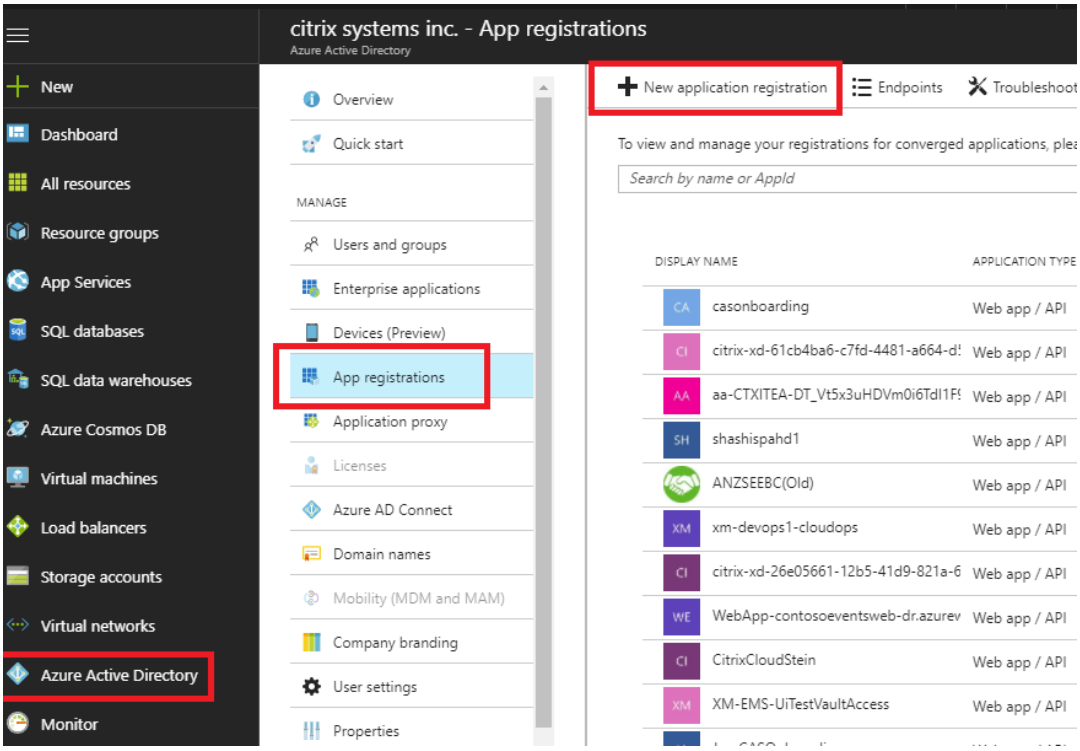
   a) En la cuenta de Azure, podemos identificar el **ID de suscripción** requerido navegando a “Más servicios”y seleccionar **Suscripciones.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

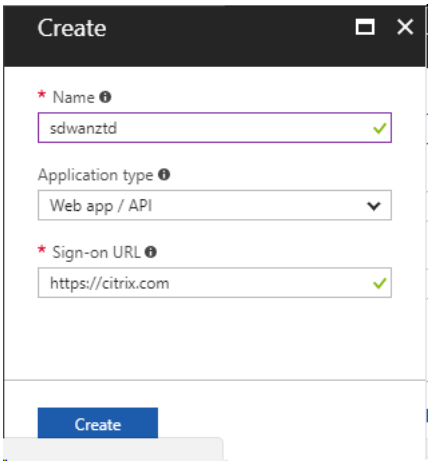


b) Para identificar el ***ID de aplicación requerido**, vaya a Azure Active Directory, Registros de aplicaciones y haga clic en **Nuevo registro de aplicaciones.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

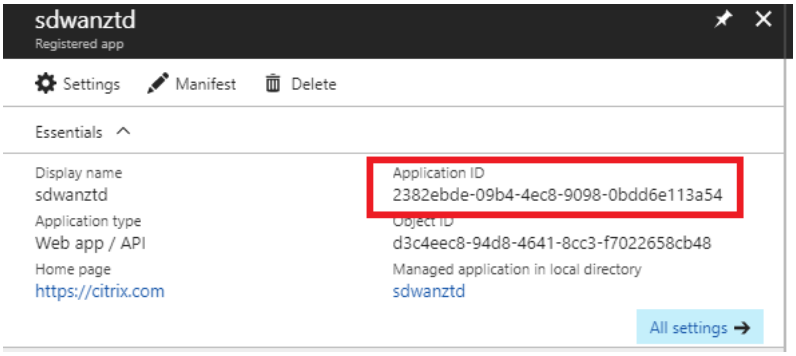


c) En el menú Crear registro de aplicaciones, introduzca un nombre y una URL de inicio de sesión (puede ser cualquier URL, el único requisito es que debe ser válida) y, a continuación, haga clic en **Crear**.

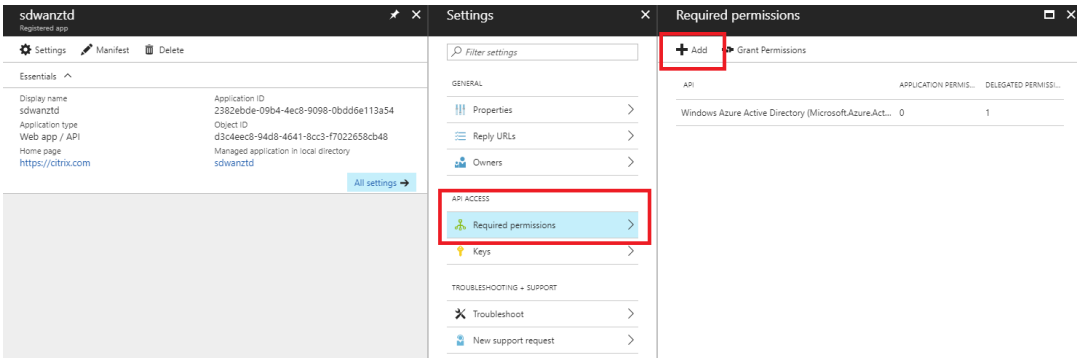


d) Busque y abra la aplicación registrada recién creada y anote el ID de aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

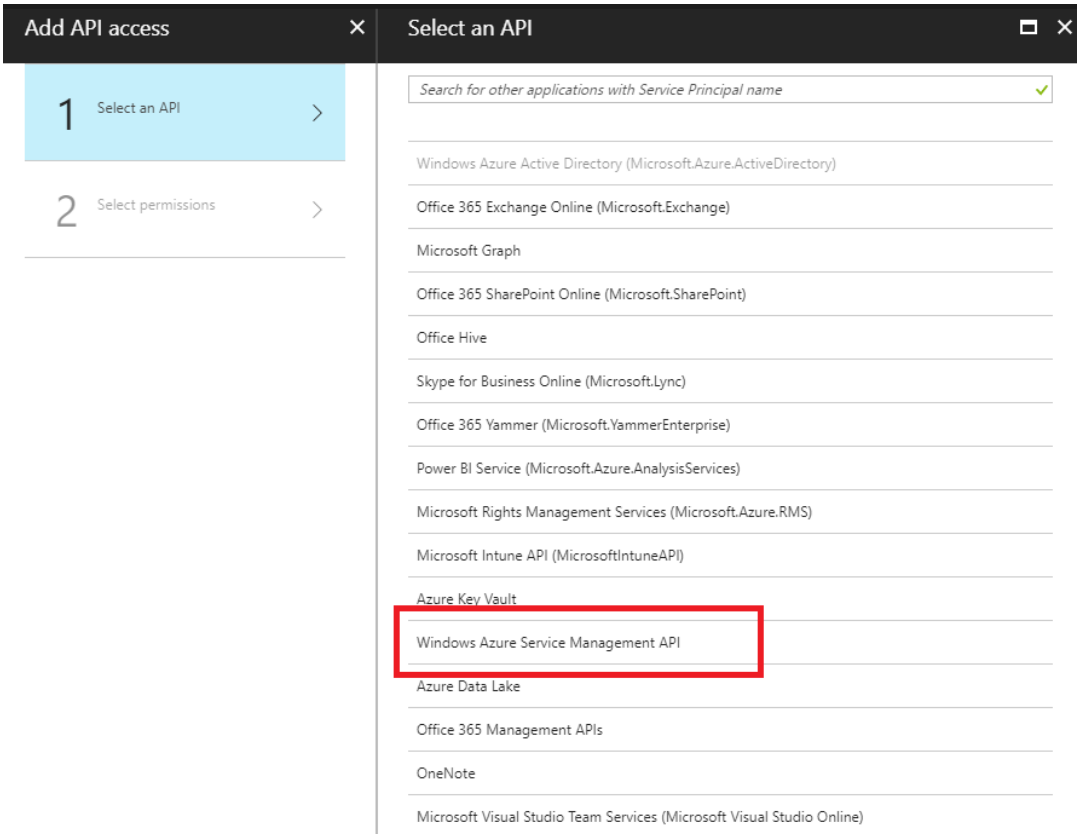


e) Vuelva a abrir la aplicación de registro recién creada e identificar la *clave de seguridad*requerida, en Acceso a API, seleccione **Permisos requeridos,** para permitir que un tercero aprovisionamiento e instancia. A continuación, seleccione **Agregar**.

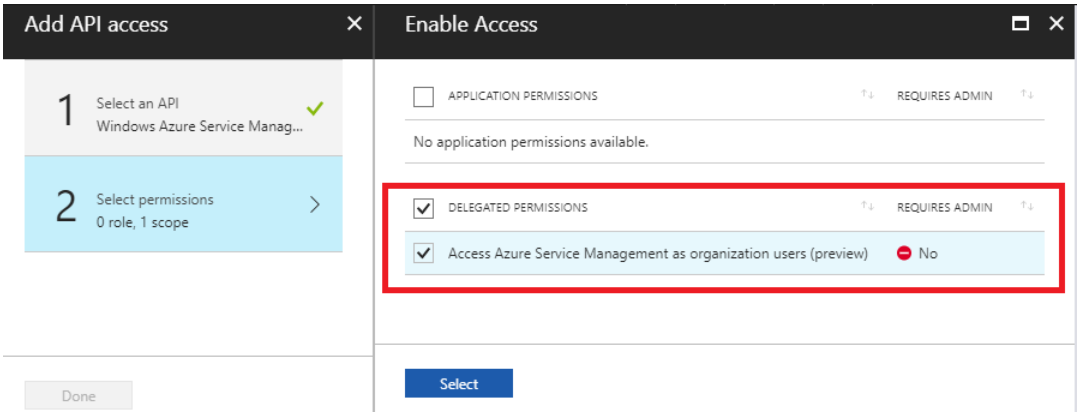


f) Al agregar los permisos necesarios, **seleccione una API y, a continuación,** resalte la **API de administración de servicios de Windows Azure.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

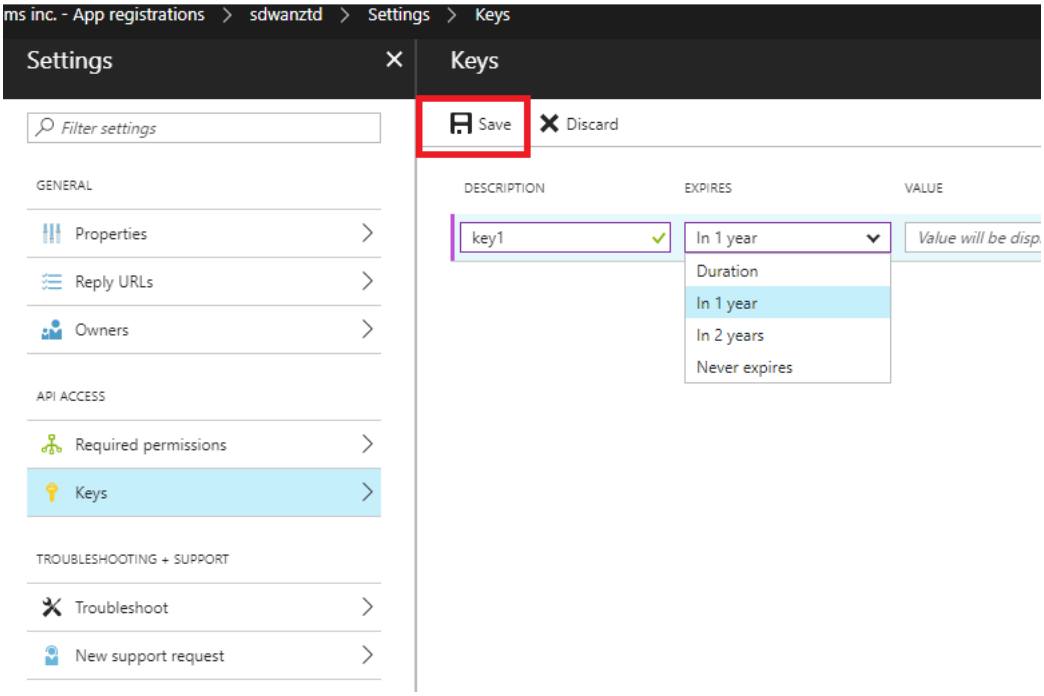


g) Active **Delegate Permissions** para aprovisionar instancias y, a continuación, haga clic en **Seleccionar** y **Terminar**.

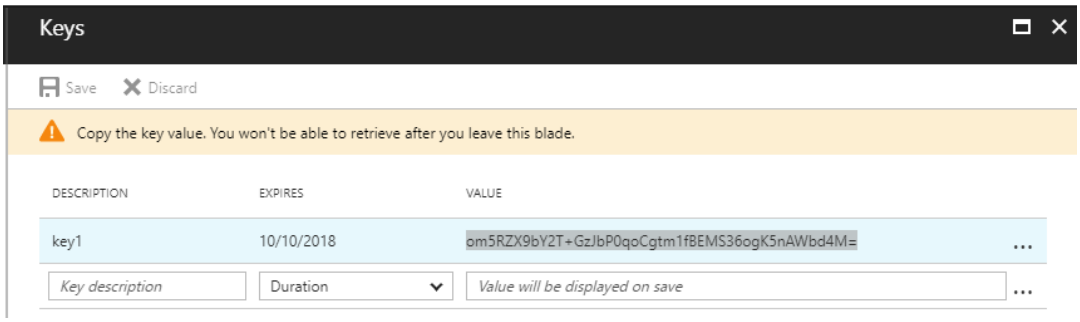


h) Para esta aplicación registrada, en Acceso API, seleccione **Claves** y cree una **descripción de clave** secreta y la **duración** deseada para que la clave sea válida. A continuación, haga clic en **Guardar**, que producirá una **clave secreta** (la clave solo es necesaria para el proceso de Provisioning, se puede eliminar después de que la instancia esté disponible).

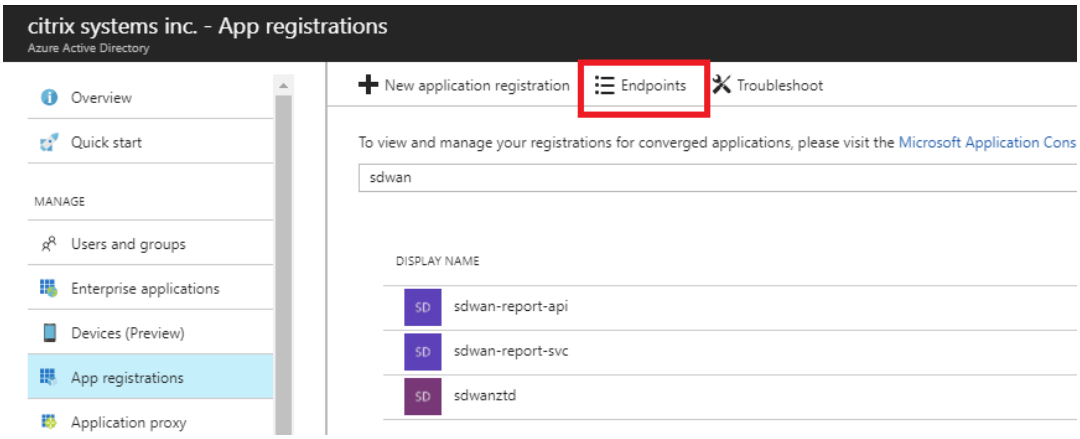
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



i) Copie y guarde la clave secreta (tenga en cuenta que no podrá recuperarla más adelante).



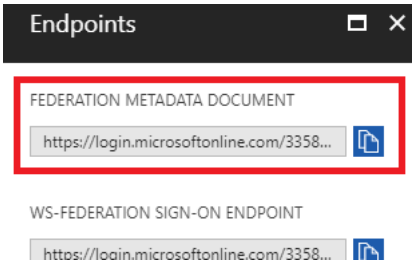
j) Para identificar el ***ID de arrendatario***necesario, vuelva al panel de registro de aplicaciones y seleccione **Dispositivos de punto final**.



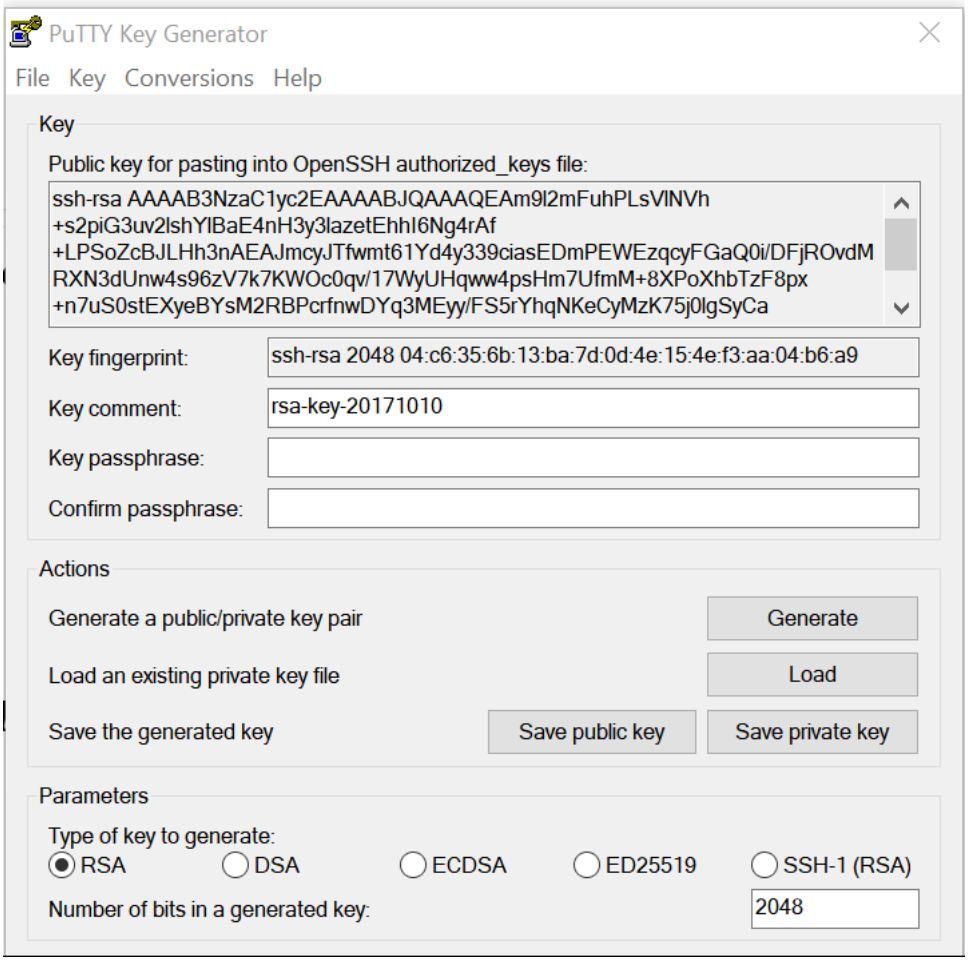
k) Copie el **documento de metadatos de federación** para identificar su Id. de arrendatario

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(tenga en cuenta que el Id. de arrendatario es una cadena de 36 caracteres ubicada entre el `online.com/` y `/federation` en la URL).

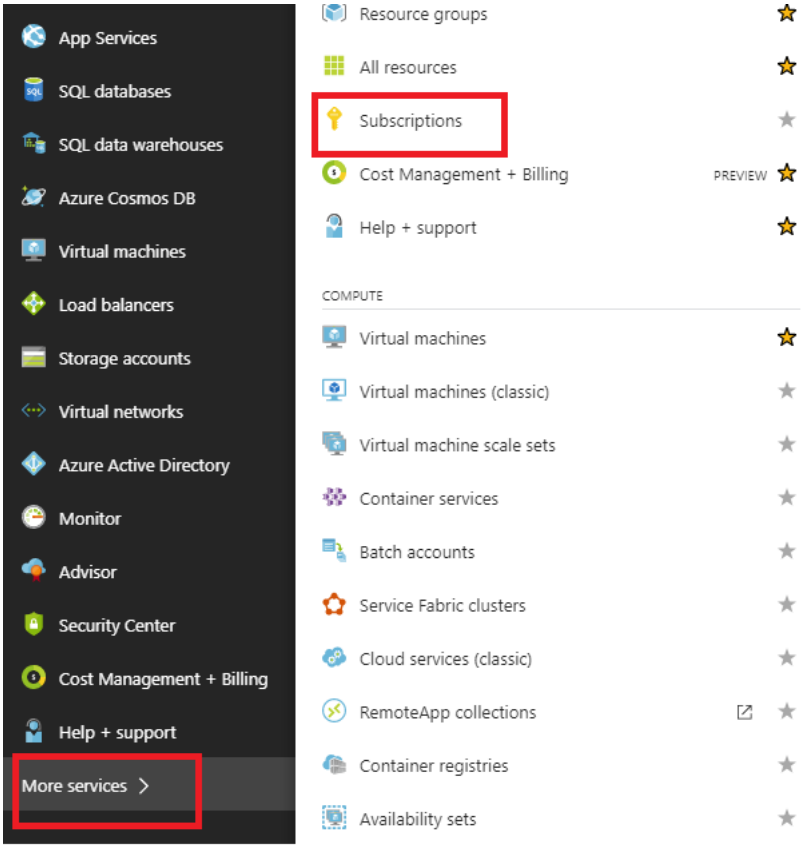


l) El último elemento necesario es la ***clave pública SSH***. Esto se puede crear mediante Putty Key Generator o ssh-keygen y se utilizará para la autenticación, eliminando la necesidad de contraseñas para iniciar sesión. La clave pública SSH se puede copiar (incluidos el encabezado ssh-rsa y las cadenas de clave rsa finales). Esta clave pública se compartirá a través de la entrada de SD-WAN Center en Citrix Zero Touch Deployment Service.

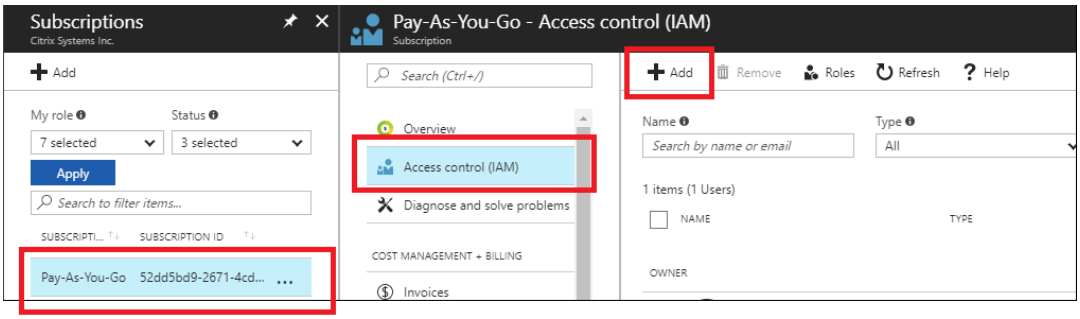


m) Se requieren pasos adicionales para asignar a la aplicación un rol. Vuelva a Más servicios y, a continuación, a Suscripciones.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

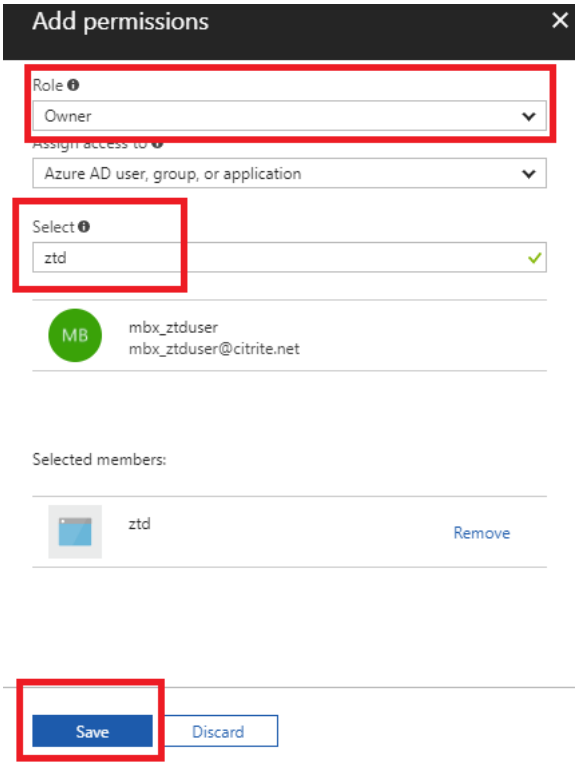


n) Seleccione la suscripción activa, luego **Control de acceso (AIM)**y, a continuación, haga clic en **Agregar.**

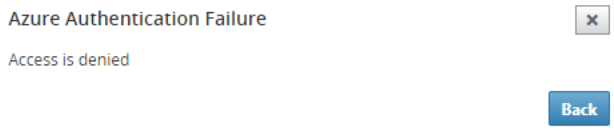


o) En el panel Agregar permisos, seleccione Rol **Propietario**, asigne acceso al **usuario, grupo o aplicación de Azure AD** y busque la aplicación registrada en el **campo Seleccionar** para permitir que el servicio de nube de implementación cero táctil cree y configure la instancia en Azure suscripción. Una vez identificada la aplicación, selecciónela y asegúrese de que se rellena como miembro seleccionado antes de hacer clic en **Guardar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



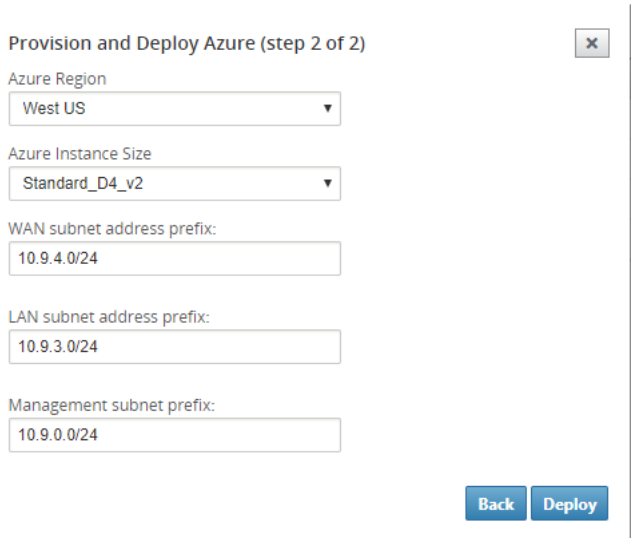
p) Después de recopilar las entradas necesarias e introducirlas en SD-WAN Center, haga clic en **Siguiente**. Si las entradas no son correctas, se producirá un error de autenticación.



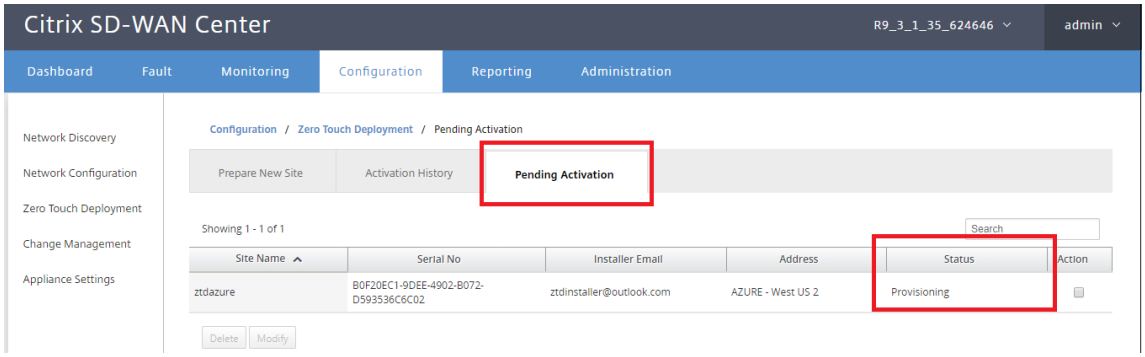
Aprovisionamiento e implementación dSD-WAN Center de Azure (paso 2 de 2)

1. Una vez que la autenticación de Azure se haya realizado correctamente, rellene los campos apropiados para seleccionar la región de Azure deseada y el tamaño de instancia adecuado y, a continuación, haga clic en **Implementar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

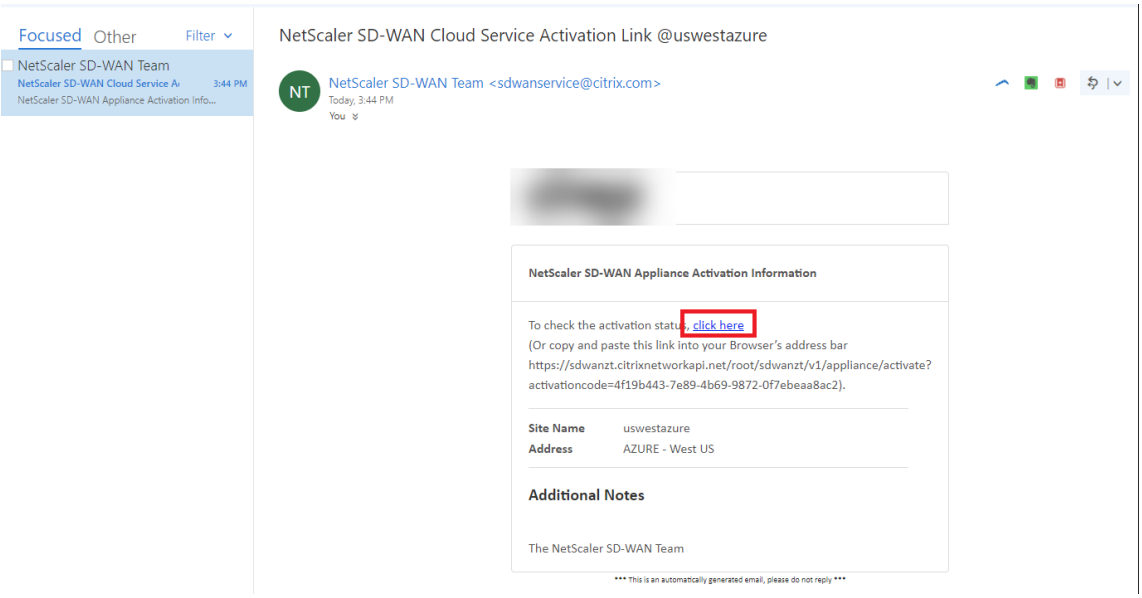


2. Si se desplaza a la ficha **Activación pendiente** en SD-WAN Center, podrá realizar un seguimiento del estado actual de la implementación.



3. Un correo electrónico con un código de activación será entregado a la dirección de correo electrónico introducida en el paso 1, obtener el correo electrónico y abrir la **URL de activación** para activar el proceso y comprobar el estado de la activación.

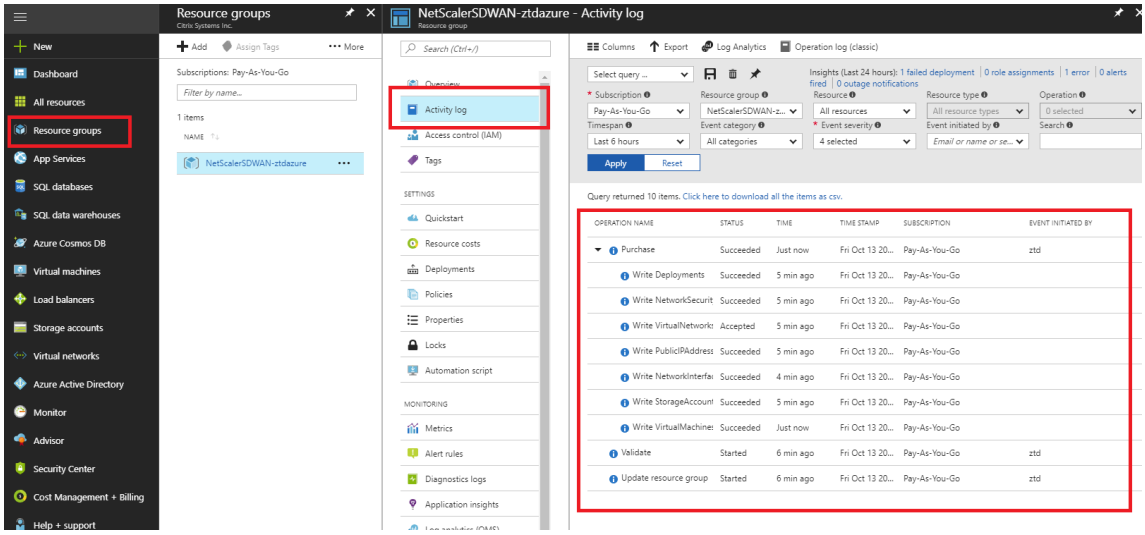
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Se enviará un correo electrónico con una URL de activación a la dirección de correo electrónico introducida en el paso 1. Obtenga el correo electrónico y abra la **URL de activación** para activar el proceso y comprobar el estado de activación.

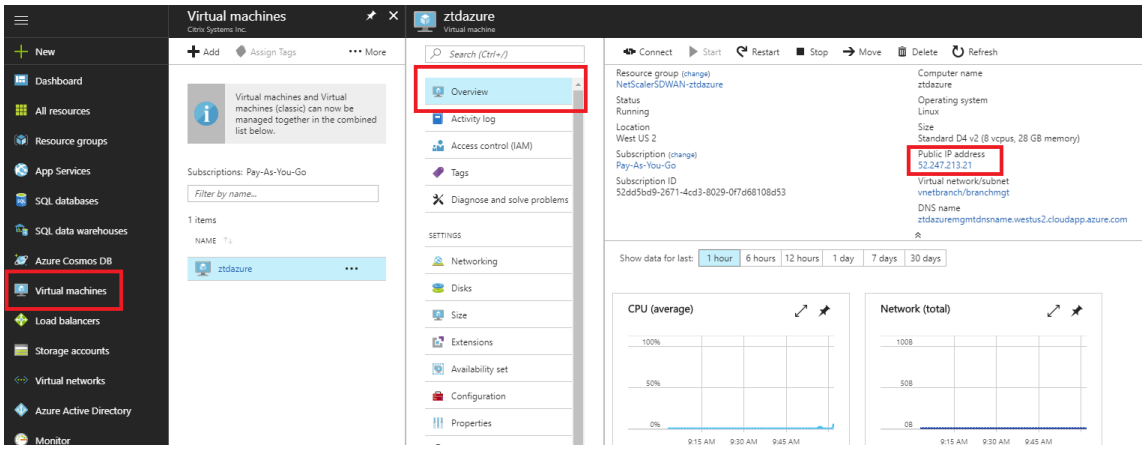
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. El servicio en la nube de SD-WAN tardará unos minutos en aprovisionar la instancia. Puede supervisar la actividad en Azure Portal, en **Registro de actividad** para el **grupo de recursos** que se crea automáticamente. Cualquier problema o error con el aprovisionamiento se rellenará aquí y se replicará en SD-WAN Center en el Estado de activación.

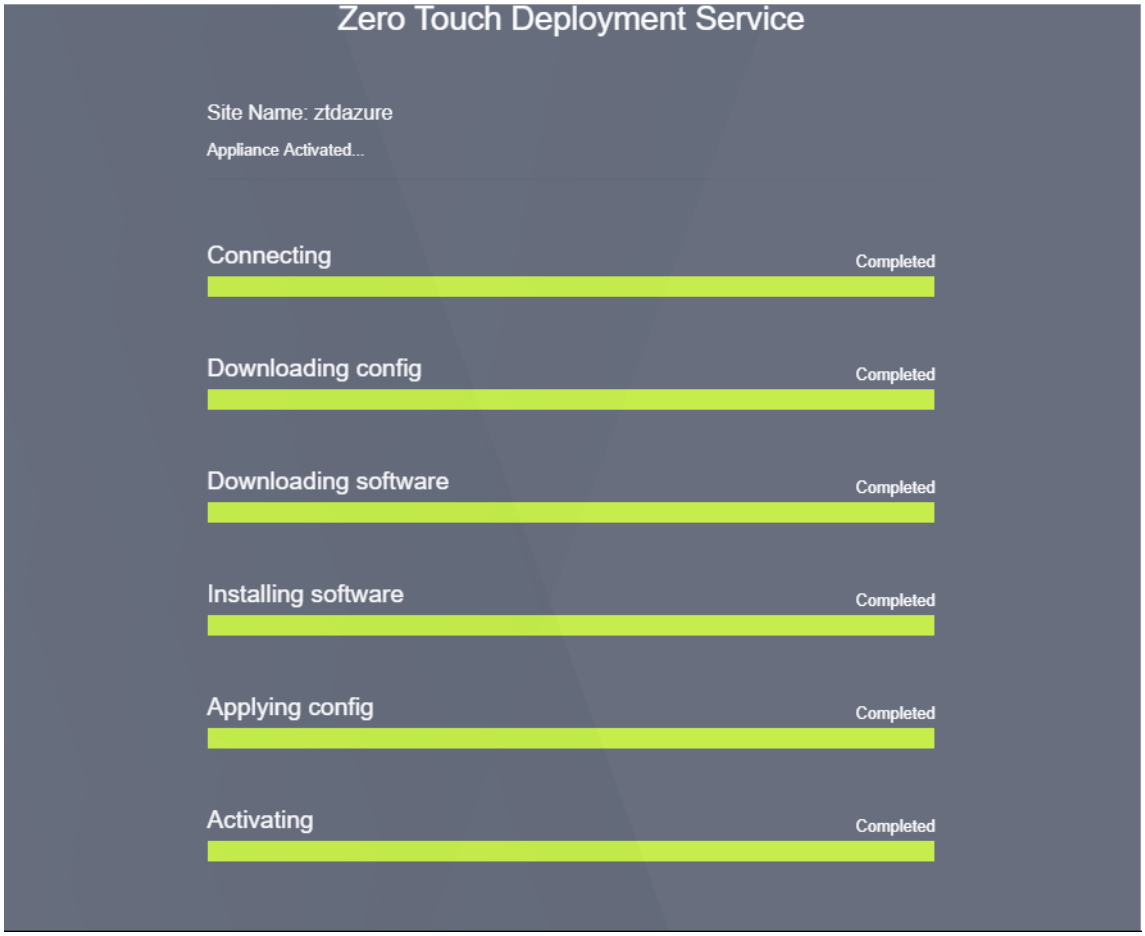


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. En el portal de Azure, la instancia iniciada correctamente estará disponible en **Máquinas virtuales.** Para obtener la IP pública asignada, desplácese hasta la Visión general de la instancia.



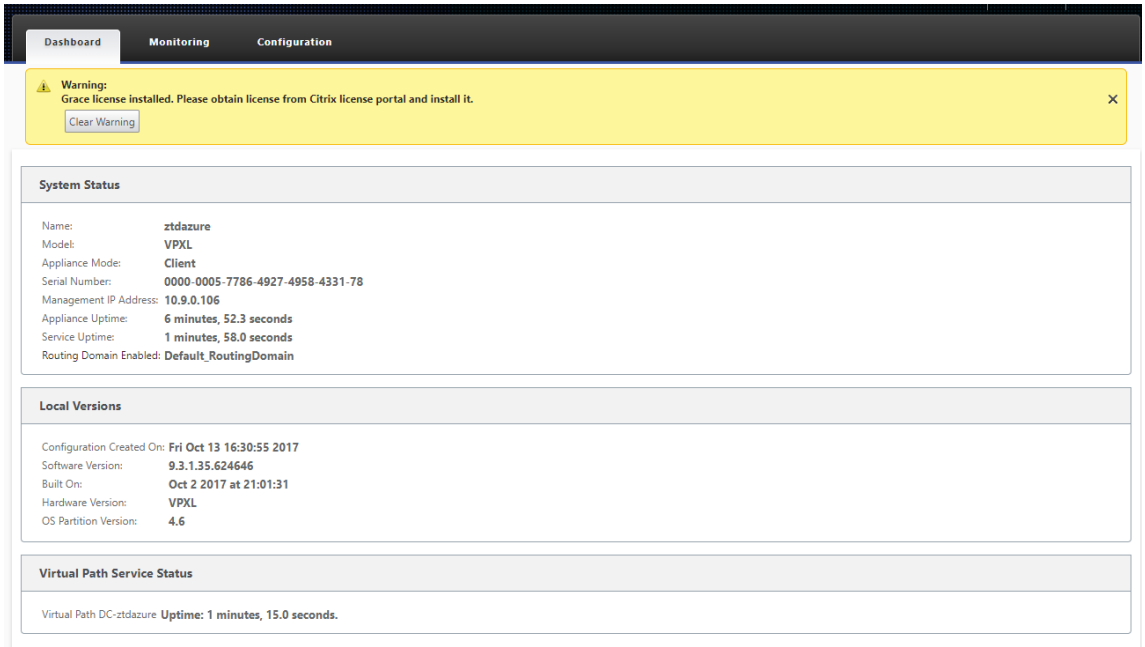
7. Después de que la máquina virtual esté en estado de ejecución, dele un minuto antes de que el servicio se ponga en contacto e inicie el proceso de descarga de la configuración, el software y la licencia.



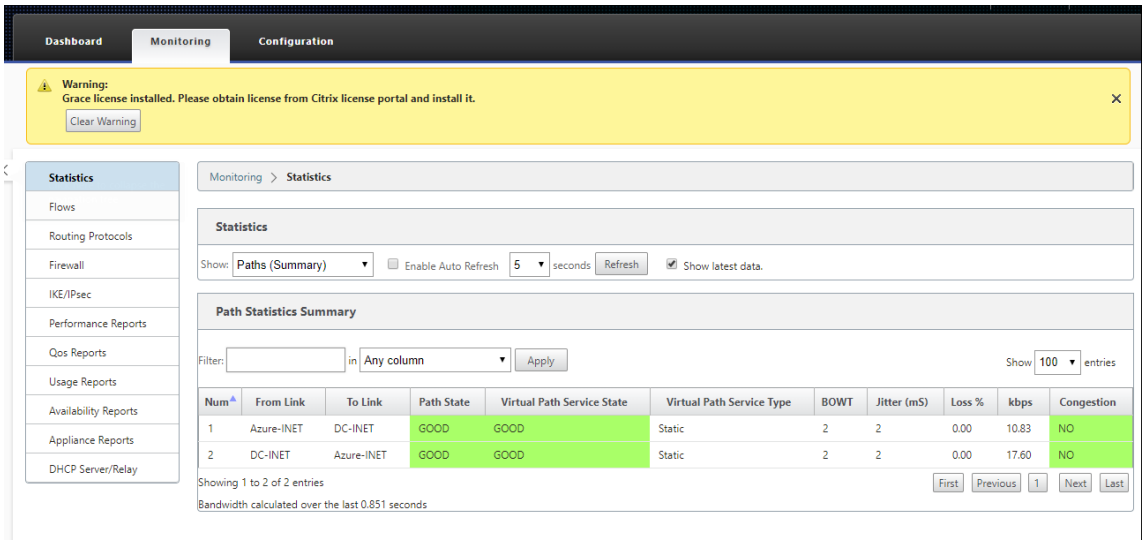
8. Después de que cada uno de los pasos del servicio SD-WAN Cloud se complica automática-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mente, inicie sesión en la interfaz web de instancias SD-WAN mediante la IP pública obtenida del portal de Azure.

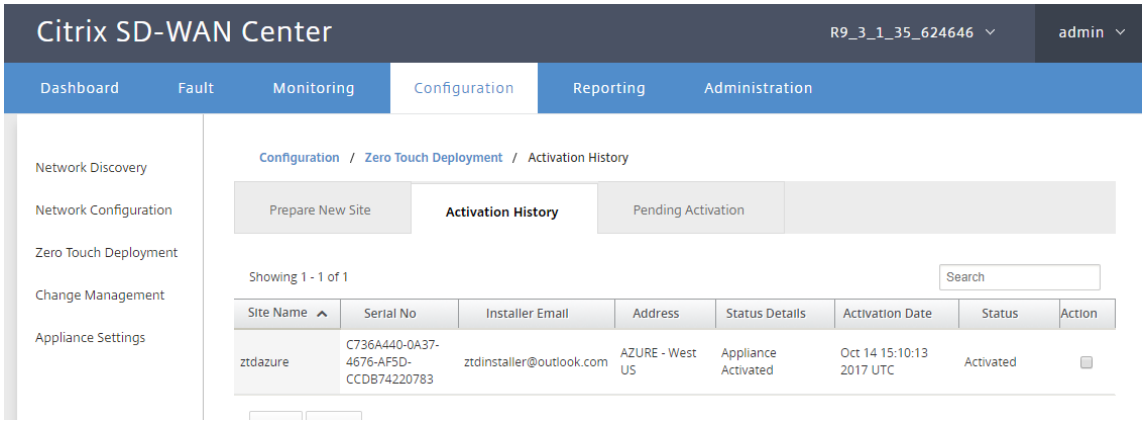


9. La página Estadísticas de supervisión de Citrix SD-WAN identificará la conectividad correcta desde el MCN a la instancia de SD-WAN en Azure.



10. Además, el intento de Provisioning correcto (o incorrecto) se registrará en la página Historial de activación de SD-WAN Center.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Implementación de una región

May 7, 2021

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.

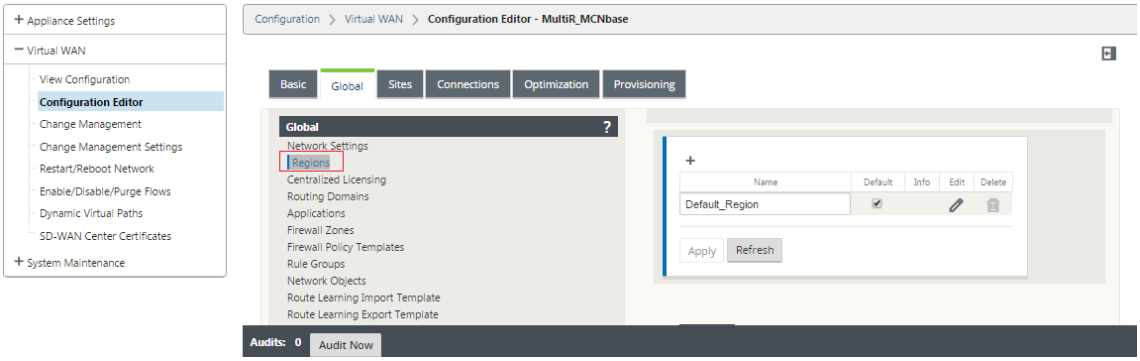
Puede configurar una región predeterminada en el Editor de configuración de la GUI del dispositivo SD-WAN. El editor Basic es útil para crear solo una pequeña red con nodos MCN y SD-WAN de cliente. Para configurar una red multiregión con MCN, RCN, Clientes o funciones avanzadas, utilice otras opciones de configuración en el editor de configuración.

Para configurar la implementación de una sola región:

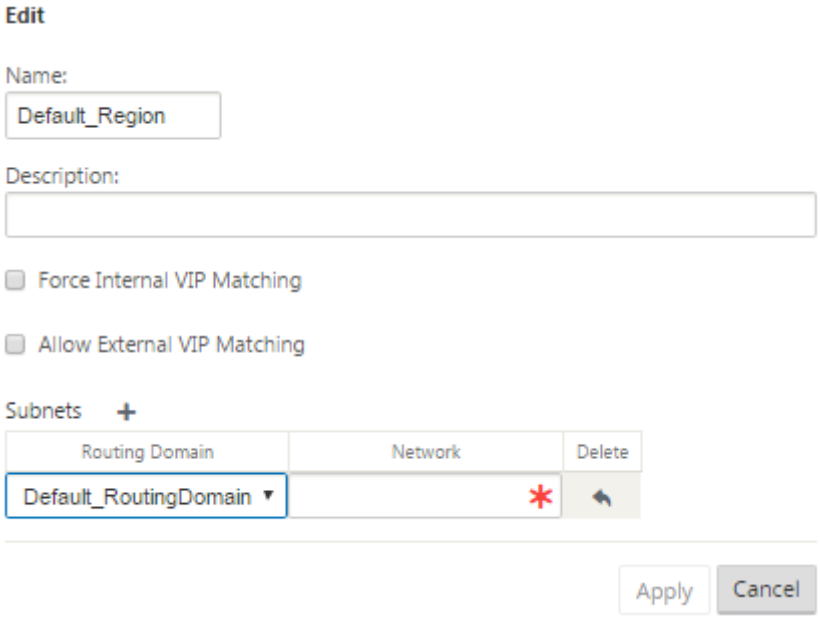
1. Acceda a la ficha **Global** del Editor de configuración. Seleccione **Regiones**. Se muestran las opciones de configuración de región predeterminadas.

   Puede cambiar el nombre y la descripción de la región predeterminada editándola.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Modifique **Default_Region** para cambiar el nombre y configurar las subredes.
3. Habilite la coincidencia VIP de intervalo según si quiere **Coincidencia VIP interna forzada** o **Permitir Coincidencia VIP externa**.
   - VIP interno forzado: Cuando está habilitado, todas las direcciones IP virtuales no privadas de la región se ven obligadas a coincidir con las subredes configuradas.
   - VIP externo permitido: Cuando está habilitado, las direcciones IP virtuales no privadas de otras regiones pueden coincidir con las subredes configuradas.
4. Haga clic en + para agregar subredes.



5. Seleccione un **dominio de enrutamiento**, introduzca la dirección de **red** . Haga clic en **Aplicar**. La dirección de red es la dirección IP y la máscara de la subred.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Implementación en varias regiones

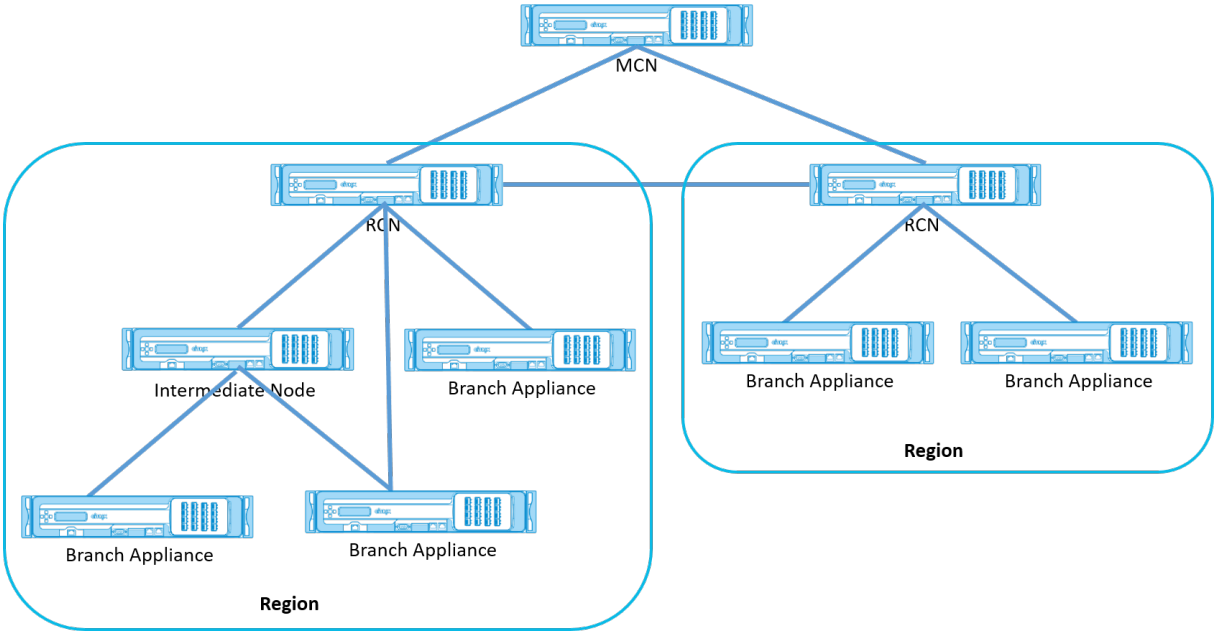
May 7, 2021

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 550 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.



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

> **NOTA**
>
> - El dispositivo Premium Edition (PE) se conocía anteriormente como Enterprise Edition (EE).
> - Utilice el dispositivo Citrix SD-WAN 210 SE como un MCN solo en las redes administradas por SD-WAN Orchestrator.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

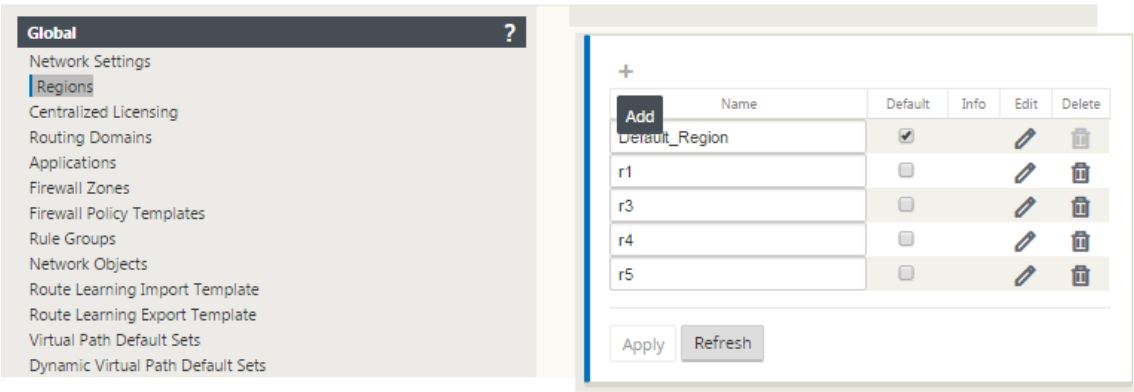
Edición de plataforma	MCN primario/secundario	RCN primario/secundario
210-SE	Sí	Sí
400-SE	Sí	No
410-SE	Sí	No
1000-SE, 1000-PE	Sí	No
1100-SE, 1100-PE	Sí	Sí
VPX-SE, VPXL-SE	Sí	Sí
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	Sí	Sí

Para configurar la implementación de varias regiones para una red SD-WAN:

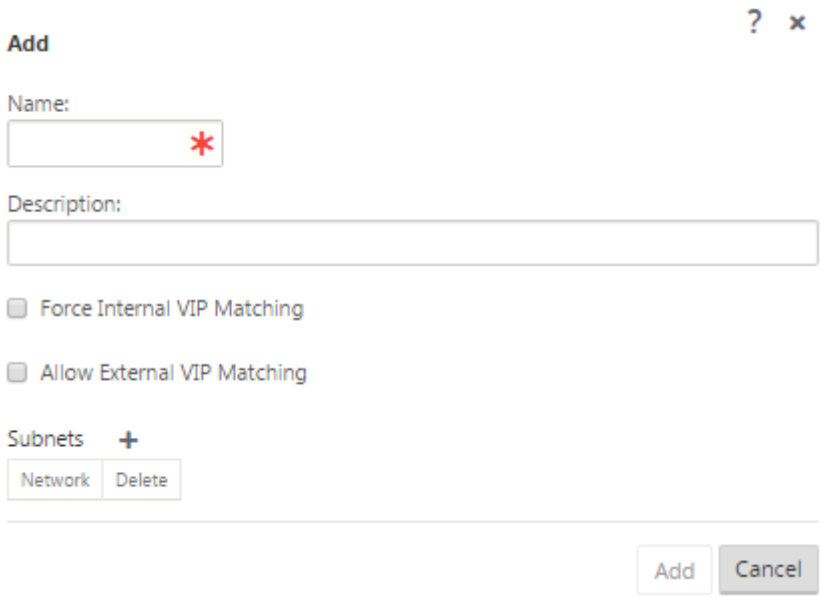
1. Acceda a la ficha **Global** del Editor de configuración. Seleccione **Regiones**. Se muestran las opciones de configuración de región predeterminadas.

   Puede cambiar el nombre y la descripción de la región predeterminada editándola.

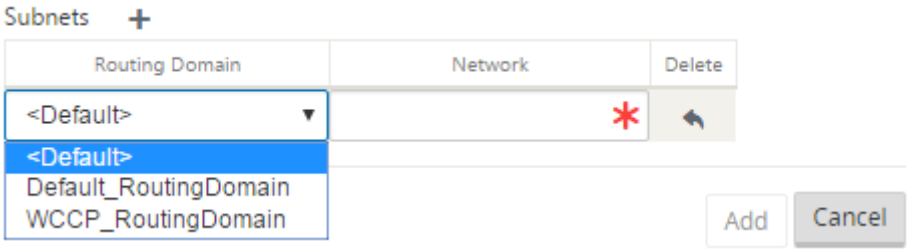
2. Haga clic en **+ Agregar** para agregar una nueva región.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



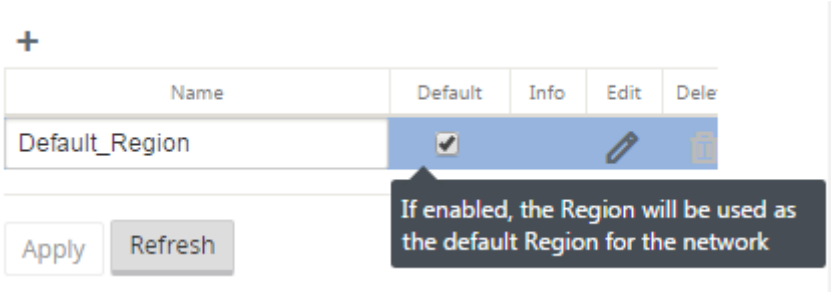
3. Introduzca un nombre y una descripción para la región.
4. Habilite la coincidencia VIP interna en función de si quiere **Coincidencia VIP interna forzada** o **Permitir Coincidencia VIP externa**.
   - VIP interno forzado: Cuando está habilitado, todas las direcciones IP virtuales no privadas de la región se ven obligadas a coincidir con las subredes configuradas.
   - VIP externo permitido: Cuando está habilitado, las direcciones IP virtuales no privadas de otras regiones pueden coincidir con las subredes configuradas.
5. Haga clic en + para agregar subredes. Elija un dominio de redirección.



6. Introduzca una dirección **de red**. Haga clic en**Agregar.** La dirección de red es la dirección IP y la máscara de la subred. La región recién creada se agrega a la lista de regiones existente.

   Puede activar la casilla de verificación **Predeterminado (Default**) para utilizar la región deseada como Default (Default).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Puede clonar MCN en un sitio GEO o cliente.

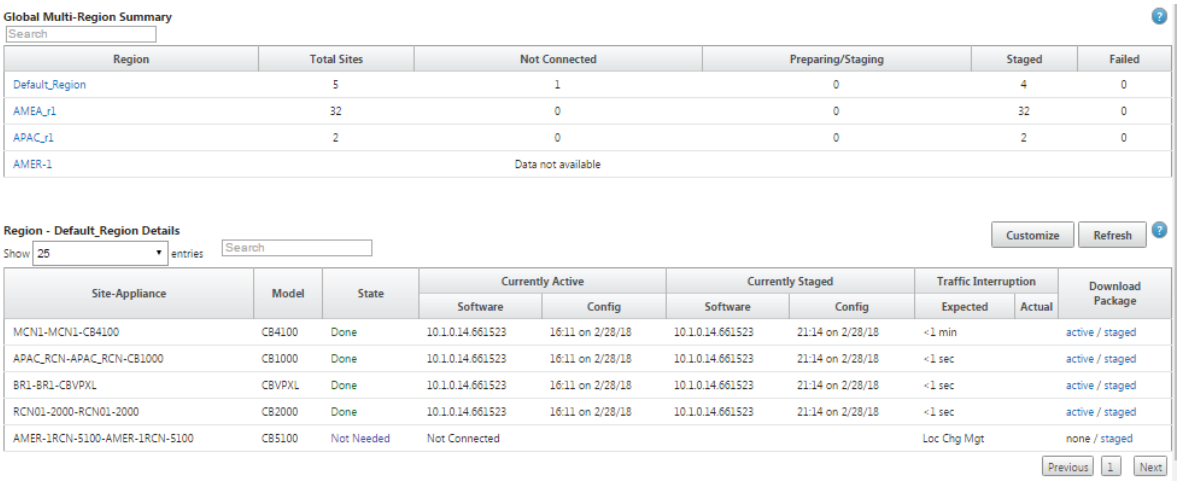
SD-WAN Center admite la implementación en varias regiones. Para obtener más información, consulte Implementación e informes en varias regiones de SD-WAN Center.

Vista de resumen de gestión de cambios

Al realizar el proceso de administración de cambios para dispositivos configurados en implementación de varias regiones, la tabla de resumen de administración de cambios se muestra en la GUI del dispositivo SD-WAN.

La columna **Región** muestra una lista de regiones configuradas actualmente en la red. Puede ver el resumen de administración de cambios para una región específica seleccionándolo en la tabla de resumen.

Resumen de región predeterminado:



Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - Default_Region Details

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 min		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
AMER-1RCN-5100-AMER-1RCN-5100	CB5100	Not Needed	Not Connected				Loc Chg Mgt		none / staged

Previous 1 Next

Resumen de la región:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - AMEA_r1 Details

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous 1 2 Next

> **Nota**
>
> En algunos casos, el valor **Total de sitios** que se muestra en la tabla **Resumen global de varias regiones** es menor que la suma de las columnas restantes.
>
> Por ejemplo, cuando un nodo de rama no está conectado, es posible que la rama se cuente dos veces; una vez como "No conectado"y otra como "Preparación/Puesta en escena. "

Configurar la funcionalidad LTE en el dispositivo 210 SE LTE

September 26, 2023

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

plataforma de hardware Citrix SD-WAN 210-SE LTE, consulte Dispositivos Citrix SD-WAN 210 Standard Edition.

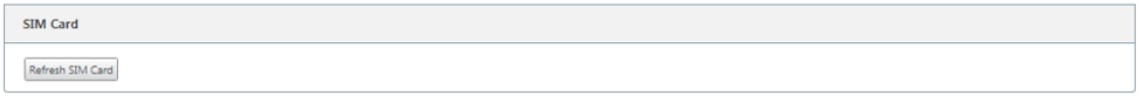
Introducción a Citrix SD-WAN 210-SE LTE

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 las antenas LTE.
3. Encienda el dispositivo.

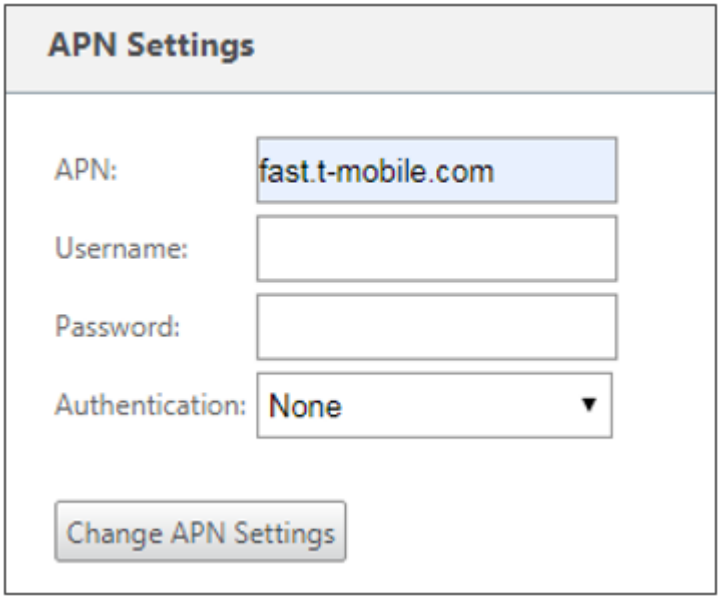
   > **Nota**
   >
   > Si ha insertado la SIM en un dispositivo que ya está encendido y arrancado, vaya a **Configuración > Configuración del dispositivo > Adaptadores de red > Banda ancha móvil > Tarjeta SIM** y haga clic en **Actualizar tarjeta SIM**.



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

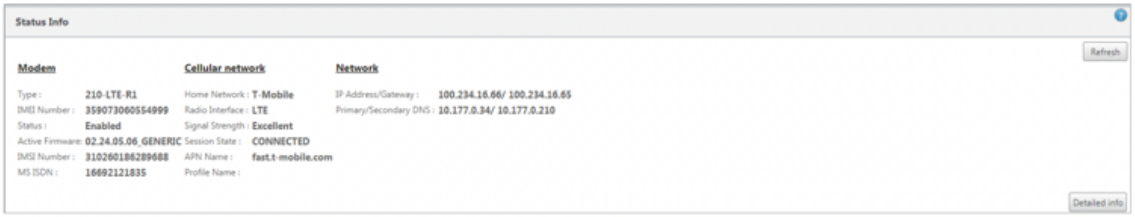
   > **Nota:**
   > Obtenga la información de APN del transportista.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Introduzca el **APN**, el nombre de **usuario**, **la contraseña**y la **autenticación**proporcionados por el transportista. 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**.

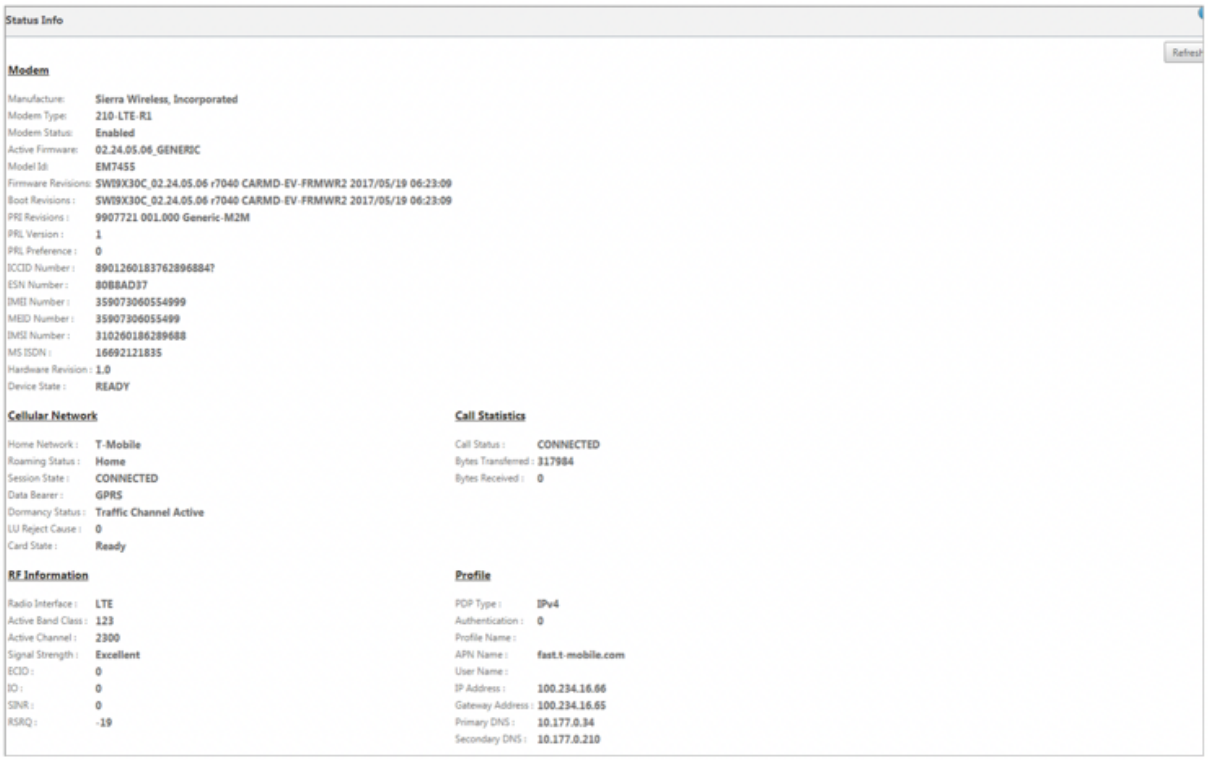
   Puede ver la información de estado de la configuración de banda ancha móvil.



A continuación se muestra información de estado útil:

- **Estado**: Habilitado indica que el módem intenta establecer la sesión de datos.
- **Estado de la tarjeta**: Presente indica que la tarjeta SIM está insertada correctamente.
- **Fuerza de la señal**: Calidad de la intensidad de la señal: Excelente, buena, justa, pobre o sin señal.
- **Red doméstica**: Portador de la SIM insertada.
- **Nombre de APN: Nombre**del punto de acceso utilizado por el módem LTE.
- **Estado de la 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.

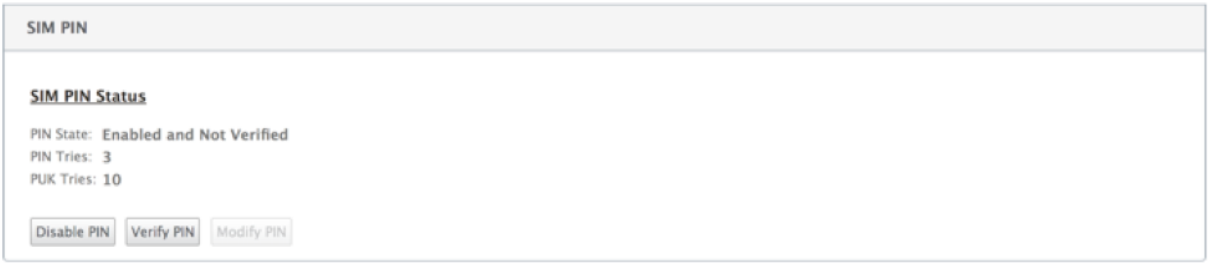
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



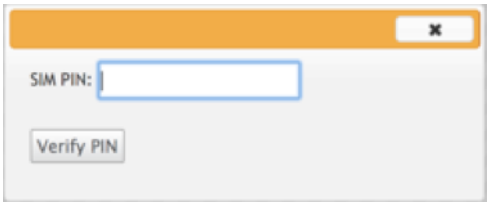
PIN SIM

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

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



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

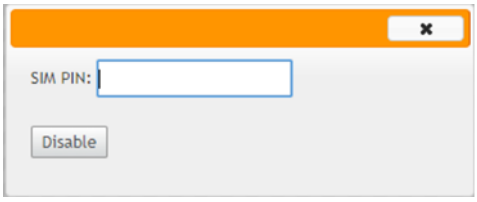


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Inhabilitar PIN SIM

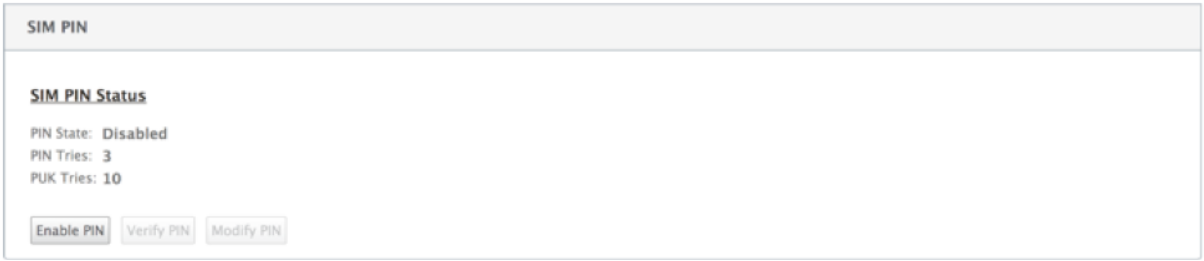
Puede optar por inhabilitar la funcionalidad PIN de SIM para una SIM para la que el PIN de SIM esté habilitado y verificado.



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

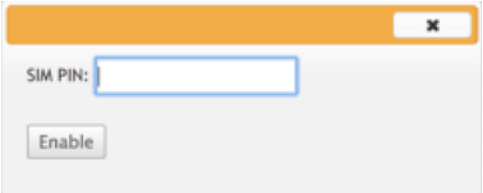
Habilitar PIN SIM

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

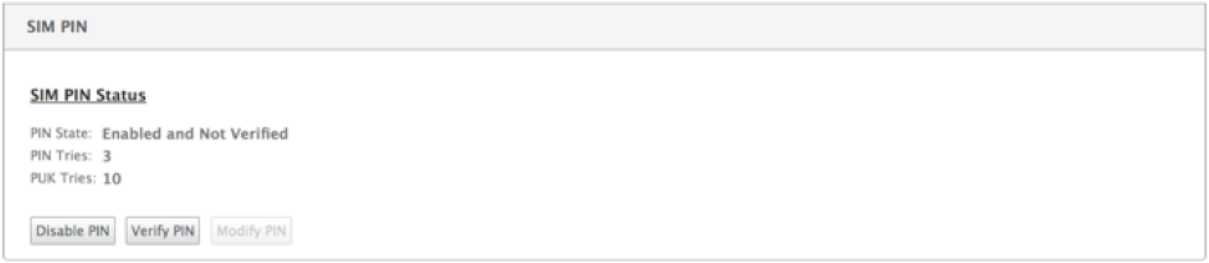


Haga clic en **Habilitar PIN**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador y haga clic en **Habilitar**.

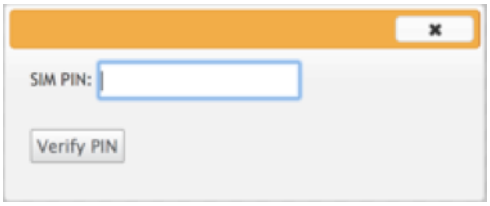
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

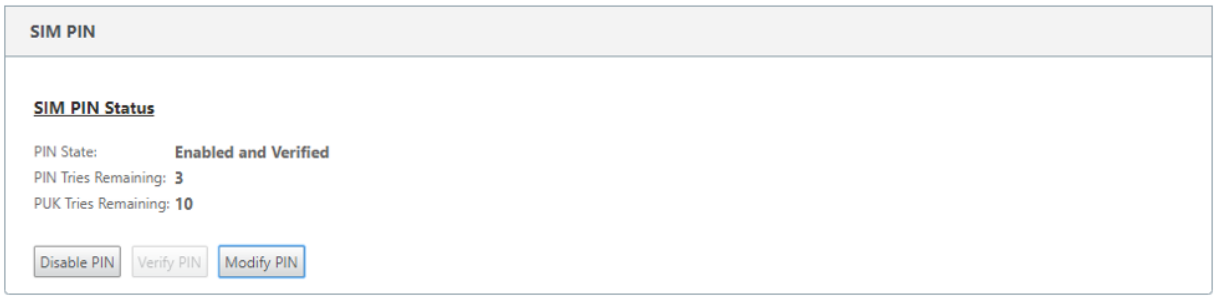


Haga clic en **Verificar PIN**. Introduce el PIN de SIM proporcionado por el operador y haz clic en **Verificar PIN**.



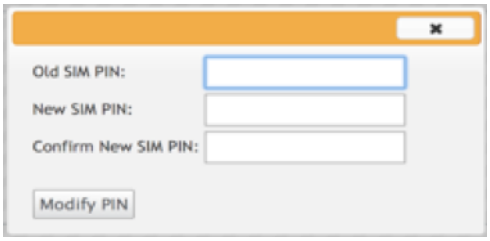
Modificar PIN SIM

Una vez que el PIN esté en estado **Activado 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**.

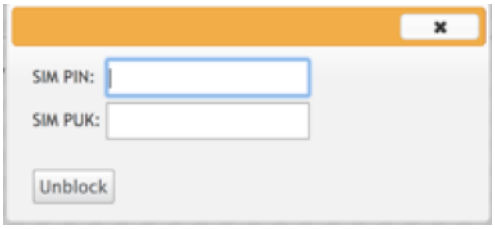
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



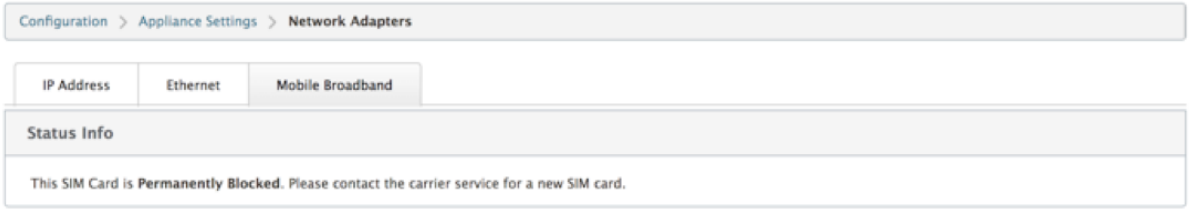
Desbloquear SIM

La tarjeta SIM se bloquea con tres intentos fallidos de entrada PIN de SIM y no tendrá acceso a la funcionalidad LTE. Puede desbloquear la SIM mediante la SIM PUK obtenida del operador.

Para desbloquear una SIM, haz clic en **Desbloquear**. Introduzca el **PIN de SIM y SIM PUK** 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. Debes ponerte en contacto con el proveedor de servicios del operador para obtener una nueva tarjeta SIM.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Administrar firmware

Cada dispositivo que tenga LTE habilitado tendrá 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 para permitir que el módem LTE elija el firmware más adecuado en función de la tarjeta SIM insertada.

> **NOTA**
>
> Con la versión 11.0.3, el firmware activo de LTE se actualiza como parte del paquete de actualización de un solo paso. Para actualizar, debe actualizar la ventana de programación mediante la página Configuración de administración de cambios o esperar a la hora programada predeterminada para actualizar el firmware LTE (diariamente a las 21:20:00).

Activar/desactivar módem

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

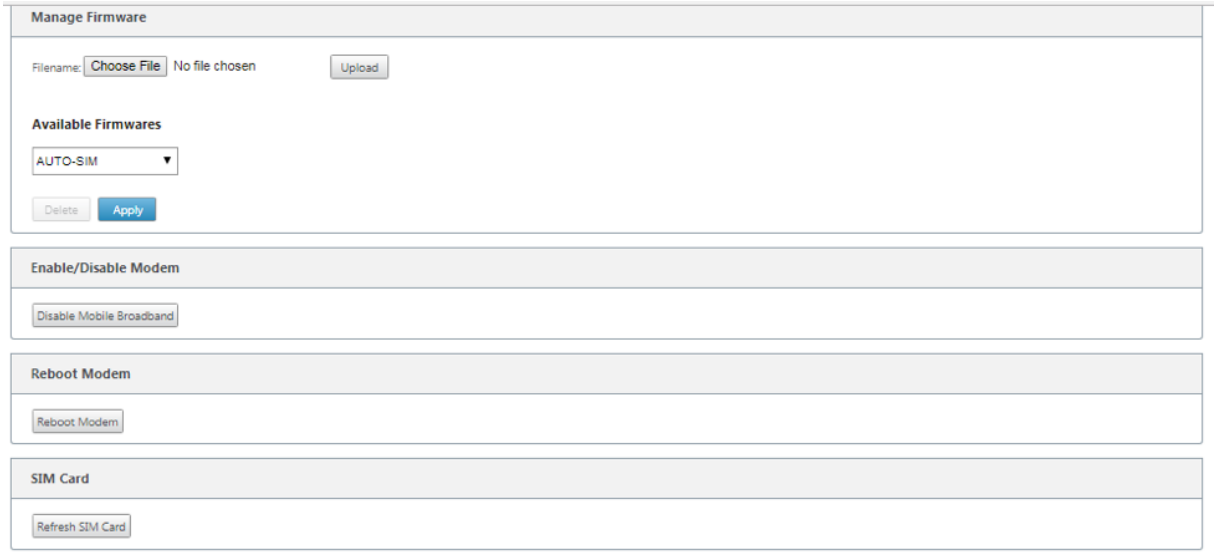
Reiniciar el módem

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 por el módem LTE 210-SE.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

Configurar la funcionalidad LTE usando CLI

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

1. Inicie sesión en la consola del dispositivo Citrix SD-WAN.
2. En el símbolo del sistema, 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

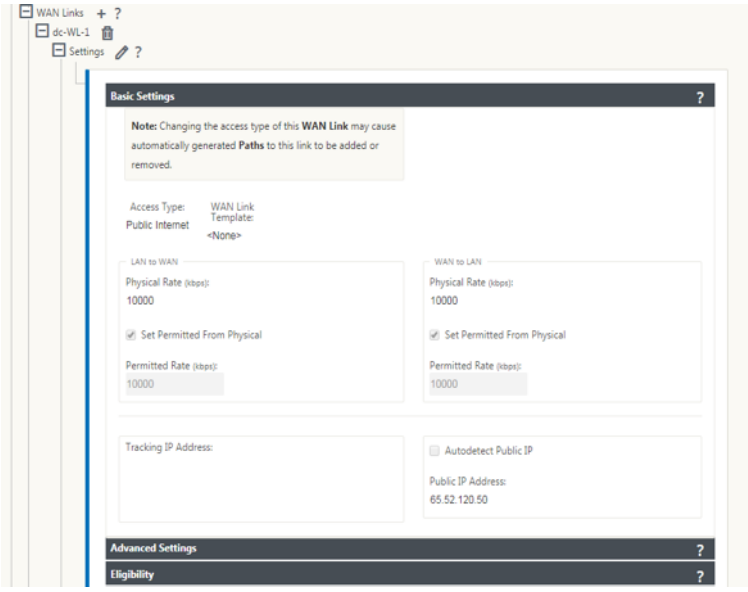
Comando	Descripción
Ayuda {lte>ayuda}	Enumera los comandos y parámetros de LTE disponibles
Estado {lte>status}	Muestra el estado de conectividad LTE
Mostrar {lte>show}	Muestra la configuración de LTE
Inhabilitar {lte>disable}	Inhabilita el módem LTE
Habilitar {lte>enable}	Habilita el módem LTE
Apn {lte>apn}	Configura la información de configuración de APN
SIM-apagado, encendido, reinicio> {lte>sim-apagado, encendido, reinicio}	Se apaga la tarjeta SIM, se enciende la tarjeta SIM, se actualiza la tarjeta SIM
PIN de SIM {lte>pin sim-pin}	Se apaga la tarjeta SIM, se enciende la tarjeta SIM, se actualiza la tarjeta SIM
Reiniciar {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

Configurar MCN para LTE

Para configurar un MCN:

1. Inicie sesión en la GUI del dispositivo SD-WAN. Vaya al Editor de configuración. Configuración completa para el sitio de MCN, consulte Configurar MCN.
2. Asegúrese de proporcionar una dirección IP pública enrutable como parte de la configuración del enlace WAN. No es necesario configurar la dirección IP pública para los dispositivos cliente.

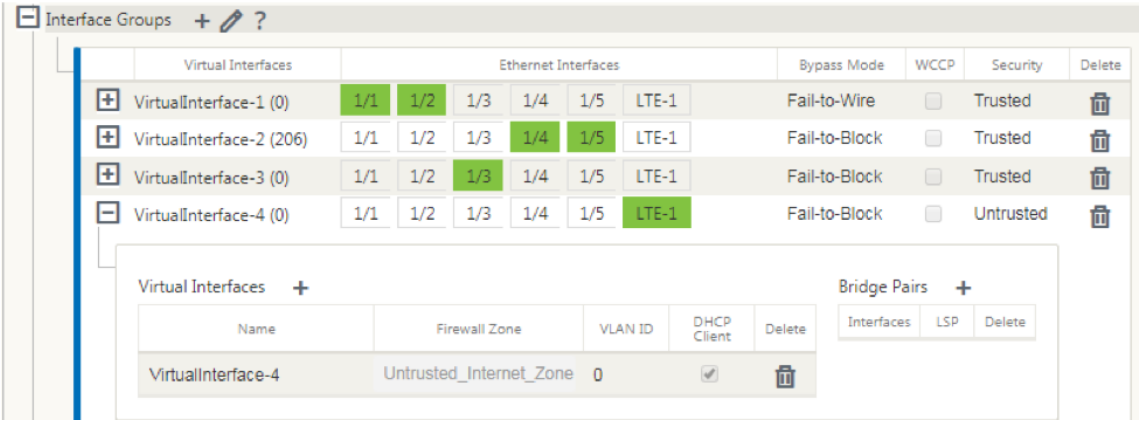
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configurar sucursal para LTE

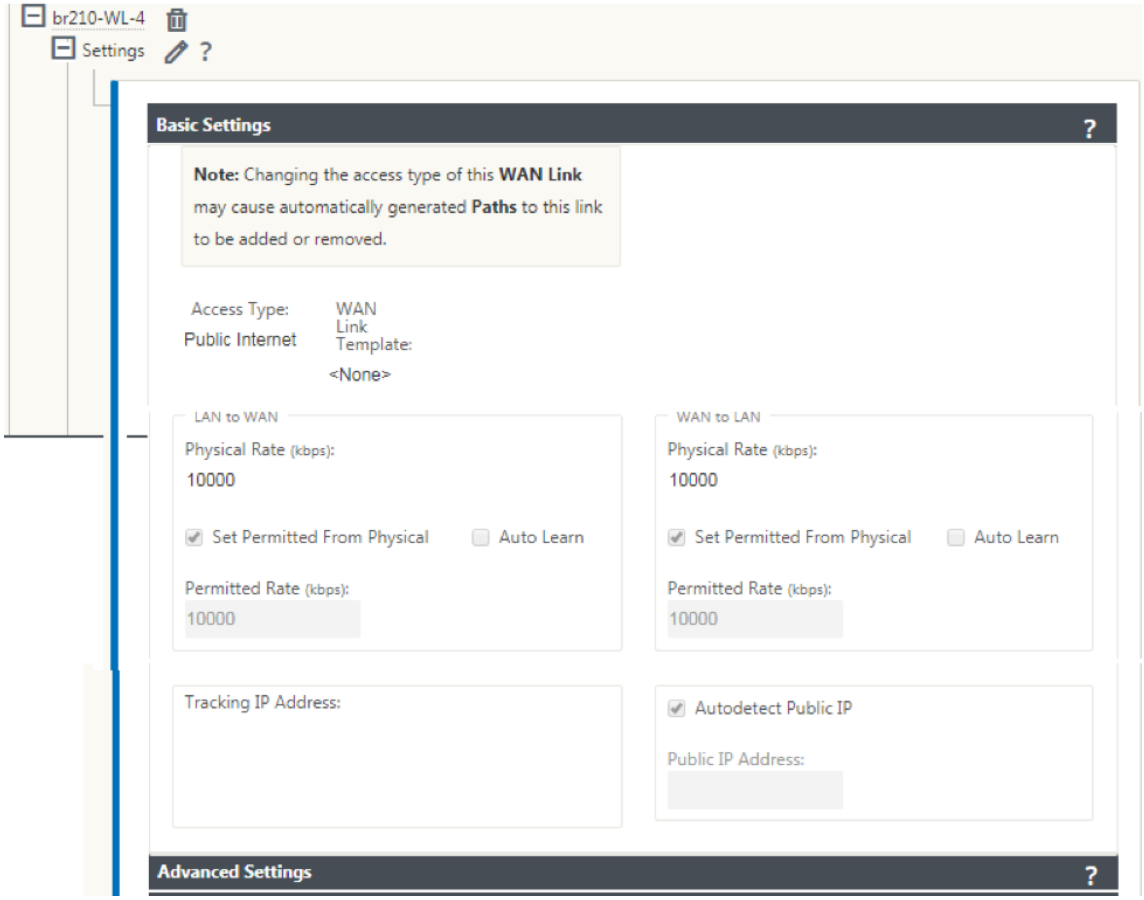
Para configurar el dispositivo LTE 210-SE como un sitio de sucursal:

1. En la GUI del dispositivo SD-WAN, vaya al editor de configuración. Consulte Configurar sucursal.
   - Crear grupos de interfaz.
   - Cree hasta una interfaz virtual y un grupo de interfaces para que el adaptador LTE configure el enlace WAN seleccionando lo siguiente:
     - Interfaz Ethernet: LTE 1
     - Seguridad: No confiable (predeterminado)
     - Cliente DHCP: Habilitado (predeterminado)

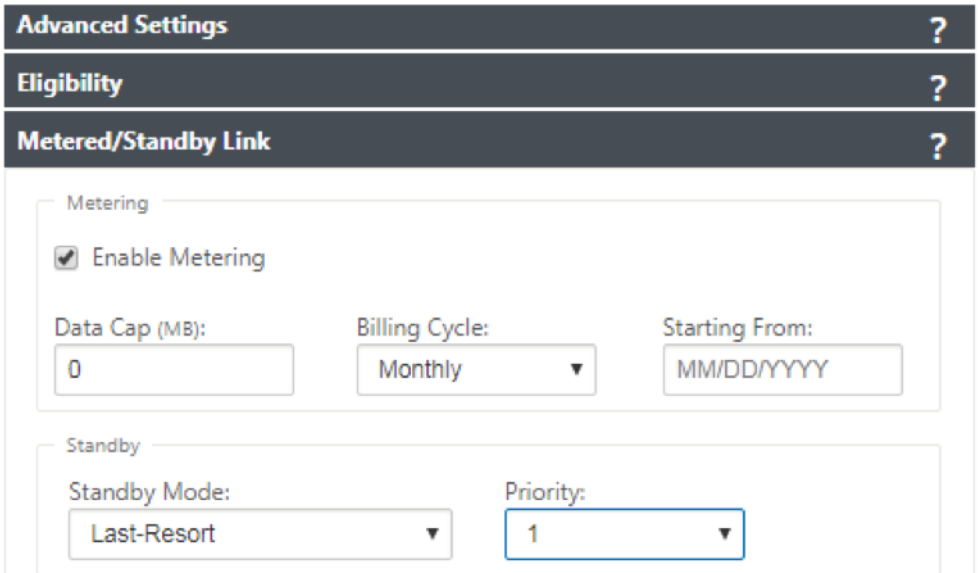


2. Habilite **AutoDetect Public IP** para la configuración de enlaces WAN al configurar el enlace WAN mediante la interfaz virtual creada para la interfaz LTE.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



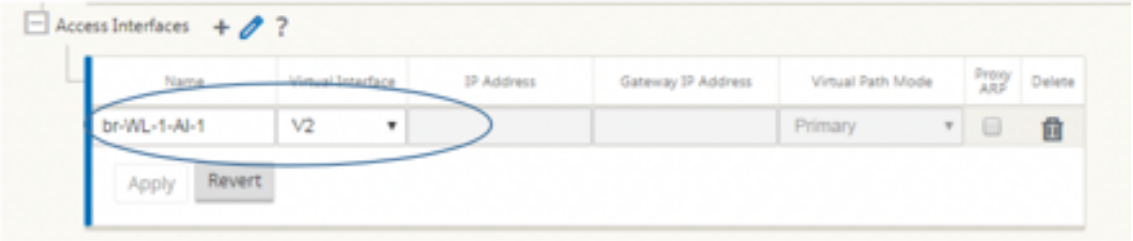
3. De forma predeterminada, cuando intenta configurar el enlace WAN mediante la interfaz LTE, el enlace WAN se marca como Enlace medido y modo de espera de último recurso. Puede cambiar esta configuración predeterminada, si es necesario.



No es necesario configurar la dirección IP y la dirección de Gateway para la interfaz de acceso

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

del enlace WAN porque recibe esa información del operador a través de DHCP.



4. Completa el resto de la configuración de Branch requerida para el dispositivo LTE 210-SE. Consulte Configurar sucursal.
5. Realice la gestión de cambios cargando el software SD-WAN. Consulte la Procedimiento de gestión de cambios.
6. Active la configuración mediante el proceso de administración de cambios locales. Al realizar la administración de cambios, la configuración se activa y se aplica la configuración necesaria.

Implementación sin contacto a través de LTE

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

1. Instale la antena y la tarjeta SIM para el dispositivo 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 un 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 solo cuando el puerto de administración no se ha conectado.

Puede utilizar la GUI del centro de SD-WAN para implementar y configurar el dispositivo LTE 210-SE para el servicio de implementación sin contacto.

Consulte procedimiento de implementación sin contacto para obtener más información acerca de la implementación y configuración del dispositivo LTE 210-SE mediante SD-WAN Center.

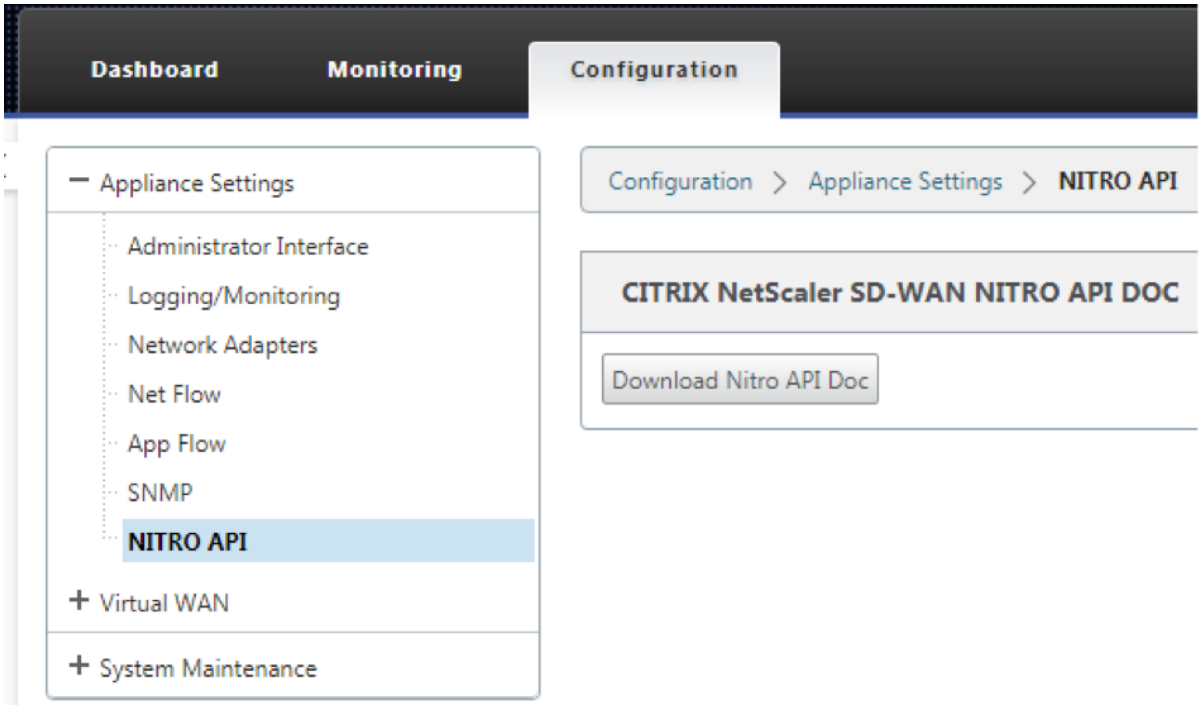
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Conecte el puerto de administración y use el estándarprocedimiento de implementación sin contactoque es compatible con todas las demás plataformas que no sean LTE.

LTE REST API

Para obtener información acerca de la API REST 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 REST para la funcionalidad PIN de SIM se introduce en Citrix SD-WAN 11.0.



Sistema de nombres de dominio

May 7, 2021

El Sistema de nombres de dominio (DNS) traduce nombres de dominio legibles por humanos a direcciones IP legibles por máquina, y viceversa. Las siguientes funciones DNS se introducen en la versión 10 de SD-WAN versión 2:

- Proxy DNS
- Reenvío transparente DNS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

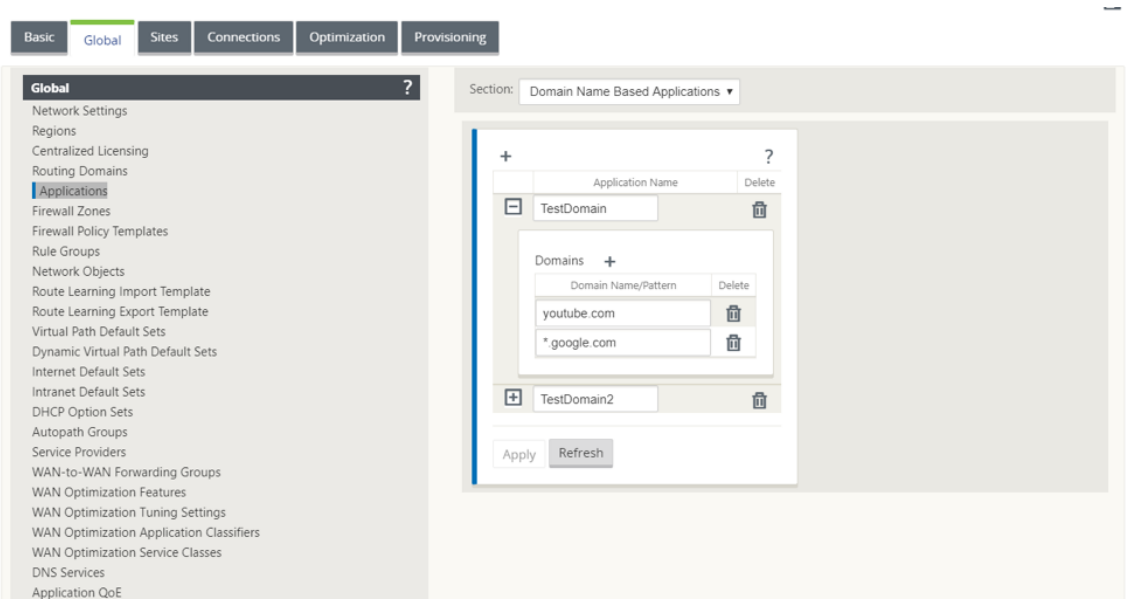
Proxy DNS

El**proxy DNS** intercepta las solicitudes DNS destinadas a la dirección IP SD-WAN y la reenvía a los servicios DNS selectivos. 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 configurar SD-WAN como proxy DNS:

1. Defina las aplicaciones basadas en nombres de dominio. En el Editor de configuración, vaya a **Global > Aplicaciones > Aplicaciones basadas en nombres de dominio**.

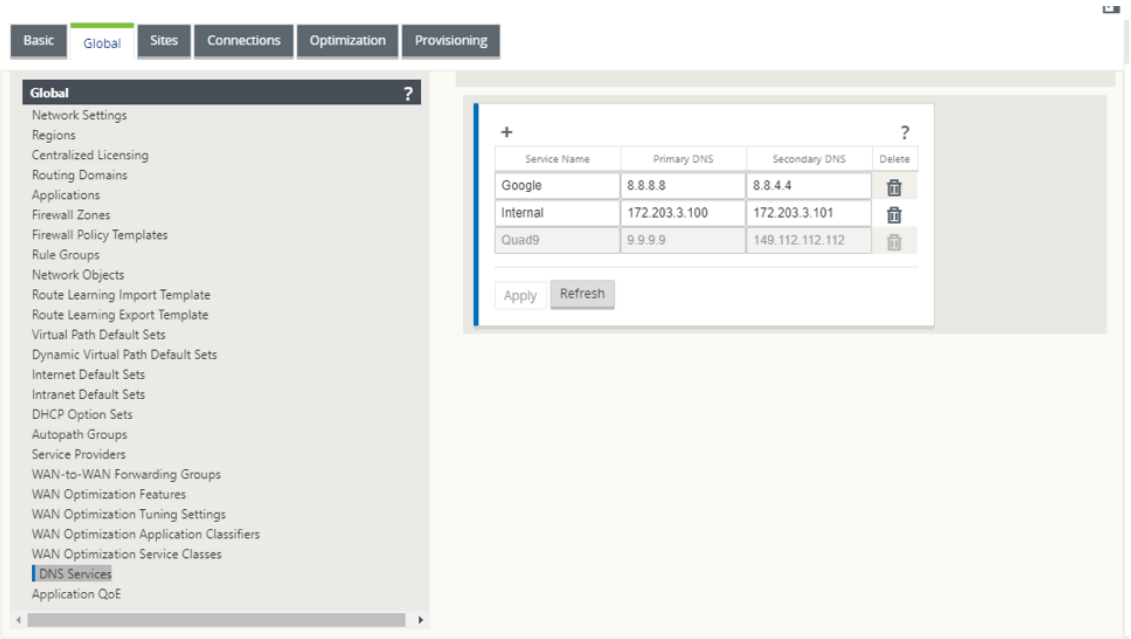
   Introduzca el nombre de la aplicación y los nombres de dominio o patrones requeridos. Puede agrupar varios nombres de dominio como una aplicación. Puede introducir el nombre de dominio completo o utilizar comodines al principio. Por ejemplo - *.google.com



2. Defina los Servicios DNS requeridos. Desplácese a **Global > Servicio DNS**. Introduzca el **nombre del servicio** y un par de **direcciones IP del servidor DNS principal y secundario**.

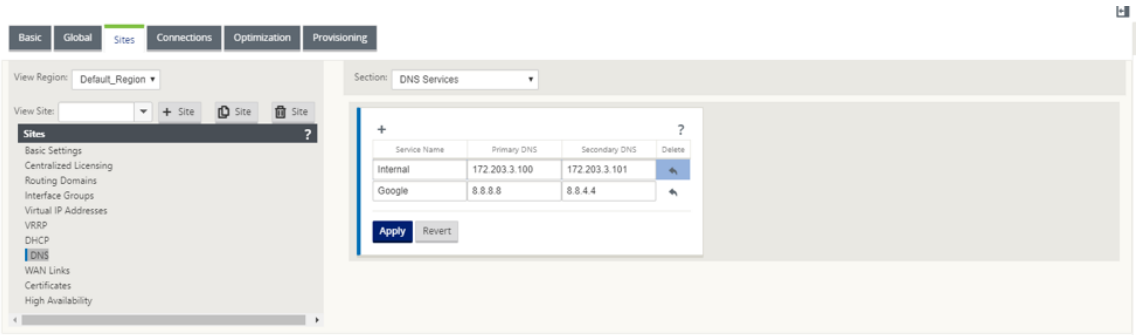
   Puede crear internos, ISP, google o cualquier otro servicio DNS de código abierto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**:
>
> Si ha configurado la directiva de grupo de Office 365, se crea automáticamente un servicio DNS de Quad9. Para obtener más información, consulte Optimización de Office 365.

También puede definir los servicios DNS a nivel de sitio individual. La configuración del servicio DNS de nivel de sitio anula la configuración global. Para configurar el servicio DNS específico del sitio, vaya a **Sitios > DNS > Servicios DNS**. Introduzca el **nombre del servicio** y un par de **direcciones IP del servidor DNS principal y secundario**.

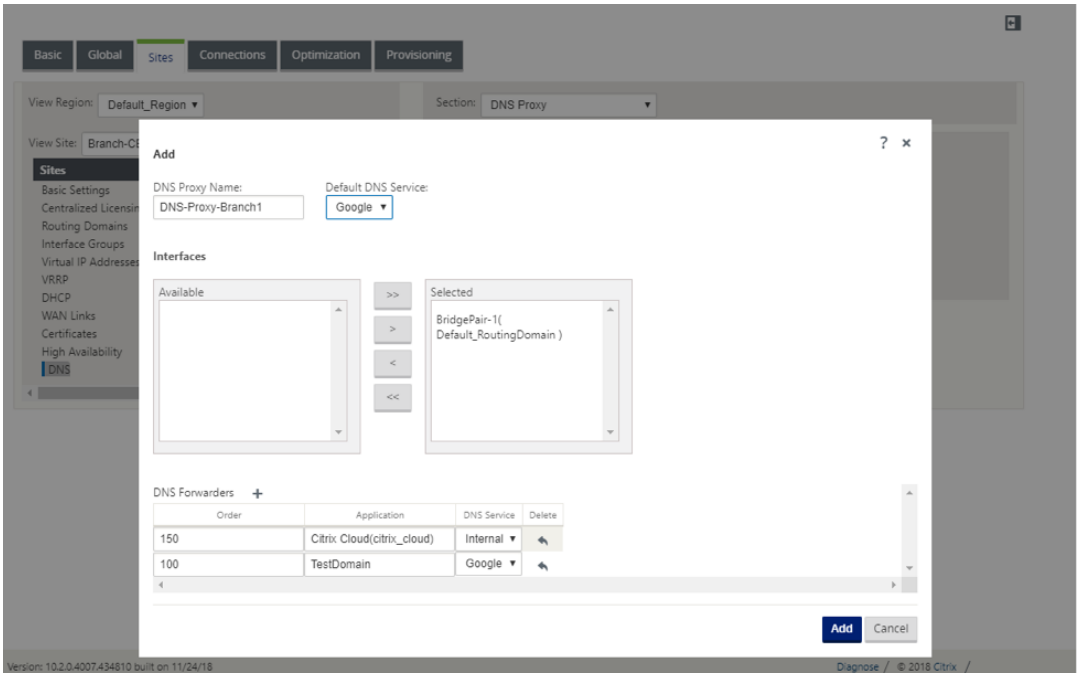


3. Configurar proxy DNS para el sitio. Desplácese hasta **Sitios > DNS > Proxy DNS**. Haga clic en **+**. Introduzca valores para los siguientes parámetros:

   - **Nombre del proxy DNS**: nombre del proxy DNS.
   - **Servicio DNS predeterminado: Servicio**DNS predeterminado al que se reenviarán las solicitudes DNS, si ninguna de las aplicaciones coincide en la búsqueda del reenviador DNS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Interfaces**: Las interfaces en las que se interceptarán las solicitudes DNS. Solo se permiten las interfaces de confianza.
- **Reenviadores DNS**: Lista de reenviadores DNS.
  - **Orden**: La prioridad del reenviador.
  - **Aplicación**: Aplicaciones para las que las solicitudes DNS deben reenviarse al servicio DNS seleccionado.
  - **Servicio DNS**: El servicio DNS al que se reenviará la solicitud DNS para la aplicación especificada.



Reenviador transparente DNS

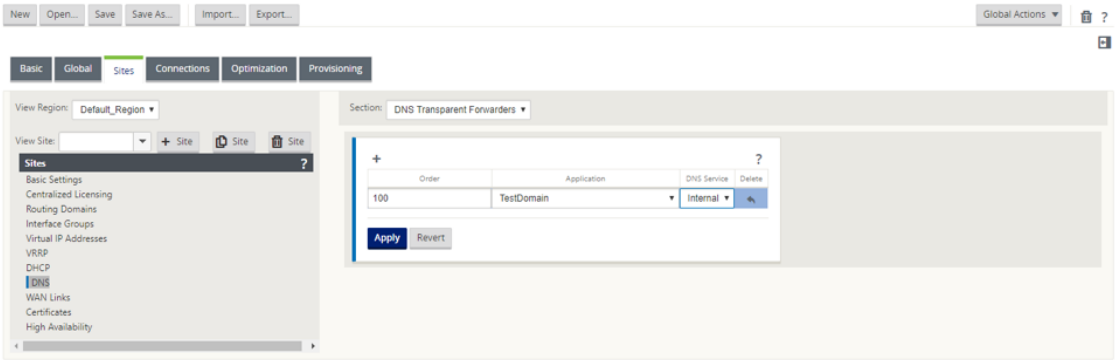
SD-WAN se puede configurar como un reenviador DNS transparente. En este modo, SD-WAN puede interceptar solicitudes DNS que no están destinadas a su dirección IP y reenviarlas al servicio DNS especificado. Solo se interceptan las solicitudes DNS procedentes del servicio local en las interfaces de confianza. 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 las solicitudes que llegan a través de conexiones UDP.

Para configurar SD-WAN como reenviador transparente DNS:

1. Desplácese hasta **Sitios > DNS > Reenviadores transparentes DNS**. Haga clic en **+**.
2. Introduzca valores para los siguientes parámetros:
   - **Orden**: La prioridad del reenviador.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Aplicación**: Aplicaciones para las que las solicitudes DNS deben reenviarse al servicio DNS seleccionado.
- **Servicio DNS**: El servicio DNS al que se reenviará la solicitud DNS para la aplicación especificada.



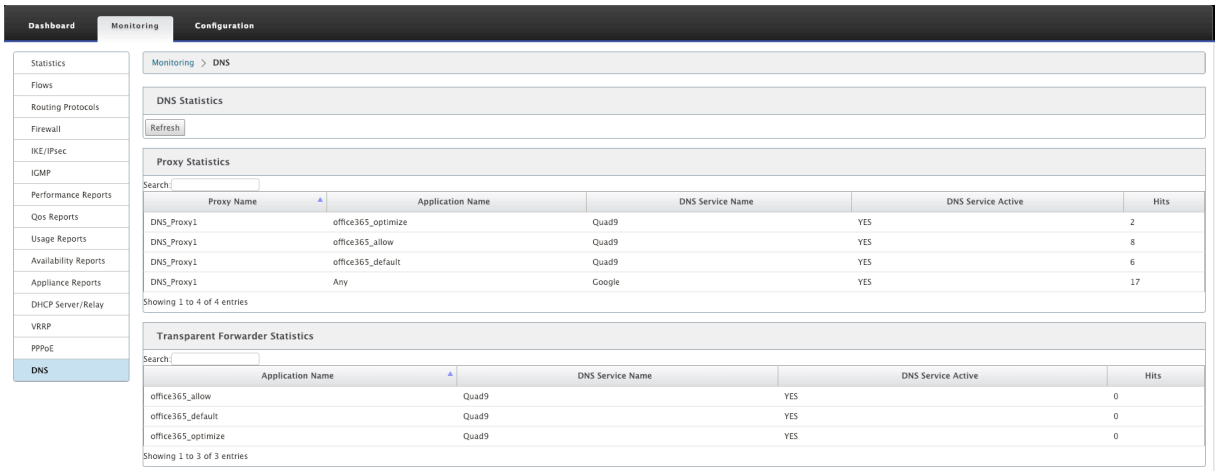
Del mismo modo, continúe agregando otros reenviadores transparentes DNS según sea necesario.

3. Haga clic en **Aplicar**.

Supervisión

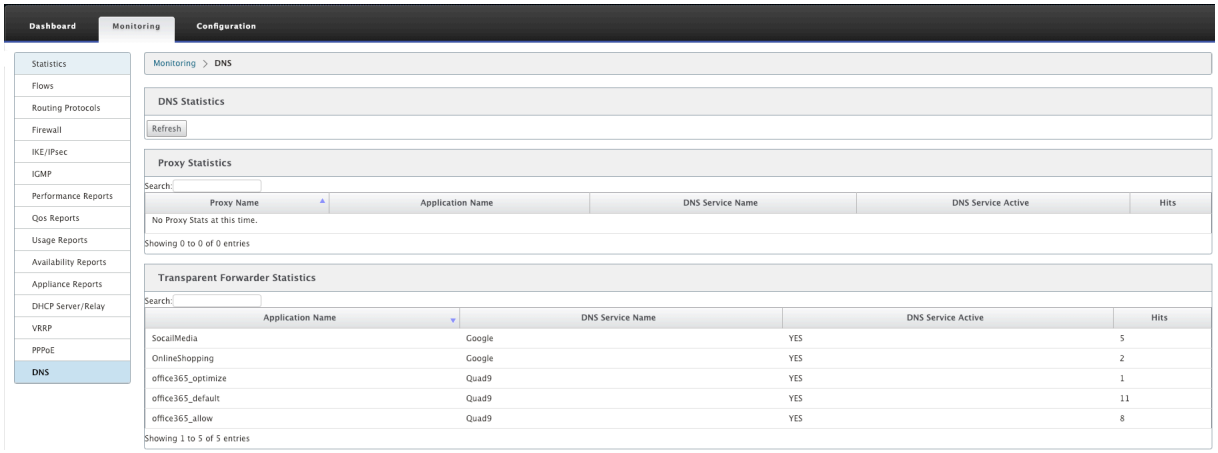
Para ver las estadísticas de proxy y las estadísticas de reenviador transparente, vaya a **Supervisión > DNS**.
Puede ver el nombre de la aplicación, el nombre del servicio DNS, el estado del servicio DNS y el número de visitas al servicio DNS.

Estadísticas de proxy



Estadísticas del reenviador transparente

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Servidor DHCP y retransmisión DHCP

May 7, 2021

Citrix SD-WAN introduce la capacidad de utilizar dispositivos Standard o Premium 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.

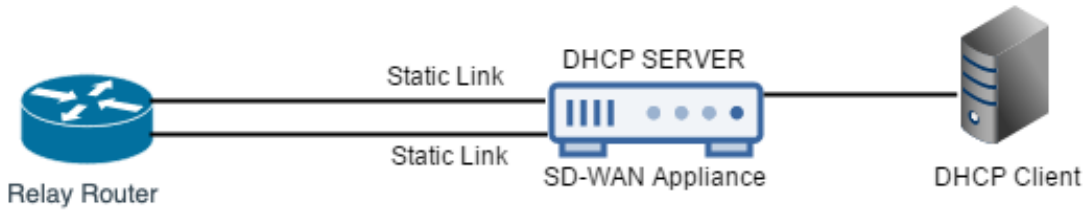
Los siguientes son los beneficios de utilizar las funciones de servidor DHCP y retransmisión DHCP:

- Reduzca la cantidad de equipo en el sitio del cliente.
- Reemplace el enrutador en el sitio del cliente (Fácil implementación de servicios de enrutador perimetral).
- Simplifique la red del sitio del cliente.
- Configuración de Router sin comandos CLI.
- Reduzca la configuración manual en sitios de cliente simples.

Servidor DHCP

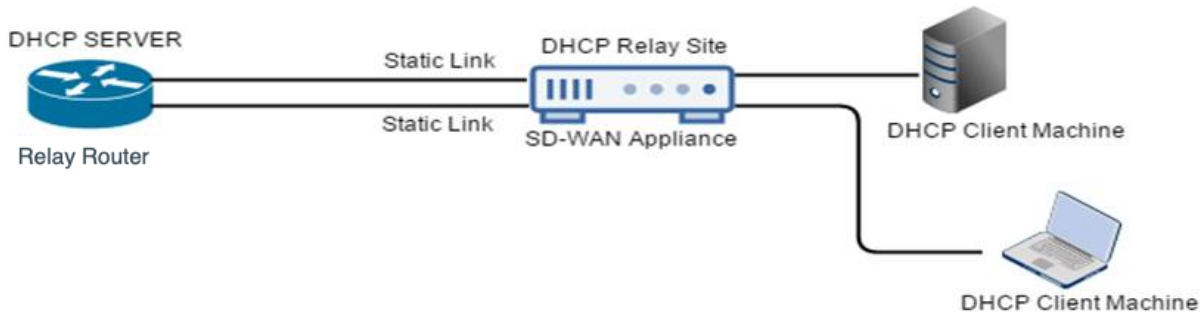
Los dispositivos Citrix SD-WAN se pueden configurar como servidor DHCP. Puede asignar y administrar direcciones IP de grupos de direcciones especificados dentro de la red a clientes DHCP. El servidor DHCP se puede configurar para asignar más parámetros, como la dirección IP del servidor del Sistema de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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Retransmisión 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 desde el servidor DHCP remoto. El agente de retransmisión recibe mensajes DHCP y genera un nuevo mensaje DHCP para enviarlo en otra interfaz.



Configuración del servidor DHCP y la retransmisión DHCP

May 7, 2021

Configurar el servidor DHCP y la retransmisión DHCP mediante el editor de configuración

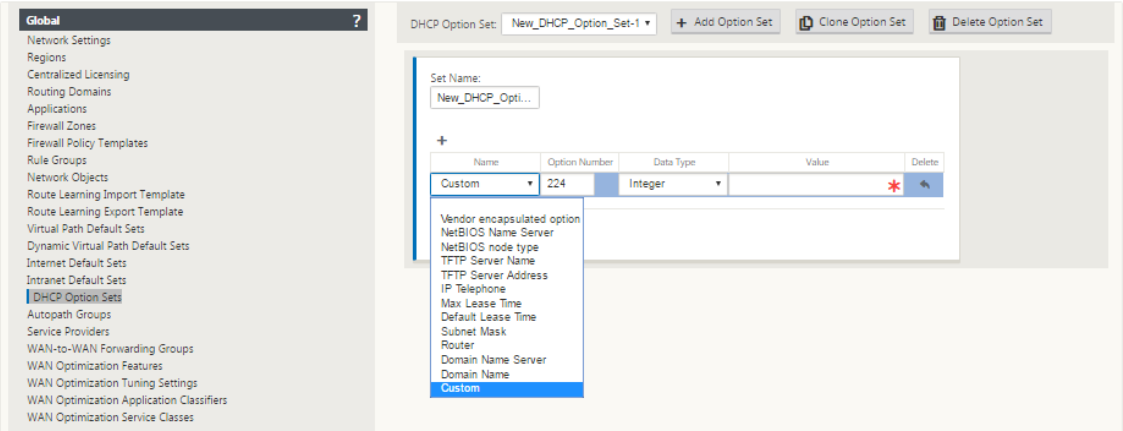
Puede configurar la configuración del servidor DHCP y de la retransmisión DHCP para los dispositivos de la red mediante el editor de configuración. La configuración se envía a los dispositivos de la red SD-WAN a través del proceso de administración de cambios.

Para configurar un sitio como servidor DHCP mediante el editor de configuración:

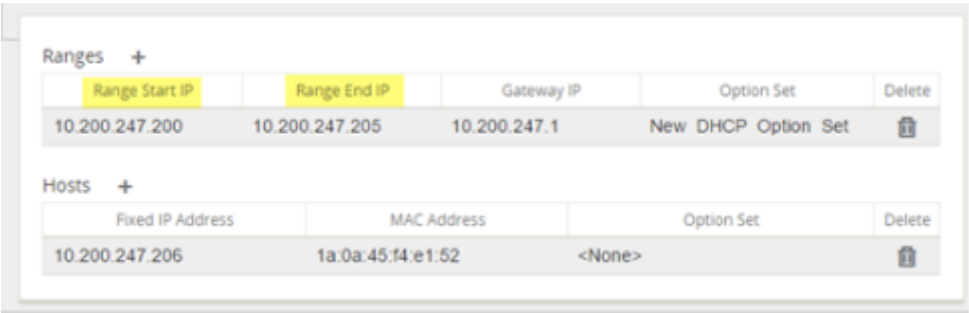
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Vaya al **Editor de configuración** > **Sitios** >[Nombre del sitio] > DHCP > **Subredes de servidor**. Haga clic en **+**.
2. Seleccione un dominio de redirección configurado, si hay varios dominios presentes.
3. Seleccione la **interfaz virtual** que se utilizará para recibir las solicitudes DHCP. La subred IP utilizada por el servidor DHCP para proporcionar direcciones se rellena automáticamente.
4. Introduzca el **nombre de dominio**, el **DNS principal** y el **DNS secundario**. El servidor DHCP reenvía esta información a los clientes.
5. Haga clic en **Habilitar** para habilitar la subred.
6. Configure agrupaciones de direcciones IP dinámicas que se utilizarán para asignar direcciones IP a los clientes. Especifique la dirección IP inicial y final del intervalo y seleccione el **conjunto de opciones**.

> **Nota**
>
> Los conjuntos de opciones DHCP son grupos de configuraciones DHCP que se pueden aplicar a intervalos de direcciones IP individuales. Para crear conjuntos de opciones DHCP, vaya a **Global** > **Conjuntos de opciones DHCP**. Seleccione las opciones DHCP requeridas y especifique un valor para ella.



7. Configure hosts individuales que requieran una dirección IP fija basada en la dirección MAC. Seleccione **Dirección IP fija, DirecciónMAC**y**Conjunto de opciones**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

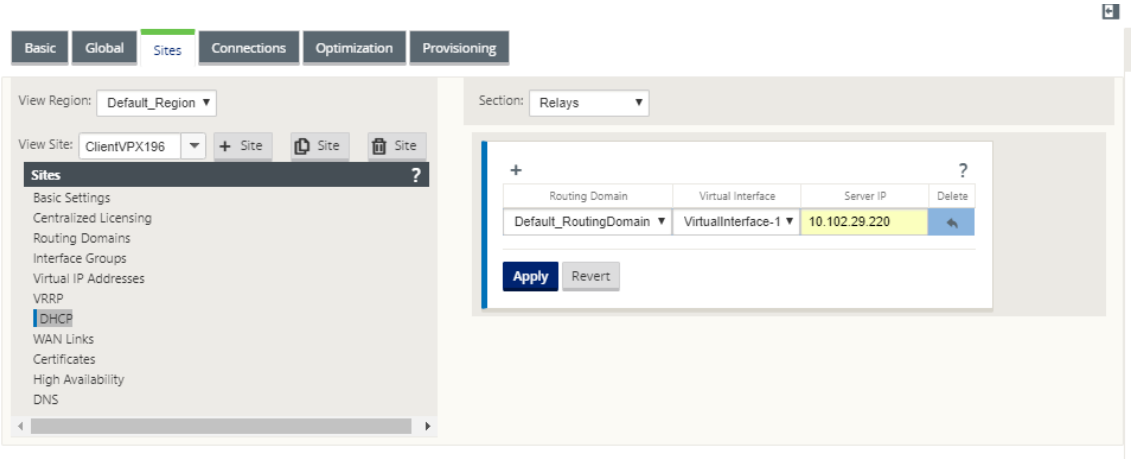
> **Nota**
>
> Para direcciones IP fijas, la **IP de la puerta** de enlace se establece configurando la opción **Router** en el **conjunto de opciones DHCP**.

Para configurar un sitio como retransmisión DHCP mediante el editor de configuración:

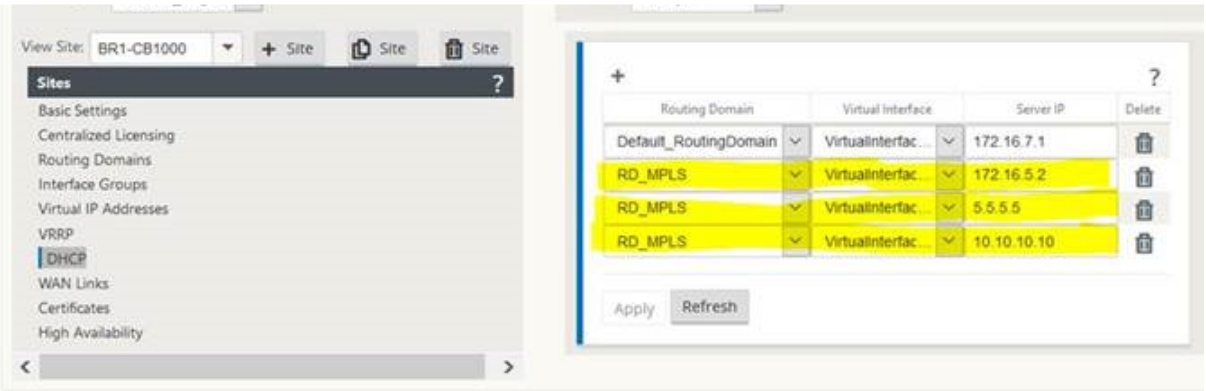
1. Vaya al **Editor** de configuración > **Sitios** >[Nombre del sitio] > **DHCP** > **Relés**. Haga clic en **+**.

   > **Nota**
   >
   > Puede configurar un máximo de 16 relés DHCP.

2. Seleccione un dominio de redirección configurado, si hay varios dominios presentes.
3. Seleccione una interfaz virtual que se comunique con un servidor DHCP remoto.
4. Introduzca la IP del servidor DHCP que utilizará la retransmisión para reenviar la solicitud y la respuesta de los clientes.

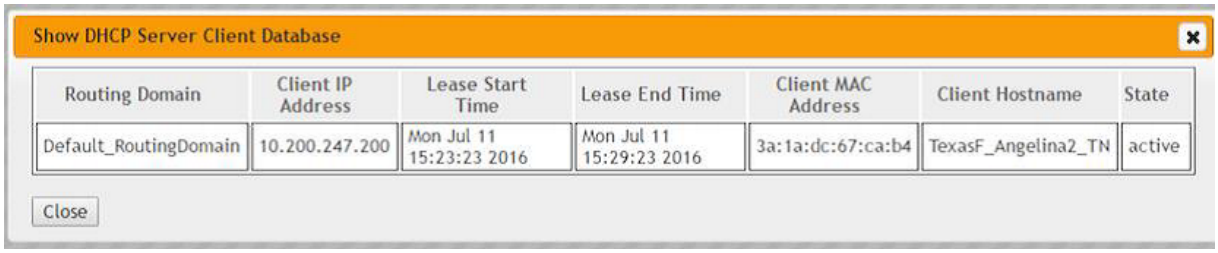


Puede configurar una única retransmisión DHCP mediante una interfaz de red virtual común y señalarla a varios servidores DHCP.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para ver una lista de clientes de la base de datos del servidor DHCP, en la interfaz de administración web, vaya a **Monitor** > **Servidor/Retransmisión DHCP**.



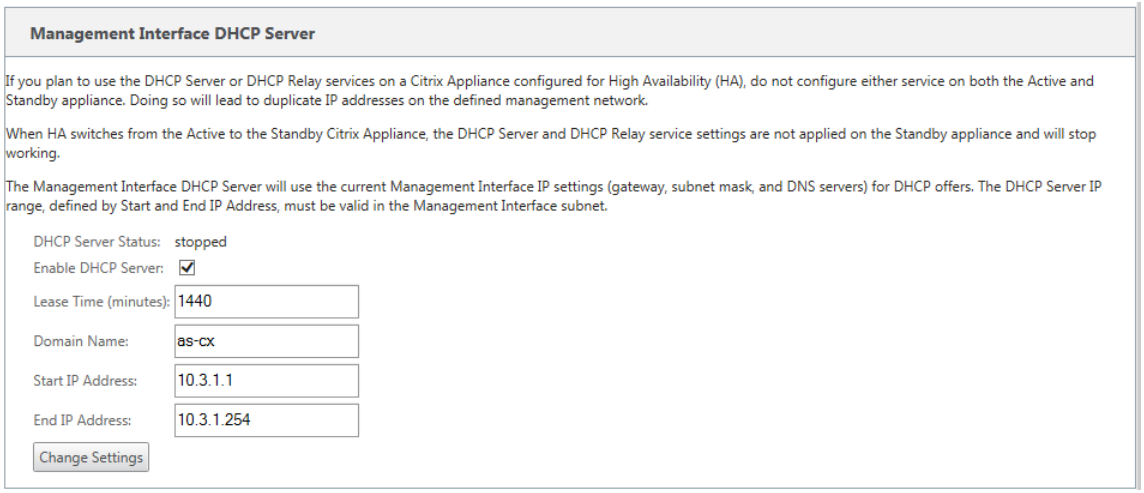
Configuración de un dispositivo SD-WAN como servidor DHCP o retransmisión DHCP mediante la configuración del dispositivo

Puede configurar manualmente un dispositivo SD-WAN individual como servidor DHCP o una reproducción DHCP desde la página de configuración del dispositivo.

Para habilitar el servidor DHCP en un dispositivo SD-WAN:

1. Vaya a **Configuración** > **Configuración del dispositivo** > **Adaptadores de red**. En la página **Adaptadores de red**, busque el panel **Servidor DHCP de la interfaz de administración**.
2. Haga clic en **Habilitar servidor DHCP** para iniciar el servidor, a continuación, introduzca el **tiempo de concesión** (en minutos), el **nombre de dominio** y defina el **rango de direcciones IP** introduciendo una **dirección IP de inicio** y una **dirección IP final**.

   > **Nota**
   >
   > El grupo de direcciones IP del servidor debe estar dentro de la red de administración.



3. Haga clic en **Cambiar configuración** para terminar de configurar el servidor DHCP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

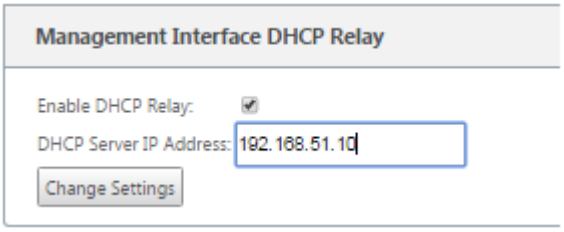
> **Nota**
>
> Si tiene previsto utilizar el servidor DHCP en un dispositivo SD-WAN configurado para alta disponibilidad (HA), no configure el servicio tanto en el dispositivo activo como en espera. Al hacerlo, se generan direcciones IP duplicadas en la red de administración definida.

4. Haga clic en **Mostrar cliente** para ver los clientes DHCP actuales y haga clic en **Borrar clientes** para liberar las concesiones de cliente DHCP

Para habilitar el servicio de retransmisión DHCP en un dispositivo SD-WAN:

1. Vaya a **Configuración** > **Configuración del dispositivo** > **Adaptadores de red**. En la página **Adaptadores de red**, busque el panel **Retransmisión DHCP de la interfaz de administración**.
2. Haga clic en la casilla de verificación **Habilitar retransmisión DHCP** para habilitar el servicio. Introduzca la **dirección IP del servidor DHCP** y haga clic en **Cambiar configuración** para comenzar a utilizar el dispositivo como agente de retransmisión DHCP.

> **Nota**
>
> Si planea utilizar el servicio de retransmisión DHCP en un dispositivo configurado para alta disponibilidad (HA), no configure el servicio tanto en los dispositivos activo como en espera. Al hacerlo, se generan direcciones IP duplicadas en la red de administración definida.



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

May 7, 2021

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 enlaces WAN en interfaces que no son de confianza.Esto elimina la necesidad de un enrutador WAN intermediario para realizar esta función.

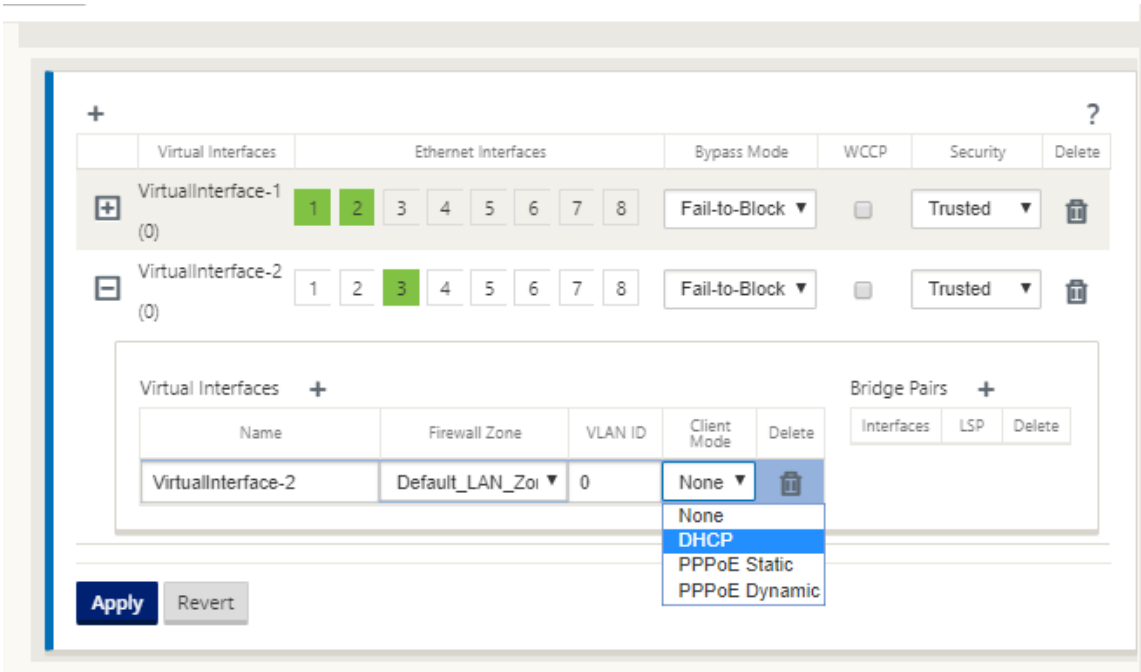
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> - El cliente DHCP solo se puede configurar para interfaces incomunicadas que no sean de confianza configuradas como nodos de cliente.
> - El cliente DHCP para puerto de datos solo se puede habilitar en sitios que no sean MCN y no RCN.
> - No se admite la implementación de enrutamiento basado en directivas (PBR) en el sitio con la configuración del cliente DHCP.
> - Los eventos DHCP se registran solo desde la perspectiva del cliente y no se generan registros de servidor DHCP.

Para configurar DHCP para una interfaz virtual que no es de confianza:

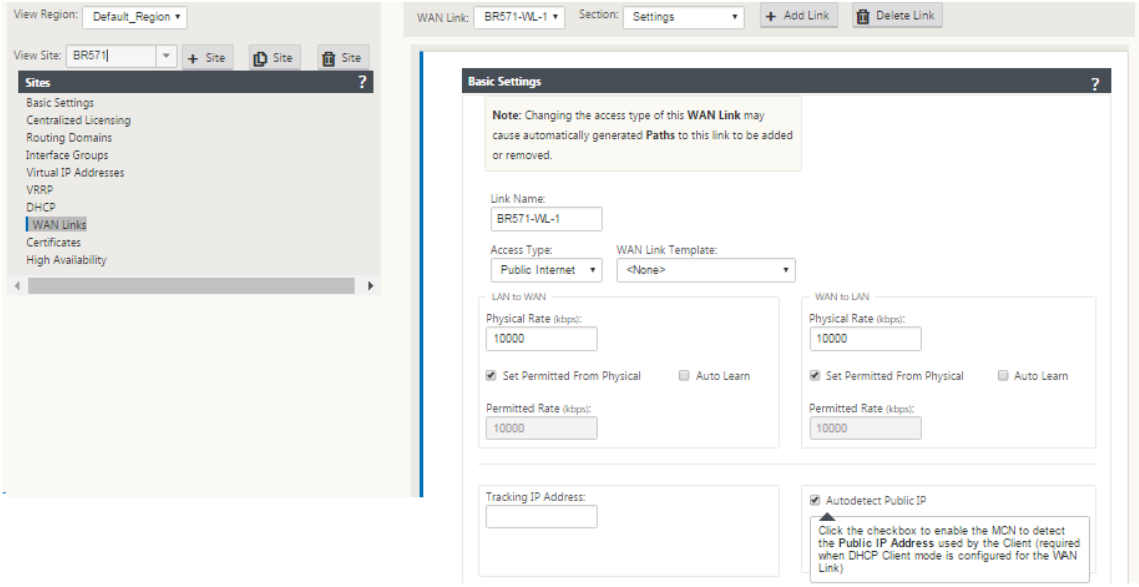
1. En el **Editor de configuración**, vaya a **Sitios**> [Nombre del sitio] > **Grupos de interfaz**> **Interfaces virtuales**.

   > **Nota**
   >
   > La interfaz física del grupo de interfaces debe ser un par incomunicado en una sola interfaz.



2. Seleccione DHCP como **modo cliente**.
3. Vaya a **Enlaces WAN[> Nombre del enlace WAN]**>**Configuración**>**Configuración básica**.
4. Haga clic en la casilla de verificación **Detectar automáticamente IP pública** para habilitar el MCN para detectar la dirección IP pública utilizada por el cliente. Esto es necesario cuando el modo Cliente DHCP está configurado para el enlace WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supervisión de enlaces WAN del cliente DHCP

La configuración de dirección IP virtual en 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 expiran las direcciones IP virtuales dinámicas, y cuando hay un problema de comunicación con la puerta de enlace o el servidor DHCP 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 renuevan hasta que todas las interfaces virtuales del sitio obtengan direcciones IP virtuales únicas.

Para supervisar los enlaces WAN del cliente DHCP:

1. En la página **Activar/Desactivar/Depurar Flujos** del dispositivo SD-WAN, la tabla Enlaces WAN del cliente DHCP proporciona el estado de las direcciones IP aprendidas.
2. 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.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Personalización dinámica de archivos PAC

May 7, 2021

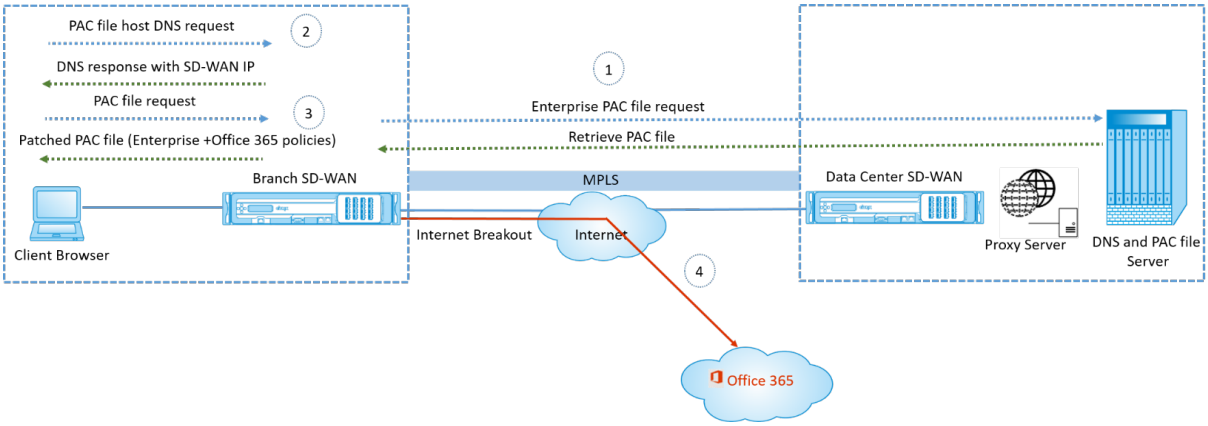
Con el aumento en la adopción empresarial de aplicaciones SaaS de misión crítica y de personal distribuido, resulta muy crítico reducir la latencia y la congestión. La latencia y la congestión son inherentes a los métodos tradicionales de backhaul del tráfico a través del centro de datos. Citrix SD-WAN 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 obtener proxy mediante la personalización del archivo PAC (Proxy Auto-Config) de empresa.

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 de host de red empresarial en el servidor web interno, estas configuraciones de proxy se distribuyen a través de la directiva de grupo. El explorador del cliente solicita archivos PAC desde el servidor web de empresa. El dispositivo Citrix SD-WAN sirve los archivos PAC personalizados para los sitios en los que está habilitada la instalación de Office 365.



1. Citrix SD-WAN solicita y recupera periódicamente la última copia del archivo PAC de empresa del servidor web de empresa. El dispositivo Citrix SD-WAN repara las direcciones URL de Office 365 al archivo PAC de empresa. Se espera que el archivo PAC de empresa tenga un marcador de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

posición (etiqueta específica de SD-WAN) donde las direcciones URL de Office 365 se parchean sin problemas.

2. El explorador cliente genera una solicitud DNS para el host de archivo PAC de empresa. Citrix SD-WAN intercepta la solicitud del FQDN del archivo de configuración de proxy y responde con Citrix SD-WAN VIP.
3. El explorador del cliente solicita el archivo PAC. El dispositivo Citrix SD-WAN sirve localmente el archivo PAC parcheado. El archivo PAC incluye la configuración de proxy de empresa y 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 conexión directa a 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 aplicar revisiones URL de Office 365.
3. La URL del archivo PAC debe estar basada en 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.

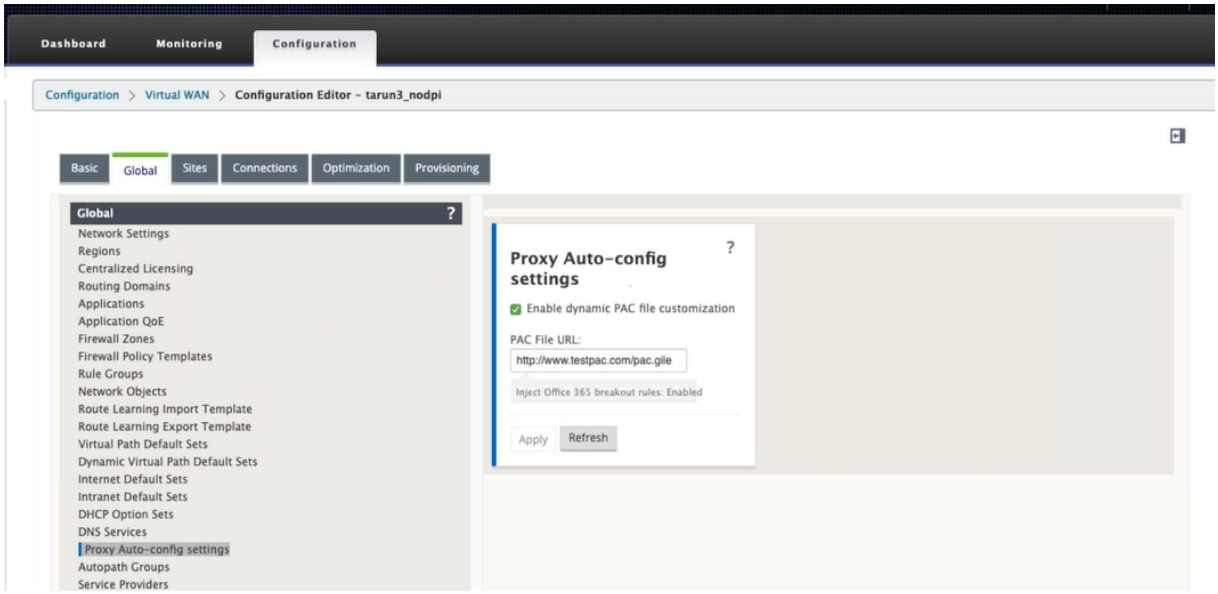
Configurar la personalización del archivo PAC

Puede habilitar la personalización de archivos PAC globalmente o a nivel de sitio.

> **Nota**
>
> La opción de grupo de Office 365 debe estar habilitada para la personalización dinámica de archivos PAC. Para obtener información sobre cómo habilitar el grupo de Office 365, consulte Optimización de Office 365.

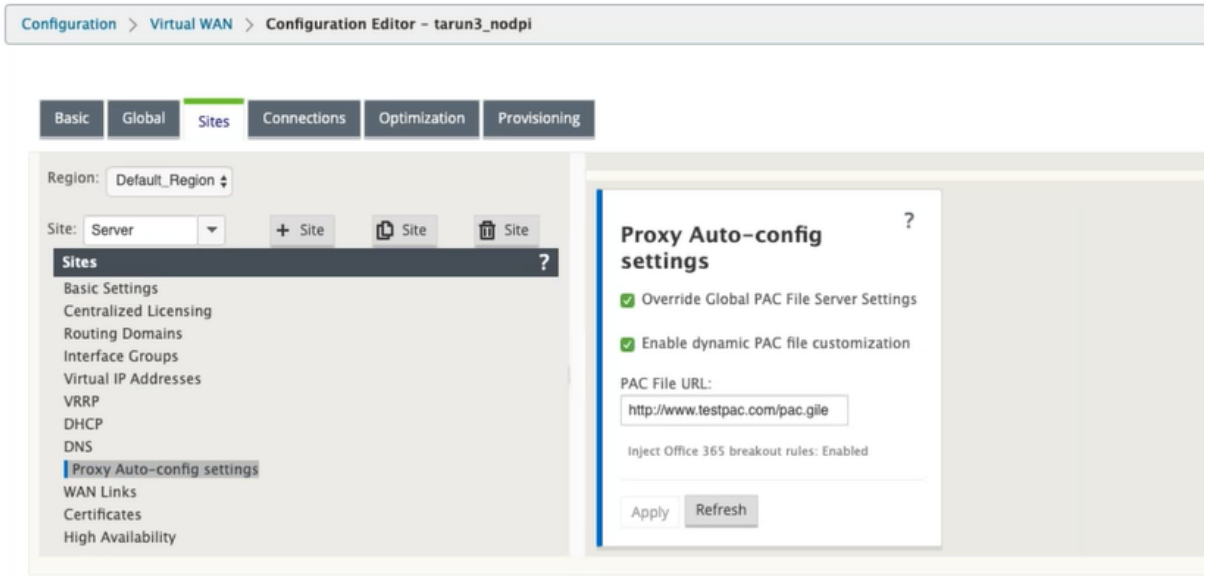
Para configurar globalmente la personalización dinámica de archivos PAC para todos los sitios, en el editor de configuración navegue hasta **Global** > **Proxy Auto-config settings**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Seleccione **Habilitar personalización de archivos PAC dinámicos**. En el campo **URL del archivo PAC**, introduzca la URL del servidor de archivos PAC de empresa. Las reglas de grupo de Office 365 se aplican de forma dinámica al archivo PAC de empresa.

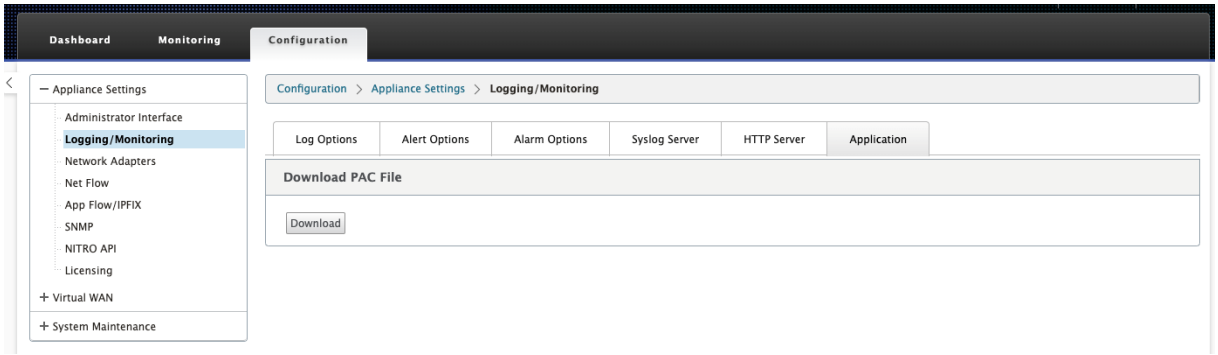
Para configurar la personalización dinámica de archivos PAC para un sitio, vaya a **Sitios** >[Sitio] > Configuración de **configuración automática del proxy**. También puede optar por anular la configuración global del servidor de archivos PAC y especificar una dirección URL del servidor de archivos PAC diferente.



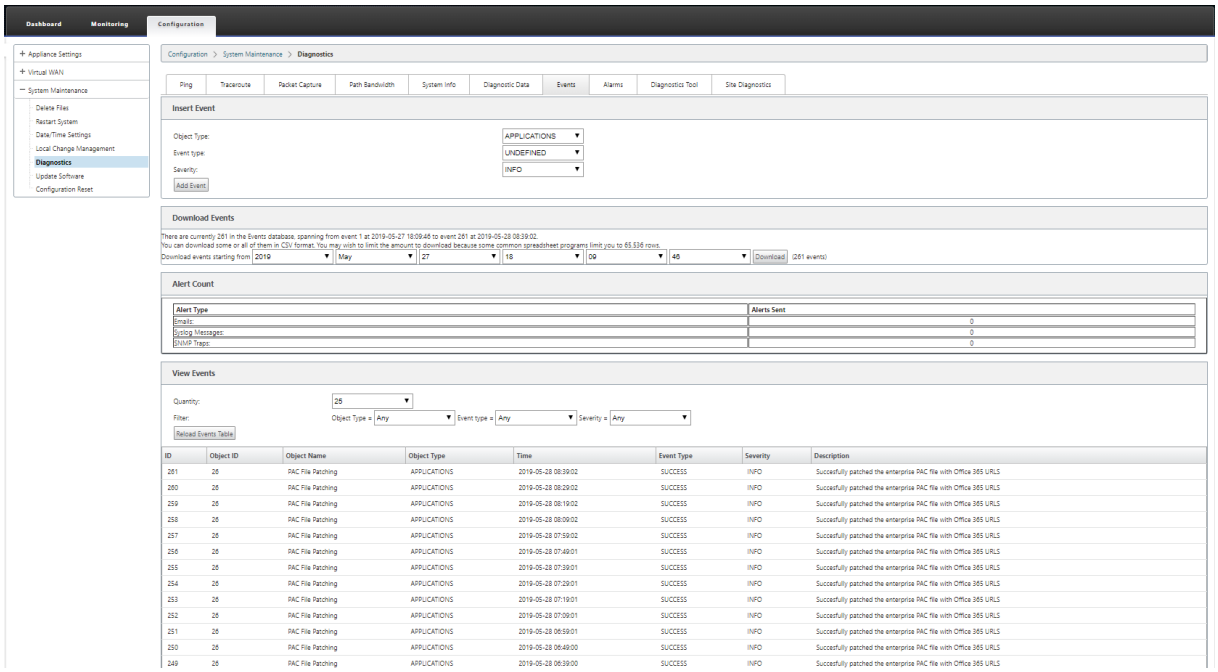
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solucionar problemas

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



También puede ver el estado de revisión del archivo PAC en la sección **Eventos**, vaya a **Configuración** > **Mantenimiento del sistema** > **Diagnósticos** 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 en una red, incluidos los archivos PAC para enrutar dominios o zonas de seguridad.
- No se admite la generación de archivos PAC en Citrix SD-WAN desde cero.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- WPAD a través de DHCP no es compatible.

Túnel GRE

May 7, 2021

La configuración del túnel GRE de SD-WAN le permite configurar los dispositivos SD-WAN para terminar los túneles GRE en la LAN. Si no desea configurar el sitio como nodo de terminación de túnel GRE, puede omitir este paso y pasar a la sección, Configuración de los enlaces WAN para el sitio de MCN.

Para configurar un túnel GRE:

Continuando en la vista **Sitios** del nuevo sitio MCN, haga clic en **+** a la izquierda de la etiqueta **GRE Tunnels**. Se abrirá la tabla **Túneles GRE** para el nuevo emplazamiento. Consulte los temas GRE para obtener más información.

Configuración de túneles GRE en el sitio de MCN.

Configuración de túneles GRE para el sitio de sucursal.

Configurar túneles GRE para el sitio de MCN (opcional)

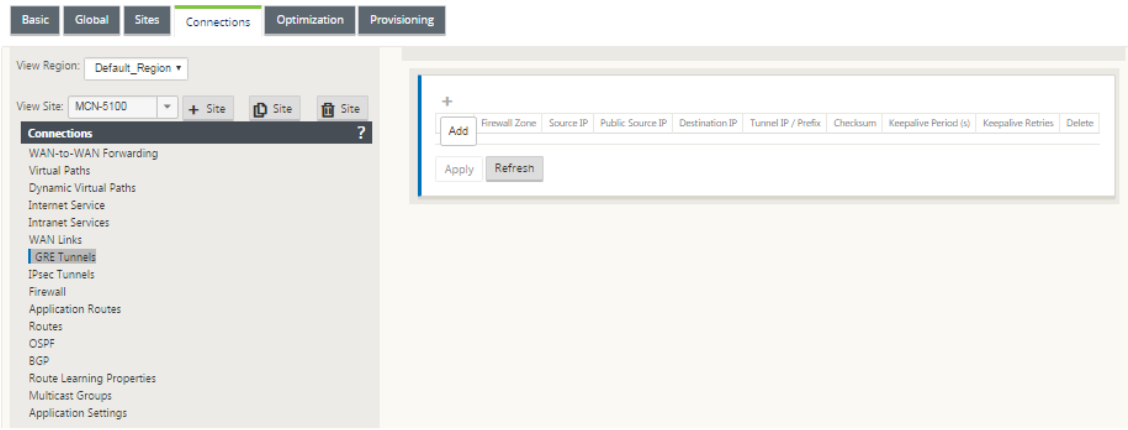
October 27, 2021

La configuración de Túneles GRE de SD-WAN permite configurar dispositivos SD-WAN para terminar túneles GRE en la LAN. Si no desea configurar este sitio como nodo de terminación del túnel GRE, puede omitir este paso y continuar con la sección Configuración de los vínculos WAN para el sitio MCN.

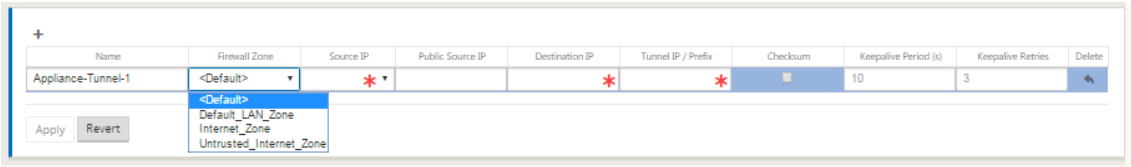
Para configurar un túnel GRE, haga lo siguiente:

1. Continuando en la ficha Conexiones del nuevo sitio MCN, haga clic en **Túneles GRE**. Esto abre la tabla **Túneles GRE** para el nuevo sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Haga clic en **+** a la derecha de los túneles **GRE**. Esto agrega una nueva entrada de túnel GRE en blanco a la tabla y la abre para su modificación.



3. Configure los ajustes del túnel GRE.

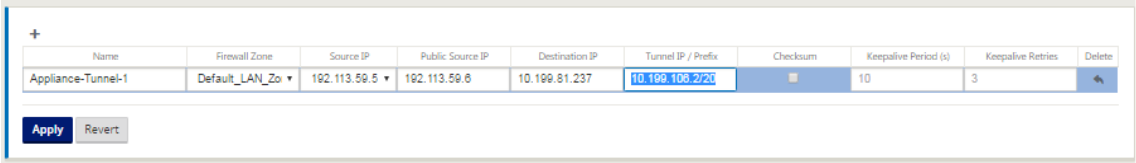
   Escriba lo siguiente:

   - **Nombre**: Introduzca un nombre para el nuevo túnel GRE o acepte el valor predeterminado. El valor predeterminado utiliza el siguiente formato de nomenclatura:
   - **Appliance-Tunnel-<number>**: Donde <*number*> es elnúmero de túneles GRE configurados para este sitio, incrementado en uno.
   - **Zona de firewall**: Seleccione la zona de archivos para el túnel GRE.
   - **IP de origen:** seleccione una dirección IP de origen para el túnel en el menú desplegable de este campo. Las opciones de menú son la lista de interfaces virtuales configuradas para este sitio. Configure al menos una interfaz virtual antes de poder configurar un túnel GRE. Para obtener instrucciones, consulte Configuración de los grupos de interfaz virtual para el sitio de MCN y Configuración de las direcciones IP virtuales para el sitio de MCN.
     - **IP de origen público**: introduzca la dirección IP que se utilizará como dirección de origen de los paquetes en el túnel GRE. La dirección IP de origen es el punto de partida del túnel GRE.
     - **IP de destino**: Introduzca la dirección IP que se utilizará como destino del host. La dirección IP de destino es el punto final del túnel GRE.
     - **IP/prefijo del túnel:** introduzca la dirección IP y el prefijo utilizados para la interfaz del túnel GRE.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Suma de comprobación:** seleccione esta opción para habilitar la suma de comprobación para el encabezado GRE del túnel.
- **Período de mantenimiento**: Introduzca el intervalo de tiempo de espera (en segundos) entre los mensajes keepalive. Si se configura en 0, no se envían paquetes keepalive, pero el túnel permanece activo. El valor predeterminado es 10.
- **Reintentos de Keepalive:** introduzca el número de reintentos de mantenimiento que debe intentar el dispositivo WAN virtual antes de que caiga por el túnel. El valor predeterminado es 3.

4. Haga clic en **Aplicar**. Esto envía la configuración y agrega el nuevo túnel GRE a la tabla.



5. Para configurar más túneles GRE, haga clic en **+** a la derecha de los **túneles GRE**y siga los pasos anteriores.

El siguiente paso consiste en configurar los vínculos WAN para el sitio de MCN.

Configurar túneles GRE para un sitio de sucursal

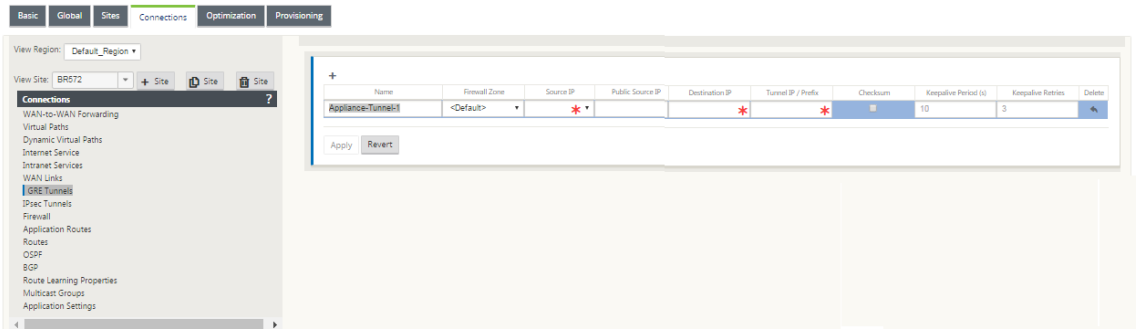
October 27, 2021

La configuración de los túneles GRE de LAN WAN virtual le permite configurar dispositivos WAN virtuales para terminar los túneles GRE en la LAN. Si no desea configurar este sitio de sucursal como nodo de terminación del túnel GRE LAN, puede omitir este paso y continuar con la sección Configuración de vínculos WAN para el sitio de sucursal.

Para configurar un túnel LAN GRE para el sitio de sucursal:

1. Continuando en la vista de conexiones del nuevo sitio de sucursal, haga clic en **Túneles GRE**. Se abrirá la vista **Túneles GRE** del nuevo sitio.
2. Haga clic en **+** a la derecha de los **túneles GRE**. Esto agrega una nueva entrada de túnel GRE en blanco a la tabla y la abre para su modificación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

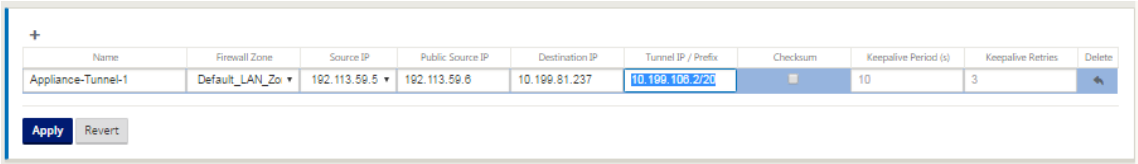


3. Configure los ajustes del túnel GRE. Escriba lo siguiente:

- **Nombre**: Introduzca un nombre para el nuevo túnel GRE o acepte el valor predeterminado. El valor predeterminado utiliza el siguiente formato de nomenclatura:
- **Appliance-Tunnel-<number>**: Donde *<number>* es el número de túneles GRE configurados para este sitio, incrementado en uno.
- **Zona de firewall**: Seleccione una zona de firewall para el túnel GRE.
- **IP de origen**: Seleccione una dirección IP de origen para el túnel en el menú desplegable de este campo. Las opciones de menú son la lista de direcciones IP virtuales que ha configurado para este sitio. Configure al menos una Interfaz Virtual y una Dirección IP Virtual antes de poder configurar un túnel LAN GRE. Para obtener instrucciones, consulte las secciones Configuración de los grupos de interfaz virtual para el sitio de sucursal y Configuración de las direcciones IP virtuales para el sitio de sucursal.
- **IP de origen público**: Introduzca la dirección IP que se utilizará como dirección de origen de los paquetes en el túnel GRE. La dirección IP de origen es el punto de partida del túnel GRE.
- **IP de destino**: Introduzca la dirección IP que se utilizará como destino del host. La dirección IP de destino es el punto final del túnel GRE.
- **IP/prefijo del túnel:** introduzca la dirección IP y el prefijo utilizados para la interfaz del túnel GRE.
- **Suma de comprobación:** seleccione esta opción para habilitar la suma de comprobación para el encabezado GRE del túnel.
- **Períodos Keepalive**: Introduzca el intervalo de tiempo de espera (en segundos) entre los mensajes keepalive. Si se configura en 0, no se envían paquetes keepalive, pero el túnel permanece activo. El valor predeterminado es 10.
- **Reintentos de Keepalive:** introduzca el número de reintentos de mantenimiento que debe intentar el dispositivo WAN virtual antes de que caiga por el túnel. El valor predeterminado es 3.

1. Haga clic en **Aplicar**. Esto envía la configuración y agrega la nueva entrada del túnel GRE a la tabla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Para configurar más túneles GRE, haga clic en **+** a la derecha de la etiqueta de los **túneles GRE** y continúe con los pasos anteriores.

El siguiente paso consiste en configurar los vínculos WAN para el sitio de la sucursal.

Administración de copias de seguridad y en banda

May 7, 2021

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, que transportan tanto datos como tráfico de administración, sin tener que configurar una ruta de administración adicional.

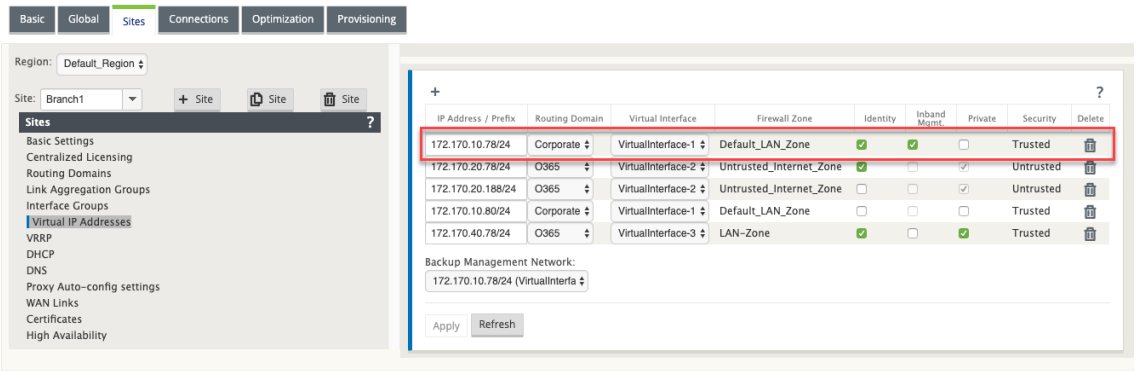
La administración en banda permite que las direcciones IP virtuales se conecten a servicios de administración como la interfaz de usuario web y SSH. Puede habilitar la administración en banda en varias interfaces de confianza habilitadas para ser utilizadas para servicios IP. Puede acceder a la interfaz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

Para habilitar la administración en banda en una IP virtual:

1. En el editor de configuración, vaya a **Sitios** > **Direcciones IP virtuales**.
2. Seleccione **Administración en banda para** las IP virtuales para las que quiere habilitar la administración en banda.

> **Nota:**
>
> La interfaz debe ser del tipo de seguridad **Confiable** e **Identidad** habilitada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



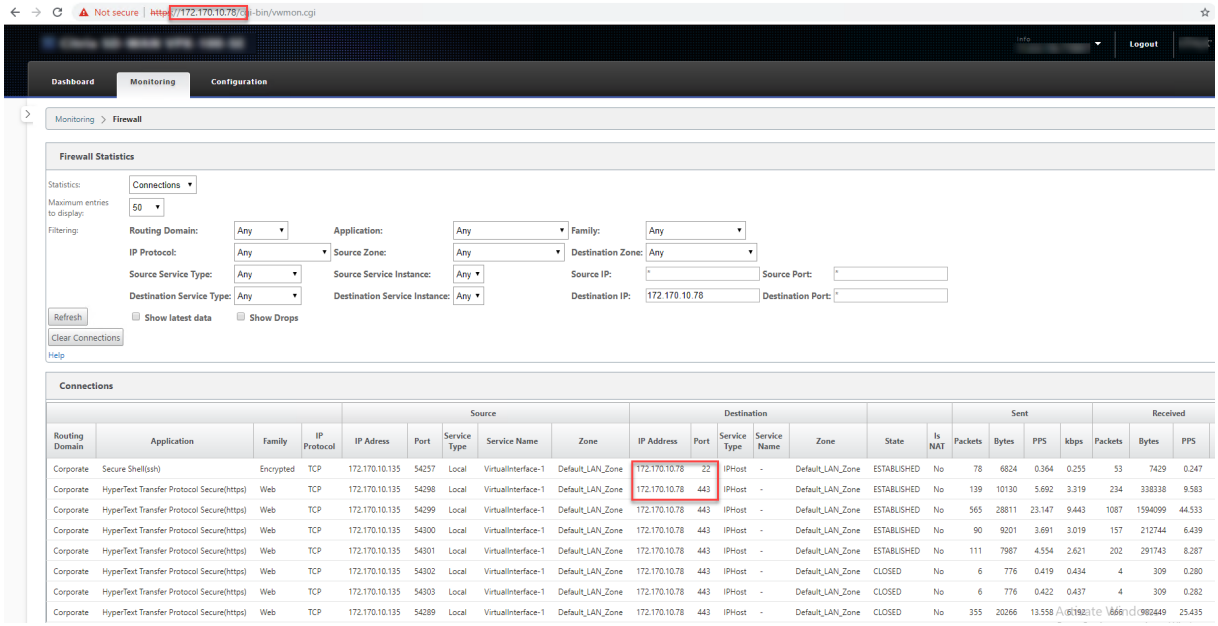
3. Haga clic en **Aplicar**

Para obtener información detallada sobre cómo configurar la dirección IP virtual, consulte Cómo configurar IP virtual.

Supervisión de la administración en banda

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



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

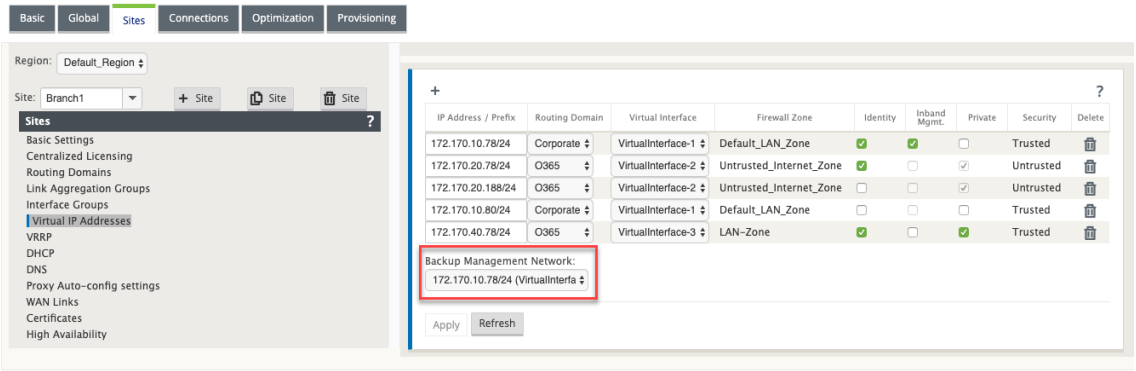
Respaldar la red de administración

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 de forma predeterminada una interfaz de confianza con identidad habilitada como red de administración de copias de seguridad.

Para seleccionar una IP virtual como una red de administración de copias de seguridad:

1. En el editor de configuración, vaya a **Sitios** > **Direcciones IP virtuales**.
2. Seleccione una dirección IP virtual como red de administración de copias de seguridad.



3. Haga clic en **Aplicar**.

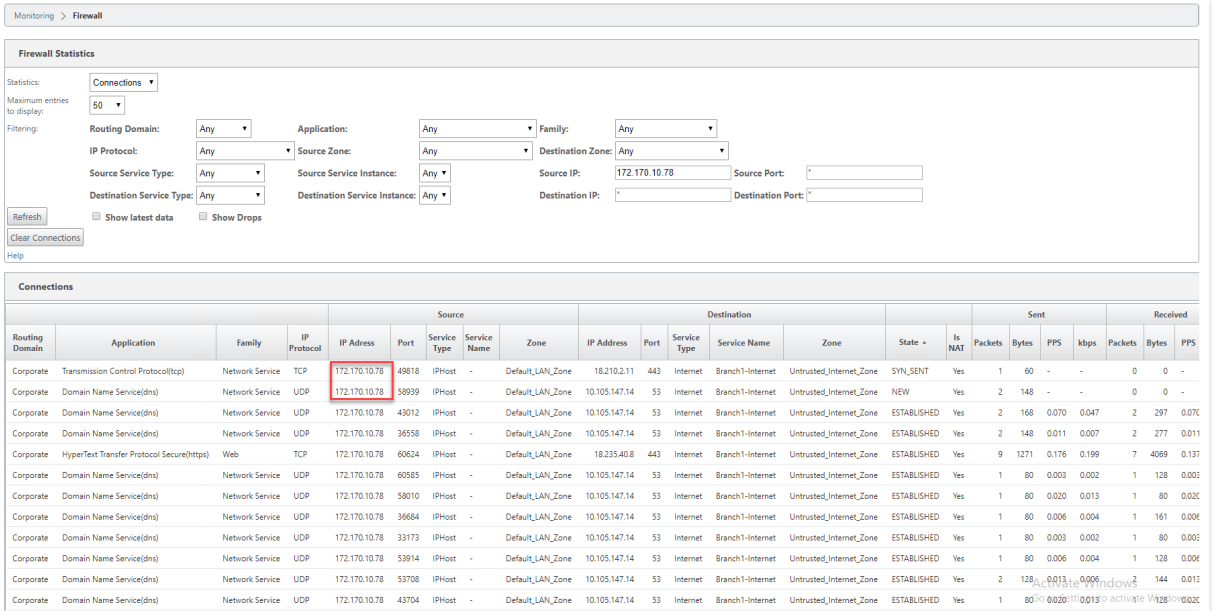
Para obtener un procedimiento detallado sobre la configuración de la dirección IP virtual, consulte la sección **Cómo configurar la dirección IP virtual** en elConfiguración tema.

Supervisión de la administración de copias de seguridad

En el ejemplo anterior, hemos seleccionado 172.170.10.78 IP virtual como la red de administración de copias de seguridad. Si la dirección IP de administración no está configurada con una Gateway predeterminada, puede utilizar esta IP para acceder a la interfaz de usuario web y 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Acceso a Internet

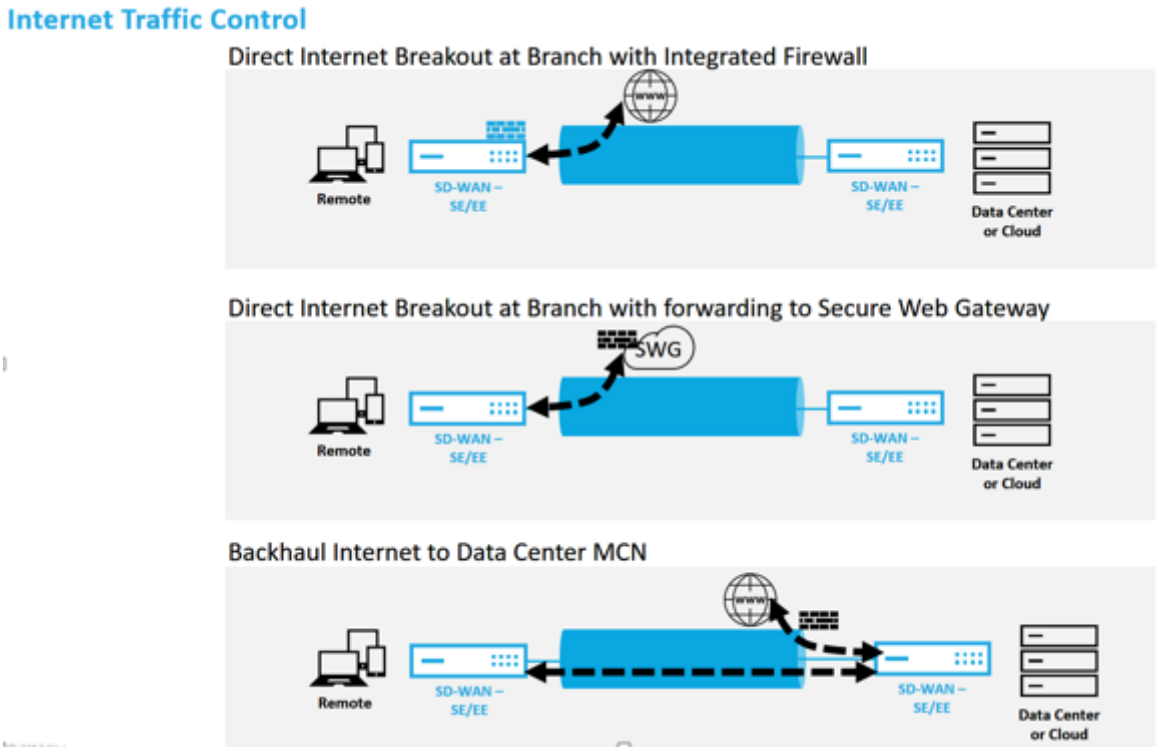
May 7, 2021

El Servicio de Internet se utiliza para el tráfico entre un sitio de usuario final y sitios de Internet público. El tráfico de servicios de Internet no está encapsulado por SD-WAN y no tiene las mismas capacidades que el tráfico que se entrega a través del servicio de rutas virtuales. Sin embargo, es importante clasificar y tener en cuenta este tráfico en la SD-WAN. El tráfico identificado como servicio de Internet permite la capacidad adicional de SD-WAN para administrar activamente el ancho de banda de 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 intranet según la configuración establecida por el administrador. Además de las capacidades de Provisioning de ancho de banda, SD-WAN tiene la capacidad agregada para equilibrar la carga del tráfico entregado a través del Servicio de Internet mediante varios enlaces WAN de Internet o, opcionalmente, utilizar los enlaces WAN de Internet en una configuración primaria o secundaria.

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

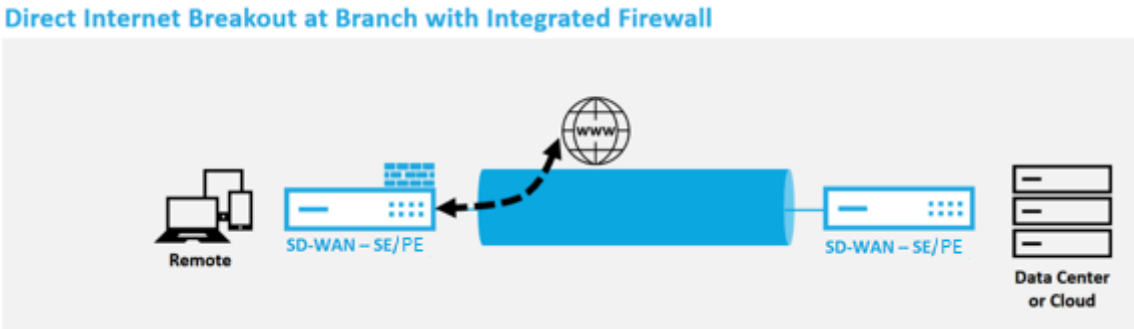
- Breakout directo de Internet en Branch con Firewall integrado
- Interrupción directa de Internet en el reenvío de sucursales a Secure Web Gateway
- Backhaul de Internet a MCN del centro de datos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Breakout directo de Internet en Branch con Firewall integrado

May 7, 2021

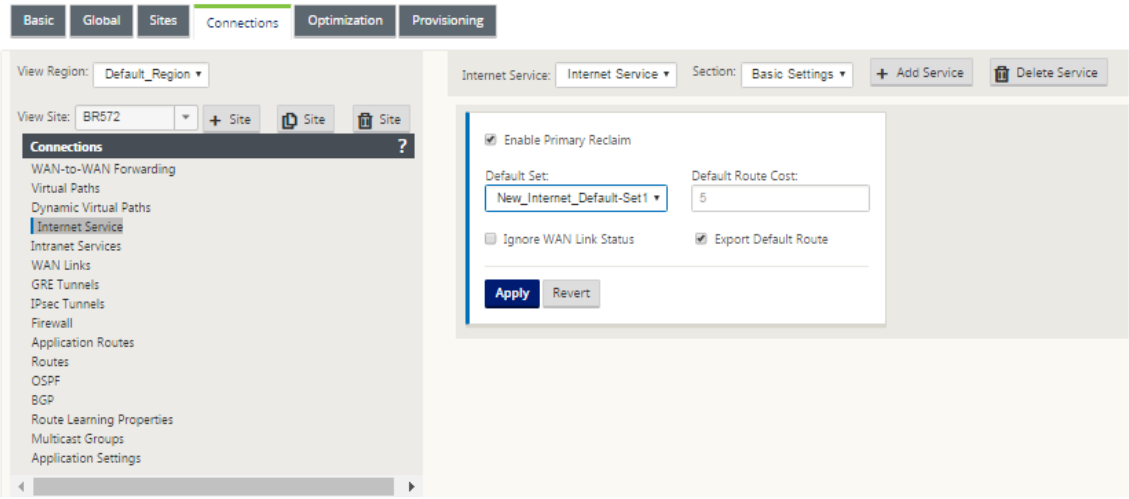


Realice los siguientes pasos para habilitar el servicio de Internet para cualquier sitio (nodo cliente o MCN):

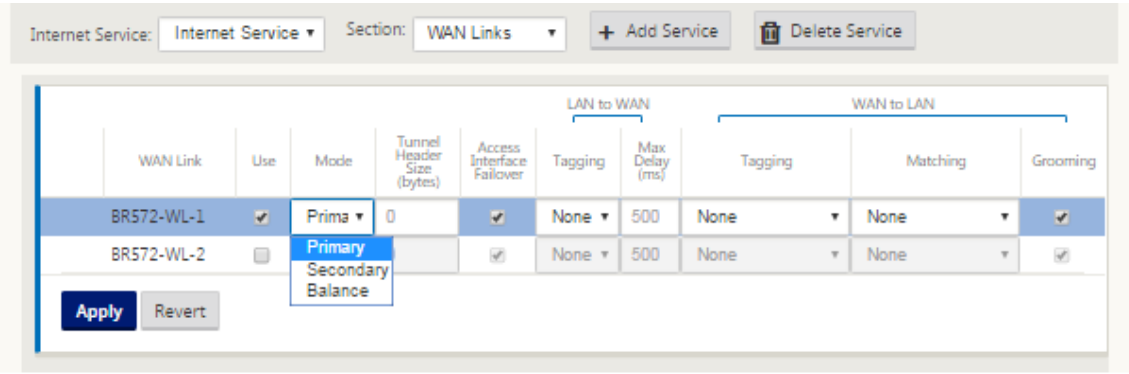
1. En el **Editor de configuración**, desplácese hasta el icono **Conexiones**. Haga clic en el icono de agregar (+) para agregar un servicio de Internet para ese sitio. Solo se puede crear un servicio de Internet por sitio.
2. En **Configuración básica** del servicio de Internet, hay varias opciones sobre cómo quiere que el servicio de Internet se comporte durante la falta de disponibilidad de enlaces WAN. Un conjunto

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

predeterminado de Internet se puede definir en el icono Global con un conjunto de reglas que se pueden aplicar a cualquier nodo de la configuración que tenga habilitado el servicio de Internet, lo que proporciona un control central para la administración del servicio de Internet sin tener que configurar cada nodo por separado.

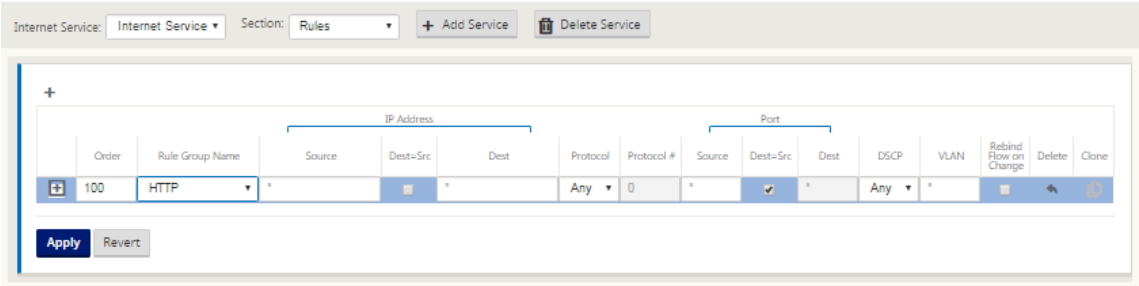


3. En el nodo Vínculos de WAN del servicio Internet, los enlaces WAN incorporados en el icono Sitio están disponibles para seleccionar el enlace WAN que quiere utilizar para el tráfico de Internet. Además de otras opciones, los Modos disponibles son Principal, Secundario y Equilibrado, lo que permite al administrador usar los enlaces WAN disponibles simultáneamente o en un rol activo/pasivo.

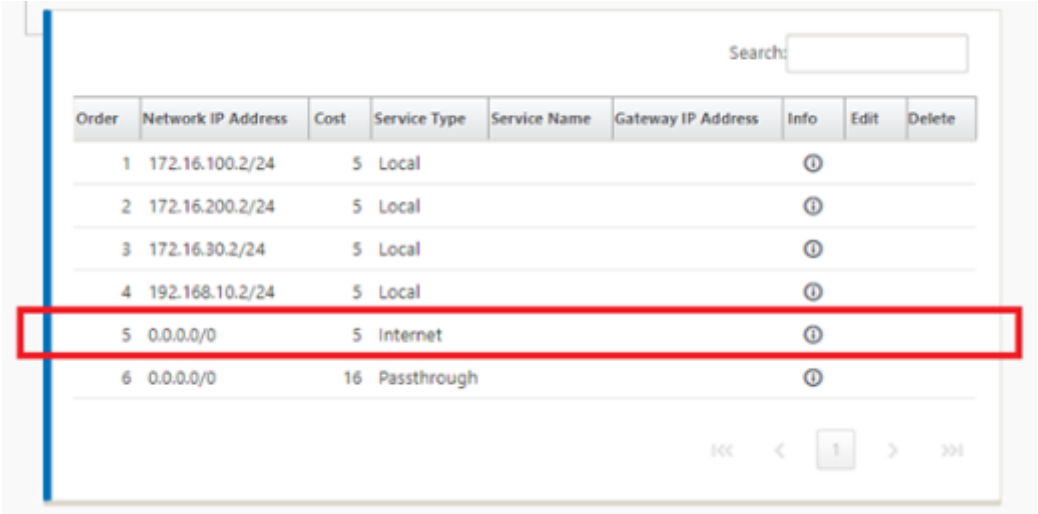


4. Están disponibles reglas específicas de nodo de sitio, lo que permite la capacidad de personalización de cada sitio, anulando de forma única cualquier configuración general configurada en el conjunto predeterminado global. Los modos incluyen la entrega quiereda a través de un enlace WAN específico, o como servicio de anulación que permite pasar o descartar el tráfico filtrado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

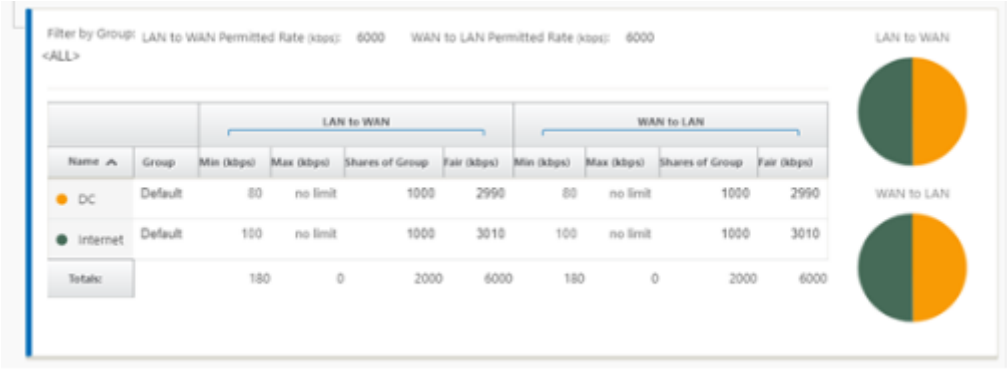


A medida que se crea un servicio de Internet para un nodo, la tabla de rutas para ese nodo en particular se actualiza automáticamente con una ruta 0.0.0.0/0 para el tipo de servicio igual a Internet y un coste de ruta de 5; de lo contrario, la ruta predeterminada con coste 16 con Passthrough como el tipo de servicio se promulgaría, y el tráfico de Internet ser entregado a la red de calco subyacente para enrutar.



Con el Servicio de Internet habilitado para un nodo de sitio, el icono Provisioning está disponible para permitir la distribución bidireccional (LAN a WAN/WAN a LAN) del ancho de banda para un enlace WAN entre los diversos servicios que utilizan el enlace WAN. La sección Servicios permite a los usuarios ajustar aún más la asignación de ancho de banda. Además, se puede habilitar la participación equitativa, permitiendo que todos los servicios reciban su ancho de banda mínimo reservado antes de que se promulgue una distribución justa.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



El Servicio de Internet se puede utilizar en los distintos modos de implementación compatibles con Citrix SD-WAN.

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

Citrix SD-WAN se puede implementar como una solución de superposición en cualquier red. Como solución de superposición, SD-WAN generalmente se implementa detrás de enrutadores perimetrales y/o firewalls existentes. Si 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 una Gateway de Internet.

- Modo de borde o puerta de enlace

Citrix SD-WAN se puede implementar como el dispositivo perimetral, reemplazando a los dispositivos de firewall y/o enrutador perimetral existentes. La función de firewall integrado permite a SD-WAN proteger 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.

Acceso directo a Internet con Secure Web Gateway

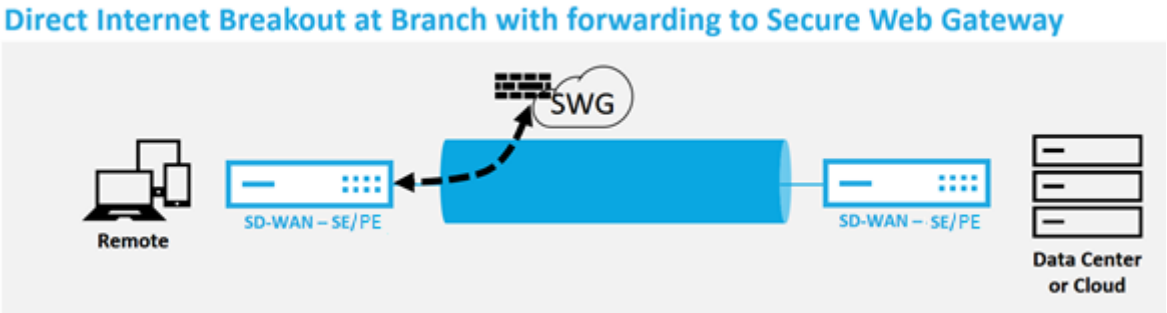
October 27, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



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

- Zscaler
- Punto de fuerza
- Palo Alto
- Citrix Secure Internet Access

Internet de red de retorno

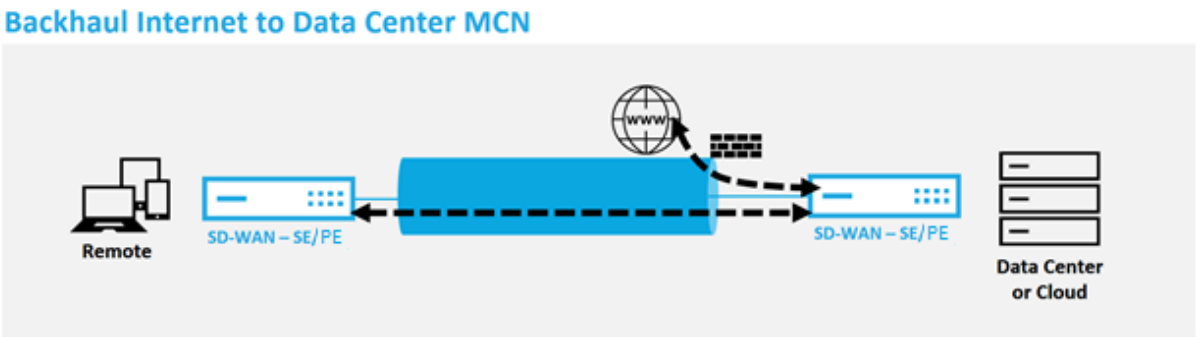
May 7, 2021

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

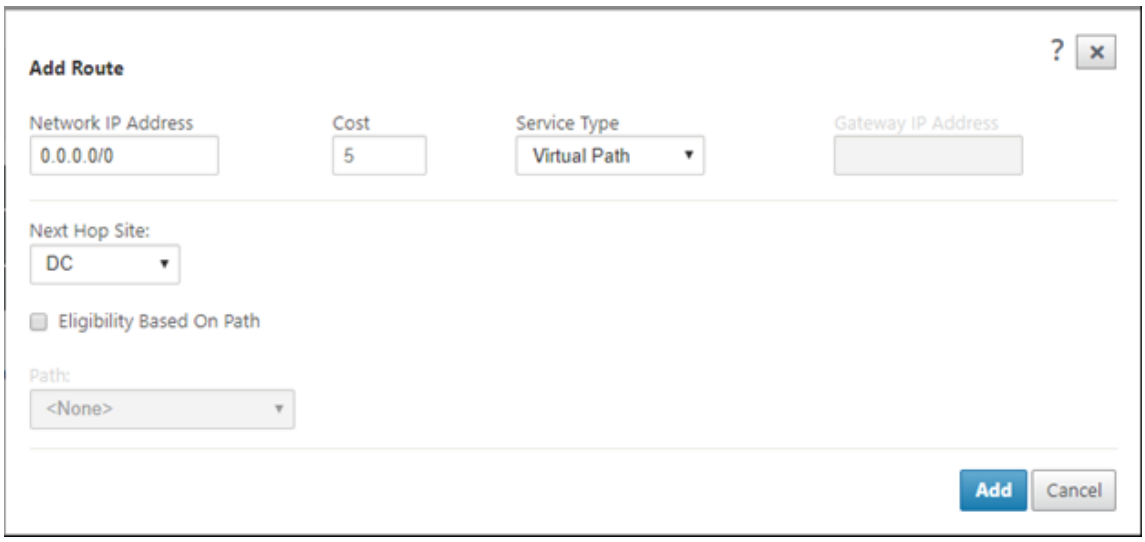
La solución Citrix SD-WAN admite el backhaul del tráfico de Internet con la siguiente configuración.

1. Habilite el Servicio de Internet en el nodo del sitio MCN o cualquier otra nota del sitio donde se quiera Servicio de Internet.

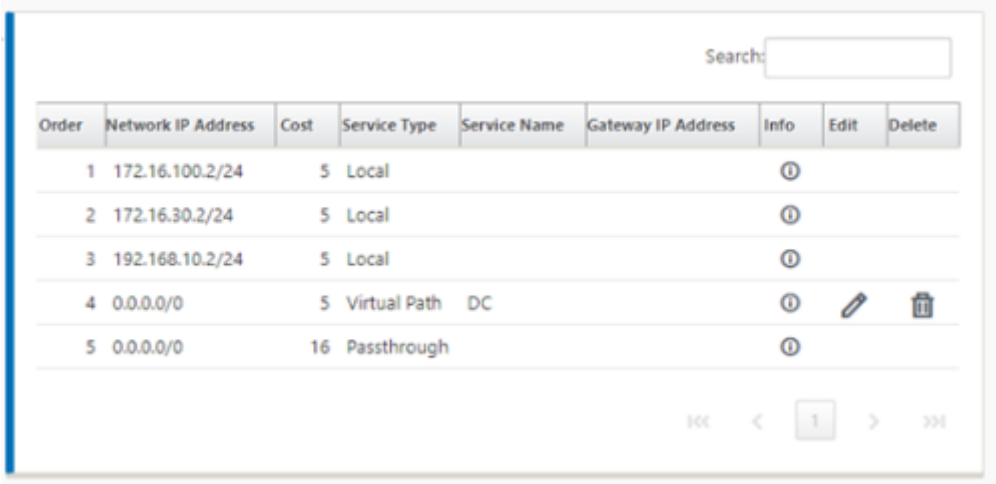
   > **Nota**
   >
   > Habilite el servicio de Internet y las rutas de exportación si todos los demás sitios se encuentran en el grupo de reenvío WAN a WAN.

2. En los nodos de sucursal donde se reactiva el tráfico de Internet, agregue manualmente una ruta 0.0.0.0/0 para dirigir todo el tráfico predeterminado al servicio de ruta virtual. El salto siguiente se denota como el MCN, o sitio intermediario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Compruebe que la tabla de rutas del sitio de sucursal no tiene ninguna otra ruta de menor coste que dirija el tráfico que no sea la ruta de backhaul quiereda.



Modo horquilla

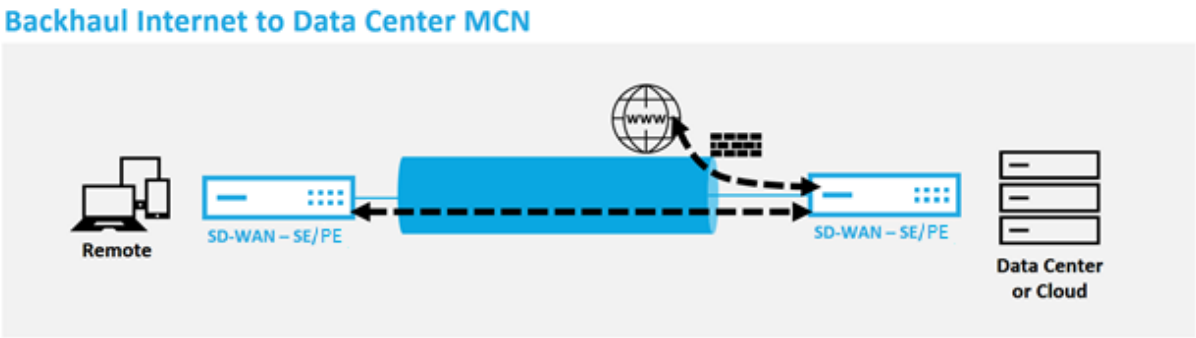
May 7, 2021

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 enrutamiento 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 lograr esto sin la complejidad de los costes de ruta estratégicamente ponderados 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 circula entre el Sitio A y el Sitio B a través del Sitio C, entonces 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 del otro, a diferencia del reenvío WAN a WAN.

Cuando el tráfico se realiza entre el Sitio A y el Sitio B a través del Sitio C, se requiere que las rutas estáticas se agreguen 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 la implementación de Hairpin tienen ciertas diferencias, a saber:

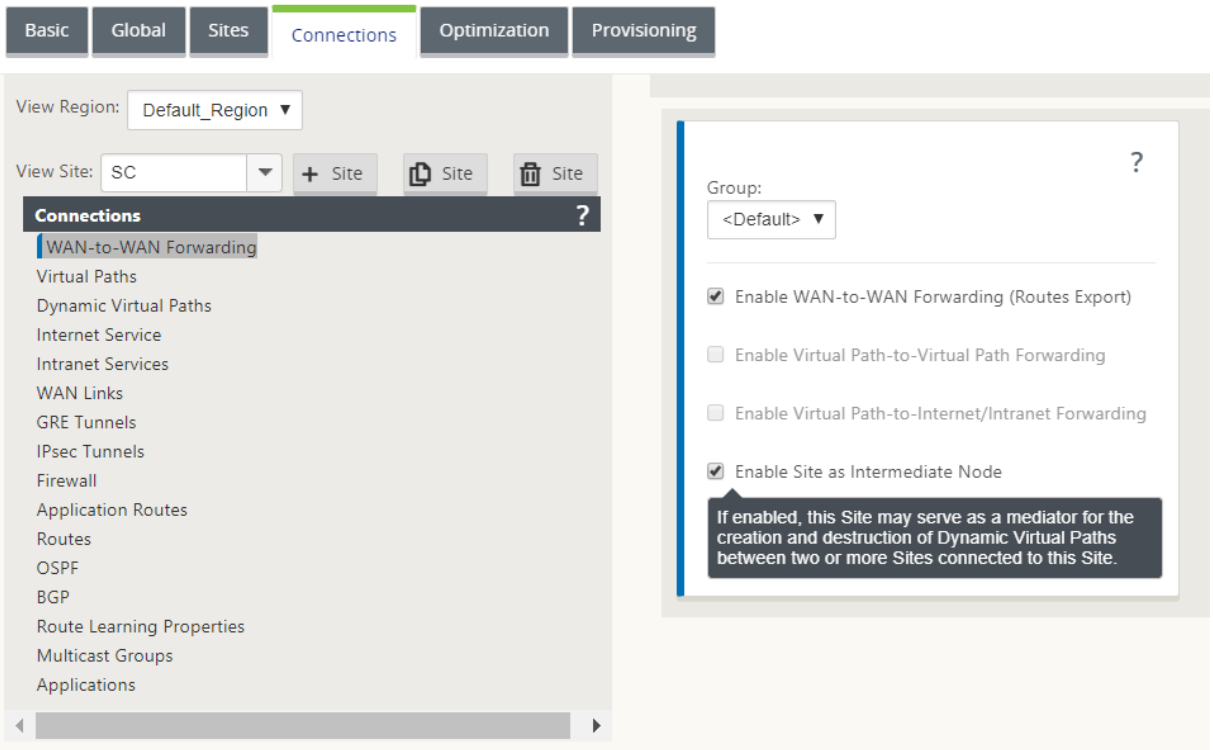
1. Las rutas virtuales dinámicas no están configuradas. Siempre, el sitio intermedio ve todo el tráfico entre los dos sitios.
2. No participa en grupos de reenvío de WAN a WAN.

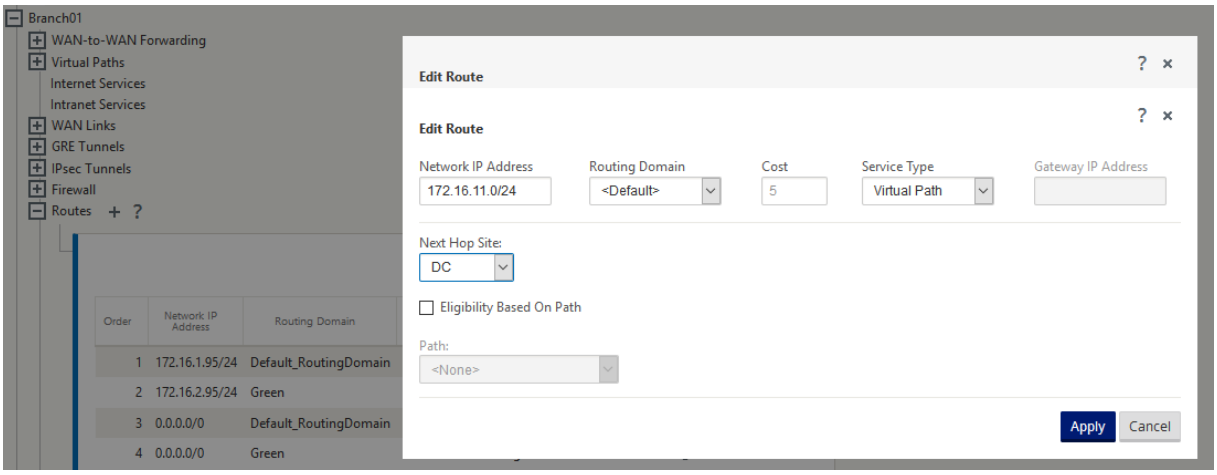
   El reenvío de WAN a WAN y la implementación de Hairpin son mutuamente excluyentes. Solo uno de ellos se puede configurar en cualquier momento dado.

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

Puede configurar la implementación de horquilla a través de la interfaz de administración web de Citrix SD-WAN desde el editor de configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





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

May 7, 2021

Citrix SD-WAN admite el hospedaje 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 del cortafuegos está integrada en 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.

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 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

Pasos de configuración

Se necesitan las siguientes configuraciones para integrar la máquina virtual Palo Alto Networks en SD-WAN:

- Aprovisionamiento de la máquina virtual de firewall
- Habilitar el redireccionamiento del tráfico a la máquina virtual

> **Nota La**
>
> máquina virtual del cortafuegos debe aprovisionarse primero antes de habilitar la redirección del tráfico.

Aprovisionamiento de máquina virtual de Palo Alto Network

Hay dos formas de aprovisionar la máquina virtual del firewall:

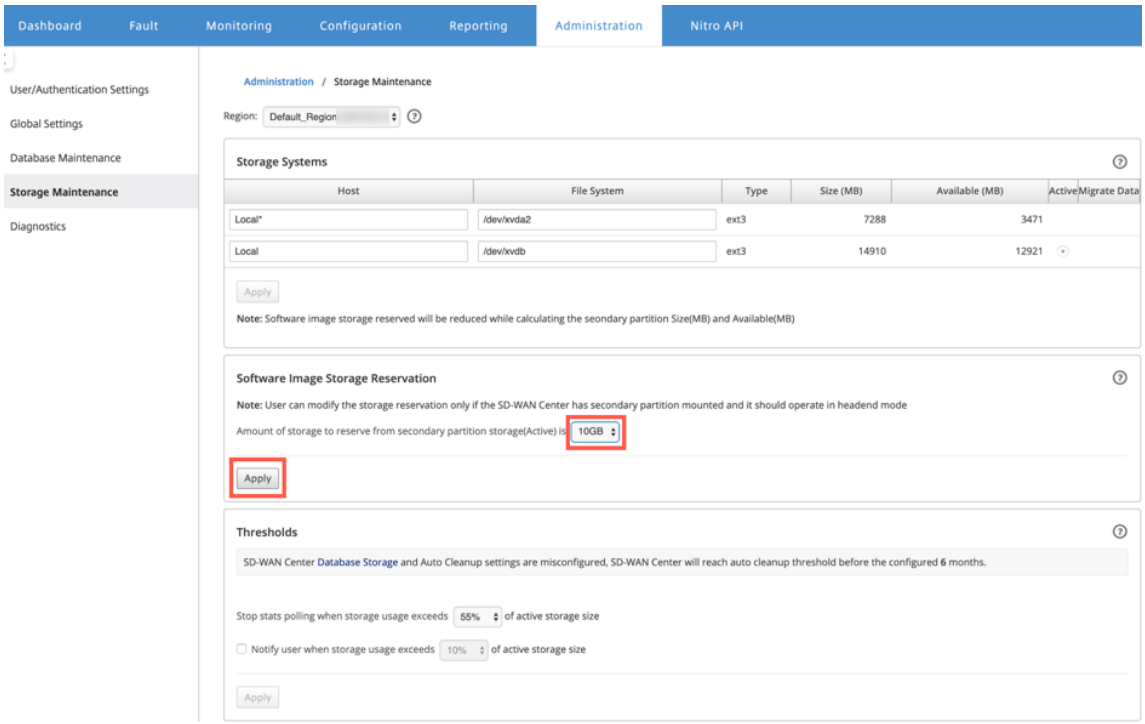
- Aprovisionamiento a través de SD-WAN Center
- Aprovisionamiento mediante GUI del dispositivo SD-WAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Provisioning de máquinas virtuales de firewall a través de SD-WAN Center

Requisitos previos

- Agregue el almacenamiento secundario a SD-WAN Center para almacenar los archivos de imagen de VM del firewall. Para obtener más información, consulte Requisitos e instalación del sistema.
- Reserve el almacenamiento de la partición secundaria para los archivos de imagen de la máquina virtual del firewall. Para configurar el límite de almacenamiento, vaya a **Administración > Mantenimiento del almacenamiento**.
  - Seleccione la cantidad de almacenamiento requerida de la lista.
  - Haga clic en **Aplicar**.

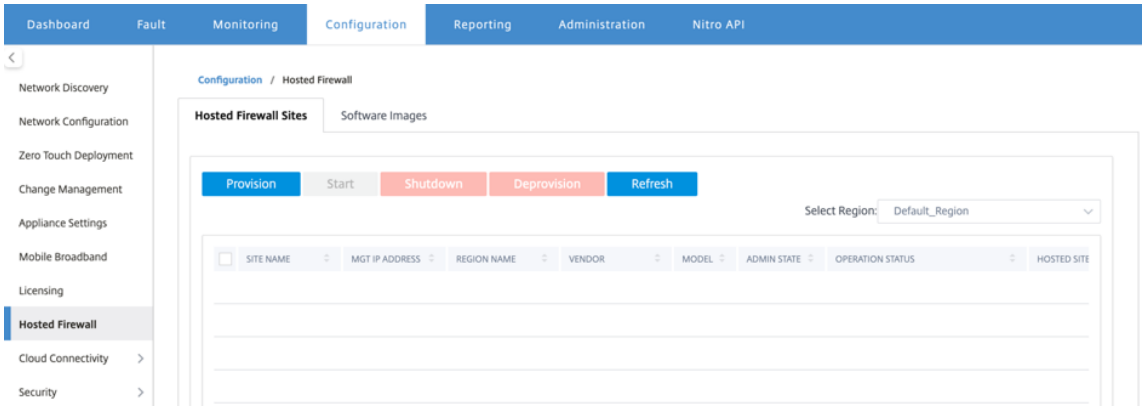


> **Nota**
>
> El almacenamiento se reserva de la partición secundaria que está activa si se cumple la condición.

Realice los siguientes pasos para Provisioning la máquina virtual de firewall a través de la plataforma SD-WAN Center:

1. En la GUI de Citrix SD-WAN Center, vaya a **Configuración >** seleccione **Firewall hospedado**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Puede seleccionar la **región** en la lista desplegable para ver los detalles del sitio aprovisionado para esa región seleccionada.

2. Cargue la imagen del software.

> **Nota**
>
> Asegúrese de que dispone de suficiente espacio en disco para cargar la imagen de software.

Vaya a **Configuración > Firewall hospedado > Imágenes de software** y seleccione el nombre del proveedor como Palo Alto Networks en la lista desplegable. Haga clic o suelte el archivo de imagen de software en el cuadro para cargarlo.

Aparecerá una barra de estado con el proceso de carga en curso. No haga clic en **Actualizar** ni realice ninguna otra acción hasta que el archivo de imagen muestre el 100% cargado.

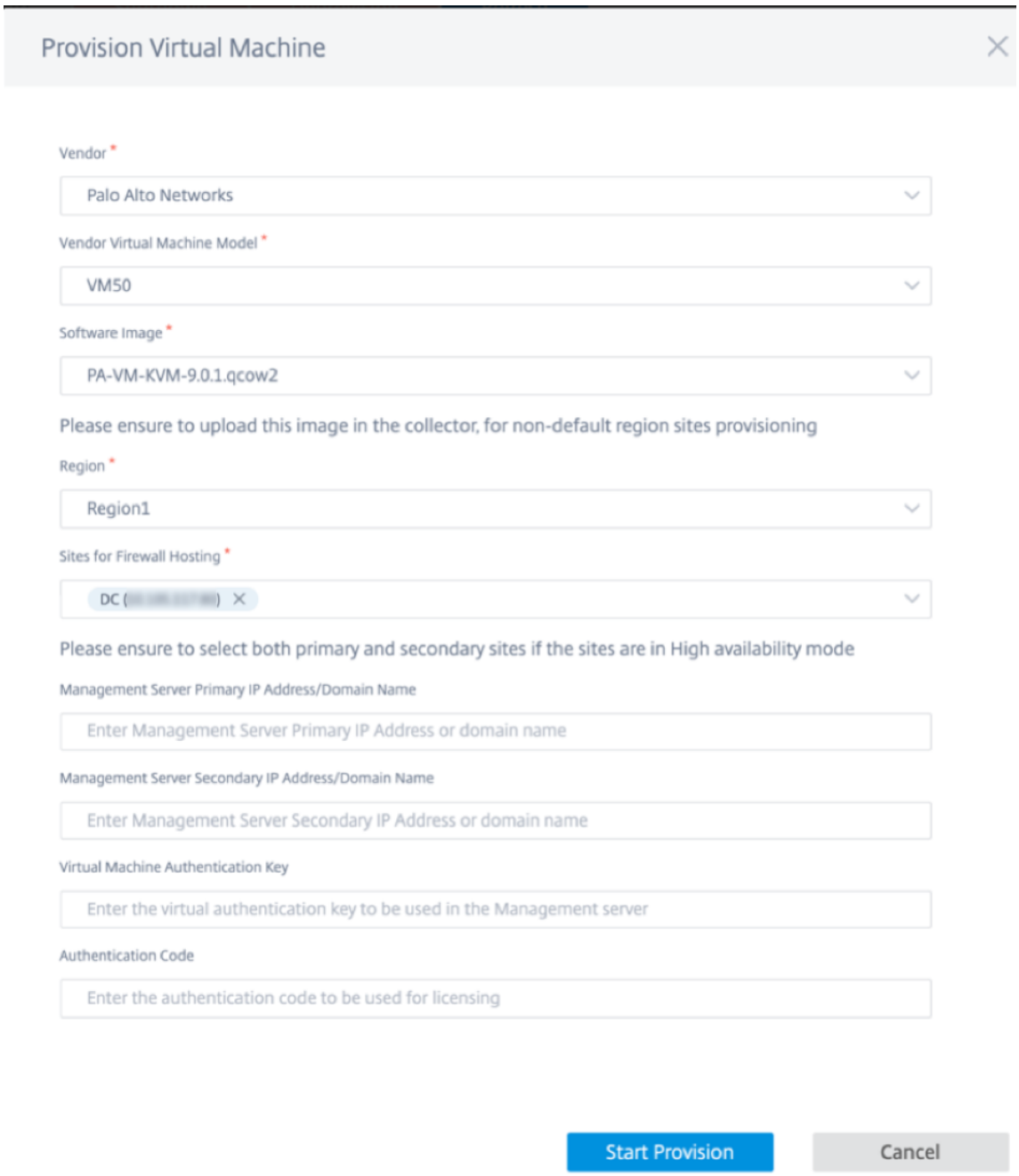
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Actualizar**: haga clic en la opción **Actualizar** para obtener los detalles más recientes del archivo de imagen.
- **Eliminar**: haga clic en la opción **Eliminar** para eliminar cualquier archivo de imagen existente.

> **Nota**
>
> - Para aprovisionar la máquina virtual del firewall en los sitios que forman parte de la región no predeterminada, cargue el archivo de imagen en cada uno de los nodos del recopilador.
> - Al eliminar la imagen de la máquina virtual Palo Alto del Centro SDWAN, se eliminará la imagen del almacenamiento de SDWAN Center y NO del dispositivo.

3. Para el aprovisionamiento, vuelva a la ficha **Sitios de firewall alojados** y haga clic en **Aprovisionar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Proveedor**: Seleccione el nombre del **proveedor** como **Palo Alto Networks** en la lista desplegable.
- **Modelo de máquina virtual de proveedor**: Seleccione el número de modelo de máquina virtual de la lista.
- **Imagen de software**: Seleccione el archivo de imagen que quiere aprovisionar.
- **Región**: Seleccione la región de la lista.
- **Sitios para alojamiento de firewall**: Seleccione sitios para la lista de alojamiento de fire-

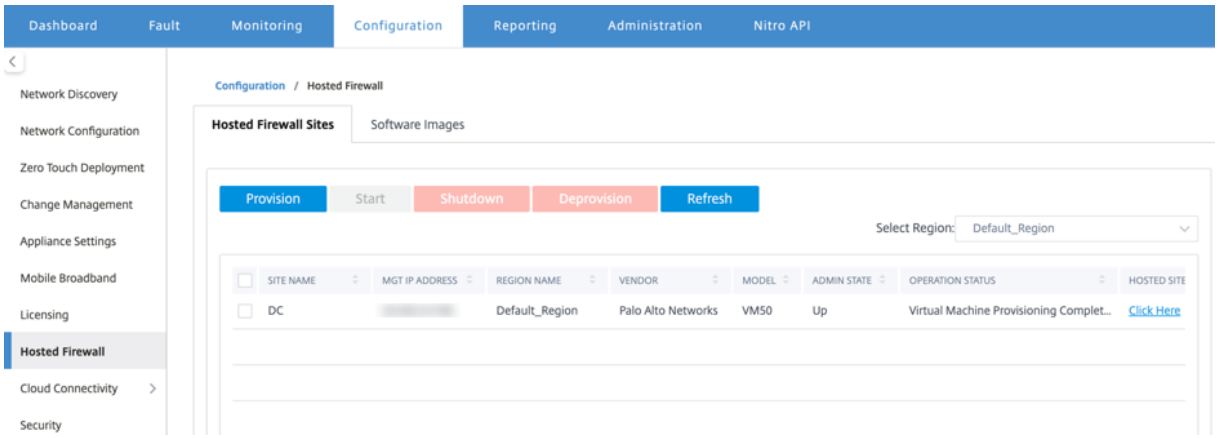
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

wall. Debe seleccionar sitios primarios y secundarios si los sitios están en modo de alta disponibilidad.

- **Dirección IP principal/nombre de dominio del servidor**de administración: Introduzca la dirección IP principal de administración o el nombre de dominio completo (opcional).
- **Dirección IP secundaria/nombre de dominio del servidor**de administración: Introduzca la dirección IP secundaria del servidor de administración o el nombre de dominio completo (opcional).
- **Clave de autenticación de máquina virtual**: Introduzca la clave de autenticación virtual que se utilizará en el servidor de administración.
- **Código de autenticación**: Introduzca el código de autenticación virtual que se utilizará para la concesión de licencias.

4. Haga clic en **Iniciar aprovisionamiento**.
5. Haga clic en **Actualizar** para obtener el estado más reciente. Después de que la máquina virtual Palo Alto Networks esté completamente arrancada, se reflejará en la interfaz de usuario dSD-WAN Center.

Puede **Iniciar, Apagar** y **Desaprovisionar** la máquina virtual según sea necesario.

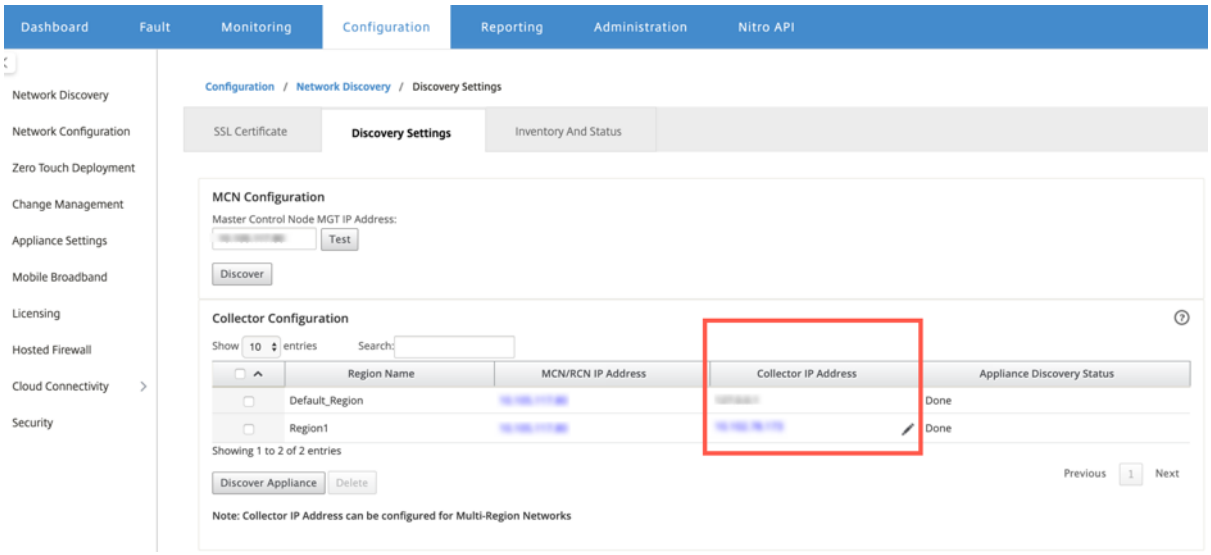


- **Nombre del Sitio**: Muestra el nombre del sitio.
- **Dirección IP de administración**: Muestra la dirección IP de administración del sitio.
- **Nombre de la región**: Muestra el nombre de la región.
- **Proveedor**: Muestra el nombre del proveedor (Palo Alto Networks).
- **Modelo**: Muestra el número de modelo (VM50/VM100).
- **Estado de administración**: Estado de la máquina virtual del proveedor (arriba/abajo).
- **Estado de Operación**: Muestra el mensaje de estado operativo.
- **Sitio alojado**: Utilice el enlace **Haga clic aquí** para acceder a la interfaz gráfica de usuario de la máquina virtual de Palo Alto Networks.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

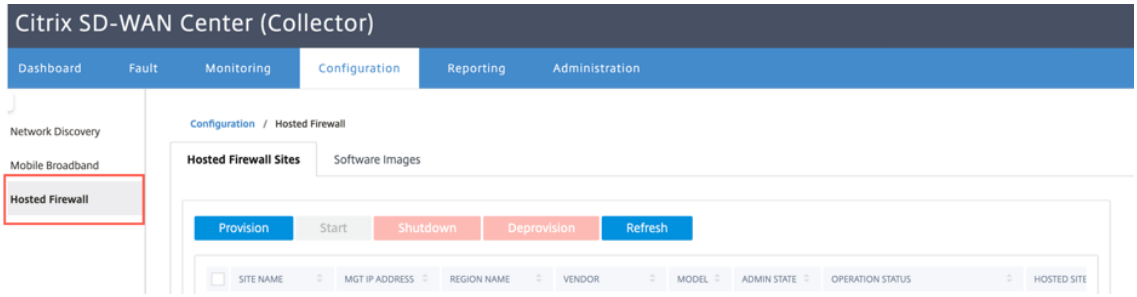
Para aprovisionar los sitios de región no predeterminados, debe cargar la imagen de software en SD-WAN Center Collector. Puede aprovisionar las redes Palo Alto tanto desde la GUI del extremo de la cabeza dSD-WAN Center o SD-WAN Center Collector.

Para obtener la dirección IP del colector de SD-WAN Center, vaya a **Configuración > Detección de red >** seleccione la ficha **Configuración de detección**.



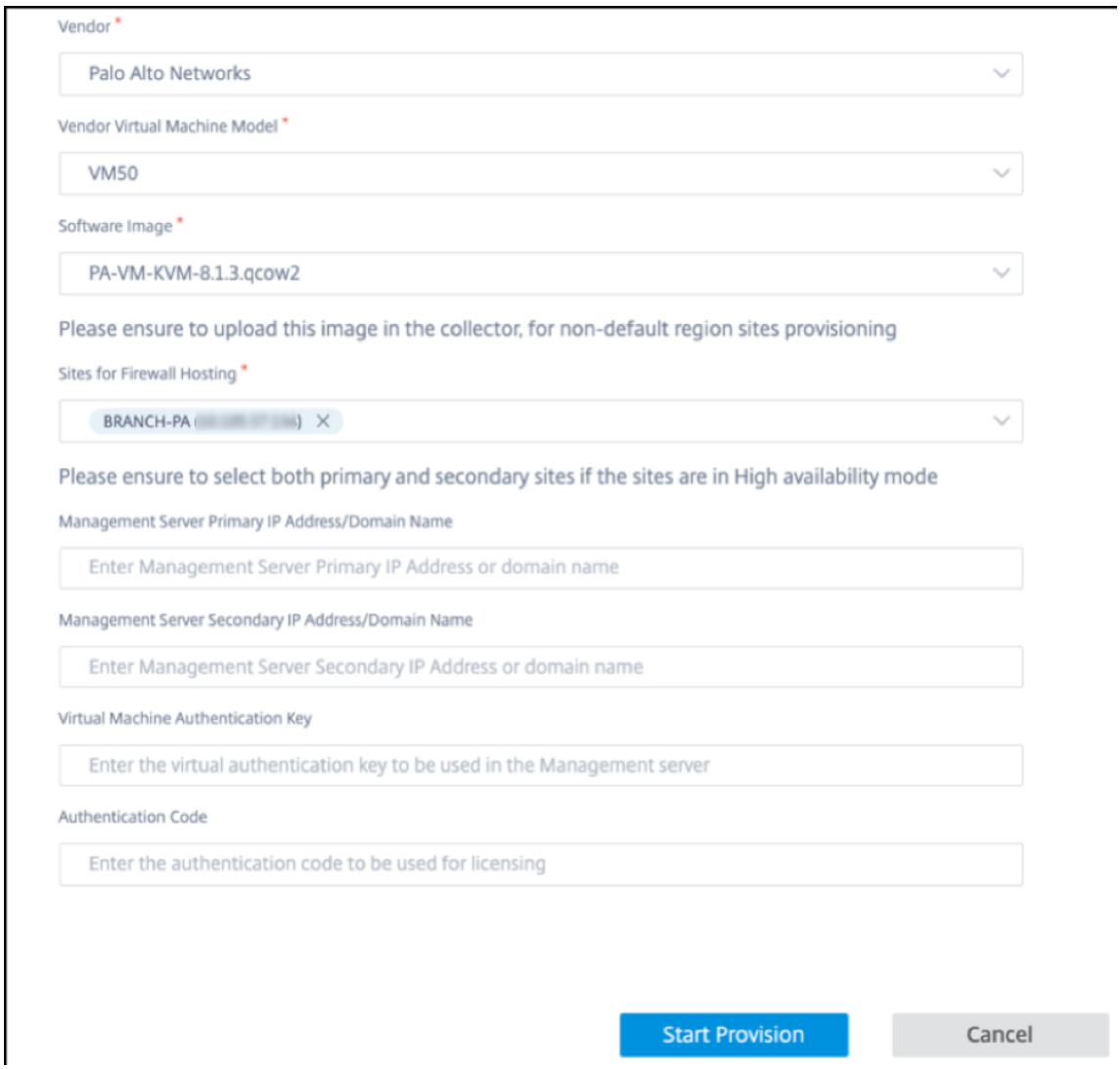
Para aprovisionar las redes Palo Alto desde SD-WAN Collector:

1. Desde SD-WAN Collector GUI, vaya a **Configuration >** seleccione **Hosted Firewall**.



2. Vaya a la pestaña **Imágenes de software** para cargar la imagen de software.
3. Haga clic en **Aprovisionar** en la ficha **Sitios de firewall alojados**
4. Proporcione los siguientes detalles y haga clic en **Iniciar aprovisionamiento**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Proveedor**: Seleccione el nombre del **proveedor** como **Palo Alto Networks** en la lista desplegable.
- **Modelo de máquina virtual de proveedor**: Seleccione el número de modelo de máquina virtual de la lista.
- **Imagen de software**: Seleccione el archivo de imagen que quiere aprovisionar.
- **Región**: Seleccione la región de la lista.
- **Sitios para alojamiento de firewall**: Seleccione sitios para la lista de alojamiento de firewall. Debe seleccionar sitios primarios y secundarios si los sitios están en modo de alta disponibilidad.
- **Dirección IP principal/nombre de dominio del servidor**de administración: Introduzca la dirección IP principal de administración o el nombre de dominio completo (opcional).
- **Dirección IP secundaria/nombre de dominio del servidor**de administración: Intro-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

duzca la dirección IP secundaria del servidor de administración o el nombre de dominio completo (opcional).

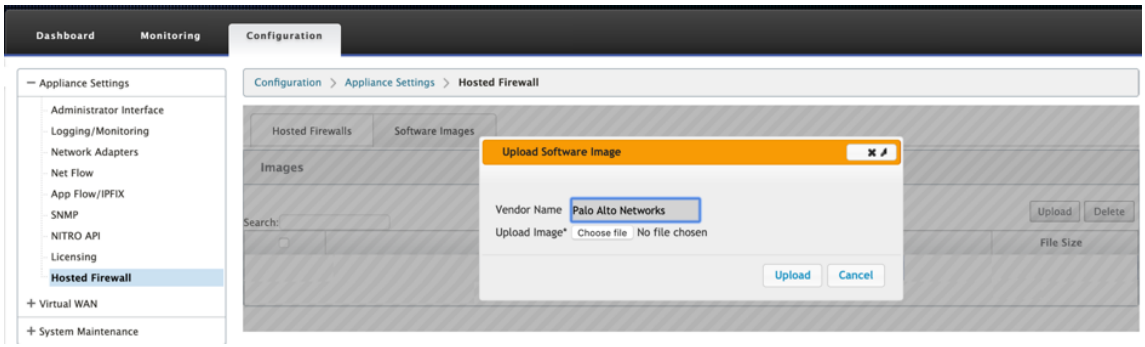
- **Clave de autenticación de máquina virtual**: Introduzca la clave de autenticación virtual que se utilizará en el servidor de administración.
- **Código de autenticación**: Introduzca el código de autenticación virtual que se utilizará para la concesión de licencias.

5. Haga clic en **Iniciar aprovisionamiento**.

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 equipo** > seleccione **Servidor de seguridad hospedado**.
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**.

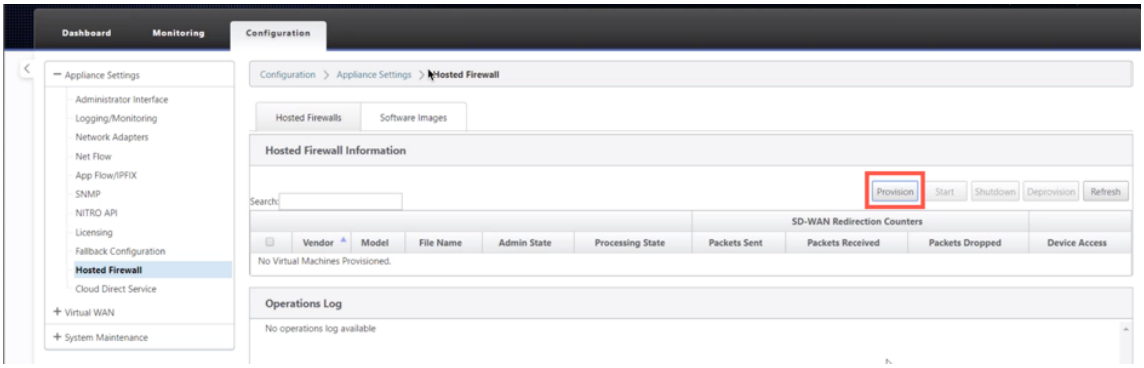


> **Nota Se**
> puede cargar un máximo de dos imágenes de software. La carga de la imagen de la máquina virtual Palo Alto Networks puede tardar más tiempo dependiendo de la disponibilidad del ancho de banda.

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 Provisioning no se puede eliminar. No realice ninguna acción ni vuelva a ninguna otra página hasta que el archivo de imagen muestre el 100% cargado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Para el aprovisionamiento, seleccione la ficha **Firewalls alojados** y haga clic en el botón **Aprovisionar**.

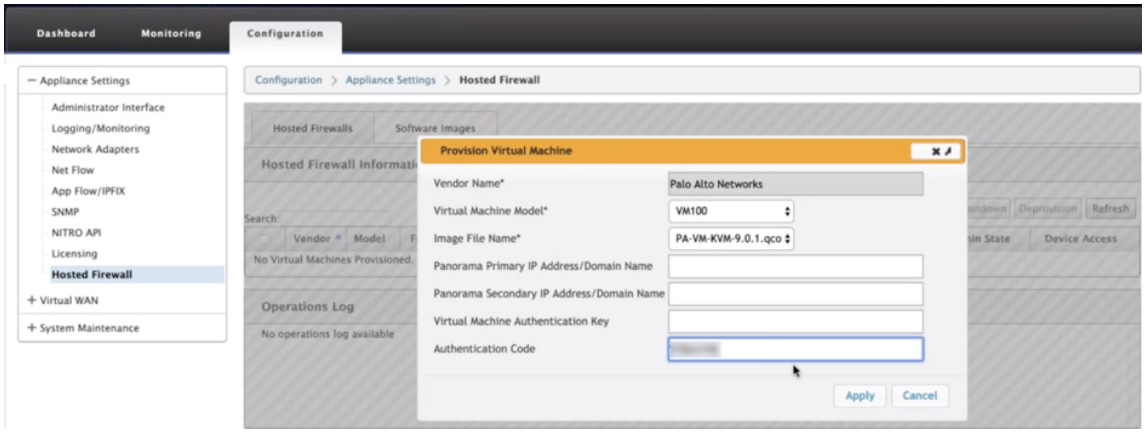


4. Proporcione los siguientes detalles para el Provisioning.

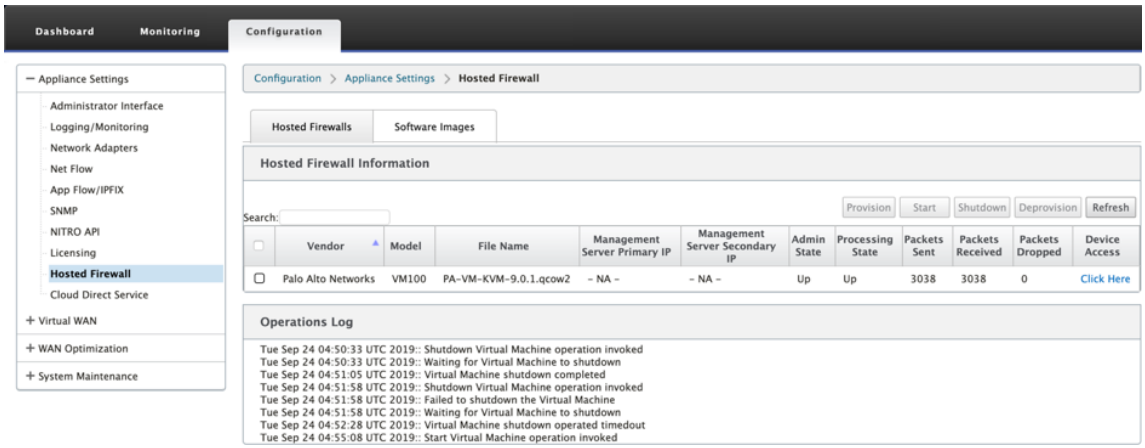
   - **Nombre del proveedor**: Seleccione el proveedor como **Palo Alto Networks**.
   - **Modelo de máquina virtual**: Seleccione el número de modelo de máquina virtual de la lista.
   - **Nombre del archivo de imagen**: Seleccione el archivo de imagen.
   - **Dirección IP principal/nombre de dominio panorámico**: Proporcione la dirección IP principal panorámica o el nombre de dominio completo (opcional).
   - **Dirección IP secundaria/nombre de dominio panorámico**: Proporcione la dirección IP secundaria panorámica 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Haga clic en **Actualizar** para obtener el estado más reciente. Después de que la máquina virtual Palo Alto Networks esté completamente arrancada, 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.
- **Paquete recibido**: Paquetes recibidos por SD-WAN desde la máquina virtual de seguridad.
- **Paquete eliminado**: Paquetes descartados por SD-WAN (por ejemplo, cuando la máquina virtual de seguridad está inactiva).
- **Acceso a dispositivos**: 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 **Click Here** para acceder a la GUI de la máquina virtual Palo Alto Networks o utilice su IP de administración junto con el puerto 4100 (dirección IP: 4100).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

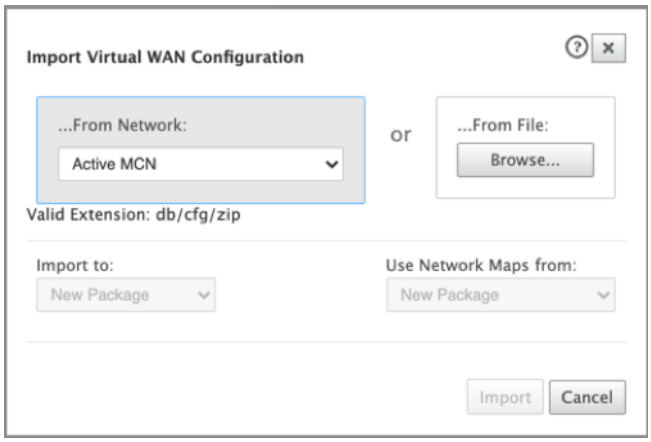
> **Nota**
> Utilice siempre el modo incógnito para acceder a la GUI de Palo Alto Networks.

Redirección de tráfico

La configuración de la redirección de tráfico se puede realizar tanto a través del Editor de configuración en MCN como del Editor de configuración en SD-WAN Center.

Para navegar a través del Editor de configuración en SD-WAN Center:

1. Abra la interfaz de usuario de Citrix SD-WAN Center, vaya a **Configuración > Importación de configuración de red**. Importe la configuración de WAN virtual desde el MCN activo y haga clic en **Importar**.

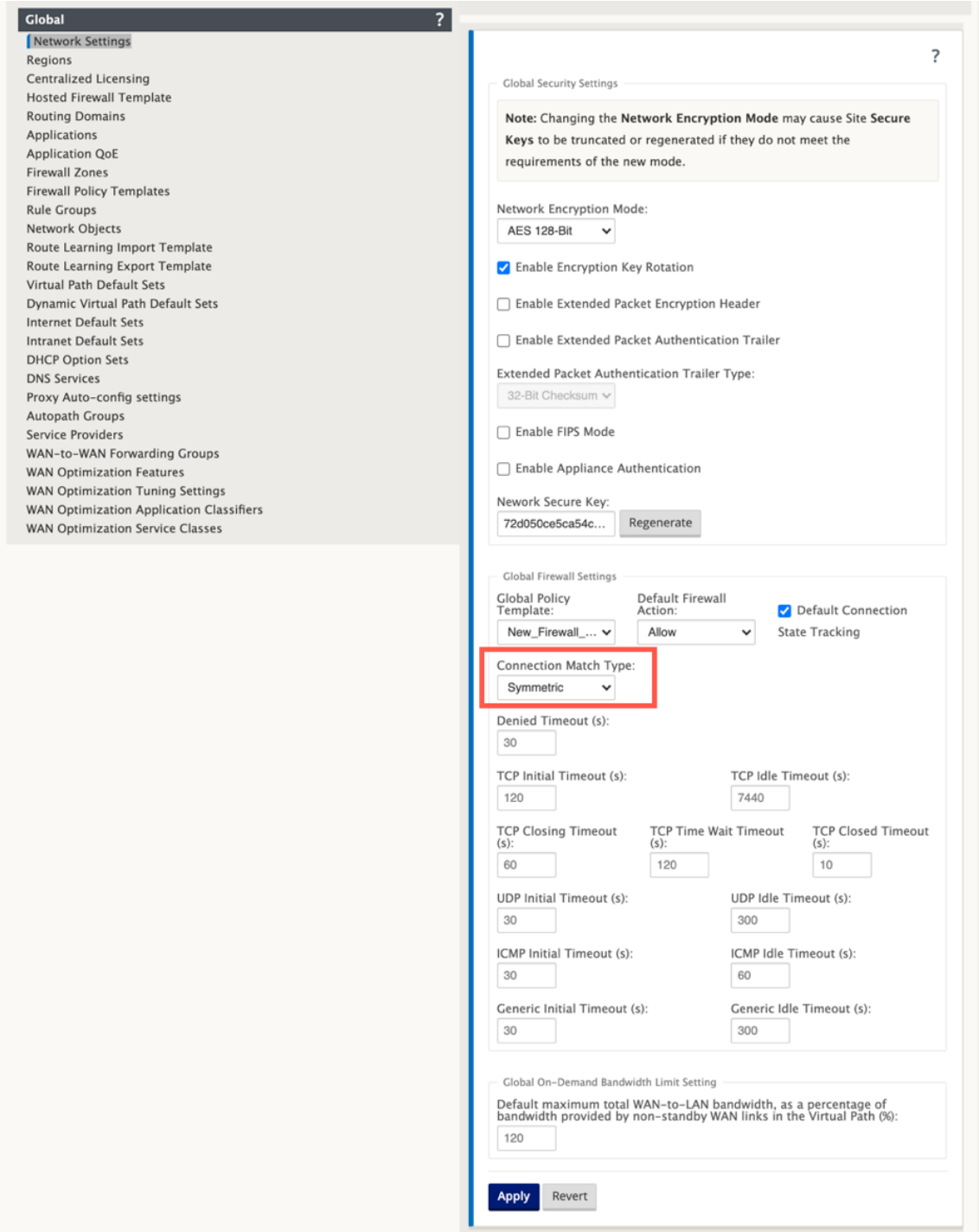


Los pasos restantes son similares a los siguientes: la configuración de redirección de tráfico a través de MCN.

Para navegar por el Editor de configuración en MCN:

1. Establezca **Tipo de coincidencia de conexión** en **Simétrico** en **Global > Configuración de red**.

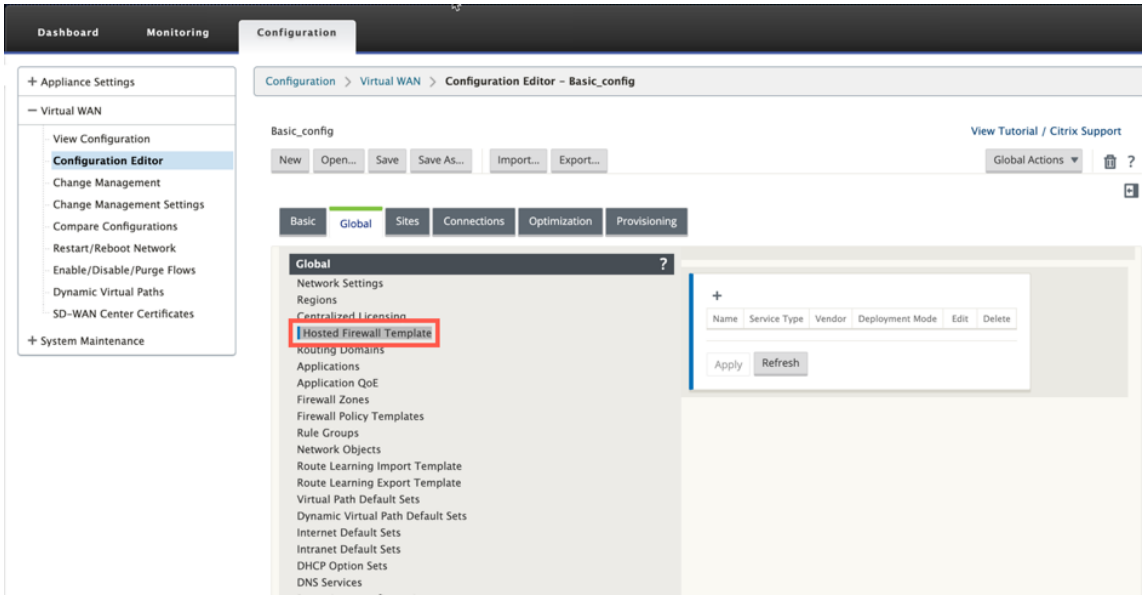
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



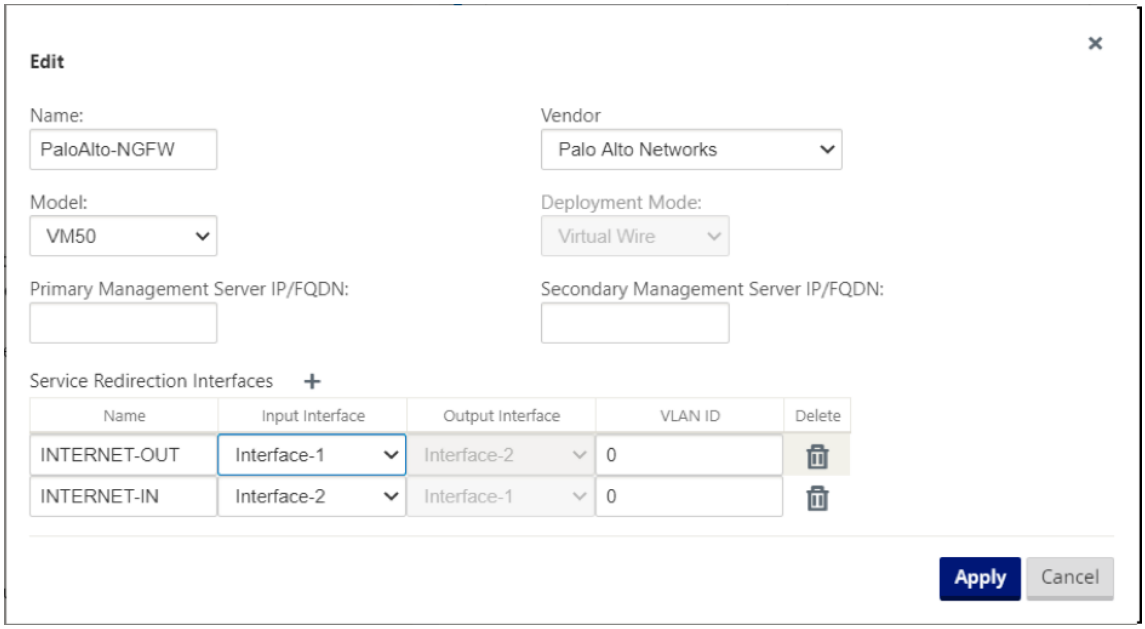
De forma predeterminada, las directivas de firewall SD-WAN son específicas de la dirección. El tipo de coincidencia simétrica coincide con las conexiones mediante criterios de coincidencia especificados y aplica la acción de directiva en ambas direcciones.

2. Abra la **interfaz de usuario de Citrix SD-WAN**, vaya a **Configuración** expanda **Virtual WAN** seleccione **Editor de configuración** > seleccione **Plantilla de cortafuegos alojada** en la sección **Global** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Haga clic en **+** y proporcione la información necesaria disponible en la siguiente captura de pantalla para agregar la plantilla **Hosted Firewall** y haga clic en **Agregar**.



La**plantilla de firewall alojado** le permite configurar la redirección de tráfico a la **máquina virtual de cortafuegos** alojada en el dispositivo SD-WAN. Las siguientes son las entradas necesarias para configurar la plantilla:

- **Nombre**: Nombre de la plantilla de firewall alojada.
- **Proveedor**: Nombre del proveedor del firewall.
- **Modo de implementación**: el campo **Modo de implementación** se rellena automáticamente y se atenuará en gris. Para el proveedor de **Palo Alto Networks**, el modo de implementación es **Virtual Wire**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Modelo: Modelo**de máquina virtual del firewall alojado. Puede seleccionar el número de modelo de la máquina virtual como VM 50/VM 100 para el proveedor de Palo Alto Networks.
- **Servidor de administración primario IP/FQDN**: servidor de administración principal IP/FQDN de Panorama.
- **Servidor de administración secundario IP/FQDN**: Servidor de administración secundario IP/FQDN de Panorama.
- **Interfaces de redirección de servicios**: Son interfaces lógicas utilizadas para la redirección de tráfico entre SD-WAN y firewall hospedado.

Interface-1, Interface-2 hace referencia a las dos primeras interfaces del firewall hospedado. Si se utilizan VLAN para la redirección del tráfico, se deben configurar las mismas VLAN en el firewall hospedado. Las VLAN configuradas para la redirección del tráfico son internas de la SD-WAN y del firewall hospedado.

> **Nota**
> La interfaz de entrada de
> redirección debe seleccionarse desde la dirección del iniciador de conexión, la interfaz de redirección se elige automáticamente para el tráfico de respuesta. Por ejemplo, si el tráfico de Internet saliente se redirige al firewall hospedado en Interface-1, entonces el tráfico de respuesta se redirige automáticamente al firewall hospedado en Interface-2. No hay necesidad de Interface-2 en el ejemplo anterior, si no hay tráfico entrante de Internet.

Solo se asignan dos interfaces físicas para alojar el firewall de Palo Alto Networks. Si el tráfico de varias zonas necesita ser redirigido al firewall hospedado, se pueden crear varias subinterfaces mediante VLAN internas y asociadas a diferentes zonas de firewall en el firewall hospedado.

A través de las directivas de firewall de SD-WAN o de las directivas de nivel de sitio, puede redirigir todo el tráfico a la máquina virtual Palo Alto Networks.

> **Nota**
> Las directivas de firewall
> SD-WAN se crean automáticamente para **permitir** el tráfico a/desde servidores de administración de firewall alojados. Esto evita la redirección del tráfico de administración que se origina desde (o) destinado al firewall hospedado.

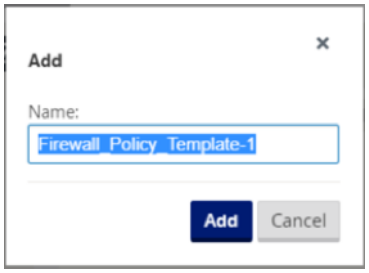
La redirección del tráfico a la máquina virtual del firewall se puede realizar mediante directivas de firewall SD-WAN. Existen dos métodos para crear directivas de firewall SD-WAN, ya sea a través de plantillas de directivas de firewall en la sección **Global** o a nivel de sitio.

Método - 1

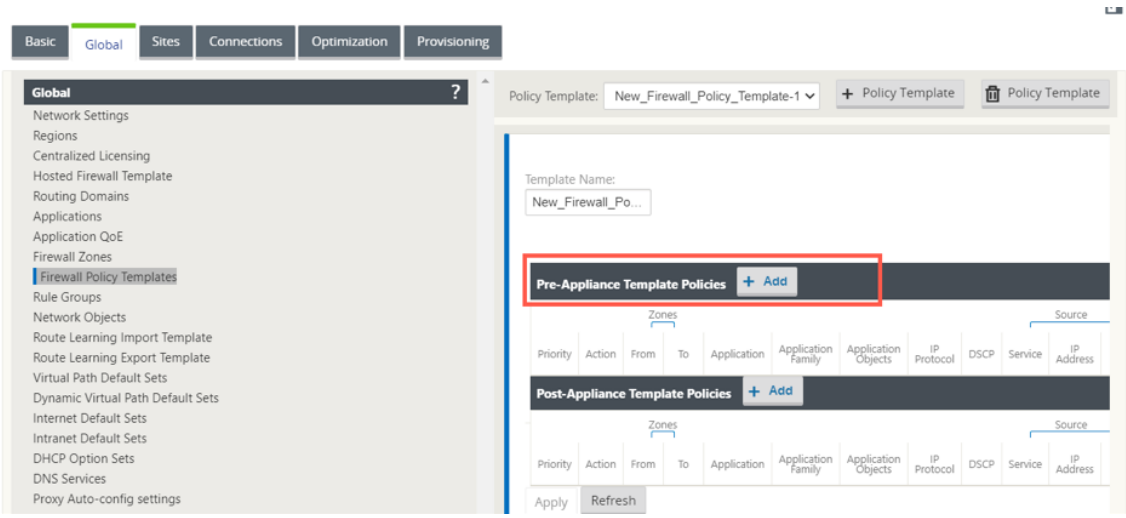
1. Desde la GUI de Citrix SD-WAN, vaya a **Configuración** expanda **Virtual WAN > Editor de configuración**. Vaya a la ficha **Global** y seleccione **Plantillas de directiva de cortafuegos**. Haga

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

clic en **+ Plantilla de directiva** Proporcione un nombre a la plantilla de directiva y haga clic en **Agregar**.

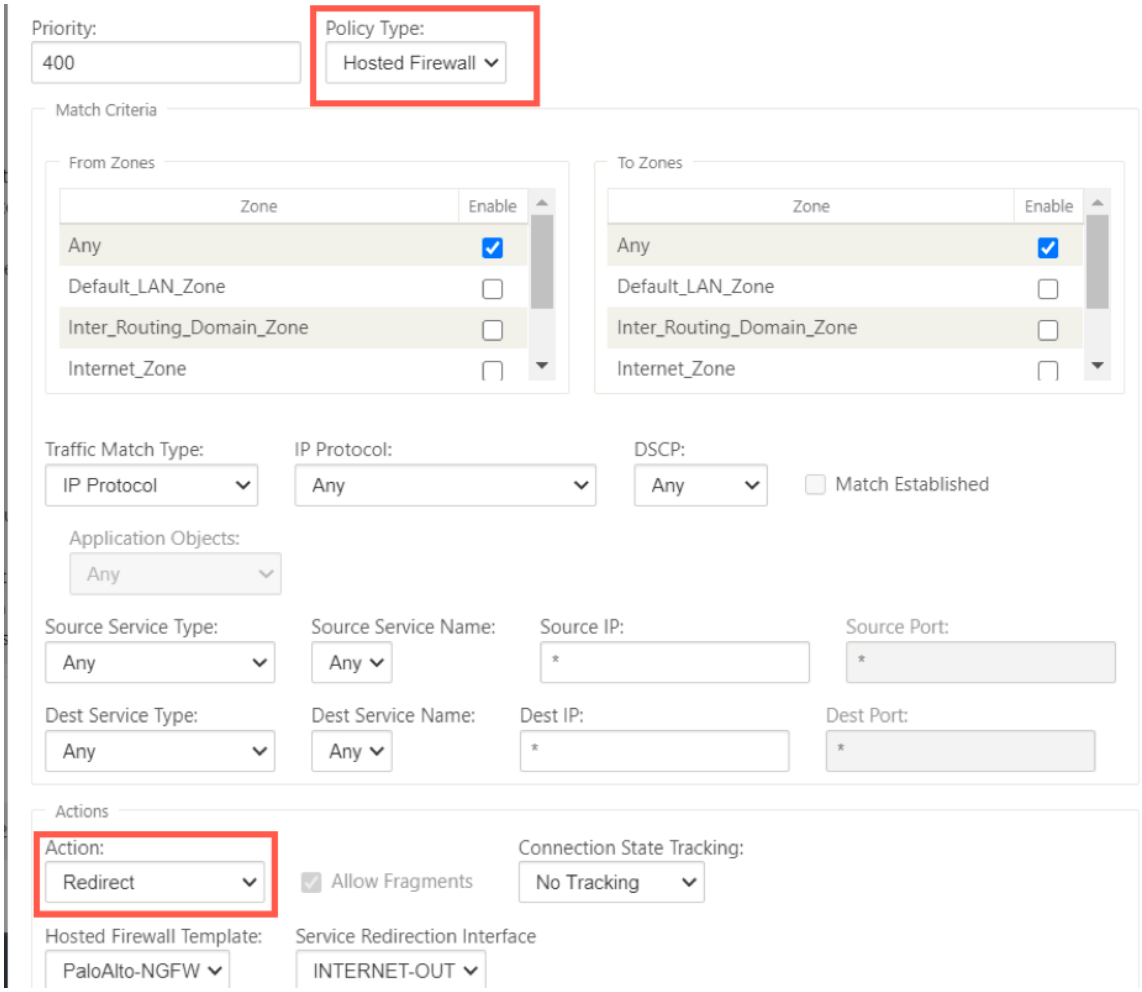


2. Haga clic en **+ Agregar** junto a **Directivas de plantillas previas al dispositivo**.

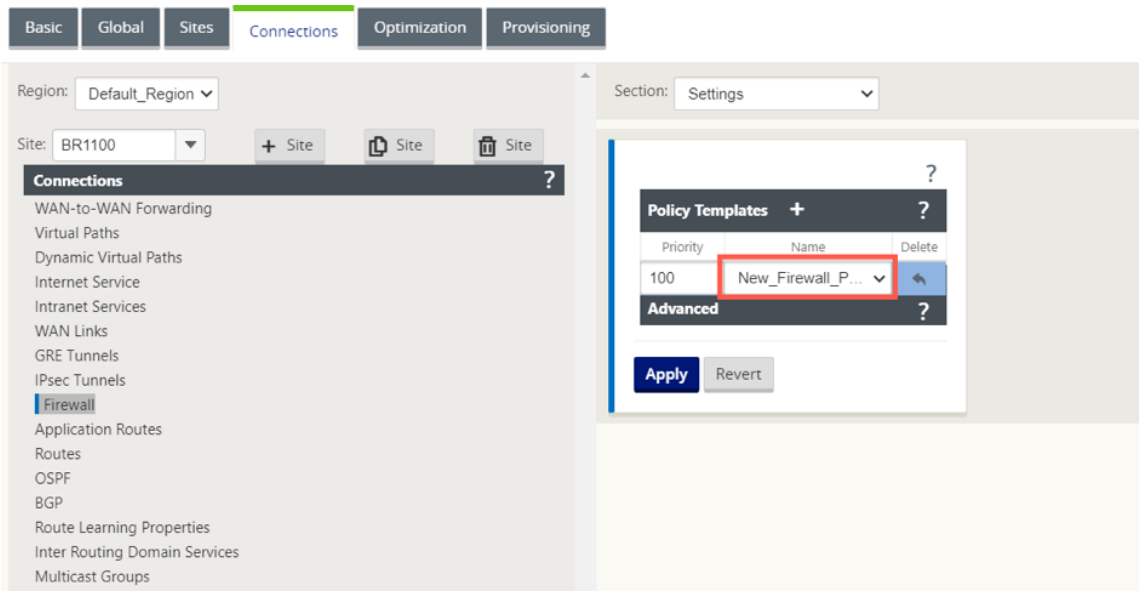


3. Cambie el **tipo de directiva** a **Firewall hospedado**. El campo **Acción** se rellena automáticamente para **Redirigir**. Seleccione la **plantilla de cortafuegos alojados** y la **interfaz de redirección de servicios** en la lista desplegable. Rellene los otros criterios de coincidencia según sea necesario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



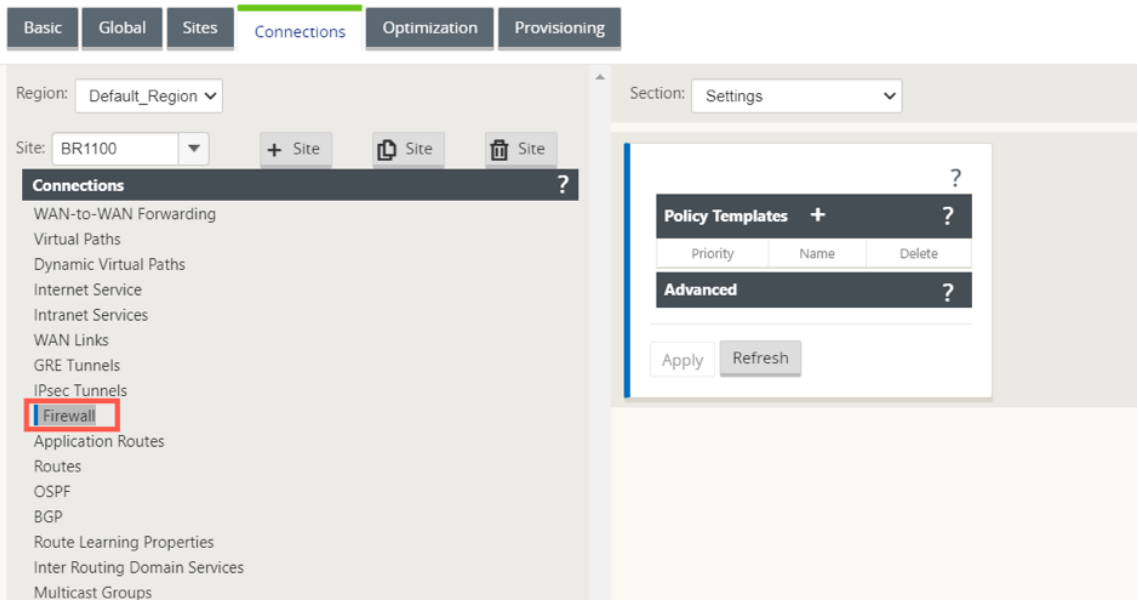
4. Desplácese hasta **Conexiones > Firewall**y, a continuación, seleccione la directiva de cortafuegos (que ha creado) en el campo Nombre. Haga clic en **Aplicar**.



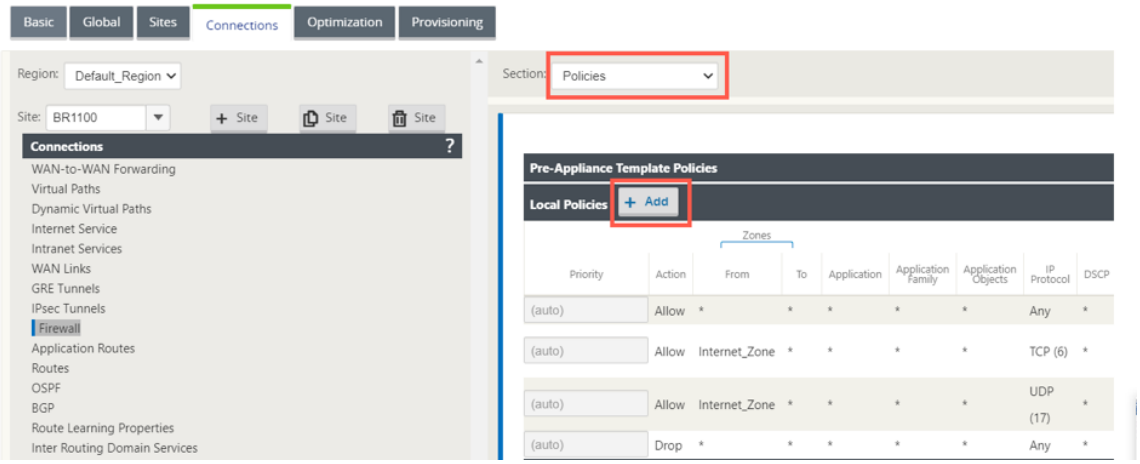
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Método - 2

1. Para redirigir todo el tráfico, en el **Editor de configuración > WAN virtual**, vaya a la ficha **Conexión** y seleccione **Firewall**.

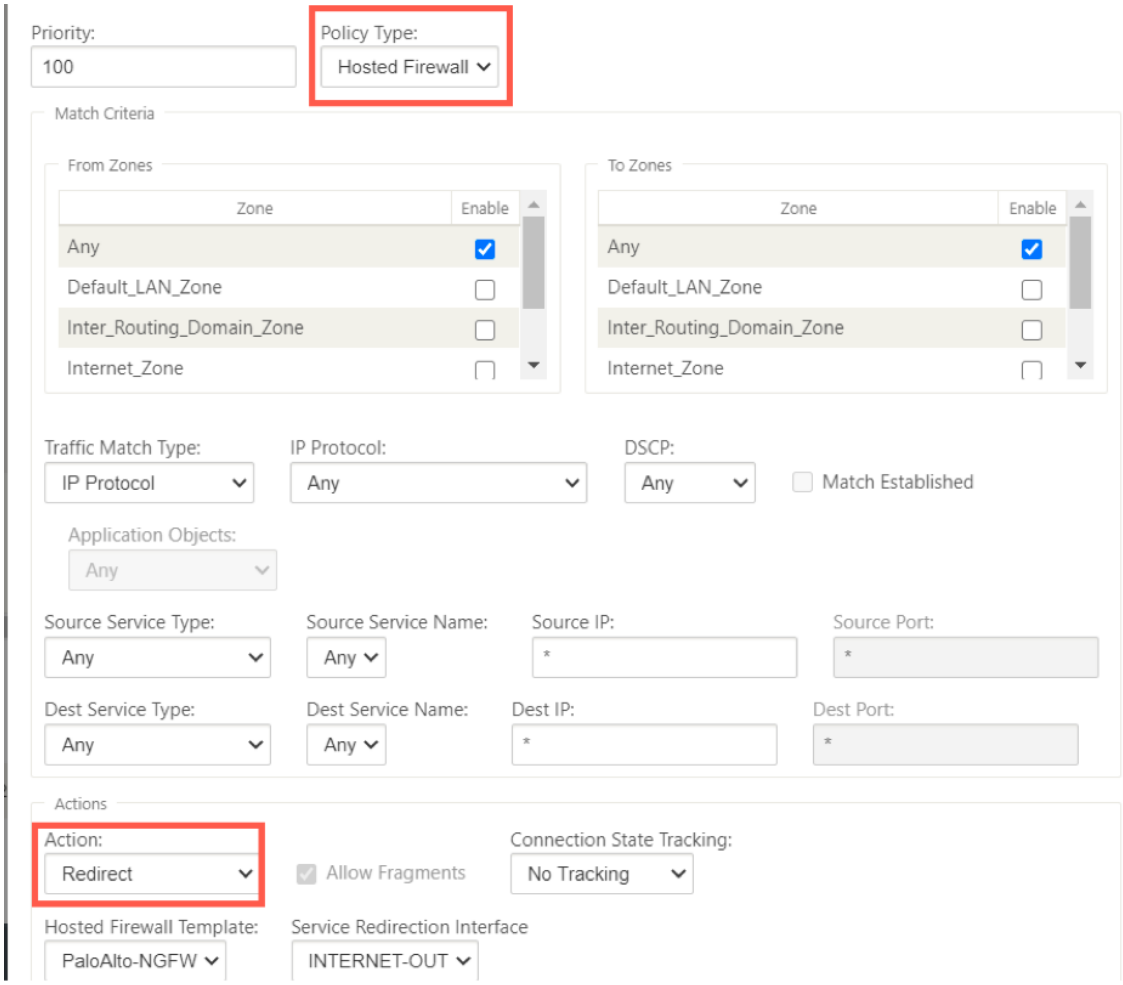


2. Seleccione **Directivas** en la lista desplegable **Sección** y haga clic en **+Agregar** para crear una nueva directiva de cortafuegos.



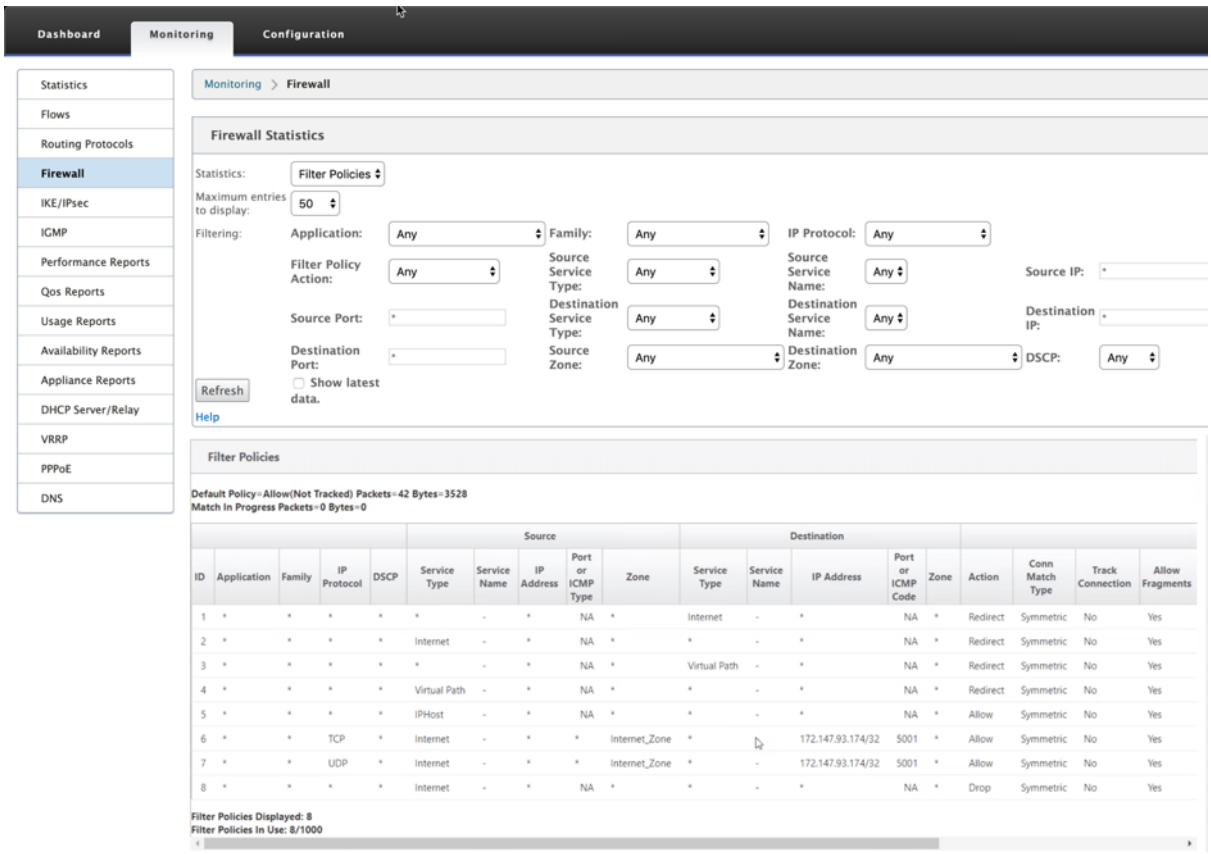
3. Cambie el **tipo de directiva** a **Firewall hospedado**. El campo **Acción** se rellena automáticamente para Redirigir. Seleccione la **plantilla de cortafuegos alojados** y la **interfaz de redirección de servicios** en la lista desplegable. Haga clic en **Agregar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

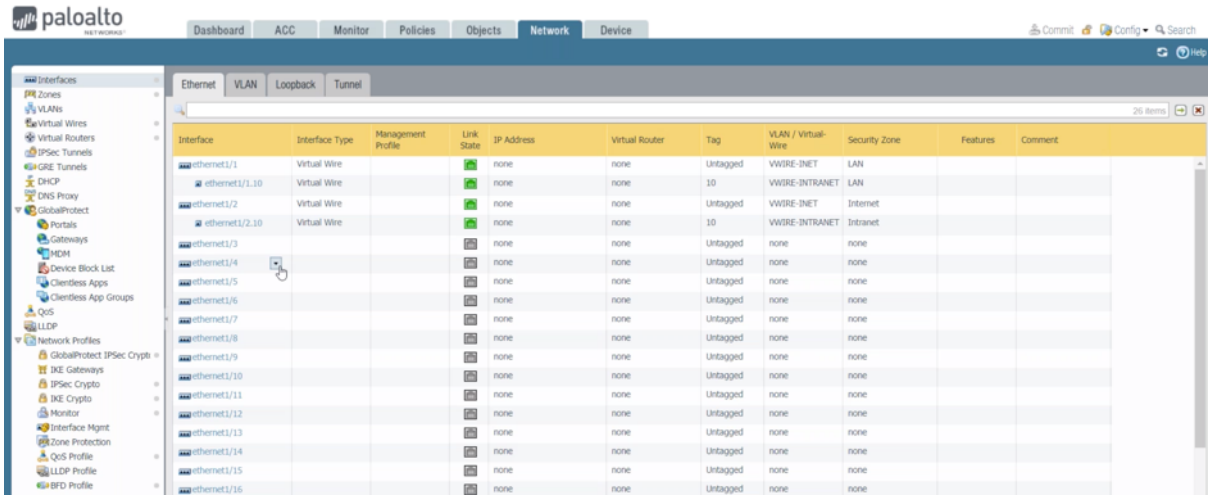


Mientras toda la configuración de red esté en modo activo y en ejecución, puede supervisar la conexión en **Supervisión > Firewall >** en la lista **Estadísticas**, seleccione **Directivas de filtro**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Puede verificar la asignación entre la configuración que realizó en la plantilla de la cadena de servicio SD-WAN y la configuración de la red de Palo Alto mediante la interfaz de usuario de Palo Alto Networks.



> **NOTA**
>
> La máquina virtual Palo Alto Networks no se puede aprovisionar si **Cloud Direct** o **SD-WAN WANOP (PE)** ya está aprovisionado en el dispositivo 1100.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

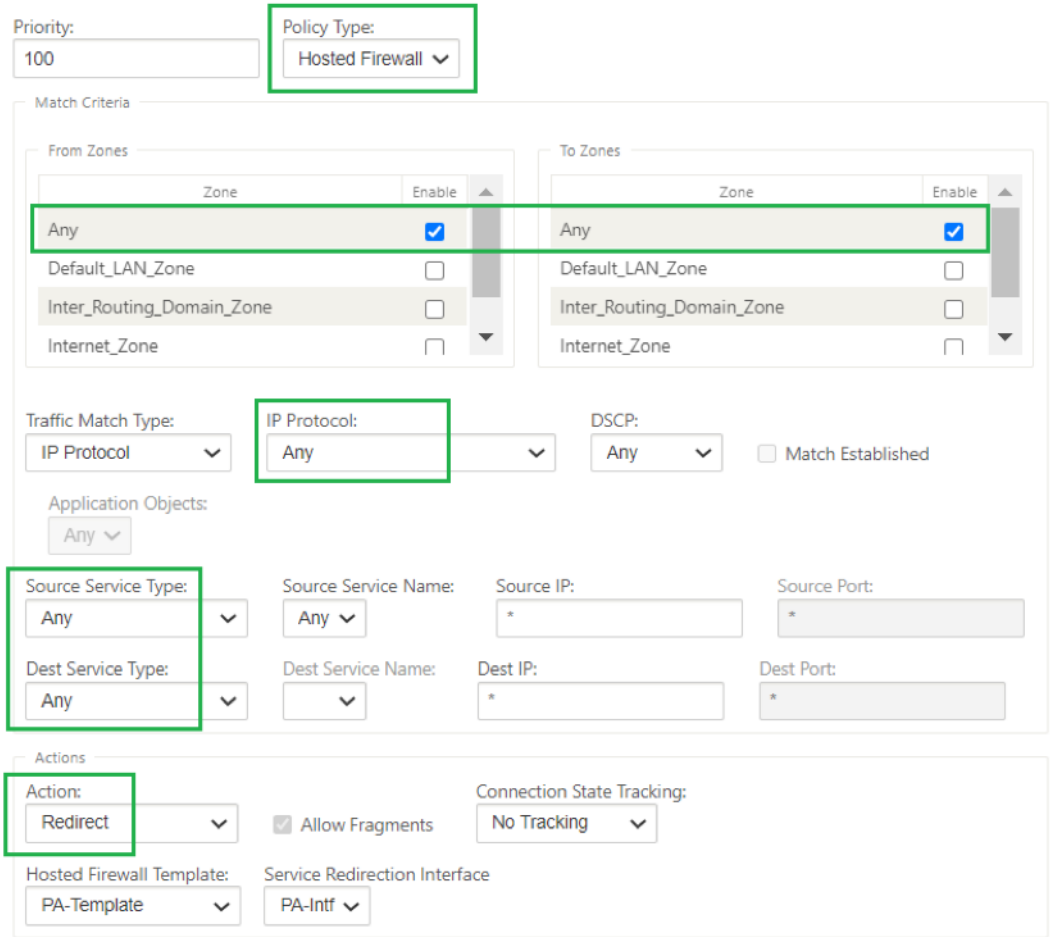
Casos de uso: Firewall alojado en SD-WAN 1100

Los siguientes son algunos de los casos de uso implementados mediante el dispositivo Citrix SD-WAN 1100:

Caso de uso 1: Redirigir todo el tráfico hacia Hosted Firewall

Este caso de uso es aplicable a casos de uso de sucursales pequeñas donde todo el tráfico es procesado por el firewall de próxima generación hospedado. Los requisitos de ancho de banda deben tenerse en cuenta, ya que la cantidad de tráfico redirigido está limitada a 100 Mbps.

Para lograrlo, cree una regla de cortafuegos que coincida con cualquier tráfico y con **Acción** como **redireccionamiento**, como se muestra en la siguiente captura de pantalla:

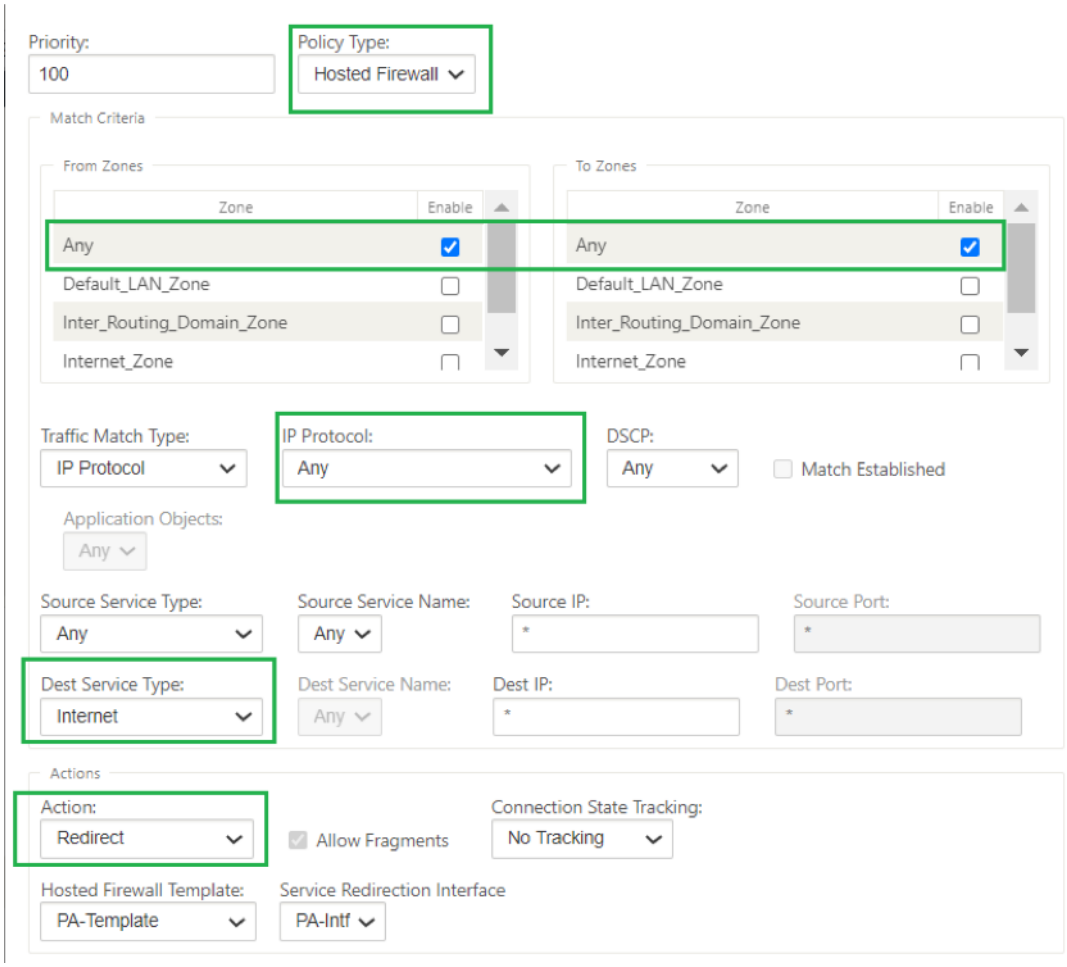


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Caso de uso 2: Redirigir solo el tráfico de Internet hacia Hosted Firewall

Este caso de uso es aplicable a cualquier sitio de sucursal en el que el tráfico vinculado a Internet no exceda la cantidad de rendimiento de tráfico redirigido admitido. En este caso, los dispositivos o servicios de seguridad implementados en centros de datos procesan el tráfico de sucursal al centro de datos.

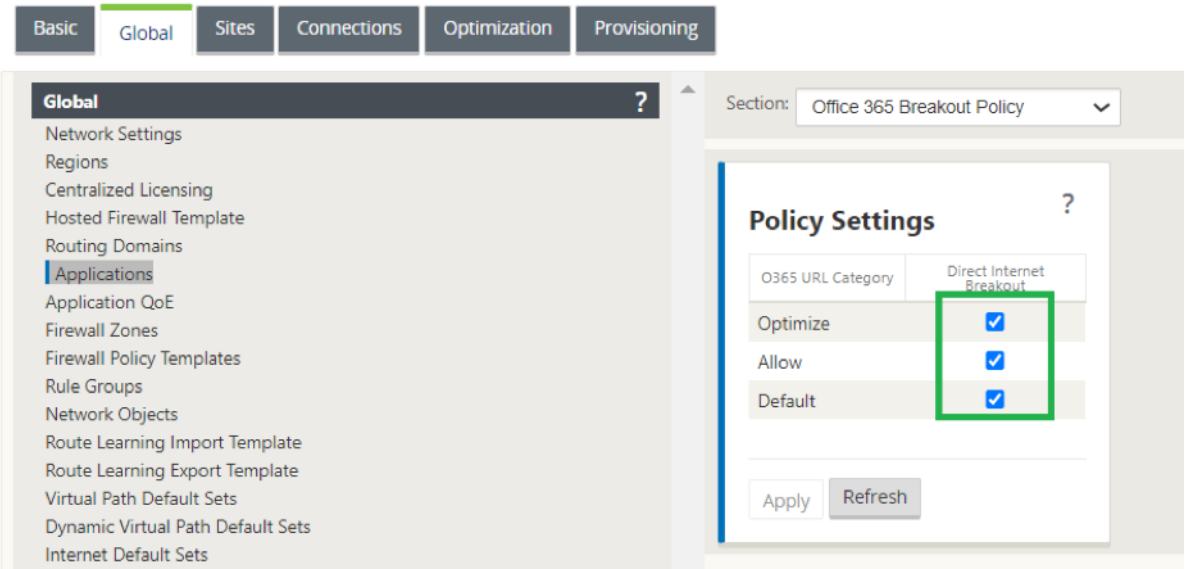
Para lograrlo, cree una regla de cortafuegos que coincida con cualquier tráfico y con **Acción** como **Redireccionamiento** como se muestra en la siguiente captura de pantalla:



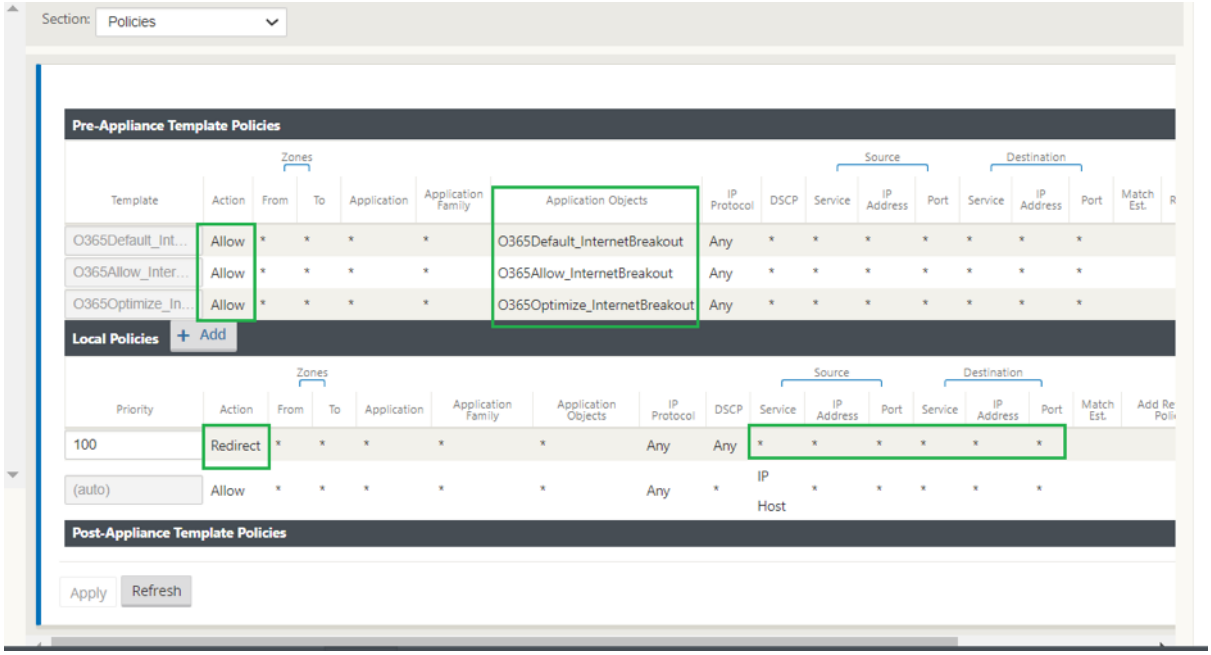
Caso de uso 3: Interrupción directa de Internet para aplicaciones SaaS de Internet de confianza y redirigir todo el tráfico restante a VM alojada

En este caso, se agrega una regla de firewall para realizar una ruptura directa de Internet para aplicaciones SaaS de confianza, como Office 365. Primero habilite la directiva de ruptura de Office 365 como se muestra en la siguiente captura de pantalla:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Esto agrega automáticamente **directivas de plantilla previas al dispositivo** para permitir el tráfico de Office 365, como se muestra en la siguiente captura de pantalla. Ahora agregue una regla de firewall para redirigir todo el tráfico restante al firewall alojado como se menciona a continuación.



Nota La

configuración del firewall alojado es independiente de la configuración de Citrix SD-WAN. Por lo tanto, el firewall alojado se puede configurar según los requisitos de seguridad de la empresa.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Grupos de agregación de enlaces

October 27, 2021

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.

En Citrix SD-WAN versión 11.0, se admite LAG simple (ACTIVE-BACKUP). Las negociaciones basadas en el protocolo 802.3ad LACP no se admiten en la versión actual. En cualquier momento, solo un puerto está 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. 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 4000, 4100 y 5100 SE
- Citrix SD-WAN 6100 SE

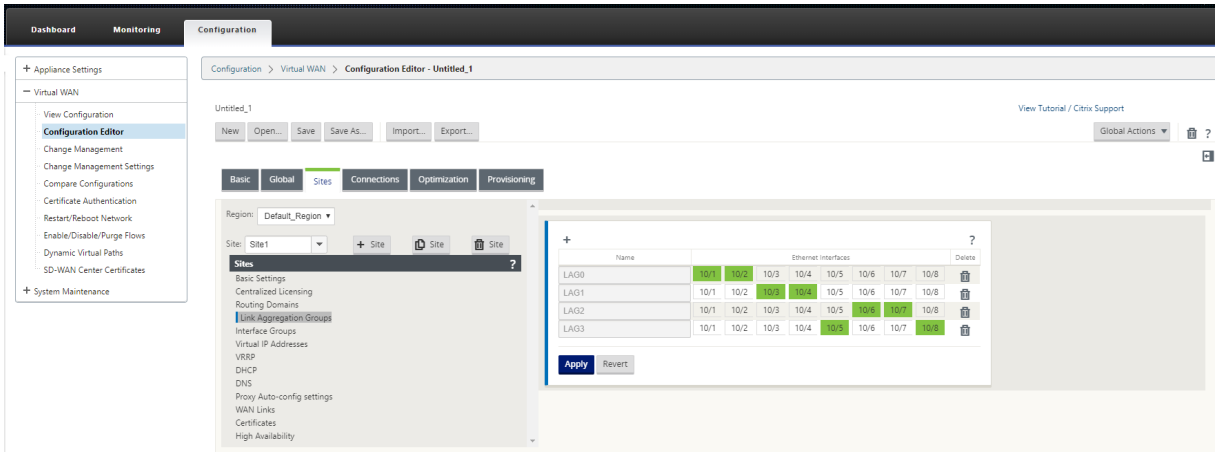
> **Nota**
>
> La funcionalidad LAG no es compatible con las plataformas VPX/VPXL.

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

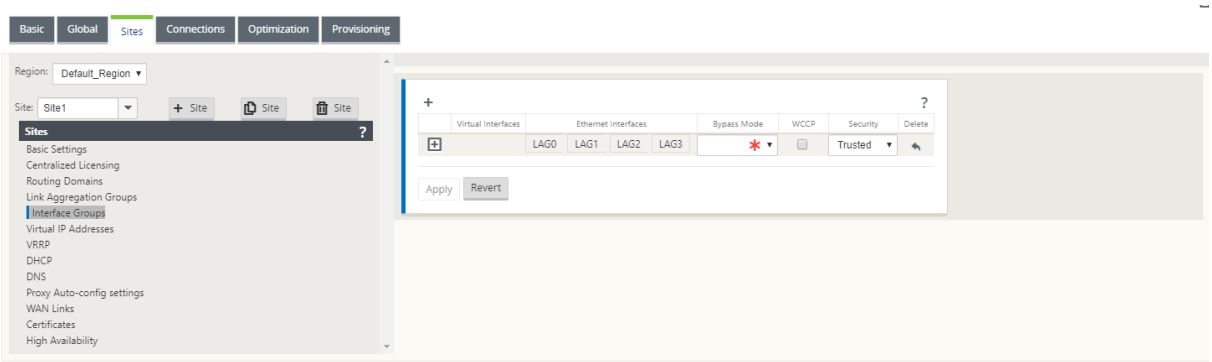
> **Nota**
>
> Para los dispositivos Citrix SD-WAN 210 y 410, solo puede crear un LAG con un máximo de tres puertos agrupados en él.

Para configurar grupos de agregación de vínculos, en el **Editor de configuración**, vaya a **Sitios** > **Grupos de agregación de vínculos**. Puede ver todos los puertos físicos e interfaces Ethernet disponibles. Haga clic en **+** para crear un LAG.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Seleccione los puertos miembros y haga clic en **Aplicar**. Una vez agregados los puertos al LAG, solo podrá ver los LAG del **grupo de interfaces** en lugar de los puertos miembros.

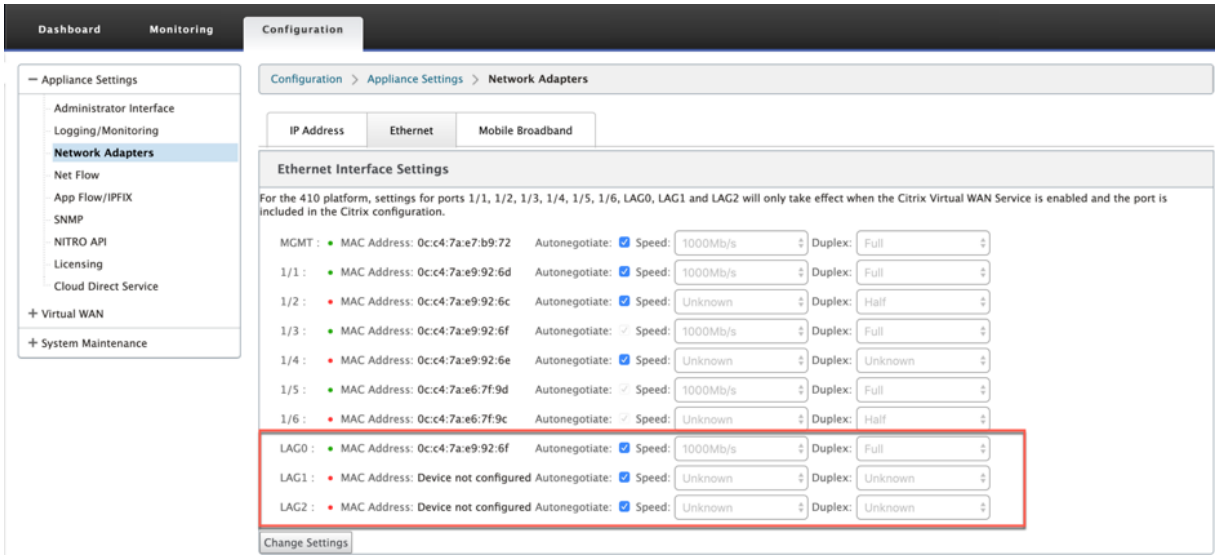


Puede crear interfaces virtuales mediante LAG y estas interfaces se utilizan para configurar enlaces LAN/WAN y HA.

> **Nota**
>
> La función de propagación del estado del enlace (LSP) no es compatible si los LAG se utilizan como interfaces Ethernet en los grupos de interfaces.

Puede ver los puertos LAG activos y en espera, vaya a **Configuración** > **Configuración del dispositivo** > **Adaptadores de red** > **Ethernet**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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.

Propagación del estado del vínculo

May 7, 2021

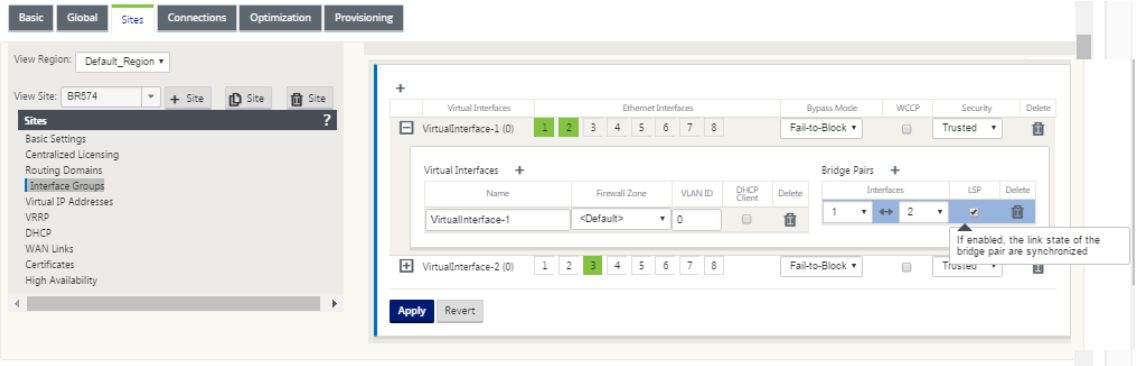
La función de propagación de estado de enlace (LSP) permite a los administradores de red mantener sincronizado el estado de enlace de un par de derivación, lo que permite a los dispositivos conectados del otro lado del vínculo ver cuando los vínculos están inactivos. Cuando un puerto de un par de bypass 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 vínculo interrumpido, su vínculo correspondiente se activa automáticamente.

Cómo configurar la propagación del estado del enlace

Para configurar la propagación del estado del vínculo:

1. Desplácese hasta **Editor de configuración** > **Sitios** > **[Nombre del sitio]** > **Grupos de interfaz**.
2. Expanda **Interfaces virtuales** y, en **Pairs de puente**, haga clic en la casilla de verificación **LSP** para habilitar **la Propagación de estado de enlace** para un par de puente. Haga clic en **Aplicar** para guardar la configuración.

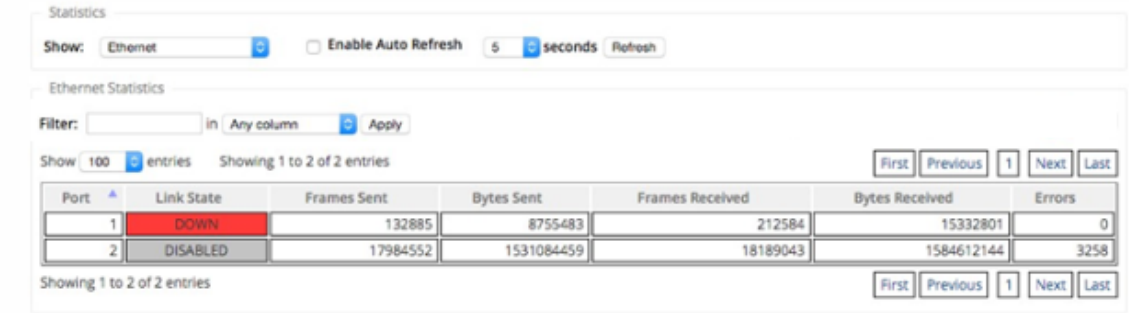
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supervisión de estadísticas de enlaces

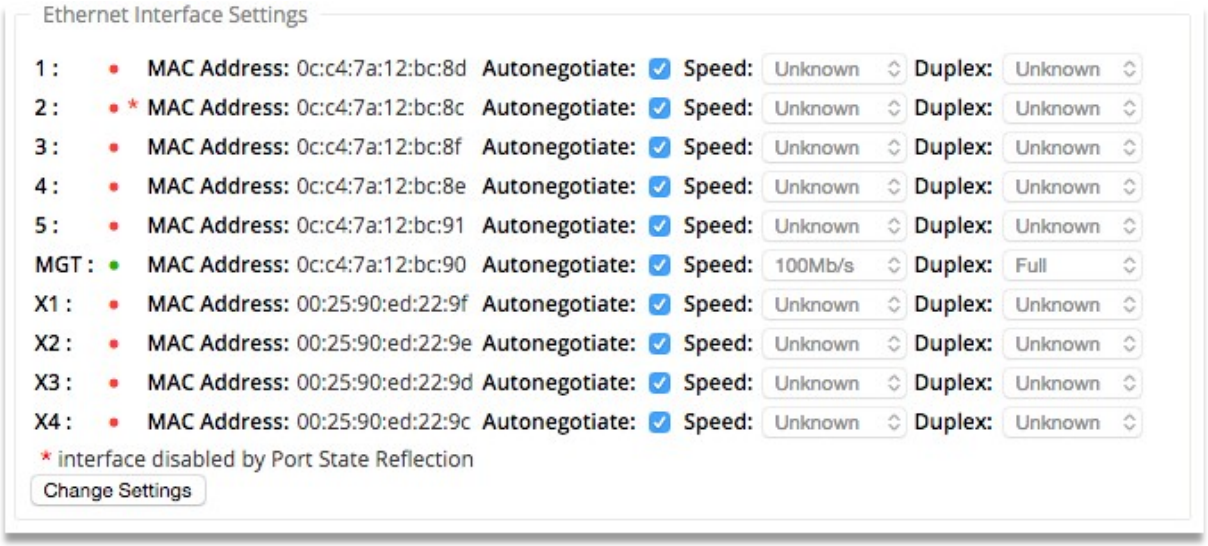
Para supervisar las estadísticas de vínculos:

1. En la página **Monitor > Estadísticas**, seleccione **Ethernet** en el menú implementable **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 equipo** > **Adaptadores de red > ficha Ethernet**. Los puertos que están administrativamente inactivos se indican con un asterisco rojo (*) en la lista **Configuración de la interfaz Ethernet**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Enlaces WAN de medición y espera

January 10, 2022

Citrix SD-WAN admite la habilitación de vínculos medidos, que se pueden configurar de modo que el tráfico de usuario se transmita en un enlace WAN de Internet específico cuando todos los demás enlaces WAN disponibles están inhabilitados.

Los enlaces medidos conservan el ancho de banda en 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. Set Last Resort normalmente está 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 ser demasiado costoso para un negocio 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 (semana/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 latido

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Se realiza un seguimiento del uso del ancho de banda en un vínculo medido local 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. Este evento de alerta de uso también se puede ver en SD-WAN Center. Una ruta de medición se puede formar con 1 o 2 enlaces de medición. Si se forma una ruta entre dos vínculos con medición, el intervalo de latido activo utilizado en la ruta con medición es el mayor de los dos intervalos de latido 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 dosificada que está en estado BUENO, una ruta dosificada lleva una cantidad reducida de tráfico de control y se evita cuando el plano de reenvío busca una ruta 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 bajo 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 bajo 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 último
  - 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Intervalo de latido activo**: Intervalo de latido que se utiliza cuando la ruta de espera está activa (por defecto 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- **Intervalo de latido en espera**: El intervalo de latido utilizado cuando la ruta de espera está inactiva (predeterminado 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/disabled)

Una ruta en espera se forma con 1 o 2 enlaces en espera.

- **Bajo demanda**: Se forma una ruta de espera bajo demanda entre:
  - un enlace no en espera y un enlace en espera bajo demanda
  - 2 enlaces en espera bajo 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 bajo demanda y un enlace en espera de último recurso
  - 2 enlaces en espera de último recurso

Los intervalos de latido utilizados en una ruta de espera se determinan de la siguiente manera:

- Si el latido de espera está inhabilitado en al menos 1 de los 2 enlaces, el latido se inhabilita en la ruta de espera mientras está inactivo.
- Si el latido de espera no está inhabilitado en ninguno de los vínculos, el mayor de los dos valores se utiliza cuando la ruta de espera está en espera.
- Si el intervalo de latido activo está configurado en ambos vínculos, el mayor de los dos valores se utiliza cuando la ruta de espera está activa.

Mensajes de latido (mantener vivo):

- En una ruta de acceso no en espera, los mensajes de latido se envían cuando no ha habido tráfico (control o usuario) durante al menos un intervalo de latido. El intervalo de latido del corazón varía según el estado de la ruta. Para rutas **no en espera y no medidas** :
  - 50 ms cuando el estado de la ruta es BUENO
  - 25 ms cuando el estado de la ruta es INCORRECTA

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 latido se envían regularmente en el intervalo de latido 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 ruta es MAL.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Mientras está activo, al igual que las rutas que no están en espera, los mensajes de latido se envían cuando no ha habido tráfico (control o usuario) durante al menos el intervalo de latido activo configurado.
- el intervalo de latido de espera configurado se utiliza cuando el estado de ruta es BUENO.
- 1/2 el intervalo de latido de espera configurado se utiliza cuando el estado de ruta es incorrecto.

Mientras están inactivas, las rutas en espera no son elegibles para el tráfico de usuarios. Los únicos mensajes de protocolo de control enviados en rutas de espera inactivas son los mensajes de latido, que son para la detección de fallos de conectividad y la recopilación de métricas de calidad. Cuando las rutas en espera están activas, son elegibles para el tráfico de usuario con un coste de tiempo adicional. Esto se hace para que las rutas no en espera, si están disponibles, sean favorecidas durante la selección de rutas de reenvío.

El estado de ruta de una ruta de acceso en espera con latido desactivado, mientras está inactivo, se supone que 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 se inicia en estado DESCONECTADA hasta que escucha de su par Ruta virtual, se inicia en estado BUEN. Si no se detecta conectividad con el par de ruta virtual, la ruta pasa mal y, a continuación, MUERTA. Si se restablece la conectividad con el par de ruta virtual, la ruta pasa mal y, a continuación, BUENA de nuevo.

Si dicha ruta de espera pasa DESCONECTADA y luego se vuelve inactiva, el estado de la ruta no cambia inmediatamente a (supuesto) BUENO. En su lugar, 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 ruta de menor prioridad con rutas MUERTO buenas asumidas y un grupo de ruta de mayor prioridad con rutas BUENO realmente. Este período de espera (NO_HB_PATH_ON_HOLD_PERIOD_MS) se establece en 5 min y se puede cambiar a través de 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 hace una transición entre modo de espera y activo.

Requisitos previos de configuración:

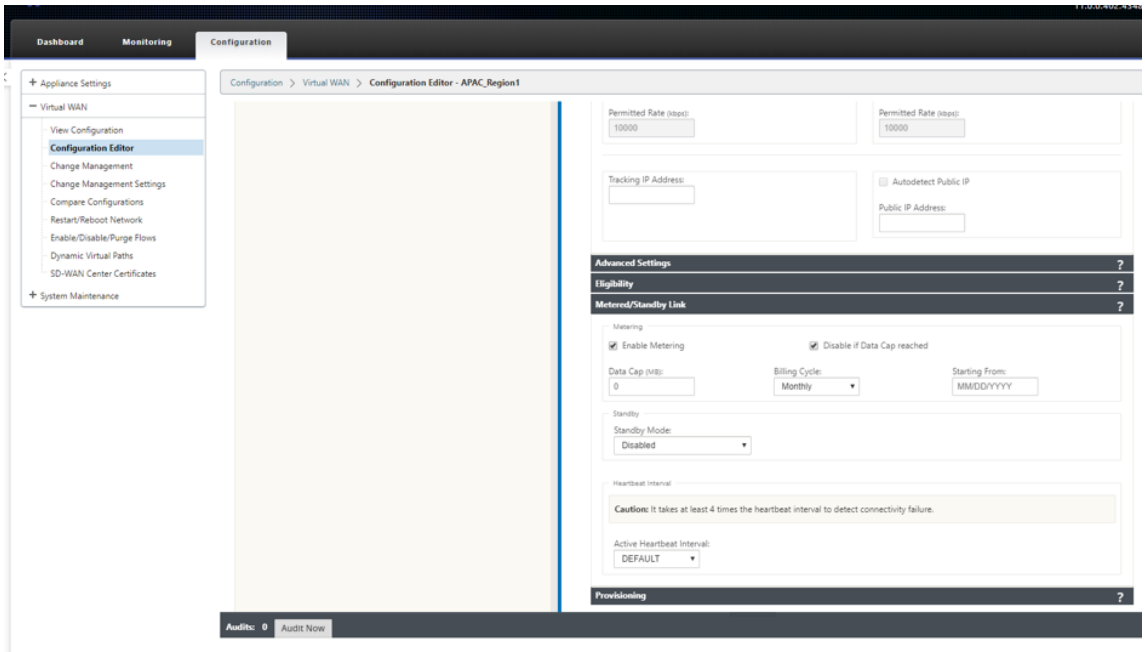
- Un enlace de medidor puede ser de cualquier tipo de acceso.
- Todos los enlaces de un sitio se pueden configurar con la medición habilitada.
- Un vínculo en espera puede ser del tipo de acceso a Internet público o Intranet privada. Un enlace WAN del tipo de acceso MPLS privado no se puede configurar como vínculo en espera.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Debe configurarse al menos un vínculo 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 bajo demanda. Los vínculos en espera bajo demanda admiten el servicio de ruta virtual.
- El servicio de Internet puede configurarse en un vínculo de espera de último recurso, pero se admite el modo de equilibrio de carga.
- El servicio de intranet puede configurarse en un vínculo en espera de último recurso, pero se admite el modo secundario y debe habilitarse la recuperación primaria.

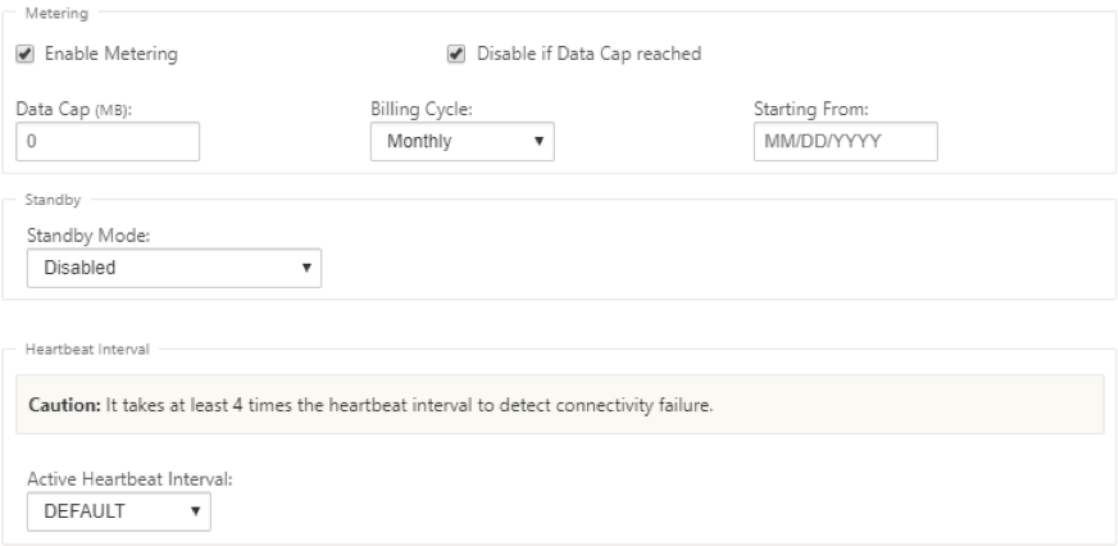
Para configurar vínculos medidos:

1. En la interfaz de administración web de SD-WAN, vaya a **Configuración > Virtual WAN >** seleccione **Editor de configuración >** agregar o seleccionar **Sitios** en la lista implementable > seleccione **Enlaces WAN >** Haga clic en la ficha **Vínculo medido/en espera** para expandir.it.



2. Active la casilla de verificación **Habilitar medición**. Puede proporcionar valores para el límite de datos, la fecha de inicio del ciclo de facturación y el intervalo de latido activo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

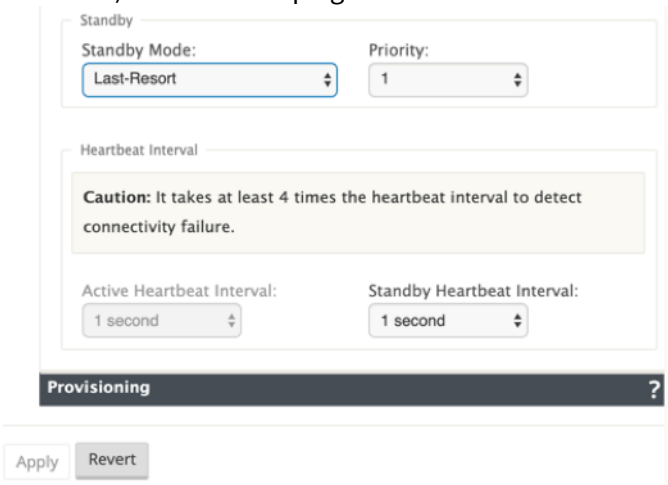


3. Desactivar si se alcanza el límite de datos:

   - Si la casilla **Inhabilitar si se alcanza el límite de datos** está activada, el vínculo medido y todas sus rutas relacionadas se inhabilitarán hasta el siguiente ciclo de facturación, si el uso de datos alcanza el límite de datos.
   - De forma predeterminada, la casilla de verificación **Inhabilitar si se alcanza el límite de datos** estará desactivada, donde conserva el modo actual o el estado establecido para que el vínculo medido continúe después de alcanzar el límite de datos hasta el siguiente ciclo de facturación.

Para configurar vínculos en espera:

1. De forma predeterminada, el modo de espera de un enlace WAN está inhabilitado. Para configurar el enlace WAN como en espera, seleccione uno de los modos de espera (Last-Resort/Bajo demanda) en la lista desplegable.



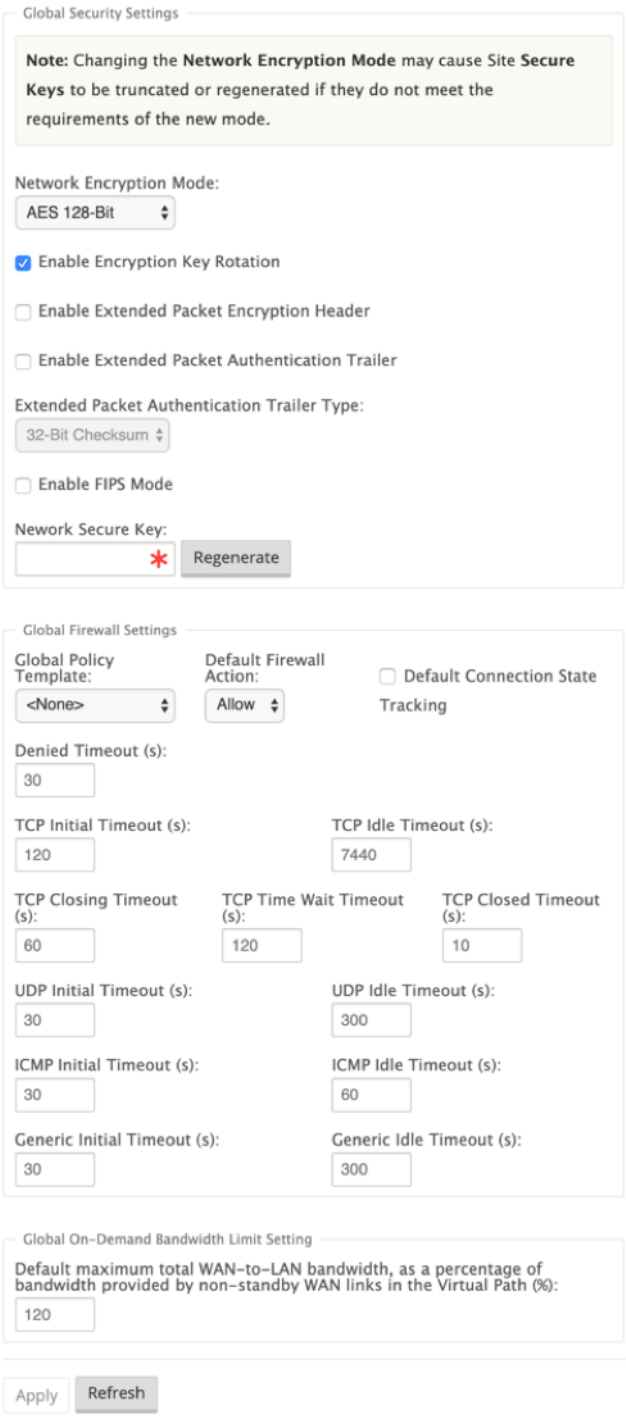
2. Una vez seleccionado un modo en espera, seleccione la prioridad en espera, el intervalo de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

latido activo y el intervalo de latido en espera según corresponda. Haga clic en **Aplicar** para validar la configuración.

3. Si se configura un vínculo en espera bajo demanda, el límite global de ancho de banda bajo demanda predeterminado (120%) se aplica a la ruta virtual. Especifica el ancho de banda máximo de WAN a LAN permitido para la ruta virtual. Se expresa como un porcentaje del ancho de banda total proporcionado por todos los enlaces no en espera de la ruta virtual. Siempre que el ancho de banda disponible en la ruta virtual esté por debajo del límite y si hay suficiente uso, el dispositivo intentará activar rutas bajo demanda para complementar el ancho de banda.
4. Para ver o cambiar el límite de ancho de banda bajo demanda predeterminado global, abra las secciones **Global** > Configuración de **red WAN virtual**.

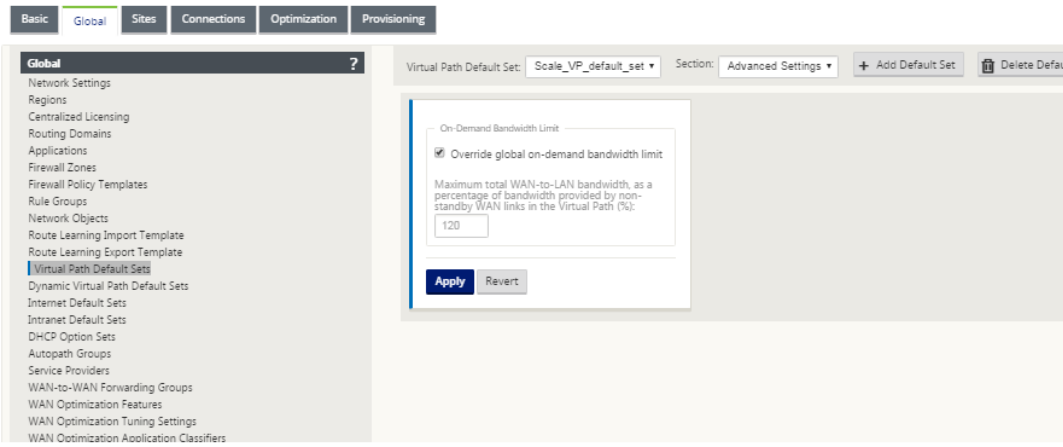
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



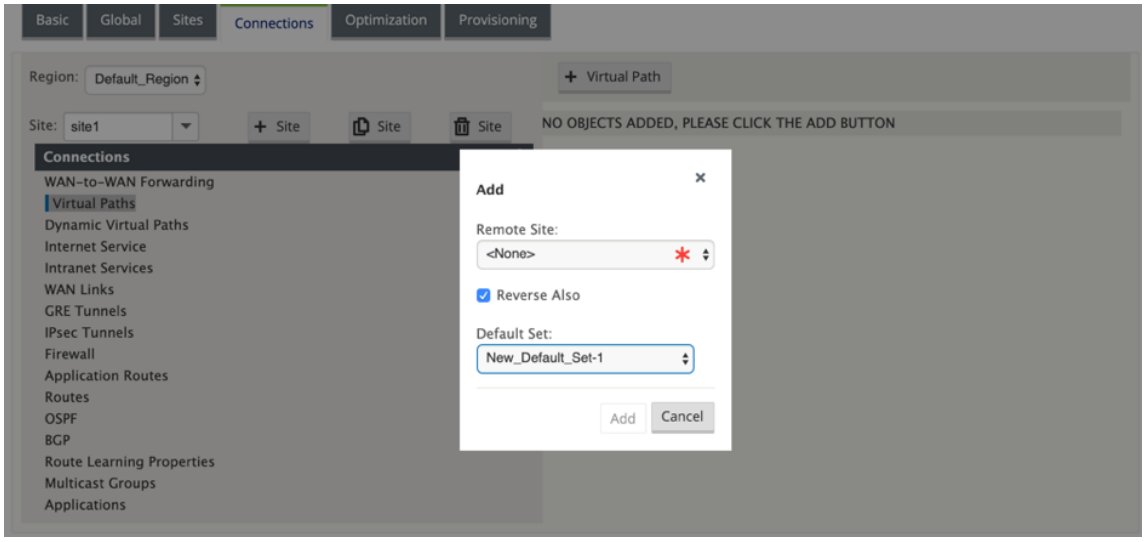
5. Si quiere aplicar un límite de ancho de banda bajo demanda específico a una ruta virtual y mantener sin cambios la configuración predeterminada global, debe crearse un conjunto predeterminado de ruta virtual y se puede cambiar el límite de ancho de banda bajo demanda en Config-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

uración avanzada.



6. Para aplicar la configuración de una ruta virtual específica, vaya a la sección **Conexiones > Rutas virtuales** y haga clic en **+ Ruta virtual**.

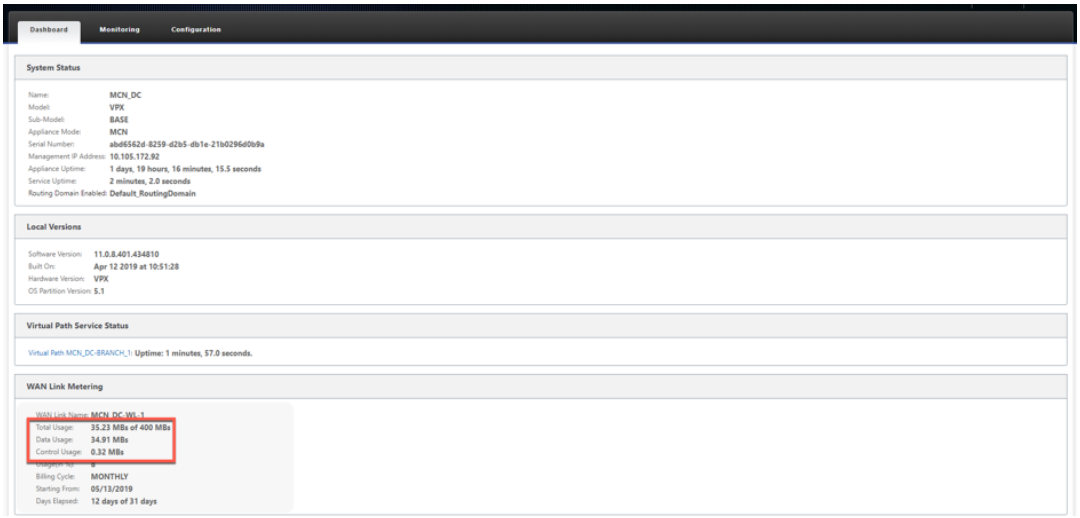


Supervisar enlaces WAN medidos y en espera

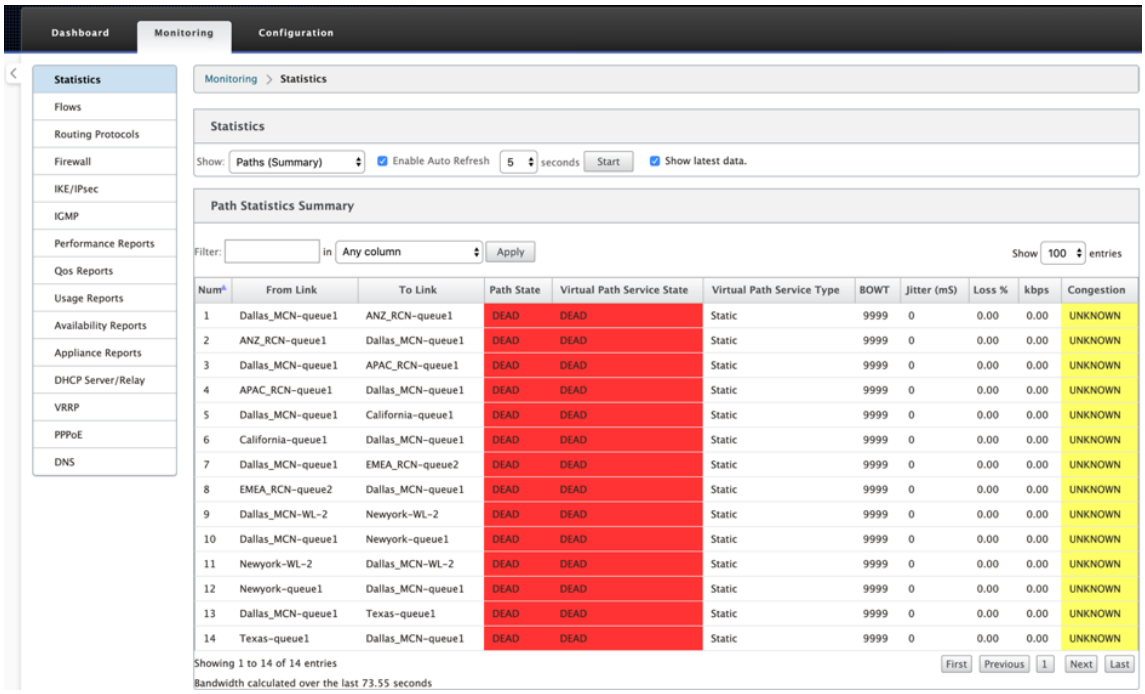
- La página Panel proporciona la siguiente información de **medición de enlaces WAN** con los valores de uso:
  - **Nombre del enlace WAN**: Muestra el nombre del enlace WAN.
  - **Uso total**: Muestra el uso total del tráfico (Uso de datos + Uso de control).
  - **Uso de datos**: Muestra el uso por tráfico de usuario.
  - **Uso de Control**: Muestra el uso por tráfico de control.
  - **Uso (en %)**: Muestra el valor del límite de datos utilizado en porcentaje (Uso total/Límite de datos) x 100.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Ciclo de**Facturación: Frecuencia de Facturación (semana/mensual)
- **De Inicio**: Fecha de inicio del ciclo de facturación
- **Días Transcurridos**: El tiempo transcurrido (en días, horas, minutos y segundos)

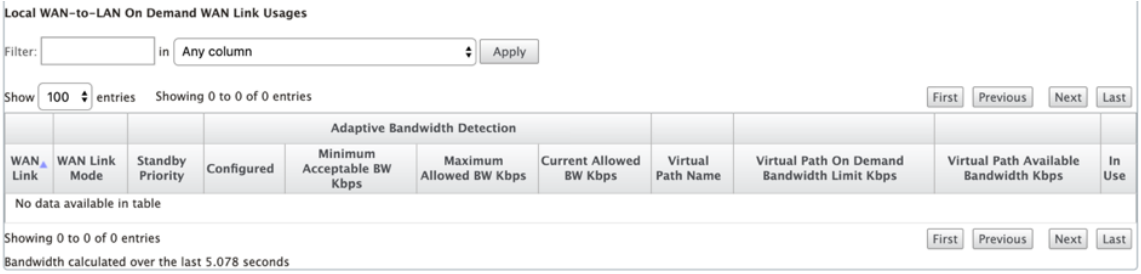


- Cuando se muestran las estadísticas de ruta (**Supervisión > Estadísticas > Rutas**), los enlaces medidos y los vínculos en espera se marcan como se muestra en la captura de pantalla.

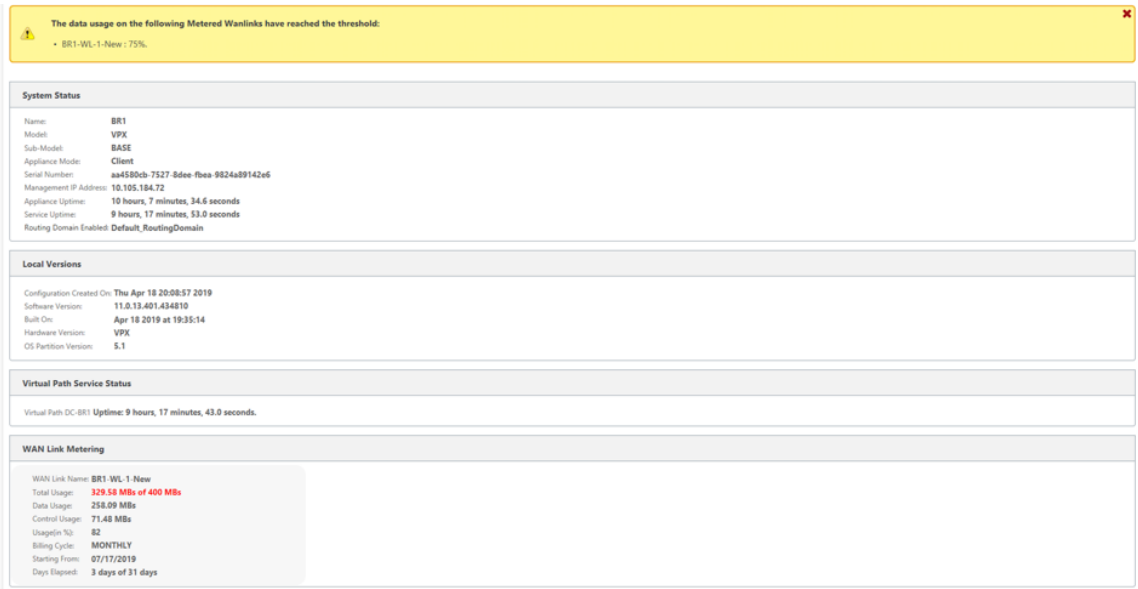


- Si el dispositivo tiene una ruta virtual que tiene un vínculo en espera a petición local o remoto, cuando se visualizan las estadísticas de uso de enlaces WAN, se muestra una tabla adicional que muestra el ancho de banda bajo demanda en la parte inferior de la página (**Supervisión > Estadísticas > Uso de enlaces WAN**).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 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 supera el 75% del límite de datos configurado, se resalta la información de medición numérica hacia la parte inferior del panel.



También se genera un evento de uso de enlaces WAN en el dispositivo cuando el uso supera el 50%, el 75% y el 90% del límite de datos configurado.

17654	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:22:58	USAGE_3	WARNING	Total usage 1.84 GBytes used (91% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17653	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:17:58	USAGE_2	WARNING	Total usage 1.52 GBytes used (75% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17652	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:09:58	USAGE_1	WARNING	Total usage 1.00 GBytes used (50% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017

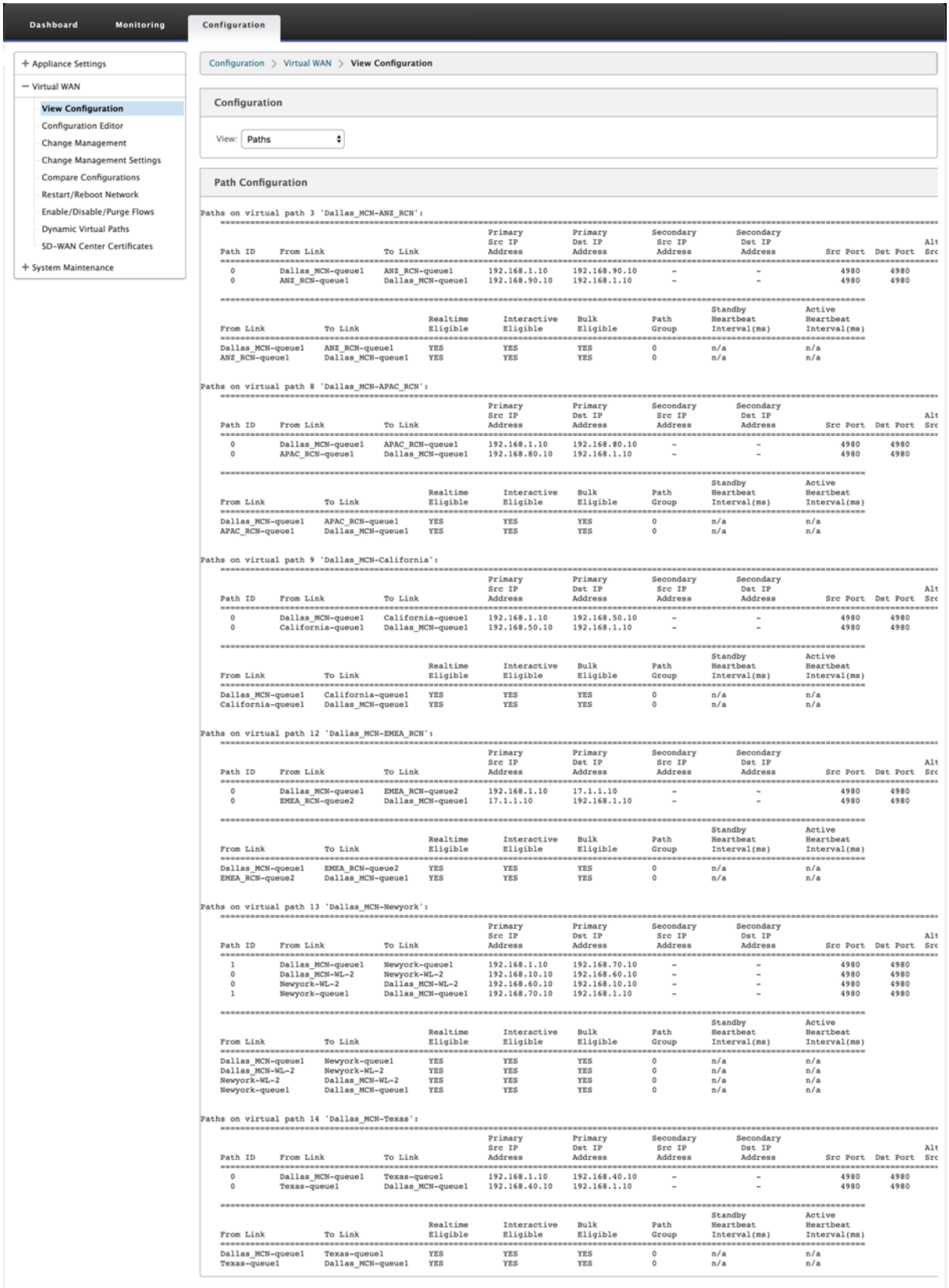
1. Cuando una ruta en espera pasa entre el estado en espera y activo, el dispositivo genera un evento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Optimización de Office 365

May 7, 2021

Las características de **optimización de Office 365** se adhieren a Principios de conectividad de red de Microsoft Office 365, para 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 y evitar prácticas como el backhaul a un proxy central. Esto se debe a que el tráfico de Office 365, como Outlook, Word, etc., es sensible a la latencia y el tráfico de backhauling introduce latencia adicional, 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 extremo de servicio de Office 365 más cercano, que existe en los bordes 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. Esto minimiza la latencia a medida que se reduce el tiempo de ida y vuelta de la red del cliente al dispositivo de punto final 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 se separan en las tres categorías siguientes:

- **Optimizar**: Estos dispositivos de punto final proporcionan conectividad a todos los servicios y funciones de Office 365, y son muy 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 dispositivos de punto final deben separarse de la sucursal a Internet y no deben pasar por el centro de datos.
- **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 significativamente menor. Estos extremos están alojados en centros de datos de Microsoft. Las solicitudes de servicio a estos dispositivos de punto final pueden separarse de la sucursal a Internet o pasar por el centro de datos.
- **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. Algunos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de estos extremos pueden no estar 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, es posible que el tráfico de esta categoría no siempre sea tráfico de Office 365, por lo que se recomienda inhabilitar esta opción al habilitar el grupo de trabajo de Office 365 en la red.

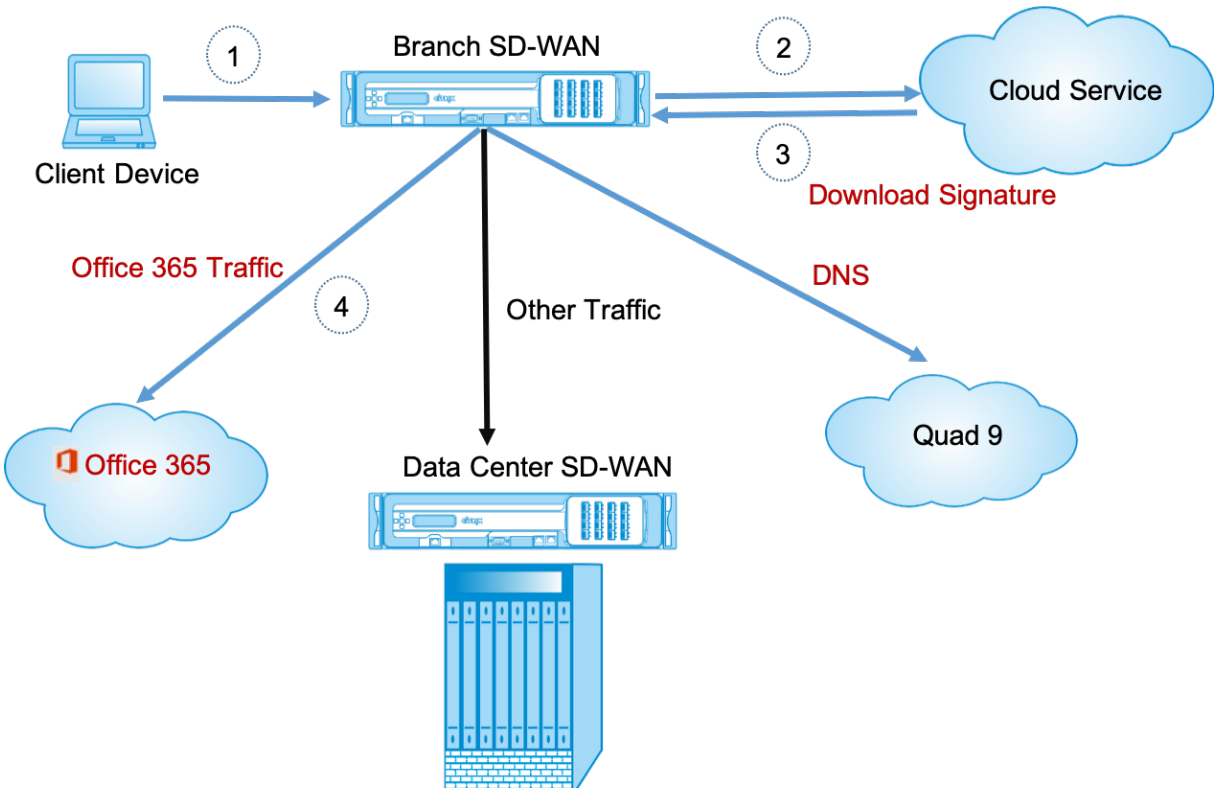
Cómo funciona la optimización de Office 365

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 activado y la optimización de Office 365 está habilitada. 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**
>
> Primera detección y clasificación de paquetes del tráfico de Office 365 se realiza si la función de ruptura de Office 365 está habilitada.

Cuando llega una solicitud de aplicación de Office 365, el clasificador de aplicaciones realiza una 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Las firmas se descargan desde Cloud Service (sdwan-app-routing.citrixnetworkapi.net).

Configurar el grupo de trabajo de Office 365

La directiva de grupo de Office 365 le permite especificar qué categoría de tráfico de Office 365 puede separar directamente de la sucursal. Al habilitar el grupo de Office 365 y compilar la configuración, se crea automáticamente un objeto DNS, un objeto de aplicación, una ruta de aplicación y una plantilla de directiva de firewall y se aplica a sitios de sucursales con servicio de Internet.

Requisitos previos

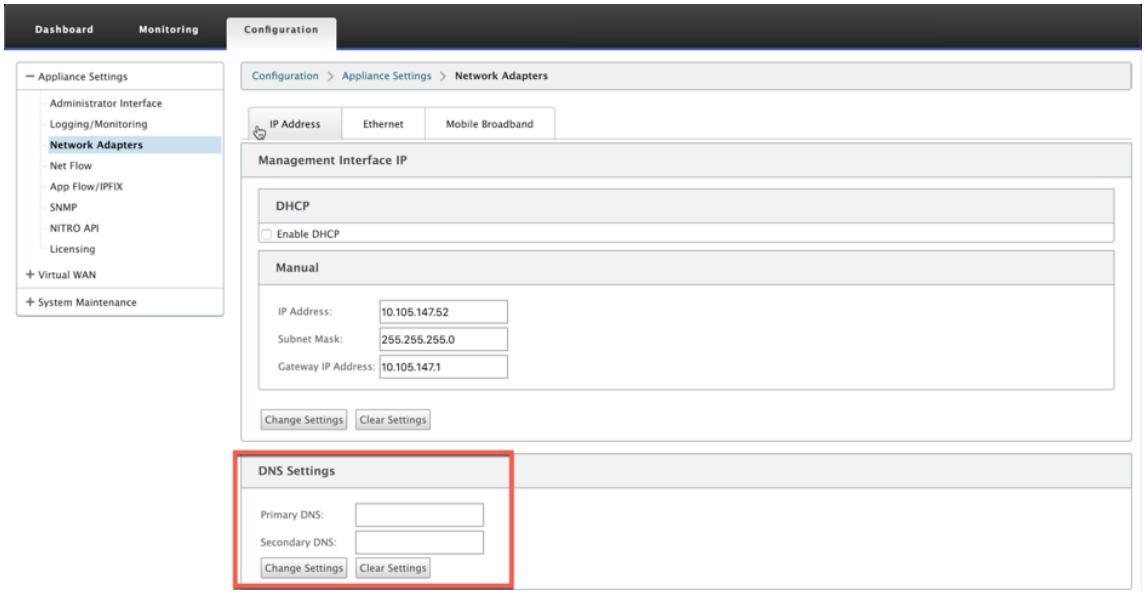
Asegúrese de que dispone de lo siguiente:

1. Para realizar una ruptura de Office 365, se debe configurar un servicio de Internet en el dispositivo. Para obtener más información sobre la configuración del servicio de Internet, consulte Acceso a Internet.
2. Asegúrese de que la interfaz de administración tenga conectividad a Internet.

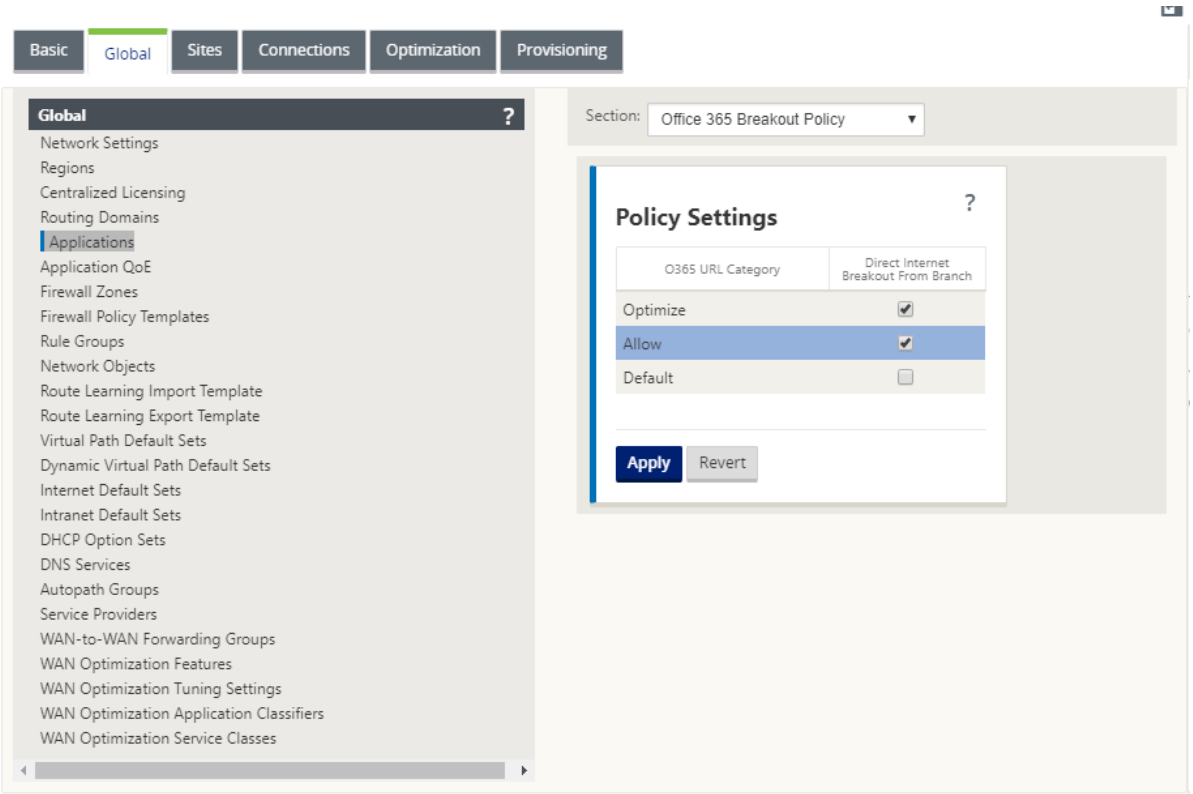
   Puede utilizar la interfaz web de Citrix SD-WAN para configurar los parámetros de la interfaz de administración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Asegúrese de que el DNS de administración esté configurado. Para configurar el DNS de la interfaz de administración, vaya a **Configuración > Configuración del dispositivo > Adaptador de red**. En la sección **Configuración de DNS**, proporcione los detalles del servidor DNS principal y secundario y haga clic en **Cambiar configuración**.



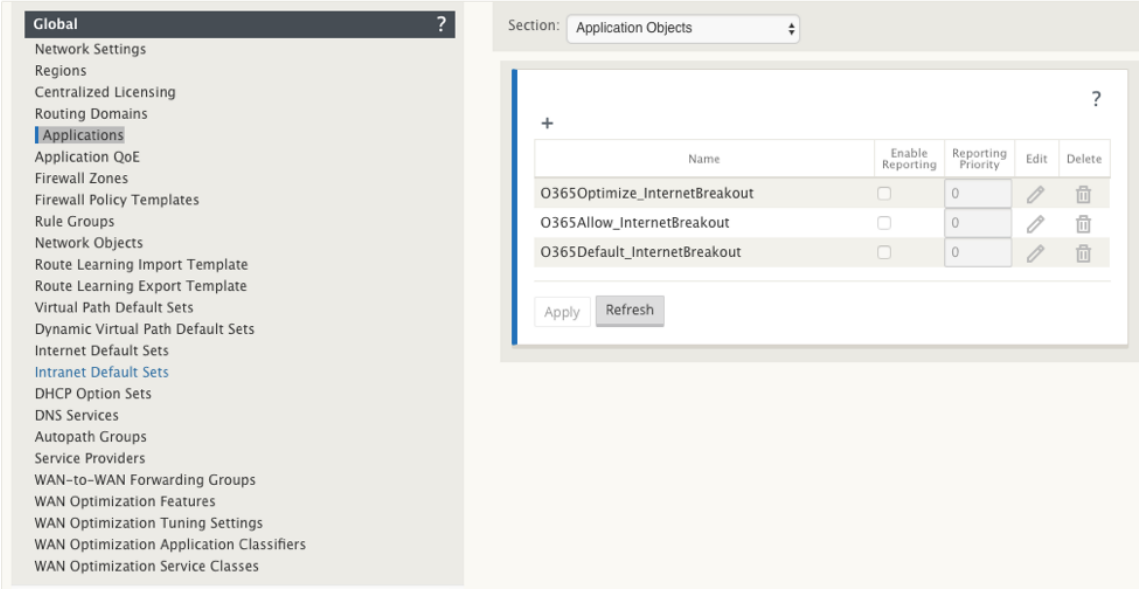
La configuración de **directiva de grupo de Office 365** está disponible en configuración global, seleccione la categoría de Office 365 necesaria para el grupo de trabajo de Internet y haga clic en **Aplicar**.



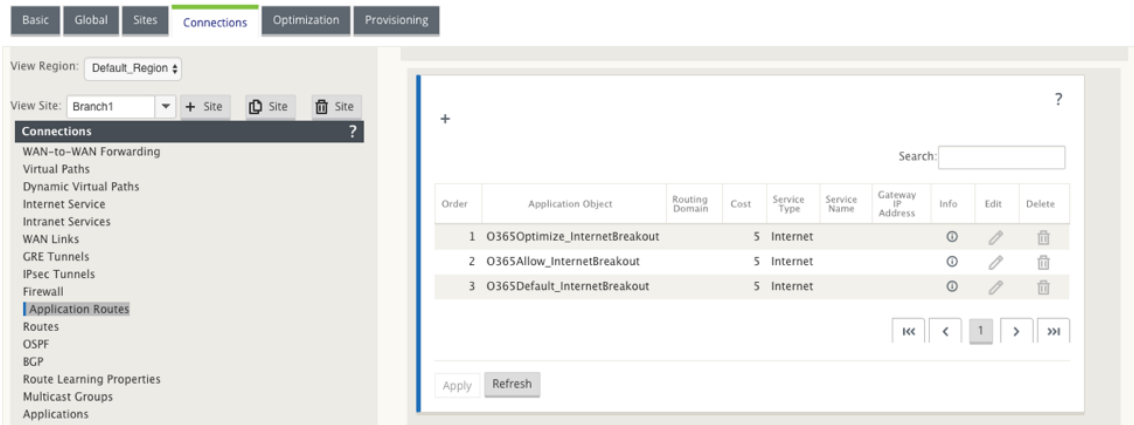
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de configurar la configuración de directiva de ruptura de Office 365 y compilar la configuración. Los siguientes ajustes se rellenan automáticamente.

- **Objeto DNS**: El objeto DNS especifica el tipo de tráfico que se reenviará al servicio DNS que está configurado el usuario. Las solicitudes DNS se escuchan en todas las interfaces de confianza y los reenviadores DNS se incluyen para dirigir las solicitudes DNS de Office 365 al servicio Quad9. Esta regla de reenviador tiene la máxima prioridad. Para obtener más información, vea la sección **Servicio de nombres de dominio**.
- **Objeto Application**: Se crea un objeto de aplicación con la categoría Office 365 seleccionada por el usuario. Si ha seleccionado optimizar, permitir y categorías predeterminadas, se crean los objetos de aplicación **O365Optimize_InternetBreakout, O365Allow_InternetBreakout** y **O365Default_InternetBreakout**.



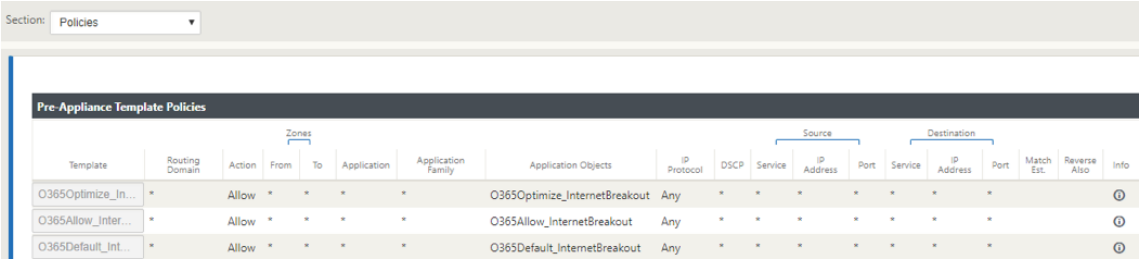
- **Ruta de aplicación**: Se crea una ruta de aplicación para cada uno de los objetos de aplicación de Office 365 con el tipo de servicio de Internet.



- **Plantilla de directiva previa al dispositivo de firewall**: Se crea una plantilla de directiva

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

global previa al dispositivo para cada categoría configurada de Office 365. Esta plantilla se aplica a todos los sitios de sucursales que tienen servicio de Internet. La directiva previa al dispositivo tiene prioridad sobre las plantillas de directiva local y posterior al dispositivo.

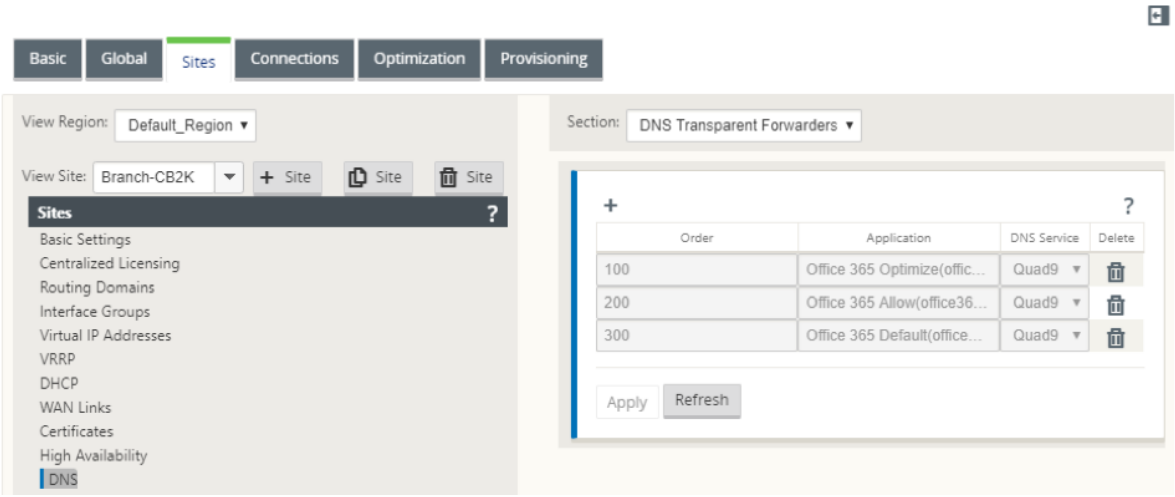


Reenviador transparente para Office 365

La sucursal se descompone para Office 365 comienza con una solicitud DNS. La solicitud DNS que pasa por dominios de Office 365 tiene que ser dirigida 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.

Se crearán reenviadores transparentes para aplicaciones de Office 365 en cada sucursal que tenga habilitado el servicio de Internet y la división 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.

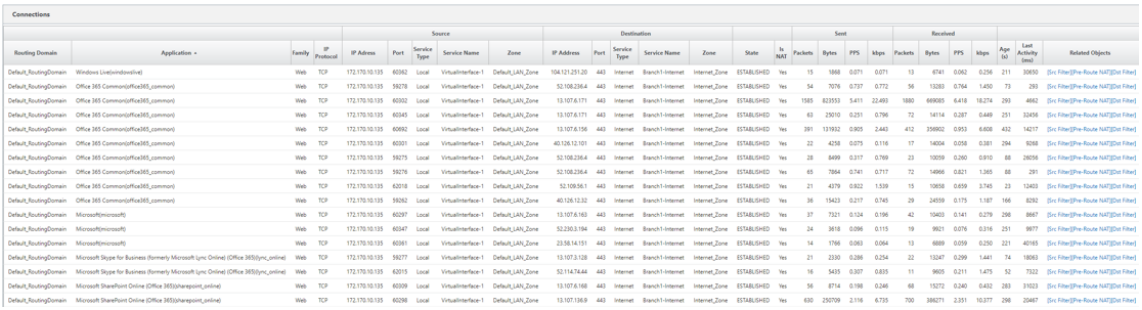


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Supervisión

Puede supervisar las estadísticas de aplicaciones de Office 365 en los siguientes informes estadísticos de SD-WAN:

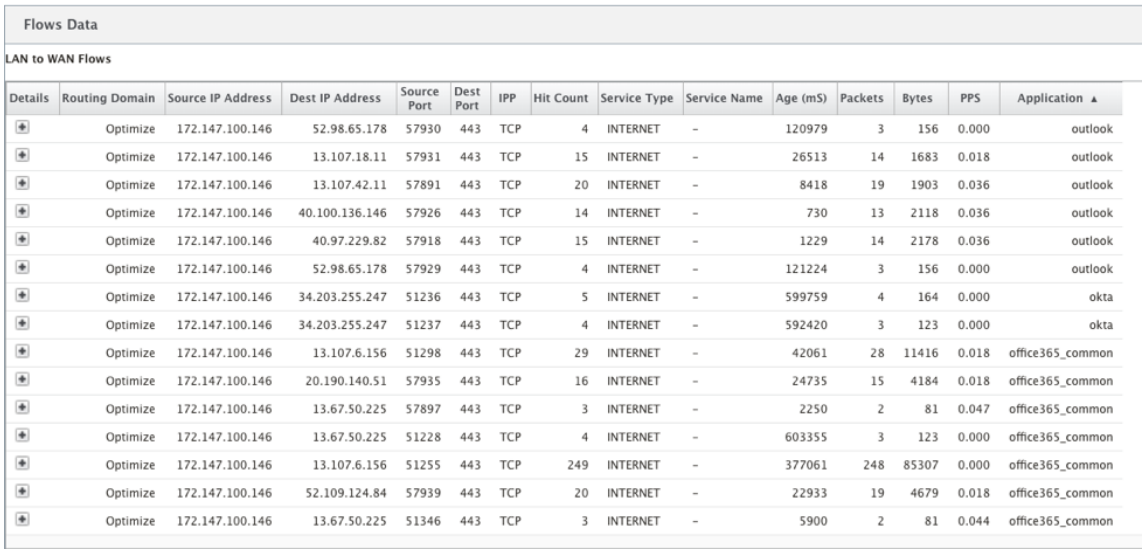
- Estadísticas del firewall



Connections

				Source					Destination							Sent				Received						
Routing Domain	Application	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (s)	Last Activity (ms)	Related Objects
Default_RoutingDomain	Windows Live(windowslive)	Web	TCP	172.170.10.135	60362	Local	VirtualInterface-1	Default_LAN_Zone	104.121.251.20	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	15	1868	0.071	0.071	13	4741	0.062	0.256	211	30850	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59278	Local	VirtualInterface-1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	54	7076	0.737	0.772	56	13283	0.764	1.450	73	293	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60302	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	1585	823553	3.411	22.493	1880	669085	6.418	18.274	293	4662	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60345	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	63	25010	0.251	0.796	72	14114	0.287	0.449	251	32436	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60692	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.156	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	391	131932	0.905	2.443	412	356902	0.953	6.608	432	14217	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60301	Local	VirtualInterface-1	Default_LAN_Zone	40.126.12.101	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	22	4258	0.075	0.116	17	14004	0.058	0.381	294	9268	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59275	Local	VirtualInterface-1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	28	8499	0.317	0.769	23	10059	0.260	0.910	88	28256	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59276	Local	VirtualInterface-1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	65	7864	0.741	0.717	72	14966	0.821	1.365	88	291	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	62018	Local	VirtualInterface-1	Default_LAN_Zone	52.109.56.1	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	21	4379	0.922	1.539	15	10858	0.659	3.745	23	12403	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59262	Local	VirtualInterface-1	Default_LAN_Zone	40.126.12.32	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	36	15423	0.217	0.745	29	24559	0.175	1.187	166	8292	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft(microsoft)	Web	TCP	172.170.10.135	60297	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.163	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	37	7321	0.124	0.196	42	10403	0.141	0.279	298	8867	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft(microsoft)	Web	TCP	172.170.10.135	60347	Local	VirtualInterface-1	Default_LAN_Zone	52.230.3.194	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	24	3618	0.096	0.115	19	9921	0.076	0.316	251	9877	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft(microsoft)	Web	TCP	172.170.10.135	60361	Local	VirtualInterface-1	Default_LAN_Zone	23.58.14.151	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	14	1766	0.063	0.064	13	6889	0.059	0.250	221	40185	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)(lync_online)	Web	TCP	172.170.10.135	59277	Local	VirtualInterface-1	Default_LAN_Zone	13.107.3.128	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	21	2330	0.286	0.254	22	13247	0.299	1.441	74	18063	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)(lync_online)	Web	TCP	172.170.10.135	62015	Local	VirtualInterface-1	Default_LAN_Zone	52.114.74.44	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	16	5435	0.307	0.835	11	9605	0.211	1.475	52	7322	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	Web	TCP	172.170.10.135	60309	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.168	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	56	8714	0.198	0.246	68	15272	0.240	0.432	283	31023	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	Web	TCP	172.170.10.135	60298	Local	VirtualInterface-1	Default_LAN_Zone	13.107.136.9	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	630	250709	2.116	6.735	700	386271	2.351	10.377	298	20487	[Src Filter][Pre-Route NAT][Dst Filter]

- Fluye

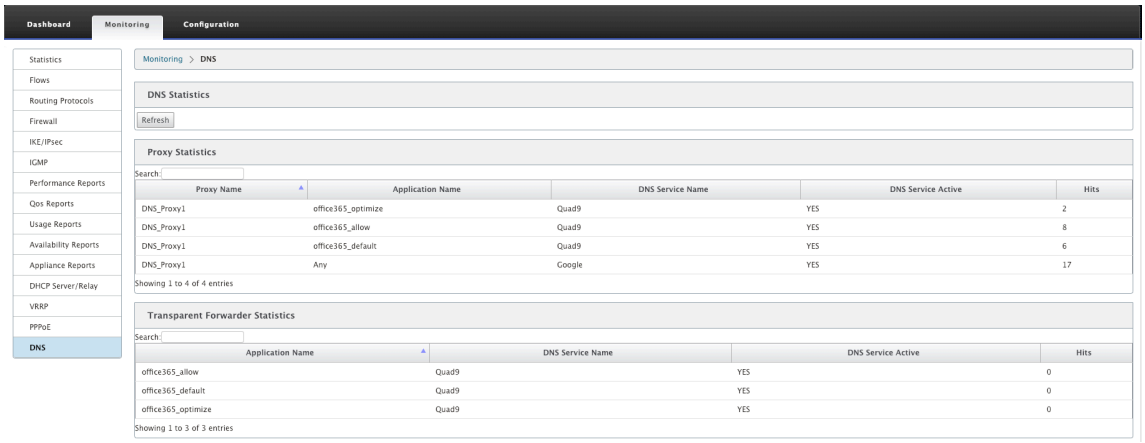


Flows Data

LAN to WAN Flows

Details	Routing Domain	Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Hit Count	Service Type	Service Name	Age (mS)	Packets	Bytes	PPS	Application ▲
⊞	Optimize	172.147.100.146	52.98.65.178	57930	443	TCP	4	INTERNET	-	120979	3	156	0.000	outlook
⊞	Optimize	172.147.100.146	13.107.18.11	57931	443	TCP	15	INTERNET	-	26513	14	1683	0.018	outlook
⊞	Optimize	172.147.100.146	13.107.42.11	57891	443	TCP	20	INTERNET	-	8418	19	1903	0.036	outlook
⊞	Optimize	172.147.100.146	40.100.136.146	57926	443	TCP	14	INTERNET	-	730	13	2118	0.036	outlook
⊞	Optimize	172.147.100.146	40.97.229.82	57918	443	TCP	15	INTERNET	-	1229	14	2178	0.036	outlook
⊞	Optimize	172.147.100.146	52.98.65.178	57929	443	TCP	4	INTERNET	-	121224	3	156	0.000	outlook
⊞	Optimize	172.147.100.146	34.203.255.247	51236	443	TCP	5	INTERNET	-	599759	4	164	0.000	okta
⊞	Optimize	172.147.100.146	34.203.255.247	51237	443	TCP	4	INTERNET	-	592420	3	123	0.000	okta
⊞	Optimize	172.147.100.146	13.107.6.156	51298	443	TCP	29	INTERNET	-	42061	28	11416	0.018	office365_common
⊞	Optimize	172.147.100.146	20.190.140.51	57935	443	TCP	16	INTERNET	-	24735	15	4184	0.018	office365_common
⊞	Optimize	172.147.100.146	13.67.50.225	57897	443	TCP	3	INTERNET	-	2250	2	81	0.047	office365_common
⊞	Optimize	172.147.100.146	13.67.50.225	51228	443	TCP	4	INTERNET	-	603355	3	123	0.000	office365_common
⊞	Optimize	172.147.100.146	13.107.6.156	51255	443	TCP	249	INTERNET	-	377061	248	85307	0.000	office365_common
⊞	Optimize	172.147.100.146	52.109.124.84	57939	443	TCP	20	INTERNET	-	22933	19	4679	0.018	office365_common
⊞	Optimize	172.147.100.146	13.67.50.225	51346	443	TCP	3	INTERNET	-	5900	2	81	0.044	office365_common

- Estadísticas DNS



Dashboard | Monitoring | Configuration

Statistics
Flows
Routing Protocols
Firewall
IKE/IPsec
ICMP
Performance Reports
Qos Reports
Usage Reports
Availability Reports
Appliance Reports
DHCP Server/Relay
VRRP
PPPoE
DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
DNS_Proxy1	office365_optimize	Quad9	YES	2
DNS_Proxy1	office365_allow	Quad9	YES	8
DNS_Proxy1	office365_default	Quad9	YES	6
DNS_Proxy1	Any	Google	YES	17

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

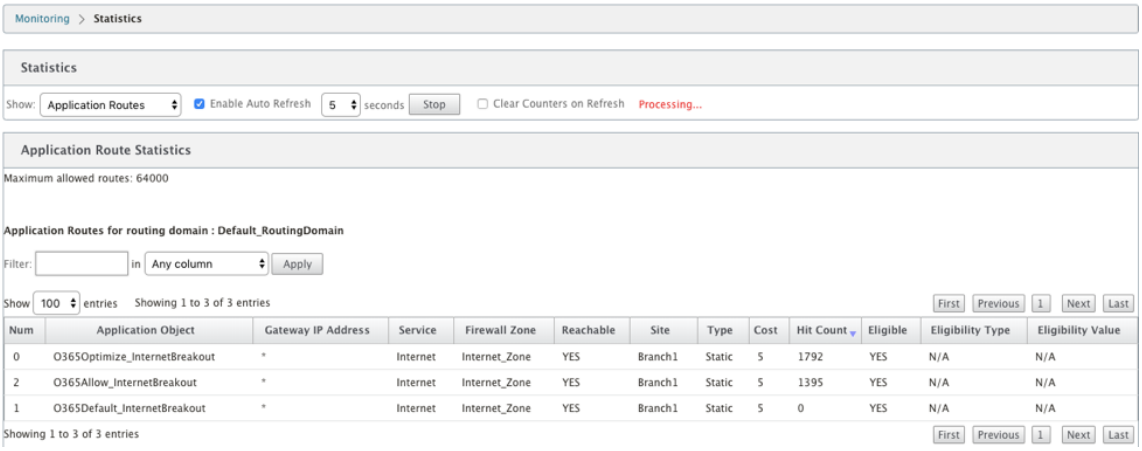
Search:

Application Name	DNS Service Name	DNS Service Active	Hits
office365_allow	Quad9	YES	0
office365_default	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 3 of 3 entries

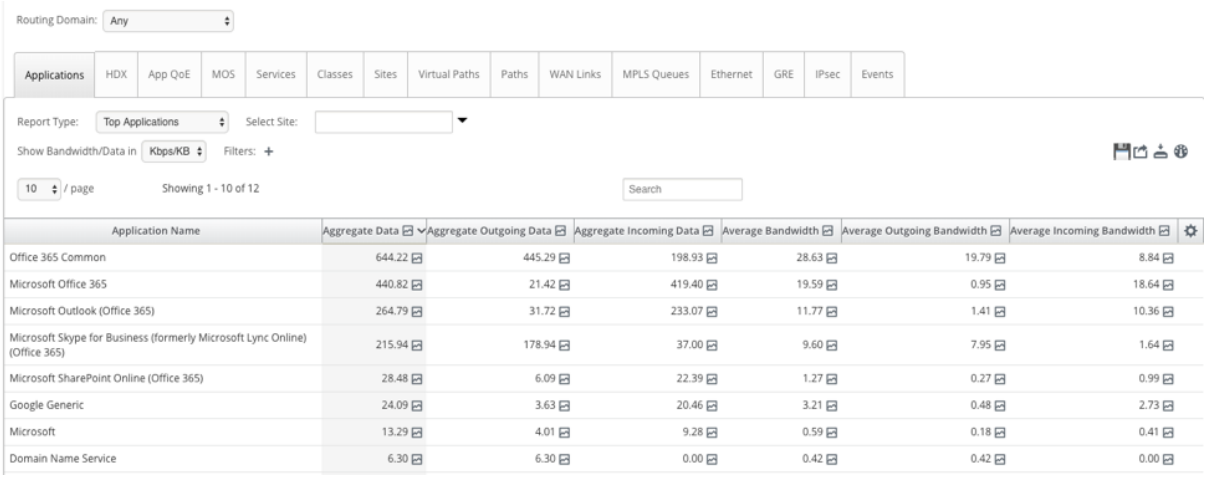
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Estadísticas de ruta de aplicación



Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1792	YES	N/A	N/A
2	O365Allow_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1395	YES	N/A	N/A
1	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

También puede ver las estadísticas de aplicaciones de Office 365 en el informe de aplicaciones de SD-WAN Center.



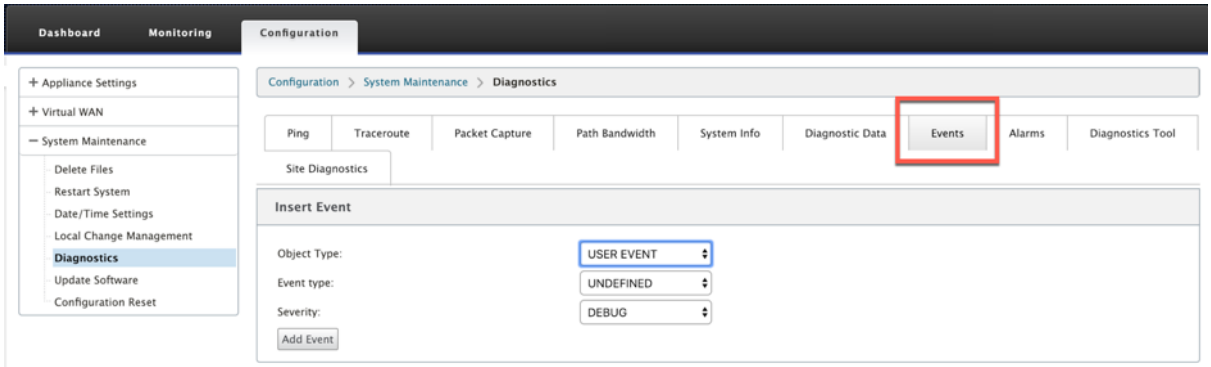
Application Name	Aggregate Data	Aggregate Outgoing Data	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth	Average Incoming Bandwidth
Office 365 Common	644.22	445.29	198.93	28.63	19.79	8.84
Microsoft Office 365	440.82	21.42	419.40	19.59	0.95	18.64
Microsoft Outlook (Office 365)	264.79	31.72	233.07	11.77	1.41	10.36
Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)	215.94	178.94	37.00	9.60	7.95	1.64
Microsoft SharePoint Online (Office 365)	28.48	6.09	22.39	1.27	0.27	0.99
Google Generic	24.09	3.63	20.46	3.21	0.48	2.73
Microsoft	13.29	4.01	9.28	0.59	0.18	0.41
Domain Name Service	6.30	6.30	0.00	0.42	0.42	0.00

Solucionar problemas

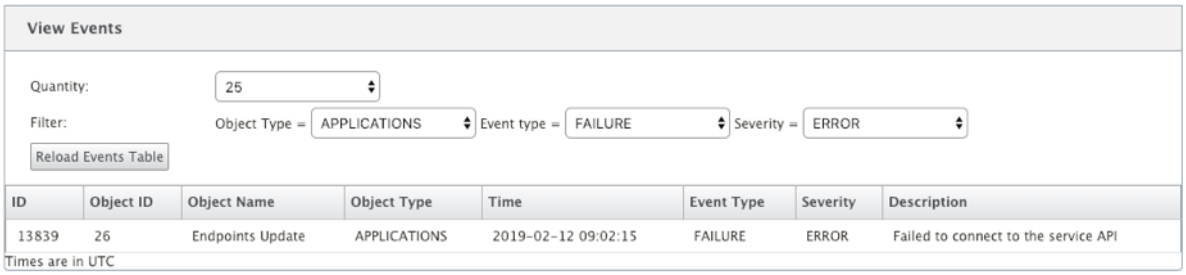
Puede ver el error de servicio en la sección **Eventos** del dispositivo SD-WAN.

Para comprobar los errores, vaya a **Configuración > Mantenimiento del sistema > Diagnósticos**, haga clic en la ficha **Eventos**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

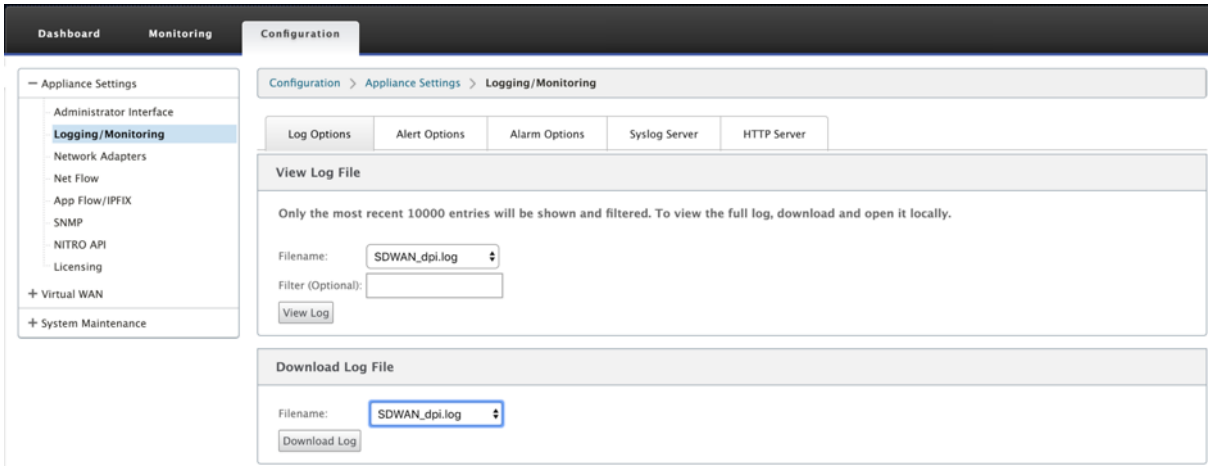


Si hay un problema al conectarse al servicio Citrix (sdwan-app-routing.citrixnetworkapi.net), el mensaje de error se refleja en la tabla **Ver eventos**.



Los errores de conectividad también se registran en **SDWAN_DPI.log**. Para ver el registro, vaya a **Configuración > Configuración del equipo > Registro/ Supervisión > Opciones de registro**. Seleccione **SDWAN_DPI.log** en la lista implementable 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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Limitaciones

- Si se configura la directiva de grupo de Office 365, no se realiza una inspección profunda de paquetes en 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.

Sesiones PPPoE

May 7, 2021

El protocolo punto a punto sobre Ethernet (PPPoE) conecta varios usuarios de equipos en una red de área local 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 conexiones de acceso telefónico, con el protocolo Ethernet, que admite varios usuarios en una red de área local. 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 aprender las direcciones de red de cada uno a través de un intercambio inicial llamado descubrimiento. Después de establecer una sesión entre un usuario individual y el sitio remoto, por ejemplo, un proveedor de ISP, se puede supervisar la sesión. Las empresas utilizan acceso compartido a Internet 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 la dirección IP estática para establecer conexiones PPPoE.

Se requiere lo siguiente para establecer sesiones PPPoE exitosas:

- Configurar la interfaz de red virtual (VNI).
- Credenciales únicas para crear sesión PPPoE.
- Configure el enlace WAN. Cada VNI puede tener configurado un enlace WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 un 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 VNIs configurados.
- Cree varios VNIs para admitir varias sesiones PPPoE por grupo de interfaz.

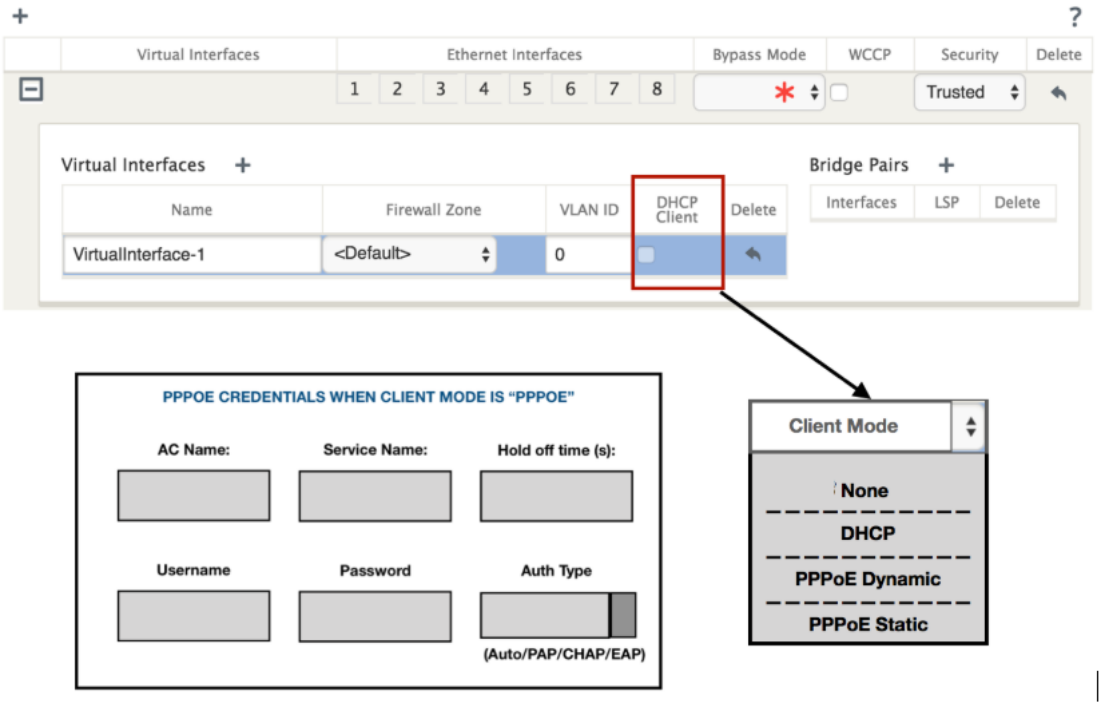
> **Nota**:
>
> Se permite crear varias VNIs con la misma etiqueta VLAN 802.1Q.

Limitaciones para la configuración PPPoE:

- No se admite el etiquetado VLAN 802.1q.
- No se admite la autenticación EAP-TLS.
- Compresión de dirección/control.
- Desinflar compresión.
- Negociación de compresión de campo de protocolo.
- Protocolo de control de compresión.
- Compresión de compresión BSD.
- Protocolos IPv6 e IPX.
- PPP Multi Vínculo.
- Compresión de encabezado TCP/IP estilo Van Jacobson.
- Opción de compresión de ID de conexión en la compresión de encabezado TCP/IP estilo Van Jacobson.
- PPPoE no es compatible con interfaces LTE

Para facilitar la configuración PPPoE, la opción **Cliente DHCP** se sustituye por una nueva opción denominada **Modo cliente** en la interfaz de administración web SD-WAN en Configuración de **sitios**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



En la siguiente tabla se describen las opciones de configuración PPPoE de modo cliente disponibles en un dispositivo MCN y SD-WAN de sucursal, respectivamente.

MCN

- Ninguno
- PPPoE estático

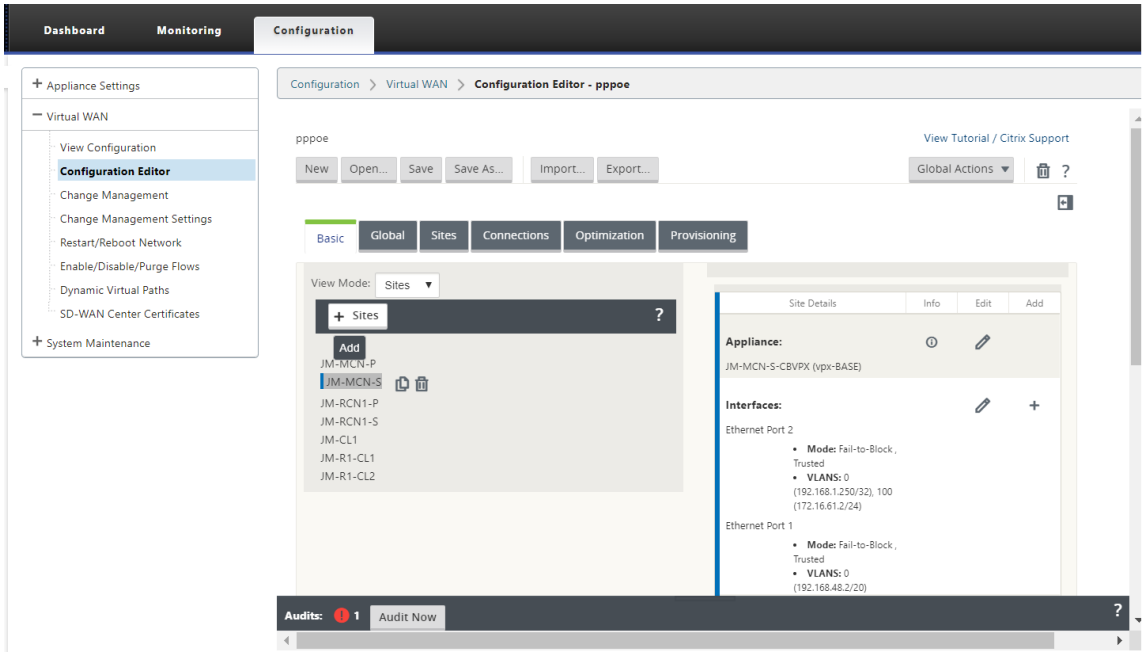
Sucursal

- Ninguno
- PPPoE estático
- PPPoE Dinámico
- DHCP

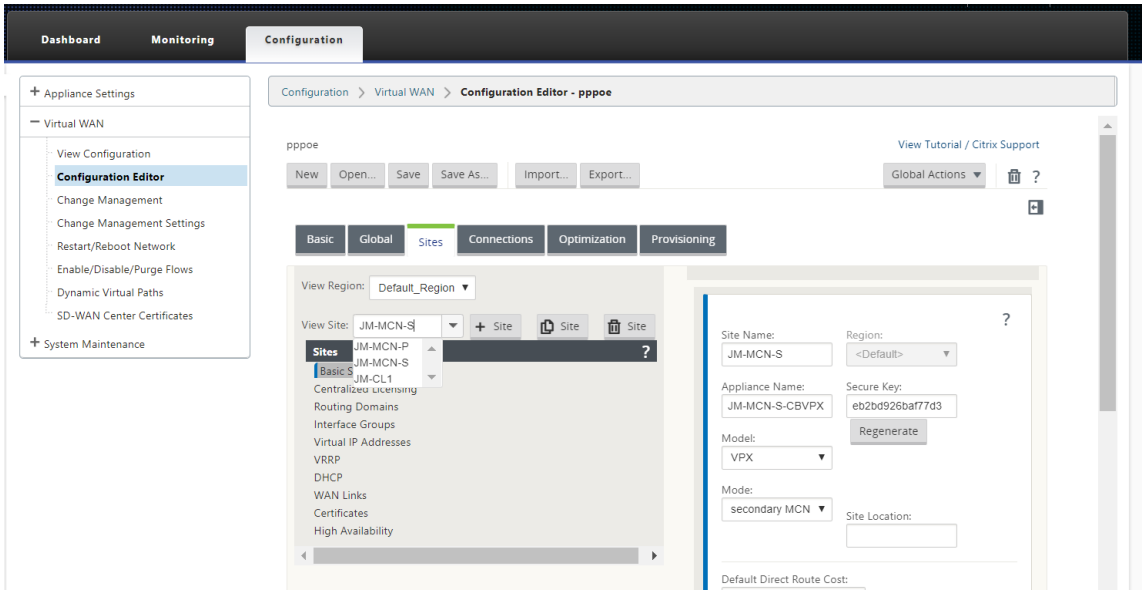
Configurar dispositivo MCN

1. En la GUI del dispositivo SD-WAN MCN, vaya a **configuración** > **WAN virtual** > **Editor de configuración**. Agregue sitio en la ficha **Básico**. Para obtener más información, consulte la configuración del nodo de rama en, configurar mcn.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Una vez creado el nuevo sitio, abra la ficha **Sitios**. Seleccione el sitio recién creado en la lista implementable **Ver sitio**.



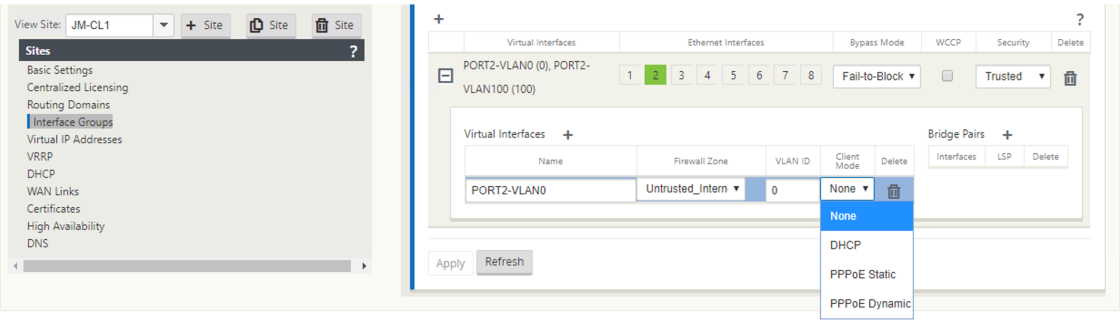
3. Seleccione **Grupos de interfaz** para el sitio de MCN. Haga lo siguiente:

   - Agregar interfaces virtuales.
   - Configurar interfaces Ethernet.
   - Configurar el modo de omisión.
   - Elija **WCCP**, si es necesario.
   - Elija Seguridad: Confiada/No de confianza.

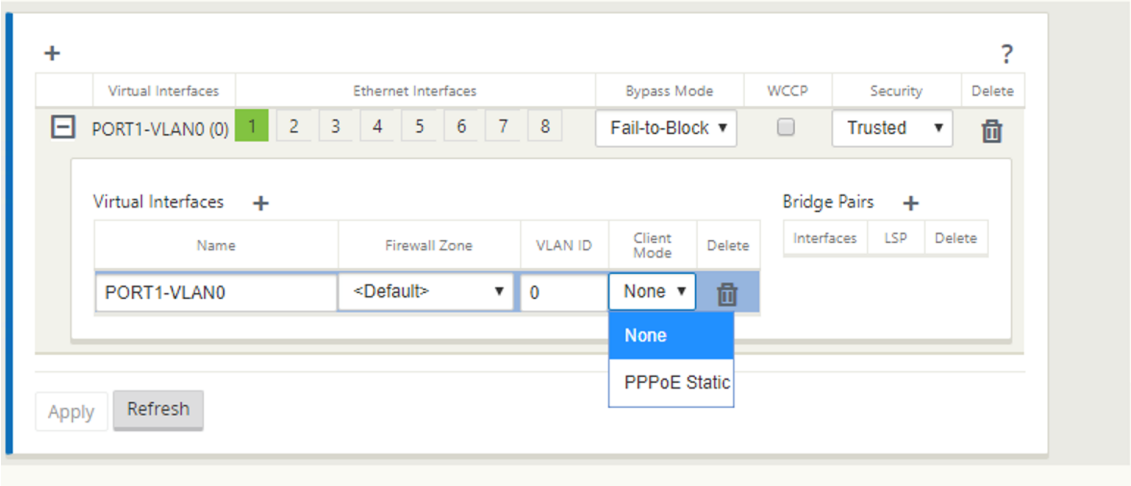
   Para interfaz virtual:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configure el nombre, la zona del firewall, el ID de VALN y el modo cliente.
- Un VNI configurado con múltiples interfaces puede tener una interfaz utilizada para la conectividad PPPoE.
- Si un VNI configurado con múltiples interfaces y una conectividad PPPoE se cambia a una interfaz diferente, entonces la página del monitor se puede utilizar para detener la sesión existente e iniciar una nueva sesión, entonces se puede establecer una nueva sesión a través de la nueva interfaz.



4. Seleccione **PPPoE Static o Ninguno** según los requisitos de configuración de red para la opción Modo cliente del dispositivo MCN. Se muestran las siguientes opciones adicionales.



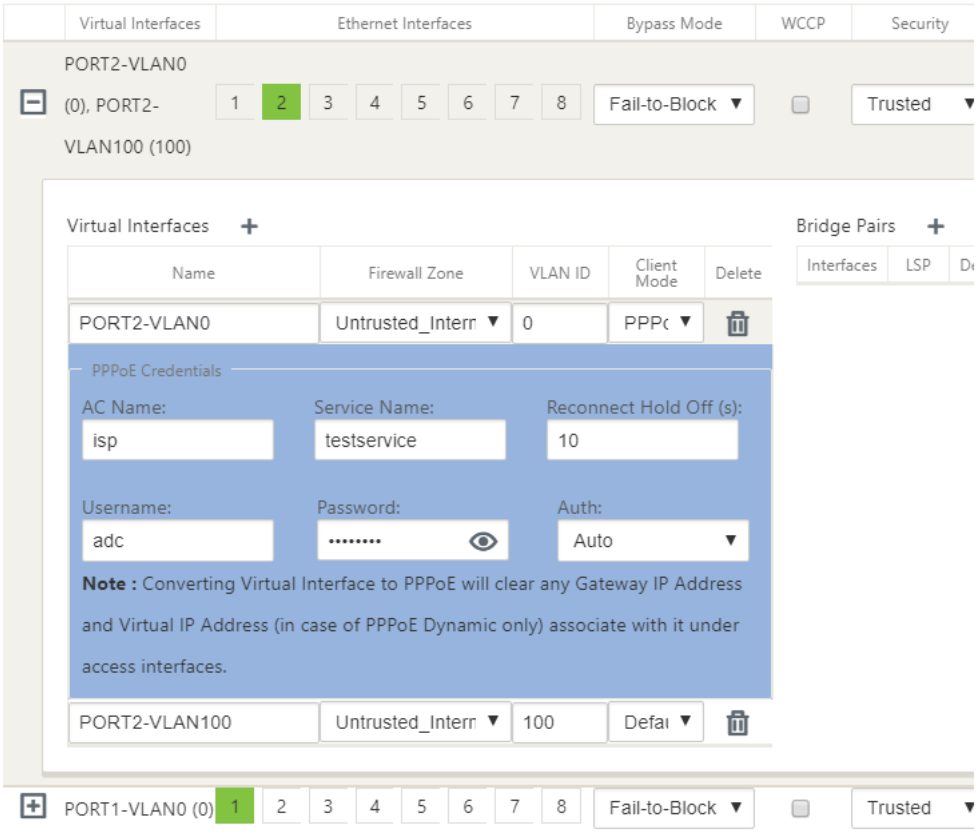
Configure los siguientes parámetros PPPoE y haga clic en **Aplicar**.

- Campo Nombre del concentrador de acceso (AC).
- Nombre del servicio.
- Tiempo de reconexión de retención (el valor predeterminado es volver a conectarse inmediatamente, ‘0’)
- Tipo de autenticación - (AUTO/PAP/CHAP/EAP).
  - Cuando la opción Auth está establecida en Auto, el dispositivo SD-WAN respeta la solicitud de protocolo de autenticación admitida recibida del servidor.

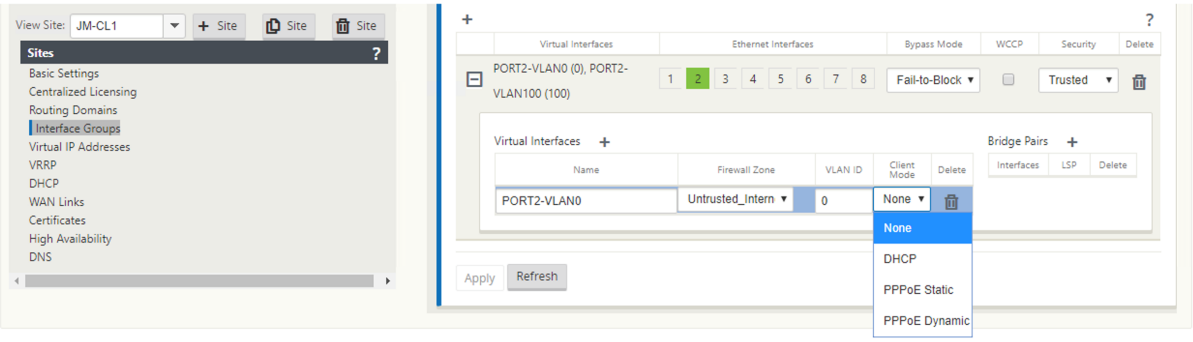
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Cuando la opción Auth se establece en PAP/CHAP/EAP, solo se respetan los protocolos de autenticación específicos. Si PAP está en la configuración y el servidor envía una solicitud de autenticación con CHAP, se rechaza la solicitud de conexión. Si el servidor no negocia con PAP, se produce un error de autenticación.

- CHAP incluye: CHAP, CHAP de Microsoft y CHAPv2.
- EAP admite EAP-MD5.
- Nombre de usuario y contraseña.



En la siguiente figura se muestran las opciones de modo cliente PPPoE para un dispositivo SD-WAN de sucursal. Si PPPoE Dynamic está seleccionado, se requiere que el VNI sea “Untrusted.”

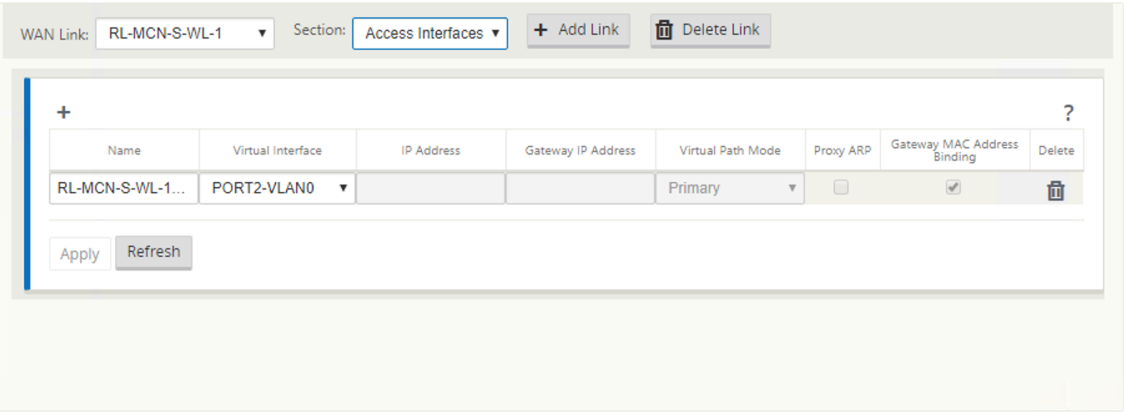


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

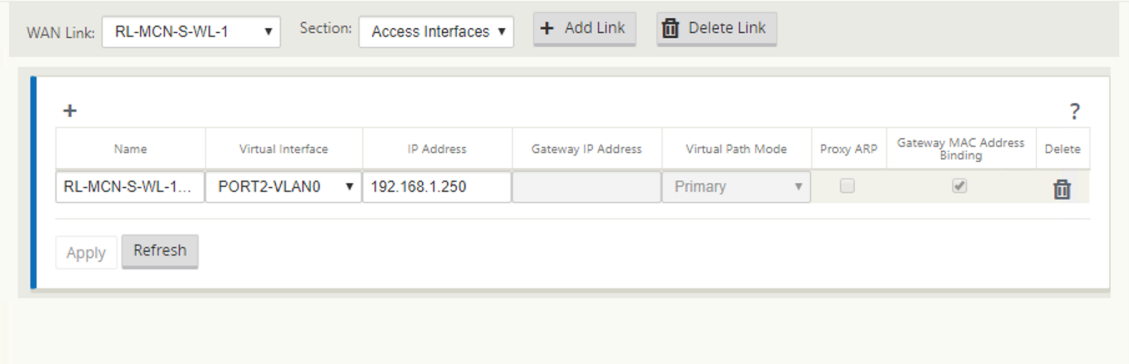
Configurar enlaces WAN

1. En la GUI de SD-WAN, vaya a **Sitios > Enlaces WAN**. Solo se permite la creación de un enlace WAN por VNI estático o dinámico PPPoE. La configuración del enlace WAN varía en función de la selección de VNI del modo cliente.
2. Si el VNI está configurado con el modo de cliente dinámico PPPoE:
   - Los campos Dirección IP y Dirección IP de puerta de enlace se vuelven inactivos.
   - El modo de ruta virtual se establece en "Principal."
   - No se puede configurar el ARP de proxy.

   De forma predeterminada, se selecciona Enlace de dirección MAC de puerta de enlace.



3. Si el VNI está configurado con el modo de cliente estático PPPoE, configure la dirección IP.



> **Nota**:
>
> Si el servidor no respeta la dirección IP estática configurada y ofrece una dirección IP diferente, se produce un error. La sesión PPPoE intenta restablecer la conexión periódicamente, hasta que el servidor acepte la dirección IP configurada.

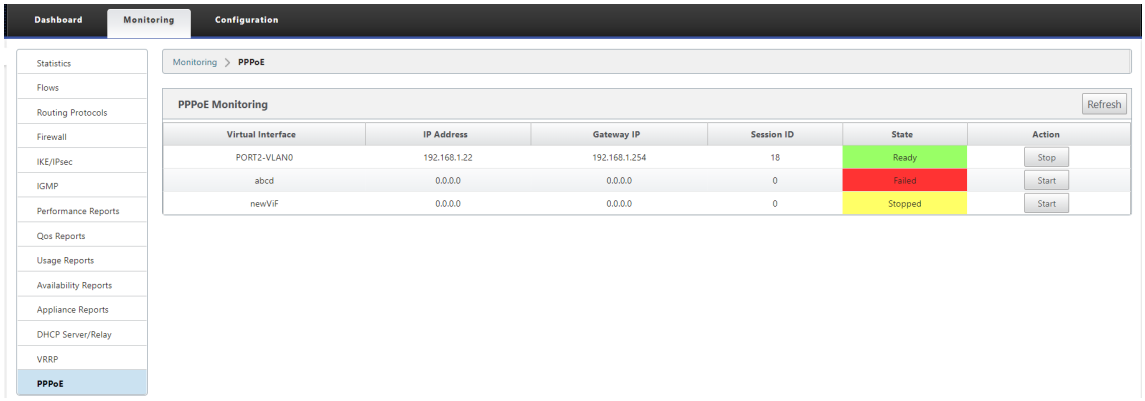
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Supervisar sesiones PPPoE

Puede supervisar sesiones PPPoE navegando a la página **Supervisión > PPPoE** en la GUI de SD-WAN.

La página PPPoE proporciona información de estado de los VNIs configurados con el modo cliente estático o dinámico PPPoE. Le permite iniciar o detener manualmente las sesiones para solucionar problemas.

- Si el VNI está activo y listo, las columnas **IP y IP de puerta** de enlace muestran los valores actuales en la sesión. Indica que estos son valores recibidos recientemente.
- Si el VNI está detenido o está en estado fallido, los valores son los últimos valores recibidos.
- Al pasar el ratón sobre la columna IP de la puerta de enlace se muestra la dirección MAC del concentrador de acceso PPPoE desde donde se recibe la sesión y la IP.
- Al pasar el ratón sobre el valor "state"se muestra un mensaje, que es más útil para un estado "Failed".



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 cursor sobre los estados para obtener descripciones.

Tipo de sesión PPPoE	Color	Descripción
Configurado	Amarillo	Un VNI está configurado con PPPoE. Este es un estado inicial.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tipo de sesión PPPoE	Color	Descripción
Marcando	Amarillo	Después de configurar un VNI, el estado de sesión PPPoE pasa al estado de marcado iniciando el descubrimiento PPPoE. Se captura la información del paquete.
Sesión	Amarillo	VNI se mueve del estado de descubrimiento al estado de sesión. esperando a recibir IP, si es dinámico o esperando confirmación del servidor para la IP anunciada, si es estática.
Listo	verde	Se reciben paquetes IP y VNI y el enlace WAN asociado están listos para su uso.
Fallo	rojo	La sesión PPP/PPPoE ha finalizado. El motivo de la falla puede deberse a una configuración no válida o a un error fatal. La sesión intenta volver a conectarse después de 30 segundos.
Detenido	amarillo	La sesión PPP/PPPoE se detiene manualmente.
Terminando	amarillo	Un estado intermedio que termina debido a una razón. Este estado se inicia automáticamente después de cierta duración (5 segundos para un error normal o 30 segundos para un error fatal).
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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Al pasar el ratón sobre el estado Fallido, se muestra el motivo del error reciente.
- Para establecer una nueva sesión o para solucionar problemas de una sesión PPPoE activa, utilice la página Monitoring->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 podría fallar debido a las siguientes razones:

- Cuando SD-WAN no puede autenticarse en el par debido a un nombre de usuario/contraseña incorrectos en la configuración.
- La negociación PPP falla: La negociación no llega al punto en el que se está ejecutando al menos un protocolo de red.
- Problema de memoria del sistema o recursos del sistema.
- Configuración invalida/incorrecta (nombre de CA o nombre de servicio incorrecto).
- Error al abrir el puerto serie debido a un error del sistema operativo.
- No se recibió respuesta para los paquetes de eco (el enlace es incorrecto o el servidor no responde).
- Hubo varias sesiones de marcado sin éxito continuas con en un minuto.

Después de 10 fallas consecutivas, se observa la razón de la falla.

- Si el fallo es normal, se reinicia inmediatamente.
- Si el error es un error, reinicie la operación durante 10 segundos.
- Si el error es fatal, el reinicio se reinicia durante 30 segundos antes de reiniciar.

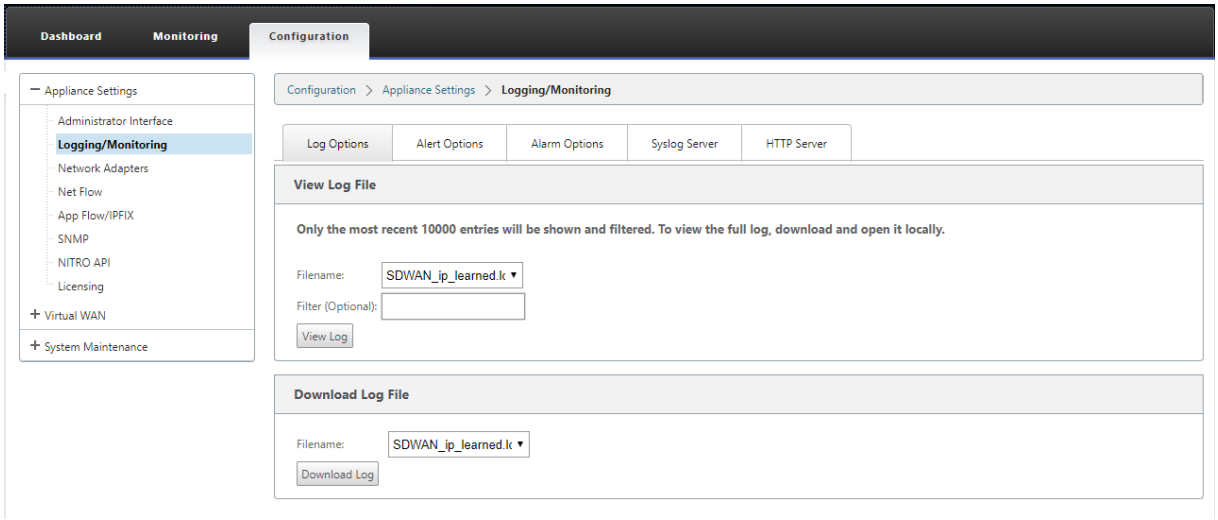
Los paquetes de solicitud de LCP Echo se generan desde SD-WAN por cada 60 segundos y la falta de recepción de 5 respuestas de eco se considera un error de enlace y restablece la sesión.

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 equipo** > **Logging/Monitoring** > **Opciones de registro**. Vea o descargue el archivo *SDWAN_IP_Learned.log*.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Calidad del servicio

May 7, 2021

La red entre las oficinas y el centro de datos o la nube debe transportar una multitud de aplicaciones y datos, incluyendo 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 retardo, la fluctuación, 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 prioriza las aplicaciones críticas. También comprende los requisitos para la calidad de la red WAN y elige 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.

Clases

October 27, 2021

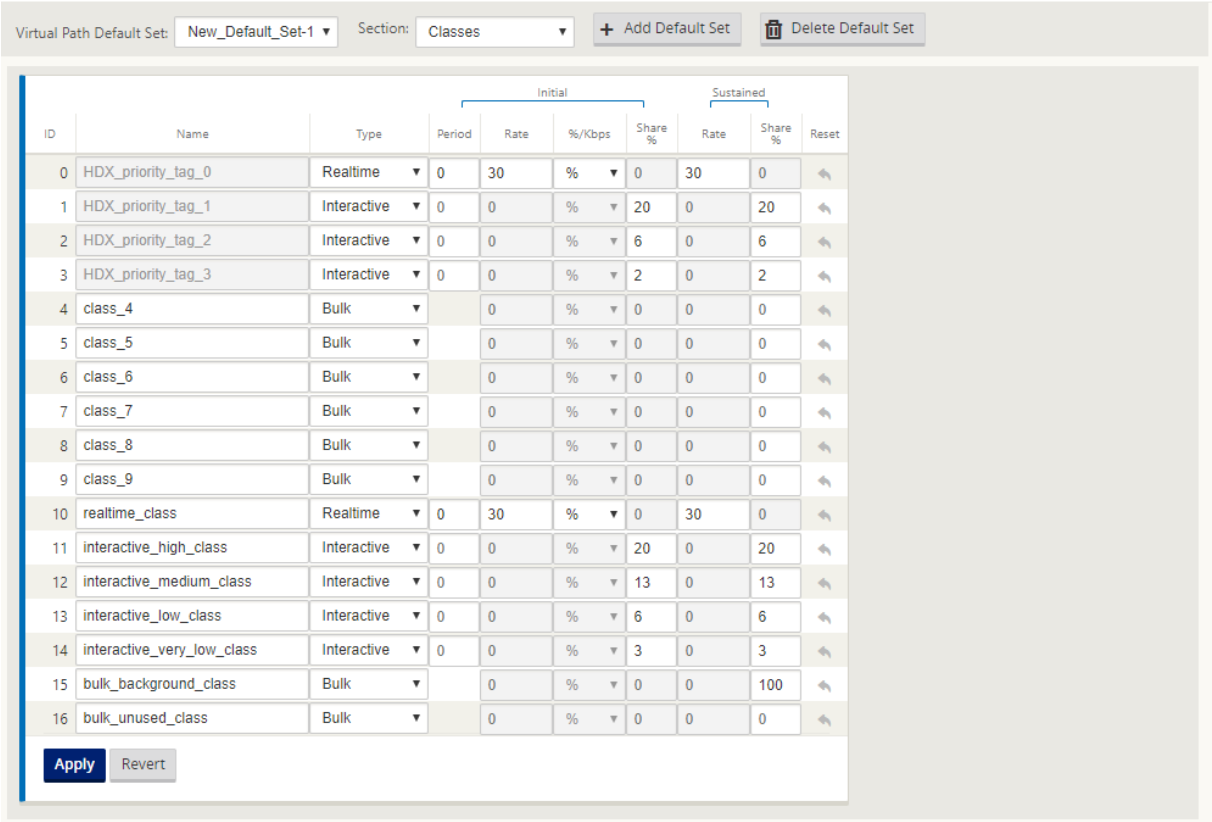
La configuración de Citrix SD-WAN proporciona un conjunto predeterminado de directivas de QoS basadas en aplicaciones e IP/puertos que se aplican a todo el tráfico que pasa por Rutas virtuales. Esta configuración se puede personalizar para adaptarse a las necesidades de implementación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Para obtener más información sobre QoS de la aplicación y QoS basada en direcciones IP/puertos, consulte Reglas por nombre de aplicación y Reglas por dirección IP y número de puerto, respectivamente.

El SD-WAN proporciona 17 clases (ID: 0—16). A continuación se presenta la configuración predeterminada de todas las 17 clases.



ID	Name	Type	Initial Period	Initial Rate	Initial %/Kbps	Initial Share %	Sustained Rate	Sustained Share %	Reset
0	HDX_priority_tag_0	Realtime	0	30	%	0	30	0	
1	HDX_priority_tag_1	Interactive	0	0	%	20	0	20	
2	HDX_priority_tag_2	Interactive	0	0	%	6	0	6	
3	HDX_priority_tag_3	Interactive	0	0	%	2	0	2	
4	class_4	Bulk		0	%	0	0	0	
5	class_5	Bulk		0	%	0	0	0	
6	class_6	Bulk		0	%	0	0	0	
7	class_7	Bulk		0	%	0	0	0	
8	class_8	Bulk		0	%	0	0	0	
9	class_9	Bulk		0	%	0	0	0	
10	realtime_class	Realtime	0	30	%	0	30	0	
11	interactive_high_class	Interactive	0	0	%	20	0	20	
12	interactive_medium_class	Interactive	0	0	%	13	0	13	
13	interactive_low_class	Interactive	0	0	%	6	0	6	
14	interactive_very_low_class	Interactive	0	0	%	3	0	3	
15	bulk_background_class	Bulk		0	%	0	0	100	
16	bulk_unused_class	Bulk		0	%	0	0	0	

Los siguientes son los diferentes tipos de clases:

- En**tiempo real**: se utiliza para baja latencia, bajo ancho de banda, tráfico sensible al tiempo. 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 baja a media y requisitos de ancho de banda 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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%

El resultado de distribución de 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para personalizar las clases:

1. Si los conjuntos predeterminados de ruta virtual están en uso, las clases se pueden modificar en **Global > Conjuntos predeterminados de ruta virtual**.

   > **Nota**
   >
   > También puede modificar clases en el nivel de Ruta virtual (**Conexiones -> Rutas virtuales -> Clases**)

2. Haga clic en **Agregar conjunto predeterminado**, escriba un nombre para el conjunto predeterminado y haga clic en **Agregar**. En el campo **Sección**, seleccione **Clases**.
3. En el campo **Nombre**, deje el nombre predeterminado o escriba el nombre de su elección.
4. En el campo **Tipo**, seleccione el tipo de clase (en tiempo real, interactivo o masivo).
5. Para las clases en tiempo real, puede especificar los siguientes atributos:
   - **Período Inicial**: Período de tiempo en milisegundos para aplicar una velocidad inicial antes de cambiar a una velocidad sostenida.
   - **Tasa Inicial**: Tasa o porcentaje máximo con el que los paquetes salen de la cola durante el período inicial.
   - **Tasa sostenida**: tasa máxima o porcentaje al que los paquetes salen de la cola después del período inicial.
6. Para las clases interactivas, puede especificar los siguientes atributos:
   - **Periodo inicial**: Período de tiempo, en milisegundos, durante el cual se aplicará el porcentaje inicial del ancho de banda disponible antes de cambiar al porcentaje sostenido. Normalmente, 20 ms.
   - **% compartido inicial**: el porcentaje máximo de ancho de banda de ruta virtual restante después de servir en tiempo real durante el período inicial.
   - **Porcentaje compartido sostenido**: la cuota máxima de ancho de banda de ruta virtual que queda después de servir el tráfico en tiempo real después del período inicial.
7. Para las clases masivas, solo puede especificar el **porcentaje compartido sostenido**, que determina el ancho de banda de ruta virtual restante que se utilizará para una clase masiva después de servir tráfico interactivo e en tiempo real.
8. Haga clic en **Aplicar**.

> **Nota**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Guarde la configuración, exporte a la bandeja de entrada de administración de cambios e inicie el proceso de administración de cambios.

Reglas por dirección IP y número de puerto

May 7, 2021

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)».

Con el editor de configuración, puede crear reglas para el flujo de tráfico y asociar las reglas con aplicaciones y clases. Puede especificar criterios para filtrar el tráfico de un flujo y aplicar el comportamiento general, el comportamiento de LAN a WAN, el comportamiento de WAN a LAN y las reglas de inspección de paquetes.

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.

Crear reglas por dirección IP y número de puerto

1. En el Editor de configuración de SD-WAN, vaya a **Global** > **Conjuntos predeterminados de rutas virtuales.**

   > **Nota**
   >
   > Puede crear reglas a nivel de sitio navegando a **Sitios > Conexiones > Rutas virtuales > Reglas**.

2. Haga clic en **Agregar conjunto predeterminado**, escriba un nombre para el conjunto predeterminado y haga clic en **Agregar**. En el campo Sección, seleccione **Reglas** y haga clic en **+**.
3. En el campo **Orden**, introduzca el valor de orden que se va a definir cuando se aplica la regla en relación con otras reglas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. En el campo **Nombre de grupo de reglas**, seleccione un grupo de reglas. Las estadísticas de las reglas con el mismo grupo de reglas se agruparán y se pueden ver juntas.

   Para ver grupos de reglas, vaya a**Supervisión > Estadísticas**y, en el campo **Mostrar**, seleccione**Grupos de reglas**.

   También puede agregar aplicaciones personalizadas. Para obtener más información, consulte Agregar grupos de reglas y habilitar MOS.

5. En el campo **Dominio de enrutamiento**, elija uno de los dominios de enrutamiento configurados.

6. Puede definir criterios de coincidencia de reglas para filtrar servicios en función de los parámetros que se enumeran a continuación. Después del filtrado, la configuración de regla se aplica a los servicios que coinciden con estos criterios.

   - **Dirección IP de origen**: Dirección IP de origen y la máscara de subred para que coincidan con el tráfico.
   - **Dirección IP de destino**: Dirección IP de destino y la máscara de subred que coinciden con el tráfico.

     > **Nota**
     >
     > Si la casilla **Dest=Src** está activada, la dirección IP de origen también se utilizará para la dirección IP de destino.

   - **Protocolo**: Protocolo para que coincida con el tráfico.
   - **Puerto de origen**: Número de puerto de origen o rango de puertos para que coincida con el tráfico.
   - **Puerto de destino**: Número de puerto de destino o intervalo de puertos para que coincida con el tráfico.

     > **Nota**
     >
     > Si la casilla **Dest=Src** está activada, el puerto de origen también se utilizará para el puerto de destino.

   - **DSCP**: La etiqueta **DSCP**en el encabezado IP para que coincida con el tráfico.
   - **VLAN**: **ID de VLAN**que debe coincidir con el tráfico.

7. Haga clic en el icono de agregar (+) situado junto a la nueva regla.

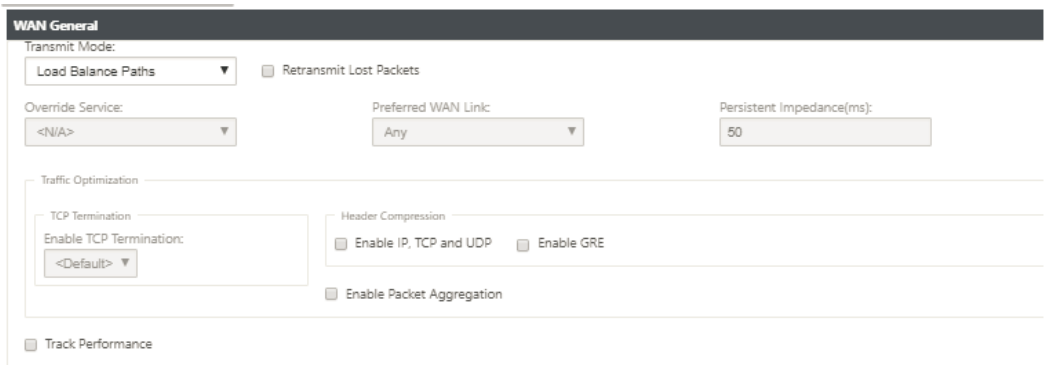
8. Haga clic en **Inicializar propiedades mediante protocolo** para inicializar las propiedades de la regla aplicando los valores predeterminados de la regla y la configuración recomendada para el protocolo. Esto rellena la configuración predeterminada de la regla. También puede personalizar la configuración manualmente, como se muestra en los pasos siguientes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. Haga clic en el icono **General de WAN** para configurar las siguientes propiedades.

   - **Modo de transmisión**: Seleccione uno de los siguientes modos de transmisión.
     - **Ruta de equilibrio de carga**: El tráfico para el flujo se equilibrará a través de múltiples rutas para el servicio. El tráfico se envía a través de la mejor ruta hasta que se utiliza esa ruta. Los paquetes sobrantes se envían a través de la siguiente mejor ruta.
     - **Ruta persistente**: El tráfico del flujo permanece en la misma ruta hasta que la ruta ya no está disponible.
     - **Ruta duplicada**: El tráfico del flujo se duplica a través de múltiples rutas, lo que aumenta la fiabilidad.
     - **Servicio de anulación**: El tráfico de las anulaciones de flujo a un servicio diferente. En el campo Sustituir servicio, seleccione el tipo de servicio al que sobrescribe el servicio. Por ejemplo, un servicio de ruta de acceso virtual puede anular a un servicio de intranet, Internet o de paso a través.
   - **Retransmitir paquetes perdidos**: Envíe el tráfico que coincida con esta regla al dispositivo remoto a través de un servicio fiable y retransmita los paquetes perdidos.
   - **Habilitar terminación TCP**: Habilitar la terminación TCP del tráfico para este flujo. El tiempo de ida y vuelta para el reconocimiento de paquetes se reduce y, por lo tanto, mejora el rendimiento.
   - **Enlace WAN preferido**: El enlace WAN que los flujos deben utilizar primero.
   - **Impedancia persistente**: tiempo mínimo en milisegundos para el que el tráfico permanecería en la misma ruta, hasta el tiempo de espera en el que la ruta es mayor que el valor configurado.
   - **Habilitar IP, TCP y UDP**: Comprime encabezados en paquetes IP, TCP y UDP.
   - **Habilitar GRE**: Comprimir encabezados en paquetes GRE.
   - **Habilitar agregación de paquetes**: Agregue paquetes pequeños en paquetes más grandes.
   - **Seguimiento de rendimiento**: registra los atributos de rendimiento de esta regla en una base de datos de sesión (por ejemplo, pérdida, fluctuación, latencia y ancho de banda).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

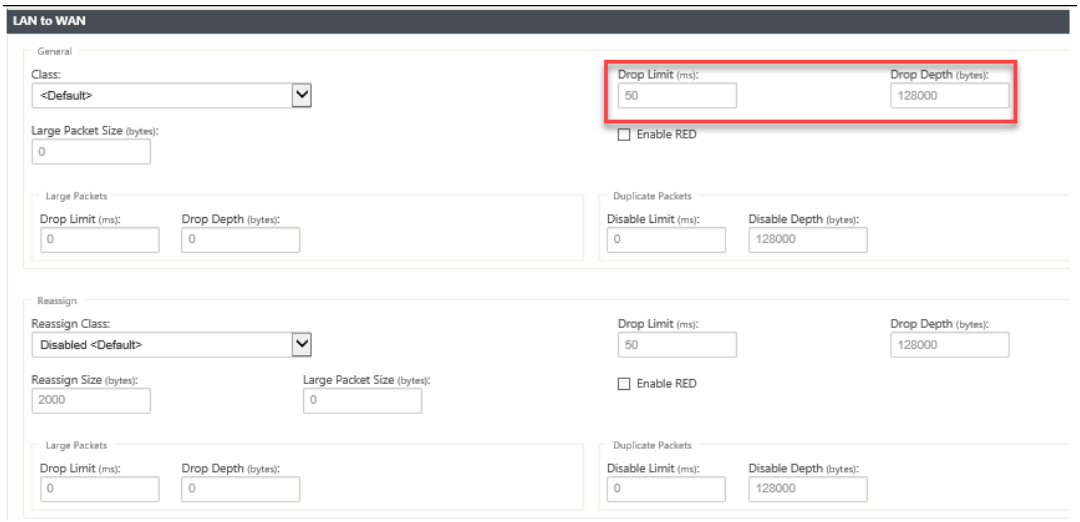


10. Haga clic en el icono **LAN a WAN** para configurar el comportamiento de LAN a WAN para esta regla.

    - **Clase**: Seleccione una clase con la que asociar esta regla.

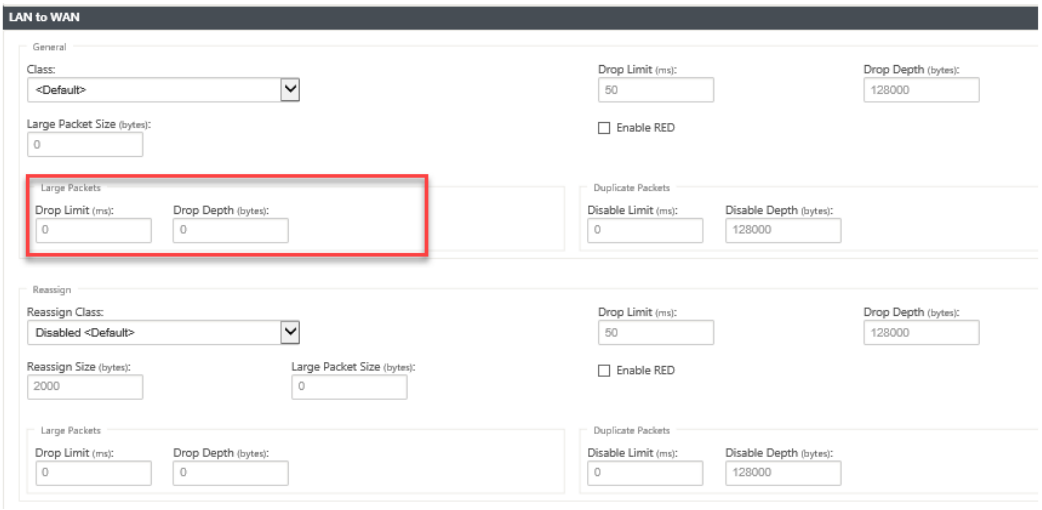
      > **Nota**
      >
      > También puede personalizar las clases antes de aplicar reglas. Para obtener más información, consulte Cómo personalizar clases.

    - **Tamaño de paquete grande**: A los paquetes más pequeños o iguales a este tamaño se les asignan los valores **Límite**de **caída y Profundidad**de caída especificados en los campos situados a la derecha del campo **Clase**.



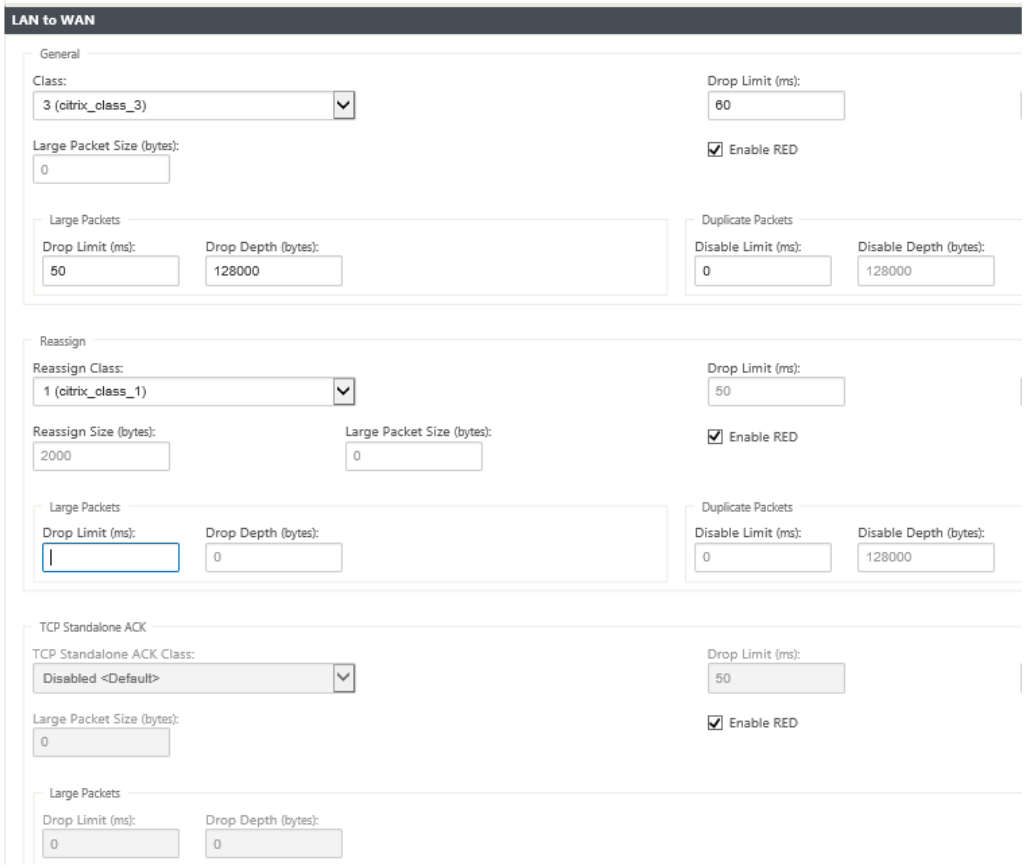
    A los paquetes mayores de este tamaño se les asignan los valores especificados en los campos**Límite de caíday Profundidad**de caída predeterminados en la sección**Paquetes grandes**de la pantalla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



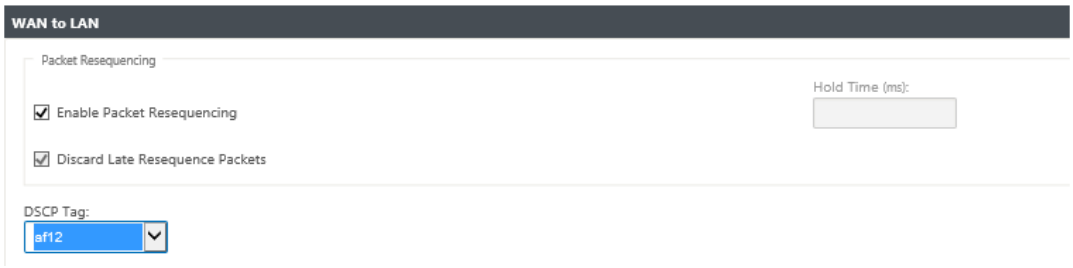
- **Límite de caída**: Tiempo después del cual se descartan los paquetes que esperan en el programador de clases. No aplicable a una clase a granel.
- **Profundidad de caída**: Umbral de profundidad de cola después del cual se descartan los paquetes.
- **Habilitar RED**: La detección temprana aleatoria (RED) garantiza un intercambio justo de los recursos de la clase descartando paquetes cuando se produce la congestión.
- **Tamaño de reasignación**: Longitud del paquete que, cuando se excede, hace que el paquete se reasigne a la clase especificada en el campo Reasignar Clase.
- **Reasignar Clase**: Clase utilizada cuando la longitud del paquete excede la longitud del paquete especificada en el campo Reasignar Tamaño.
- **Disable Limit**: Tiempo durante el cual se puede deshabilitar la duplicación para evitar que los paquetes duplicados consuman ancho de banda.
- **Inhabilitar profundidad**: Profundidad de cola del programador de clases, momento en el que no se generarán los paquetes duplicados.
- Clase**TCP Standalone ACK: Clase**de prioridad alta a la que se asignan las confirmaciones independientes de TCP durante las transferencias de archivos grandes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



11. Haga clic en el icono de **WAN a LAN** para configurar el comportamiento de WAN a LAN para esta regla.

    - **Habilitar la resecuenciación de paquetes**: Secuenciación de los paquetes en el orden correcto en el destino.
    - **Tiempo de espera**: Intervalo de tiempo para el que los paquetes se retienen para volver a secuenciar, después del cual los paquetes se envían a la LAN.
    - **Descartar paquetes de resecuenciación tardía**: Deseche los paquetes fuera de pedido que llegaron después de que los paquetes necesarios para la resecuenciación se hayan enviado a la LAN.
    - Etiqueta**DSCP: Etiqueta**DSCP aplicada a los paquetes que coinciden con esta regla, antes de enviarlos a la LAN.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

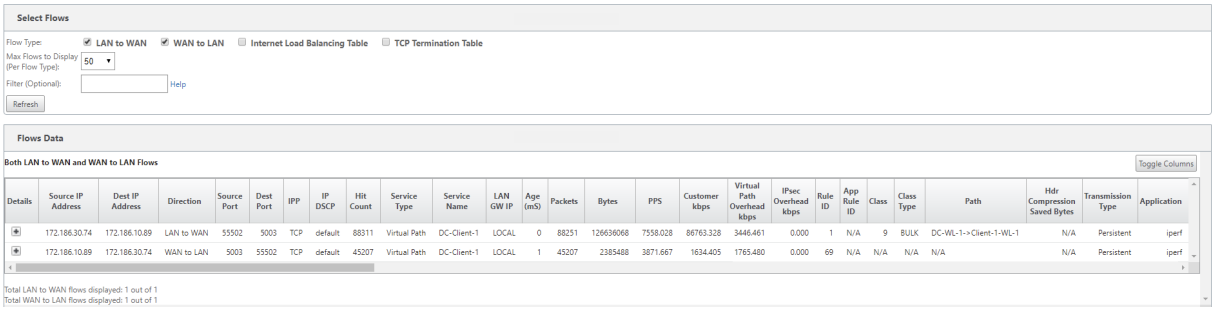
12. Haga clic en el icono **Inspección profunda de paquetes** y seleccione **Activar detección FTP pasiva** para permitir que la regla detecte el puerto utilizado para la transferencia de datos FTP y aplique automáticamente la configuración de regla al puerto detectado.
13. Haga clic en **Aplicar**.

> **Nota**
>
> Guarde la configuración, exporte a la bandeja de entrada de administración de cambios e inicie el proceso de administración de cambios.

Verificar reglas

En el Editor de configuración, 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 desea ver. Compruebe si la información de flujo se ajusta a las reglas configuradas.

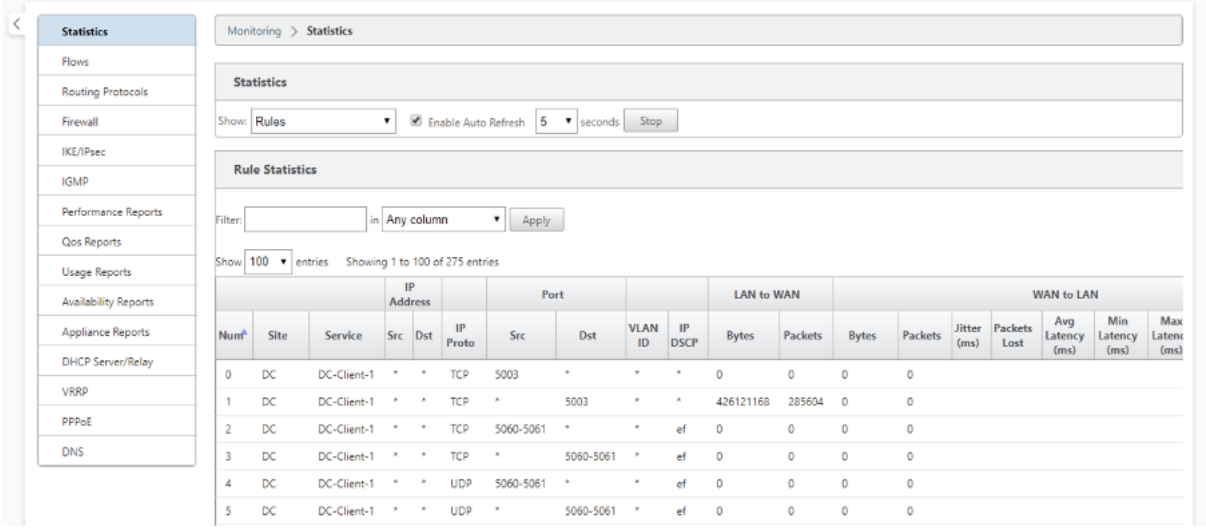
Ejemplo:
La regla «Si la dirección IP de origen es 172.186.30.74 y la dirección IP de destino es 172.186.10.89, establezca el **modo de transmisión** como Ruta persistente» muestra los siguientes **datos de flujos**.



Details	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	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
	172.186.30.74	172.186.10.89	LAN to WAN	55502	5003	TCP	default	88311	Virtual Path	DC-Client-1	LOCAL	0	88251	126636068	7558.028	86763.328	3446.461	0.000	1	N/A	9	BULK	DC-WL-1->Client-1-WL-1	N/A	Persistent	iperf
	172.186.10.89	172.186.30.74	WAN to LAN	5003	55502	TCP	default	45207	Virtual Path	DC-Client-1	LOCAL	1	45207	2385488	3871.667	1634.405	1765.480	0.000	69	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

En el Editor de configuración, vaya a **Supervisión > Estadísticas** y compruebe las reglas configuradas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Reglas por nombre de aplicación

May 7, 2021

La función de clasificación de aplicaciones permite al dispositivo Citrix SD-WAN analizar el tráfico entrante y clasificarlo como pertenecientes a una aplicación o familia de aplicaciones en particular. 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 en función de los tipos de coincidencias de aplicación, familia de aplicaciones o objeto 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 de IP, consulte Reglaspor 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 entre múltiples 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 de acceso persistente**: El tráfico de la aplicación permanece en la misma ruta hasta que la ruta de acceso ya no está disponible.
- **Ruta de acceso duplicada**: El tráfico de aplicaciones se duplica en múltiples paths, lo que aumenta la confiabilidad.

Las reglas de aplicación están asociadas a clases. Para obtener información sobre las clases, consulte Personalización de clases.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

De forma predeterminada, las siguientes cinco reglas de aplicación predefinidas están disponibles para las aplicaciones Citrix ICA:

Regla	Clase	Modo de transmisión	Retransmitir paquetes perdidos	Habilitar agregación de paquetes	Habilitar la resecuenciación de paquetes	Tiempo de retención de resecuencia (ms)	Descartar paquetes de resecuenciación tardía	Límite de caída (ms)	Profundidad de caída (bytes)	Activar RED	Límite de desactivación (ms)	Inhabilitar profundidad (bytes)
HDX_Priority_0	(HDX_priority_tag_0)	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_1	(HDX_priority_tag_1)	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_2	(HDX_priority_tag_2)	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Regla	Clase	Modo de transmisión	Retransmitir paquetes perdidos	Habilitar agregación de paquetes	Habilitar la resecuenciación de paquetes	Tiempo de retención de resecuencia (ms)	Descartar paquetes de resecuenciación tardía	Límite de caída (ms)	Profundidad de caída (bytes)	Activar RED	Límite de desactivación (ms)	Inhabilitar profundidad (bytes)
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 DPI. En este punto, los atributos de regla IP como Clase, terminación TCP se aplican a los paquetes. Después de la clasificación PPP, los atributos de regla de aplicación como Clase, modo de transmisión anulan los atributos de regla IP.

Las reglas IP tienen más atributos que las reglas de aplicación. La regla de aplicación anula unos pocos atributos de regla IP, el resto de los atributos de regla IP permanecen procesados en los paquetes.

Por ejemplo, considere 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.

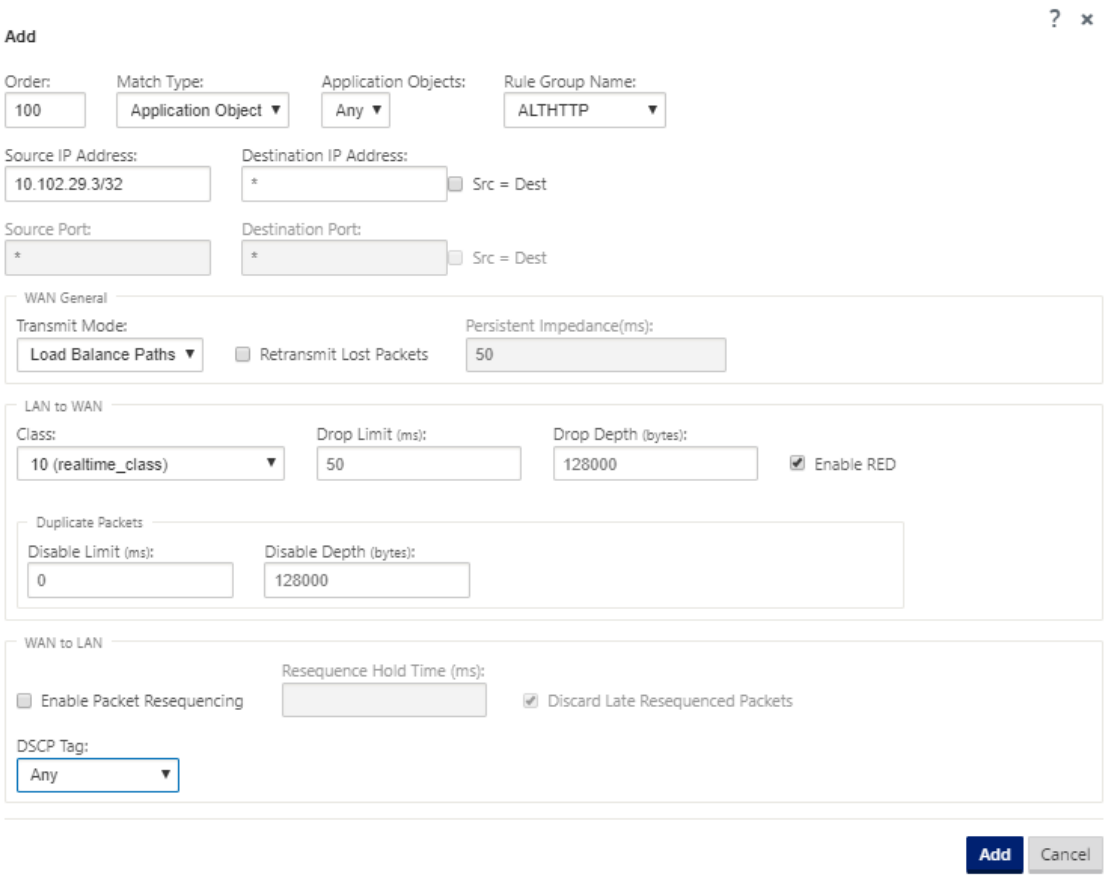
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Creación de reglas de aplicación

Para crear reglas de aplicación:

1. En el Editor de configuración de SD-WAN, vaya a **Global** > **Conjuntos predeterminados de rutas virtuales.**
2. Haga clic en **Agregar conjunto predeterminado**, escriba un nombre para el conjunto predeterminado y haga clic en **Agregar**. En el campo **Sección**, seleccione **QoS de aplicación** y haga clic en **+**.

> **Nota**
>
> También puede crear reglas de aplicación navegando a **Conexiones** > **Rutas virtuales** > **QoS de la aplicación** o **Global** > **Conjunto predeterminado de ruta virtual dinámica** > **QoS de la aplicación.**



3. En el campo **Orden**, escriba el valor de orden que se va a definir cuando se aplica la regla en relación con otras reglas.
4. En el campo **Tipo de coincidencia**, elija uno de los siguientes tipos de coincidencia:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Aplicación**: Si se selecciona este tipo de coincidencia, especifique la aplicación que se utiliza como criterio de coincidencia para este filtro.
- **Familia de aplicaciones**: Si se selecciona este tipo de coincidencia, seleccione una familia de aplicaciones que se utilice como criterio de coincidencia para este filtro.
- **Objeto de aplicación** : si se selecciona este tipo de coincidencia, seleccione un objeto de aplicación que se utilice como criterio de coincidencia para este filtro.

Para obtener más información sobre la aplicación, la familia de aplicaciones y el objeto de aplicación, consulte
Clasificación de aplicaciones.

5. En el campo **Nombre de grupo de reglas**, seleccione un grupo de reglas. Las estadísticas de las reglas con el mismo grupo de reglas se agruparán y se pueden ver juntas.

   Para ver grupos de reglas, vaya a **Supervisión** > **Estadísticas** y, en el campo **Mostrar**, seleccione **Grupos de reglas**.

   También puede agregar grupos de reglas personalizados. Para obtener más información, consulte Agregar aplicaciones personalizadas y habilitar MOS.

6. Especifique los siguientes criterios de coincidencia de reglas de aplicación para filtrar el tráfico de aplicaciones. Después del filtrado, la configuración de regla se aplica a los servicios que coinciden con estos criterios.

   - **Dirección IP de origen**: Dirección IP de origen y la máscara de subred para que coincidan con el tráfico.
   - **Dirección IP de destino**: Dirección IP de destino y la máscara de subred que coinciden con el tráfico.
   - **Puerto de origen**: Número de puerto de origen o rango de puertos para que coincida con el tráfico.
   - **Puerto de destino**: Número de puerto de destino o intervalo de puertos para que coincida con el tráfico.

   > **Nota**
   >
   > Elija **Src = Dest**, si la dirección de protocolo de Internet de origen y destino son la misma.

7. Configure las siguientes opciones generales de WAN:

   - En el campo **Modo de transmisión**, elija uno de los siguientes modos de transmisión:
     - **Ruta de equilibrio de carga**: El tráfico de aplicaciones para el flujo se equilibra entre múltiples rutas. El tráfico se envía a través de la mejor ruta hasta que esa ruta se utiliza completamente. Los paquetes restantes se envían a través de la siguiente mejor ruta.
     - **Ruta de acceso persistente**: El tráfico de la aplicación permanece en la misma ruta hasta que la ruta de acceso ya no está disponible.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En el campo **Impedancia persistente**, especifique el tiempo mínimo en milisegundos para el que el tráfico permanecería en la misma ruta, hasta que el tiempo de espera en la ruta sea mayor que el valor configurado.

  - **Ruta de acceso duplicada**: El tráfico de aplicaciones se duplica en múltiples paths, lo que aumenta la confiabilidad.

- Compruebe **Retransmitir paquetes perdidos** para enviar el tráfico que coincida con esta regla al dispositivo remoto a través de un servicio fiable y retransmitir los paquetes perdidos.

8. Configure la configuración de LAN a WAN:

   - **Clase**: Seleccione una clase con la que asociar esta regla.

     También puede personalizar las clases antes de aplicar reglas. Para obtener más información, consulte Personalizar clases.

   - **Límite de caída**: Tiempo después del cual se descartan los paquetes que esperan en el programador de clases. No aplicable a una clase a granel.
   - **Profundidad de caída**: Umbral de profundidad de cola después del cual se descartan los paquetes.
   - **Habilitar RED**: La detección temprana aleatoria (RED) garantiza un intercambio justo de los recursos de la clase descartando paquetes cuando se produce la congestión.
   - **Límite de desactivación:** Tiempo durante el cual se puede inhabilitar la duplicación para evitar que los paquetes duplicados consuman ancho de banda.
   - **Inhabilitar profundidad**: Profundidad de cola del programador de clases, momento en el que no se generarán los paquetes duplicados.

9. Configure el siguiente comportamiento de WAN a LAN para esta regla:

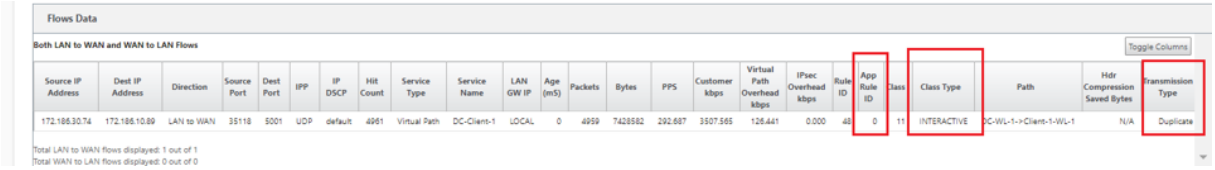
   - **Habilitar la resecuenciación de paquetes**: Secuenciación de los paquetes en el orden correcto en el destino.
   - **Tiempo de retención de resecuencia**: Intervalo de tiempo para el que se retienen los paquetes para la resecuenciación, después del cual los paquetes se envían a la LAN.
   - **Descartar paquetes de resecuenciación tardía**: Deseche los paquetes fuera de pedido que llegaron después de que los paquetes necesarios para la resecuenciación se hayan enviado a la LAN.

10. Haga clic en **Aplicar**.

Para confirmar si las reglas de aplicación se aplican al flujo de tráfico, vaya a **Supervisión** > **Flujos**.

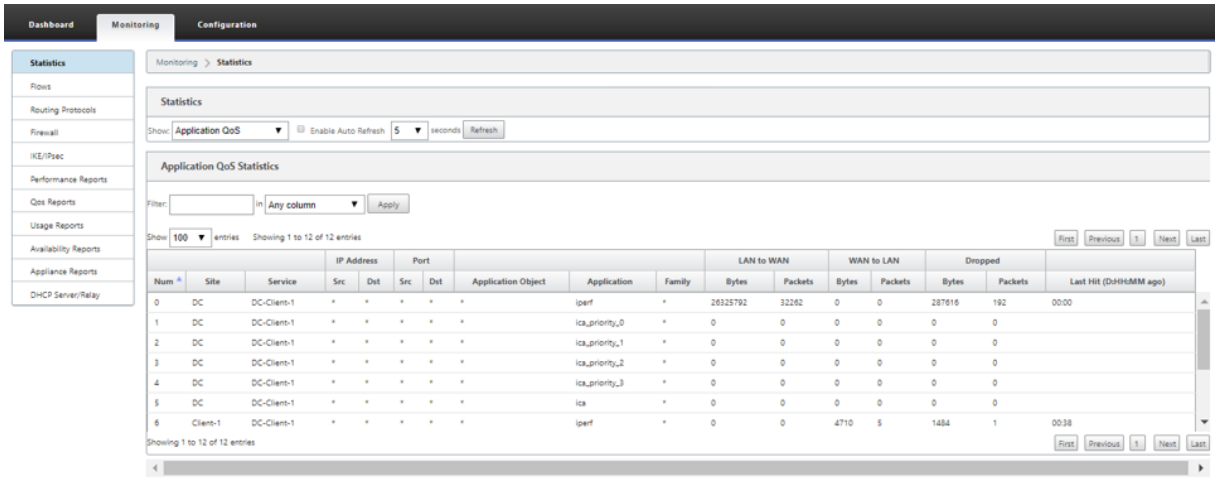
Anote el ID de la regla de la aplicación y compruebe si el tipo de clase y el modo de transmisión son según la configuración de la regla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Puede supervisar la QoS de la aplicación, como el número de paquetes/bytes cargados, descargados o descartados en cada sitio, navegando a **Monitoring** > **Statistics** > **Application QoS**.

El parámetro **Num** indica el ID de regla de aplicación. Compruebe el ID de regla de aplicación obtenido del flujo.



Creación de aplicaciones personalizadas

Puede utilizar objetos de aplicación para definir aplicaciones personalizadas basadas en los siguientes tipos de coincidencia:

- Protocolo IP
- Nombre de la aplicación
- Familia de aplicaciones

El clasificador DPI 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 enrutamiento de aplicaciones.

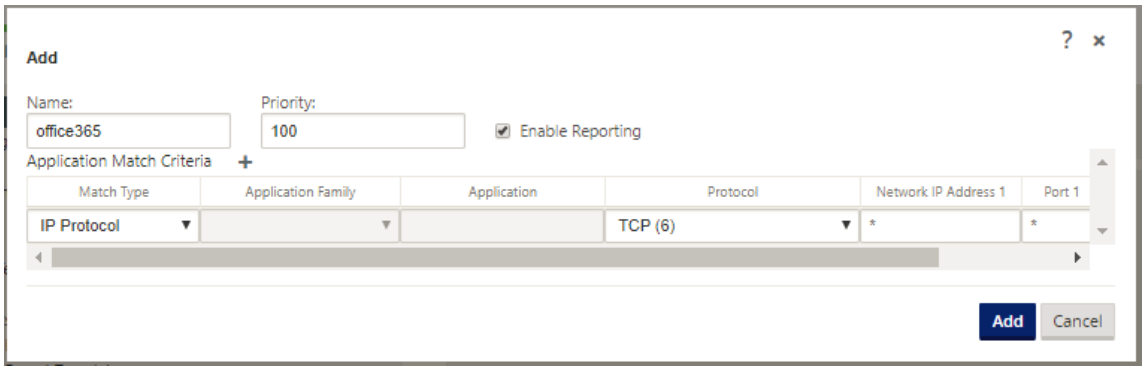
> **Sugerencia**
>
> Puede especificar uno o varios tipos de coincidencia.

Puede ver los informes de las aplicaciones personalizadas clasificadas en SD-WAN Center. Para obtener más información, consulte Informe de aplicación.

Para crear aplicaciones personalizadas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el Editor de configuración, vaya a **Global** > **Aplicaciones > Aplicacionespersonalizadas**y haga clic en**+**.



2. Defina los siguientes parámetros:

   - **Nombre:** Nombre de la aplicación personalizada
   - **Habilitar informes**: Permite ver informes de aplicaciones personalizadas en SD-WAN Center. Para obtener más información, consulte Informe de aplicación.
   - **Prioridad**: Prioridad de la aplicación personalizada. Cuando los paquetes entrantes coinciden con dos o más definiciones de aplicación personalizadas, se aplica la definición de aplicación personalizada con la prioridad más alta.

3. Haga clic en + en la sección **Criterios de coincidencia de aplicaciones**.

4. Seleccione uno de los siguientes tipos de coincidencia:

   - **Protocolo IP**: Especifique el protocolo, la dirección IP de red, el número de puerto y la etiqueta DSCP.
   - **Aplicación**: Especifique el nombre de la aplicación, la dirección IP de red, el número de puerto y la etiqueta DSCP.
   - **Familia de aplicaciones**: Seleccione una familia de aplicaciones y especifique la dirección IP de red, el número de puerto y la etiqueta DSCP.

5. Haga clic en **+** para agregar más criterios de coincidencia de aplicaciones.

6. Haga clic en **Aplicar**.

Agregar grupos de reglas y habilitar MOS

May 7, 2021

Una aplicación concreta en la red se puede definir mediante el grupo de reglas que se le aplica. El editor de configuración de SD-WAN proporciona una lista predeterminada de grupos de reglas. Tam-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

bién puede crear grupos de reglas personalizados y etiquetar reglas IP individuales o reglas QoS de aplicación a las aplicaciones.

Para obtener más información acerca de las reglas, consulteReglas por dirección IP y número de puertoyReglas por nombre de aplicación.

Las estadísticas de las reglas con el mismo grupo de reglas se agruparán y se pueden ver juntas.

Para ver estadísticas basadas en grupos de reglas, vaya a **Supervisión > Estadísticas**y, en el **campo Mostrar**, seleccione **Grupos de reglas**.

La puntuación media de opinión (MOS) es una medida numérica de la calidad de la experiencia que una aplicación entrega a los usuarios finales. Se utiliza principalmente para aplicaciones VoIP. En SD-WAN, MOS también se utiliza para evaluar la calidad de las aplicaciones que no son VoIP juzgando el tráfico como si se tratara de una llamada VoIP.

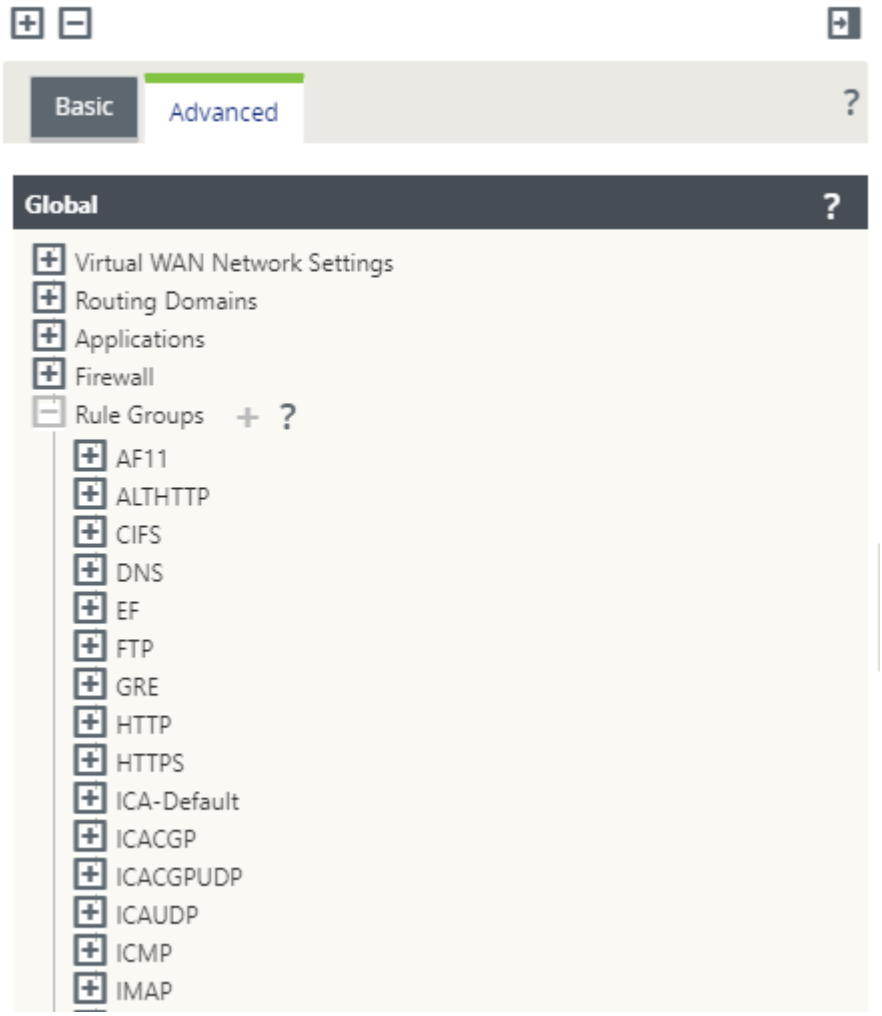
La puntuación media de MoS se calcula con un intervalo de muestreo de 1 minuto. La puntuación de MoS calculada por otras herramientas de terceros puede variar, dependiendo del intervalo de muestreo utilizado.

SD-WAN Center muestra el MOS para el tráfico existente que pasa a través de la ruta virtual. Para obtener más información acerca de cómo ver MOS en SD-WAN Center, consulte MOS para Aplicaciones.

Para agregar un grupo de reglas personalizado:

1. En el Editor de configuración, vaya a **Global** > **Grupos de reglas.**. Aparecerá la lista predeterminada de grupos de reglas.
2. Haga clic en el icono de agregar (+).
3. Introduzca el nombre de la aplicación.
4. Haga clic en el icono de edición y seleccione **Activar MOS**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Haga clic en **Aplicar**.

> **Nota**
>
> - También puede habilitar la estimación de MOS para las aplicaciones predeterminadas, seleccionando **Habilitar MOS**.
> - Active la opción Seguimiento de rendimiento en Reglas para estimar MOS para aplicaciones y mostrarlo en SD-WAN Center. Para obtener más información, consulte MOS para Aplicaciones.

Clasificación de aplicaciones

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los dispositivos Citrix SD-WAN realizan una inspección profunda de paquetes (DPI) para identificar y clasificar aplicaciones mediante las siguientes técnicas:

- Clasificación de bibliotecas de DPI
- Clasificación de Arquitectura de Computación Independiente (ICA) propietaria de Citrix
- API de proveedores de aplicaciones (por ejemplo, API REST de Microsoft para Office 365)
- Clasificación de aplicaciones basada en nombres de dominio

Clasificación de bibliotecas de DPI

La biblioteca Deep Packet Inspection (DPI) reconoce miles de aplicaciones comerciales. Permite el descubrimiento en tiempo real y la clasificación de aplicaciones. Mediante la tecnología DPI, 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 el **Editor de configuración**, vaya a **Global > Aplicaciones > Configuración de PPP** y active la casilla de verificación **Habilitar inspección profunda de paquetes** .

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 sobre TCP
- ICA sobre UDP/EDT
- ICA sobre puertos no estándar (incluyendo ICA multipuerto)
- Transporte adaptable HDX
- ICA sobre WebSocket (utilizado por HTML5 Receiver)

> **Nota**
>
> La clasificación del tráfico ICA entregado a través de SSL/TLS o DTLS no es compatible con SD-WAN Standard Edition, pero es compatible con SD-WAN Premium Edition y SD-WAN WANOP Edition.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 notifican como UDP o Protocolo desconocido.
>
> Desde la versión 10, versión 1, el dispositivo SD-WAN puede diferenciar cada flujo de datos ICA en ICA de varias secuencias incluso en una configuración de un solo puerto. Cada secuencia ICA se clasifica como una aplicación independiente con su propia clase QoS predeterminada para la priorización.
>
> - Para que la funcionalidad Multi-Stream ICA funcione correctamente, debe tener SD-WAN Standard Edition 10.1 o superior, o SD-WAN Premium Edition.
> - Para que los informes basados en usuarios HDX se muestren en SDWAN-Center, debe tener SD-WAN Standard Edition o Premium Edition 11.0 o superior.
>
> Requisitos mínimos de software para el canal virtual de información HDX:
>
> - La versión de servicio a largo plazo 7—1912 o una versión actual de Citrix Virtual Apps and Desktops (anteriormente XenApp y XenDesktop), ya que la funcionalidad de requisitos previos se introdujo en XenApp y XenDesktop 7.17 y no se incluye en la versión de servicio a largo plazo 7.15.
> - 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 Multiport/Multistream ICA entabla de funciones de la aplicación Citrix Workspace. Consulte las versiones de versión admitidas actualmente en.Perspectivas de HDX

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 Interactive (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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 que el tráfico de esos puertos coincida con las reglas IP válidas, debe actualizar las reglas IP ICA.

En ICA IP y lista de puertos 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. Utilice '*'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 clasifica 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 el **Editor de configuración**, vaya a **Global > Aplicaciones > Configuración de PPP** y active la casilla de verificación **Habilitar inspección profunda de paquetes para aplicaciones Citrix 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 del servicio de gateway.

Clasificación de aplicaciones basada en nombres de dominio

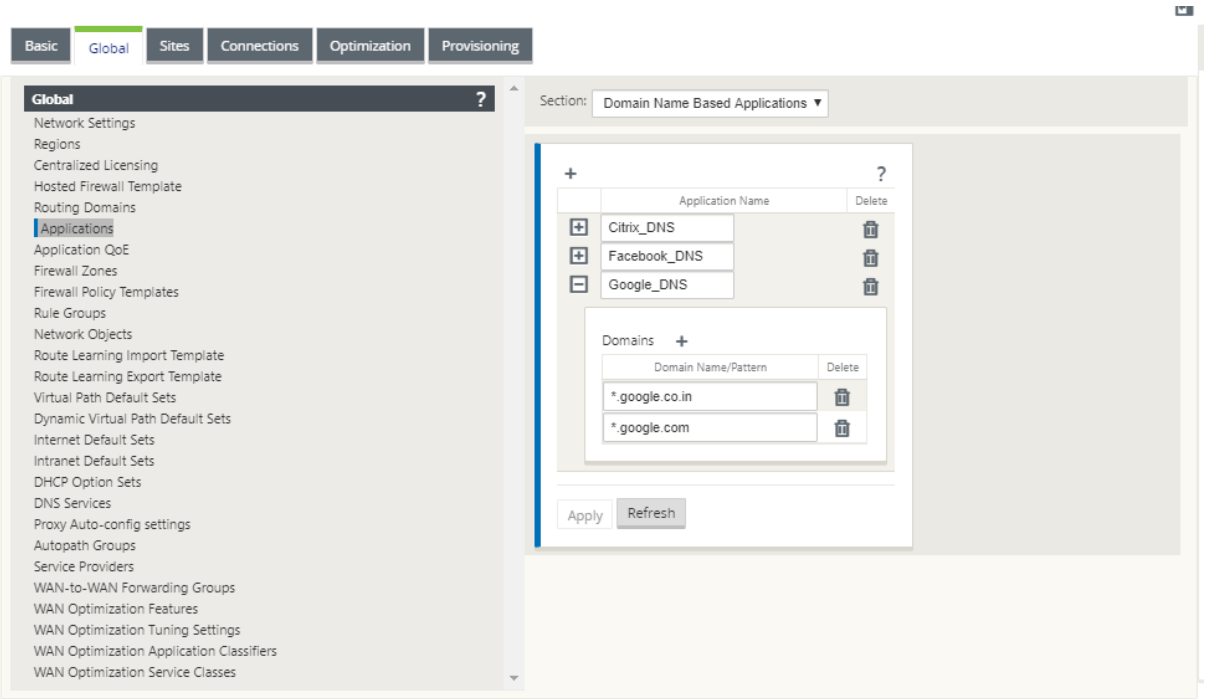
El motor de clasificación de DPI se ha mejorado para clasificar las aplicaciones en función del nombre de dominio y los patrones. Después de que el reenviador DNS intercepta y analiza las solicitudes DNS, el motor DPI utiliza el clasificador IP para realizar la primera clasificación de paquetes. Se realizan más bibliotecas de DPI y clasificación ICA y se anexa el identificador de aplicación basado en el nombre de dominio.

La función de aplicación basada en nombres de dominio permite agrupar varios nombres de dominio y tratarlos como una sola aplicación. Facilitando la aplicación de firewall, dirección de aplicaciones, QoS y otras reglas. Se puede configurar un máximo de 64 aplicaciones basadas en nombres de dominio.

Para definir aplicaciones basadas en nombres de dominio, en el Editor de configuración, vaya a **Global > Aplicaciones > Aplicacionesbasadas en nombres de dominio**. Introduzca un nombre de aplicación y agregue los nombres de dominio o patrones requeridos. Puede introducir el nombre de dominio completo o utilizar comodines al principio. Se permiten los siguientes formatos de nombre de dominio:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ejemplo.com
- *.ejemplo.com



Las aplicaciones basadas en nombres de dominio clasificados se utilizan para configurar lo siguiente:

- Proxy DNS
- Reenviador transparente DNS
- Objetos de aplicación
- Rutas de aplicación
- Directiva de firewall
- Reglas de QoS de la aplicación
- QoE de aplicaciones

Limitaciones

- Si no hay solicitud/respuesta DNS correspondiente a una aplicación basada en nombres de dominio, el motor DPI 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 DPI no clasifica la aplicación basada en nombres de dominio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 DPI, 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.
- No se admiten registros AAAA o registros IPv6.
- Los registros de respuesta DNS divididos en varios paquetes no se procesan. Solo se procesan las respuestas DNS en un solo paquete.
- DNS sobre TCP no es compatible.
- Solo los dominios de nivel superior son compatibles como patrones de nombres de dominio.

Clasificación del tráfico cifrado

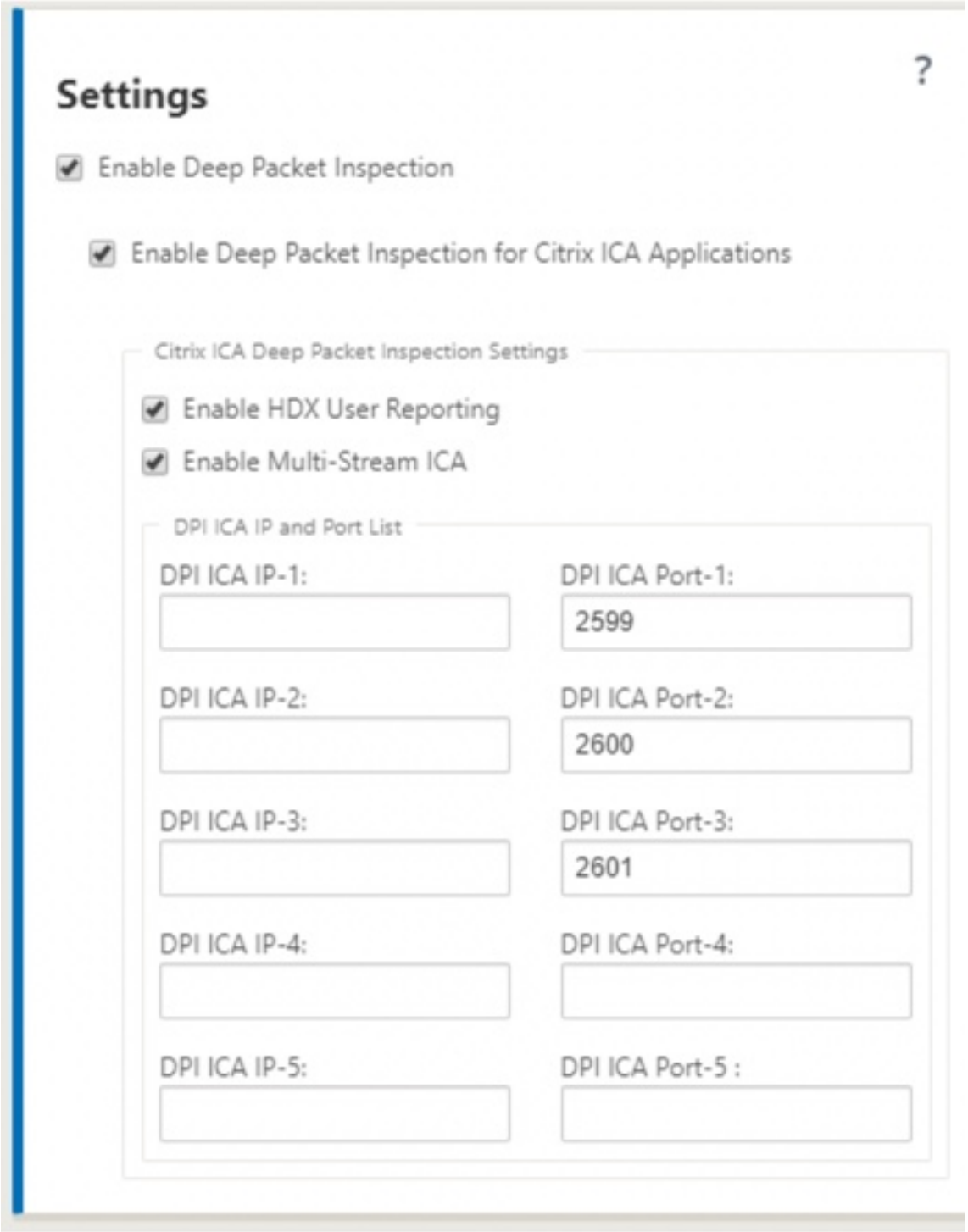
El dispositivo Citrix SD-WAN detecta e informa el tráfico cifrado, como parte de los informes de aplicaciones, en los dos métodos siguientes:

- Para el tráfico HTTPS, el motor DPI inspecciona el certificado SSL para leer el nombre común, que lleva el nombre del servicio (por ejemplo, Facebook, Twitter). Dependiendo de la arquitectura de la aplicación, solo se puede usar un certificado para varios tipos de servicios (por ejemplo, correo electrónico, noticias, etc.). Si diferentes servicios utilizan certificados diferentes, el motor DPI podría diferenciar entre servicios.
- Para aplicaciones que utilizan su propio protocolo de cifrado, el motor DPI busca patrones binarios en los flujos, por ejemplo, en el caso de Skype, el motor DPI busca un patrón binario dentro del certificado y determina la aplicación.

Para configurar los valores de clasificación de aplicaciones:

1. En el **Editor de configuración**, haga clic en **Global**> **Aplicaciones**> **Configuración**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

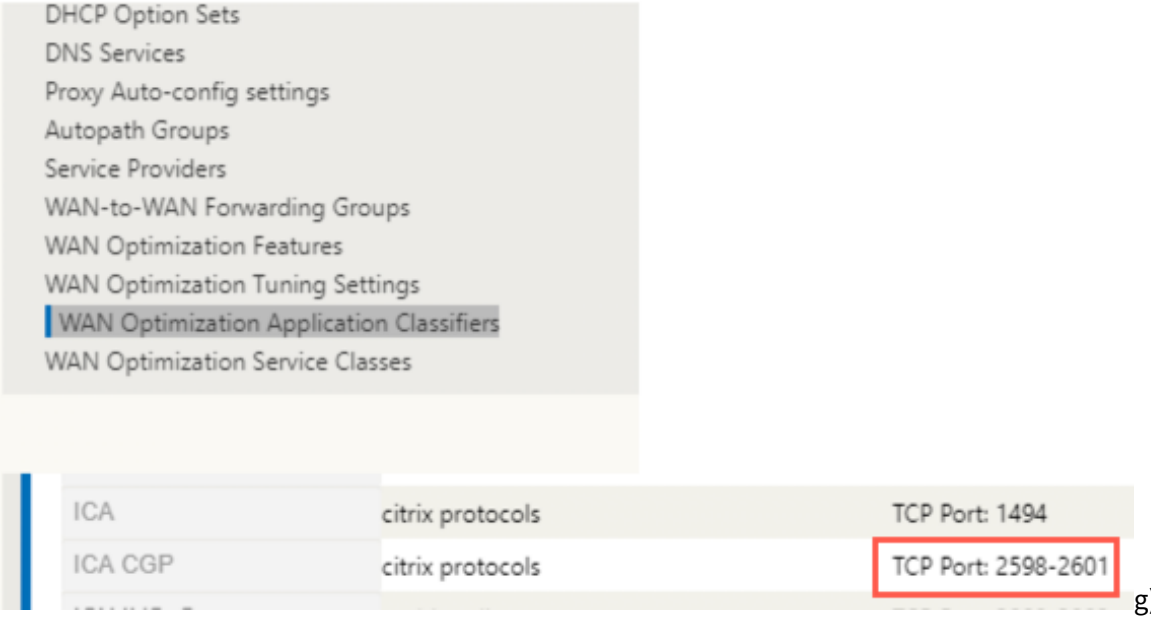


Nota

Si agrega un puerto ICA adicional para la implementación multipuerto, estos puertos deben agregarse en los clasificadores de aplicaciones de optimización de Wan. De lo contrario, el tráfico en los tres puertos adicionales no se reenviará a wanop. Solo se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> reenvía el puerto predeterminado 2598 si ICA está configurado para optimizar.



g)

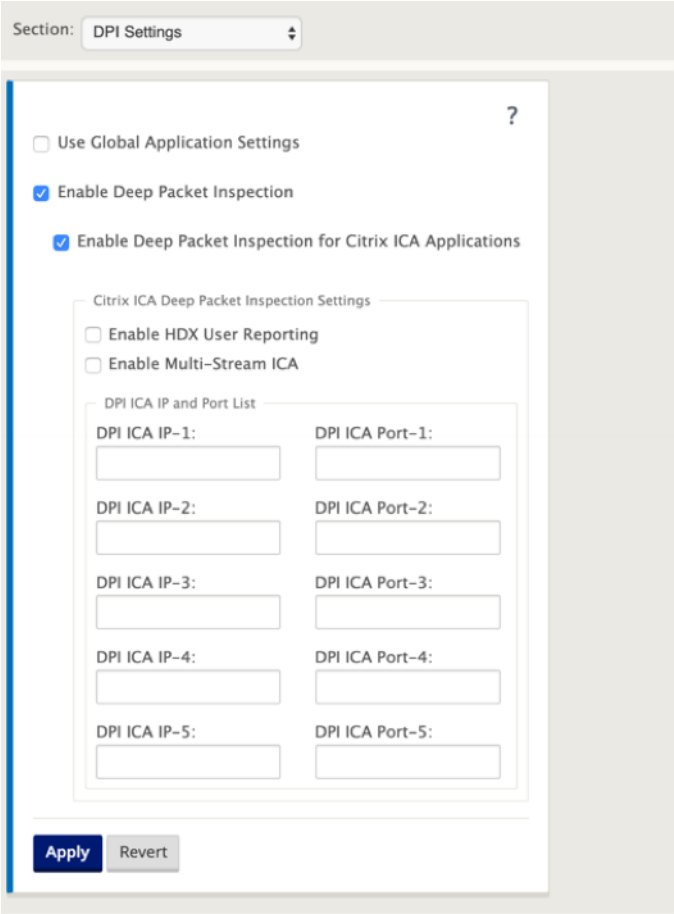
2. Seleccione **Activar inspección profunda de paquetes**. Esto permite la clasificación de aplicaciones en el dispositivo. Puede, ver y supervisar las estadísticas de aplicaciones en SD-WAN Center. Para obtener más información, consulte Informe de aplicación.

   > **Nota**
   >
   > De forma predeterminada, **Enable Deep Packet Inspection** recopila estadísticas de datos clasificados.

3. Seleccione **Habilitar inspección profunda de paquetes para aplicaciones Citrix ICA.** Esto permite la clasificación de las aplicaciones ICA de Citrix y recopila estadísticas para los recuentos de usuarios, sesiones y flujos. Sin esta opción activada, es posible que parte del tipo del tráfico HDX aún se clasifique y se calcule QoE, pero las estadísticas sobre SD-WAN Center no están disponibles. Puede, ver y supervisar las estadísticas de aplicaciones ICA en SD-WAN Center. Esta opción está habilitada de forma predeterminada. Para obtener más información, consulte Informes HDX.

4. Seleccione **Habilitar informes de usuario de HDX** para generar informes basados en usuarios recién agregados (Resumen de HDX, Sesiones de usuario de **HDX y Aplicaciones** de HDX) y estos informes están disponibles en SD-WAN Center. Esto no es aplicable al informe **Estadísticas del sitio HDX**. Esta opción está disponible en el nivel global y de sitio similar para habilitar la opción DPI. Para **habilitar los informes de usuario de HDX** a nivel de sitio, en el **Editor de configuración**, haga clic en **Conexiones > Aplicaciones**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. En el **puerto ICA DPI**, especifique los puertos no estándar utilizados en la directiva XA/XD para procesar la clasificación HDX. No incluya los números de puerto estándar 2598 o 1494 en esta lista, ya que estos ya están incluidos internamente.
6. En **DPI ICA IP**, especifique la dirección IP que se utilizará para restringir aún más los puertos a un destino específico.

   > **Nota**
   >
   > Utilice '*'para el puerto destinado a cualquier dirección IP.

7. Haga clic en **Aplicar**

Puede configurar las opciones de clasificación de aplicaciones en cada sitio individualmente. Haga clic en **Conexiones**, seleccione un sitio y haga clic en **Configuración de aplicaciones**. También puede optar por utilizar la configuración global de la aplicación.

Buscar aplicaciones

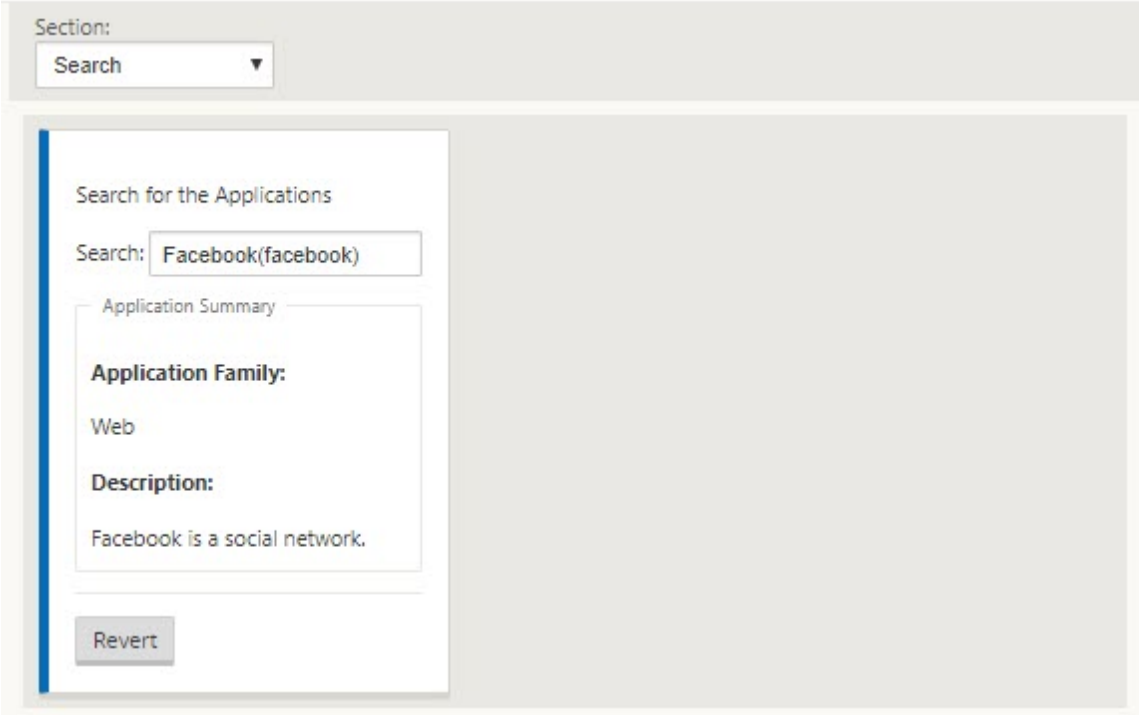
Puede buscar una aplicación para determinar el nombre de familia de la aplicación. También se proporciona una breve descripción de la aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para buscar una aplicación:

1. En el Editor de configuración, haga clic en **Global** > **Aplicaciones** > **Buscar**.
2. En el campo Buscar, escriba el nombre de la aplicación y haga clic en Intro.

   Aparecerá una breve descripción del nombre de la aplicación y de la familia de aplicaciones.



Las siguientes funciones utilizan la aplicación como un tipo de coincidencia:

- Directiva de firewall
- Reglas de QoS de la aplicación
- QoE de aplicaciones

> **Nota**
>
> Para obtener información sobre las aplicaciones que el dispositivo SD-WAN puede identificar mediante la inspección profunda de paquetes, consulte Biblioteca de firmas de aplicaciones.

Objetos de aplicación

Los objetos de aplicación permiten agrupar diferentes tipos de criterios de coincidencia en un único 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.

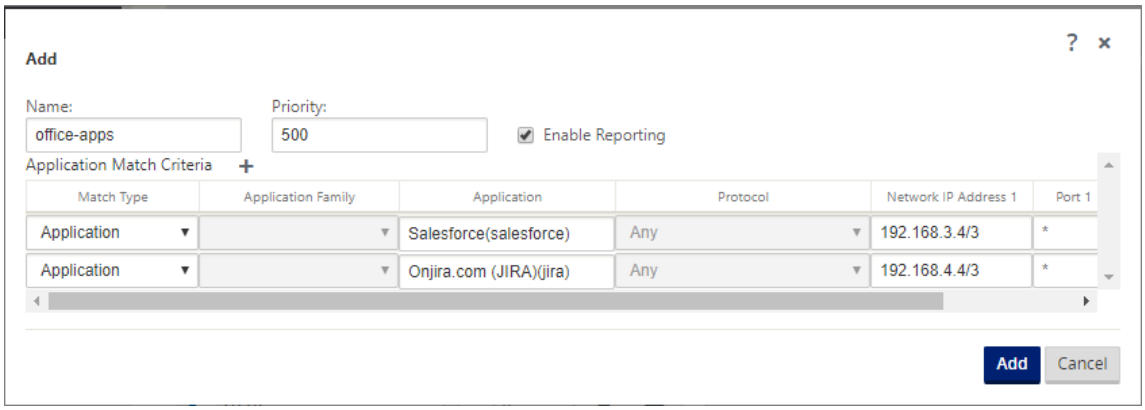
Las siguientes funciones utilizan el objeto de aplicación como un tipo de coincidencia:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Rutas de aplicación
- Directiva de firewall
- Reglas de QoS de la aplicación
- QoE de aplicaciones

Para crear un objeto de aplicación:

1. En el Editor de configuración, haga clic en **Global** > **Aplicaciones** > **Objetos de aplicación**.
2. Haga clic en **Agregar** y, en el campo **Nombre**, escriba un nombre para el objeto.

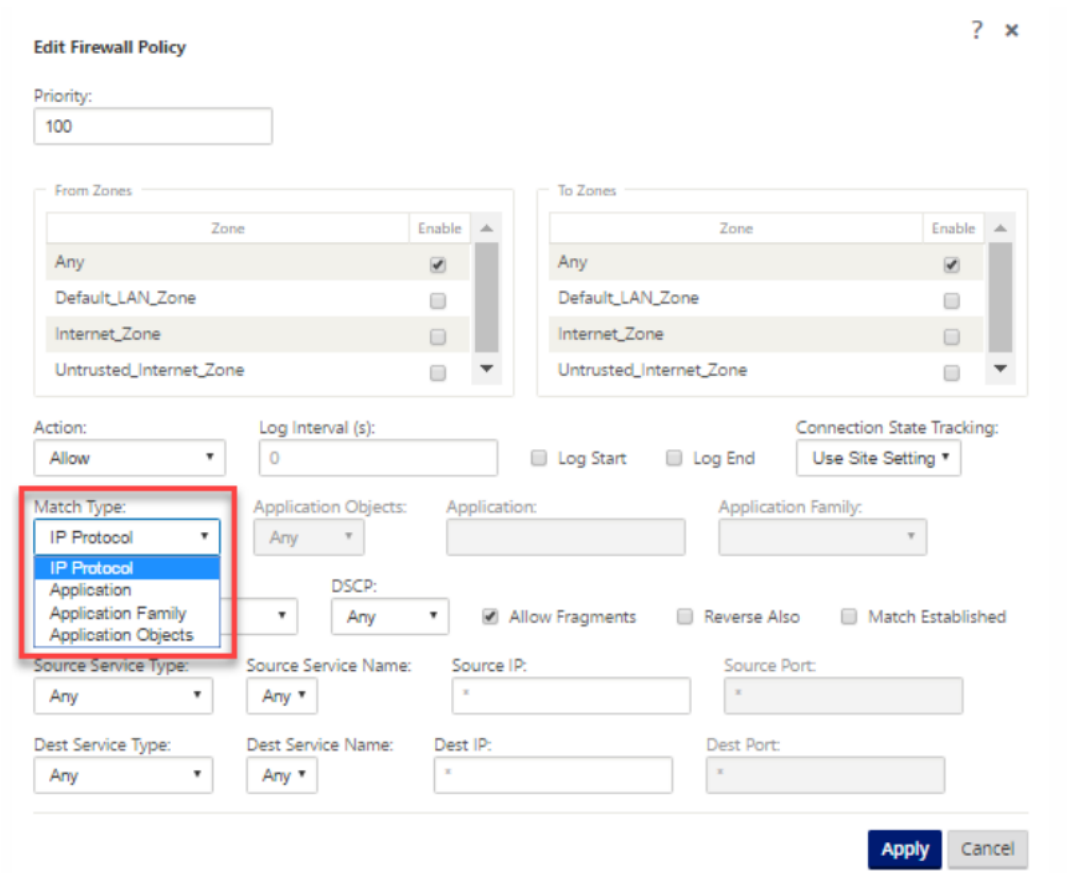


3. Seleccione **Habilitar informes** para habilitar la visualización de informes de aplicaciones personalizadas en Citrix SD-WAN Center. Para obtener más información, consulte Informe de aplicación.
4. En el campo **Prioridad**, introduzca la prioridad del objeto de aplicación. Cuando los paquetes entrantes coinciden con dos o más definiciones de objeto de aplicación, se aplica el objeto de aplicación con la prioridad más alta.
5. Haga clic en **+** en la sección **Criterios de coincidencia de aplicación**.
6. Seleccione uno de los siguientes tipos de coincidencia:
   - **Protocolo IP**: Especifique el protocolo, la dirección IP de red, el número de puerto y la etiqueta DSCP.
   - **Aplicación**: Especifique el nombre de la aplicación, la dirección IP de red, el número de puerto y la etiqueta DSCP.
   - **Familia de aplicaciones**: Seleccione una familia de aplicaciones y especifique la dirección IP de red, el número de puerto y la etiqueta DSCP.
7. Haga clic en **+** para agregar más criterios de coincidencia de aplicaciones.
8. Haga clic en **Agregar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 directivas y reglas de firewall. Se aplica a todas las directivas pre, post y local. Para obtener más información acerca del firewall, consulte Soporte de firewall con estado y NAT.



Visualización de Clasificación de Aplicaciones

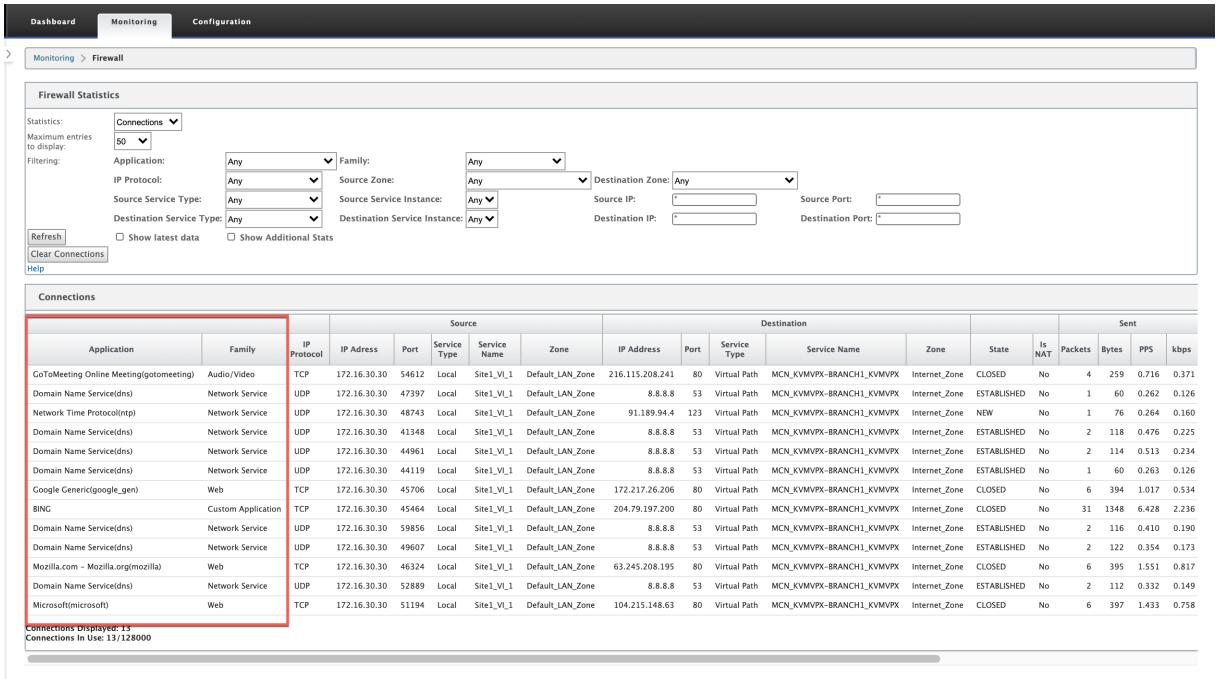
Después de habilitar la clasificación de aplicaciones, puede ver el nombre de la aplicación y los detalles de la familia de aplicaciones en los siguientes informes:

- Estadísticas de conexión al firewall
- Información sobre flujos
- Estadísticas de aplicación

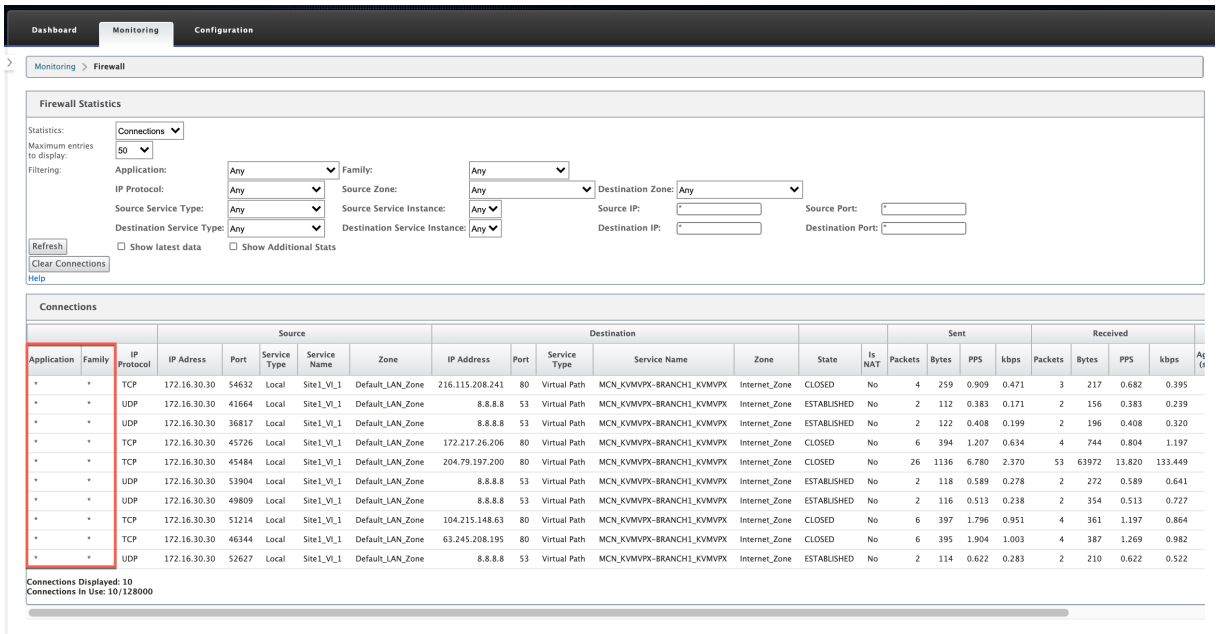
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Estadísticas de conexión de firewall

En el **Editor de configuración**, vaya a **Supervisión > Firewall**. En la sección **Conexiones**, las columnas **Aplicación** y **Familia** muestran las aplicaciones y su familia asociada.



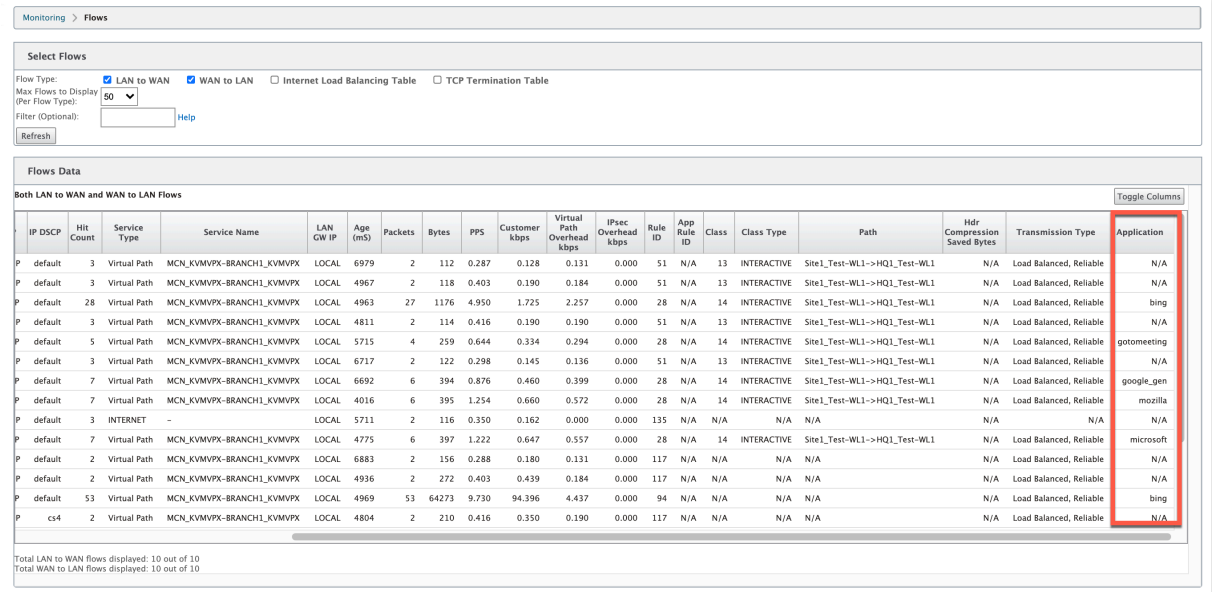
Si no habilita la clasificación de aplicaciones, las columnas **Aplicación** y **Familia** no muestran ningún dato.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Información sobre flujos

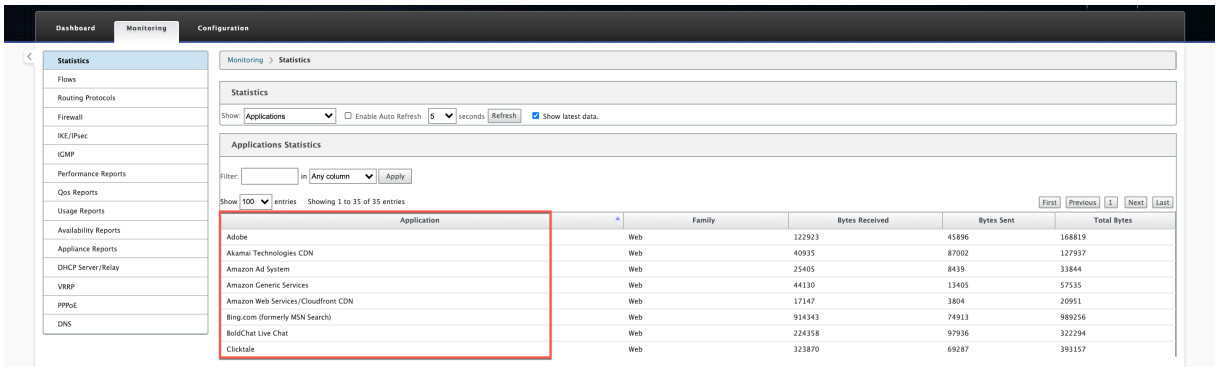
En el **Editor de configuración**, vaya a **Supervisión > Flujos**. En la sección **Datos de flujos**, la columna **Aplicación** muestra los detalles de la aplicación.



	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	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
P	default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6979	2	112	0.287	0.128	0.131	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P	default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4967	2	118	0.403	0.190	0.184	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P	default	28	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4963	27	1176	4.950	1.725	2.257	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	bing
P	default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4811	2	114	0.416	0.190	0.190	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P	default	5	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5715	4	259	0.644	0.334	0.294	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	gotomeeting
P	default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6717	2	122	0.298	0.145	0.136	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
P	default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6692	6	394	0.876	0.460	0.399	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	google_gen
P	default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4016	6	395	1.254	0.660	0.572	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	mozilla
P	default	3	INTERNET	–	LOCAL	5711	2	116	0.350	0.162	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	N/A
P	default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4775	6	397	1.222	0.647	0.557	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	microsoft
P	default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6883	2	156	0.288	0.180	0.131	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
P	default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4936	2	272	0.403	0.439	0.184	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
P	default	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4969	53	64273	9.730	94.396	4.437	0.000	94	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	bing
P	cs4	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4804	2	210	0.416	0.350	0.190	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A

Estadísticas de aplicación

En el **Editor de configuración**, vaya a **Supervisión > Estadísticas**. En **la sección Estadísticas** de la aplicación, la columna **Aplicación** muestra los detalles de la aplicación.



Application	Family	Bytes Received	Bytes Sent	Total Bytes
Adobe	Web	122923	45896	168819
Akamai Technologies CDN	Web	40935	87002	127937
Amazon Ad System	Web	25405	8439	33844
Amazon Generic Services	Web	44130	13405	57535
Amazon Web Services/Cloudfront CDN	Web	17147	3804	20951
Bing.com (formerly MSN Search)	Web	914343	74913	989256
BoldChat Live Chat	Web	224358	97936	322294
Clicktale	Web	323870	69287	393157

Solucionar 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 Clasificación de Aplicaciones.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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)

May 7, 2021

La función de equidad de QoS mejora la equidad de múltiples flujos de rutas virtuales mediante el uso de clases de QoS y detección temprana aleatoria (RED). Se puede asignar una ruta virtual a una de las 16 clases diferentes. Una clase puede ser uno de los tres tipos básicos:

- Las clases en tiempo real sirven flujos de tráfico que demandan un servicio rápido hasta un cierto límite de ancho de banda. Se prefiere una latencia baja sobre el rendimiento agregado.
- Las clases interactivas tienen menor prioridad que en 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 diferentes clases, lo que permite al programador de rutas virtuales arbitrar las solicitudes de ancho de banda de la competencia 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 HFSC en orden primero en entrar, primero en salir (FIFO). Antes de programar paquetes, Citrix SD-WAN examina la cantidad de tráfico pendiente para la clase de paquetes. Cuando el tráfico excesivo está pendiente, los paquetes se descartan en lugar de ser puestos en la cola (caída de cola).

¿Por qué TCP causa la puesta en cola?

TCP no puede controlar la rapidez con que la red puede transmitir datos. Para controlar el ancho de banda, TCP implementa el concepto de una 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 confirmaciones. Esto se denomina fase de inicio lento o crecimiento exponencial.

TCP identifica la congestión de red detectando paquetes descartados. Si la pila TCP envía una ráfaga de paquetes que introducen un retraso de 250 ms, TCP no detecta congestión si ninguno de los paque-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tes se descarta, por lo que continúa aumentando el tamaño de la ventana. Podría continuar haciéndolo hasta que el tiempo de espera llegue a 600-800 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. TCP, por lo tanto, alterna entre poner presión al alza en el ancho de banda y retroceder. Desafortunadamente, si el tiempo de espera alcanza los 800 ms en el momento en que se detecta la pérdida de paquetes, la reducción del ancho de banda provoca un retraso de transmisión.

Impacto en la equidad QoS

Cuando se produce un retraso de transmisión TCP, proporcionar cualquier tipo de garantía de equidad dentro de una clase de ruta virtual es difícil. 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 tráfico fluye para llenar la ruta virtual, lo que dificulta que una nueva conexión TCP logre una parte justa del ancho de banda. Compartir el ancho de banda de manera justa requiere asegurarse de que el ancho de banda está disponible para que los nuevos paquetes se transmitan.

Detección temprana aleatoria

La detección temprana aleatoria (RED) evita que las colas de tráfico se llenen y provoquen acciones de caída de cola. Evita que el programador de rutas virtuales realice una cola innecesaria, sin afectar el rendimiento que una conexión TCP puede lograr.

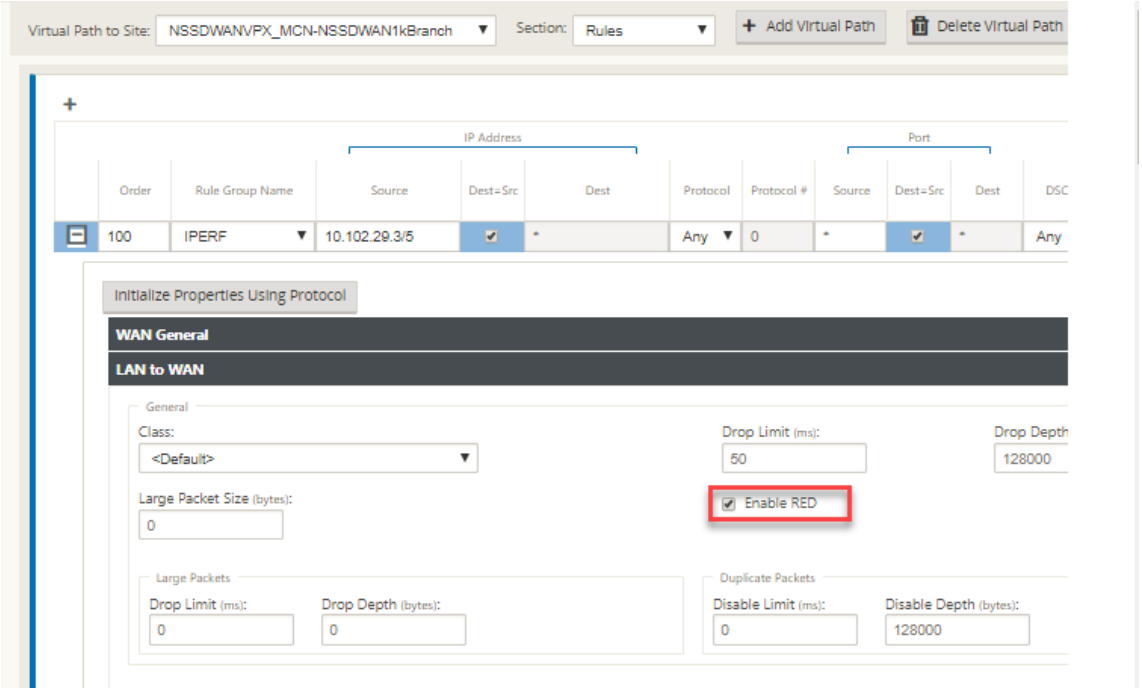
Cómo utilizar RED

1. Inicie una sesión TCP para crear la ruta virtual. Verifique que con RED habilitado, el tiempo de espera en esa clase permanezca alrededor de 50 ms en el estado estacionario.
2. Inicie una segunda sesión TCP y compruebe que ambas sesiones TCP comparten el ancho de banda de ruta virtual de manera uniforme. Verifique que el tiempo de espera de la clase permanezca en el estado estacionario.
3. Compruebe que el Editor de configuración se puede utilizar para habilitar y inhabilitar RED y que muestra el valor correcto para el parámetro.
4. Compruebe que la página Ver Configuración de la GUI de SD-WAN muestra si RED está habilitado para una regla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cómo habilitar RED

1. Vaya al **Editor de configuración** > **Conexiones** > **Rutas virtuales** > **[Seleccionar ruta virtual]** > **Reglas** > Seleccionar regla, por ejemplo; **(VOIP)**.
2. Expanda el panel **LAN a WAN**. En la sección **LAN a WAN**, haga clic en la casilla de verificación **Habilitar RED** para habilitarla para reglas basadas en TCP.



Colas MPLS

May 7, 2021

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 única de punto de código de servicios diferenciados (DSCP) correspondiente al esquema de cola del proveedor. Después de definir un enlace WAN para cada cola MPLS, se define el servicio de intranet para asignar 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Permite a los proveedores de MPLS identificar el tráfico basado en marcas DSCP para que el proveedor pueda aplicar la clase de servicio.

> **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.

Configurar enlaces WAN MPLS privados

1. Defina el tipo de acceso de enlace WAN como MPLS privado.
2. Defina las colas MPLS correspondientes a las colas MPLS del proveedor de servicios.
3. Habilite el Enlace WAN para el servicio de rutas virtuales (habilitado de forma predeterminada para Enlaces WAN MPLS privados).
4. Desde la ruta virtual de un enlace WAN, asigne un grupo de ruta automática.

   > **Nota**
   >
   > Si el grupo de rutas automáticas se asigna desde el nivel de enlace WAN, SD-WAN crea rutas automáticamente entre las colas de MCN y MPLS cliente basándose en etiquetas DSCP coincidentes. Si el grupo de rutas automáticas se asigna desde el nivel de cola MPLS, SD-WAN crea rutas automáticamente independientemente de si las etiquetas DSCP coinciden.

5. Asegúrese de que el mismo grupo de rutas automáticas esté configurado en el MCN y en el cliente.
6. Compruebe que las rutas de acceso para el enlace WAN se crean automáticamente.
7. Asigne el servicio de intranet a una cola específica, si es necesario.

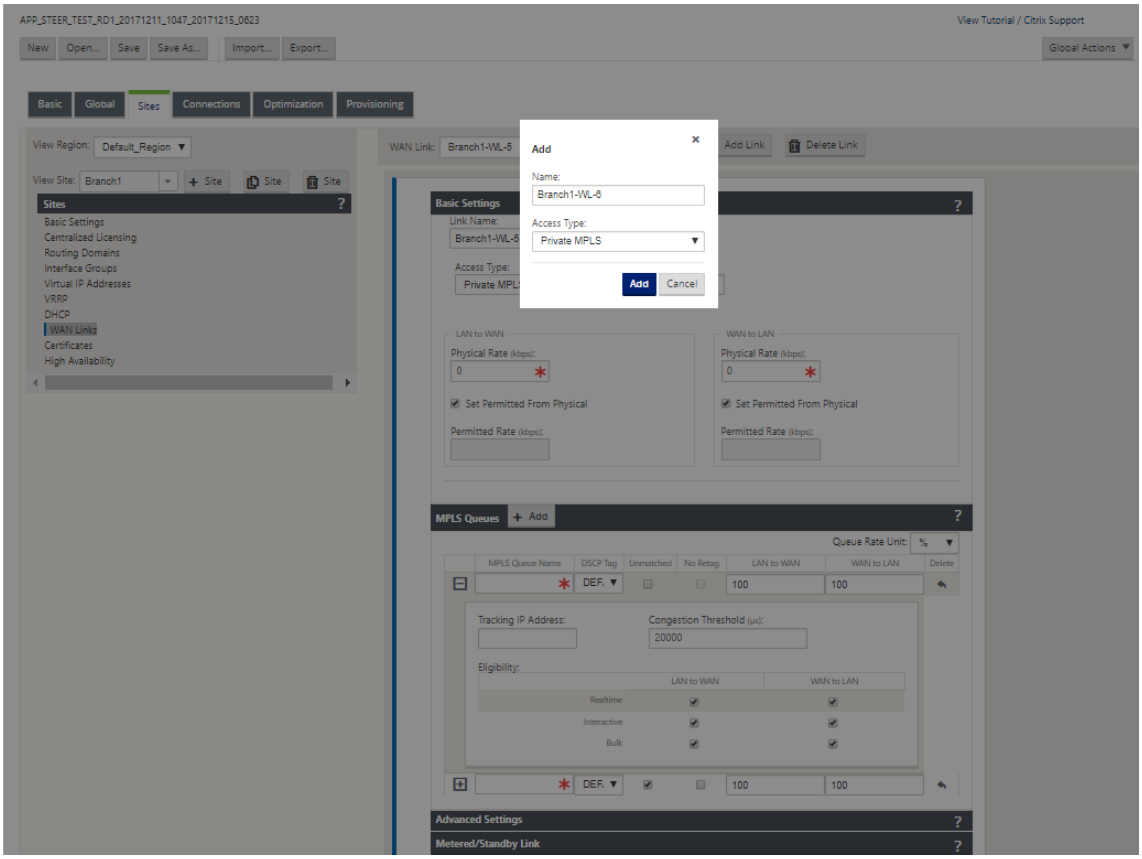
> **Nota**
>
> Es posible que la configuración de SD-WAN no tenga una asignación uno a uno para las colas basadas en el proveedor. Esto se basa en casos de implementación específicos. No puede crear grupos de rutas automáticas entre diferentes tipos de acceso privado. Por ejemplo, no puede crear grupos de rutas automáticas entre un tipo de acceso privado a Internet y un tipo de acceso MPLS privado.

Cómo agregar MPLS WAN LINK privado

Para configurar un nuevo tipo de acceso de enlace WAN para MPLS privado:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el Editor de configuración, vaya a **Sitios** > **[Nombre del sitio]** > **Vínculos WAN.** Haga clic en **Agregar vínculo.** Escriba el nombre del enlace WAN y seleccione **MPLS Privado** como Tipo de acceso.



2. En **Configuración básica**, ahora hay una nueva ficha **Colas MPLS**. Haga clic en + Agregar para agregar colas MPLS específicas. Estos deben corresponderse con las colas definidas por el proveedor de servicios.

Campo	Descripción
Nombre de cola MPLS	El nombre de la cola MPLS
Etiqueta DSCP	Configuración de la etiqueta DSCP del proveedor de servicios para la cola.
Incomparable	Cuando se habilita, todas las tramas que lleguen que no coincidan con las etiquetas definidas dentro del archivo de configuración se asignan a esta cola y al ancho de banda definido para esta cola.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Descripción
Velocidad permitida de LAN a WAN (kbps)	La cantidad de ancho de banda que los dispositivos SD-WAN pueden utilizar para la carga, que no puede exceder la velocidad de carga física definida del enlace WAN.
Velocidad permitida de WAN a WAN (kbps)	La cantidad de ancho de banda que los dispositivos SD-WAN pueden utilizar para la descarga, que no puede exceder la velocidad de descarga física definida del enlace WAN.

Expanda la definición de cola MPLS (haciendo clic en +) y aparecerán más opciones. Estas opciones incluyen:

Campo	Descripción
Dirección IP de seguimiento	Dirección de seguimiento de enlace WAN
Umbral de congestión	La cantidad de tiempo definida para la congestión (en microsegundos) después del cual MPLS Queue acelera la transmisión de paquetes para evitar más congestión. Cuando la congestión supera el umbral establecido, SD-WAN retrocede la velocidad de envío.
Elegibilidad	La elegibilidad de la cola MPLS para procesar clases específicas de tráfico. Cuando la elegibilidad está inhabilitada para una clase de tráfico específica, es poco probable que esa clase de tráfico se enrute a través de la cola MPLS a menos que las condiciones de red lo requieran.

Configure las colas MPLS que correspondan a las definiciones de cola de enlace WAN de Service Provider existentes.

> **Nota**
>
> Los enlaces WAN MPLS existentes configurados antes de SD-WAN 9.1 no se verán afectados.

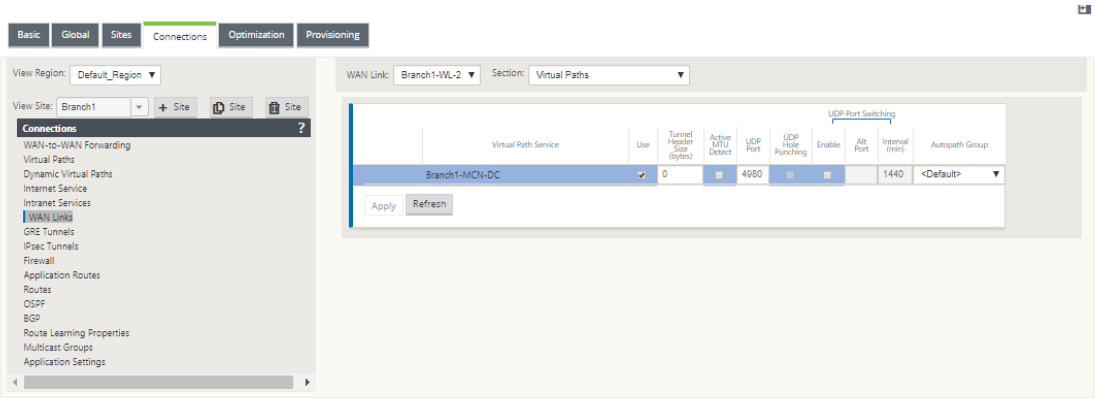
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Definir propiedades de enlace WAN para MPLS privados

Una vez definido el enlace WAN MPLS privado con sus colas MPLS, debe asignar un grupo de rutas automáticas para el enlace WAN bajo una definición de ruta virtual específica.

Para asignar un grupo de rutas automáticas:

1. Vaya a **Conexiones** > **[Nombre del sitio]** > **Enlaces WAN** >[**Nombre del enlace WAN MPLS**] > **Rutas virtuales** > [**Nombre de ruta virtual**] > [**Sitio local**] > **Enlaces WAN** y haga clic en **Modificar** ().
2. Haga clic en el menú implementable **Grupo de rutas automáticas** y elija uno de los grupos disponibles. De forma predeterminada, las colas MPLS heredan el grupo de rutas automáticas asignado al enlace WAN MPLS. Puede elegir definir las colas MPLS individuales para Heredar el grupo de rutas automáticas elegido o elegir una alternativa en el menú desplegable Grupo de rutas automáticas para cada cola MPLS.



> **Nota**
>
> Si no hay ninguna asignación de uno a uno, basada en la etiqueta DSCP, entre las colas del sitio local y el sitio remoto, debe asignar colas MPLS a grupos de rutas automáticas específicos. Heredar un grupo de rutas automáticas del enlace WAN MPLS genera automáticamente rutas entre colas con etiquetas DSCP coincidentes.

Asignar grupo de ruta automática al enlace de WAN de ruta virtual

El grupo de rutas automáticas definido es el mismo para el dispositivo MCN y el cliente. Esto permite que el sistema construya los Caminos automáticamente. En el sitio de MCN, también puede expandir el enlace WAN asociado a la ruta virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ver la velocidad permitida y la congestión para enlaces WAN

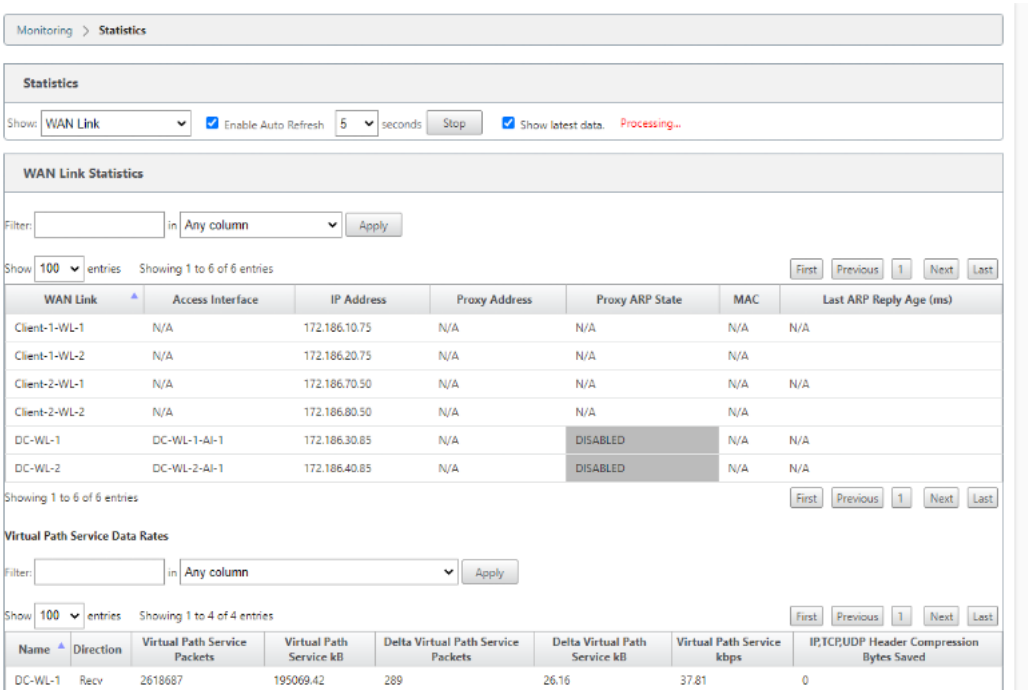
La interfaz web SD-WAN permite ahora ver la tasa permitida para los Vínculos WAN y los Usos de Vínculos WAN y si un Vínculo WAN, Path o Ruta Virtual está en estado congestionado. En las versiones anteriores, esta información estaba disponible en archivos de registro SD-WAN y a través de la CLI. Estas opciones están ahora disponibles en la interfaz web para ayudar con la solución de problemas.

Ver tarifa permitida

La velocidad permitida es la cantidad de ancho de banda que se permite utilizar un enlace WAN determinado, un servicio de ruta virtual, un servicio de intranet o un servicio de Internet en un momento determinado. La velocidad permitida para un enlace WAN es estática y se define explícitamente en la configuración SD-WAN. La tasa permitida para un Servicio de Ruta Virtual, Servicio de Intranet o Servicio de Internet fluctuará con el tiempo, en respuesta a la congestión, la demanda del usuario y las acciones justas, pero siempre será superior o igual al Ancho de banda mínimo reservado para el Servicio.

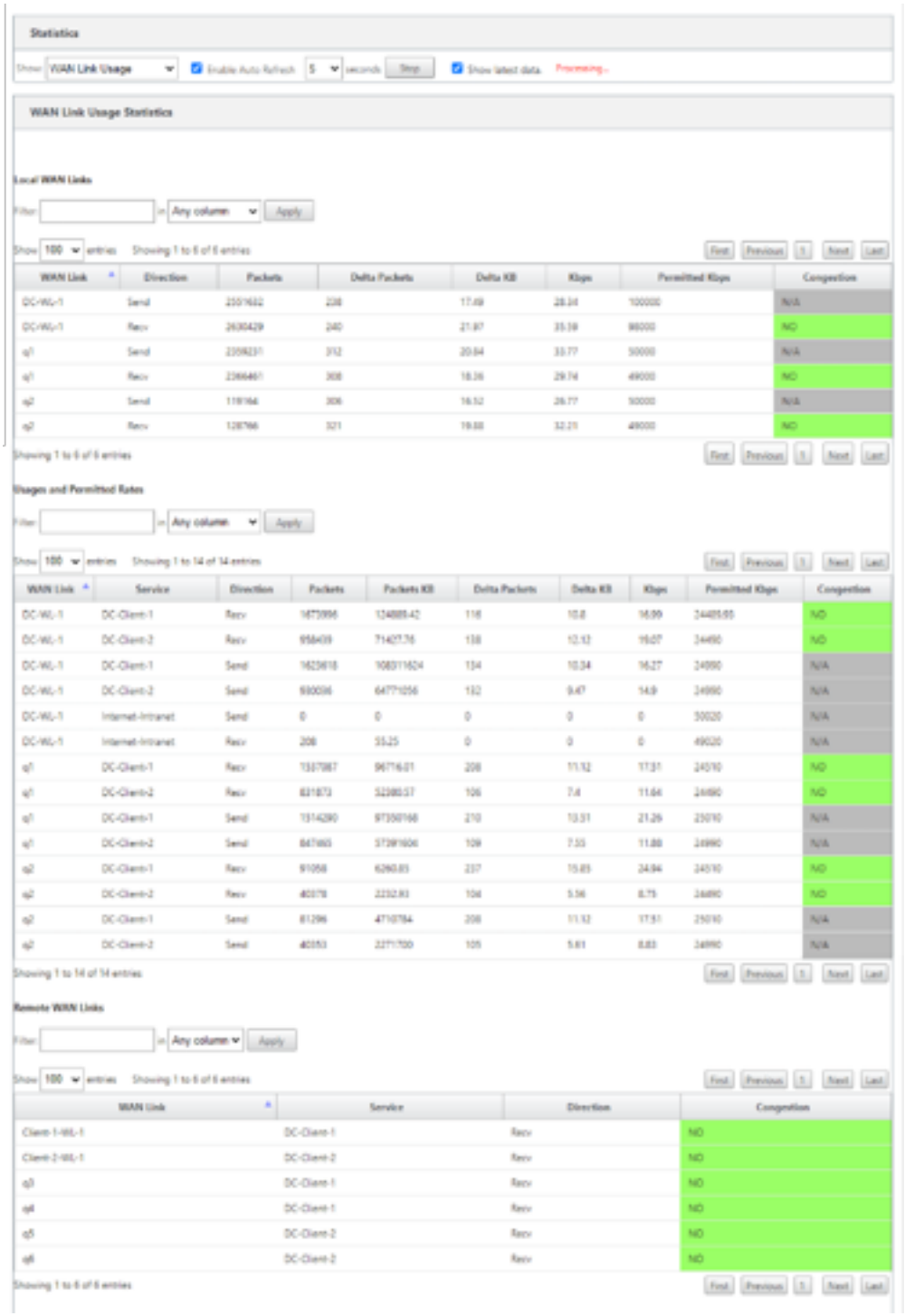
Supervisar enlace WAN

Vaya a **Monitor Estadísticas**y seleccione **Vínculo WAN** en la lista desplegable **Mostrar** .



Vaya a **Monitor > Estadísticas**y seleccione **Uso de vínculos WAN** en la lista desplegable **Mostrar** .

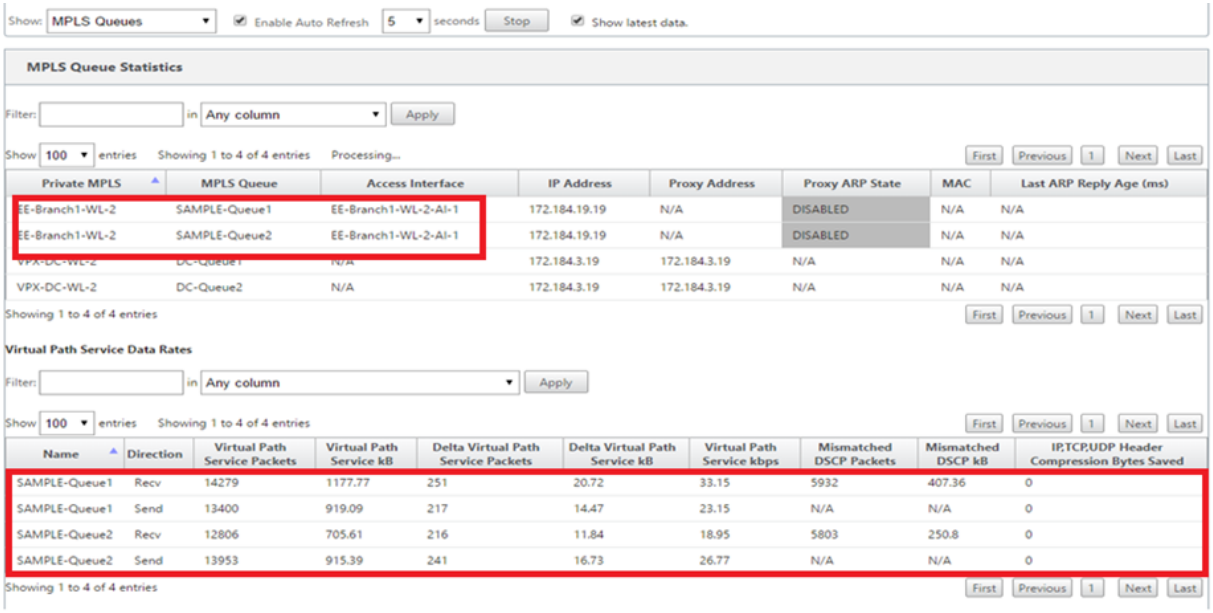
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supervisar colas MPLS

Vaya a **Supervisar Estadísticas**y seleccione **Colas MPLS** en la lista desplegable **Mostrar**.

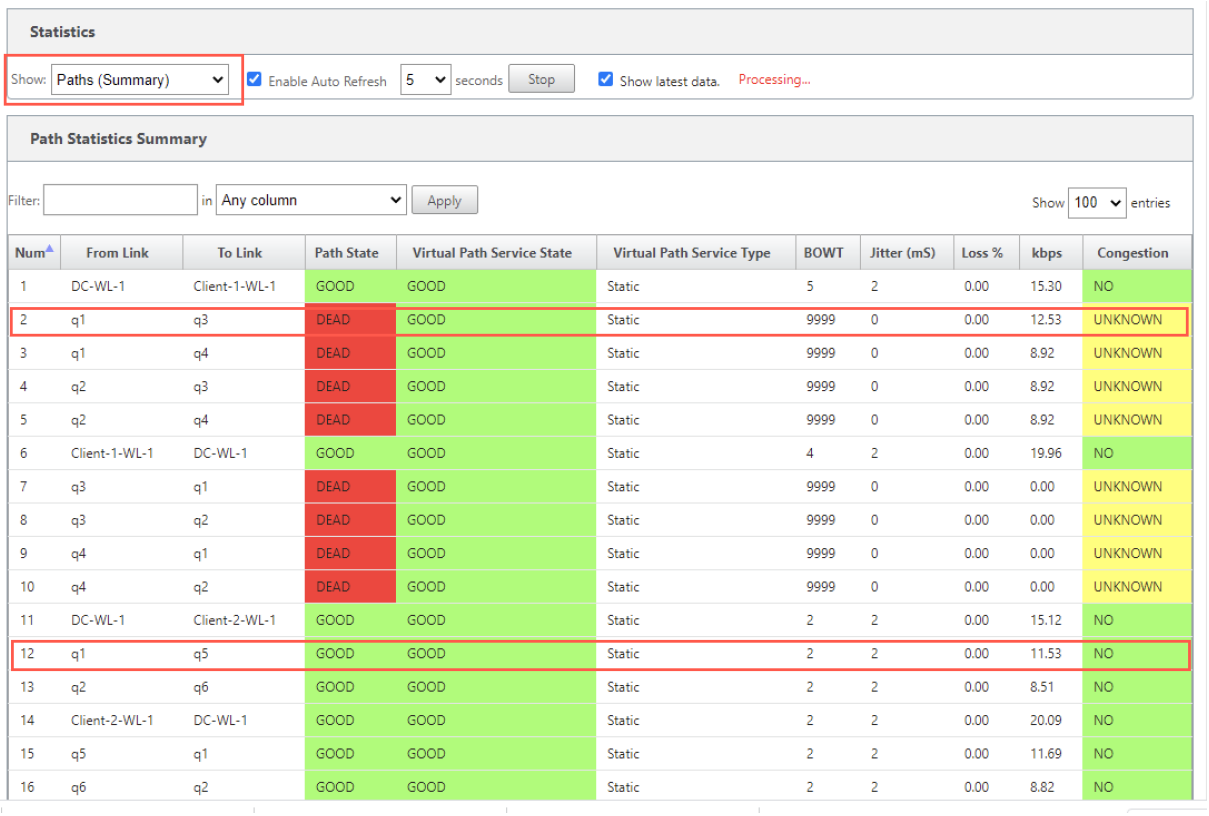
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

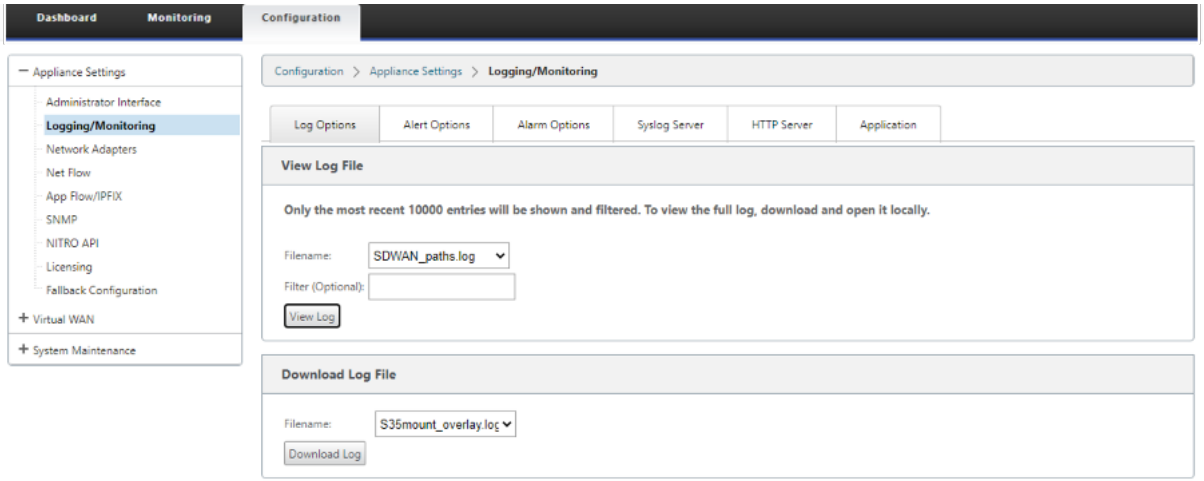
Show 100 entries Showing 1 to 12 of 12 entries First Previous 1 Next Last

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-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ración > Registro/Supervisión y seleccione **SDWAN_paths.log** o **SDWAN_common.log** en la ficha **Opciones de registro**.



Informes

May 7, 2021

QoE de aplicaciones

Múltiples colectores de flujo neto

QoE de aplicaciones

May 7, 2021

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 a través de 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	Intervalo
Bueno	8–10
Justo	4–8
Mala	0–4

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Calidad	Intervalo

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 para 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 la aplicación 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 fluctuación: 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 oscila entre 0 y 10.

Puede crear perfiles QoE con valores de umbral personalizados y aplicarlos a aplicaciones u objetos de aplicación.

> **Nota**:
>
> El valor QoE puede ser cero si las condiciones de red están fuera de los umbrales configurados para el tráfico en tiempo real.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

QoE de aplicaciones interactivas

La QoE de aplicaciones para aplicaciones interactivas utiliza una técnica innovadora de Citrix basada en umbrales de pérdida de paquetes y velocidad de ráfagas.

Las aplicaciones interactivas son sensibles a la pérdida de paquetes y el rendimiento. Por lo tanto, medimos el porcentaje de pérdida de paquetes y la velocidad de ráfaga 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 menor que el umbral configurado.
- La velocidad de ráfaga de salida es al menos el porcentaje configurado de velocidad de ráfaga de entrada.

Configuración de la QoE de la aplicación

Asigne objetos de aplicación o aplicación a perfiles QoE predeterminados o personalizados.
Puede crear perfiles de QoE personalizados para el tráfico en tiempo real e interactivo.

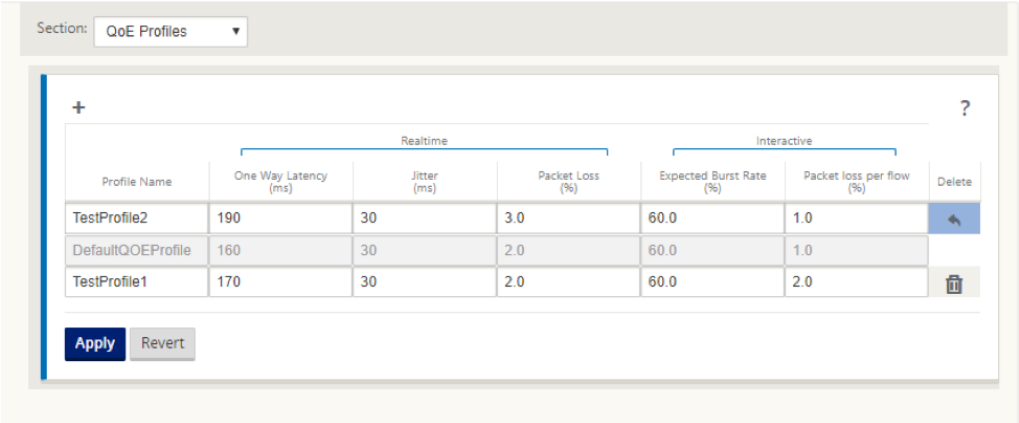
Para crear perfiles de QoE personalizados:

1. En el Editor de configuración, vaya a **Global > Aplicación QoE > Perfiles de QoE** y haga clic en **+**.
2. Introduzca el valor para los siguientes parámetros:
    - **Nombre de Perfil**: Nombre para identificar el perfil que establece umbrales para el tráfico interactivo y en tiempo real.
    - **Tiempo real**: Configure umbrales para los flujos de tráfico que se aplican a la directiva QoS en tiempo real. Un flujo de una aplicación en tiempo real que cumple con los umbrales de latencia, pérdida y fluctuación por debajo de los umbrales de latencia, pérdida y fluctuación se considera de buena calidad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Latencia One Way**: El umbral de latencia en milisegundos. El valor del perfil QoE predeterminado es 160 ms.
  - **Fluctuación**: Umbral de fluctuación en milisegundos. El valor del perfil QoE predeterminado es 30 ms.
  - **Pérdida de paquetes**: El porcentaje de pérdida de paquetes. El valor del perfil QoE predeterminado es 2%.

- **Interactivo**: Configure umbrales para los flujos de tráfico que se aplican a la directiva interactiva de QoS. Se considera que un flujo de una aplicación interactiva que cumpla con ese umbral por debajo del ratio de ráfagas y pérdida de paquetes es de buena calidad.
  - **Velocidad de ráfaga esperada**: El porcentaje de velocidad de ráfaga esperada. La velocidad de ráfaga de salida debe ser al menos el porcentaje configurado de velocidad de ráfaga de entrada. El valor del perfil QoE predeterminado es 60%.
  - **Pérdida de paquetes por flujo**: Porcentaje de pérdida de paquetes. El valor del perfil QoE predeterminado es 1%.

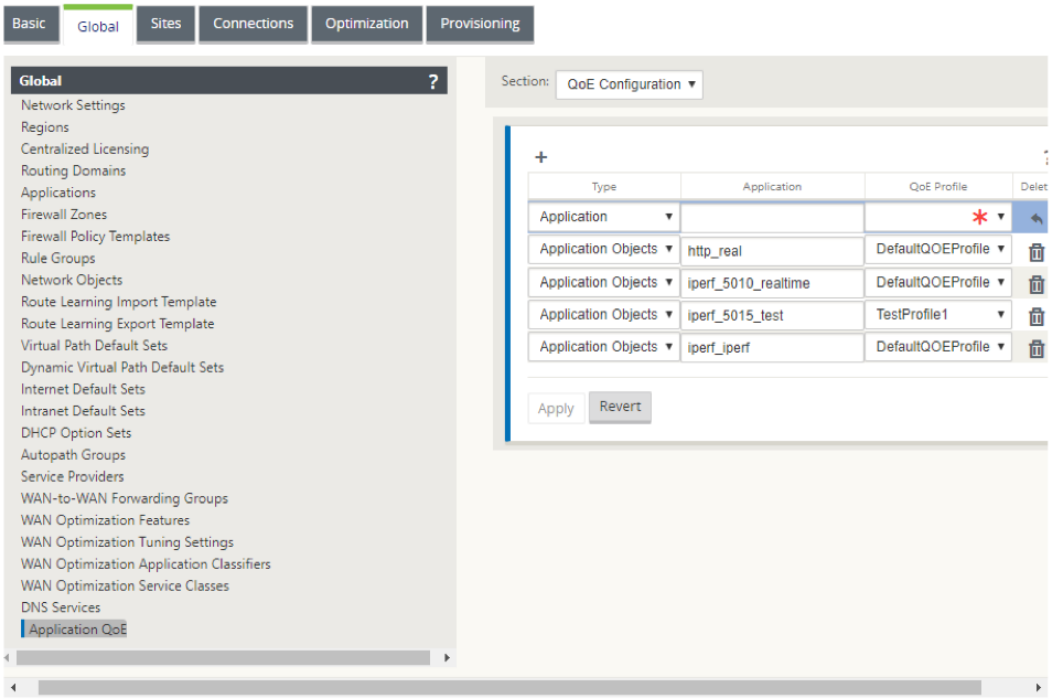


3. Haga clic en **Aplicar**.

Para asignar aplicaciones u objetos de aplicación con perfiles QoE:

1. En el Editor de configuración, vaya a **Global > Application QoE > QoE Configuration** y haga clic en **+**.
2. Seleccione valores para los siguientes parámetros:
   - **Tipo**: Una aplicación DPI o un objeto de aplicación.
   - **Aplicación**: Busque y seleccione una aplicación u objeto de aplicación según el tipo seleccionado.
   - **Perfil de QoE**: Seleccione un perfil de QoE para asignarlo a la aplicación o al objeto de la aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Haga clic en **Aplicar**.

Puede asignar hasta 10 aplicaciones u objetos de aplicación con perfiles QoE. Puede ver los informes de QoE de la aplicación en SD-WAN Center. Para obtener más información, consulte elInforme QOE de la aplicacióninforme.

HDX QoE

May 7, 2021

Los parámetros de red como latencia, fluctuación y caída de paquetes afectan a la experiencia de usuario de los usuarios de HDX. Quality of Experience (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 directivas 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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 SD-WAN Center, 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	Gama QoE
Bueno	80–100
Justo	50–80
Mala	0–50

En el panel de control de Citrix SD-WAN Center también se muestra una lista de los cinco sitios inferiores con la menor QoE.

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, consulte Tablero central de SD-WAN.

También puede ver los informes detallados de HDX de cada sitio en Citrix SD-WAN Center. Para obtener más información, consulte Informes HDX.

> **Nota**
>
> - *No espere que la latencia de 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 inferior a la pérdida de enlaces WAN.*
> - *La latencia de enlace WAN que se muestra en la GUI es BOWT (Best One Way Time). Es la mejor métrica del enlace como un medio para medir el estado del enlace. La aplicación QoE 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 enlace ICA, la sesión se puede contar 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*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> *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

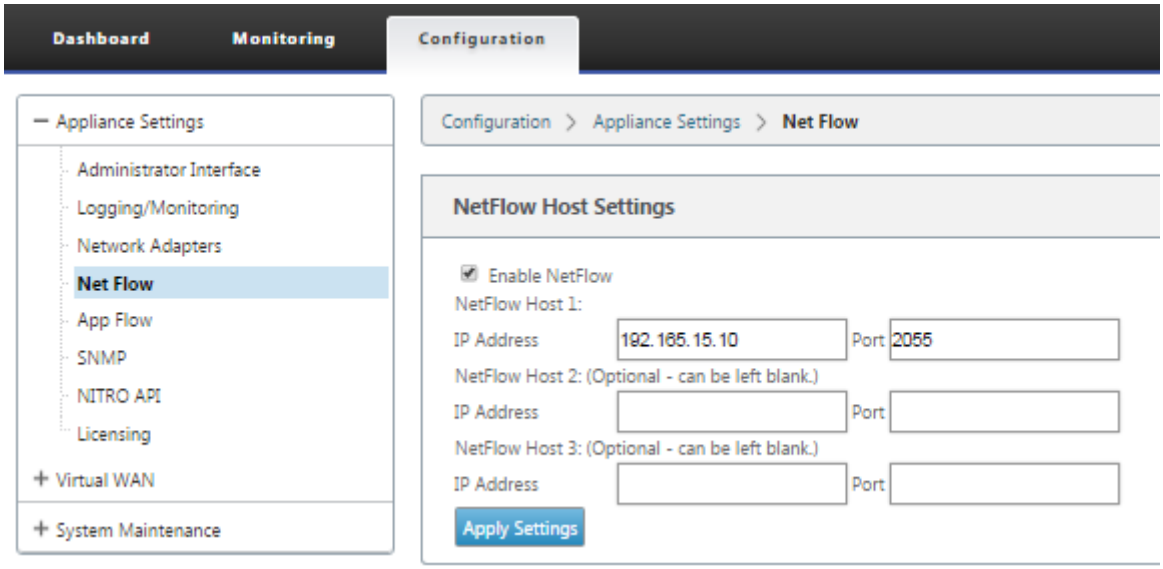
October 27, 2021

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 es compatible con los dispositivos Citrix SD-WAN Standard y Premium (Enterprise) Edition.

Para configurar hosts de flujo neto:

Vaya a **la página Configuración > Configuración del dispositivo > Flujo de red > Configuración del host de NetFlow**. Haga clic en la **casilla de verificaciónHabilitar NetFlow**, escriba la**dirección IP**y los números de**puerto**para hasta tres hosts de flujo de red y, a continuación, haga clic en**Aplicar configuración para** guardar los cambios.

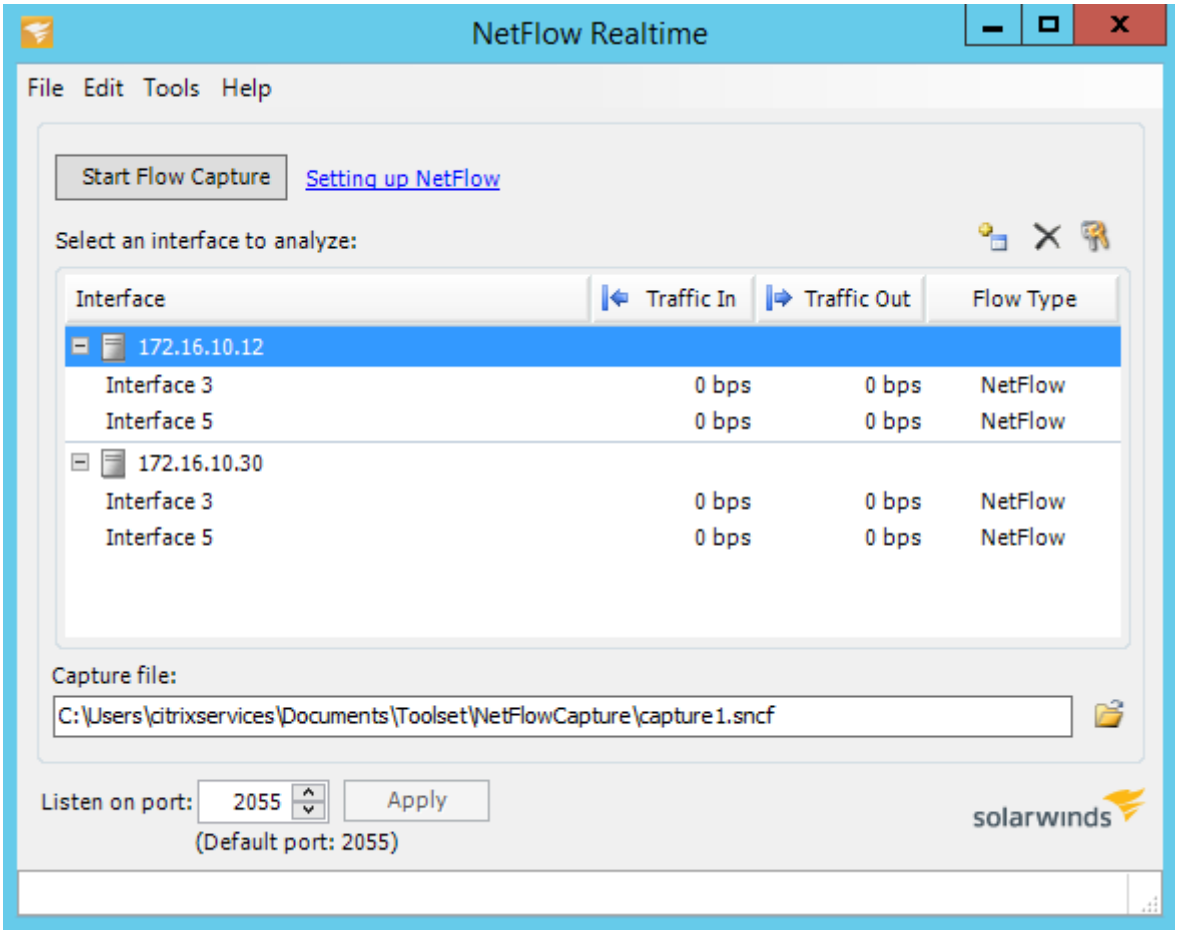
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



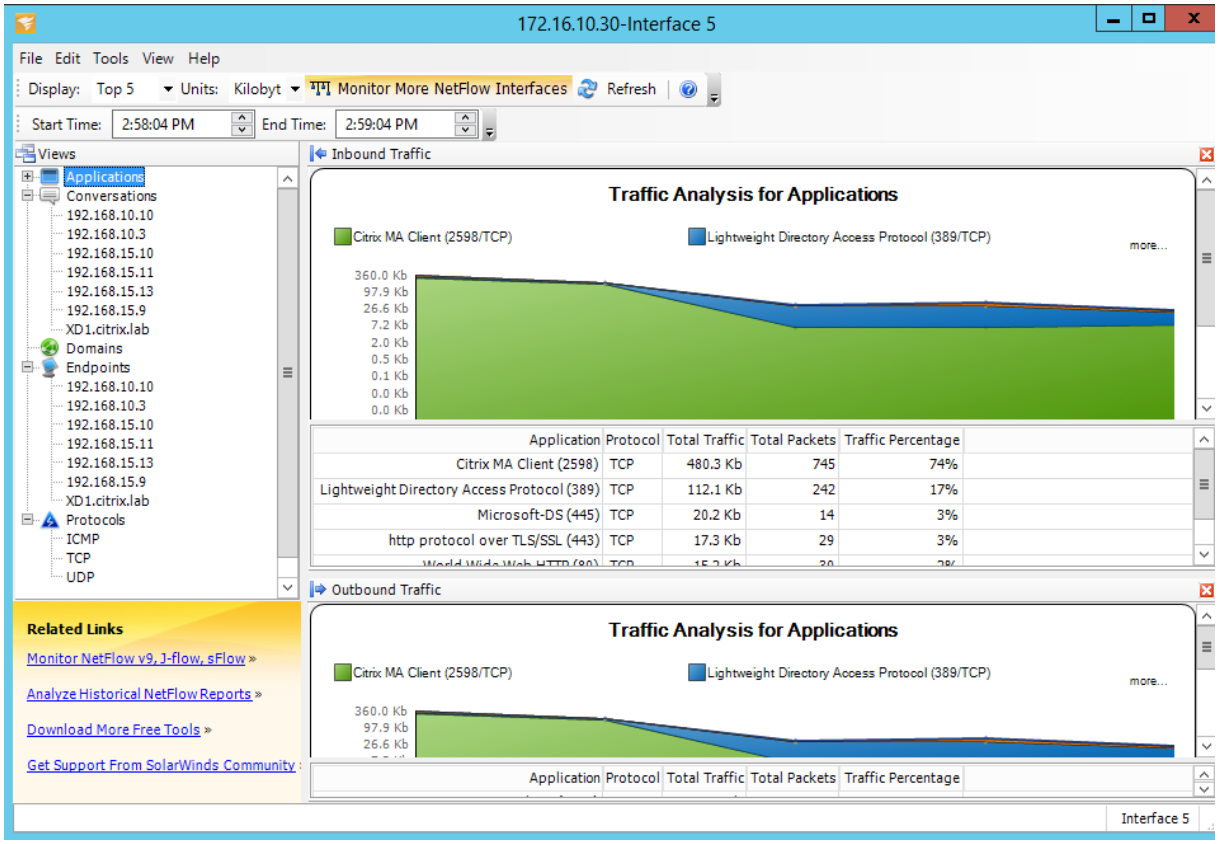
Exportación NetFlow

Los datos de Net Flow se exportan desde el puerto de administración del dispositivo 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Limitaciones de NetFlow

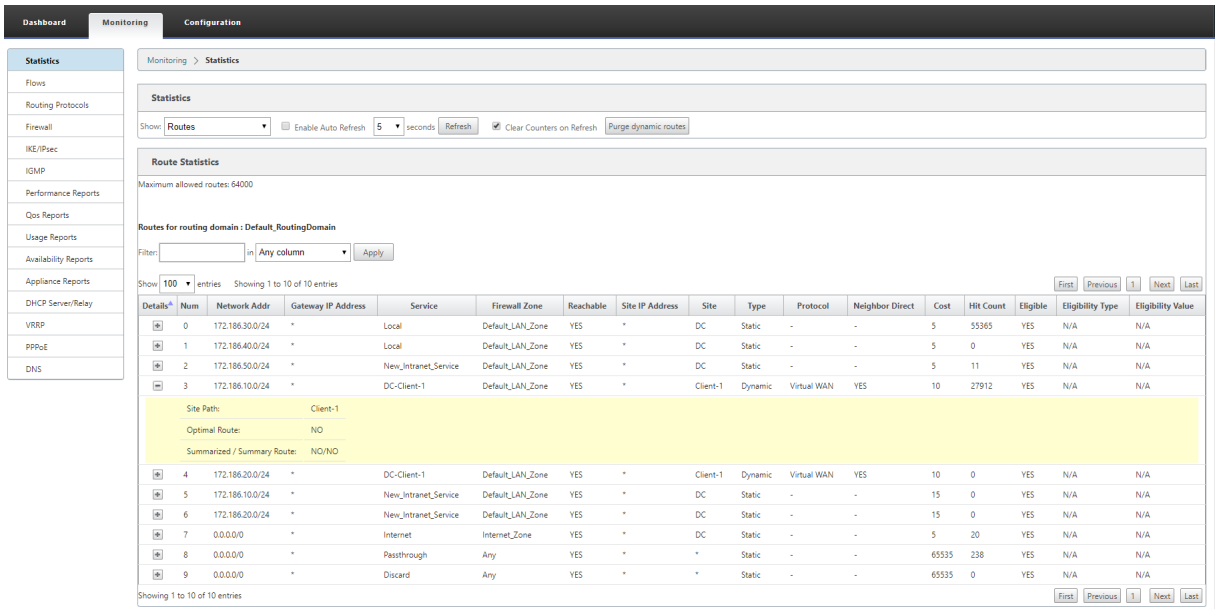
- Con NetFlow habilitado en los dispositivos SD-WAN Standard y Premium (Enterprise) Edition, los datos de Virtual Path se transmiten a los recopiladores de NetFlow designados. Una limitación con esto es que no se puede diferenciar qué enlace WAN físico está siendo utilizado por SD-WAN, ya que la solución 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Estadísticas de rutas

January 10, 2022

Para ver las estadísticas de ruta de los dispositivos SD-WAN, en la GUI de SD-WAN vaya a **Supervisión** > **Estadísticas** > **Rutas**.



Puede ver los siguientes parámetros:

- **Dirección de red**: La dirección de red y la máscara de subred de la ruta.
- **Detalles**: Haga clic en + para mostrar la siguiente información.
  - **Ruta del sitio**: Ruta del sitio es un origen de métrica 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 de estos prefijos y los administradores pueden juzgar los atributos del prefijo al ver la ruta del sitio.

    Por ejemplo, considere una topología simple de Branch1, Branch2 y MCN junto con un Geo MCN. Branch1 tiene un prefijo 172.16.1.0/24 y tiene que llegar a Branch2. Geo MCN y MCN tienen habilitado el reenvío 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 de sitio indica el origen del prefijo de ruta y el coste que implica llegar a Branch2.
  - **Ruta óptima**: La 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 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 que se encuentran debajo de la ruta de resumen.

    Por ejemplo, supongamos que tenemos una ruta de resumen 172.16.0.0/16. Se trata de una ruta de resumen y no de una ruta resumida. Una ruta de resumen tiene Resumen 'SÍ'y Resumido 'NO '. Si hay pocas otras subredes como 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24, estas tres rutas caen bajo la ruta de resumen o la superred y, por lo tanto, se denominan rutas resumidas. Una ruta resumida tiene Resumido SÍ y Resumen NO.

- **Dirección IP de la Gateway**: La dirección IP de la puerta de enlace o ruta utilizada para llegar a esta ruta.
- **Servicio**: El tipo de servicio Citrix SD-WAN.
- **Zona de firewall**: 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 ruta. Las rutas en el 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 del mismo nivel.
  - **OSPF**: Prefijos aprendidos del par de enrutamiento dinámico OSPF.
  - **BGP**: Prefijos aprendidos del par de enrutamiento 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 de acceso a una red de destino.
- Número de**visitas**: Número de veces que se ha usado una ruta para reenviar un paquete a esa subred.
- **Elegible**: Indica que la ruta es elegible y se utiliza para reenviar o enrutar los paquetes al prefijo usado durante el procesamiento del tráfico.
- **Tipo de elegibilidad**: Los dos tipos de elegibilidad siguientes están disponibles.
  - **Elegibilidad de la Gateway**: Determina si la puerta de enlace es accesible o no.
  - **Elegibilidad de la ruta**: Determina si la ruta es DESCONECTADA o NO DESCONECTADA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Valor de elegibilidad**: El valor seleccionado para la Gateway o la ruta en la configuración mientras se crea la ruta en el sistema. Por ejemplo, una ruta puede ser llamada 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

May 7, 2021

Redirección dinámica

Citrix SD-WAN introduce compatibilidad con protocolos de enrutamiento conocidos en la función de **enrutamiento 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 ruta única que se utiliza para representar varias rutas. Ahorra ancho de banda mediante el envío de un anuncio de ruta único, lo que reduce el número de enlaces entre enrutadores. Ahorra memoria porque se mantiene una dirección de ruta. Los recursos de CPU se utilizan de manera más eficiente evitando búsquedas recursivas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VRRP

Virtual Router Redundancy Protocol (VRRP) es un protocolo ampliamente utilizado que proporciona redundancia de dispositivos para eliminar el único punto de error inherente al entorno estático de redirección predeterminado. VRRP le permite configurar dos o más enrutadores 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 el enrutamiento dinámico 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

January 10, 2022

Citrix SD-WAN proporciona conectividad sólida y resistente entre sitios remotos, centros de datos y redes en la nube. La solución SD-WAN puede lograr esto estableciendo túneles entre dispositivos SD-WAN en la red, lo que permite la conectividad entre sitios mediante la aplicación de tablas de ruta que superponen 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 configuración de SD-WAN permite entradas de ruta estáticas para sitios específicos y entradas de ruta aprendidas de la red de calco 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. A continuación se presentan los principales tipos de servicios en uso:

- **Servicio local**: Indica cualquier ruta o subred local para el dispositivo SD-WAN. Esto incluye las subredes de Interfaz Virtual (crea automáticamente rutas locales) 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 se configura esta ruta cuando se confía como asociado.

> **Nota**
>
> Tenga cuidado al agregar rutas predeterminadas y rutas de resumen como rutas locales, ya que pueden dar lugar a rutas de ruta virtual en otros sitios. Compruebe siempre las tablas de redirección para asegurarse de que el enrutamiento correcto esté en vigor.

- **Ruta virtual** : indica cualquier ruta local aprendida desde un sitio SD-WAN remoto. Eso es lo que se puede alcanzar 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 para 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 salto siguiente, 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 a enlaces WAN de Internet públicos en lugar de enlaces WAN privados. Una diferencia única es que el servicio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de Internet puede asociarse con varios enlaces WAN y establecerse en equilibrio de carga (por flujo) o estar activo/copia de seguridad. Una ruta predeterminada de Internet se crea 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 del servicio de Internet se pueden anunciar a los demás dispositivos SD-WAN o impedir que se exporten dependiendo de si se está realizando una copia de seguridad del acceso a Internet a través de las rutas virtuales.

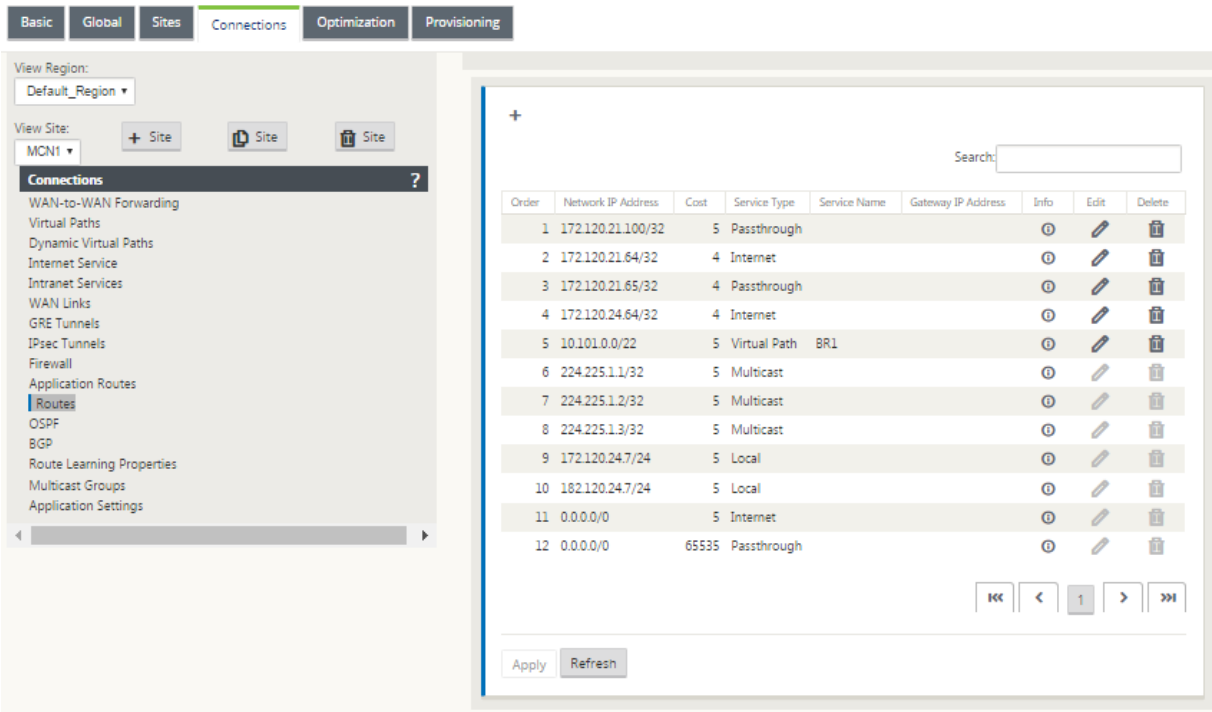
- **Passthrough**: Este servicio actúa como último recurso o reemplaza el servicio cuando un dispositivo está en modo en línea. Si una dirección IP de destino no coincide con cualquier otra ruta, el dispositivo SD-WAN simplemente la reenvía al siguiente salto del enlace WAN. Una ruta predeterminada: El coste 0.0.0.0/0 de 16 rutas de paso se crea automáticamente. El paso a través 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).

  El Editor de configuración de SD-WAN permite la personalización de la tabla de rutas para cada sitio disponible:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



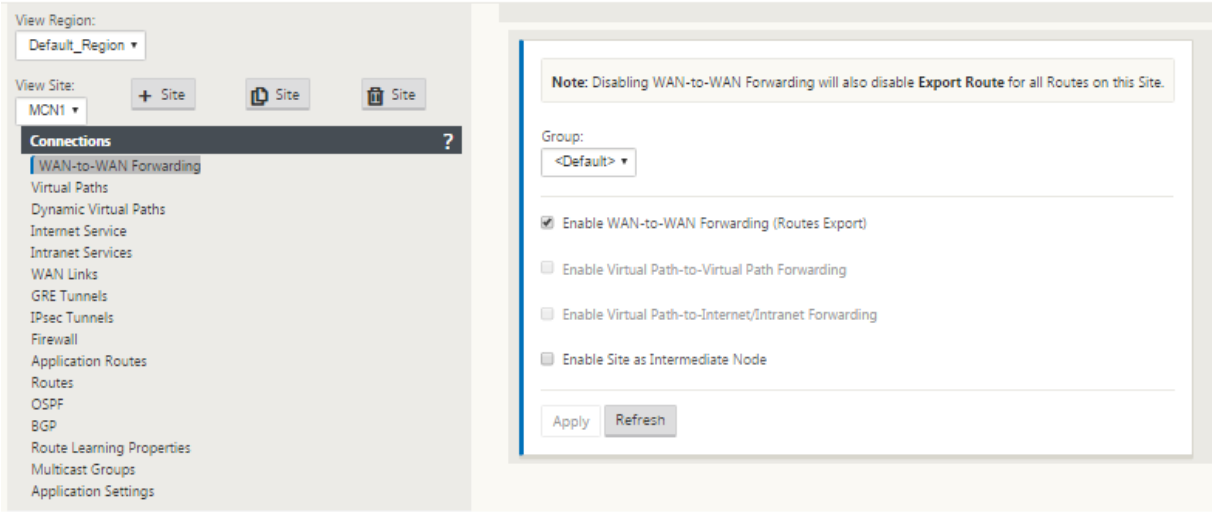
Las entradas de la tabla de rutas se rellenan a partir de diferentes entradas:

- La dirección IP virtual (VIP) configurada se rellena automáticamente como ruta local de tipo de servicio. El Editor de configuración evita la misma asignación VIP a diferentes nodos del sitio.
- Los servicios de Internet habilitados en un sitio local rellenan automáticamente una ruta predeterminada (0.0.0.0/0) localmente para la ruptura directa de Internet.
- El administrador definió rutas estáticas por sitio, que también se definirán como una ruta local de tipo de servicio.
- Un valor predeterminado (0.0.0.0/0) captura todas las rutas con el coste 16 definido como Passthrough

Los administradores pueden configurar una de las rutas anteriores, pero también incluir un tipo de servicio, salto siguiente o Gateway dependiendo del tipo de servicio, además del coste de la ruta. Se agregará automáticamente un coste de ruta predeterminado a cada tipo de ruta (consulte la siguiente tabla para ver los costes de ruta predeterminados). Además, solo las rutas de confianza se anuncian a otros dispositivos SD-WAN. Las rutas que no son de confianza las utiliza el dispositivo local.

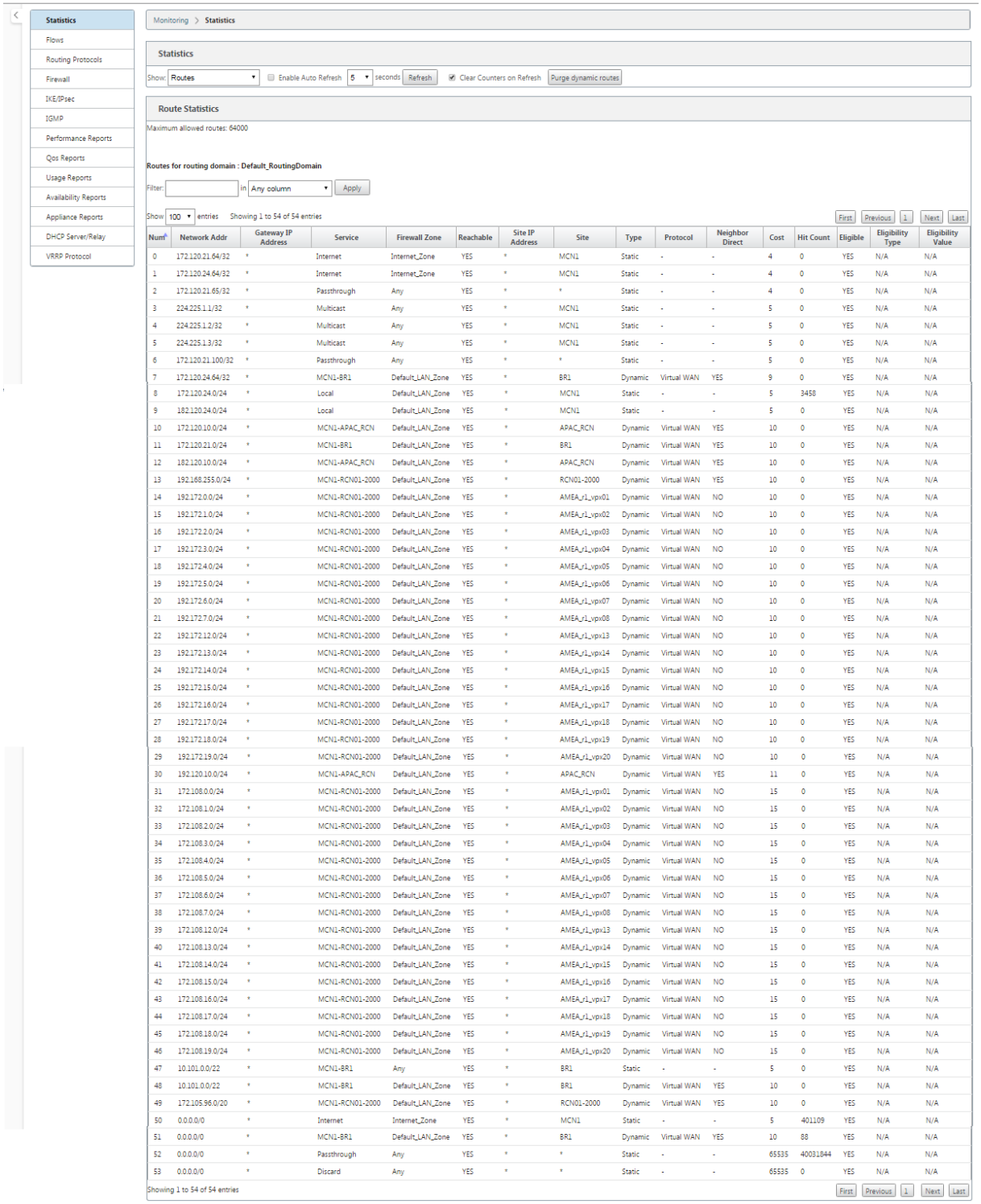
Las rutas de nodo de cliente se anuncian al nodo MCN y no a otros nodos de cliente de forma predeterminada. Para que las rutas de nodo cliente sean visibles para otros nodos cliente WAN to WAN Forwarding debe estar habilitado en el nodo MCN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Con el reenvío WAN a WAN (plantilla de exportación de rutas) habilitado en Configuración global, el sitio de MCN comparte las rutas anunciadas a todos los clientes que participan en la superposición SD-WAN. Al activar esta función, se habilita la conectividad IP entre hosts en diferentes sitios de nodos de cliente con la comunicación que viaja a través del MCN. 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



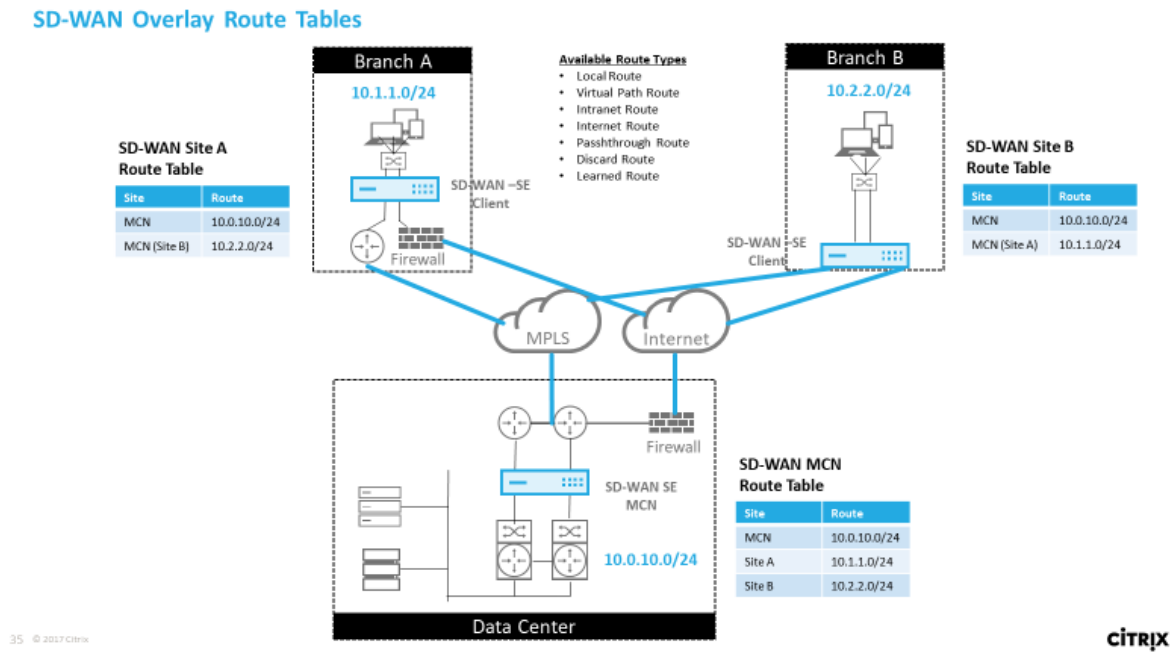
Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
2	172.120.21.65/32	*	Passthrough	Any	YES	*	*	Static	-	-	4	0	YES	N/A	N/A
3	224.225.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.225.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.225.1.3/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
6	172.120.21.100/32	*	Passthrough	Any	YES	*	*	Static	-	-	5	0	YES	N/A	N/A
7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/A
8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	3458	YES	N/A	N/A
9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
10	172.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
11	172.120.21.0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
12	182.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
13	192.168.255.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
14	192.172.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
15	192.172.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
16	192.172.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
24	192.172.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
25	192.172.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
26	192.172.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
28	192.172.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
30	192.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
35	172.108.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
36	172.108.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
46	172.108.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
47	10.101.0.0/22	*	MCN1-BR1	Any	YES	*	BR1	Static	-	-	5	0	YES	N/A	N/A
48	10.101.0.0/22	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
50	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	5	401109	YES	N/A	N/A
51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
52	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 en función del host IP ordenado. El orden de servicio es el siguiente: Local, Ruta virtual, Intranet, Internet, Passthrough, Descartar.

Como ejemplo, considere las dos rutas siguientes:

- 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 ruta de tráfico LAN a WAN (ruta virtual):
  1. El tráfico entrante es recibido por la interfaz LAN y se procesa.
  2. El marco recibido se compara con la tabla de enrutamiento 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 ruta de tráfico de WAN a LAN (ruta virtual):
  1. El tráfico de ruta virtual es recibido por SD-WAN 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 enrutamiento 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, se facilitó la configuración de las subredes indicadas para hacer uso de la superposición 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 quiereda, si no tienes cuidado.

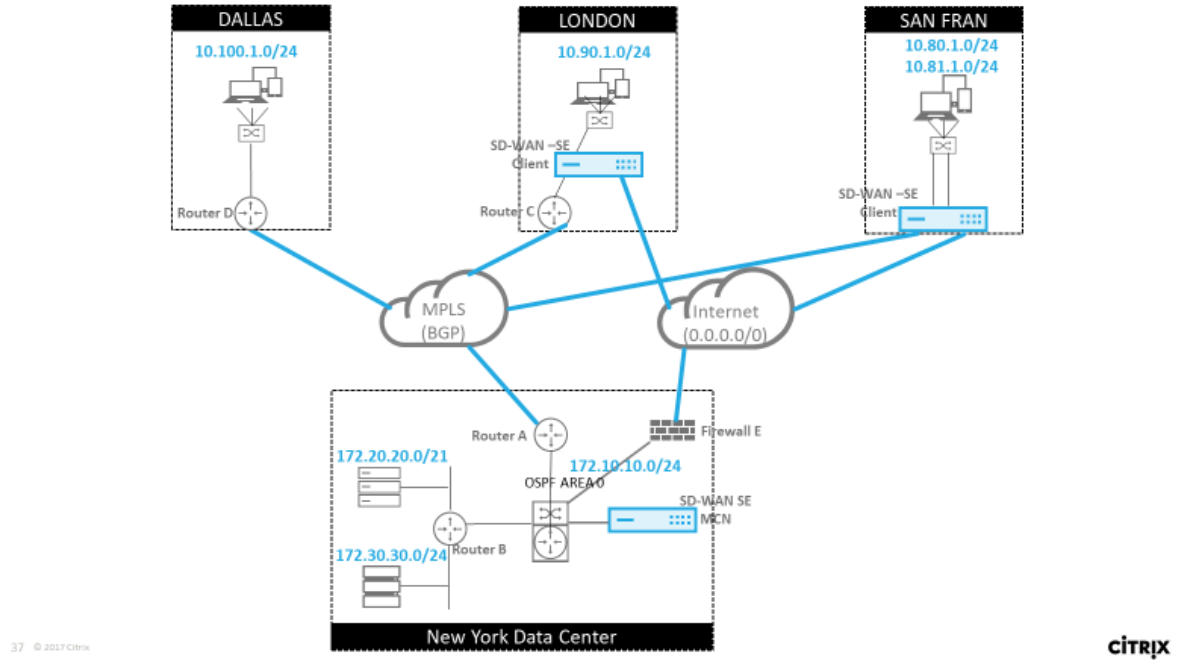
La tabla de ruta de ruta de ruta virtual de SD-WAN funciona como un protocolo de puerta de enlace externa (EGP), similar a BGP (pensar sitio a sitio). Por ejemplo, cuando SD-WAN anuncia rutas desde el dispositivo SD-WAN a OSPF, normalmente se consideran externas al sitio y al protocolo.

> **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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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, tenemos que considerar la mejor manera de integrarlo con los protocolos de ruta existentes a ese sitio para garantizar una conectividad completa entre las redes de superposición de capas subyacentes y 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 el SD-WAN se implementa en modo Virtual Inline. 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 despliega en modo tradicional en línea. El router WAN ascendente (C) seguirá siendo la Gateway predeterminada para la subred de Londres.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El sitio de San Francisco es un sitio recientemente introducido en esta red y se planea implementar SD-WAN en modo Edge/Gateway y actuar como la Gateway 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:

```
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, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
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
```

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 Dallas (10.90.1.0/24) y London (10.100.1.0/24) están disponibles a través de 172.10.10.1 (MPLS Router A). Los costes de 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 más bajo y coste por defecto 20/1 en comparación con OSPF 110/10.

Router D de Dallas:

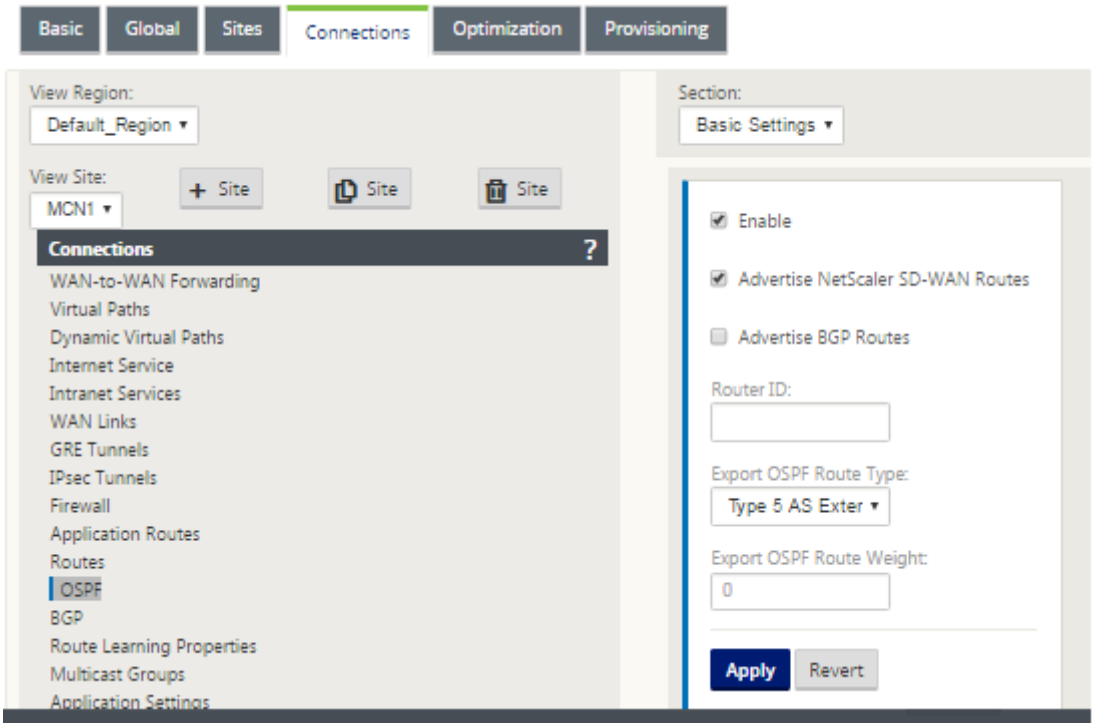
Para Dallas WAN Router (D), todas las rutas se aprenden a través de MPLS.

```
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.

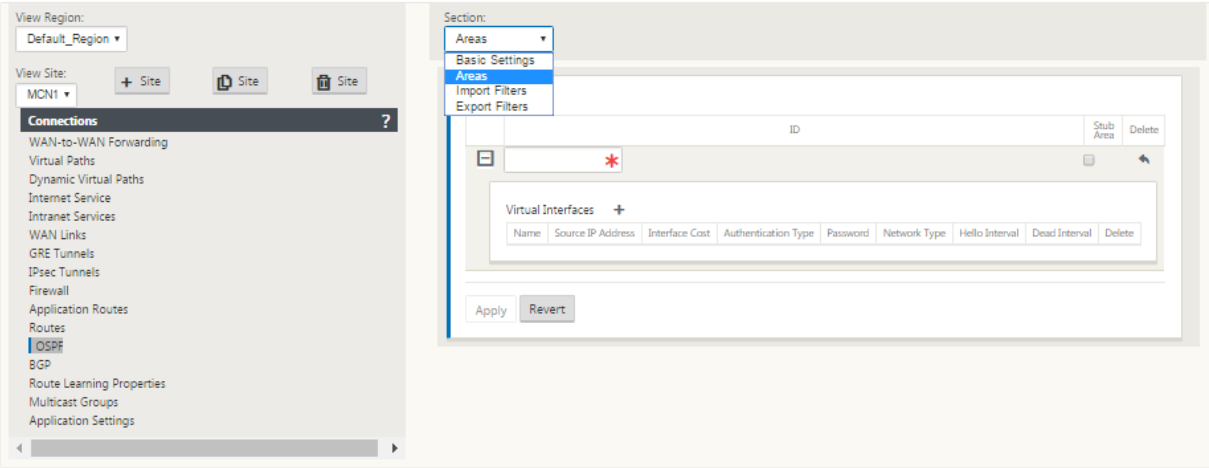
En Citrix SD-WAN, podemos agregar la superposición SD-WAN habilitando OSPF en la SD-WAN ubicada en el sitio de Nueva York, en **Conexiones** > **Ver sitio** > **OSPF** > **Configuración básica** :

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> El **tipo de ruta OSPF de exportación** es de tipo 5 externo de forma predeterminada. Esto se debe a que la tabla de redirección SD-WAN se considera externa al protocolo OSPF y, por lo tanto, OSPF preferirá una ruta aprendida interna (intra-area), por lo que las rutas anunciadas por SD-WAN podrían no tener prioridad.

Cuando se utiliza OSPF a través de la WAN (es decir, redes MPLS), esto se puede cambiar a Tipo uno dentro del área. Las áreas OSPF se pueden configurar de la siguiente manera.

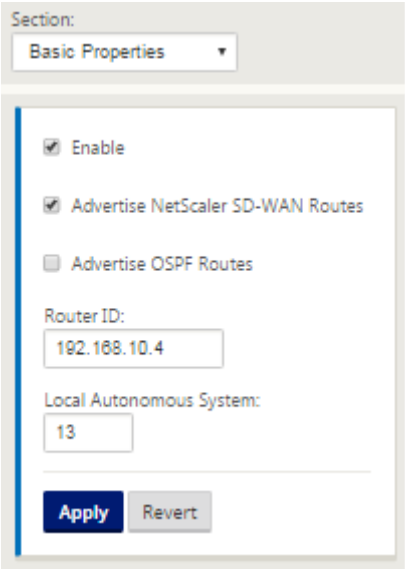


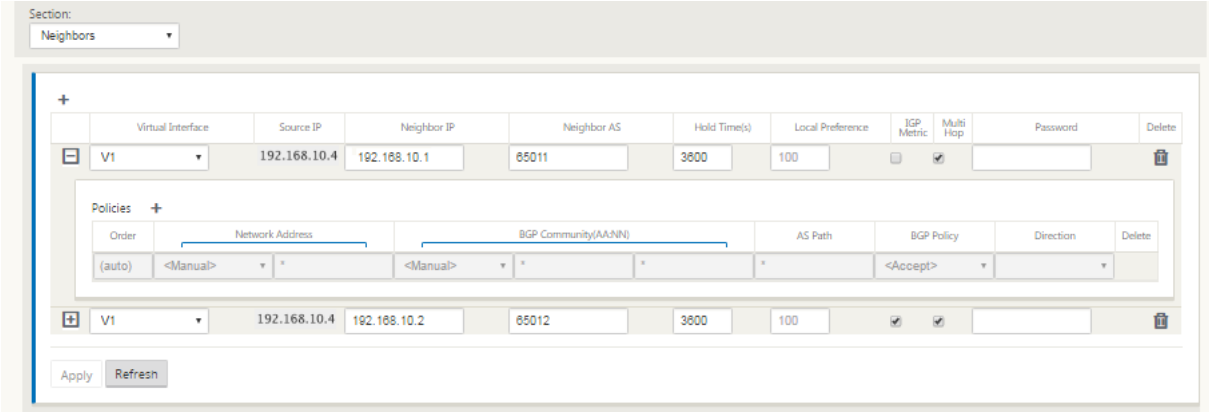
Área 0 agregada con la red local derivada de la interfaz virtual (172.10.10.0), todas las demás configuraciones se dejaron por defecto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para el nuevo sitio de San Francisco, necesitamos habilitar eBGP ya que se conectará directamente a la red MPLS y funcionará como la ruta de borde del cliente para el sitio. BGP se puede habilitar en **Conexiones** > **Ver sitio** > **BGP** > **Configuración básica.**

Tenga en cuenta el número del sistema autónomo 13.





El eBGP se empareja con cada ubicación. Cada ASN es diferente.

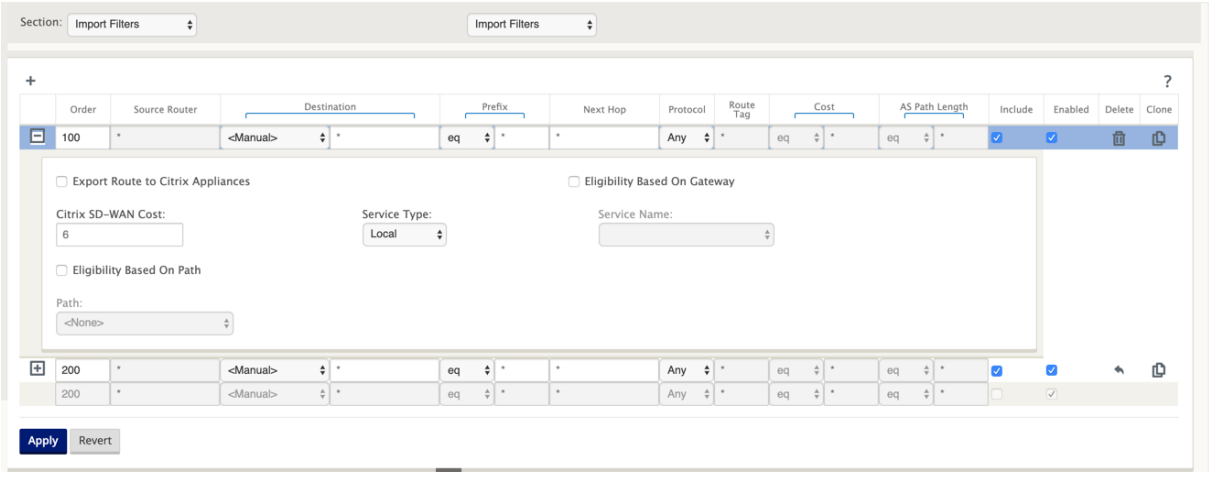
Es importante comprender cómo se pasan las rutas entre la tabla de redirección de ruta virtual y los protocolos de ruta dinámica en uso. Es fácil crear bucles de redirección o anunciar rutas de una manera adversa. El mecanismo de filtro nos da la capacidad de controlar lo que entra y sale de la tabla de redirección. Consideramos cada lugar 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

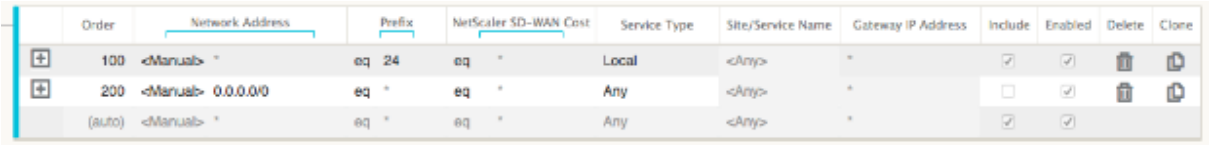
volver a anunciar nada que SD-WAN aprenda de eBGP a los routers SD-WAN. Para lograr esto, los filtros deben configurarse de la siguiente manera:

- Importe todas las rutas desde eBGP. No leer/exportar rutas a dispositivos SD-WAN.



- Exportar rutas locales a eBGP

La regla predeterminada para exportar es exportar todo. La regla 200 se utiliza para anular la regla de error y 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 están viendo correctamente a través de eBGP desde la SD-WAN de San Francisco.

Enrutador D de Dallas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 ya

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

que 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.

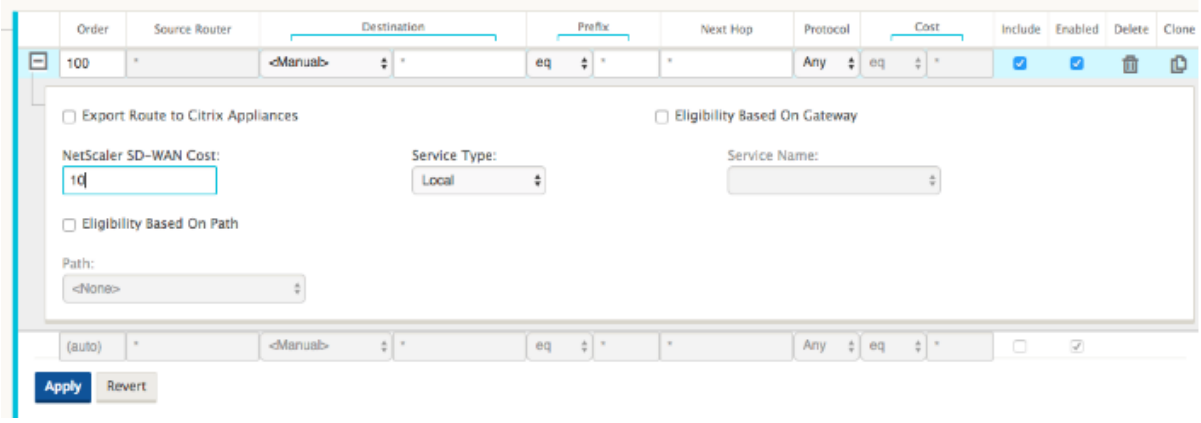
- Como ruta anunciada a través de BGP (Número 6), con un coste de 6. Ahora se considera una ruta alternativa.

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.

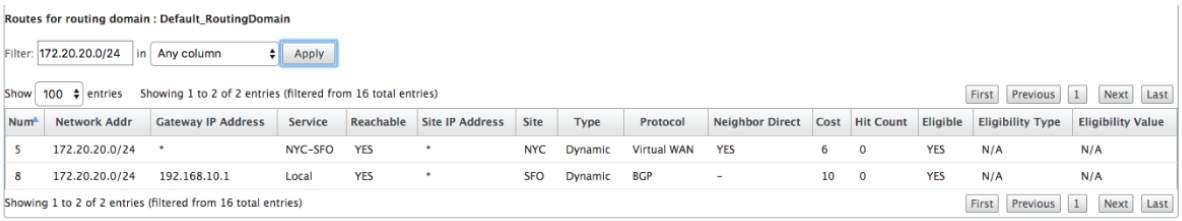
Ahora, consideremos la ruta 172.20.20.0/24.

- 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 puede ser preferida sobre la ruta de ruta virtual.

Para garantizar el enrutamiento correcto, 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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Finalmente, echemos un vistazo a la ruta predeterminada aprendida en la SD-WAN de San Francisco. Queremos traspasar 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 eliminar. 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 de borde/puerta de enlace, no hay servicio de paso, en cuyo caso SD-WAN descarta el paquete mediante la ruta de descarte predeterminada. El número de visitas indica el número de paquetes que están llegando a cada ruta, lo que puede ser valioso a la hora de 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 esté activa.

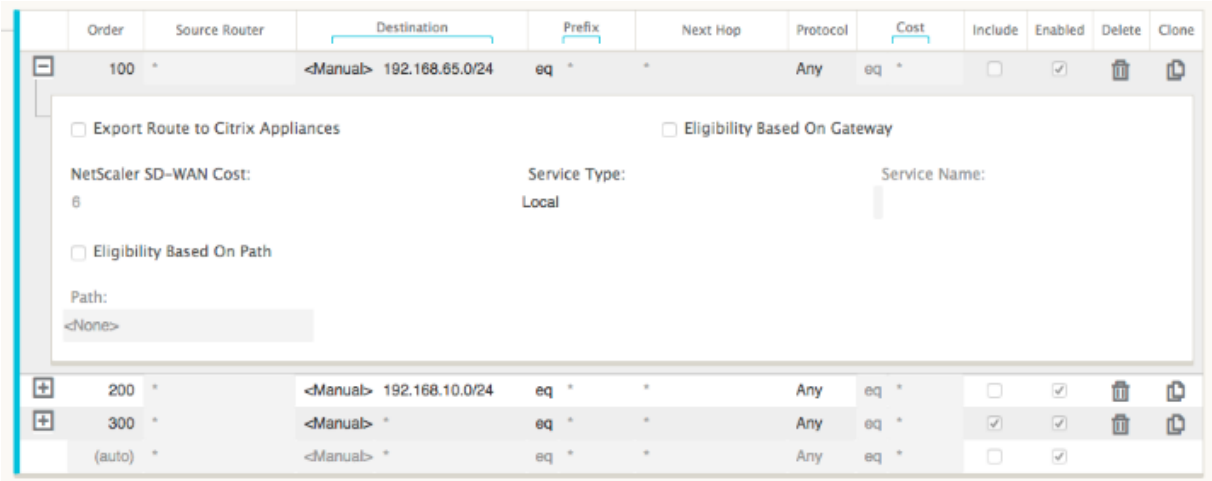
Hay varias subredes disponibles en el sitio de Nueva York:

- 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)

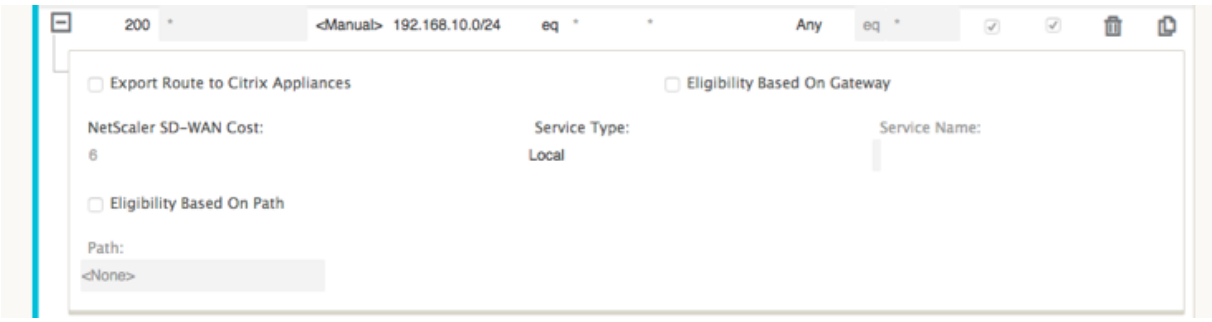
También estamos obligados a proporcionar flujo de tráfico a Dallas (10.100.1.0/24) a través de MPLS.

Por último, queremos que toda la ruta de tráfico enlazada a Internet al Firewall E a través de 172.10.10.3 como salto siguiente. SD-WAN aprende esta ruta predeterminada a través de OSPF y para anunciar a través de la ruta virtual. Los filtros para el sitio de Nueva York son:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

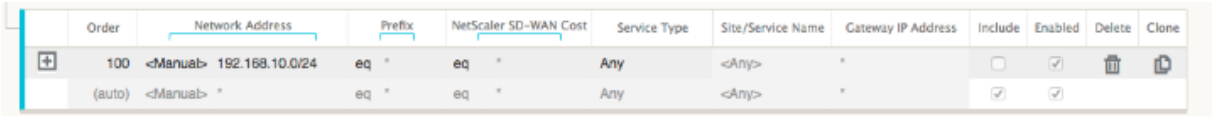


El sitio SD-WAN de Nueva York importa todas las rutas para la red de administración. Esto puede ser ignorado. Podemos centrarnos en el filtro 200.



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. Active la casilla de verificación **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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 todavía se está anunciando a través del subcalco MPLS Router A. Revisemos la tabla de rutas SD-WAN 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 puerta trasera para forzar 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 enrutar al dispositivo SD-WAN del sitio de Nueva York si la ruta de acceso MPLS falla. Dado que hay una ruta para el 10.90.1.0/24 que se anuncia a través de 172.10.10.10 (Nueva York SD-WAN). También se recomienda crear una regla de servicio de anulación para eliminar cualquier paquete UDP 4.980 en el dispositivo SD-WAN para evitar que la ruta virtual vuelva a sí misma.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Rutas virtuales dinámicas

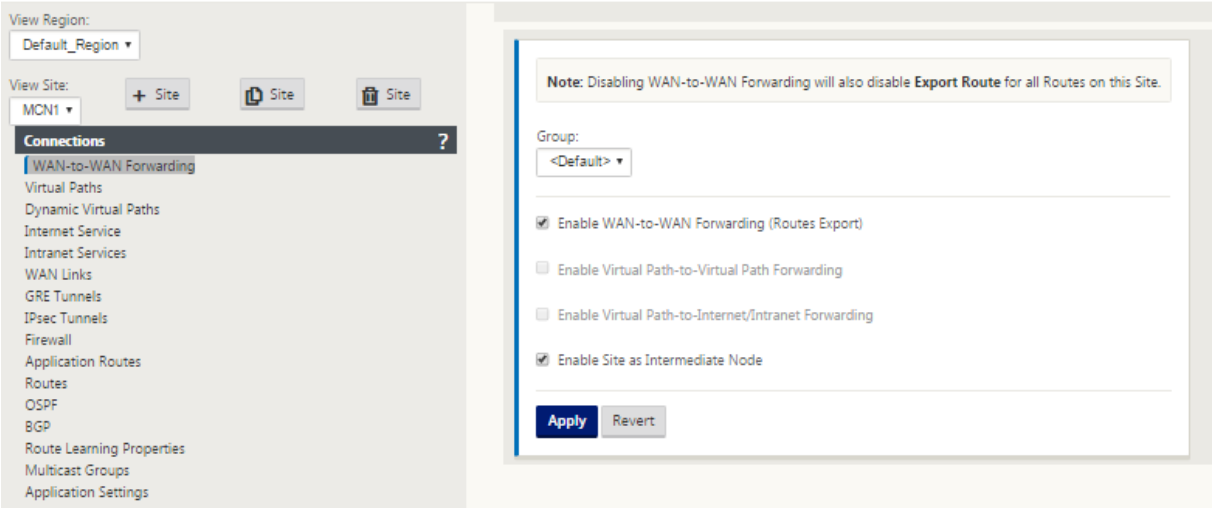
Se pueden permitir rutas virtuales dinámicas entre dos nodos de cliente para crear rutas virtuales bajo demanda para la comunicación directa entre los dos sitios. La ventaja de una ruta virtual dinámica es que el tráfico puede fluir directamente de un nodo cliente al segundo sin tener que atravesar el MCN o dos rutas virtuales, lo que podría 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 dinámica de superposición SD-WAN de malla completa.

Una vez que se cumplen los umbrales de rutas virtuales dinámicas, los nodos cliente crean dinámicamente su ruta virtualizada entre sí mediante todas las rutas WAN disponibles entre los sitios y lo utilizan al máximo de la siguiente manera:

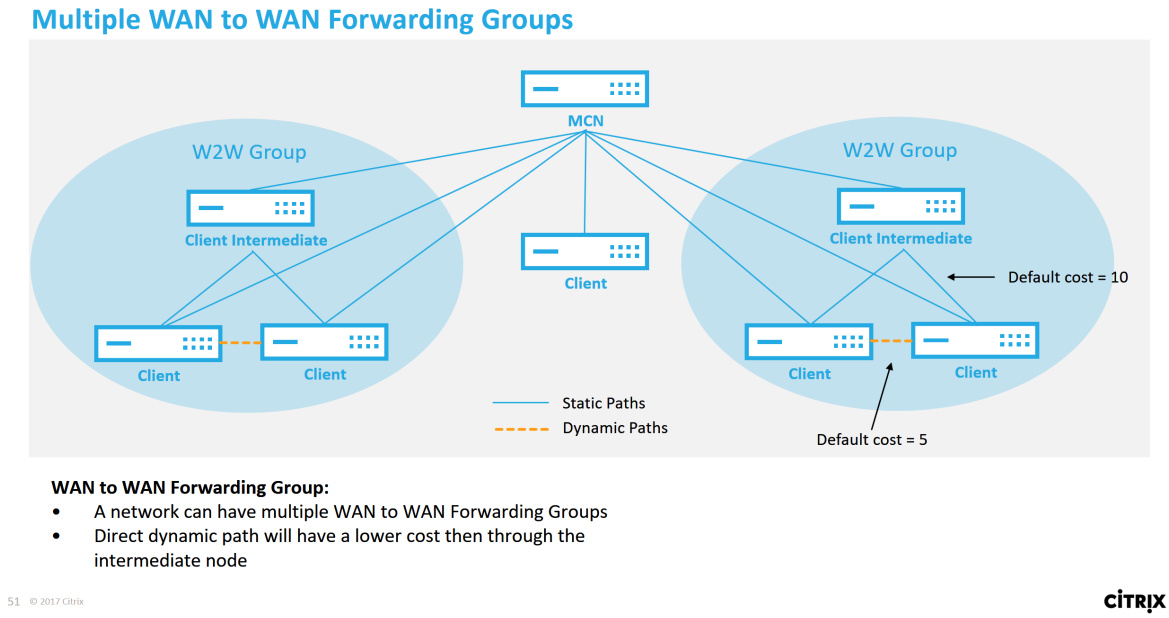
- Envíe datos masivos si existe alguno y verifique que no haya pérdida, entonces
- Envíe datos interactivos y verifique que no haya pérdida, entonces
- Enviar datos en tiempo real después de que los datos masivos e interactivos se consideren estables (sin pérdidas ni niveles aceptables)
- Si no hay datos 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 podría ser un sitio MCN o cualquier otro sitio de la red que tenga una ruta virtual estática configurada y conectada a dos o más nodos de 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. **Habilitar sitio como nodo intermedio** debe estar habilitado además del **reenvío WAN** a WAN para que este sitio intermedio supervise la comunicación del nodo cliente y dicte cuándo debe establecerse y desactivarse la ruta dinámica.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

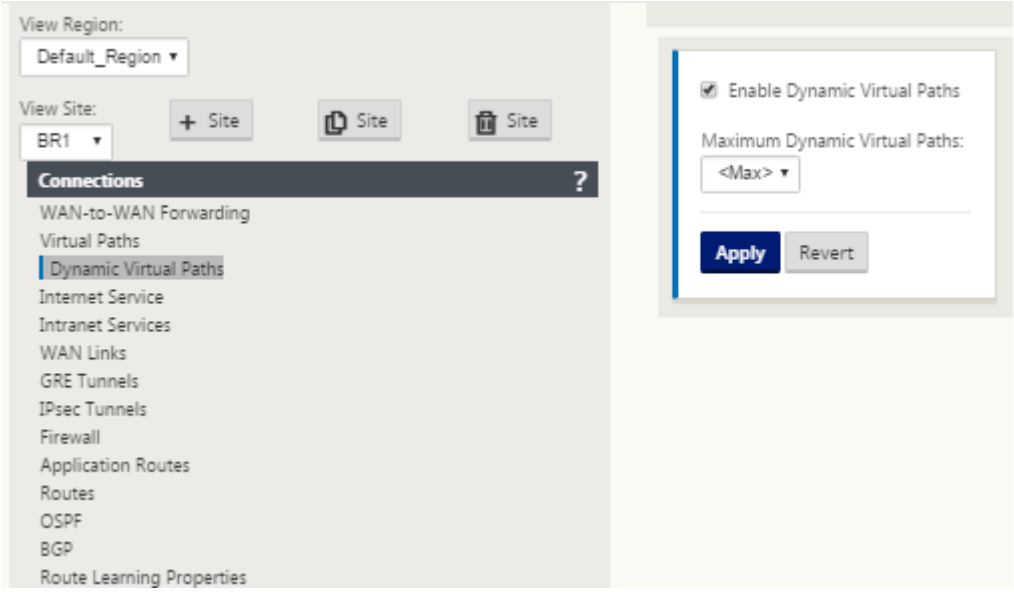


Se pueden permitir varios grupos de reenvío de WAN a WAN en la configuración de SD-WAN, lo que permite el control total del establecimiento de rutas entre determinados nodos de cliente y no entre otros.



Para que los nodos de cliente funcionen como sitios intermedios, se requiere que se configure una ruta virtual estática entre ella y los clientes asociados a ese **grupo de reenvío de WAN a WAN**. Además, los nodos de cliente necesitan la opción **Habilitar ruta virtual dinámica** activada para cada nodo de cliente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cada dispositivo SD-WAN tiene su propia tabla de rutas única con los siguientes detalles definidos para cada ruta:

- Num: Orden de ruta de este dispositivo basado en el proceso de coincidencia (el número más bajo procesado primero)
- Dirección de red: Dirección de subred o host
- Puerta de enlace si es necesario
- Servicio: Qué servicio se aplica para esta ruta
- Zona del firewall: Clasificación de la zona del firewall de la ruta
- Accesible: Identifica si el estado de ruta virtual está activo para este sitio
- Sitio: El nombre del sitio donde se espera que exista la ruta
- Tipo: Identificación del tipo de ruta (estático o dinámico)
- Vecino directo
- Coste - coste de la ruta específica
- Número de visitas: Cuántas veces se ha utilizado la ruta por paquete. Esto se usaría para verificar que una ruta se está usando correctamente.
- Elegible
- Tipo de elegibilidad
- Valor de elegibilidad

A continuación se muestra un ejemplo de tabla de ruta del sitio SD-WAN:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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: Estas 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 inexistente 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 hacer coincidir el tráfico de entrada 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ruta 12 —Descartar es la ruta predeterminada que el sistema siempre agrega para soltar cualquier cosa indefinida.

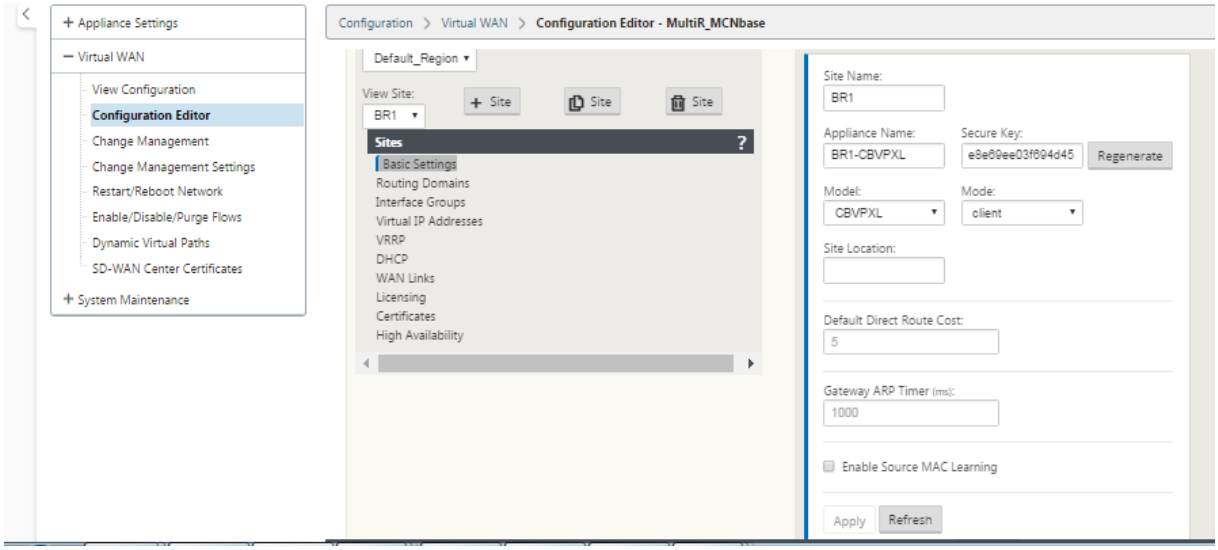
Valores de coste de ruta predeterminados:

- 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 un nivel de servicio

Después de definir estas rutas, es importante entender cómo fluye el tráfico mediante las rutas definidas. Estos flujos de tráfico se dividen en los siguientes flujos:

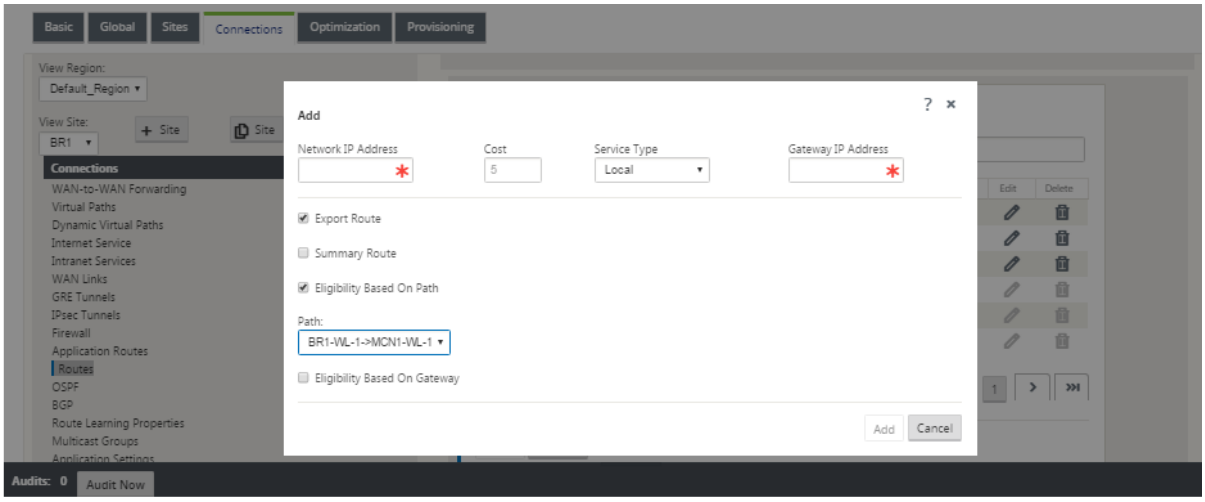
- LAN a WAN (Ruta Virtual): Tráfico que entra en el túnel de superposición SD-WAN
- WAN a LAN (Ruta Virtual): Tráfico existente en el túnel de superposición SD-WAN
- Tráfico de ruta no virtual: Tráfico enrutado a la red de calco subyacente

El coste de ruta predeterminado se puede modificar en función de cada sitio. La configuración se puede encontrar en **Ver sitio** > **Configuración básica** :

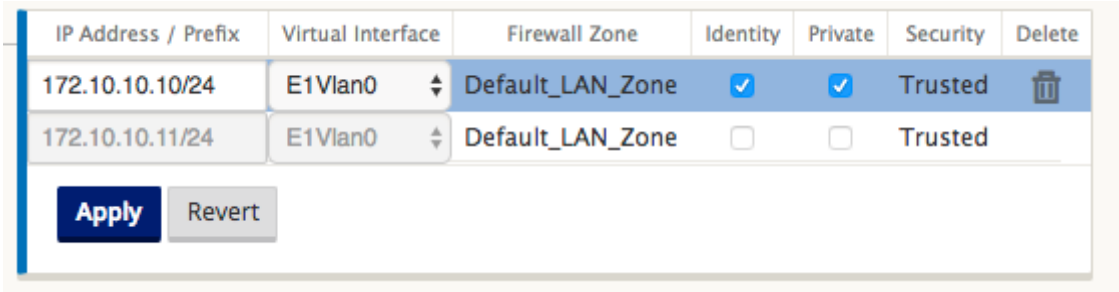


Las rutas estáticas se pueden definir por sitio en el nodo **Conexiones** > **Sitio** > **Ruta** s:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Observe que las rutas se pueden vincular a la disponibilidad de IP de la ruta virtual o de la puerta de enlace. Las rutas de Internet se pueden exportar a la superposición Ruta virtual o no dependiendo del comportamiento quieredo. También puede crear rutas de ruta virtual estáticas para forzar el tráfico a una ruta virtual aunque no recibamos el prefijo anunciado a SD-WAN (es decir, una ruta de último recurso de mayor coste). SD-WAN también puede suprimir la publicidad de subredes locales haciendo privada la dirección IP virtual (VIP).



> **Nota**
>
> La configuración requiere al menos un VIP no privado en cada dominio de ruta.

Intranet y rutas de Internet

Para los tipos de servicio 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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Intranet/Internet debe tener una Gateway 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 quieredo
- Las tablas de redirección son estáticas a menos que la función de aprendizaje de rutas esté habilitada

  El siguiente es el límite máximo admitido para varios parámetros de redirección:

- Dominios de enrutamiento máximos: 255
- Máximo de interfaces de acceso por enlace WAN: 64
- Número máximo de vecinos BGP por sitio: 255
- Superficie máxima de OSPF por emplazamiento: 255
- Máximo de interfaces virtuales por área OSPF: 255
- Máximo de filtros de importación de Route Learning por sitio: 512
- Máximo de filtros de exportación de Route Learning por sitio: 512
- Máximo de directivas de redirección BGP: 255
- Máximo de objetos de cadena de comunidad BGP: 255

Dominio de enrutamiento

May 7, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 interfaz
  - 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 vínculo de Internet público, se puede crear una interfaz de acceso primaria y secundaria.
- Para un vínculo Intranet/MPLS privado, se puede crear una interfaz de acceso primaria y secundaria por dominio de enrutamiento.

Configurar dominio de enrutamiento

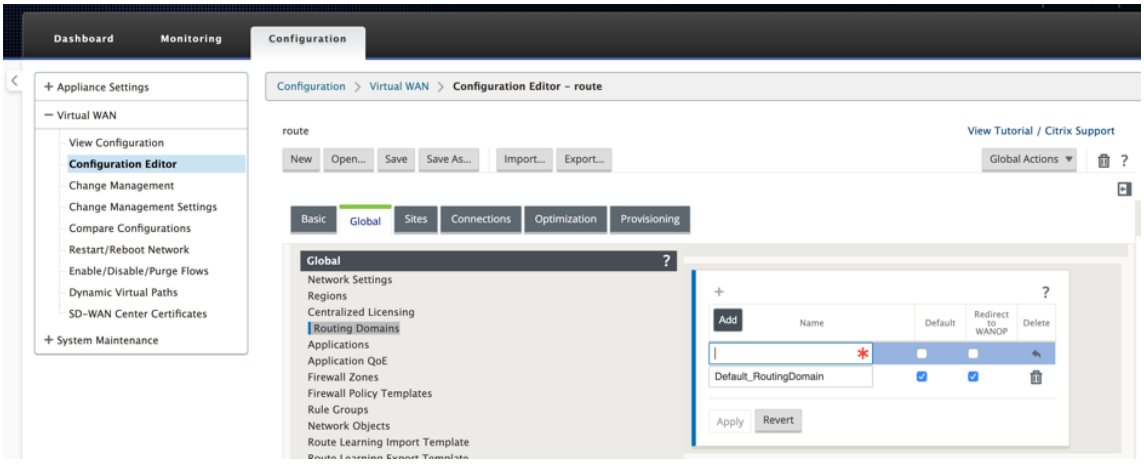
May 7, 2021

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.

Para configurar el dominio de redirección:

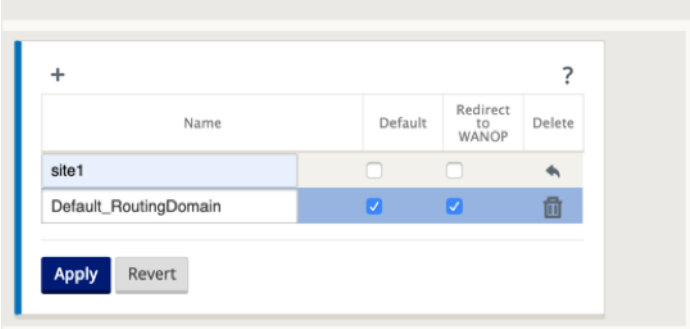
1. En la interfaz web de SD-WAN, vaya a **Configuración** > **Virtual WAN** > **Editor de configuración**. En el **Editor de configuración**, vaya a **Global**> **Redirección de dominios**, haga clic en **Agregar (+)**e introduzca un nombre para su nuevo dominio de enrutamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Si quiere establecer de forma predeterminada este dominio de enrutamiento, haga clic en la casilla de verificación **Predeterminado**. Haga clic en **Aplicar** para guardar los cambios. Si planea implementar un único dominio de redirección, no se requiere ninguna configuración explícita.

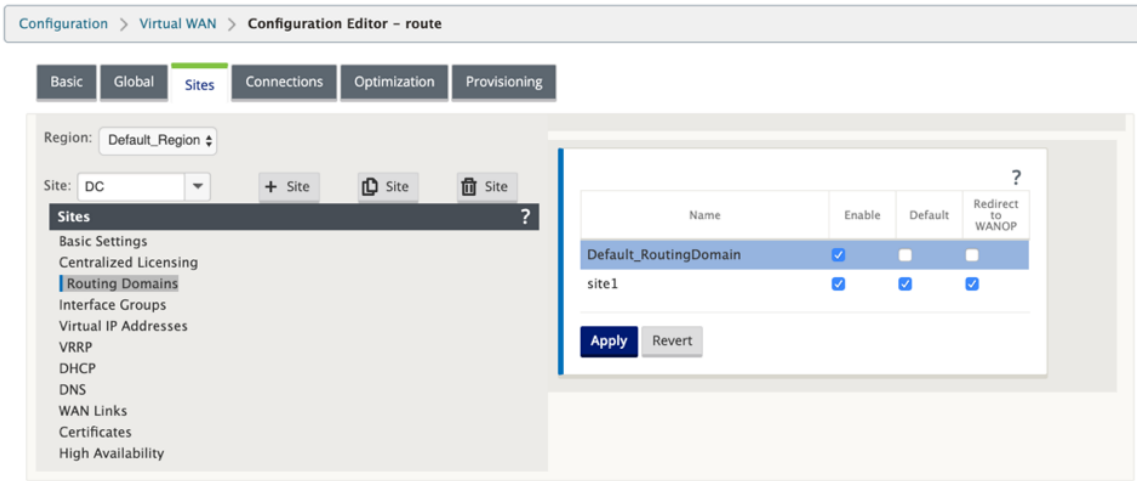
   Todas las configuraciones nuevas se rellenan automáticamente con un dominio de redirección predeterminado.



3. Desplácese hasta **Sitios** → **[Nombre del sitio del cliente]** > **Dominios de enrutamiento**. Haga clic en la casilla de verificación **Habilitar** para habilitar un dominio de enrutamiento configurado para el sitio.

4. Haga clic en la casilla de verificación **Predeterminado** para que el dominio de enrutamiento sea el predeterminado para el sitio. Haga clic en **Aplicar** para guardar los cambios.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Al desactivar **Habilitar** para un dominio de enrutamiento, no estará disponible para su uso en el sitio.

Con la versión 11.0.2, se permite el **enrutamiento de dominios sin IP virtuales (VIPs) enrutables** 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.

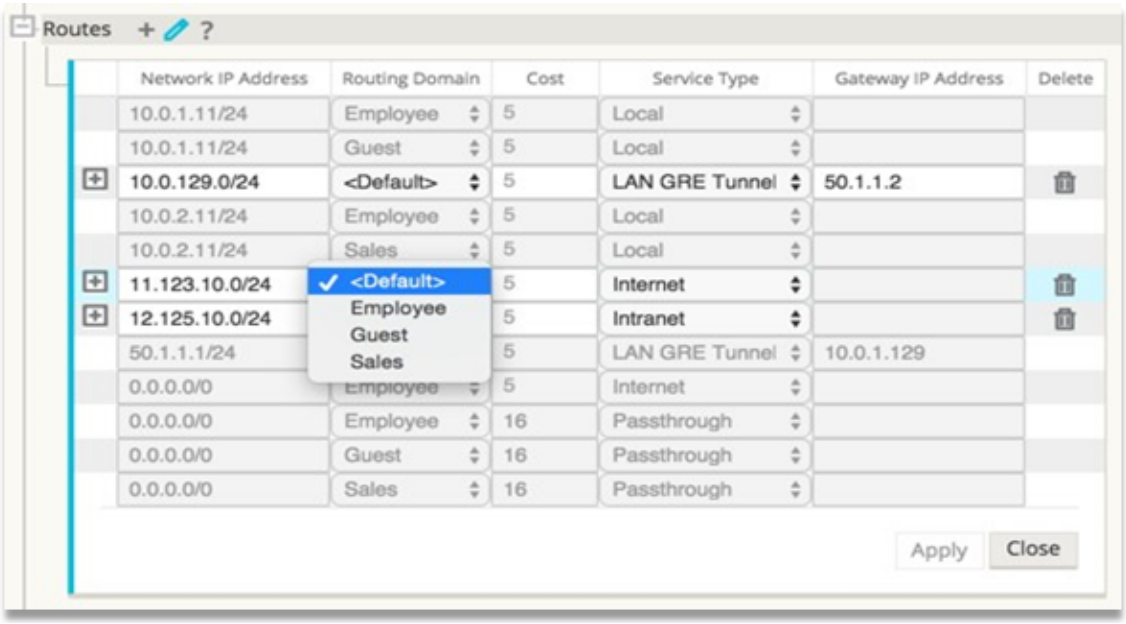
Configurar rutas

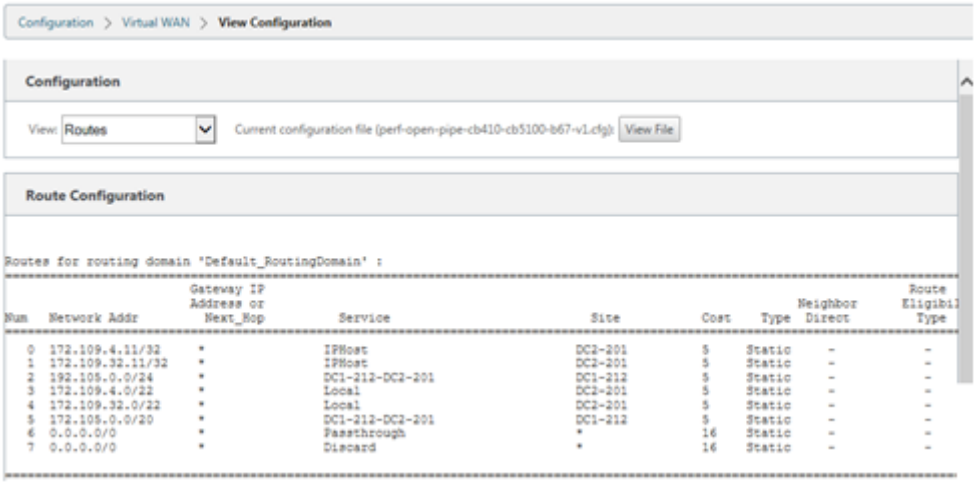
May 7, 2021

Para configurar rutas:

1. En el **Editor de configuración**, vaya a **Conexiones**> **[Nombre del sitio]**> **Rutas**.
2. Elija un **dominio de enrutamiento** en el menú implementable. Las nuevas rutas se asocian automáticamente con el dominio de enrutamiento predeterminado. Para obtener instrucciones detalladas, consulte Configuración de Rutas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





Después de configurar rutas, valide las tablas de enrutamiento para el dominio de enrutamiento configurado navegando a **Configuración** > **WAN virtual** > **Ver** > **Rutas**.

Usar CLI para acceder al enrutamiento

May 7, 2021

En la versión 10.0 de Citrix SD-WAN, puede ver información adicional relacionada con el enrutamiento dinámico y el estado del protocolo. Escriba el siguiente comando y sintaxis para acceder al demonio de enrutamiento y ver la lista de comandos.

```
dynamic_routing?
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Redirección dinámica

May 7, 2021

Citrix SD-WAN admite los siguientes dos protocolos de redirección dinámica:

- Abrir primero la ruta más corta (OSPF)
- Protocolo de puerta de enlace de frontera (BGP)

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 versión temprana 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 está en el dominio público (RFC 1247). OSPF se basa en el algoritmo de ruta más corta primero (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 las interfaces adjuntas, las métricas utilizadas y otras variables se incluyen 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.

Ahora puede configurar dispositivos Citrix SD-WAN (ediciones estándar y premium (Enterprise)) para conocer rutas y anunciar rutas mediante OSPF.

> **Nota**
>
> - Los dispositivos Citrix SD-WAN no participan como enrutador designado (DR) y BDR (enrutador designado de copia de seguridad) en cada red de acceso múltiple, ya que la prioridad de DR predeterminada se establece en “0.”
> - El dispositivo Citrix SD-WAN no admite el resumen como enrutador de borde de área (ABR).

Configurar OSPF

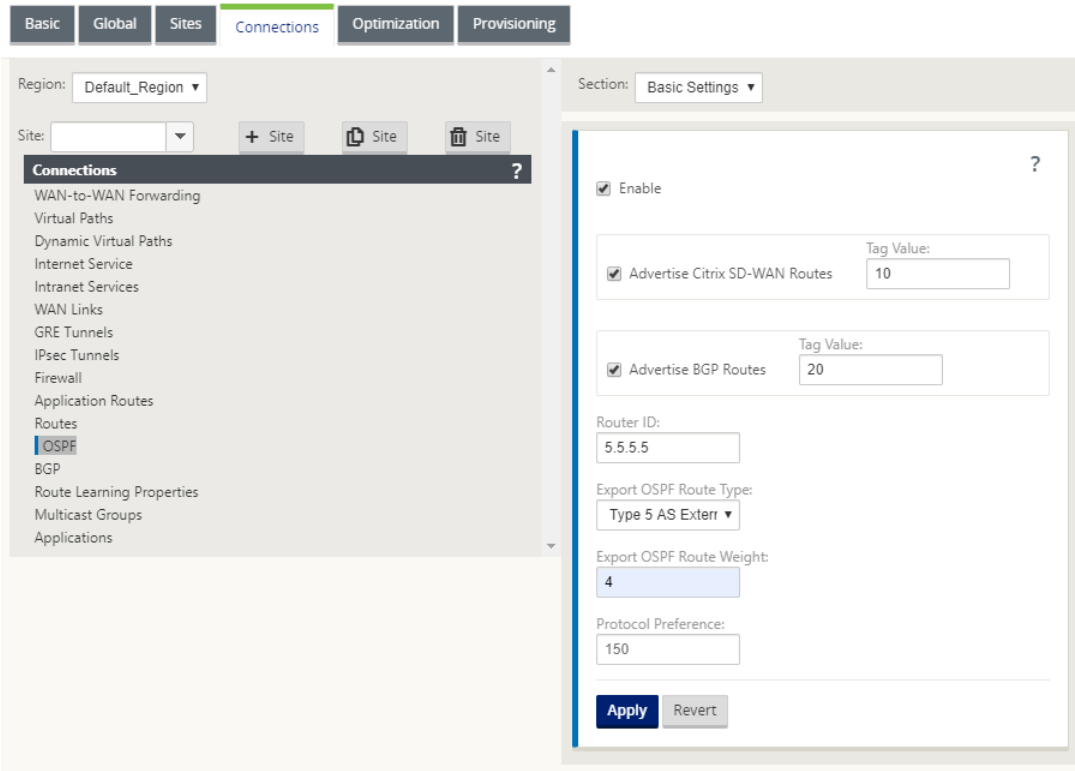
Para configurar OSPF:

1. En el **Editor de configuración**, vaya a **Conexiones > Región > Sitio > OSPF > Configuración básica**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

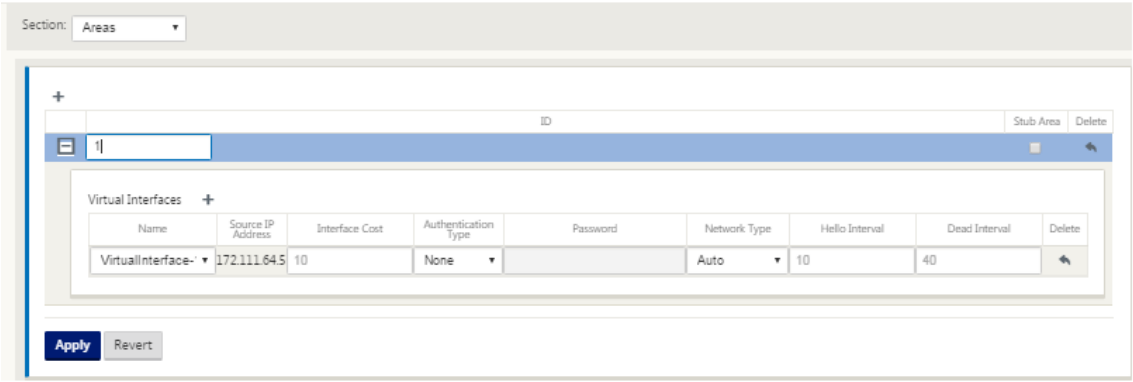
2. Haga clic en **Habilitar**, seleccione o introduzca valores para los siguientes parámetros y haga clic en **Aplicar**.

   - **Anunciar rutas de Citrix SD-WAN**: Permita que las rutas de Citrix SD-WAN se publiquen a través de OSPF. También puede especificar una etiqueta para la redistribución OSPF.
   - **Anunciar rutas BGP**: Permitir que las rutas aprendidas de los pares BGP se publiquen a través de OSPF. También puede especificar una etiqueta para la redistribución OSPF.
   - **Id. de enrutador**: Identificador único del enrutador, el enrutador se utiliza para anuncios OSPF. Si no se especifica el ID del enrutador, se selecciona automáticamente como la IP virtual más baja alojada en la red SD-WAN.
   - **Exportar tipo de ruta OSPF**: Anuncie las rutas Citrix SD-WAN a los pares OSPF como rutas dentro del área o rutas externas.
   - **Exportar peso de ruta OSPF**: Al exportar rutas Citrix SD-WAN a OSPF, agregue este peso al coste SD-WAN de cada ruta.
   - **Preferencia de protocolo**: Si los prefijos se aprenden a través de varios protocolos de enrutamiento, el valor de preferencia de protocolo determina la selección del protocolo de enrutamiento. Para obtener más información, consulte Preferencia de protocolo.



3. Expanda **OSPF** > **Área** y haga clic en **Modificar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



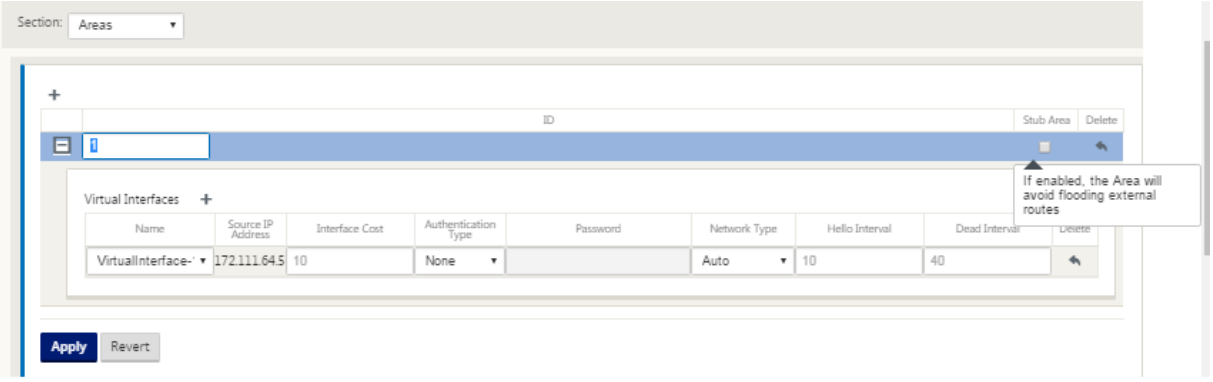
4. Introduzca un **ID de área** para conocer las rutas y anunciarse a.
5. Si Identity no está marcada para una dirección IP virtual específica, la interfaz virtual asociada no está disponible para los servicios IP.
6. Elija una de las interfaces virtuales disponibles en el menú **Nombre**. La interfaz virtual determina la **dirección IP de origen**.
7. Introduzca el **coste de interfaz** (10 es el valor por defecto).
8. Elija un **tipo de autenticación** en el menú.
9. Si ha seleccionado **Contraseña** o **MD5** en el paso 8, introduzca el campo de texto asociado Contraseña.
10. En el campo **Intervalo de saludo**, introduzca la cantidad de tiempo que debe esperar entre el envío de paquetes de protocolo de saludo a vecinos conectados directamente (10 segundos es el valor predeterminado).
11. En el campo **Intervalo muerto**, introduzca el intervalo que debe esperar antes de marcar un router como muerto. El intervalo indefinido predeterminado es de 40 segundos.
12. Haga clic en **Aplicar** para guardar los cambios.

Área de Stub

Las áreas de código auxiliar están protegidas de rutas externas y reciben información sobre redes que pertenecen a otras áreas del mismo dominio OSPF.

Active la casilla de verificación **Área de código auxiliar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

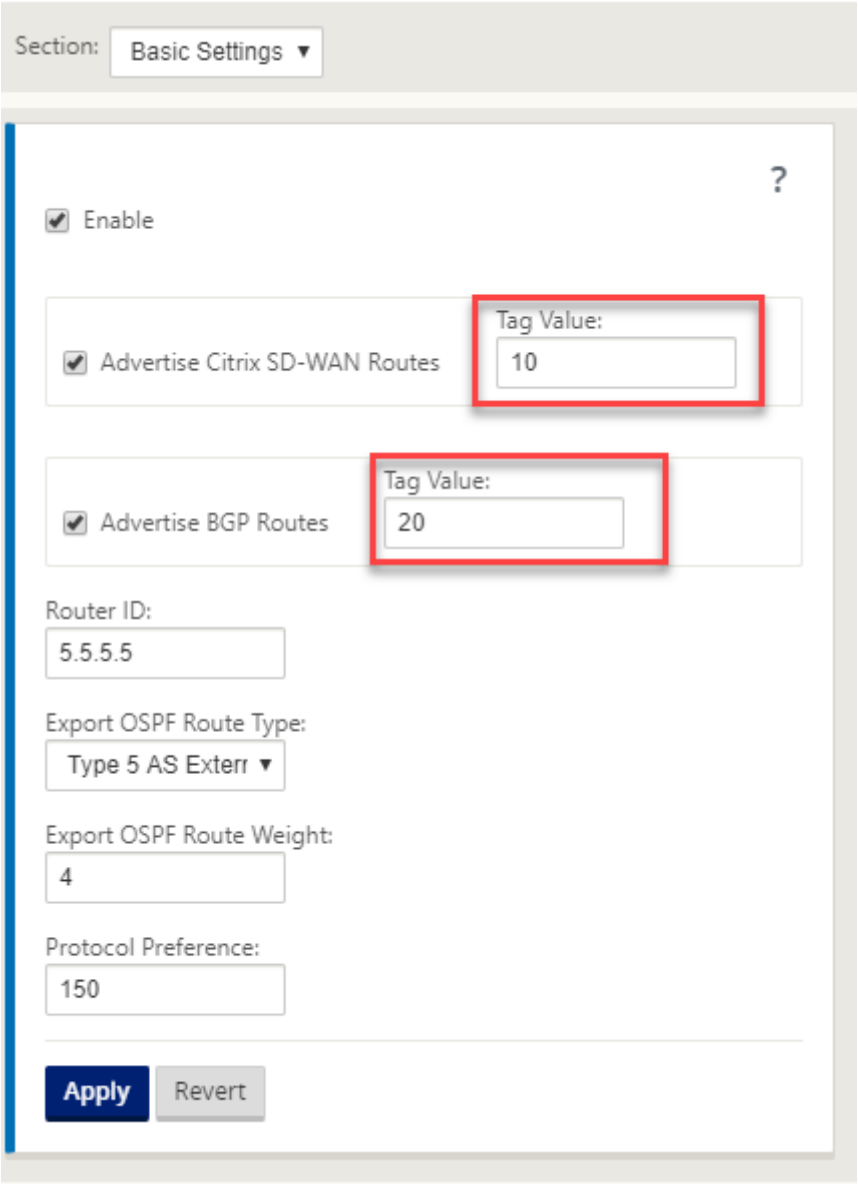


Etiquetas de redistribución OSPF

Puede utilizar etiquetas OSPF para evitar bucles de redirección durante la redistribución mutua entre OSPF y otros protocolos. En el dominio OSPF, si hay rutas SD-WAN y BGP aprendidas a la misma subred, el mecanismo de prevención de bucles OSPF lo identifica como un bucle e ignora las rutas. La especificación de etiquetas diferentes para rutas aprendidas SD-WAN y BGP permite que estas rutas se instalen en la tabla de redirección OSPF.

Puede configurar las etiquetas de redistribución OSPF para las rutas aprendidas a través de SD-WAN y BGP en la sección OSPF, **Configuración básica**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 está utilizando BGP para intercambiar rutas dentro de un AS, entonces el protocolo se denomina Interior BGP (IBGP).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

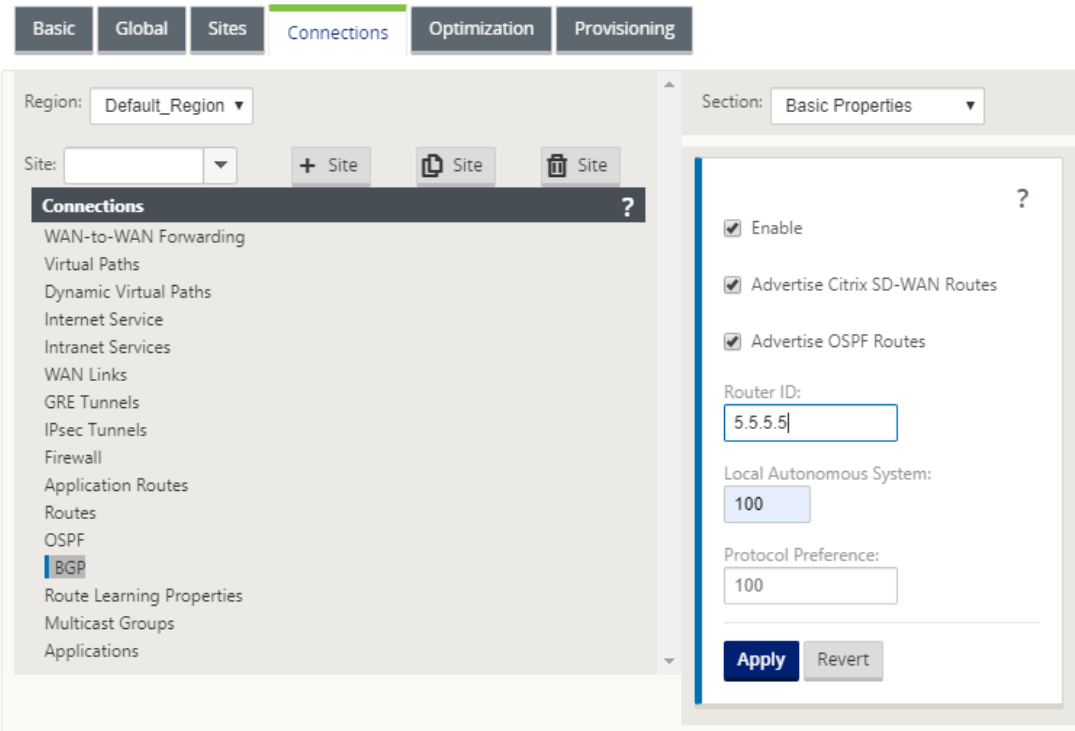
BGP es un protocolo de redirección robusto y escalable implementado en Internet. Para lograr la escalabilidad, BGP utiliza muchos parámetros de ruta llamados atributos para definir directivas de redirección y mantener un entorno de redirección estable. Los vecinos BGP intercambian información de redirección 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 dispositivos Citrix SD-WAN para conocer rutas y anunciar rutas mediante BGP.

Configurar BGP

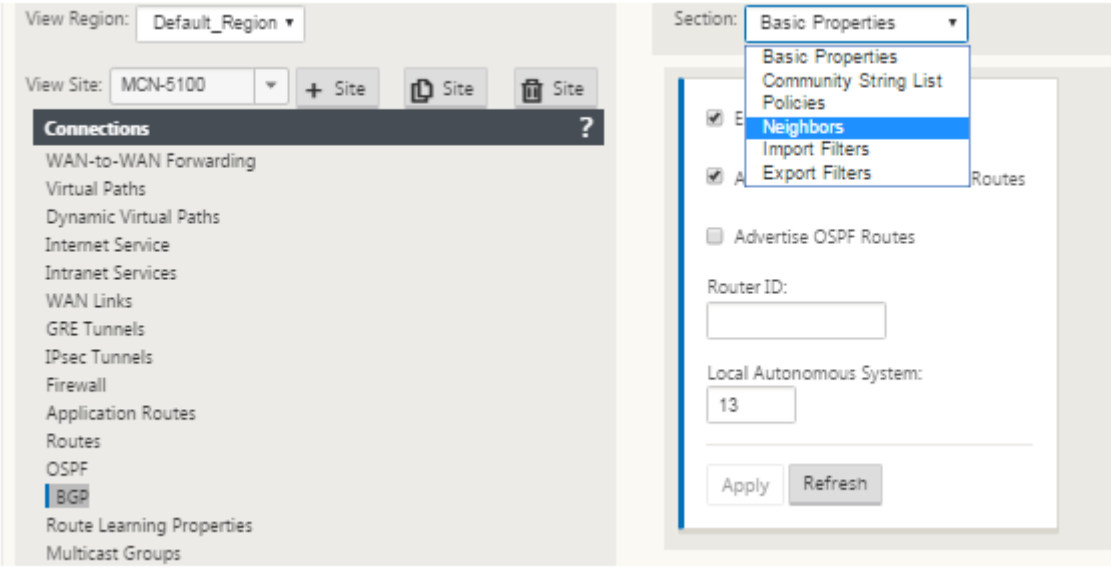
Para configurar BGP:

1. En el **Editor de configuración**, vaya a **Conexiones > Región > Sitio > BGP > Configuración básica.**
2. Haga clic en **Habilitar**, seleccione o introduzca valores para los siguientes parámetros y haga clic en **Aplicar**.
    - **Anunciar rutas de Citrix SD-WAN**: Permita que las rutas de Citrix SD-WAN se publiquen a través de BGP.
    - **Anunciar rutas OSPF**: Permitir que las rutas aprendidas de los pares OSPF se publiquen a través de BGP.
    - **Id. de enrutador**: Identificador único del enrutador, el enrutador se utiliza para anuncios OSPF. Si no se especifica el ID del enrutador, se selecciona automáticamente como la IP virtual más baja alojada en la red SD-WAN.
    - **Sistema Autónomo Local**: Número del sistema autónomo local desde el que se aprenden y anuncian las rutas. El número de sistema autónomo debe coincidir con uno de los enrutadores vecinos.
    - **Preferencia de protocolo**: Si los prefijos se aprenden a través de varios protocolos de enrutamiento, el valor de preferencia de protocolo determina la selección del protocolo de enrutamiento. Para obtener más información, consulte Preferencia de protocolo.

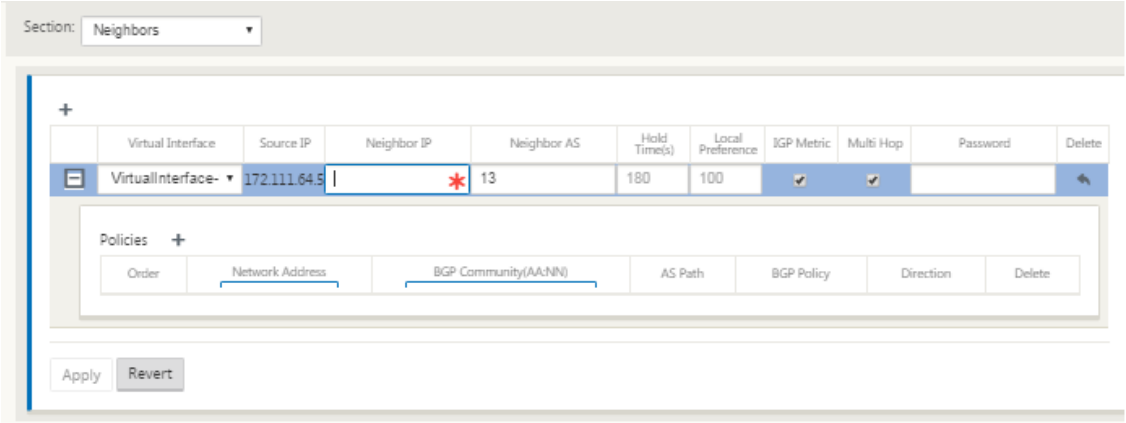
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Expanda **Configuración básica > Vecinos** y haga clic en el icono **Agregar (+)**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para Sitios con varios dominios de redirección, elija un dominio de redirección. Dominio de redirección determina qué interfaces virtuales están disponibles.

4. Seleccione una **interfaz virtual** en el menú. La interfaz virtual determina la dirección IP de origen.
5. Introduzca la **dirección IP** del router IBGP Neighbor en el campo IP Neighbor y el número de **sistema autónomo local** en el campo Neighbor AS.
6. En el campo **Tiempo de espera**, escriba el Tiempo de espera, en segundos, para esperar antes de declarar un vecino caído (el valor predeterminado es 180).
7. En el campo **Preferencia local**, introduzca el valor de Preferencia local, en segundos, que se utiliza para la selección de varias rutas BGP (el valor predeterminado es 100).
8. Haga clic en la casilla de verificación **Métrica IGP** para habilitar la comparación de distancias internas para calcular la mejor ruta.
9. Haga clic en la casilla de verificación **Varios saltos** para habilitar varios saltos para la ruta.
10. En el campo **Contraseña**, introduzca una contraseña para la autenticación MD5 de sesiones BGP (la autenticación no es necesaria).

> **Nota**
>
> La configuración de Reflectores de ruta y Confederaciones para iBGP no es compatible con la red SD-WAN.

BGP exterior (eBGP)

Los dispositivos Citrix SD-WAN se conectan a un conmutador en el lado LAN y a un enrutador en el lado WAN. A medida que la tecnología SD-WAN comienza a ser más integral en las implementaciones de redes empresariales, los dispositivos SD-WAN reemplazan a los routers. SD-WAN implementa el protocolo de redirección dinámica eBGP para funcionar como un dispositivo de redirección dedicado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El dispositivo SD-WAN establece una vecindad con enrutadores de par que utilizan eBGP hacia el lado WAN y es capaz de aprender, anunciar rutas desde y hacia 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:

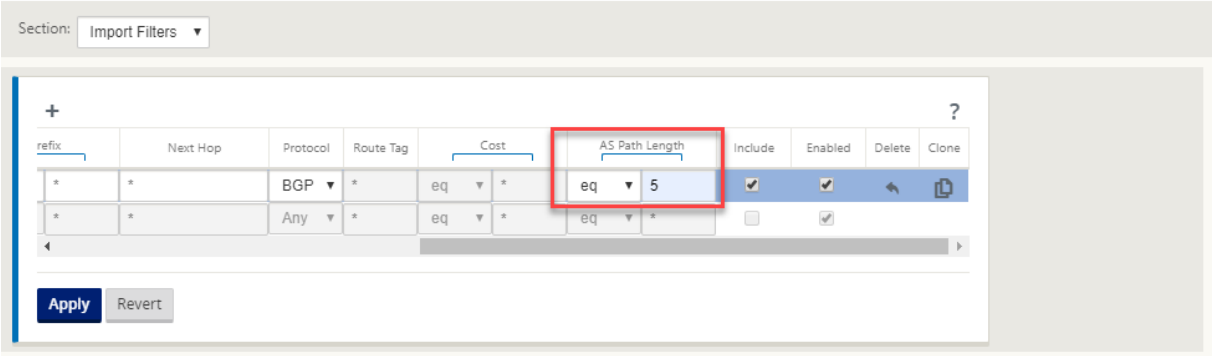
- Sitio SD-WAN Comunicación con sitio que no es SD-WAN a través de eBGP
- Comunicación entre sitios SD-WAN mediante Ruta Virtual y eBGP
- Implementación de OSPF en topología de un brazo
- Implementación de OSPF de tipo 5 a tipo 1 en la red MPLS
- Implementación de OSPF de dispositivos SD-WAN y no SD-WAN (de 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 ruta AS indica el número de sistemas autónomos atravesados en una ruta. Citrix SD-WAN utiliza el atributo de **longitud de ruta BGP AS** para filtrar e importar rutas.

Los dispositivos que no son SD-WAN pueden elegir enrutar el tráfico a los dispositivos SD-WAN de CC primarios o secundarios importando rutas según su longitud de ruta AS. También puede dirigir dinámicamente el tráfico de un enrutador a DC secundario simplemente aumentando la longitud de ruta AS del dispositivo de CC principal en el enrutador, por lo que no es preferible. Eliminación de la necesidad de cambiar el coste de ruta y realizar una actualización de configuración.

Para configurar la longitud de ruta AS en los filtros de importación, seleccione BGP como protocolo, seleccione un predicado e introduzca la **longitud de ruta AS**. Para obtener más información, consulte Filtrado de rutas



Supervisar estadísticas de rutas

Vaya a **Monitor** > **Estadísticas**. Seleccione **Rutas** en el menú implementable **Mostrar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Todas las funciones de las rutas aplicables se admiten en la red de 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	Eligibilit 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

OSPF

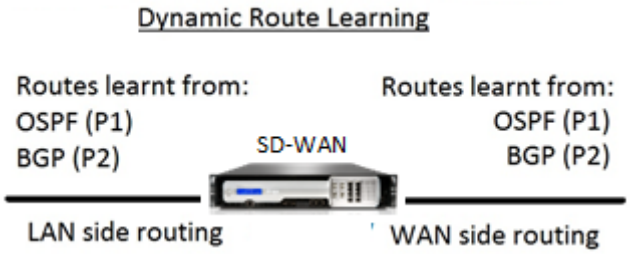
January 10, 2022

Lado LAN: Aprendizaje dinámico de rutas

OSPF que se ejecuta en el puerto LAN del dispositivo Citrix SD-WAN implementado en el modo de 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 quieredos (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 con un ÁREA definido como un área STUB limitando el aprendizaje de LSA AS-externa de tipo 5.

Los dispositivos Citrix SD-WAN pueden anunciar las rutas dinámicas aprendidas localmente con el MCN. A continuación, 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 sitios a través de la red cambiante.

Modos de implementación OSPF

En versiones anteriores, las rutas aprendidas de instancia OSPF de SD-WAN se trataban como rutas externas con LSA de tipo 5 solamente. Estas rutas se anunciaron a sus routers vecinos en LSA externa de tipo 5. Esto dio como resultado que las rutas SD-WAN fueran rutas menos preferidas según el algoritmo de selección de rutas OSPF.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Con la última versión, SD-WAN ahora puede anunciar rutas como rutas dentro de 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 brazo, el router necesita una complicada configuración PBR o WCCP en 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.

Para configurar OSPF Tipo 1:

1. Configure **las interfaces virtuales** y **los enlaces WAN** en los sitios DC y Branch para que pueda crear ruta virtual entre ellos.
2. En **Conexiones** > [**MCN**] > **Aprendizaje de rutas** > **OSPF** ->**Configuración básica**, seleccione **Exportar tipo de ruta OSPF** para ser **Tipo 1 Intra Area**.
3. Guarde la configuración, el caso y active la configuración.

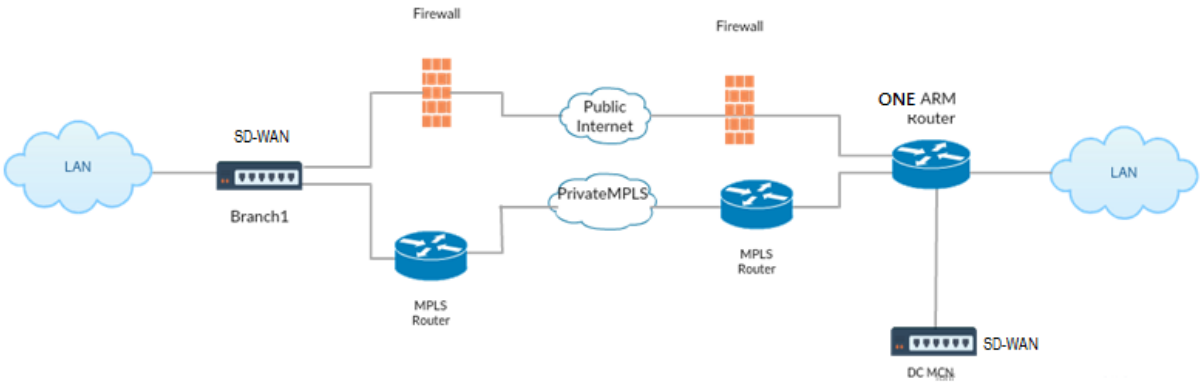
Debe poder ver los siguientes tipos de ruta en
Exportar tipo de ruta OSPF

- Tipo 5 AS externo
- Área Intra Tipo 1

Debe ser capaz de configurar la ruta **externa de tipo 5 AS**.

Después de activar la configuración cambiada, debe ver los cambios de tipo de ruta en **Configuración** > **WAN virtual** > **Ver configuración** > **Enrutamiento dinámico**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



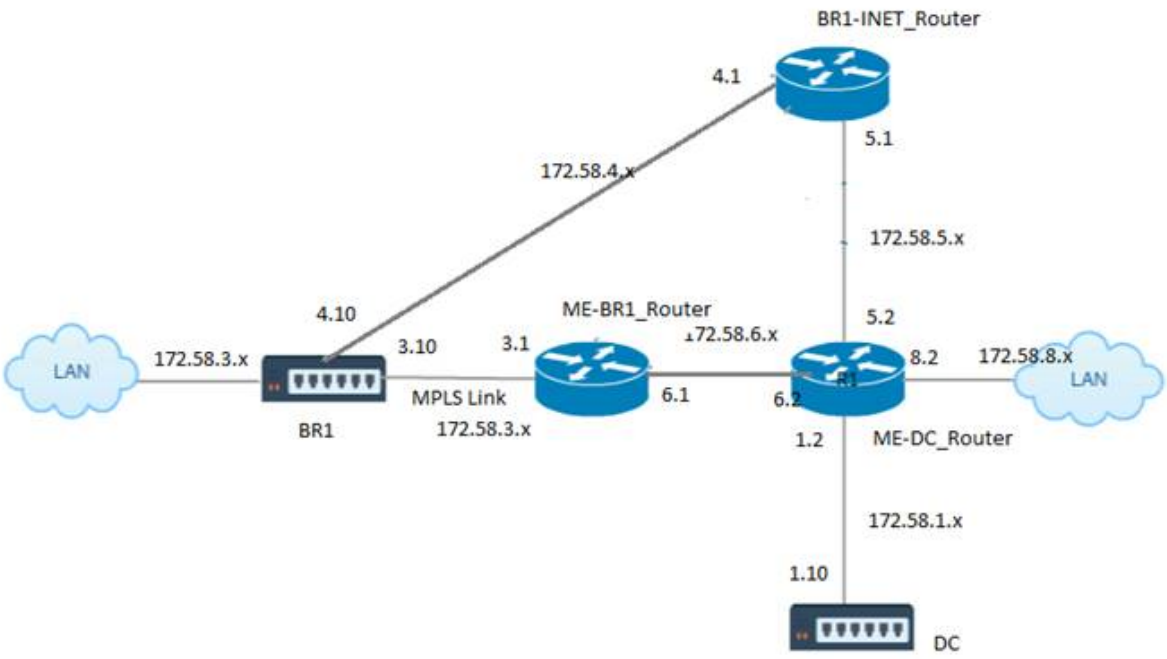
Como se muestra en la ilustración anterior, el MCN de CC se implementa en topología de un brazo. Cuando el sitio de DC está activo, un enrutador de un solo brazo reenvía todo el tráfico de la LAN local a otros sitios, como la LAN local de la sucursal cuya dirección IP de destino está dentro de la misma subred a la 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 LAN local a otros sitios (LAN local del sitio de sucursal, IP de destino está dentro de la subred) a 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 con dispositivos SD-WAN. La ilustración siguiente describe la implementación de red MPLS estándar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



En la ilustración anterior:

- OSPF se configura entre *ME-BR1_Router* y *ME-DC_Router* en el área 0.
- OSPF está configurado entre *ME-DC_Router* y *DC* en el área 0.

Configuración recomendada:

- DC VW y ME-DC_router en área0
- ME-BR1_Router y ME-DC_Router en area0
- BR1 VW y ME-BR1_Router en el área 0

En el router ME-DC_Router:

1. Agregar, ruta estática para 172.58.3.10/32 (IP virtual de BR1 para MPLS Link) a través de 172.58.6.1
2. Agregar, ruta estática para 172.58.4.10/32 (IP virtual de BR1 para INET) a través de 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, el MCN reenvía el paquete encapsulado destinado a uno de los VIP BR1 al router ME-DC y de vuelta desde el 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 al 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 router 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para configurar rutas exportadas OSPF como Tipo1 en **Configuración básica de OSPF**:

1. Configure **las interfaces virtuales** y **los vínculos WAN** tanto en sitios de DC como de sucursal para crear la ruta virtual entre ellos.
2. En **Conexiones**->[**MCN**]>**Aprendizaje de rutas**->**OSPF**->**Configuración básica**, seleccione **Exportar tipo de ruta OSPF**para ser **Tipo 1 Intra Area**.
3. Guarde la configuración, el caso y active la misma. Debe poder ver los dos tipos de ruta siguientes en **Exportar tipo de ruta OSPF**:
   - Tipo 5 AS externo
   - Área Intra Tipo 1

Después de activar la configuración modificada, puede ver los cambios de tipo de ruta en **Configuración** > **WAN virtual** > **Configuración de vista** > **Redirección dinámico**.

El dispositivo SD-WAN debe anunciar las rutas como AS externas de Type5. Las rutas aprendidas a través de SD-WAN deben mostrarse en los routers vecinos como Rutas externas Type5 AS.

Para configurar el peso de ruta exportado OSPF en **Configuración básica de OSPF**:

1. Configurar interfaces virtuales y vínculos WAN en sitios de DC y sucursales para crear la ruta virtual entre ellos.
2. En **Conexiones** >[**MCN**] > **Aprendizaje de rutas** > **OSPF** > **Configuración básica**, configure **Exportar peso de ruta OSPF**.
3. Guarde la configuración, el caso y active la misma.
4. Ahora, configure Exportar peso de ruta OSPF en cualquier valor numérico comprendido entre **1** y **65529**.
5. Después de activar la configuración modificada, puede ver el Peso de ruta en **Configuración** > **WAN virtual** > **Configuración de visualización** > **Redirección dinámico**. El peso de ruta predeterminado exportado debe ser 0. El coste real de la ruta solo debe ser el coste de SD-WAN.

Para configurar las rutas exportadas de OSPF como Tipo 1 en la configuración del filtro de exportación:

1. Configurar **interfaces virtuales** y **enlaces WAN** tanto en DC como en Branch para que podamos crear la Ruta Virtual entre ellos1. En **Conexiones** > **[MCN]** > **Aprendizaje de rutas** > **OSPF** > **Exportar filtros** configure un filtro de exportación.
2. Expanda el filtro. Configure **Exportar tipo de ruta OSPF** en ruta **Intra Area Tipo 1**.
3. Guarde la configuración, el caso y active la misma. Debe poder ver los dos tipos de ruta siguientes en **Exportar tipo de ruta OSPF**

- Tipo 5 AS externo
- Área Intra Tipo 1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de activar la configuración modificada, un usuario debe poder ver los cambios del tipo de ruta en**Configuración** > **WAN virtual** > **Ver configuración**. El tipo de ruta debe mostrarse como Tipo 5 AS Externo.

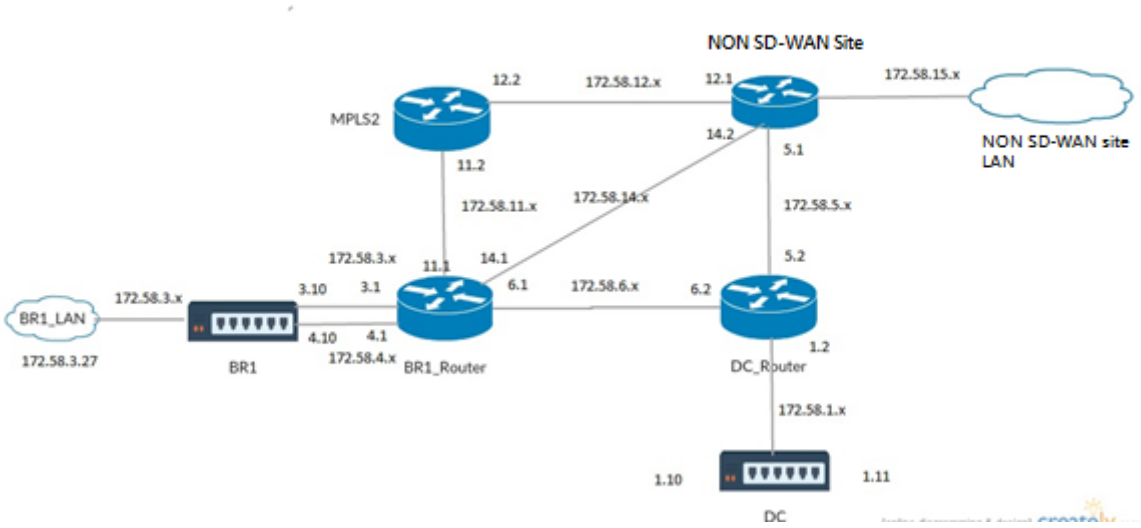
Para configurar el peso de ruta exportada OSPF en la configuración del filtro de exportación:

1. Configurar interfaces virtuales y enlaces WAN tanto en DC como en Branch para que podamos crear la Ruta Virtual entre ellos.
2. En **Conexiones** >[**MCN**] ->**Aprendizaje de rutas** >**OSPF** >**Exportar filtros** configure un filtro de exportación.
3. Expanda el filtro. Configure Exportar peso de ruta OSPF en cualquier valor numérico comprendido entre **1** y **65529**.
4. Guarde la configuración, el caso y active la misma.

Después de activar la configuración modificada, un usuario debe poder ver los cambios del tipo de ruta en**Configuración** > **WAN virtual** > **Ver configuración**.
Peso de ruta configurado en Filtro de exportación debe reemplazar el peso configurado en **Configuración básica de OSPF**.

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.



Pasos de configuración:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

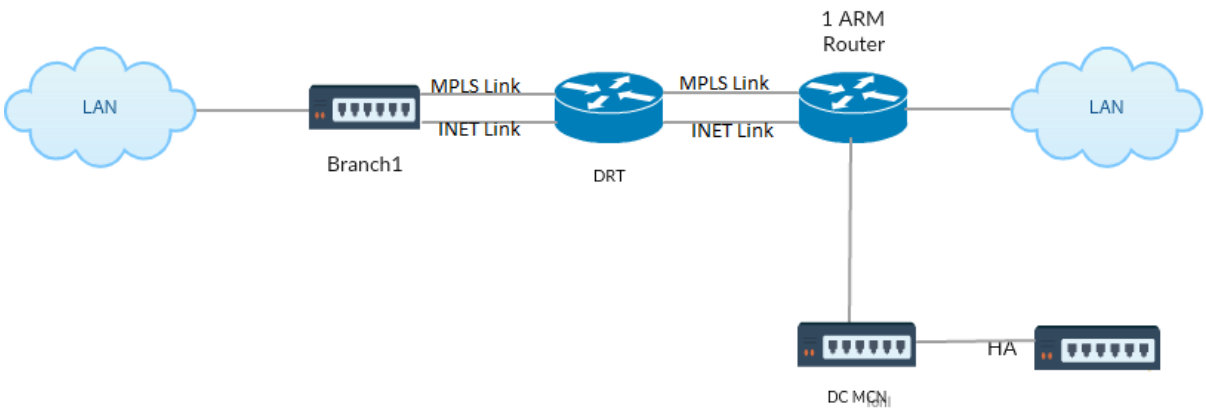
1. Configure **las interfaces virtuales** y **los enlaces WAN** en DC y Branch para que se cree una ruta virtual entre los sitios.
2. Configure el **tipo de ruta de exportación** como **Type1** y asigne el coste como **195** en el dispositivo SD-WAN.
3. Guarde, escenificar y active la configuración.
4. Enviar tráfico entre los hosts finales en los sitios DC y Branch.
5. Apague el enlace entre R1 y R2.
6. Enviar tráfico entre los hosts finales en los sitios DC y Branch.
7. Descierre el enlace entre R1 y R2.
8. Enviar tráfico entre los hosts finales en los sitios DC y Branch.
9. Inhabilite el servicio WAN virtual en el sitio de DC para que las rutas virtuales caian.
10. Enviar el tráfico entre los hosts finales en los sitios DC y Branch.

Verificación de la configuración:

1. Inicialmente, en el paso 4, todo el tráfico pasa a través del dispositivo SD-WAN.
2. En el paso 6, cuando se interrumpe el enlace entre R1 y R2, el tráfico se enruta hacia SD-WAN a través de R3.
3. En el paso 8, el tráfico fluye a través del dispositivo SD-WAN con R2 como el siguiente salto para el enrutador LAN R1.
4. En el paso 10, los paths de WAN virtual descienden entre DC y el dispositivo BR1 y el tráfico debe fluir normalmente como antes de que se configurara la red SD-WAN.

El flujo de tráfico se puede observar en la interfaz gráfica de SD-WAN en **Monitoring** > **Flows**.

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:

Para configurar OSPF en la implementación de alta disponibilidad:

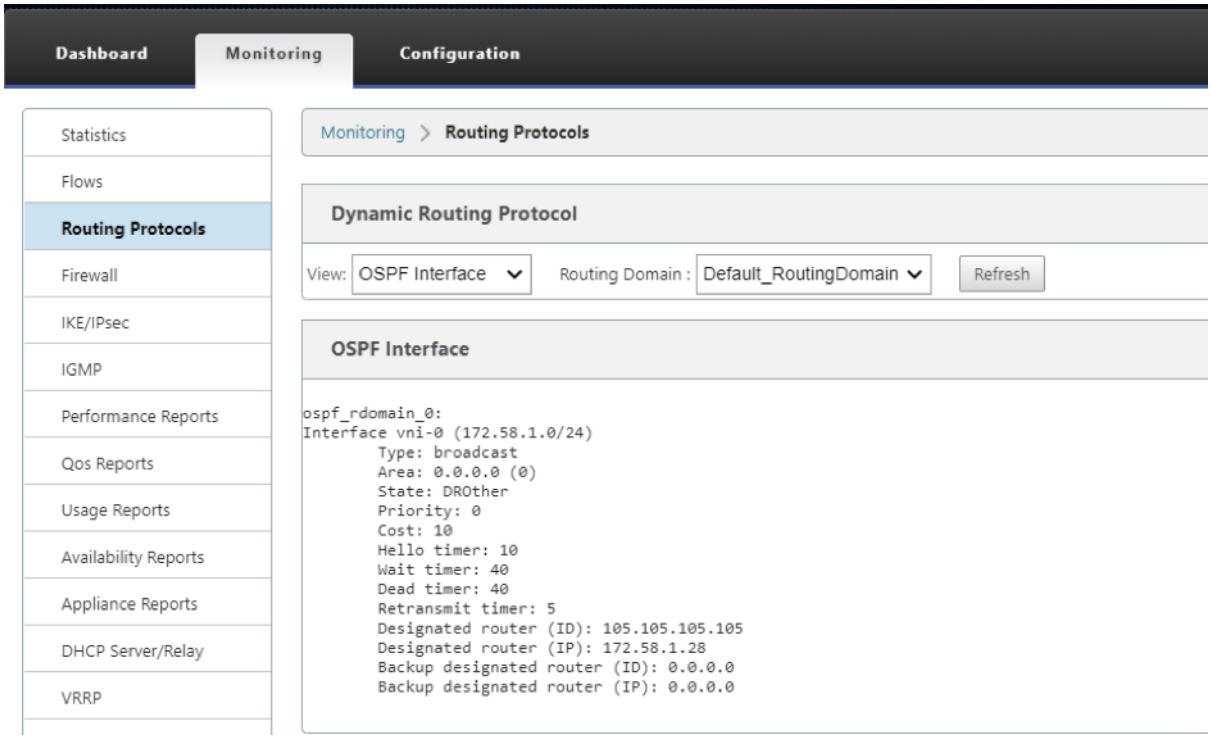
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

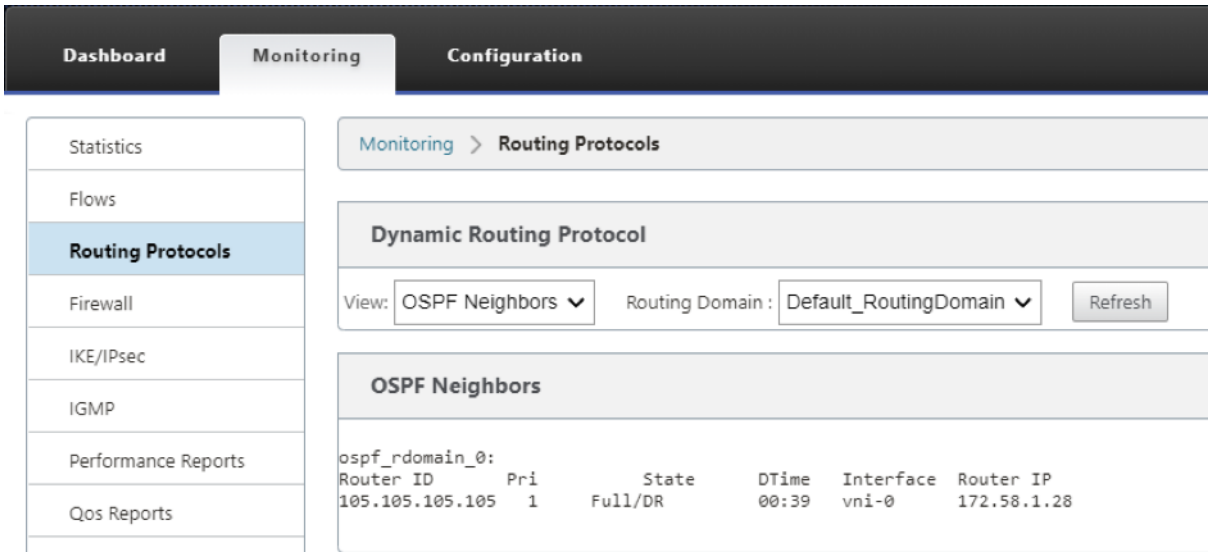
1. Configure **las interfaces virtuales** y **los vínculos WAN** tanto en DC como en Branch para crear la ruta virtual entre ellos.
2. Configuración de alta disponibilidad.
3. Exportar el **tipo de ruta** configurado como **Tipo 1** y el **peso de ruta** como **50**.
4. Guarde la configuración, el caso y active la misma.
5. Iniciar flujo de tráfico.
6. Observe que en **Monitor** > **Estadísticas** > **Rutas**, el recuento de aciertos aumenta para las rutas OSPF con menos costes.
7. Bajar el MCN activo y observar el comportamiento.
8. Vuelva a activar el MCN activo original.
9. El **Panel** > **Estado de alta disponibilidad** se muestra correctamente para HA Local Appliance y Peer Appliance para Active y Standby.
10. En **Configuración** > **Configuración de vista** > **Redirección dinámico**, OSPF está habilitado y **export_ospf_route_type** muestra **Tipo 1** y **export_ospf_route_weight** como **50**.
11. Incluso después de la conmutación por error, el estado de alta disponibilidad muestra la configuración OSPF correcta para el dispositivo local y del mismo nivel.
12. Ver **Monitor** > **Estadísticas** > **Rutas**. El recuento de aciertos aumenta para las rutas OSPF con menos costes.
13. Después de la conmutación por recuperación, el estado de alta disponibilidad muestra la configuración OSPF correcta para el dispositivo local y del mismo nivel.
14. Compruebe que el recuento de aciertos aumente para rutas OSPF con bajo coste en Ver **Monitor** > **Estadísticas** > **Rutas**.

Solucionar problemas

Puede ver los parámetros OSPF en **Supervisión >Protocolos de enrutamiento**.

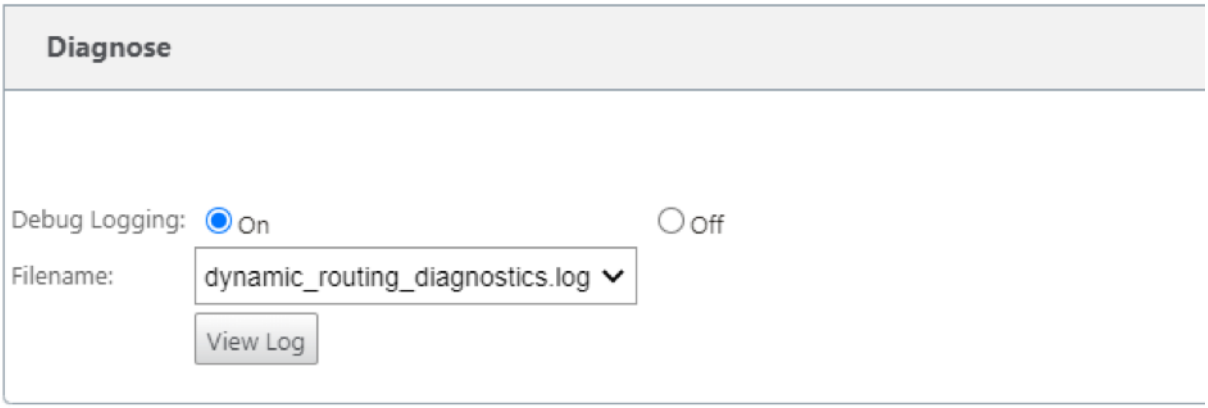
© 1999–2024 Cloud Software Group, Inc. All rights reserved.





También puede observar los registros de redirección dinámica para ver si hay algún problema con OSPF Convergence.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



BGP

May 7, 2021

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 aplicarlas selectivamente a un conjunto de redes por vecino, en cualquier dirección (importar o exportar). 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 directivas

En la interfaz de administración web de SD-WAN, el editor de configuración tiene una nueva sección, directiva BGP, en **Route Learning** > **BGP**. En esta sección, los usuarios pueden agregar atributos BGP que constituyen una directiva. Se admiten agregar cadenas de comunidad, anteponer rutas AS y configurar MED.

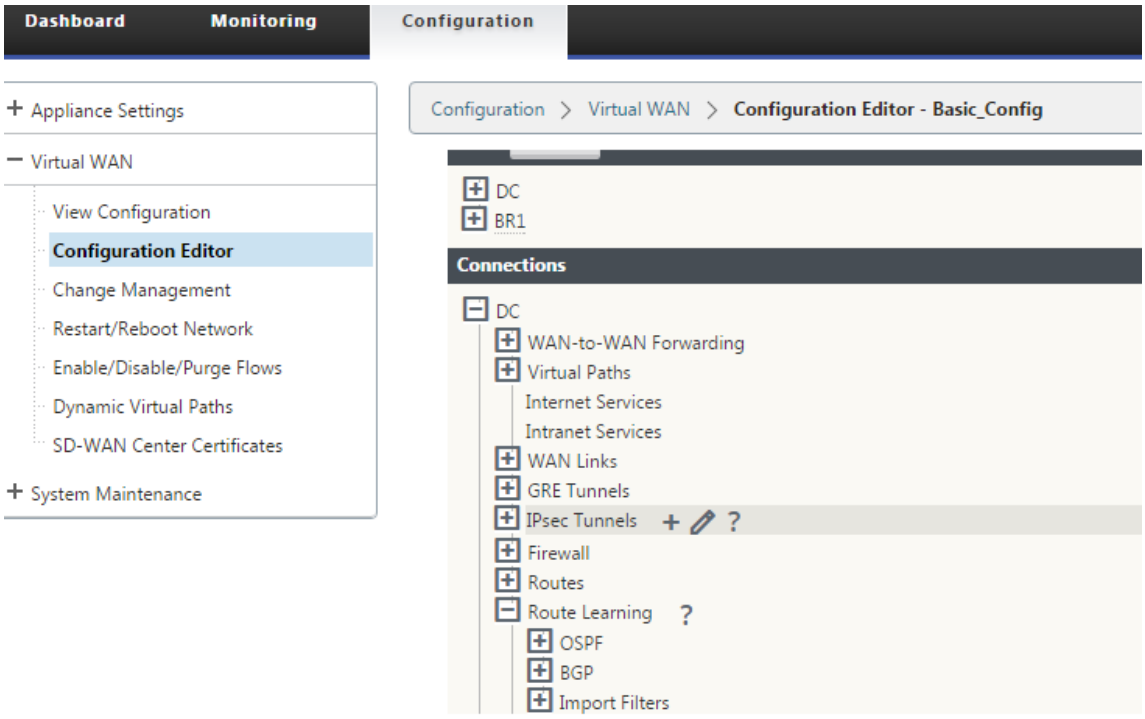
Puede configurar manualmente cada cadena de comunidad o seleccionar ninguna cadena de comunidad publicitaria o ninguna cadena de comunidad exportada en un menú desplegable. Para la configuración manual, puede introducir un número de AS y una comunidad. Puede seleccionar **Insertar/Quitar** para etiquetar las rutas o eliminar la comunidad de las rutas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede configurar el número de veces que quiere anteponer el AS local a la ruta AS antes de hacer publicidad fuera de la red local. Puede configurar MED para rutas coincidentes.

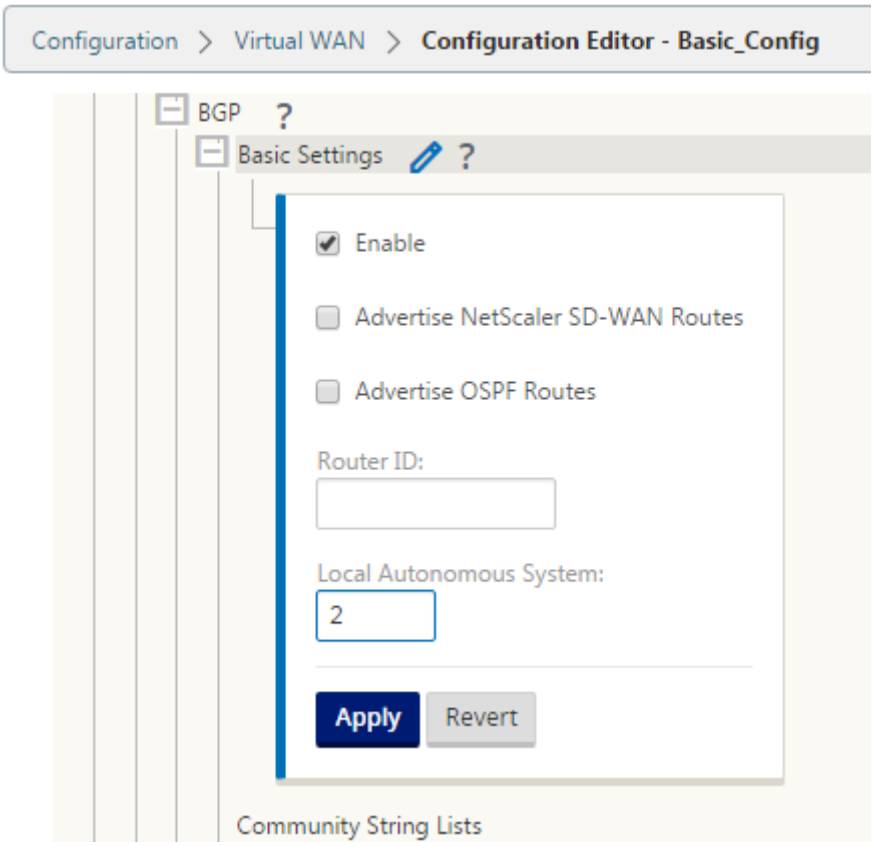
Para configurar la directiva BGP:

1. En la interfaz de administración web de NetScaler SD-WAN, vaya a **Configuración** > **Virtual WAN** > **Editor de configuración**. Abra un paquete de configuración existente. Vaya a **Sitios** > Configuración de **DC** o **Branch**.



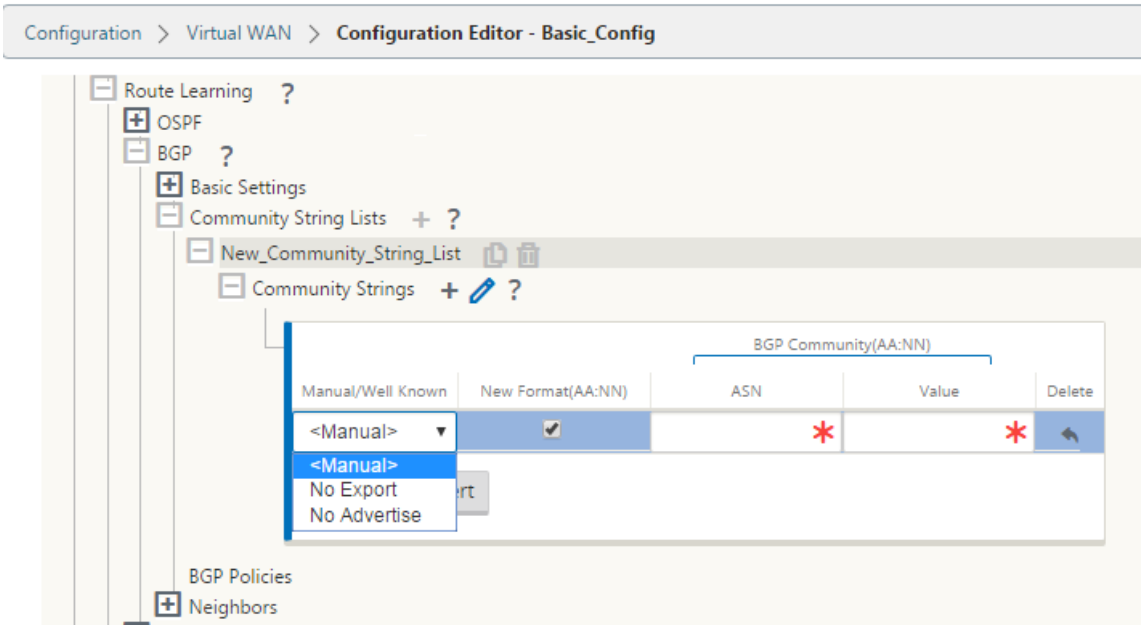
2. Expanda **BGP** y haga clic en **Habilitar** en **Configuración básica**. Introduzca el valor **del ID del router** y **del sistema autónomo local** y haga clic en **Aplicar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

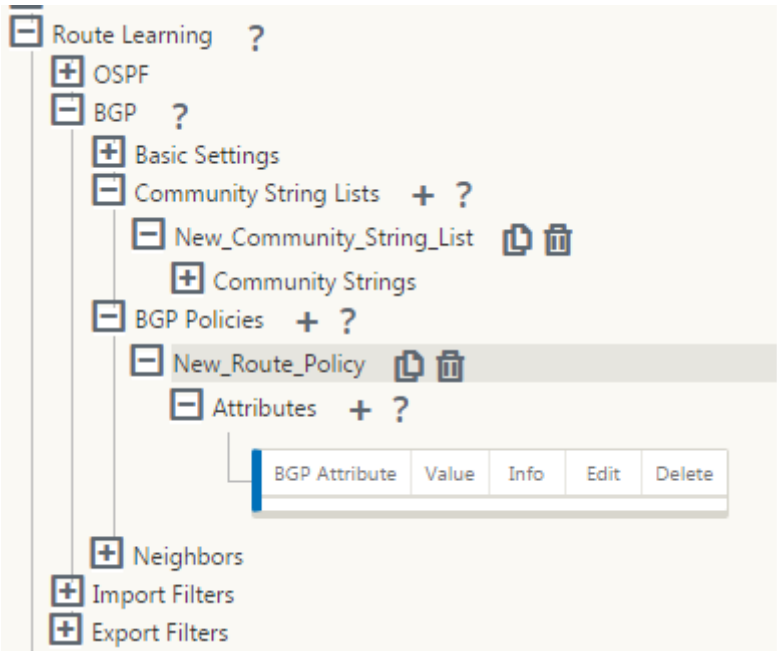


3. Haga clic en el signo **+** junto a las **Listas de cadenas de la comunidad**. Configure cada cadena de comunidad manualmente o seleccionando ninguna cadena de comunidad publicitaria o ninguna cadena de comunidad exportada en el menú desplegable. Para la configuración manual, puede introducir un número de AS y una comunidad. Puede seleccionar **Insertar/Quitar** etiqueta las rutas con la cadena de comunidad o eliminar la cadena de comunidad de las rutas recibidas de los pares.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

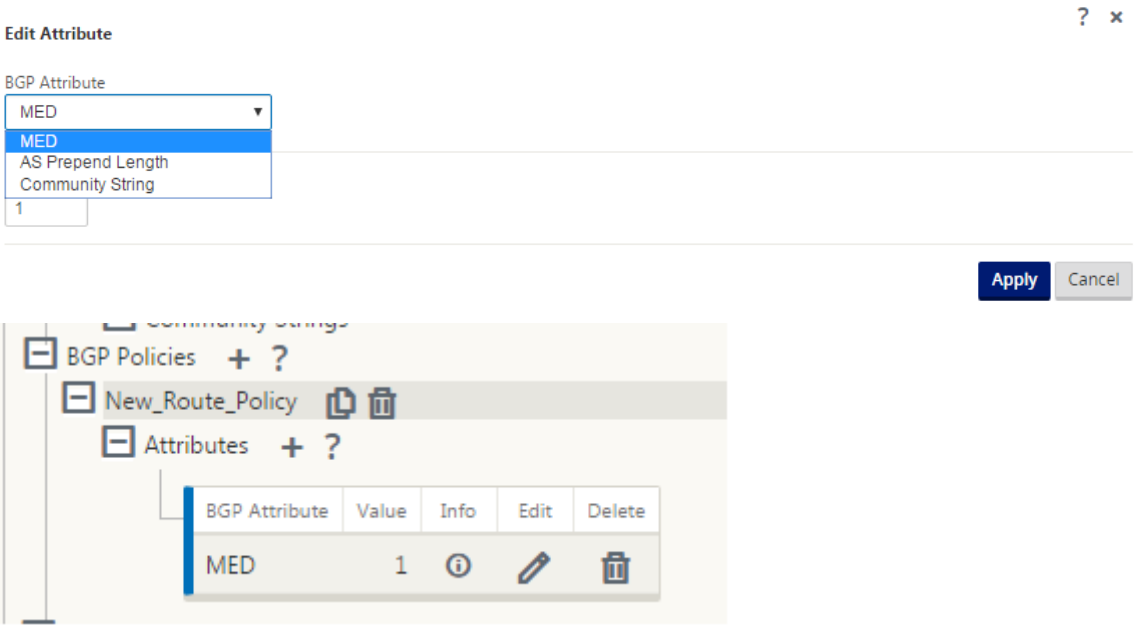


4. Configure la directiva BGP expandiendo **las directivas BGP.** Agregue atributos BGP a la **nueva directiva de ruta**.



5. Haga clic en el signo **+** situado junto a **Atributos** para modificar los atributos BGP. Aparecerá la ventana **Modificar atributos**. Seleccione el atributo BGP quieredo en el menú desplegable. Introduzca el valor deseado para **MED**, **AS Prepend Length** o **Community String**, según su selección. Haga clic en **Aplicar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Cualquier directiva puede tener una sola aparición de un atributo y no puede tomar varias apariciones del mismo atributo. No puede tener 2 MED o 2 AS Path Prepend. Puede tener MED/AS-PATH Prepend/Community String o una combinación.

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 ruta y ACL para que coincidan con ciertas rutas y configurar atributos BGP para ese vecino. Puede especificar la dirección para indicar si esta directiva se aplica a las rutas entrantes o salientes.

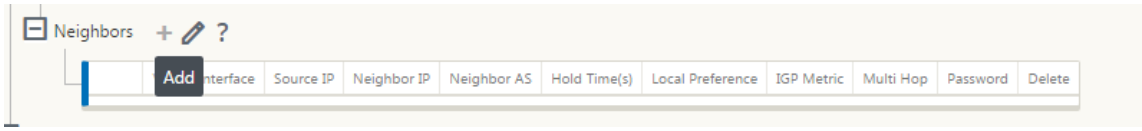
La directiva predeterminada es para <accept> todas las rutas. Las directivas de aceptación y rechazo son predeterminadas y no se pueden modificar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

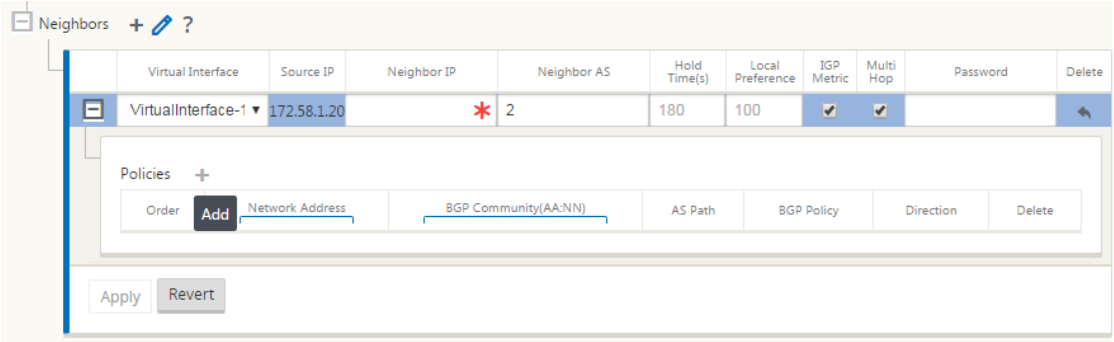
Tiene la capacidad de hacer coincidir rutas en función de la dirección de red (dirección de destino), ruta de acceso AS, cadena de comunidad y asignar una directiva y seleccionar la dirección para la directiva que se va a aplicar.

Para configurar vecinos:

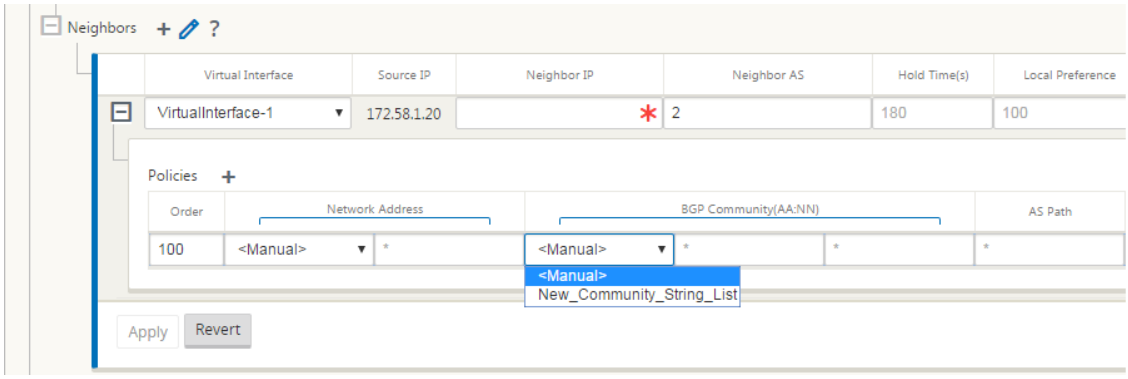
1. Configure vecinos haciendo clic en **Agregar** como se muestra a continuación.



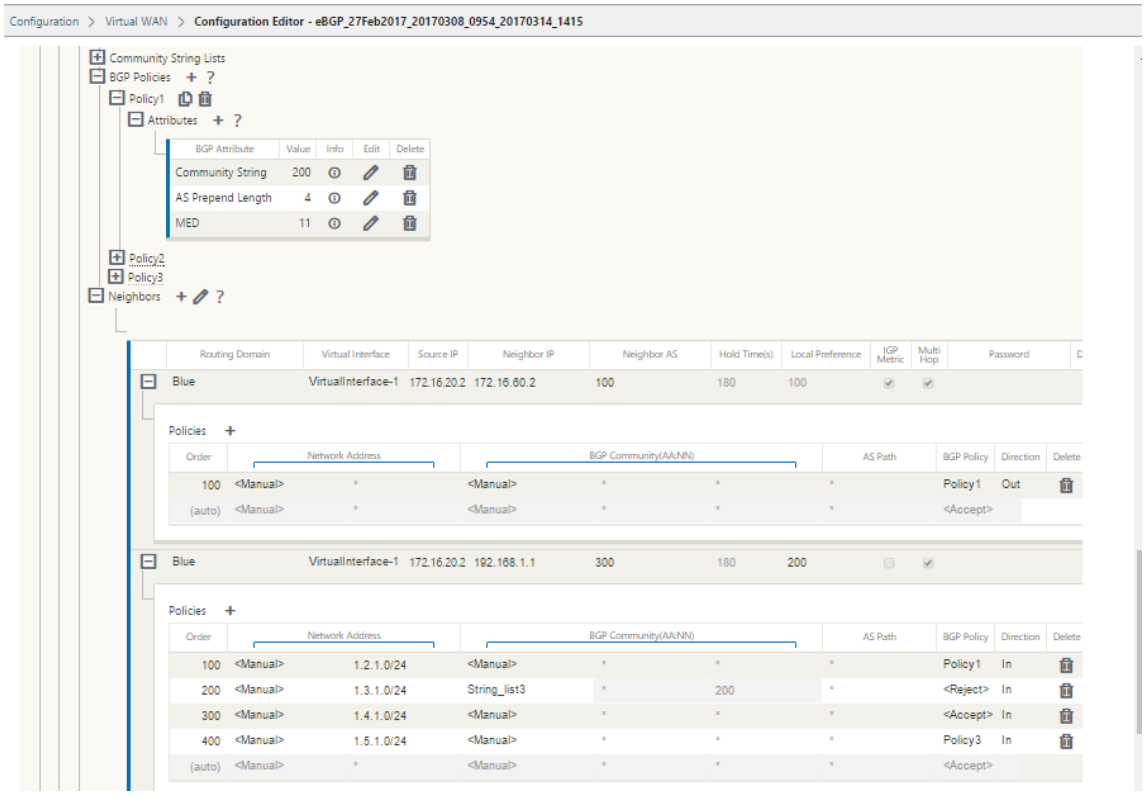
2. Haga clic en el signo **+**. Seleccione una **interfaz virtual**. Introduzca la dirección **IP del vecino**.



3. Agregar directivas. Seleccione **Dirección de red**, **Comunidad BGP**y **Ruta de acceso AS**según quiera. Haga clic en **Aplicar**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Vaya a **Supervisión** > Protocolos de **enrutamiento > Protocolos** de **enrutamiento 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 el enrutamiento desde la página **Monitor** > **Protocolo de enrutamiento**. Los registros del demonio de redirección se dividen en archivos de registro independientes. La información de enrutamiento estándar se almacena en *dynamic_routing.log* mientras que los problemas de enrutamiento dinámico se capturan en *dynamic_routing_diagnostics.log*, que se puede ver desde la supervisión de protocolos de enrutamiento.

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.

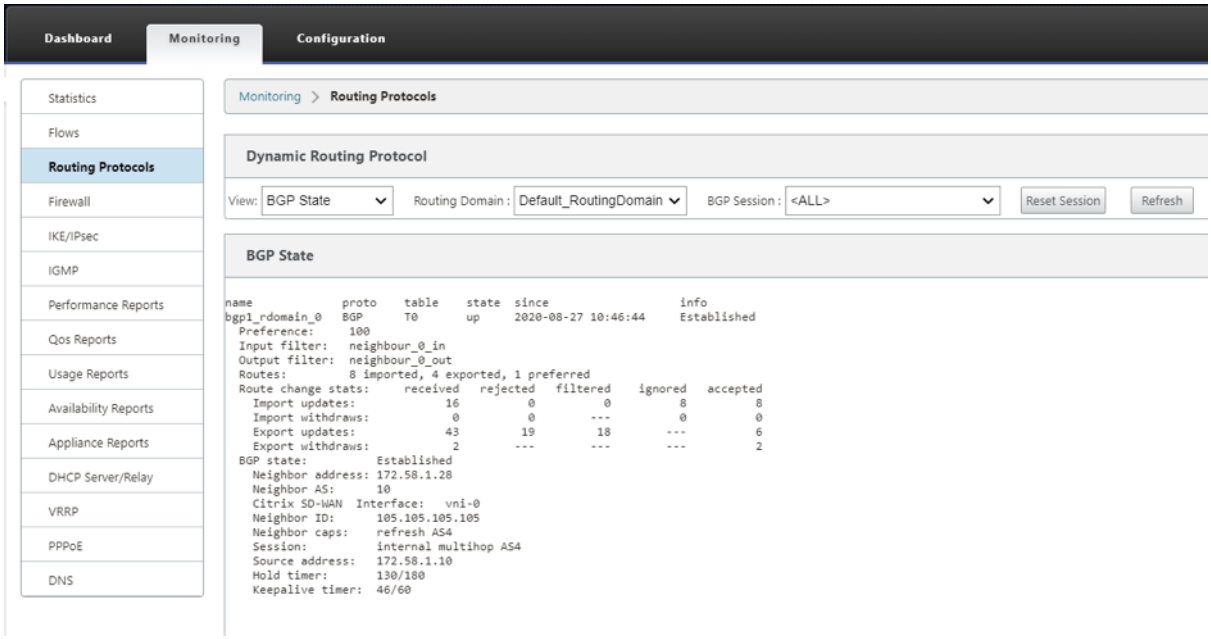
Al borrar una sesión BGP mediante un restablecimiento completo, se invalida la caché y se produce un impacto negativo en el funcionamiento de las redes, ya que la información de la caché deja de estar disponible.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

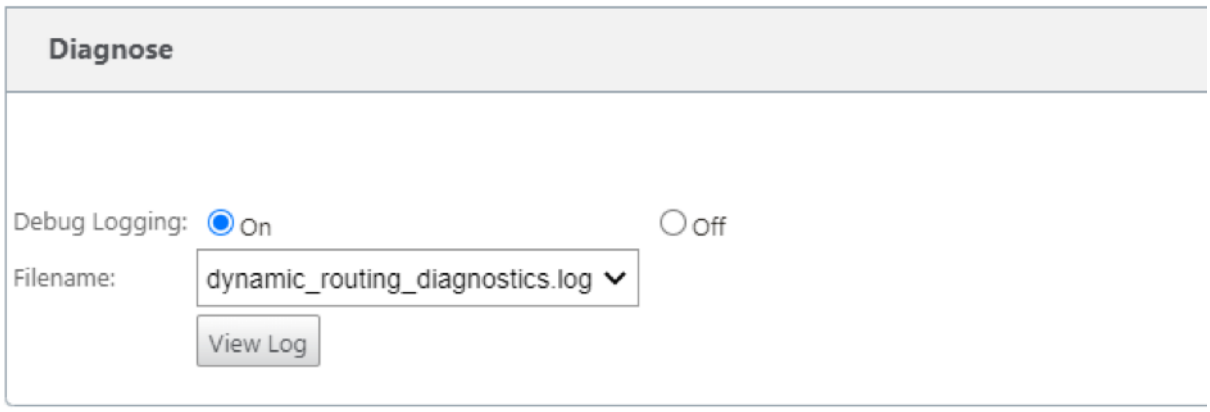
La función BGP Soft Reset Enhancement proporciona compatibilidad automática para el restablecimiento dinámico de las actualizaciones entrantes de la tabla de redirección BGP que no dependen de la información de actualización de la tabla de redirección almacenada.

Solucionar problemas

Para ver los parámetros BGP, vaya a **Supervisión > Protocolos de enrutamiento** > seleccione **Estado BGP** en el campo **Ver**.



Puede observar los registros de redirección de Dynamic para ver si hay algún problema con BGP Convergence.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

iBGP

May 7, 2021

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.

Múltiples routers LAN iBGP en una topología de red lineal con emparejamiento directo y mallados con Citrix SD-WAN.

Limitaciones:

- No se admiten los atributos Prepend, Med y Community.
- No se admite el filtrado de rutas entre OSPF y BGP durante la redistribución. Todas (o) ninguna de las rutas aprendidas de OSPF se anuncia 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

May 7, 2021

Sitio SD-WAN que se comunica con sitio no SD-WAN a través de eBGP:

Cuando un sitio sin dispositivo SD-WAN se comunica con otro sitio con dispositivo SD-WAN (Sitio-A) a través de una única ruta WAN (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 desde el sitio sin 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

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 del sitio de sucursal intenta acceder a una aplicación SaaS, el tráfico se puede enrutar de manera que las sucursales puedan acceder a las aplicaciones SaaS en Internet directamente, sin tener que pasar por el centro de datos primero.

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 path y se adapta a la demanda de aplicaciones cambiantes y a las condiciones 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 sitios de Internet público. El tráfico de Internet no está encapsulado. Cuando se produce congestión, la SD-WAN administra activamente el ancho de banda limitando la velocidad del tráfico de Internet en relación con la ruta de acceso virtual y el tráfico de intranet.
- **Intranet**: Este servicio administra el tráfico de Intranet de empresa que no se ha definido para su transmisión a través de una ruta de acceso 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 los tiempos de congestión. En determinadas condiciones, y si la repliegue de intranet está configurada en la ruta de acceso virtual, el tráfico que normalmente viaja a través de la ruta de acceso virtual se puede tratar como tráfico de intranet.
- **Local**: Este servicio administra el tráfico local al 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 GRE LAN configurado en el sitio. La función Túnel GRE le permite configurar los dispositivos SD-WAN para terminar los túneles GRE en la LAN. Para una ruta con el tipo de servicio GRE Tunnel, la Gateway debe residir en una de las subredes de túnel del túnel GRE local.
- **Túnel IPSec de LAN:** Este servicio administra el tráfico IP destinado a un túnel IPSec de LAN y coincide con el túnel IPSec de LAN configurado en el sitio. La función Túnel IPSec de LAN le permite configurar los dispositivos SD-WAN para terminar los túneles IPSec en el lado LAN o WAN.

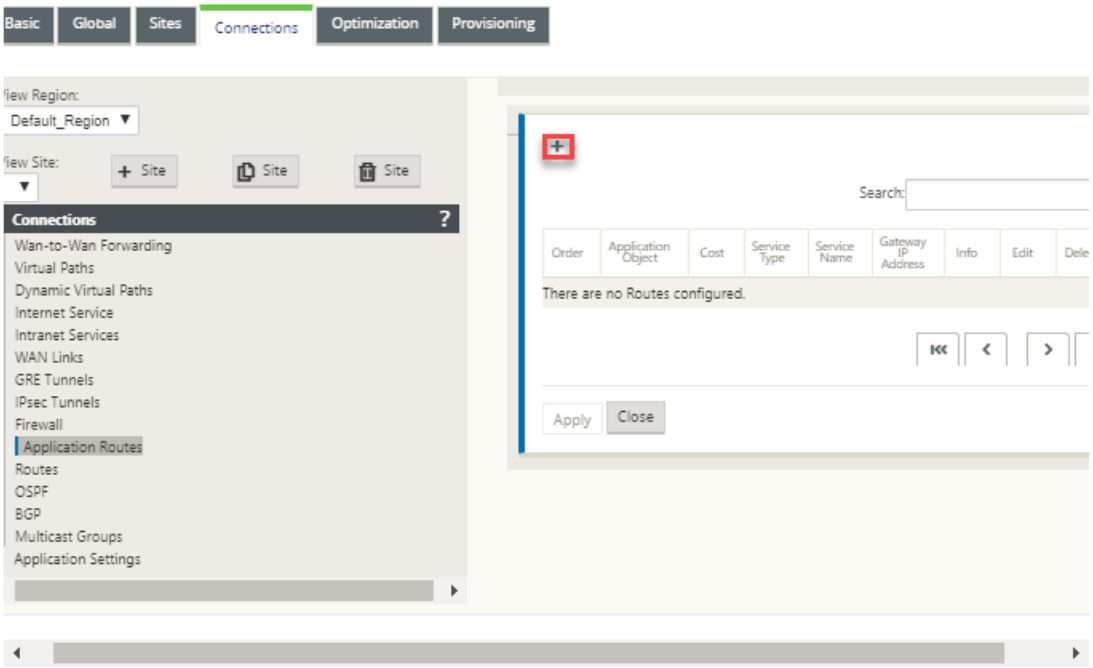
Para realizar la dirección de servicio para las aplicaciones, es importante identificar una aplicación en el primer paquete. Inicialmente, los paquetes fluyen a través de la ruta IP una vez que se haya clasificado el tráfico y se haya conocido la aplicación, se utiliza la ruta de aplicación correspondiente. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

clasificador DPI y los tipos de coincidencia de puertos IP configurados por el usuario.

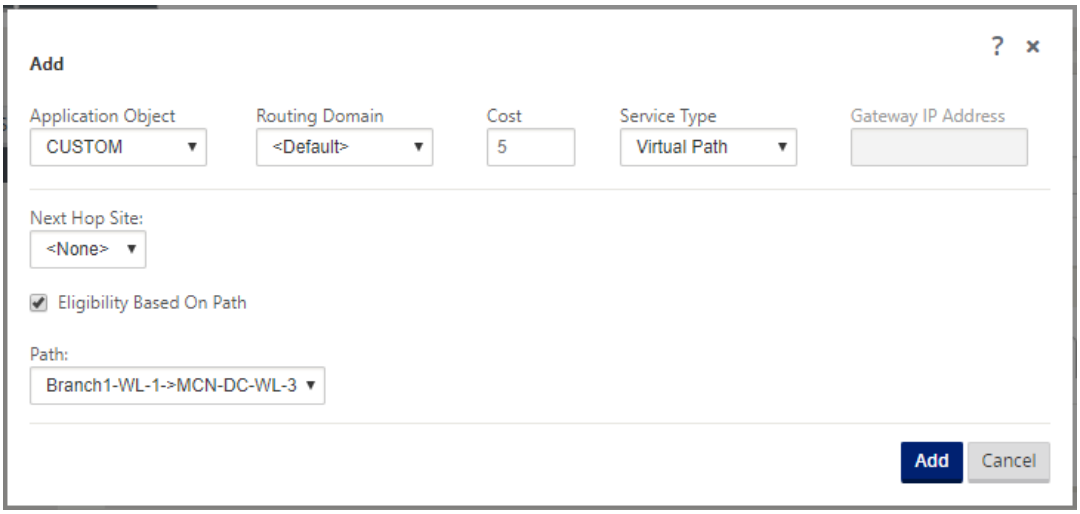
Para configurar el enrutamiento de aplicaciones:

1. En el Editor de configuración, vaya a **Conexiones** > **Rutas de aplicación** y haga clic en +.



2. En la página **Agregar**, establezca los siguientes parámetros:

   - **Objeto Application**: El objeto de aplicación, que desea dirigir. Aquí se enumeran los objetos de aplicación creados por usted. Para obtener más información, consulte la sección **Objetos de aplicación** en el Clasificación de aplicaciones tema.



   - **Dominio de enrutamiento**: Dominio de enrutamiento que utilizará la ruta de la aplicación. Elija uno de los dominios de redirección configurados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Coste**: Peso para determinar la prioridad de ruta para esta ruta. Las rutas de menor coste tienen prioridad sobre las rutas de mayor coste. El intervalo es de 1 a 65534. El valor predeterminado es 5.
- **Tipo de servicio:** Seleccione uno de los siguientes servicios. Esto asigna la aplicación a un servicio.
- **Ruta virtual**: Identifica el tráfico de aplicaciones como tráfico de ruta virtual y coincide con una ruta virtual basada en reglas de ruta virtual. En el campo **Sitio de salto siguiente**, introduzca el sitio remoto de salto siguiente al que se dirigen los paquetes de ruta virtual.

  > **Nota**
  >
  > Cualquier flujo que afecte a Virtual Path Application Routes no pasa por la ruta virtual dinámica.

- **Internet**: Identifica el tráfico de aplicaciones como tráfico de Internet y coincide con el servicio de Internet.
- **Intranet**: Identifica el tráfico de aplicaciones como tráfico de intranet y coincide con un servicio de intranet basado en las reglas de intranet. En el campo **Servicio de intranet**, seleccione un servicio de intranet que se utilizará para la ruta.
- **Local**: Identifica el tráfico de aplicaciones como local para el sitio y no coincide con ningún servicio. Se ignora el tráfico originado y destinado a una ruta local.

  > **Nota**
  >
  > Para el tipo de servicio local, una vez completada la clasificación de DPI, las rutas IP configuradas toman la decisión de redirección.

- **Túnel GRE**: Identificó el tráfico de la aplicación como destinado a un túnel GRE y coincide con el túnel GRE LAN configurado en el sitio. En **el campo Dirección IP de la Gateway**, introduzca la dirección IP de la puerta de enlace que debe estar en la subred del túnel LAN GRE. Seleccione **Elegibilidad basada en la puerta de enlace** para permitir que la ruta no reciba tráfico cuando la puerta de enlace no sea accesible.
- **Túnel IPSec de LAN**: Identificó el tráfico de la aplicación como destinado a un túnel IPSec de LAN y coincide con el túnel IPSec de LAN configurado en el sitio. En el campo **Túnel IPSec**, seleccione uno de los túneles IPSec configurados. Seleccione **Elegibilidad basada en túnel** para permitir que la ruta no reciba tráfico cuando el túnel no sea accesible.

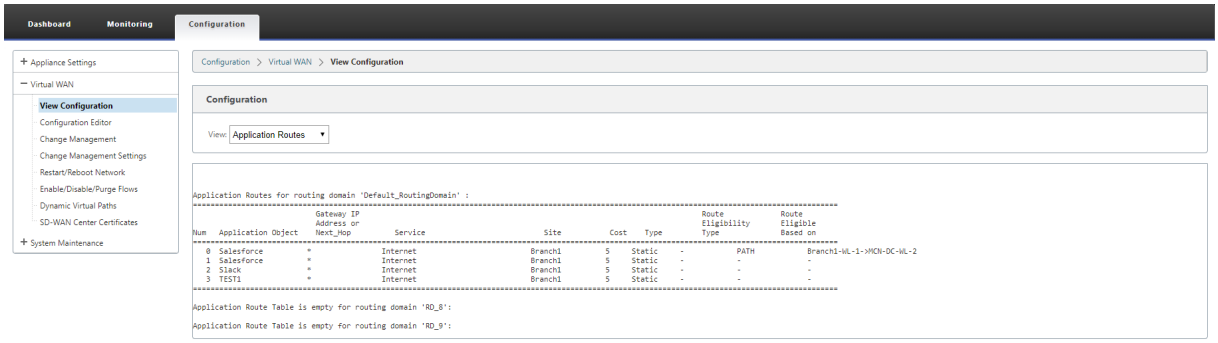
  > **Nota**
  >
  > Una vez que haya seleccionado un servicio para una aplicación personalizada, no lo cambie.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Elegibilidad Basada en Ruta:** Seleccione esta opción para habilitar la ruta para que no reciba tráfico cuando la ruta especificada esté inactiva. En el campo **Ruta** de acceso, especifique la ruta que se utilizará para determinar la elegibilidad de la ruta.

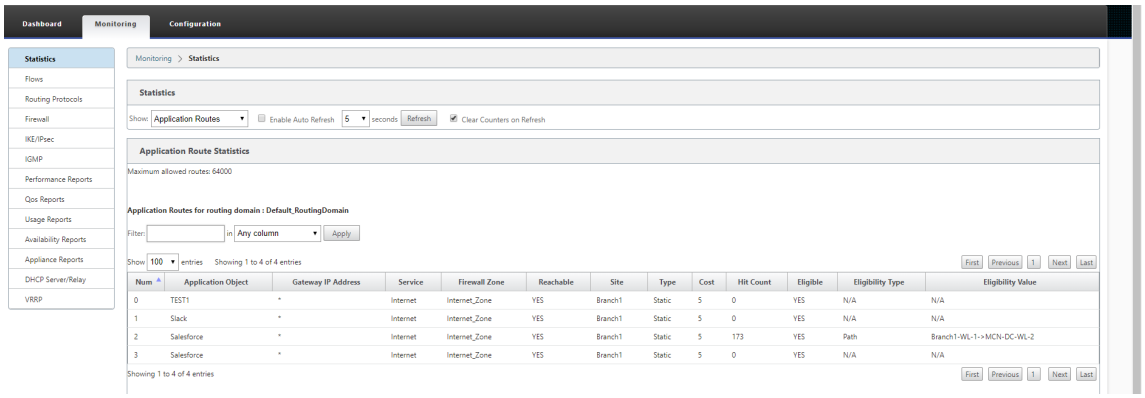
3. Haga clic en **Aplicar**.

Para ver las rutas de aplicación configuradas en el dispositivo SD-WAN. En la GUI de SD-WAN, vaya a **Configuración** > **Virtual WAN** > **Ver configuración**. Seleccione **Rutas de aplicación** en el menú implementable **Ver**.



Para ver datos estadísticos de las rutas de la aplicación:

1. En la GUI de SD-WAN, vaya a **Monitoring** > **Statistics**.
2. En la lista implementable **Mostrar**, seleccione **Rutas de aplicación**.



Puede ver las siguientes estadísticas:

- **Objeto Application**: Nombre del objeto Application.
- **Dirección IP de Gateway: Dirección**IP de puerta de enlace utilizada por los objetos de aplicación con el tipo de servicio de 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.
- **Accesible**: El estado de la ruta de la aplicación.
- **Sitio**: Nombre del sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.
- **Elegible**: Es la ruta de la solicitud elegible para enviar el tráfico.
- **Tipo de elegibilidad**: Tipo de condición de elegibilidad de ruta aplicada a esta ruta. El tipo de elegibilidad puede ser Ruta, Puerta de enlace o Túnel.
- **Valor de elegibilidad**: El valor especificado para la condición de elegibilidad de ruta.

> **Nota**
>
> En la versión actual, las aplicaciones que pertenecen a una familia de aplicaciones, tipo de coincidencia definido en un objeto de aplicación, no se pueden dirigir.

Solucionar problemas

Después de crear la ruta de la aplicación, puede confirmar que la aplicación se enruta correctamente al servicio deseado mediante la sección **Supervisión**.

Para ver si la aplicación se enruta 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

May 7, 2021

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 deexportación 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

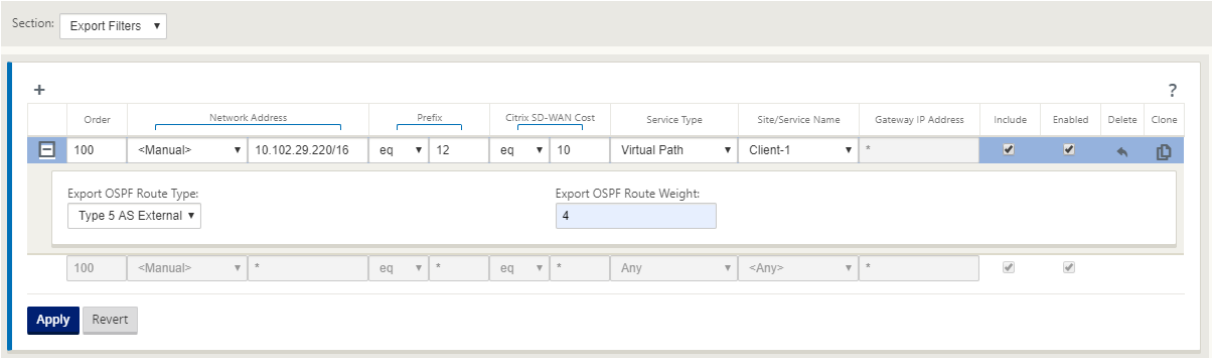
- Los filtros de importación se utilizan para aceptar o no las rutas que se reciben mediante vecinos OSPF y BGP basados en criterios de coincidencia específicos. Las reglas de filtro de importación son las reglas que se deben cumplir antes de importar rutas dinámicas en la base de datos de rutas SD-WAN. 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.

Configurar filtros de exportación

En el **Editor de configuración**, vaya a **Conexiones > Regiones > Sitio > OSPF**o **BGP > Exportar filtros**.



Utilice los siguientes criterios para crear cada filtro de exportación que quiera crear.

Criterios de campo	Descripción	Valor
Orden	El orden en el que se priorizan los filtros. El primer filtro que coincide con una ruta se aplica a esa ruta	100, 200, 300, 400, 500, 600
Dirección de red	Introduzca la **dirección IP** y la máscara de subred del objeto de red configurado que describe la red de la ruta	• Dirección IP
Prefix	Para hacer coincidir rutas por prefijo, elija un predicado de coincidencia en el menú e introduzca un prefijo de ruta en el campo adyacente	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to

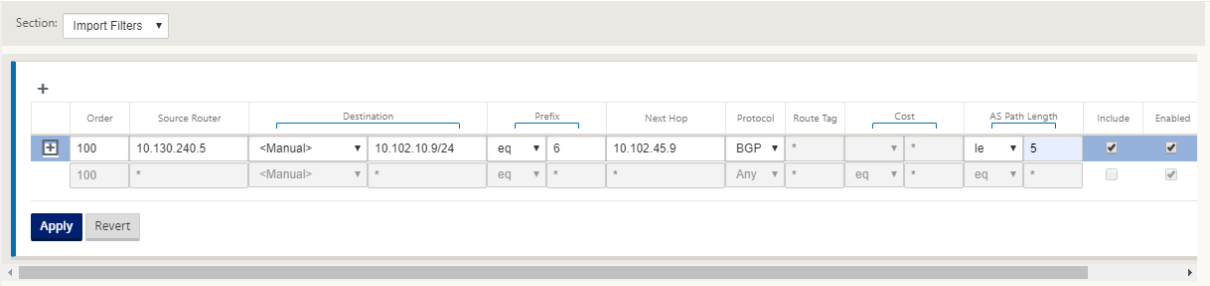
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Criterios de campo	Descripción	Valor
Coste Citrix SD-WAN	El método (predicado) y el coste de ruta SD-WAN que se utilizan para restringir la selección de rutas exportadas	Valor numérico
Tipo de servicio	Seleccione los tipos de servicio asignados a rutas coincidentes de una lista de servicios de Citrix SD-WAN	Cualquiera, Local, Ruta virtual, Internet, Intranet, Túnel GRE LAN, Túnel IPSec LAN
Nombre de sitio/servicio	Para Intranet, LAN GRE Tunnel e LAN IPSec Tunnel, especifique el nombre del tipo de servicio configurado para utilizar	Cadena de texto
Dirección IP de la puerta de enlace	Si elige LAN GRE Tunnel como Tipo de servicio, introduzca la IP de Gateway para el túnel	Dirección IP
Incluir	Active la casilla de verificación Incluir rutas que coincidan con este filtro. De lo contrario, las rutas coincidentes se ignoran	Ninguno
Habilitado	Active la casilla de verificación Habilitar este filtro. De lo contrario, el filtro se ignora	Ninguno
Eliminar	Seleccione el icono de eliminación para eliminar este filtro.	Ninguno
Clonar	Haga clic en el icono de clon para hacer una copia de un filtro existente	Ninguno

Configurar filtros de importación

En el **Editor de configuración**, vaya a **Conexiones > Regiones > Sitio > OSPF**o **BGP > Importar filtros**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Utilice los siguientes criterios para crear cada filtro de exportación que quiera crear.

Criterios de campo	Descripción	Valor
Orden	El orden en el que se priorizan los filtros. El primer filtro que coincide con una ruta se aplica a esa ruta	100, 200, 300, 400, 500, 600
Enrutador de origen	La dirección IP del enrutador de origen, es aplicable para iBGP	• Dirección IP
Destino	La dirección IP y la máscara de subred del destino de una ruta	• Dirección IP
Prefix	Para hacer coincidir rutas por prefijo, elija un predicado de coincidencia en el menú e introduzca un prefijo de ruta en el campo adyacente	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Siguiente salto	La dirección IP del salto siguiente	• Dirección IP
Protocolo	El protocolo de redirección con el que se aprende una ruta	OSPF o BGP
Etiqueta de ruta	La etiqueta de ruta OSPF que coincide con el filtro. Las etiquetas de ruta OSPF evitan los bucles de redirección durante la redistribución mutua entre OSPF y otros protocolos	Valor numérico
Coste	El coste de ruta utilizado para coincidir con las rutas OSPF para importar	Valor numérico

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

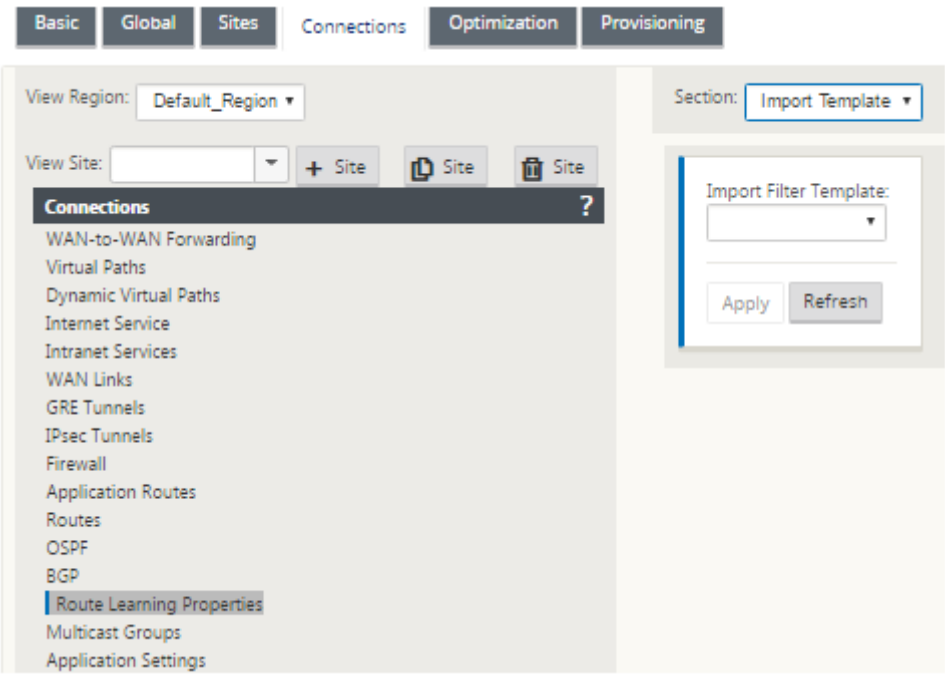
Criterios de campo	Descripción	Valor
Longitud de ruta AS	La longitud de ruta AS utilizada para coincidir con las rutas BGP para importar	Valor numérico
Incluir	Active la casilla de verificación Incluir rutas que coincidan con este filtro. De lo contrario, las rutas coincidentes se ignoran	Ninguno
Habilitado	Active la casilla de verificación Habilitar este filtro. De lo contrario, el filtro se ignora	Ninguno
Eliminar	Haga clic en el icono de eliminación para eliminar este filtro.	Ninguno
Clonar	Haga clic en el icono de clon para hacer una copia de un filtro existente	Ninguno

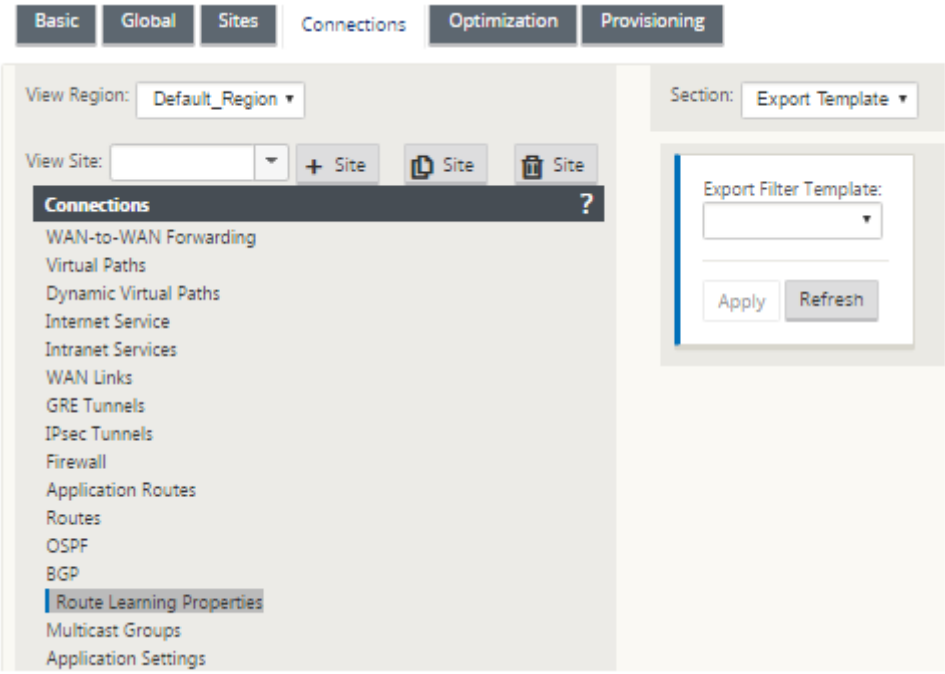
Configurar plantillas de filtro de directiva de ruta

Puede crear varias plantillas de filtro de importación o exportación con varias reglas de filtro y asociar la plantilla en cada sitio.

Las reglas de filtro de importación/exportación a nivel de sitio creadas por el usuario tienen más prioridad. Las reglas de plantilla siguen las reglas creadas por el usuario cuando se asocian al sitio en la sección **Aprendizaje de rutas** de Conexiones.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





Resumen de rutas

January 10, 2022

Con el aumento en el tamaño de las redes empresariales, los enrutadores necesitan mantener la gran

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 a los dispositivos de salto siguiente.

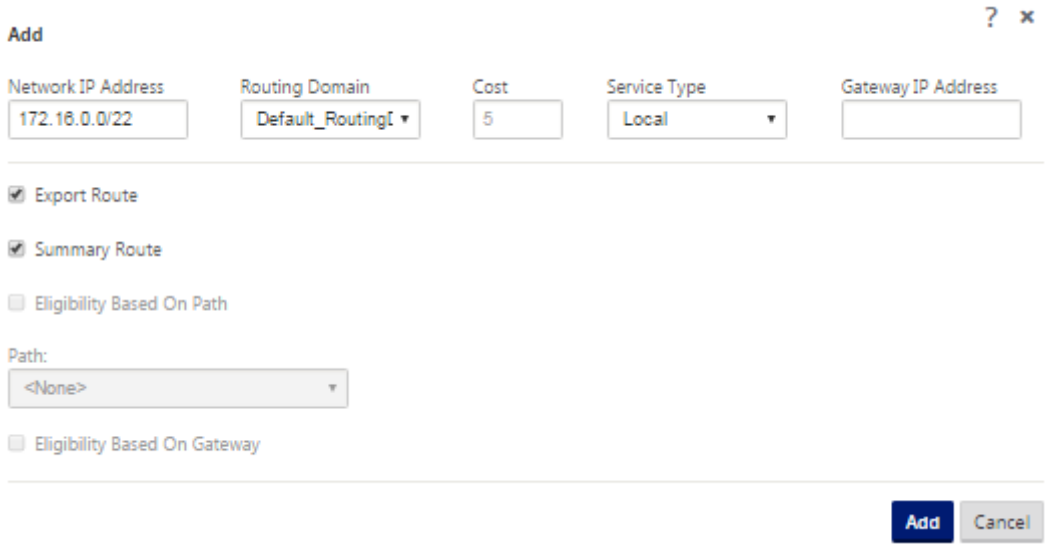
Para configurar una ruta de resumen para una subred local:

1. En el Editor de configuración, vaya a **Conexiones** > **Rutas** y haga clic en **+** para agregar una ruta.
2. En la página **Agregar ruta**, establezca los siguientes parámetros y, a continuación, haga clic en **Agregar**.

- **Dirección IP de red: La dirección**IP de la ruta de resumen calculada.
- **Coste**: Peso para determinar la prioridad de ruta para esta ruta. Las rutas de menor coste tienen prioridad sobre las rutas de mayor coste. El intervalo es de 1 a 65534.
- **Dominio**de enrutamiento: Protocolos de enrutamiento que proporcionan un único punto de administración para administrar una red corporativa, una red de sucursales o una red de centros de datos.
- **Tipo de servicio:** Seleccione Tipo de servicio local.

> **Nota**
>
> Solo puede seleccionar los tipos de servicio **Local** y **Descartar** para las rutas de resumen.

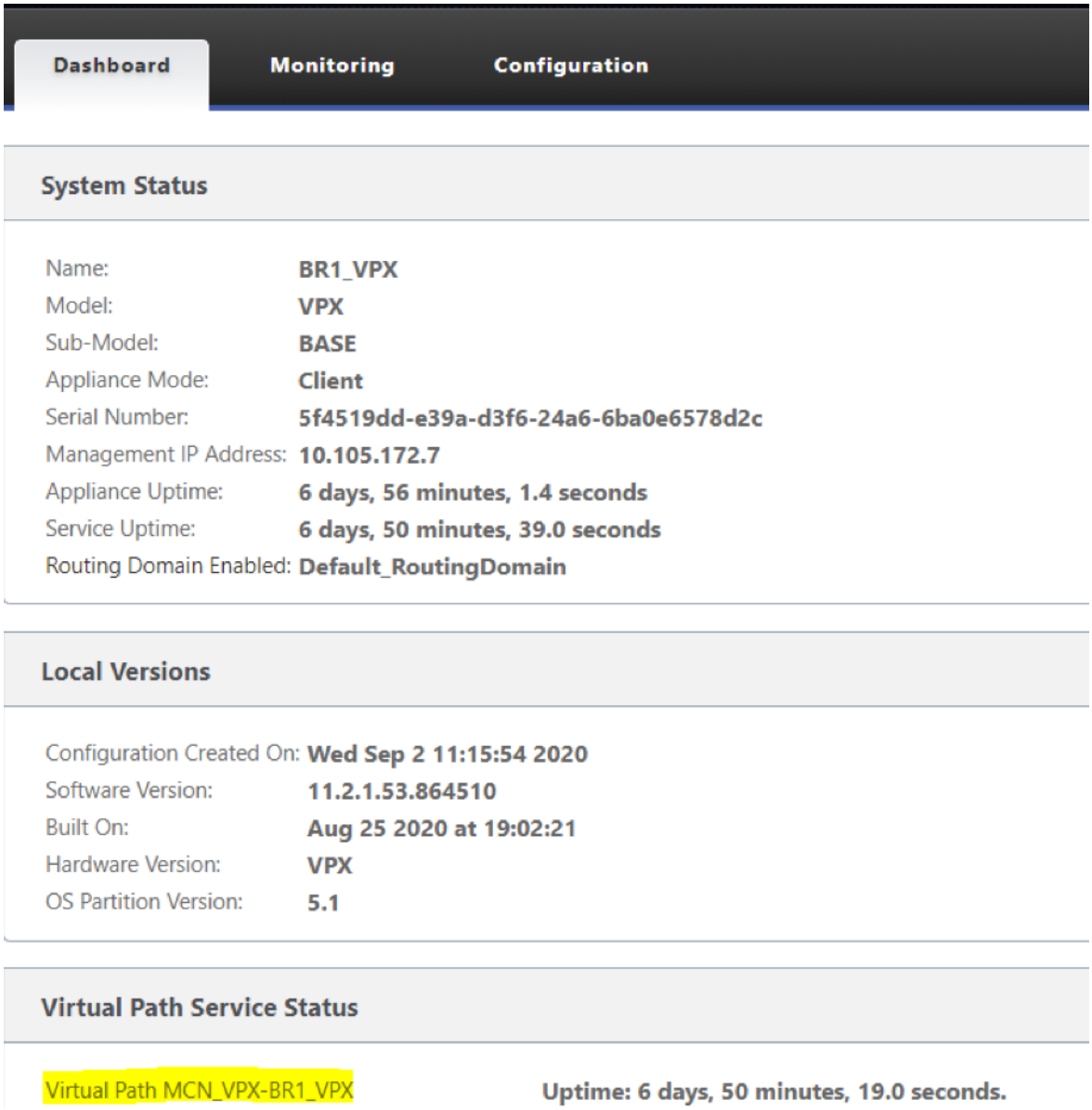
- **Dirección IP de puerta de enlace**: Dirección IP de puerta de enlace para esta ruta.
- **Exportar ruta:** Exporta la ruta a otros sitios conectados.
- **Ruta de resumen**: Anuncia la ruta como una única ruta de resumen a los demás dispositivos conectados, en lugar de todas las demás subredes coincidentes.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solucionar 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.

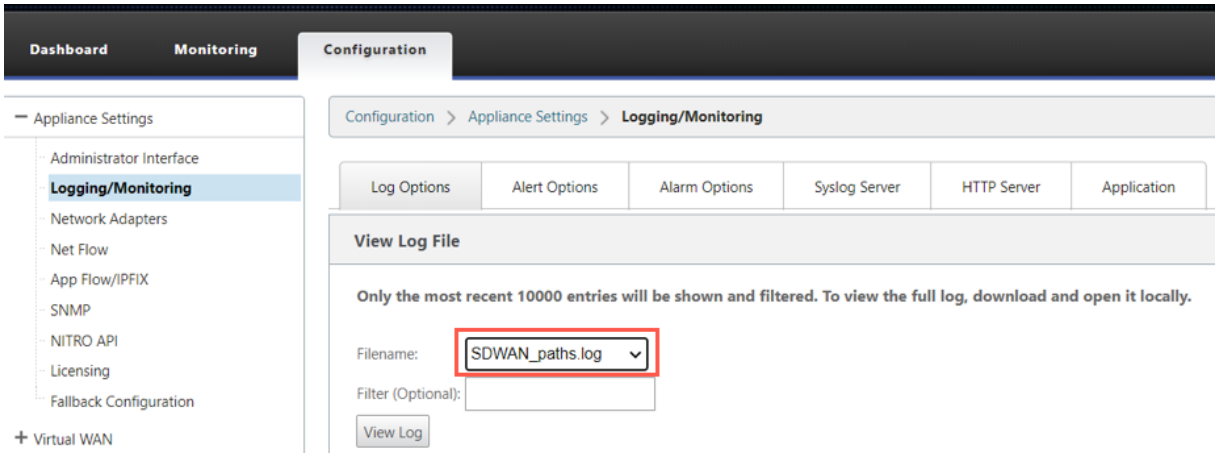


Si la ruta virtual está inactiva, compruebe el motivo en **Configuración > Registrar/Supervisión**.

Seleccione uno de los siguientes archivos de la lista desplegable **Nombre** de archivo para verificar:

- SDWAN_paths.log
- SDWAN_common.log

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Preferencia de protocolo

May 7, 2021

La preferencia de protocolo es una función específica de Citrix SD-WAN, que es similar a la distancia administrativa del router.

Cuando Citrix SD-WAN aprende un prefijo de ruta a través de rutas virtuales, protocolo OSPF o protocolo BGP, al mismo tiempo, sigue el siguiente orden de preferencia predeterminado.

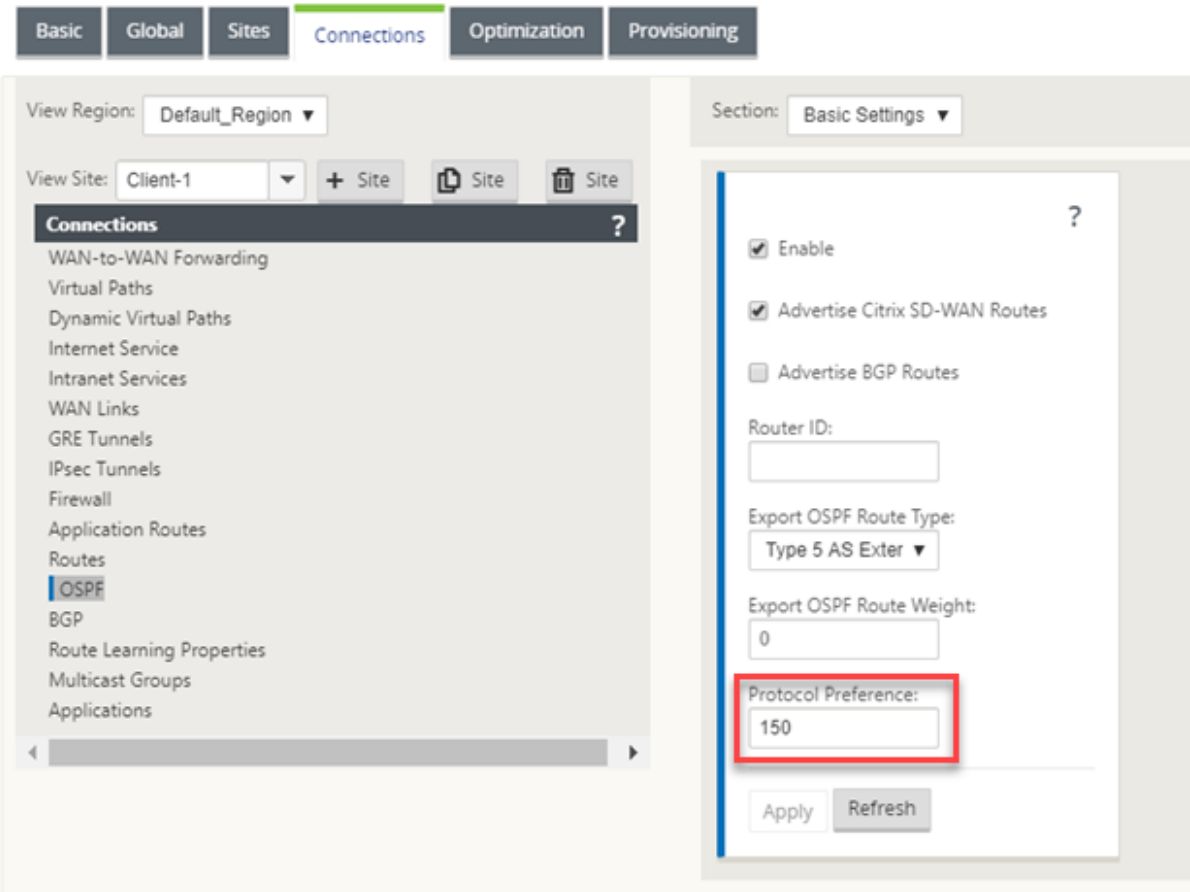
- OSPF -150
- BGP - 100
- SD-WAN - 250

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

También puede optar por utilizar el protocolo BGP sobre el protocolo OSPF estableciendo el valor de preferencia del protocolo, mientras configura el protocolo BGP o OSPF. Puede especificar una preferencia en el rango 100 a 200.

La información de precedencia de protocolo es local para el dispositivo Citrix SD-WAN y no se anuncia a elementos de red del mismo nivel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Enrutamiento de multidifusión

May 7, 2021

El enrutamiento 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 bajo demanda, Televisión IP y Videoconferencias son algunas de las tecnologías comunes que utilizan enrutamiento de multidifusión. Cuando habilita el enrutamiento de multidifusión en el dispositivo Citrix SD-WAN, el dispositivo actúa como enrutador de multidifusión.

Multidifusión específica de origen

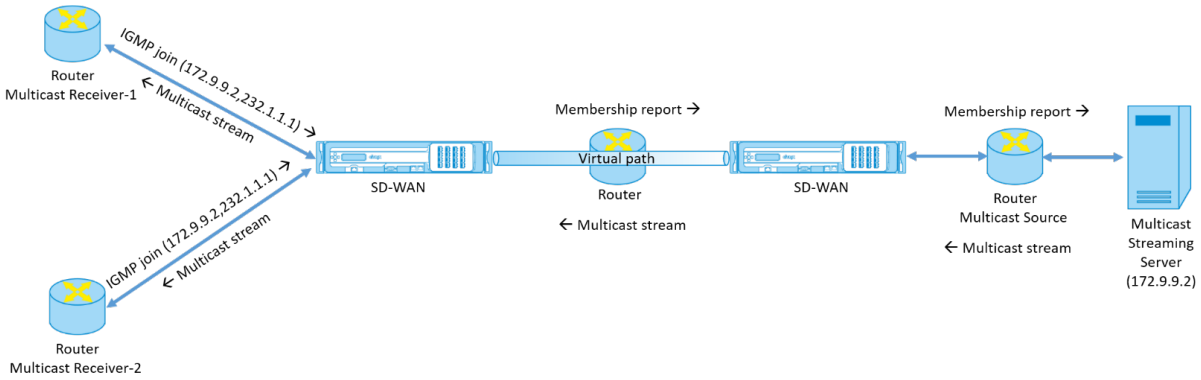
Los protocolos de multidifusión normalmente permiten a los receptores de multidifusión recibir tráfico de multidifusión desde cualquier origen. Con la multidifusión específica de origen (SSM), puede

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 232.0.0.0/8.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. El origen de multidifusión transmite la secuencia de multidifusión a través de la ruta de acceso virtual a los receptores de multidifusión.

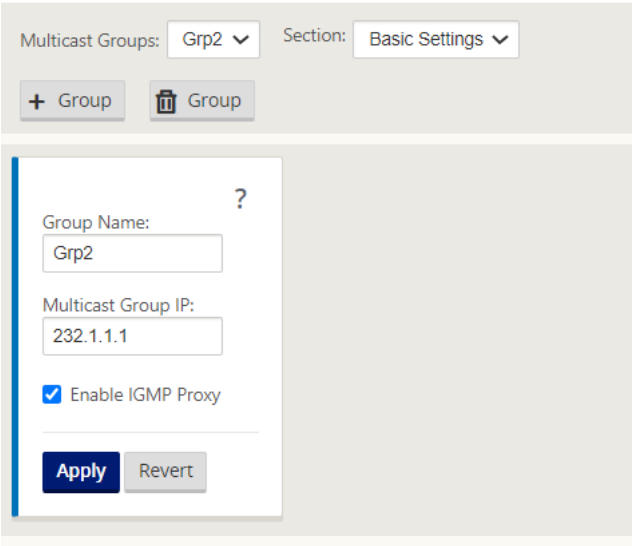
El tráfico del canal de control y el flujo de multidifusión fluyen a través de la ruta virtual establecida entre la rama y el centro de datos. La ruta de superposición Citrix SD-WAN asegura y aísla el tráfico de multidifusión de la degradación de WAN o de los apagones de enlaces.

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 232.0.0.0/8 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 el enrutamiento 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

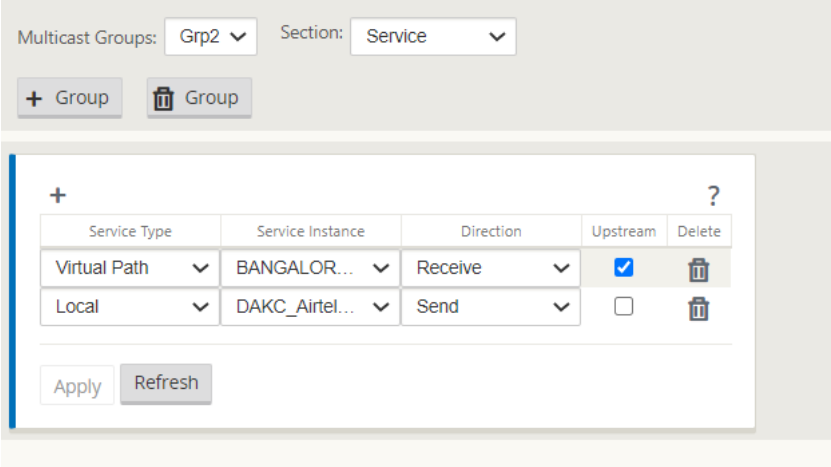
Para configurar la multidifusión en el dispositivo Citrix SD-WAN, vaya a **Conexiones** > **Grupos de multidifusión**. Cree un grupo de multidifusión proporcionando un nombre y una dirección IP para el grupo de multidifusión. Haga clic en **Habilitar proxy IGMP**.



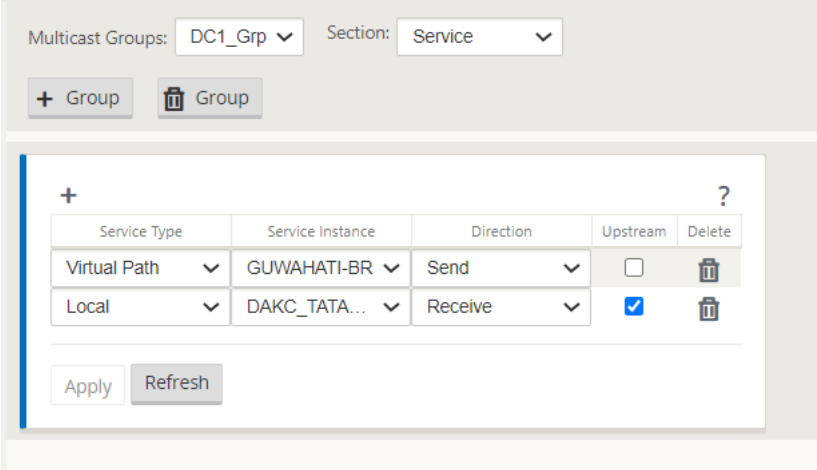
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure las rutas ascendentes y descendentes para los dispositivos de sucursal y centro de datos.

Para el dispositivo más cercano al receptor de multidifusión (Branch), el dispositivo recibe el tráfico de multidifusión en la interfaz de ruta virtual y envía el tráfico de la interfaz local hacia el receptor.



Para el dispositivo más cercano al origen de multidifusión (centro de datos), el dispositivo recibe el tráfico de multidifusión en la interfaz local y envía el tráfico en la Interfaz de ruta virtual.



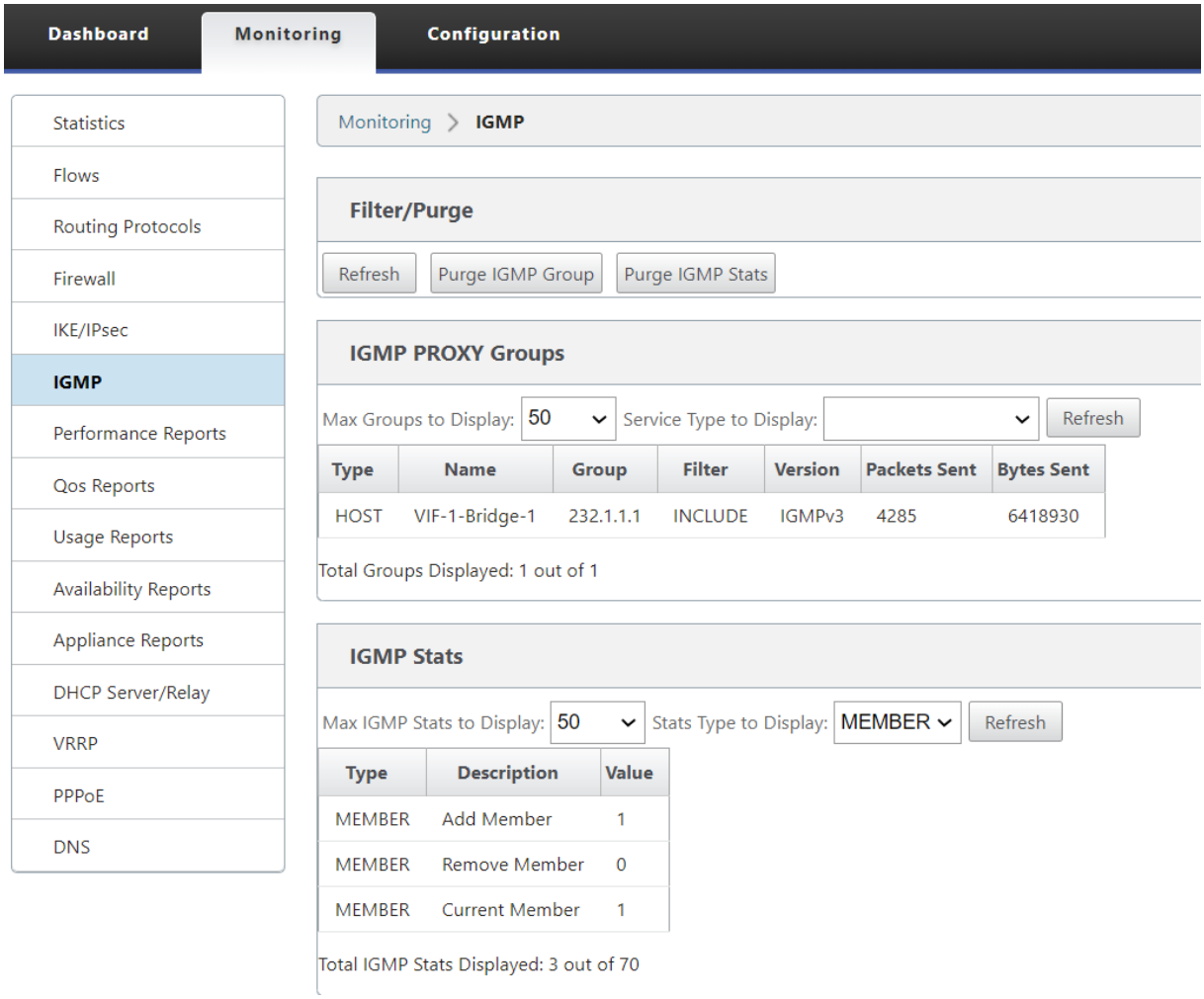
Supervisión

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 imagen siguiente muestra una combinación IGMP Versión 3 se ha iniciado y el tipo de filtro INCLUDE se utiliza para incluir direcciones de origen específicas. También puede ver las estadísticas de miembros IGMP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configurar el coste de ruta de ruta virtual

January 10, 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

remoto.

Esta función invalida o elimina el coste de reenvío de WAN a WAN.

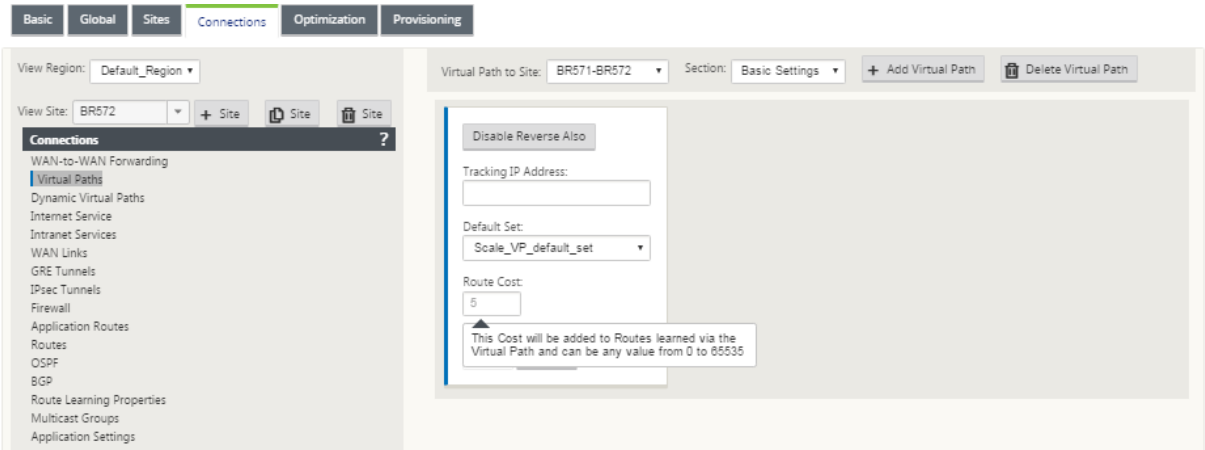
- Coste de ruta OSPF: Ahora puede importar coste de ruta OSPF (métrica tipo 1) activando **Copiar coste de ruta OSPF** en los filtros de importación. El coste de ruta OSPF se considera en la selección de ruta en lugar del coste SD-WAN. Se admite un coste de hasta 65534 en lugar de 15, pero es aconsejable 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 la 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 ruta a través de una ruta virtual específica en lugar del coste predeterminado del sitio. Con esto, podemos manipular qué centro de datos se prefiere 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 ruta de VP desaprueba el coste de reenvío de WAN a WAN que existía en versiones 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cómo configurar el coste de ruta de ruta virtual

Puede configurar Ruta de ruta virtual en la GUI de SD-WAN en **Conexiones** > **Ver región** > **Ver sitio > Rutas virtuales > Configuración básica**. Todas las rutas se instalan con coste básico de Citrix SD-WAN + coste de ruta VP para influir en los costes de ruta a través de múltiples rutas virtuales.



Caso de uso:

Por ejemplo, hay subredes 172.16.2.0/24 y 172.16.3.0/24. Supongamos que hay dos centros de datos DC1 y DC2 que utilizan ambas subredes para transmitir tráfico a SD-WAN. Con el coste de ruta de ruta virtual predeterminado, no puede influir en el enrutamiento, ya que depende de qué ruta se instaló primero, puede ser el DC2 primero o el DC1 siguiente.

Con la ruta virtual, puede influir específicamente en la ruta virtual de DC2 para que tenga un coste de ruta de ruta virtual más alto (por ejemplo, 10), mientras que DC1 tiene el coste de ruta VP predeterminado de 5. Esta manipulación ayuda a instalar rutas con DC1 primero y DC2 siguiente para ambos.

Puede tener cuatro rutas, dos rutas a 172.16.2.0/24; una a través de DC1 con menor coste y luego a través de DC2 con mayor coste, y 2 más para 172.16.3.0/24.

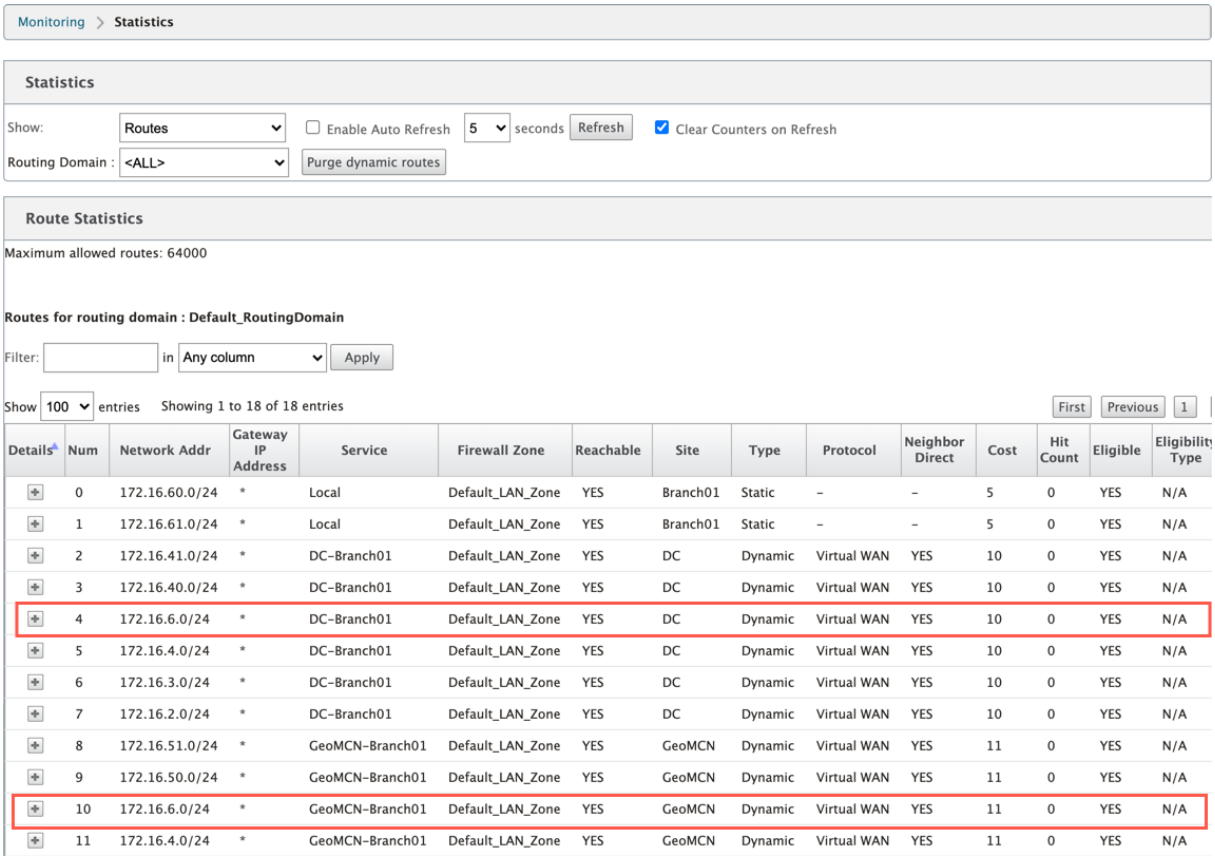
Supervisión y solución de problemas

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 enrutamiento, 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 figura 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

Configurar el protocolo de redundancia de enrutador virtual

May 7, 2021

Virtual Router Redundancy Protocol (VRRP) es un protocolo ampliamente utilizado que proporciona redundancia de dispositivos para eliminar el único punto de error inherente al entorno estático de redirección predeterminado. VRRP le permite configurar dos o más enrutadores 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 copia de seguridad se hace cargo automáticamente si falla el router principal/maestro. En una configuración VRRP, el router maestro envía un paquete VRRP conocido como un anuncio a los routers de copia de seguridad. Si el router maestro deja de enviar el anuncio, el router de copia de seguridad establece el temporizador de intervalo. Si no se recibe ningún anuncio dentro de este período de retención, el router de copia de seguridad 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

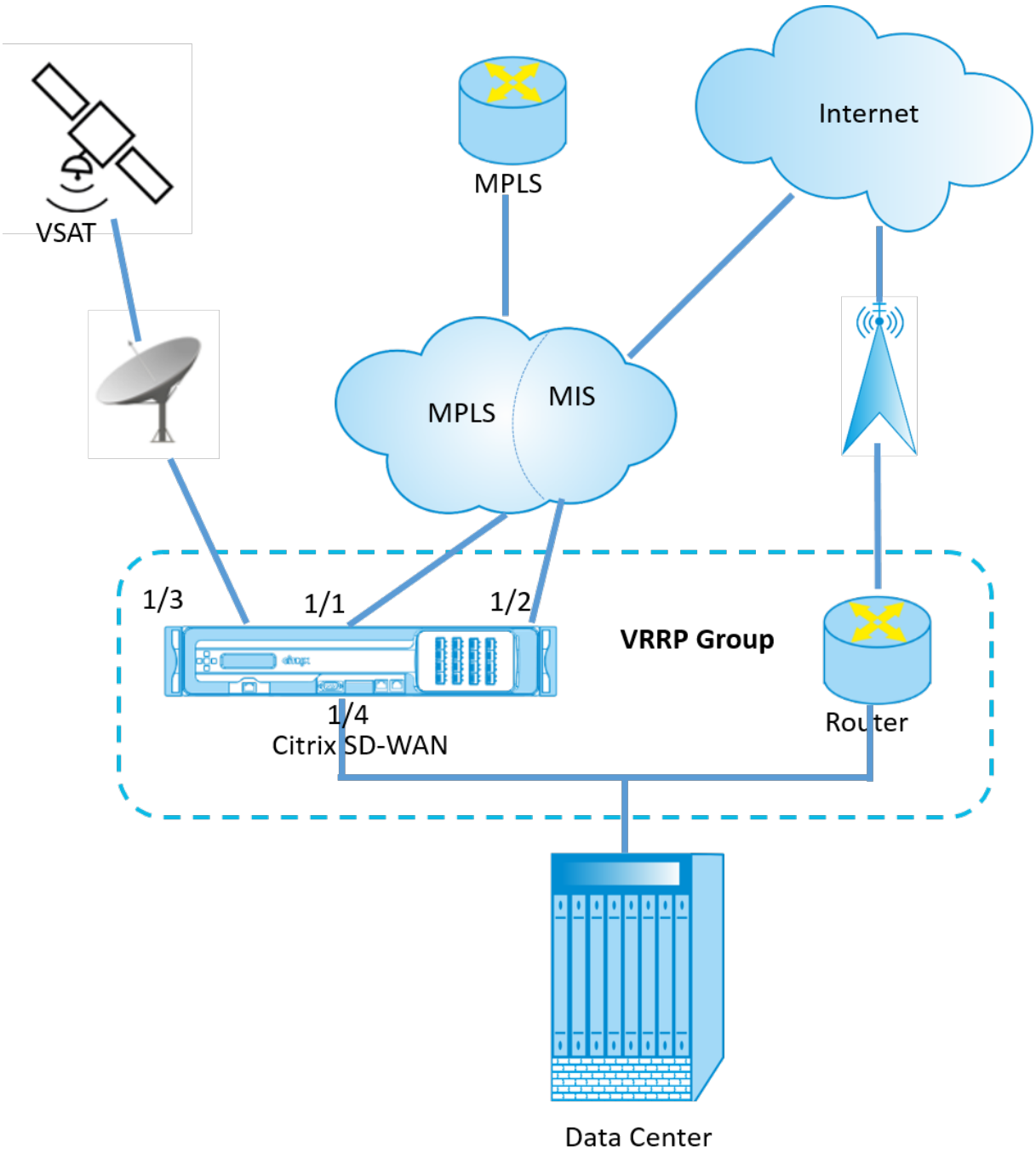
de elección se inicia de nuevo si el maestro falla, un nuevo router se une al grupo o un router existente abandona el grupo.

VRRP garantiza un path predeterminado de alta disponibilidad sin configurar el enrutamiento dinámico o los protocolos de descubrimiento de enrutadores en cada host final.

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.

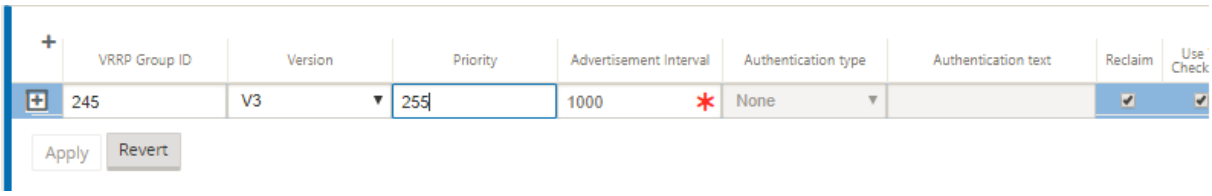
El siguiente diagrama de red muestra un dispositivo Citrix SD-WAN y un enrutador configurado como un grupo VRRP. El dispositivo SD-WAN está configurado para ser el maestro. Si se produce un error en el dispositivo SD-WAN, el router de copia de seguridad se llevará a cabo en milisegundos, lo que garantiza que no haya tiempo de inactividad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para configurar la instancia VRRP:

1. En el Editor de configuración, vaya a **Sitios > Nombre del sitio > VRRP** y haga clic en **+**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Configure una instancia VRRP. Introduzca los valores de los siguientes campos:

- **ID de grupo VRRP**: El ID del grupo VRRP. El ID de grupo debe ser un intervalo de valores entre 1 y 255. También se debe configurar el mismo ID de grupo en los routers de respaldo.

> **Nota**
>
> Actualmente puede configurar hasta cuatro grupos.

- **Versión**: La versión del protocolo VRRP. Puede elegir entre el protocolo VRRP V2 y V3.
- Prioridad**: prioridad** del dispositivo Citrix SD-WAN para el grupo VRRP. El rango de prioridad es 1-254. Establezca este valor como máximo (254) para que el dispositivo SD-WAN sea el maestro.

> **Nota**
>
> Si el router es el propietario de la dirección IP VRRP, la prioridad se establece en 255 de forma predeterminada.

- **Anuncio Interva**l: Frecuencia en milisegundos, con la que se envían los anuncios VRRP cuando el dispositivo SD-WAN es el maestro. El intervalo de anuncio predeterminado es de un segundo.
- **Tipo de autenticación:** puede elegir **Texto sin formato** para introducir una cadena de autenticación. La cadena de autenticación se envía como texto sin cifrar en los anuncios VRRP. Seleccione **Nada** si no quiere configurar la autenticación.
- **Texto de autenticación**: Cadena de autenticación que se enviará en el anuncio VRRP. Esta opción está habilitada si el **tipo de autenticación** es **Texto sin formato**.

> **Nota**
>
> La autenticación se admite en VRRPv2.

- **Reclamación:** permite la preferencia cuando la prioridad del dispositivo SD-WAN es más alta en el grupo VRRP. Esto se utiliza en el proceso de elección del VRRP.
- **Use V2 Checksum**: Permite la compatibilidad con dispositivos de red de terceros para VRRPV3. De forma predeterminada, VRRPv3 utiliza el método de cálculo de suma de comprobación v3. Algunos dispositivos de terceros solo pueden admitir el cálculo de suma de comprobación VRRPv2. En tales casos, habilite esta opción.

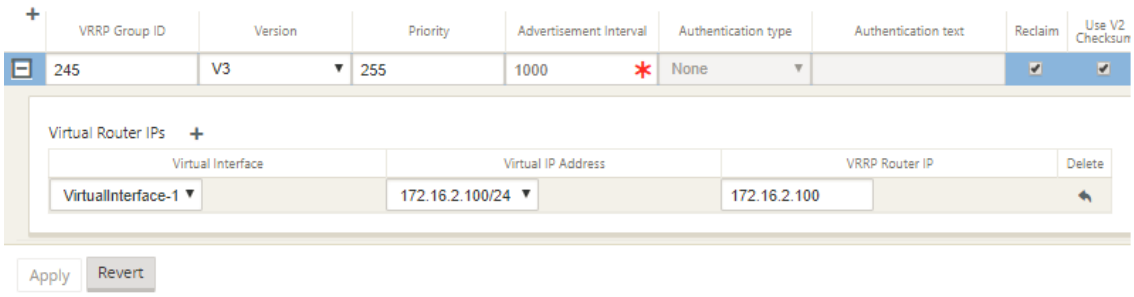
Configure la dirección IP VRRP. Introduzca los valores para los siguientes campos y haga clic en **Aplicar**.

- **Interfaz virtual**: La interfaz virtual que se utilizará para VRRP. Elija una de las interfaces virtuales configuradas.

- **Dirección IP virtual**: Dirección IP virtual asignada a la interfaz virtual. Elija una de las direcciones IP virtuales configuradas para la interfaz virtual.

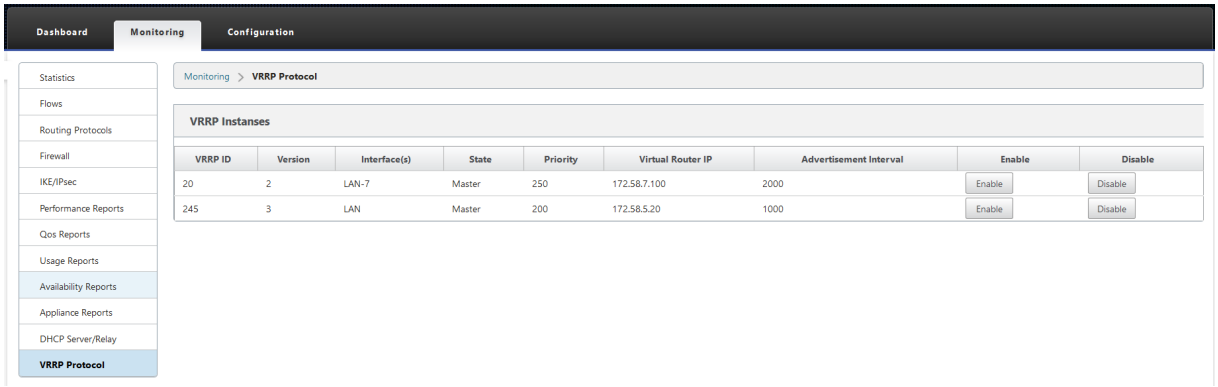
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **IP del enrutador VRRP**: La dirección IP del enrutador virtual para el grupo VRRP. De forma predeterminada, la dirección IP virtual del dispositivo SD-WAN se asigna como dirección IP del enrutador virtual.



Estadísticas de VRRP

Puede ver las estadísticas VRRP en **Supervisión** > **Protocolo VRRP**.



Puede ver los siguientes datos estadísticos:

- **ID VRRP**: ID de grupo VRRP
- **Versión:** La 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 anuncio:** 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 VRRP en el dispositivo SD-WAN.

Limitaciones

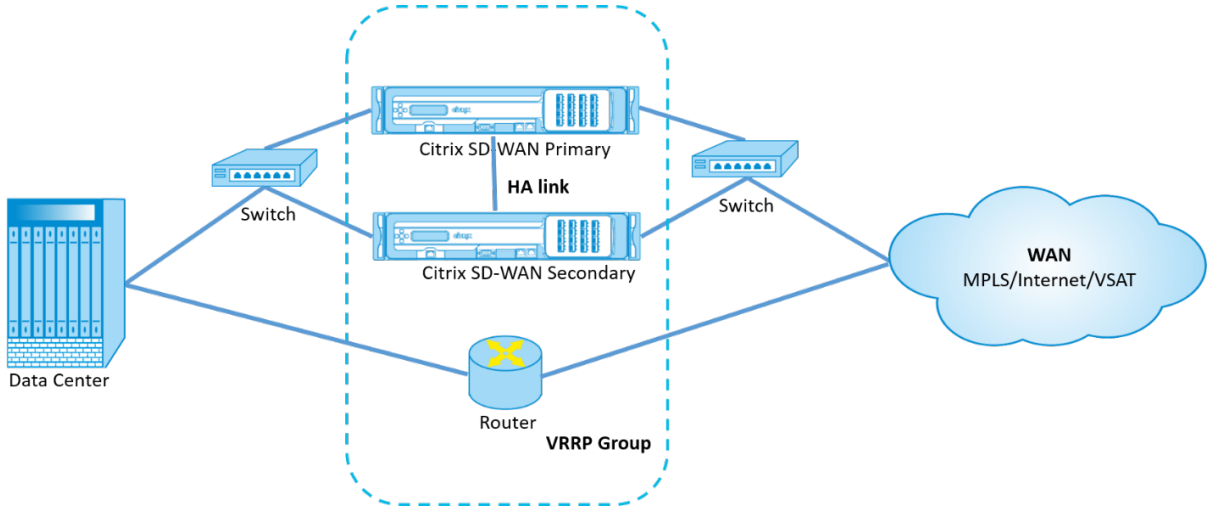
- VRRP se admite en la implementación del modo de puerta de enlace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Puede configurar hasta cuatro ID de VRRP (VRID).
- Hasta 16 interfaces de red virtual pueden participar en VRID.

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 roles activos/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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurar objetos de red

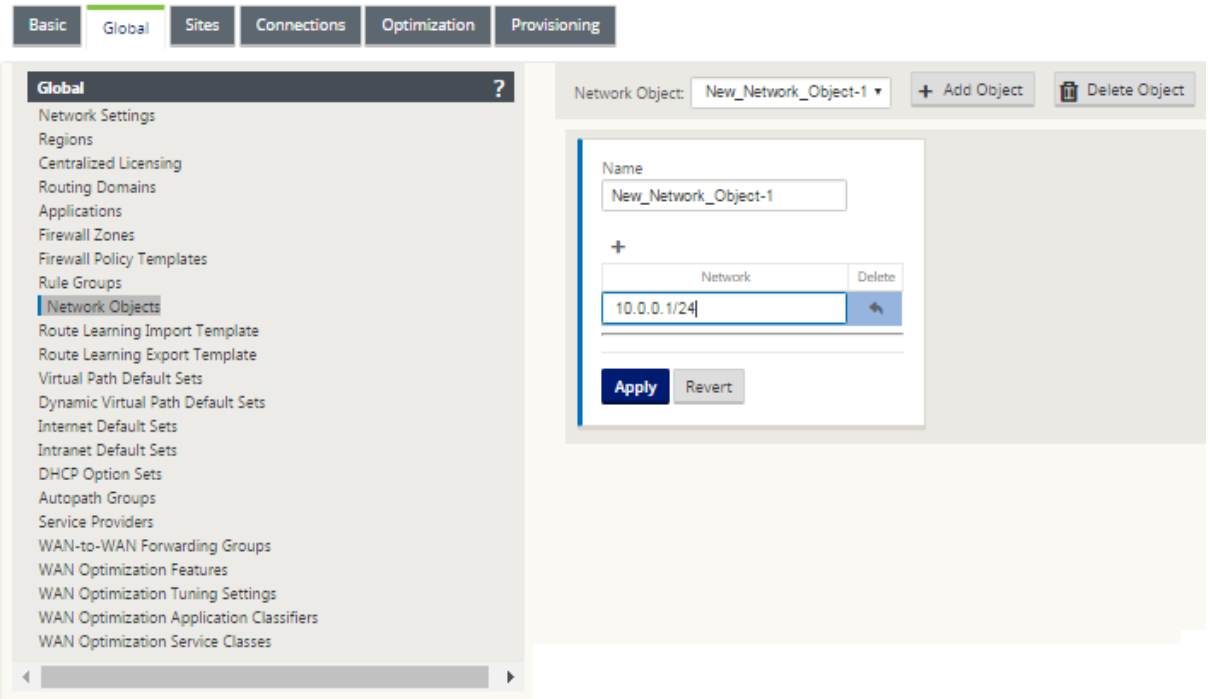
May 7, 2021

Citrix SD-WAN presenta la opción de agregar objetos de red en el panel **Global** del Editor de configuración. Puede agrupar varias subredes y hacer referencia a un único objeto de red al definir un filtro de ruta en lugar de crear un filtro para cada subred.

Para configurar objetos de red:

1. En el **Editor de configuración**, vaya a **Global**→ **Objetos de red**, haga clic en **Agregar (+)**.
2. Haga clic en **Agregar (+)** en Redes.
3. Introduzca la **dirección IP** y la **subred** del nuevo objeto de red.
4. Haga clic en **Aplicar** para guardar la configuración.

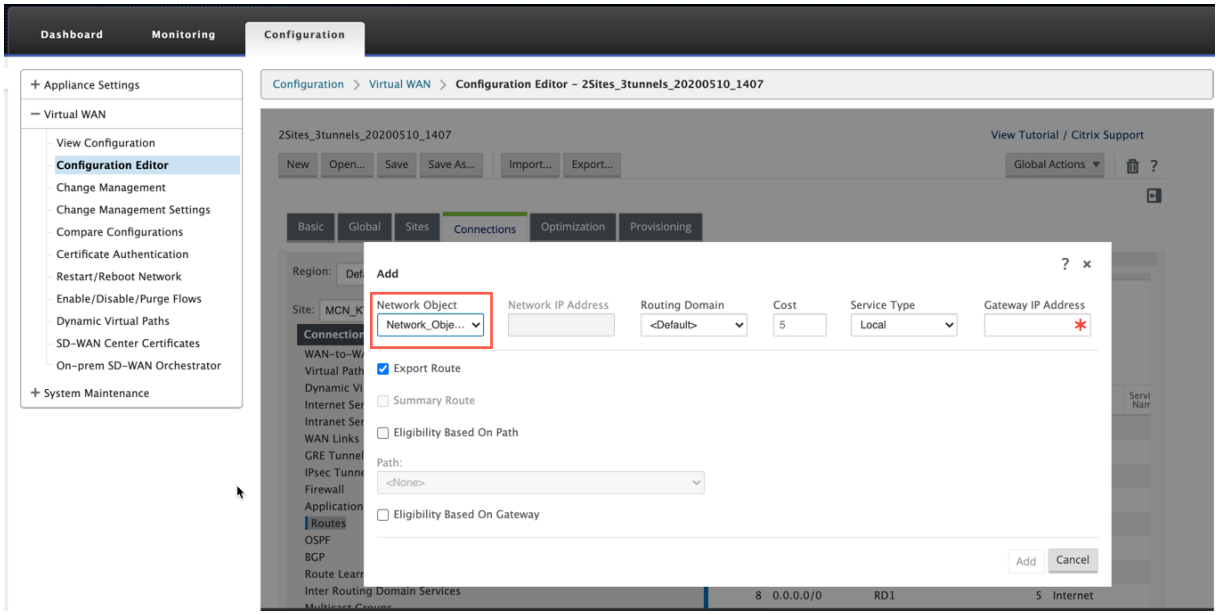
Para modificar el nombre del objeto de red, haga clic en el nombre del objeto de red e introduzca un nombre nuevo.



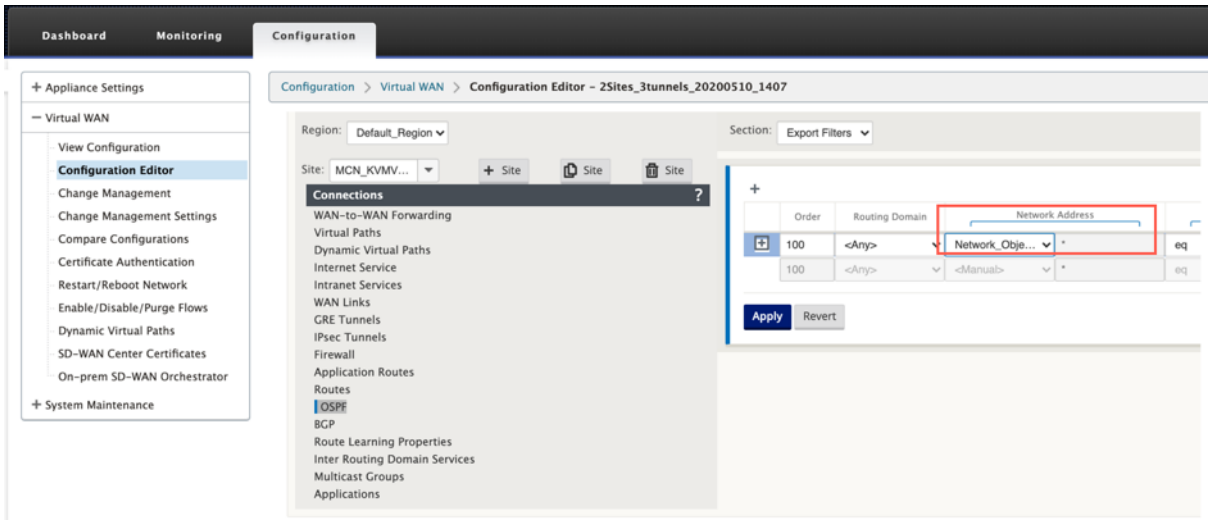
Las siguientes funciones están utilizando los objetos de red:

- Rutas (**Editor de configuración > Conexiones > Rutas** Haga clic en **+** > **Objeto de red**)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

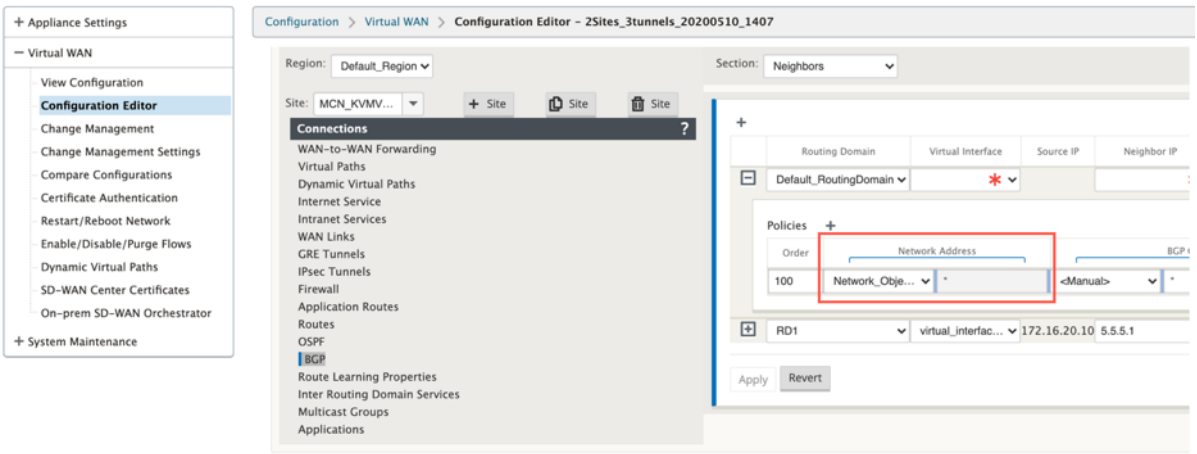


- Filtros de importación y exportación de BGP y OSPF (**Editor de configuración > Conexiones > BGP/OSPF > Exportar/Importar filtros** clic **+ > Dirección de red**)



- Directivas de vecino BGP (**Editor de configuración > Conexiones > BGP > Vecinos > Directivas** haga clic **+ > Dirección de red**)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Soporte de enrutamiento para segmentación de LAN

May 7, 2021

Los dispositivos SD-WAN Standard y Premium (Enterprise) Edition implementan la segmentación de LAN en distintos sitios donde se implementa cualquiera de los dispositivos. Los dispositivos reconocen y mantienen un registro de las VLAN del lado 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 o Premium (Enterprise) Edition.

La capacidad anterior se implementa mediante una tabla de redirección y reenvío virtual (VRF) que se mantiene en el dispositivo SD-WAN Standard o Premium (Enterprise) Edition, que realiza un seguimiento de los intervalos de direcciones IP remotas accesibles a un segmento LAN local. Este tráfico de VLAN a VLAN seguiría recorriendo la WAN a través de la misma ruta virtual preestablecida entre los dos dispositivos (no es necesario crear nuevas rutas).

Un ejemplo de caso de uso para esta funcionalidad es que un administrador de WAN puede segmentar el entorno de red de sucursales locales a través de una VLAN y proporcionar algunos de esos segmentos (VLAN) acceso a segmentos de LAN del lado de CC que tienen acceso a Internet, mientras que otros pueden no obtener dicho acceso. La configuración de las asociaciones de VLAN a VLAN se logra a través del Editor de configuración de MCN en la interfaz web de administración de SD-WAN.

Emparejamiento seguro

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El dispositivo Premium (Enterprise) Edition se puede instalar en el centro de datos y puede iniciar el emparejamiento seguro automático o manual, crear un perfil SSL y una clase de servicio asociada, y unir el dispositivo a un controlador de dominio de Windows para permitir a los usuarios/administradores utilizar la función ampliada de WANOP independiente dispositivo.

A continuación se presentan los modos de implementación compatibles con el Peering automático y el Emparejamiento seguro manual:

Implementaciones de pares de seguridad automática:

Para realizar un emparejamiento seguro automático a un dispositivo PE desde una WANOP/SDWAN SE/WANOP independiente en el sitio de DC.

Pasos para iniciar esta implementación:

- El dispositivo WANOP DC está en modo Listen ON (2312/Cualquier puerto no estándar) y Branch PE está en modo CONNECT-TO.
- WANOP DC inicia el emparejamiento seguro automático en un dispositivo PE que instala los certificados de CA privada y los pares de claves CERT y configura CONNECT-To en el dispositivo PE con WANOP LISTEN-ON IP.

Para realizar el emparejamiento de seguridad automática iniciado desde el dispositivo PE en el sitio de DC y en el dispositivo PE del sitio de sucursal.

Pasos para iniciar esta implementación:

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443). Branch PE está en modo CONNECT-A.
- El dispositivo de PE DC inicia el emparejamiento seguro automático en un dispositivo de PE Branch que instala los certificados de CA privada y los pares de CERT KEY y configura CONNECT-To en el dispositivo de PE Branch con IP LISTEN-ON de DC PE.
- LISTEN-ON IP para PE está en la IP de interfaz asociada al dominio de redirección para el que está habilitado “Redirigir a WANOP”.

Auto Emparejamiento seguro iniciado desde PE Appliance en el sitio de DC y en la sucursal con el dispositivo WANOP/ SDWAN SE.

Pasos para iniciar esta implementación:

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443). Branch WANOP/SD-WAN SE está en modo CONNECT-A.
- El dispositivo de PE DC inicia el emparejamiento seguro automático en el dispositivo Branch WANOP/SD-WAN SE que instala los certificados de CA privada y los pares de CERT KEY y configura CONNECT-To en el dispositivo PE con IP LISTEN-ON de DC PE.

Implementaciones de pares seguros manuales:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Emparejamiento seguro manual iniciado desde un dispositivo PE en el sitio de DC a un dispositivo de PE de Branch.

Pasos para iniciar esta implementación:

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443). Branch PE está en modo CONNECT-A.
- LISTEN-ON IP para PE está en la IP de interfaz asociada al dominio de redirección para el que está habilitado "Redirigir a WANOP".
- Cargue manualmente certificados de par de CA y clave de certificado obtenidos del origen auténtico de la entidad emisora de certificados.

Manual Emparejamiento seguro iniciado desde el dispositivo PE en el sitio de DC a la sucursal WANOP/SDWAN-SE Appliance.

Pasos para iniciar esta implementación:

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443). Branch WANOP/SD-WAN SE está en modo CONNECT-A.
- LISTEN-ON IP para PE está en la IP de interfaz asociada al dominio de redirección para el que está habilitado "Redirigir a WANOP"
- Cargue manualmente certificados de par de CA y clave de certificado obtenidos del origen auténtico de la entidad emisora de certificados.

Emparejamiento automático seguro con dispositivos PE desde dispositivos SD-WAN SE y WANOP independientes en el sitio de DC

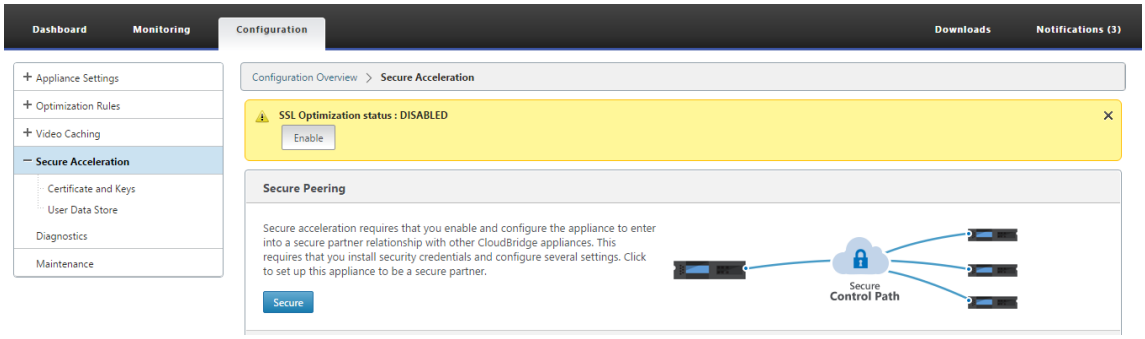
May 7, 2021

Para realizar un emparejamiento seguro automático en un dispositivo PE desde un dispositivo SD-WAN SE y WANOP independiente en el lado DC:

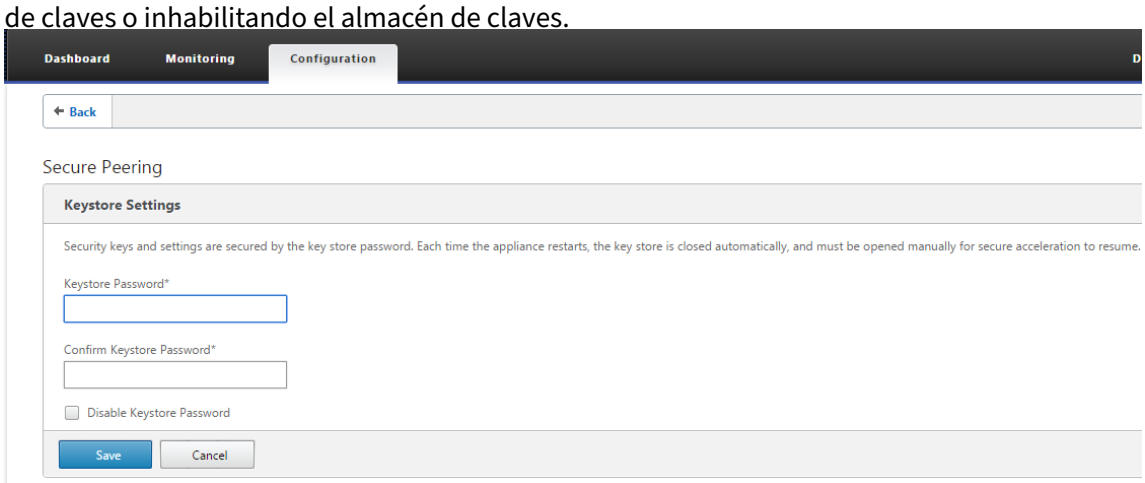
- El dispositivo WANOP DC está en modo Listen ON (2312/Cualquier puerto no estándar).
- El dispositivo Branch PE está en modo CONNECT-A.
- WANOP DC inicia el emparejamiento seguro automático en un dispositivo PE que instala los certificados de CA privada y los pares de claves CERT y configura CONNECT-To en el dispositivo PE con WANOP LISTEN-ON IP.

1. En un dispositivo WANOP independiente en el centro de datos, haga clic en **Secure** en el panel **Emparejamiento seguro** de la página **Aceleración segura**.

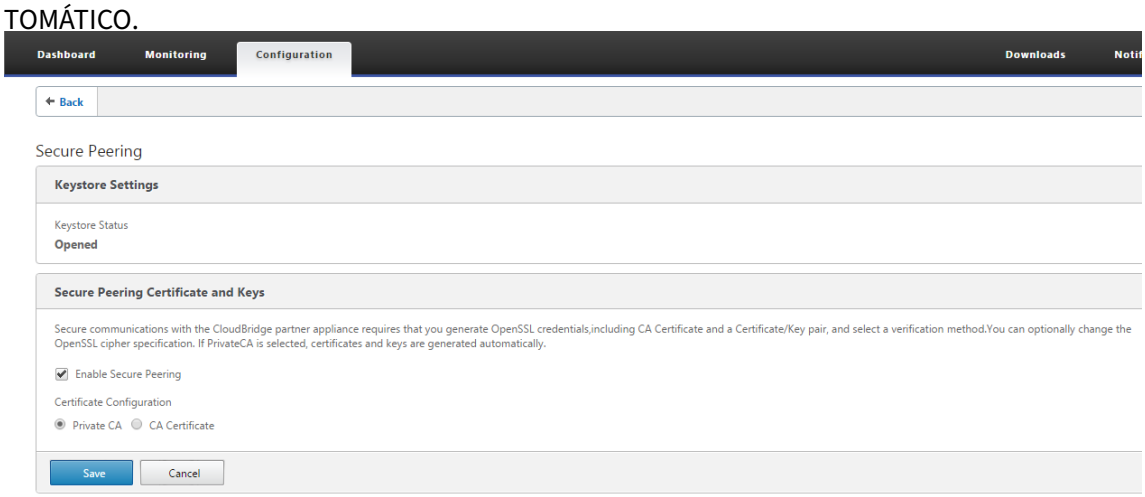
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Configure la configuración del almacén de **claves proporcionando la contraseña del almacén** de claves o inhabilitando el almacén de claves.



3. **Active Peering seguro** seleccionando **CA privada** para realizar PEERING SEGURO AUTOMÁTICO.

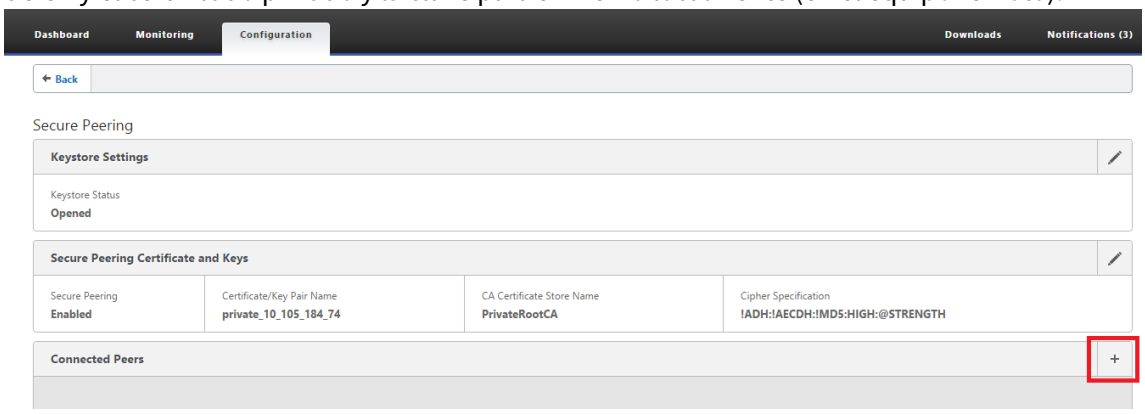


4. El certificado de CA de nivel de dispositivo y el certificado y clave privados se generan en la WANOP local y se muestra una tabla para agregar un PEER REMOTE TO Realizar el emparejamiento seguro AUTO con.

5. Haga clic en el icono '**+**'y aparecerá una ventana emergente para agregar la dirección IP con nombre de usuario y contraseña. Después de la autenticación correcta con la IP remota con las

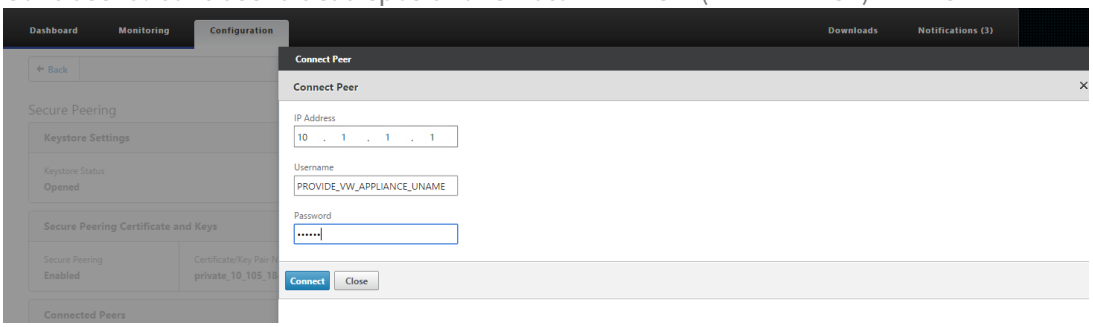
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

credenciales proporcionadas, se envía una solicitud al equipo remoto que instala el certificado de CA y el certificado privado y la clave para sí mismo localmente (en el equipo remoto).

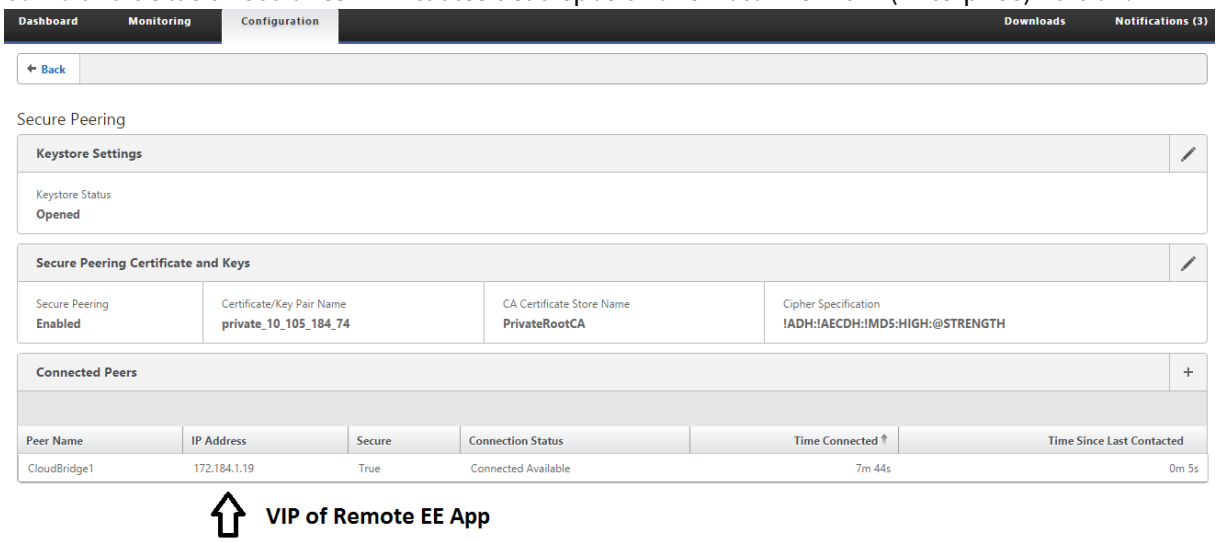


Nota

- Dirección IP —Dirección IP del dispositivo PREMIUM (ENTERPRISE) EDITION EDITION
- Nombre de usuario —Nombre de usuario de PREMIUM (ENTERPRISE
- Contraseña: contraseña del dispositivo remoto PREMIUM (ENTERPRISE) EDITION



Después de la autenticación correcta, verá Secure Peering como TRUE y la dirección IP del socio como una de las direcciones IP virtuales del dispositivo remoto Premium (Enterprise) Edition.

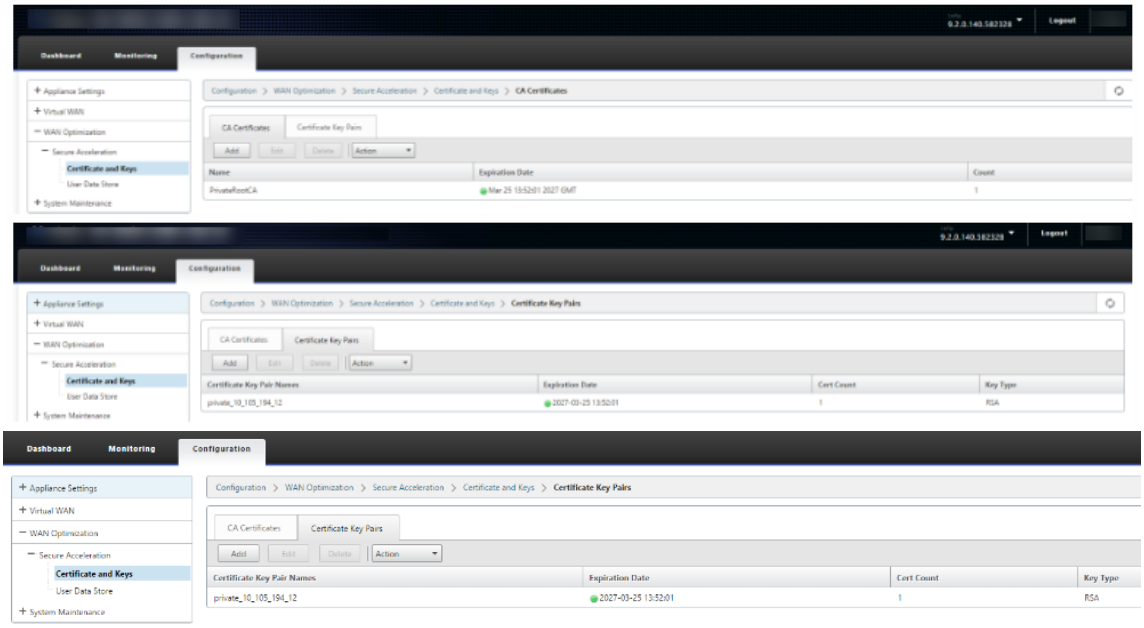


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

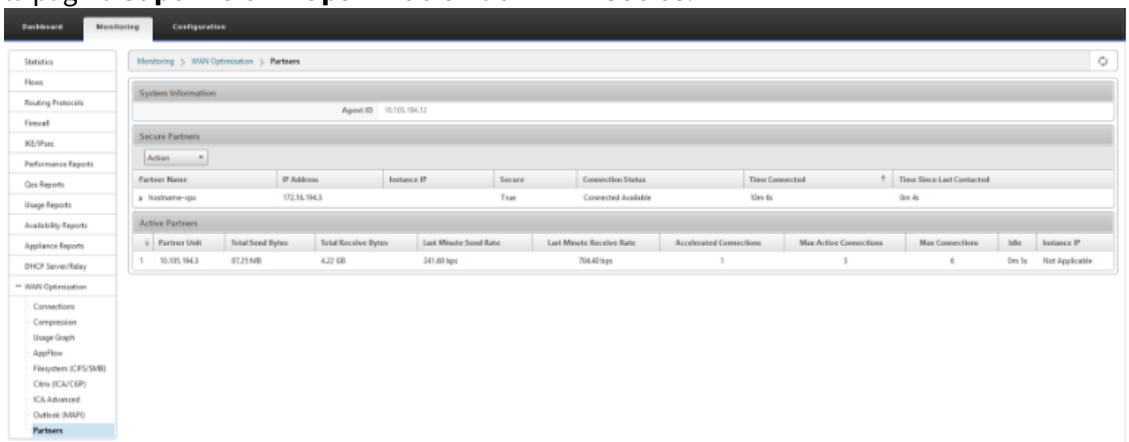
Supervisión

Consulte la información de socios seguros en el dispositivo Premium (Enterprise) Edition en **WANOPTIMIZATION** > **Asociados de negocios** en la página **Supervisión**.

1. El cifrado del almacén de datos se puede realizar en el dispositivo Premium (Enterprise) Edition mediante la activación de funciones desde el MCN en el nodo Optimization para un dispositivo Premium (Enterprise) Edition.
2. Para un dispositivo Premium (Enterprise) Edition, el emparejamiento seguro siempre está habilitado.
3. Para validar si el par de **CA privada** y **clave de certificado privado** se genera correctamente, revise la información siguiente.

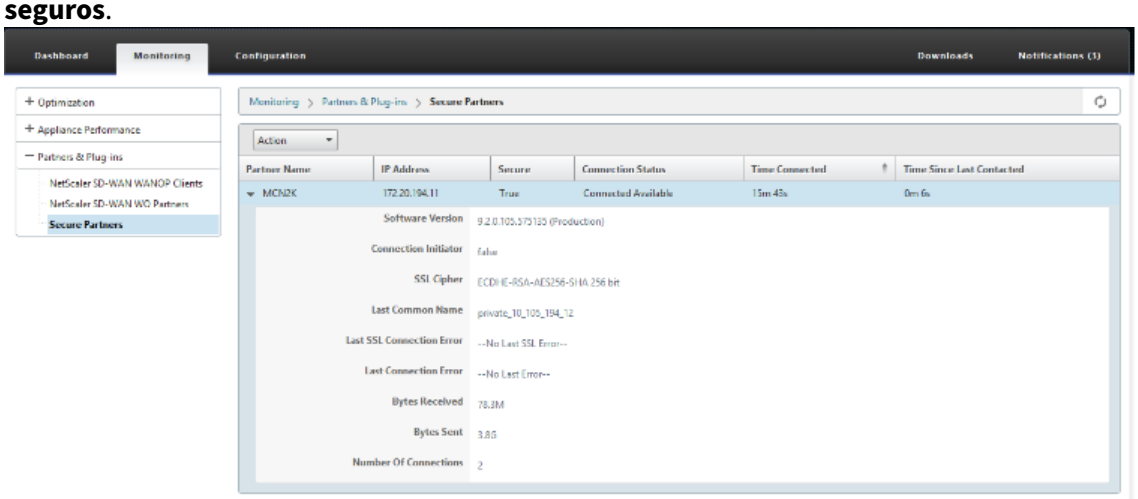


4. Consulte la **información de socios seguros** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Socios**.



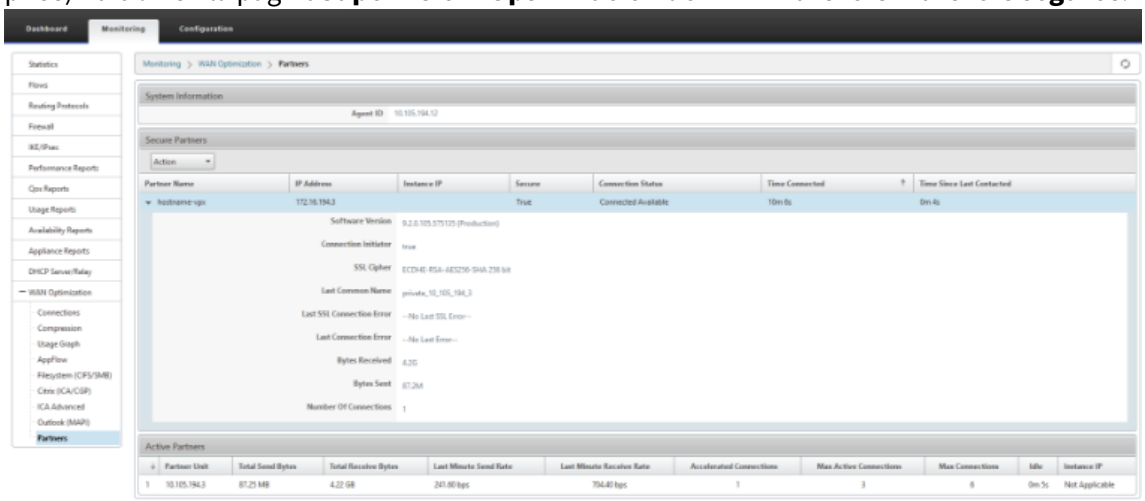
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. En el dispositivo de partners, **consulte la información de socios seguros** del dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Partners & Plugins** > **Partners seguros**.



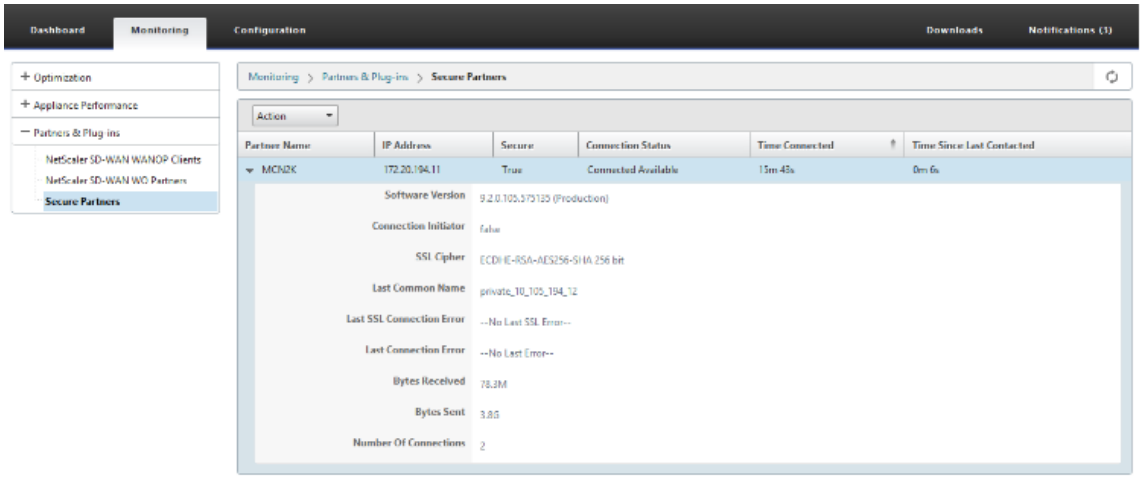
Solucionar problemas

1. Consulte la **información de éxito o errorde socios seguros**en el dispositivo Premium (Enterprise) Edition en la página**Supervisión**>**Optimización de WAN**>**Partners**>**Partners seguros**.

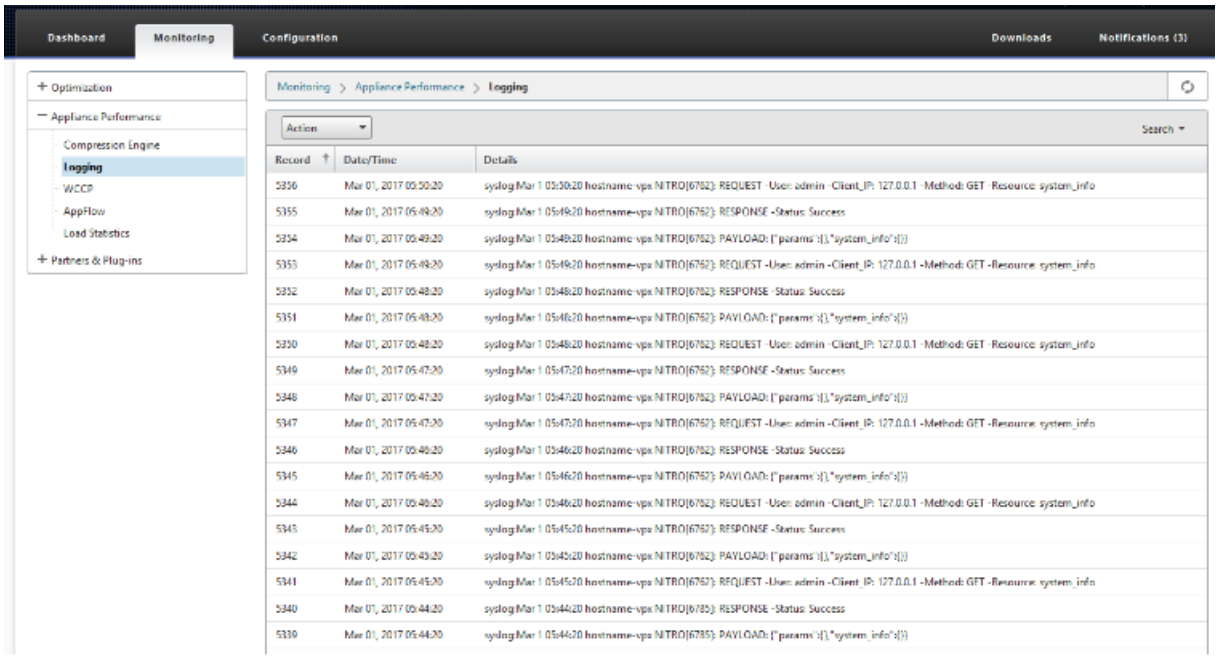


2. En el dispositivo de partners, consulte Información de socios seguros en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Partners & Plugins** > **Partners seguros**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. En el dispositivo asociado, consulte Información de socio seguro en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Rendimiento del dispositivo** > **Registro**.



Emparejamiento automático seguro iniciado desde dispositivos PE en dispositivos PE del sitio de DC y del sitio de una sucursal

May 7, 2021

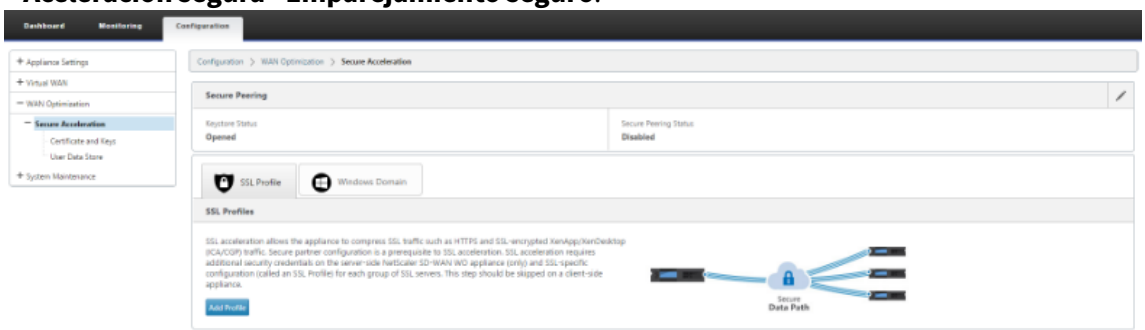
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración

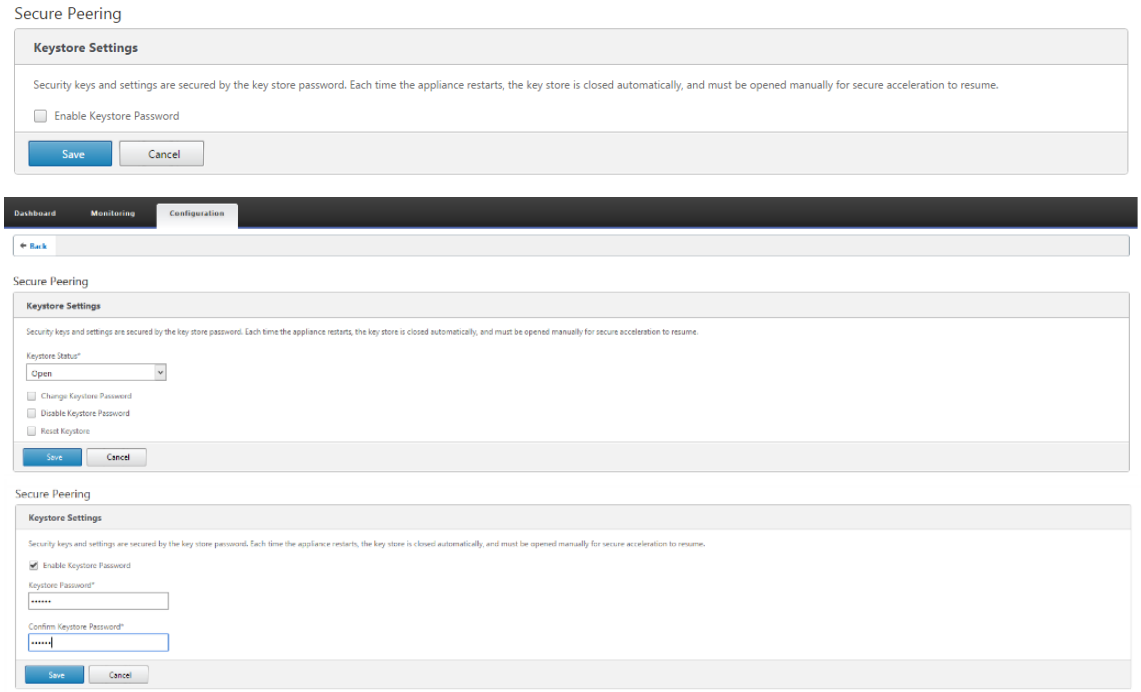
Para configurar el emparejamiento seguro automático en un nuevo dispositivo Premium (Enterprise) Edition en DC:

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443). El dispositivo Branch PE está en modo CONNECT-A.
- El dispositivo de PE DC inicia el emparejamiento seguro automático en un dispositivo de PE Branch que instala los certificados de CA privada y los pares de CERT KEY y configura CONNECT-To en el dispositivo de PE Branch con la IP LISTEN-ON de DC EE.
- La IP LISTEN-ON para el dispositivo PE se encuentra en la IP de interfaz asociada al dominio de enrutamiento para el que está habilitado "Redirigir a WANOP".

1. En la interfaz gráfica de usuario web de SD-WAN, vaya a **Configuración** > **Optimización de WAN** > **Aceleración segura**> **Emparejamiento seguro**.

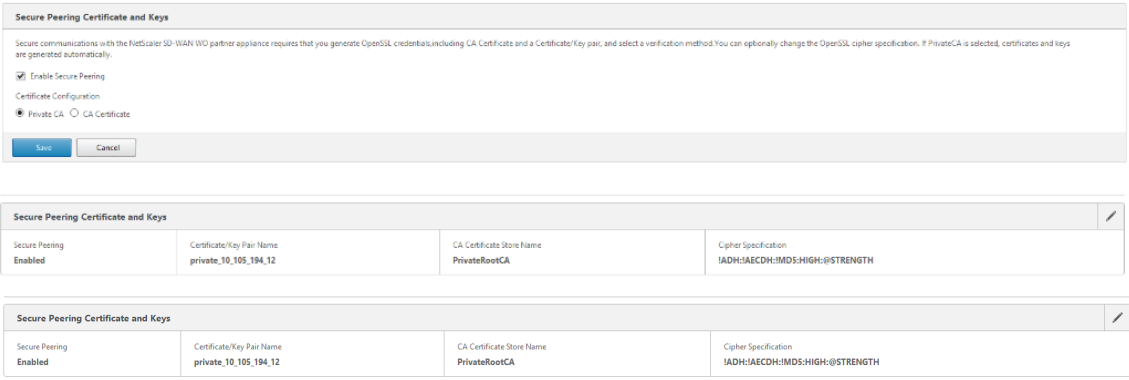


2. Configure el almacén de claves proporcionando la contraseña del almacén de claves o inhabilitando el almacén de claves.



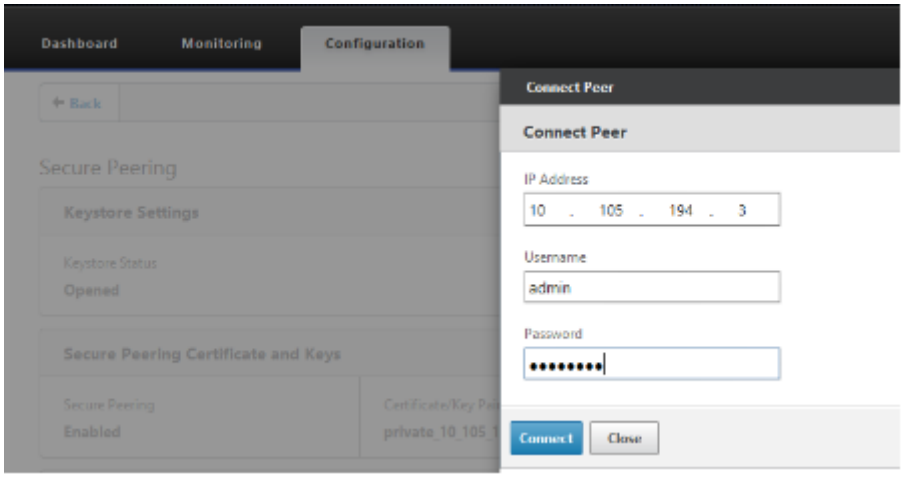
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Habilite el **Emparejamiento seguro** seleccionando **CA privada** para realizar el EMPAREJAMIENTO SEGURO AUTOMÁTICO.



4. Haga clic en el icono '+'y para agregar IP con nombre de usuario y contraseña. Después de la autenticación correcta con la IP remota y las credenciales proporcionadas, se envía una solicitud al equipo remoto que instalará el certificado de CA y el certificado privado y la clave para sí mismo localmente en el equipo remoto.

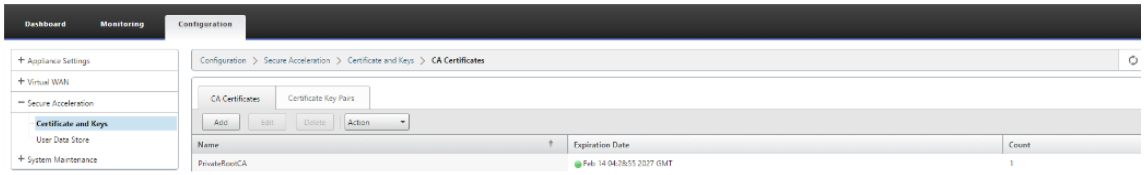
> **Nota**
>
> Dirección IP: Dirección IP de la dirección IP remota de EE Appliance MANAGEMENT
>
> Nombre de usuario: Nombre de usuario del dispositivo
> EE remoto
> Contraseña: Contraseña del dispositivo EE remoto

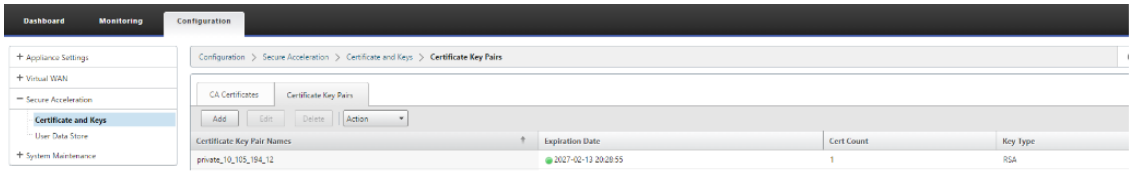


Supervisión

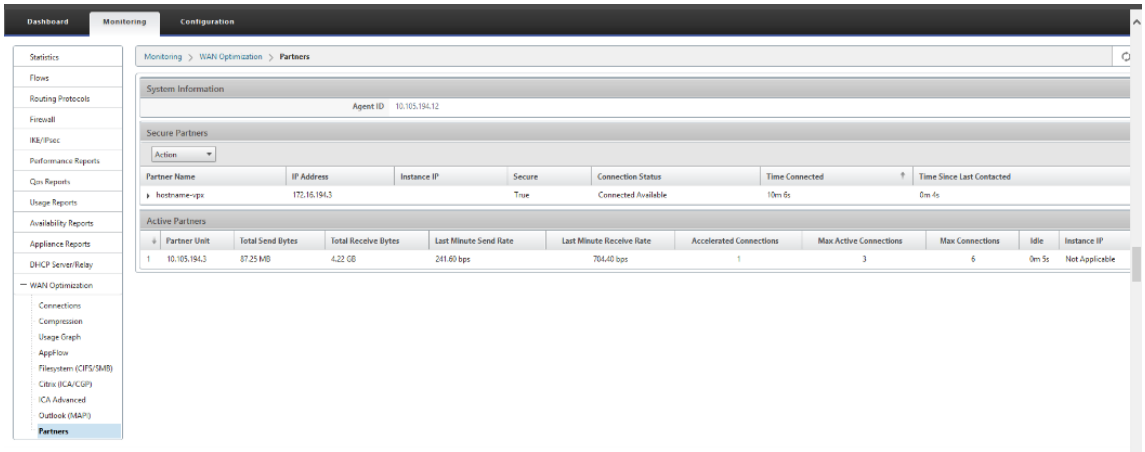
1. Para validar si el par de CA privada y clave de certificado privado se genera correctamente, revise la información que se muestra a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

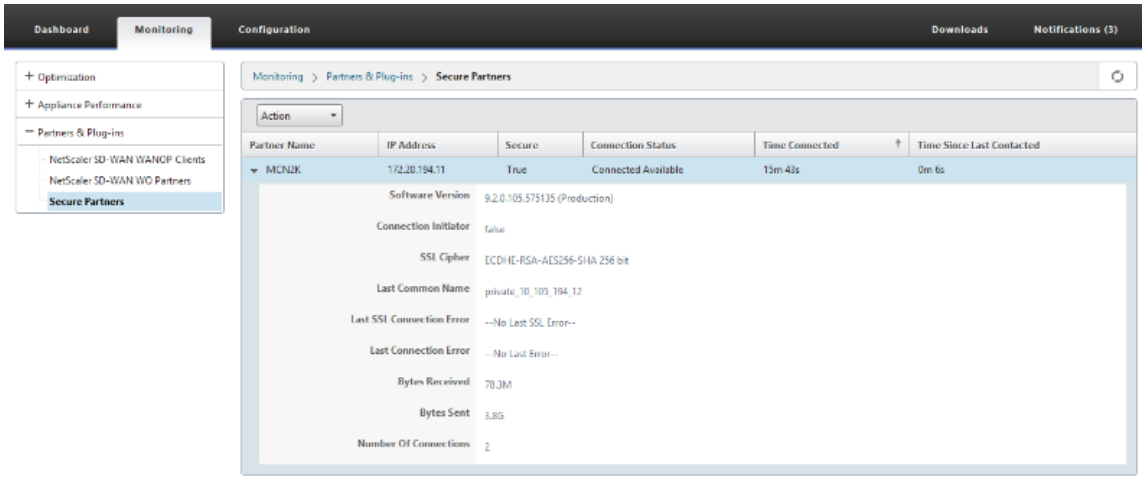




2. Consulte la **información de socios seguros** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Socios**.



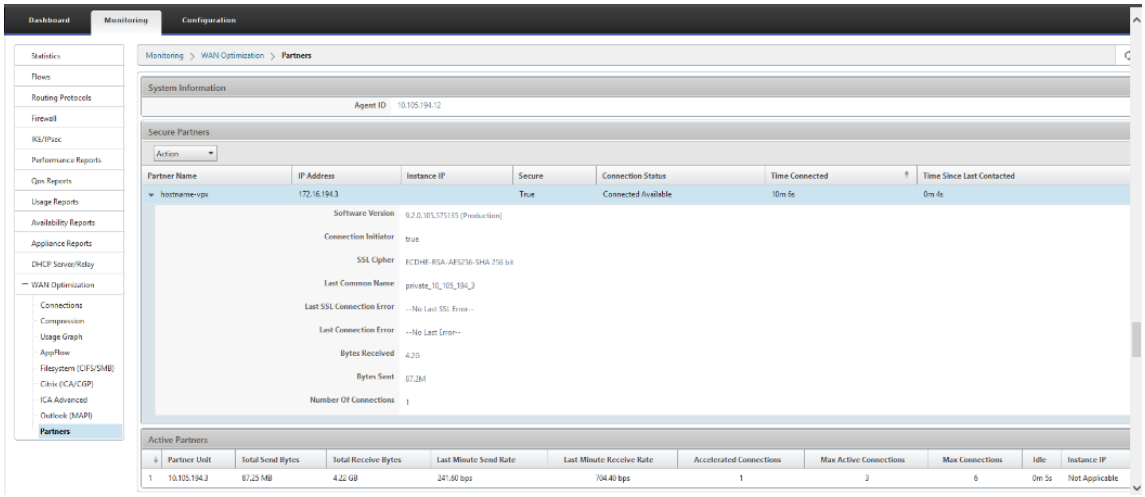
3. En el dispositivo asociado de negocios, consulte Información de socio seguro en el dispositivo Premium (Enterprise) Edition en la página **Supervisión**> **Socios y complementos** > **Socios seguros**.



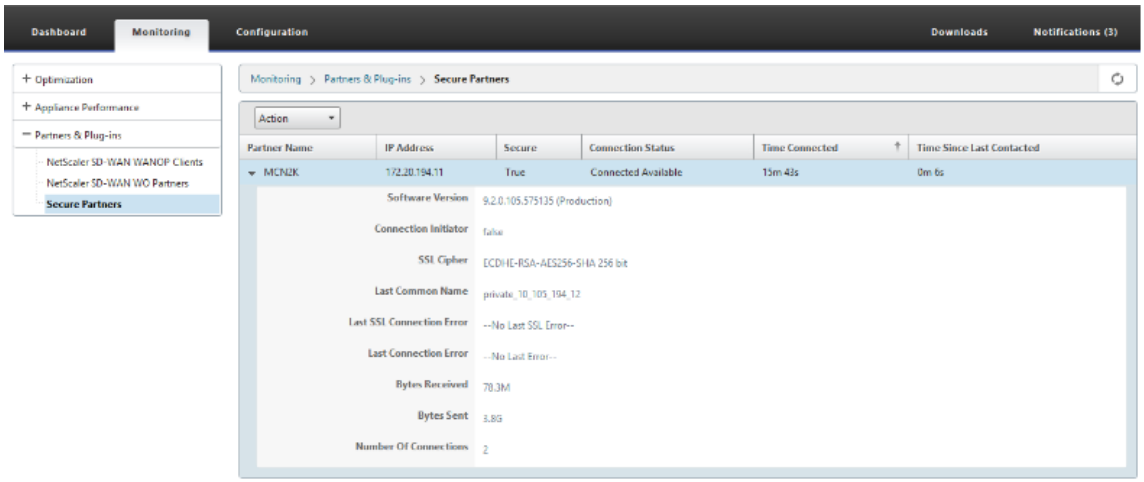
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solucionar problemas

1. Consulte la información de éxito o error de socios seguros en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Partners** > **Partners seguros**.

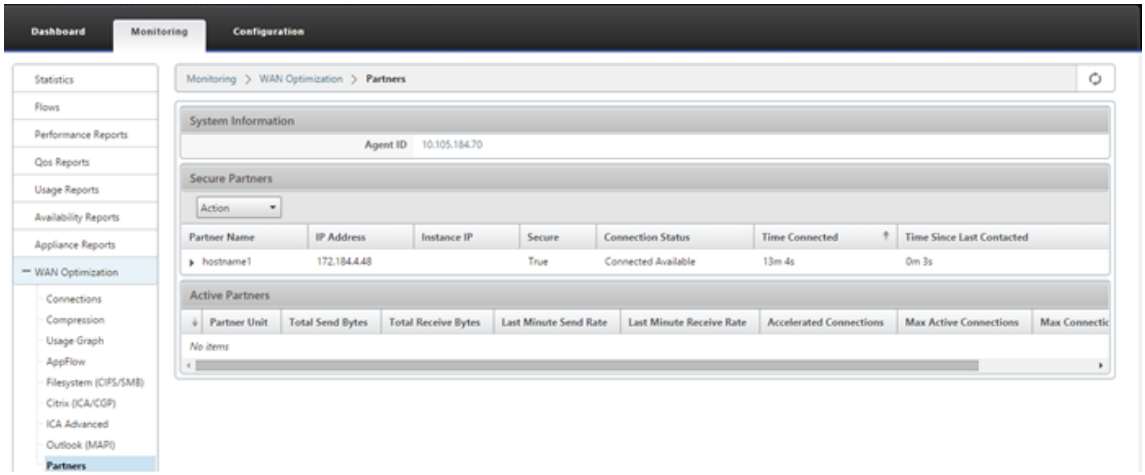


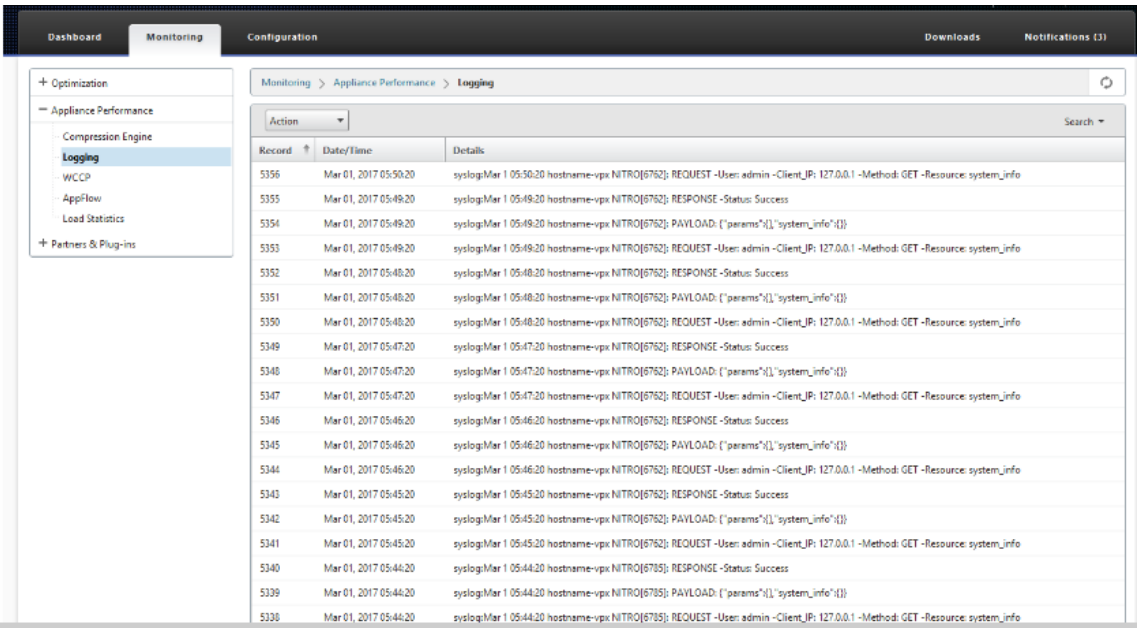
2. En el dispositivo asociado de negocios, consulte Información de socio seguro en el dispositivo Premium (Enterprise) Edition en la página **Supervisión**> **Socios y complementos** > **Socios seguros**.



3. En el equipo asociado de negocios, consulte la información de socio seguro en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Rendimiento del equipo** > **Registro**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





Emparejamiento automático seguro iniciado desde dispositivos PE en dispositivos SD-WAN SE y WANOP independientes en el sitio de DC y del sitio de una sucursal

May 7, 2021

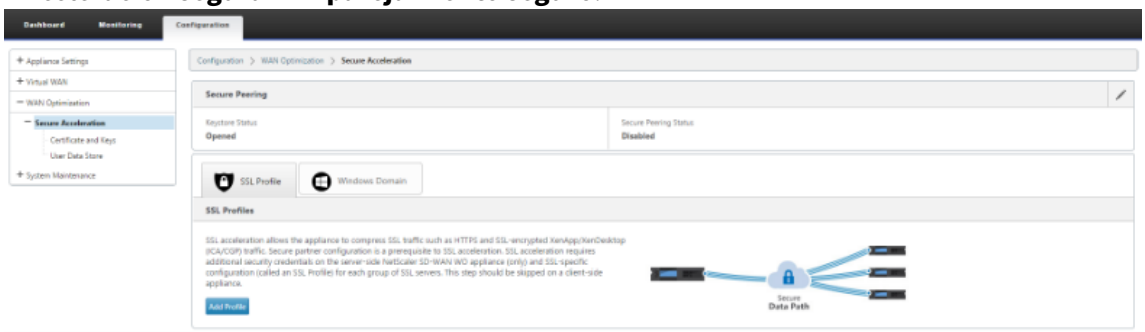
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración

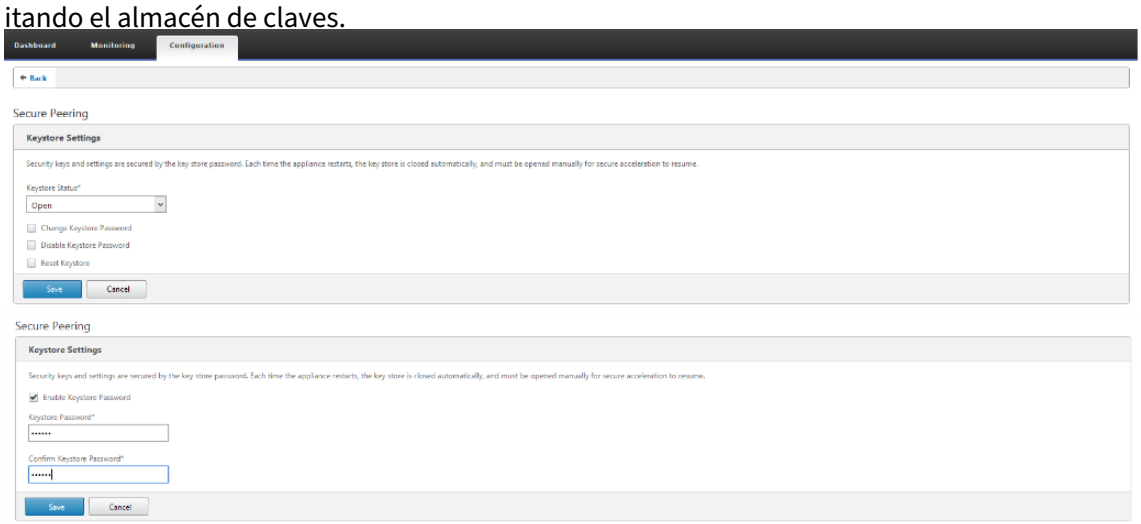
Para configurar un nuevo dispositivo Premium (Enterprise) Edition con peering automático seguro en el sitio de DC y en la sucursal con un dispositivo SD-WAN y WANOP autónomo:

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443).
- El SD-WAN SE y WANOP independiente de la sucursal está en modo CONNECT-To.
- El dispositivo de PE DC inicia el emparejamiento seguro automático en el dispositivo SD-WAN SE y WANOP independiente de Branch, que instala los certificados de CA privada y los pares de claves CERT y configura CONNECT-To en el dispositivo PE con IP LISTEN-ON de DC EE.

1. En la interfaz gráfica de usuario web de SD-WAN, vaya a **Configuración** > **Optimización de WAN** > **Aceleración segura**> **Emparejamiento seguro**.



2. Configure el almacén de claves proporcionando la contraseña del almacén de claves o inhabilitando el almacén de claves.

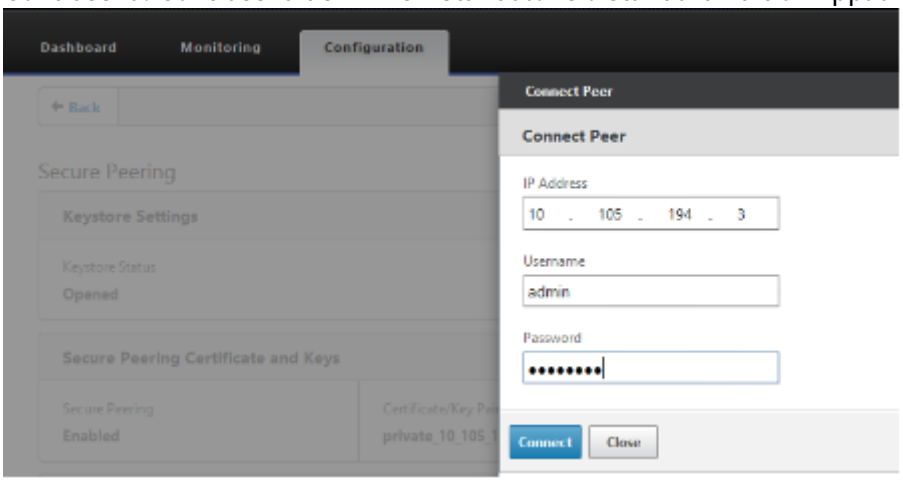


3. Habilite el **Emparejamiento seguro** seleccionando **CA privada** para realizar el EMPAREJAMIENTO SEGURO AUTOMÁTICO.

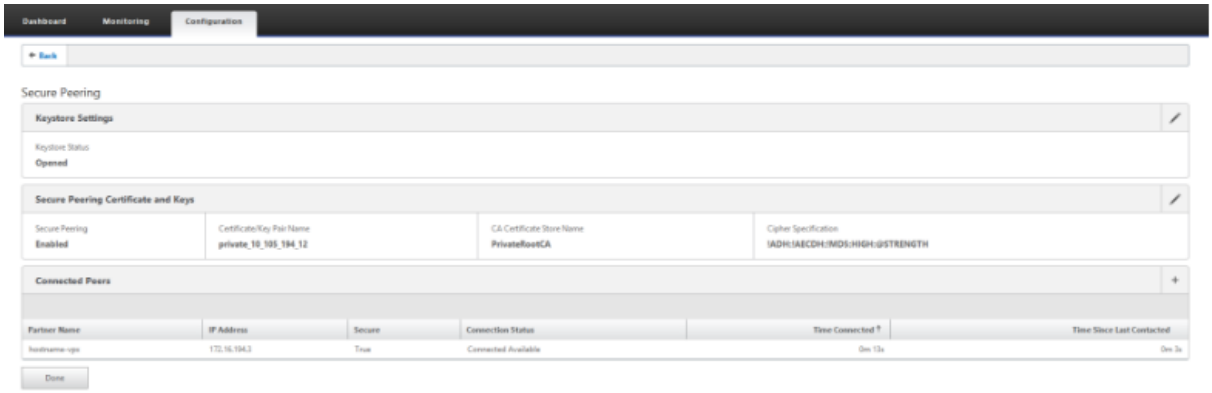
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Haga clic en el icono '+'y agregue IP con nombre de usuario y contraseña. Después de la autenticación correcta con la IP remota y las credenciales proporcionadas, se envía una solicitud al equipo remoto que instalará el certificado de CA y el certificado privado y la clave para sí mismo localmente en el equipo remoto.

   - Dirección IP: Dirección IP de WANOP Standalone o Standard Edition Appliance Management IP remota.
   - Nombre de usuario: Nombre de usuario del dispositivo remoto WANOP Standalone o Standard Edition.
   - Contraseña: Contraseña de WANOP Standalone o Standard Edition Appliance remoto.



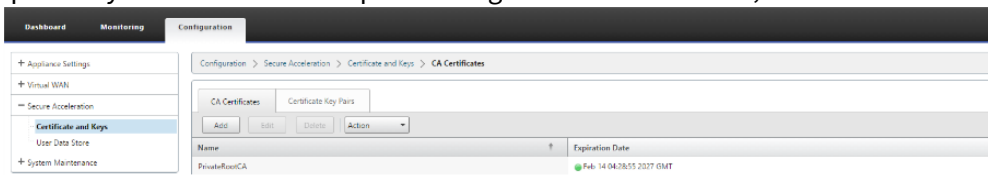
Después de la autenticación correcta, puede ver Emparejamiento seguro como TRUE y la IP asociada como una de la IP virtual del dispositivo autónomo WANOP remoto.

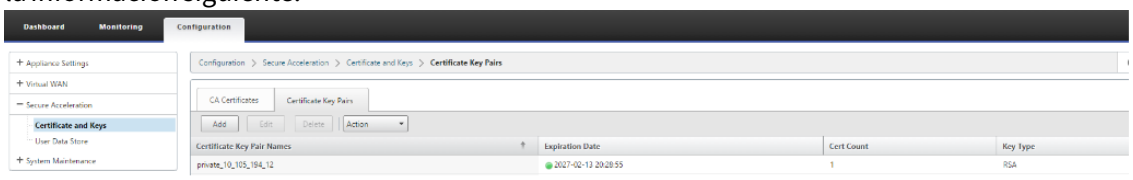


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

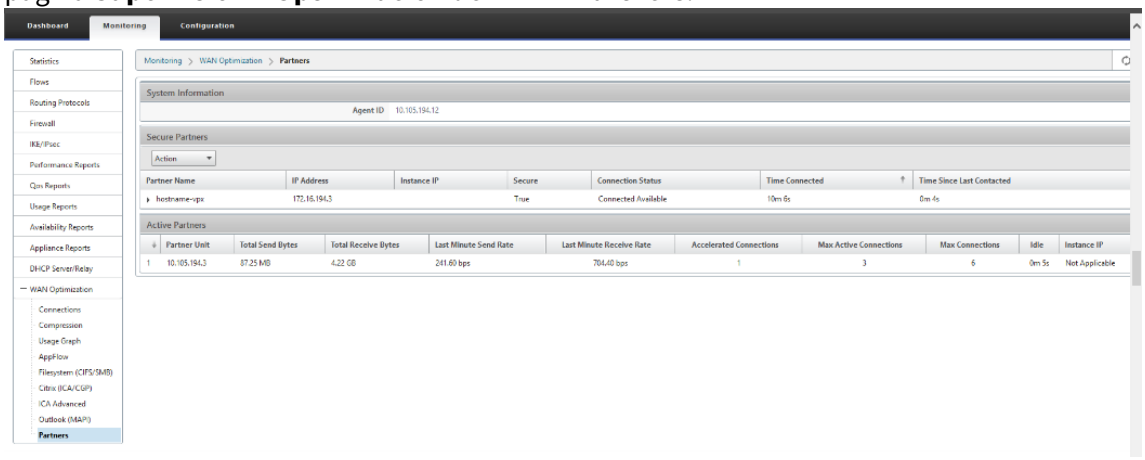
Supervisión

1. Para validar si el par de CA privada y clave de certificado privado se genera correctamente, revise la información siguiente.

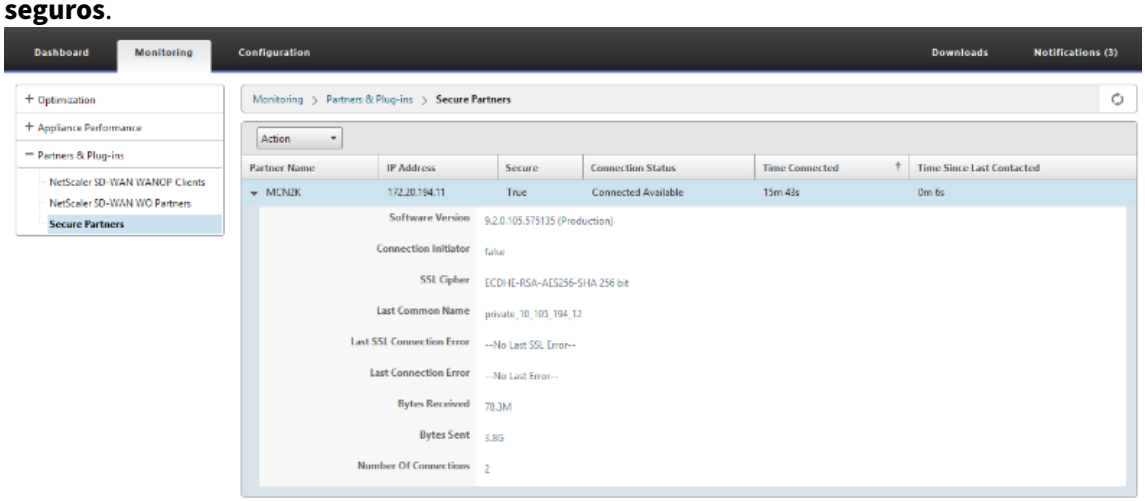




2. Consulte la información de socios seguros en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Partners**.



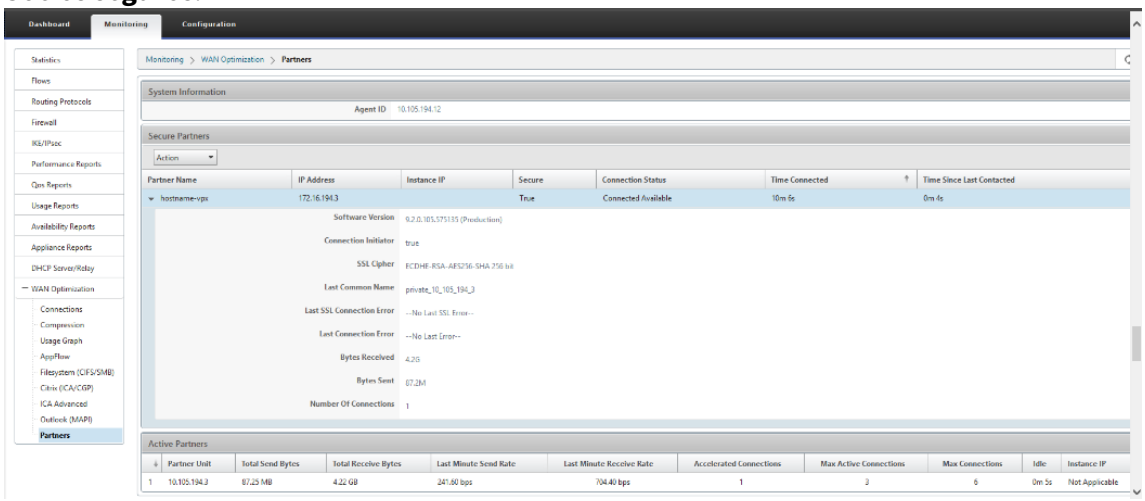
3. En el dispositivo asociado de negocios, consulte la información de socio seguro en el dispositivo Premium (Enterprise) Edition en la página **Supervisión> Socios y complementos**>**Socios seguros**.



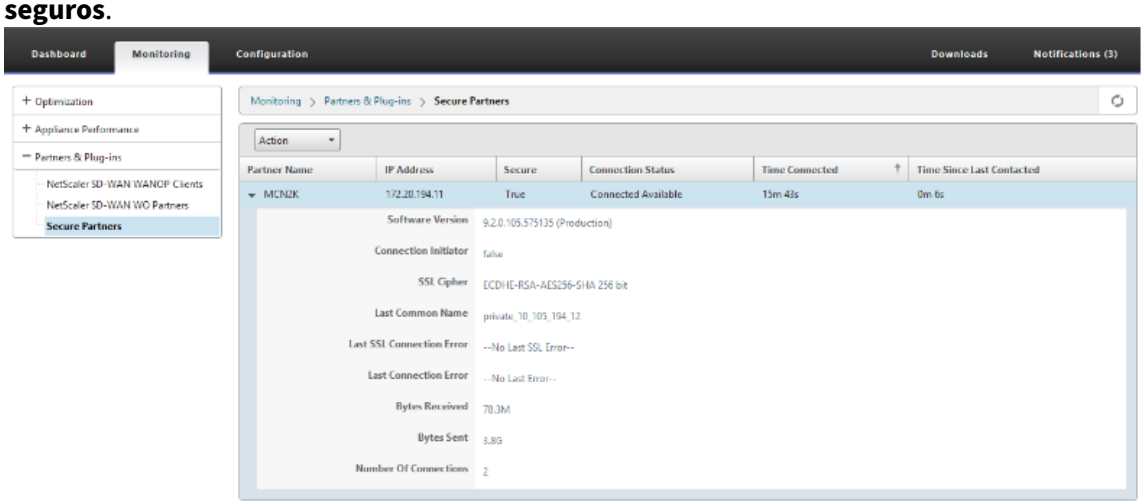
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solucionar problemas

1. Consulte la información de éxito o fallo de los asociados de seguridad en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Socios** > **Socios seguros**.

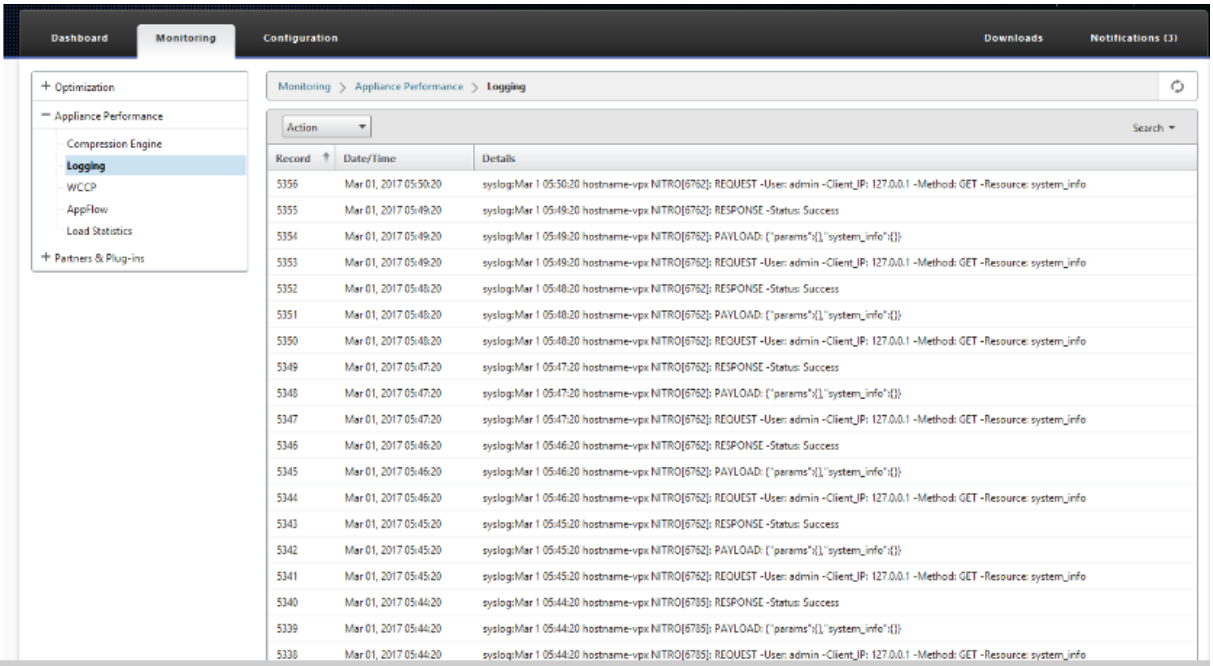


2. En el dispositivo asociado de negocios, consulte **Información de socio seguro** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión> Socios y complementos**>**Socios seguros**.



3. En el dispositivo asociado de negocios, consulte la **información de socio seguro** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Rendimiento del equipo** > **Registro**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



El emparejamiento seguro manual iniciado desde el dispositivo PE en el sitio de DC y en el dispositivo de PE de Branch

May 7, 2021

Esta implementación configura el dispositivo PE del sitio de DC en modo Listen ON y el dispositivo PE del sitio de sucursal en modo CONNECT To.

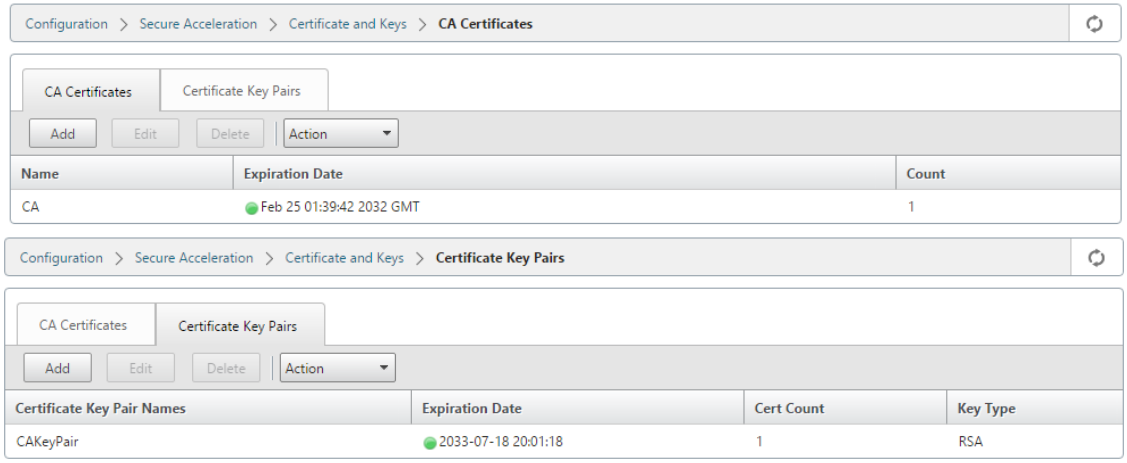
- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443).
- El dispositivo Branch PE está en modo CONNECT-A.
- LISTEN-ON IP para PE está en la IP de interfaz asociada al dominio de redirección para el que está habilitado “Redirigir a WANOP”.
- Cargue manualmente certificados de par de CA y clave de certificado obtenidos del origen auténtico de la entidad emisora de certificados.

Configuración

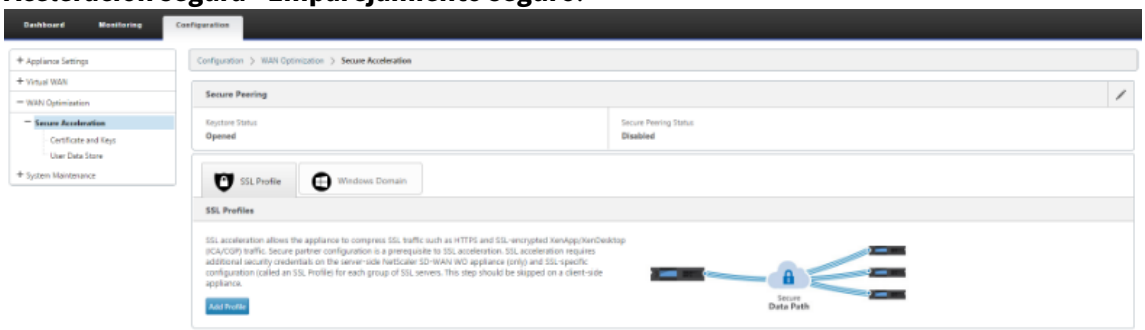
Para configurar la interconexión segura automática iniciada desde un dispositivo PE en el sitio de DC y un dispositivo PE en el sitio de sucursal:

1. Cargar **certificado de CA y certificadode clave** de CA obtenidos del certificado auténtico y proporcionar a SD-WAN como se muestra a continuación.

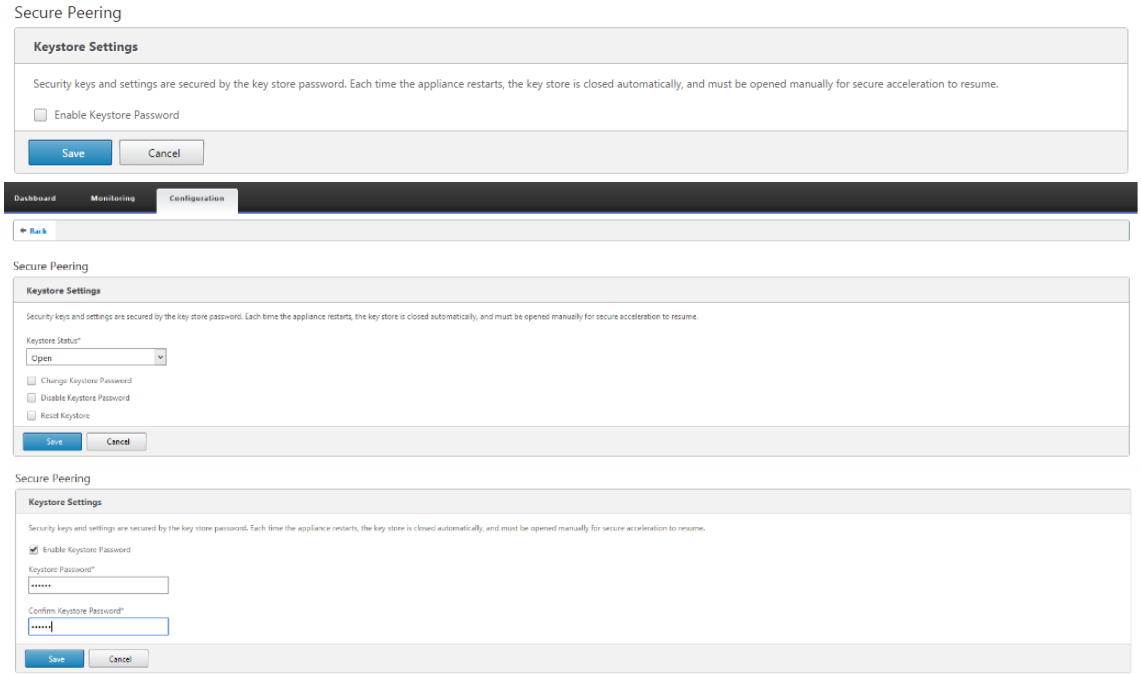
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. En un nuevo dispositivo PE en el sitio de DC, en la GUI web de SD-WAN, vaya a **Configuración** > **Aceleración segura> Emparejamiento seguro**.

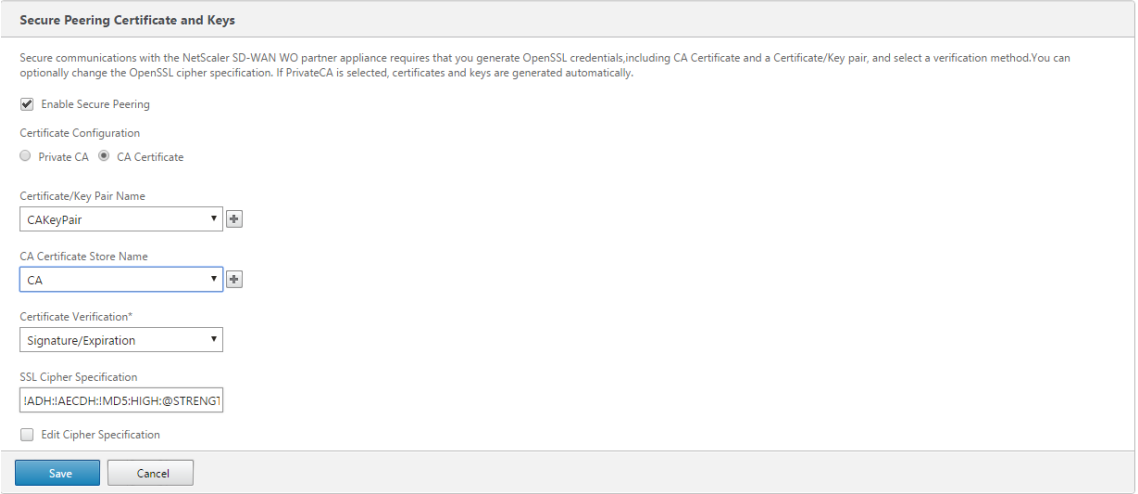


3. Configure el almacén de claves proporcionando la contraseña del almacén de claves o inhabilitando el almacén de claves.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

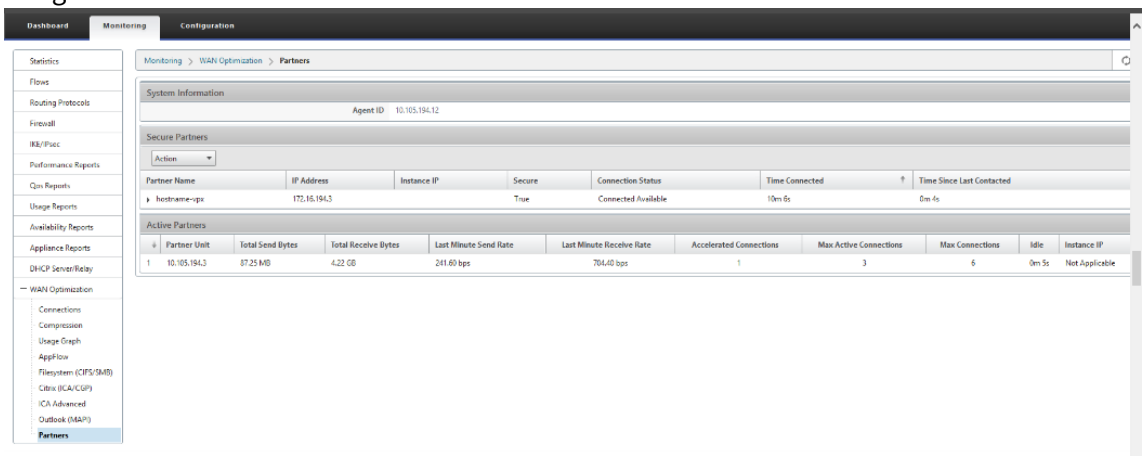
4. Habilite el emparejamiento seguro seleccionando el botón de opción **Certificado de CA** y proporcionando certificados de pares de CA y CA cargados correctamente como se muestra a continuación.



5. Proporcione la IP virtual de la máquina remota junto con el puerto 443 como se muestra a continuación.

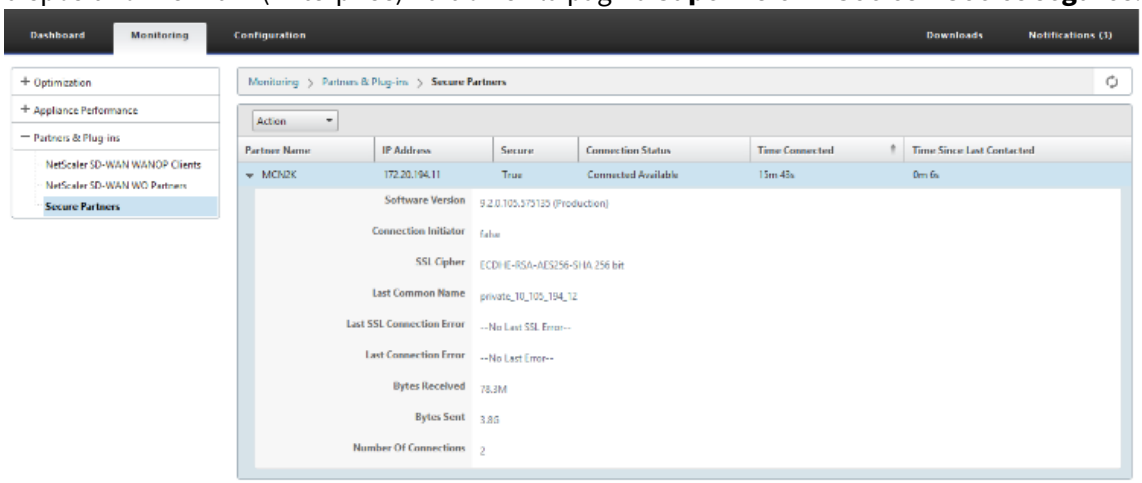
Supervisión

1. Para validar si el par **CA privada y Clavede certificado privada** se genera correctamente, revise la siguiente información.



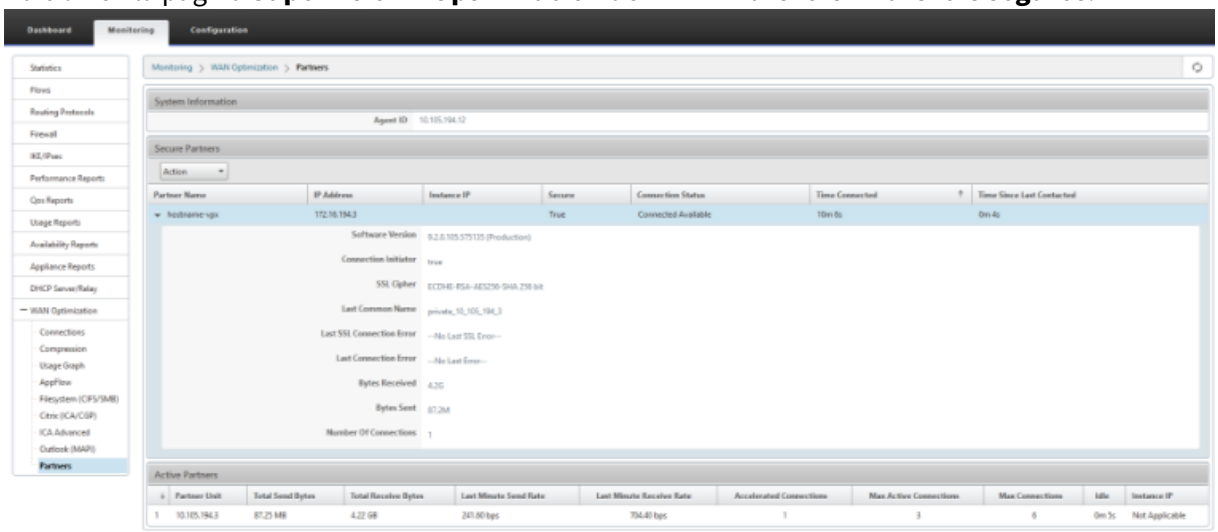
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. En el dispositivo asociado de negocios, **consulte la información de socio seguro** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Socios** > **Socios seguros**.



Solucionar problemas

Consulte la información de **éxito o error de socios seguros** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Partners** > **Partners seguros**.



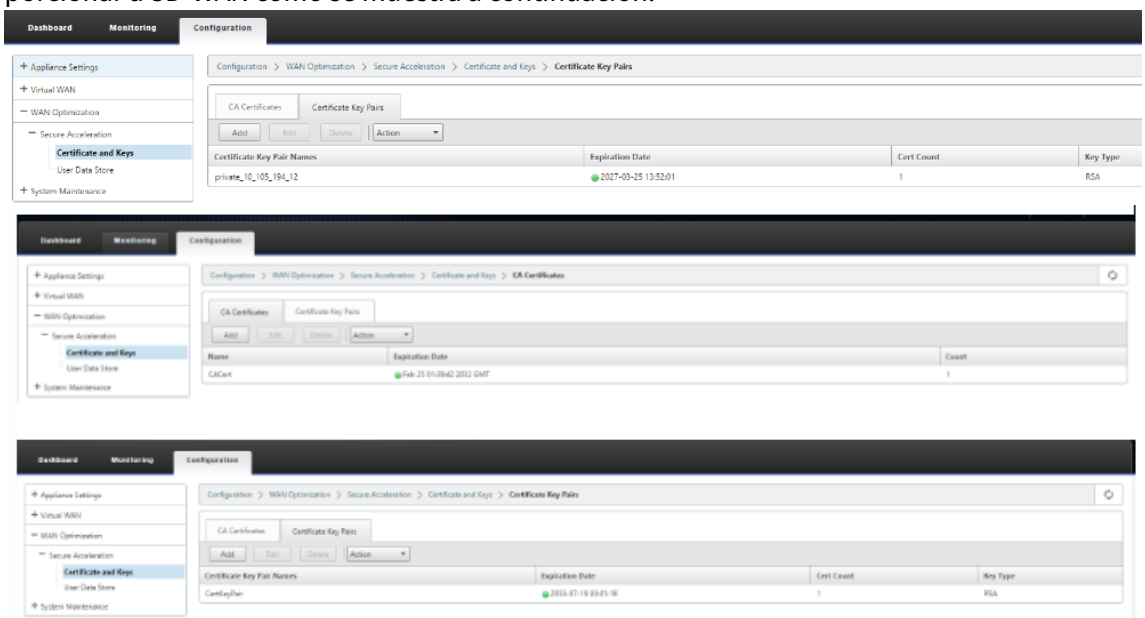
Emparejamiento seguro manual iniciado desde un dispositivo PE en el sitio de DC a un dispositivo SD-WAN SE y WANOP independiente de la sucursal

May 7, 2021

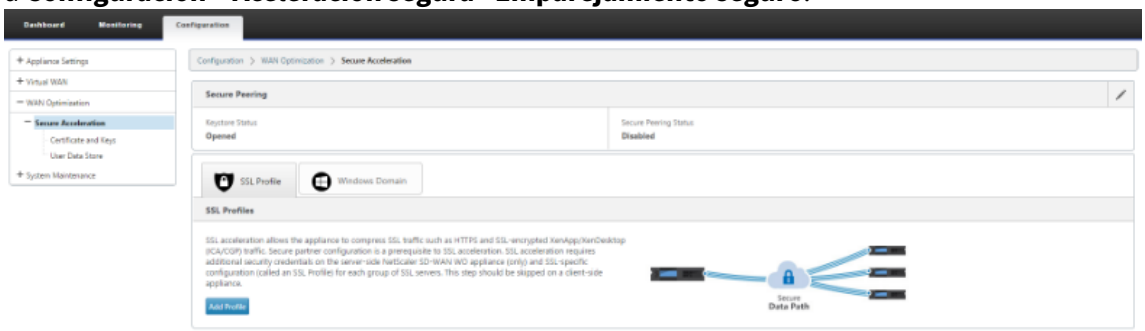
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El dispositivo de PE DC está en modo ESCUCHE ON (en el puerto 443).
- El dispositivo Branch PE está en modo CONNECT-A.
- LISTEN-ON IP para PE está en la IP de interfaz asociada al dominio de redirección para el que está habilitado “Redirigir a WANOP”.
- Cargue manualmente certificados de par de CA y clave de certificado obtenidos del origen auténtico de la entidad emisora de certificados.

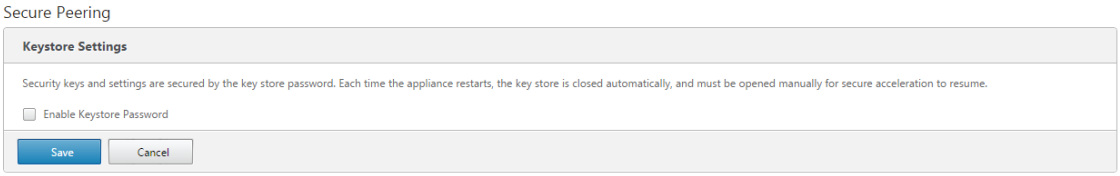
1. Cargar **certificado de CA y certificadode clave** de CA obtenidos del certificado auténtico y proporcionar a SD-WAN como se muestra a continuación.



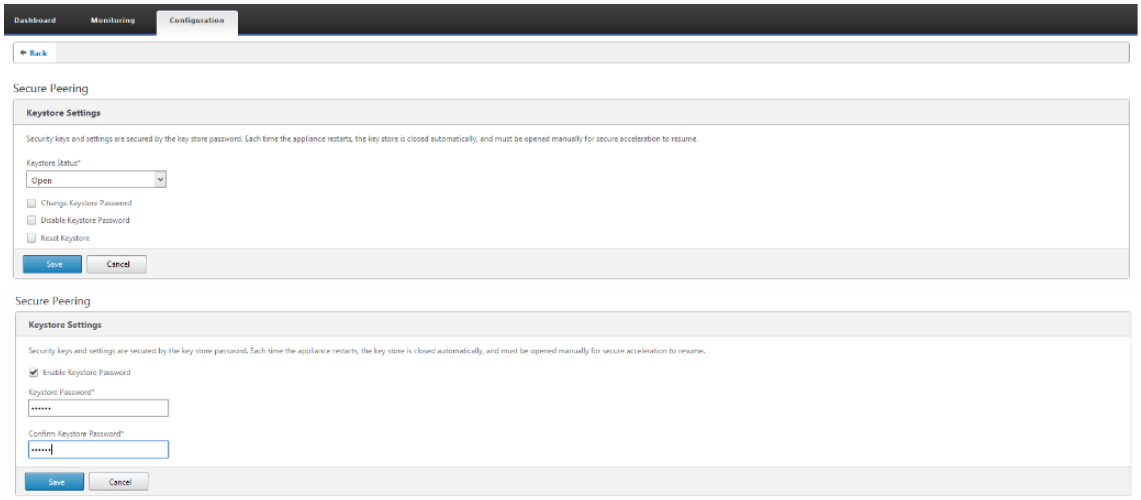
2. En un nuevo dispositivo PE (Premium Edition) en el sitio de DC, en la GUI web de SD-WAN, vaya a **Configuración** > **Aceleración segura**> **Emparejamiento seguro**.



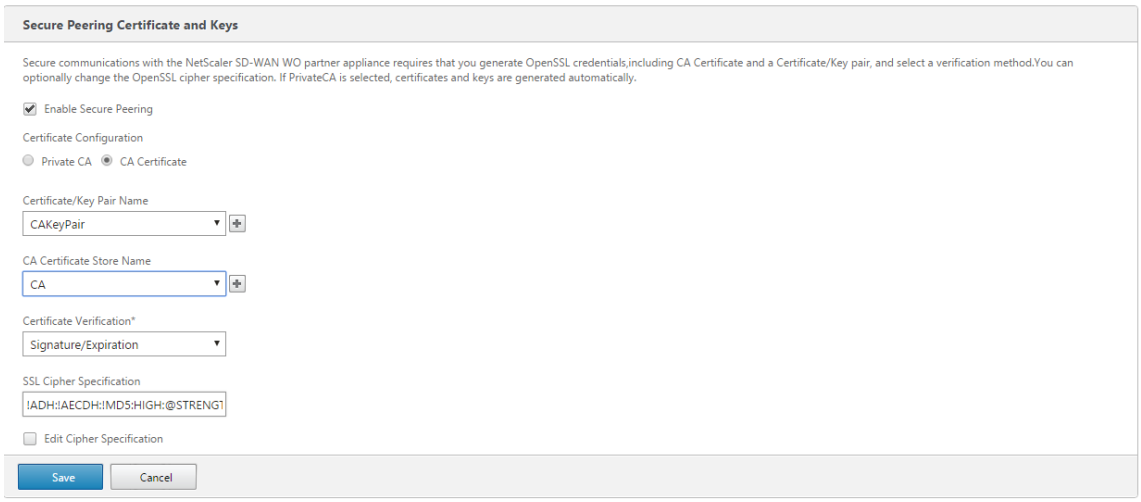
3. Habilite el almacén de claves proporcionando la **contraseña del almacén de claves** o inhabilite el almacén de claves.



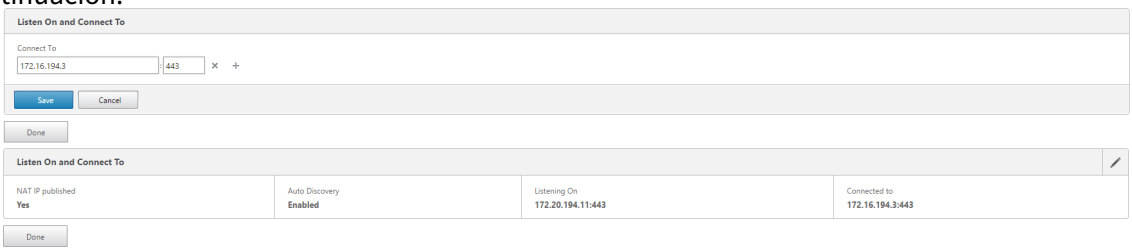
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Habilite el emparejamiento seguro seleccionando el botón de opción **Certificado de CA** y proporcionando certificados de pares de CA y CA cargados correctamente como se muestra a continuación.



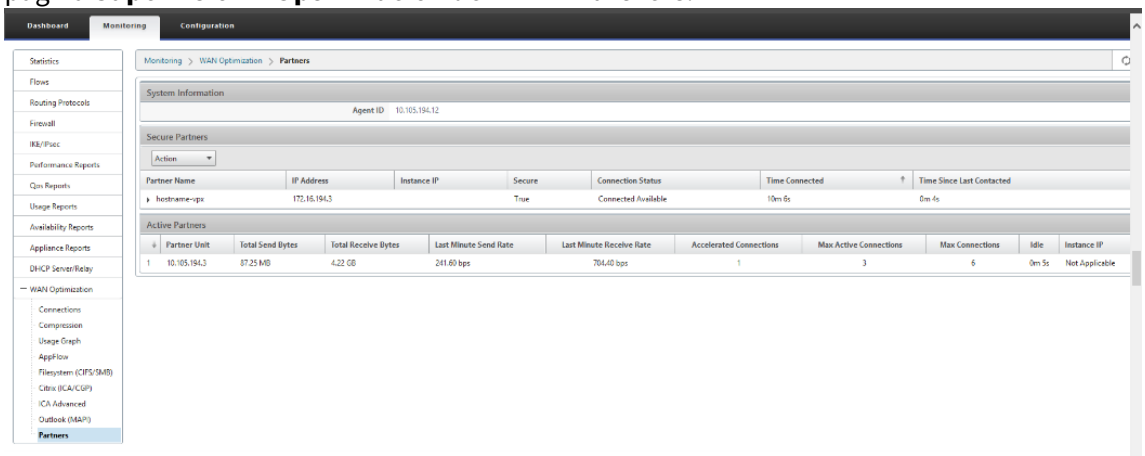
5. Proporcione la IP virtual de la máquina remota junto con el puerto 443 como se muestra a continuación.



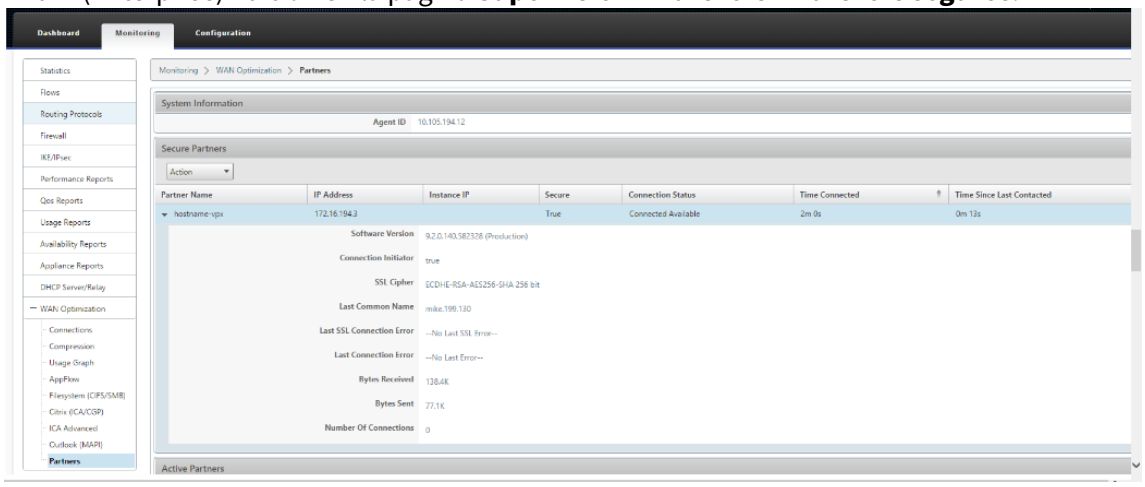
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Supervisión

1. Consulte la información de socios seguros en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Optimización de WAN** > **Partners**.



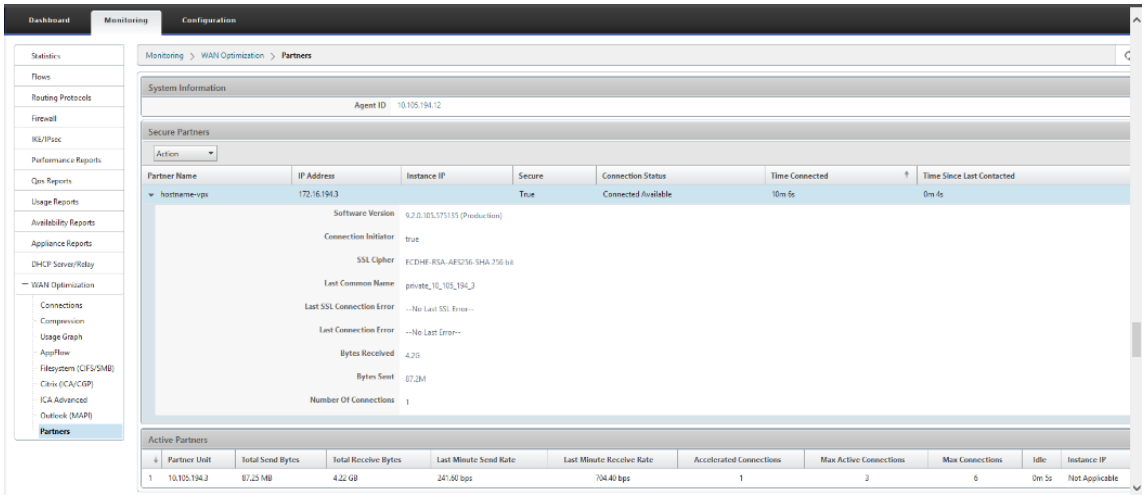
2. En el dispositivo de partners, consulte la información del socio seguro en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Partners** > **Partners seguros**.



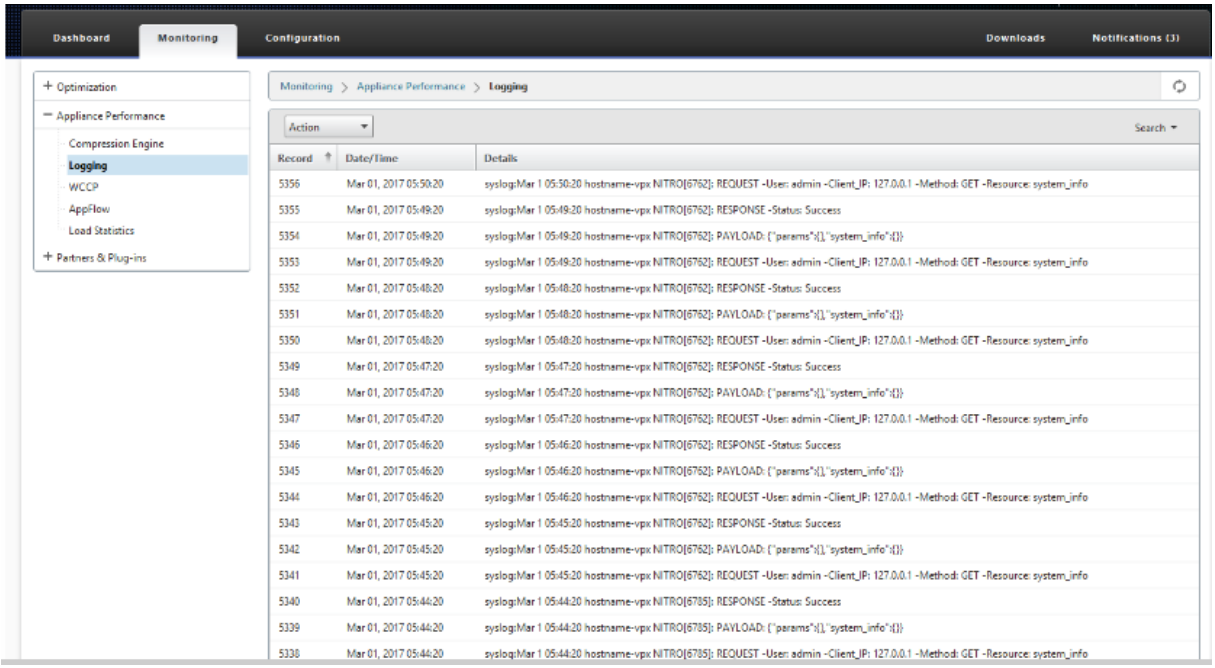
Solucionar problemas

1. Consulte la **información de éxito o fallode los socios seguros**en el dispositivo Premium (Enterprise) Edition en la página**Supervisión**>**Optimización de WAN**>**Socios**>**Socios seguros**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. En el dispositivo asociado de negocios, consulte la **información de socio seguro** en el dispositivo Premium (Enterprise) Edition en la página **Supervisión** > **Rendimiento del equipo** > **Registro**.



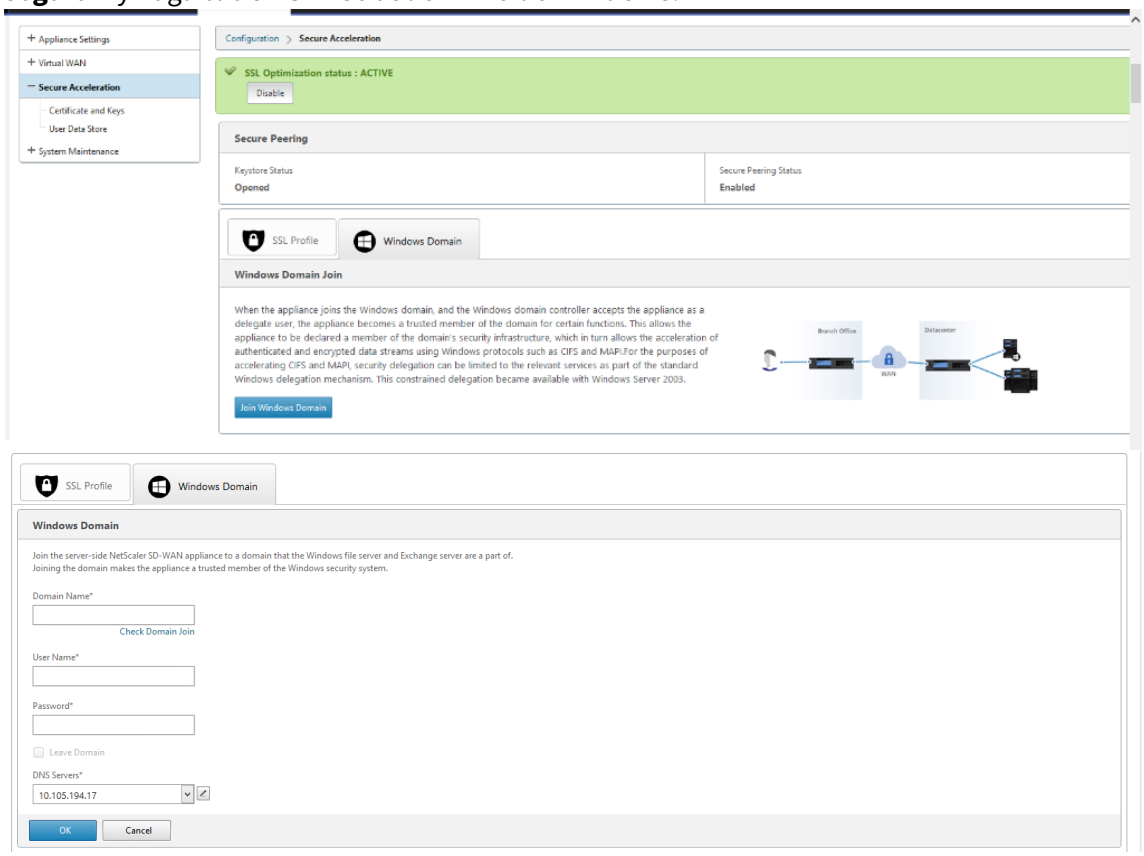
Creación de usuarios delegados y unirse a un dominio

May 7, 2021

Para configurar el nuevo dispositivo Premium (Enterprise) Edition (PE) en el dominio DC a Windows:

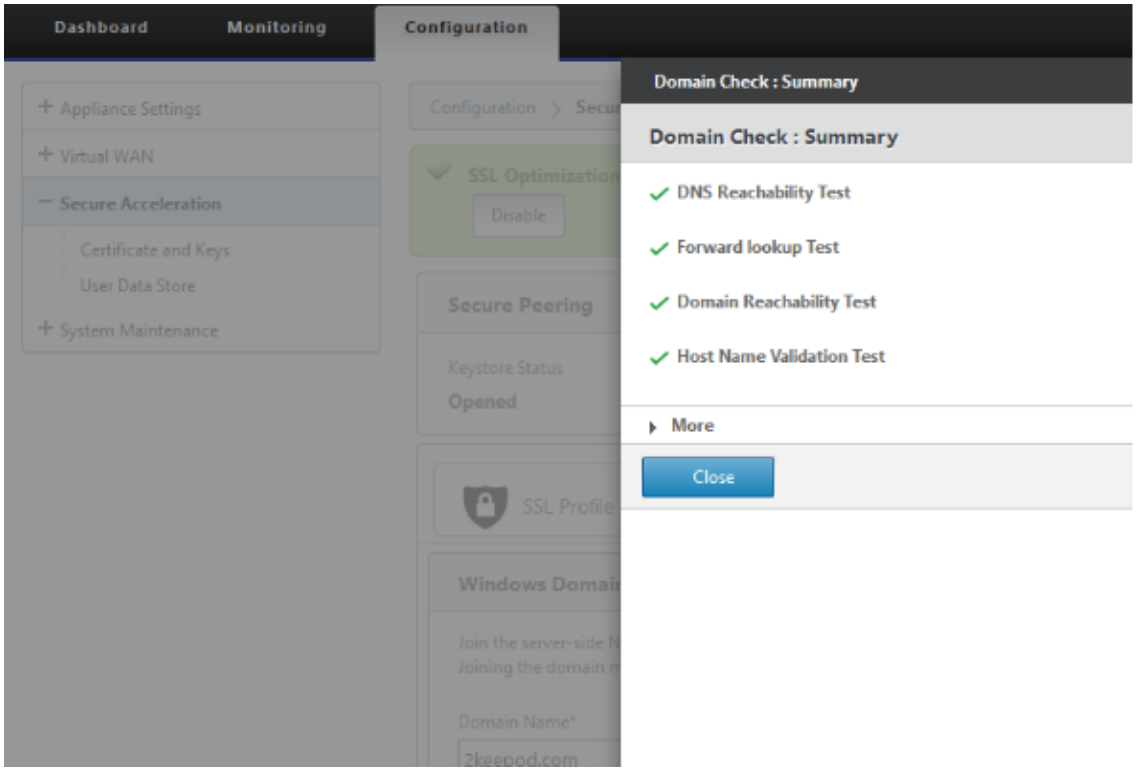
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Vaya a Dominio de Windows en la GUI web de SD-WAN, vaya a **Configuración** > **Aceleración segura** > y haga clic en **Unirse al dominio de Windows**.

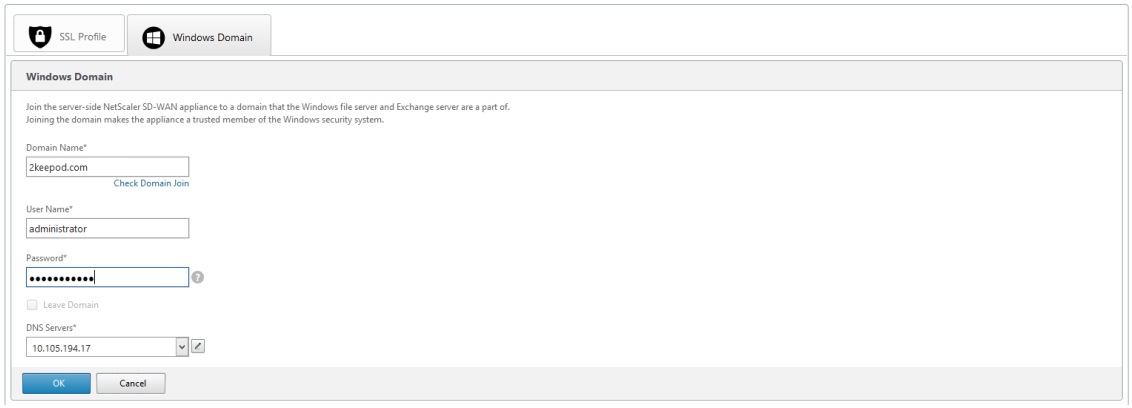


2. Proporcione **el nombre de dominio de Windows** y realice comprobaciones previas de **Unirse a dominios**.

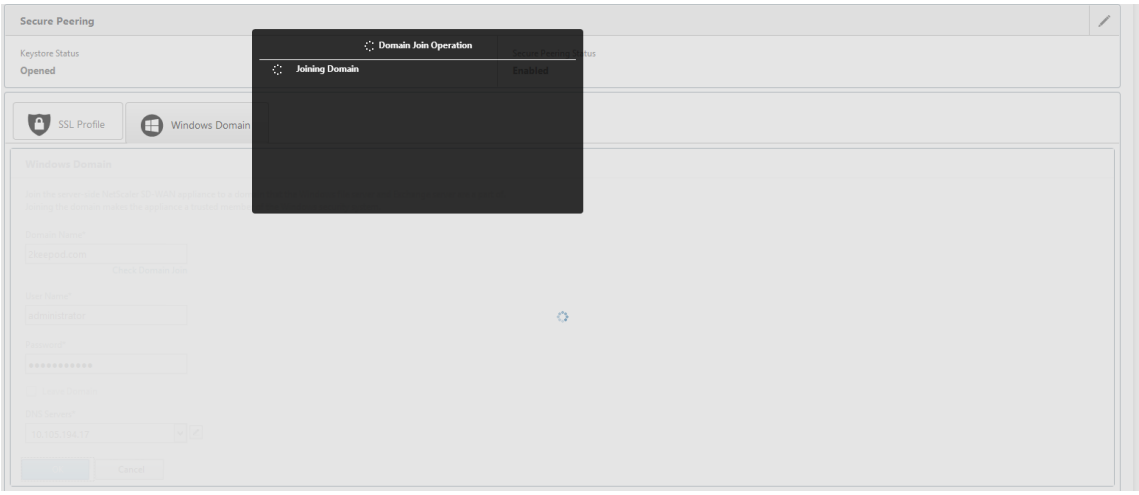
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



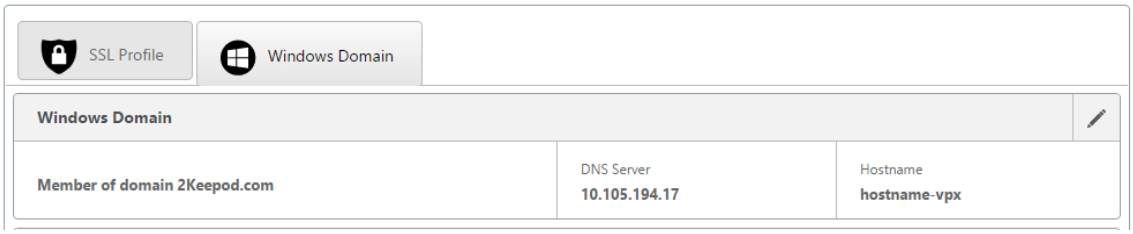
3. Después de que el resumen de comprobación previa se muestre correctamente, introduzca las credenciales del controlador de dominio.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

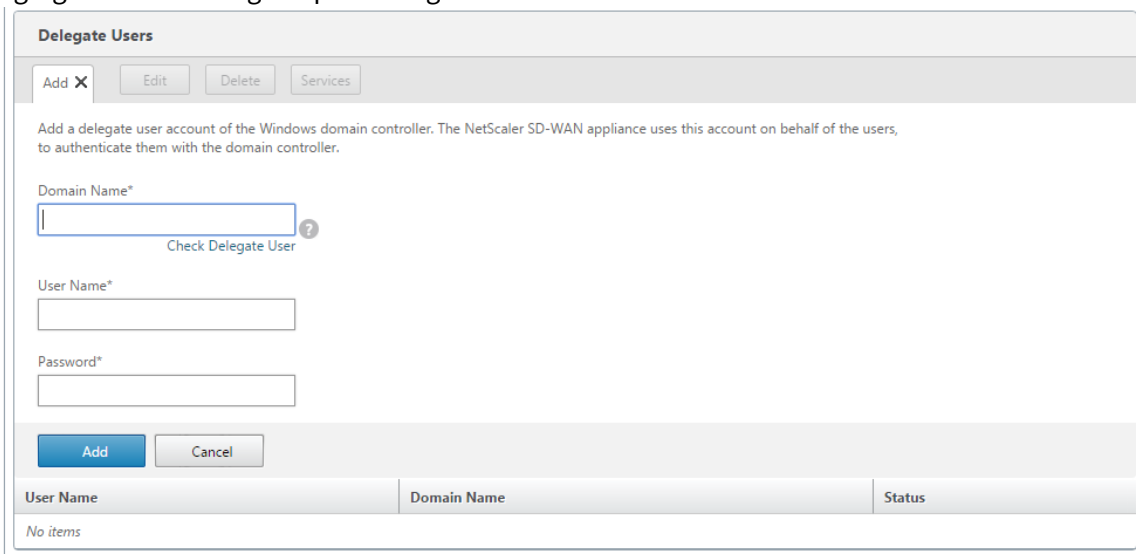


4. En una combinación de dominio exitosa, obtendrá el siguiente resultado.



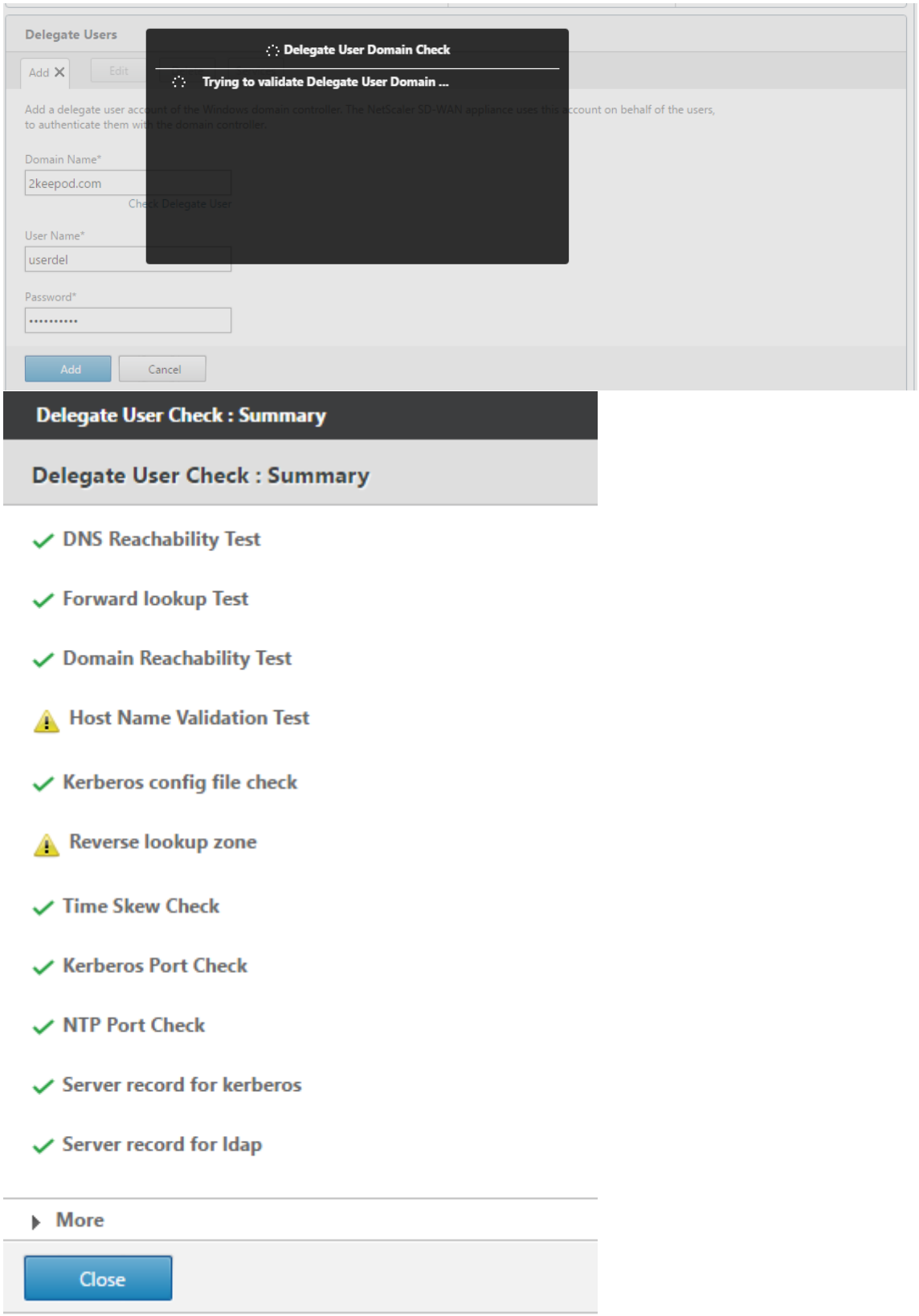
Delegar usuario

1. Agregar usuario delegado para delegar los servicios como se muestra a continuación.



2. Proporcione el nombre de dominio correcto y realice la comprobación previa del usuario delegado.

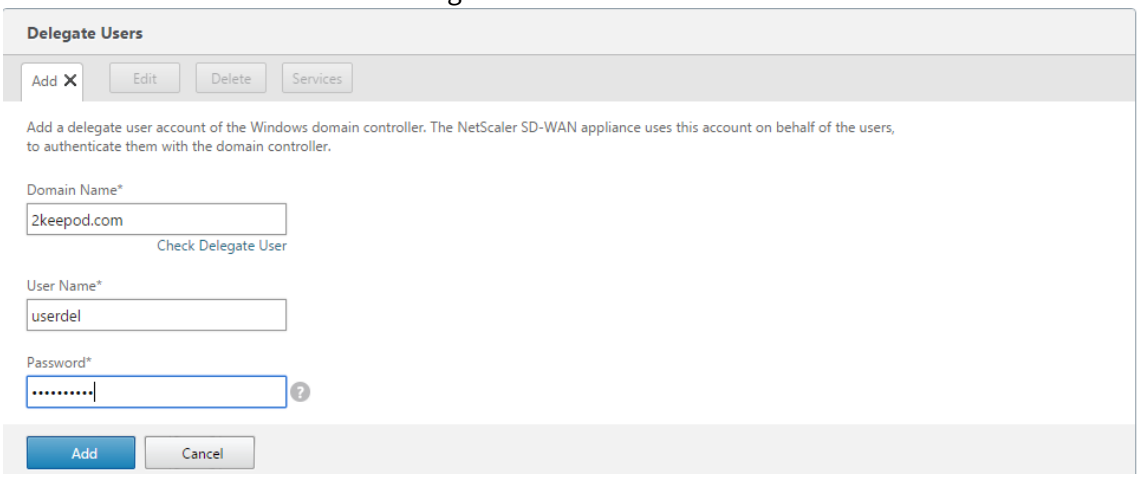
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



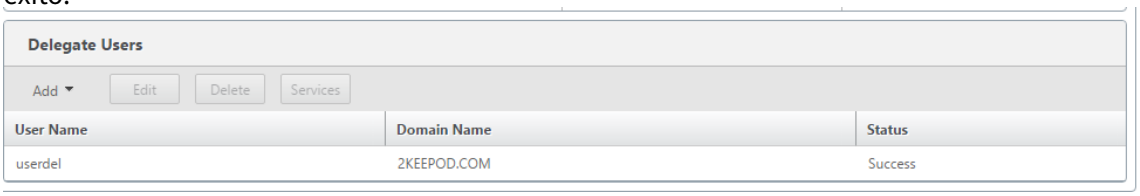
3. Una vez que las comprobaciones previas del usuario delegado sean correctas, proporcione

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

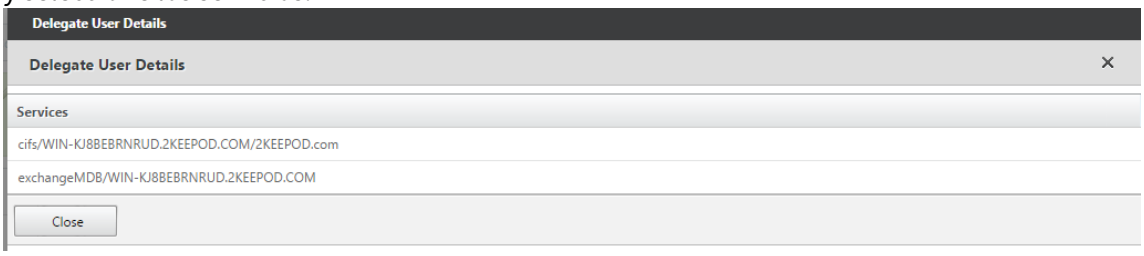
credenciales válidas del usuario delegado.



4. Después de que el usuario delegado se agrega correctamente a SD-WAN, notará un mensaje de éxito.



5. Para comprobar qué es lo que el usuario delegado delega todos los servicios, señale al usuario y seleccione los servicios.



Seguridad

May 7, 2021

Los temas de esta sección proporcionan instrucciones generales de seguridad para las implementaciones de Citrix SD-WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directrices de implementación de Citrix SD-WAN

Para mantener la seguridad durante el ciclo de vida de la implementación, Citrix recomienda la siguiente consideración de seguridad:

- Seguridad física
- Seguridad del dispositivo
- Seguridad de red
- Administración y Gestión

Los temas descritos en los vínculos siguientes proporcionan más información acerca de cómo configurar la seguridad para redes SD-WAN mediante:

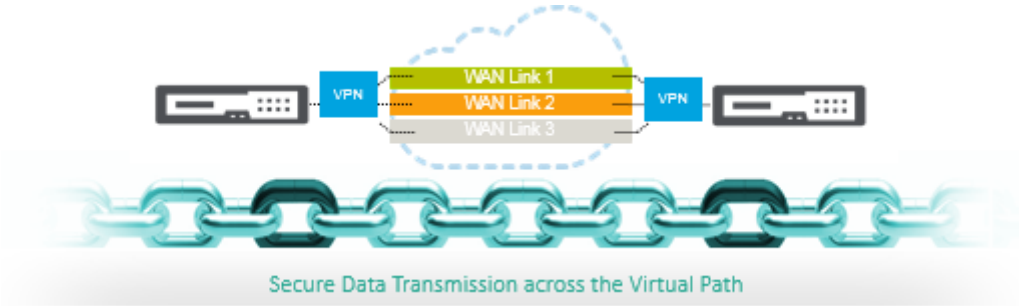
- Túneles IPSec
- Firewall

Terminación del túnel IPSec

May 7, 2021

Citrix SD-WAN admite rutas virtuales IPSec, lo que permite que los dispositivos de terceros terminen los 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 certificado FIPS 140-2 de nivel 1.

Citrix SD-WAN también admite tunelización IPSec resistente mediante un mecanismo de túnel de ruta virtual diferenciado.



Integración de Citrix SD-WAN con AWS Transit Gateway

January 10, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. La puerta de enlace de tránsito actúa como un concentrador que controla cómo se enruta 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 la puerta de enlace de tránsito y no a todas las demás redes. Cualquier VPC nueva está conectada a la puerta de enlace de tránsito y está disponible automáticamente para todas las demás redes conectadas a la puerta de enlace de tránsito. 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 la puerta de enlace de tránsito (ya sea una VPN existente o una nueva).
3. Adjunte VPN a la puerta de enlace de tránsito 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.

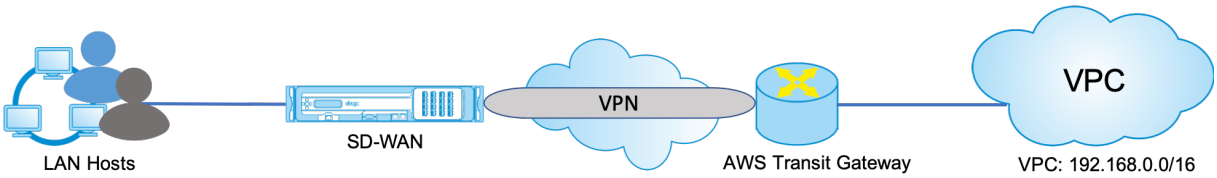
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 la puerta de enlace de tránsito sin administrar manualmente el enrutamiento dentro de la infraestructura de AWS.



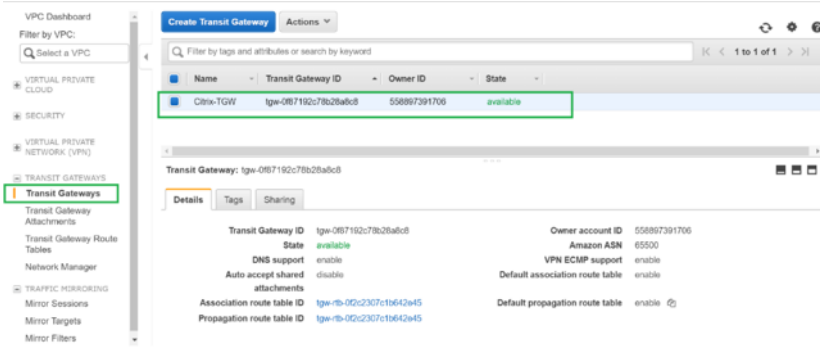
Configuración de AWS Transit Gateway

Para crear **AWS Transit Gateway**, vaya al panel de VPC y vaya a la sección **Transit Gateway** .

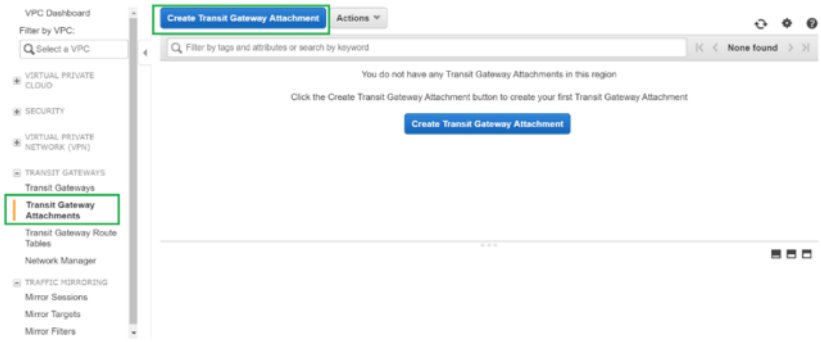
1. Proporcione el nombre de la puerta de enlace de tránsito, la descripción y el número ASN de Amazon como se resaltan en la siguiente captura de pantalla y haga clic en **Crear puerta de enlace de tránsito**.

Una vez completada la creación de la puerta de enlace de tránsito, podrá ver el estado como **Disponible**.

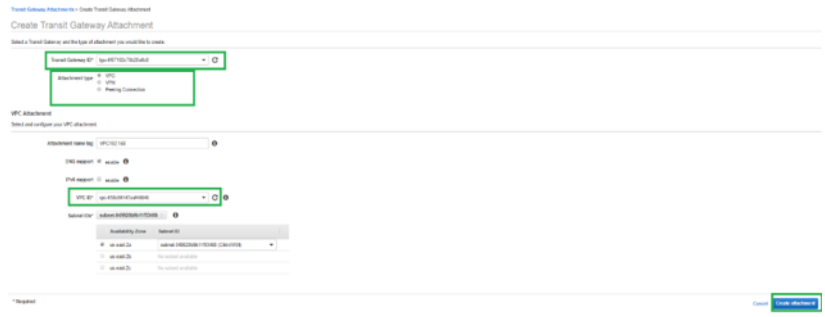
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Para crear los **anexos de puerta de enlace de tránsito**, vaya a Puertas de **enlace de tránsito > Anexos de puerta de tránsito y haga clic en Crear datos adjuntosde puerta de enlace de tránsito**

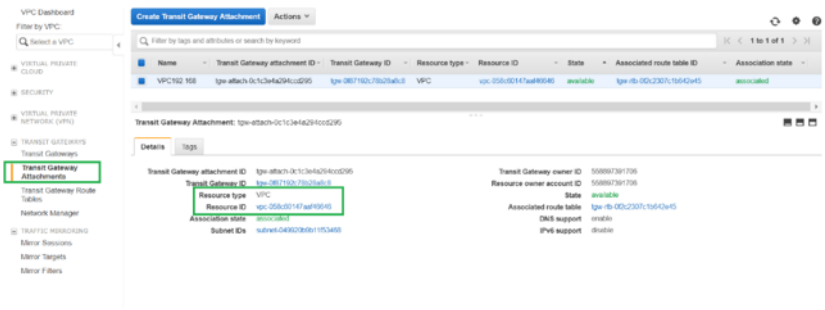


3. Seleccione la puerta de enlace de tránsito creada en la lista desplegable y seleccione el tipo de adjunto como **VPC**. Proporcione la etiqueta de nombre de datos adjuntos y seleccione el ID de VPC que quiere adjuntar a la puerta de enlace de tránsito creada. Una de las subredes de la VPC seleccionada se seleccionará automáticamente. Haga clic en **Crear datos adjuntos** para adjuntar VPC a Transit Gateway.



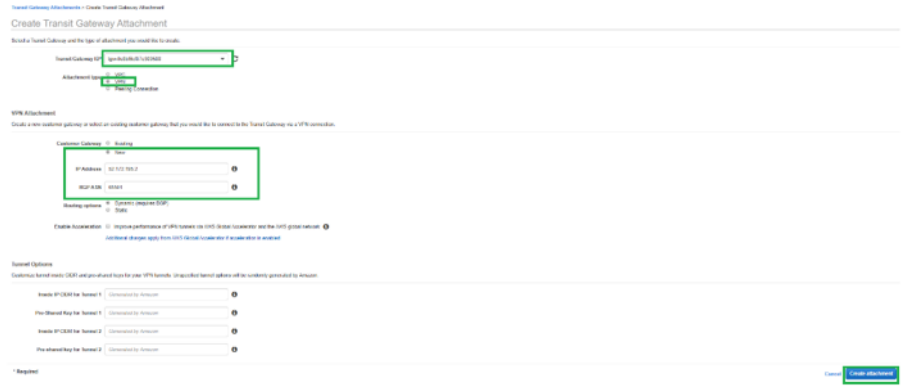
4. Después de adjuntar la VPC a la puerta de enlace de tránsito, puede ver que el **tipo de recurso VPC** se asoció a la puerta de enlace de tránsito.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

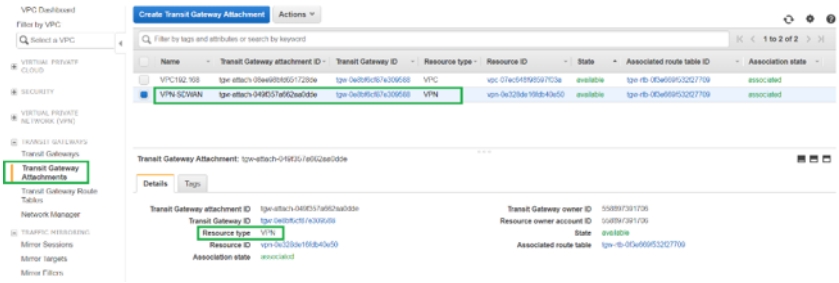


5. Para adjuntar SD-WAN a la puerta de enlace de tránsito mediante VPN, seleccione el **ID de puerta de enlace de tránsito** en la lista desplegable y seleccione **Tipo de archivo adjunto** como **VPN**. Asegúrese de seleccionar el ID de puerta de enlace de tránsito correcto.

   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.

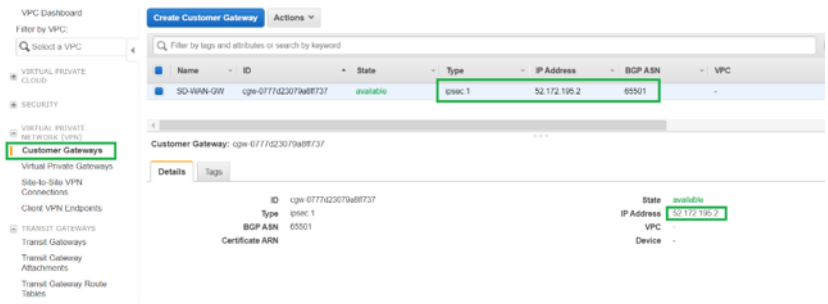


6. Una vez que la VPN esté conectada a la puerta de enlace de tránsito, puede ver los detalles como se muestra en la siguiente captura de pantalla:



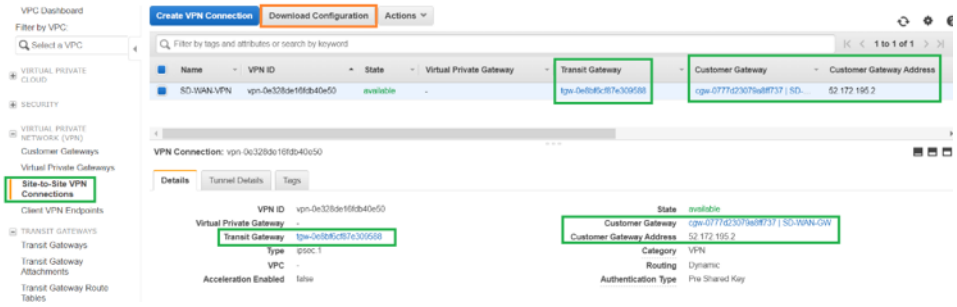
7. En Puertas de **enlace de clientes**, la puerta de enlace de cliente SD-WAN y la conexión VPN de sitio a sitio se crean como parte de la conexión VPN a puerta de enlace de tránsito. Puede ver que la puerta de enlace del cliente de SD-WAN se crea junto con la dirección IP de esta puerta de enlace de cliente que representa la dirección IP pública del vínculo WAN de SD-WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

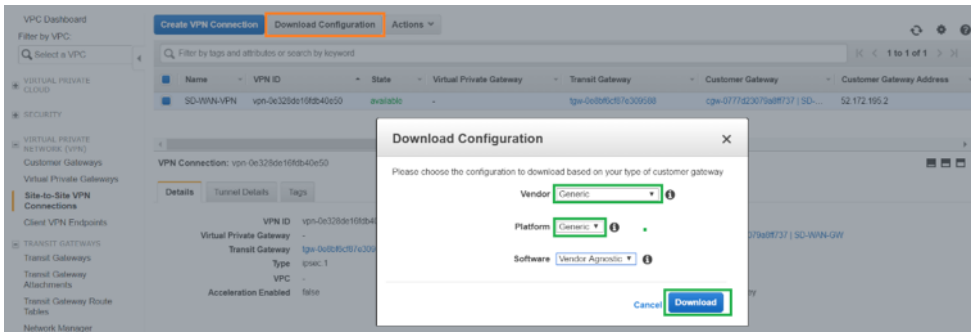


8. Vaya a **Conexiones VPN de sitio a sitio para descargar la configuración de VPNde puerta de enlace de cliente de SD-WAN**. Este archivo de configuración tiene dos detalles de túnel IPSec junto con la información del par BGP. Se crean dos túneles de SD-WAN a Transit Gateway para redundancia.

   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

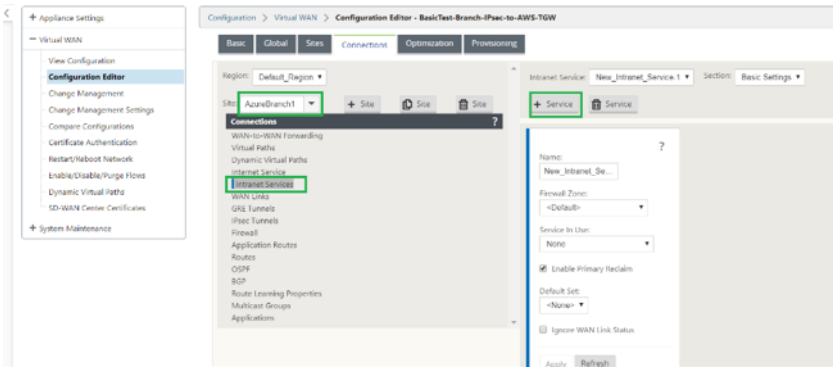
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

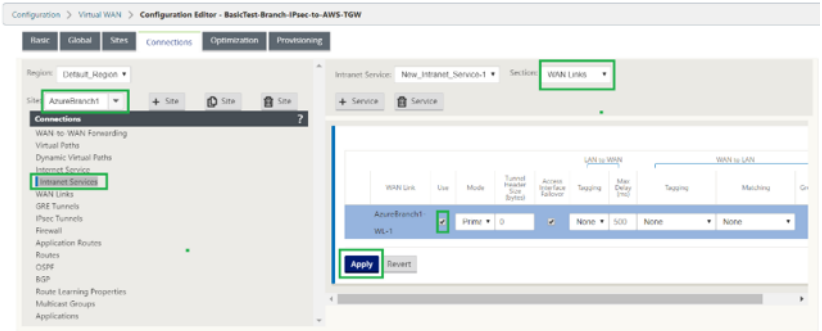
```
#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is
associated with the IPSec tunnel. All traffic transmitted to the tunnel
interface is encrypted and transmitted to the Virtual Private Gateway.


The Customer Gateway and Virtual Private Gateway each have two addresses that relate
to this IPSec tunnel. Each contains an outside address, upon which encrypted
traffic is exchanged. Each also contain an inside address associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway                  : 52.172.195.2
  - Virtual Private Gateway           : 3.133.37.22

Inside IP Addresses
  - Customer Gateway                  : 169.254.216.178/30
  - Virtual Private Gateway           : 169.254.216.177/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes
```

Configurar el servicio de Intranet en SD-WAN

1. Para configurar el servicio de Intranet que se utiliza en la configuración del túnel IPSec en SD-WAN, vaya a **Editor de configuración > Conexiones**, seleccione el sitio en la lista desplegable y seleccione **Servicio de intranet**. Haga clic en **+ Servicio** para agregar un nuevo servicio de Intranet.

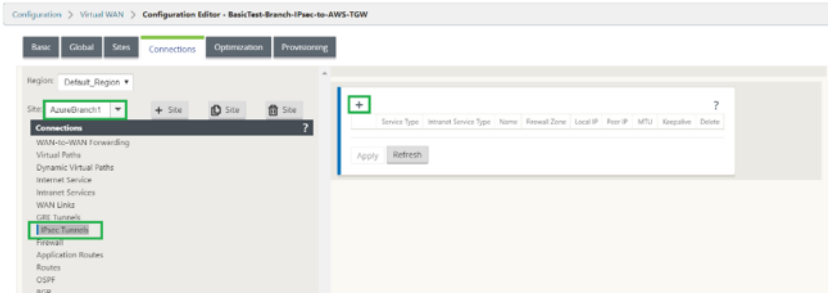


2. Después de agregar el servicio de Intranet, seleccione el enlace WAN (con el que va a establecer el túnel hacia la puerta de enlace de tránsito) que se utiliza para este servicio.



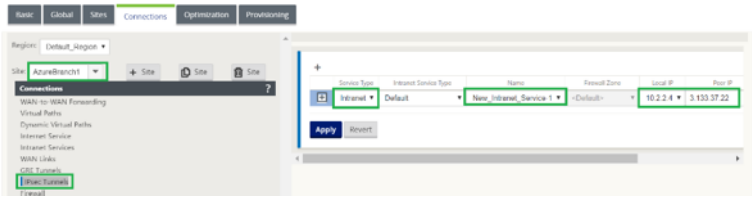
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Para configurar el túnel IPSec hacia AWS Transit Gateway, vaya a **Configuration Editor > Connections** seleccione el sitio en la lista desplegable y haga clic en **Túneles IPSec**. Haga clic en la opción **+** para agregar túnel IPsec.

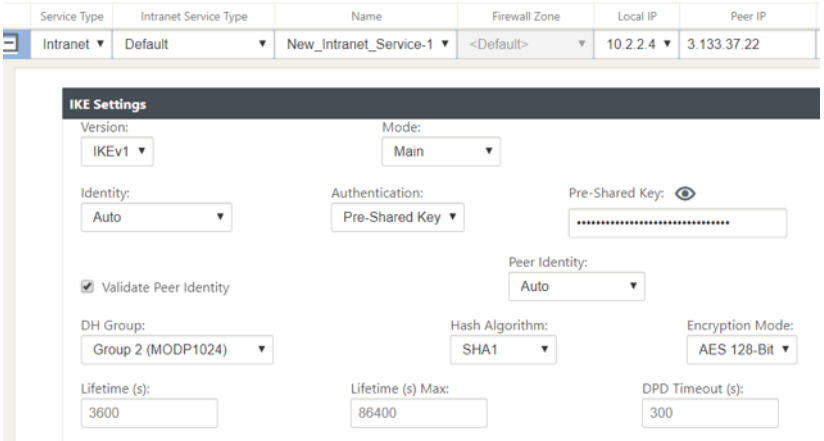


4. Seleccione el **tipo de servicio** como **intranet** y seleccione el **nombre del servicio de intranet** que ha agregado. Seleccione la dirección **IP local como la dirección IP** de enlace WAN y la dirección **del** mismo nivel como dirección IP de puerta de enlace privada virtual de tránsito.

   Haga clic en la casilla de verificación **Keepalive** para que SD-WAN inicie el túnel inmediatamente después de la activación de la configuración.

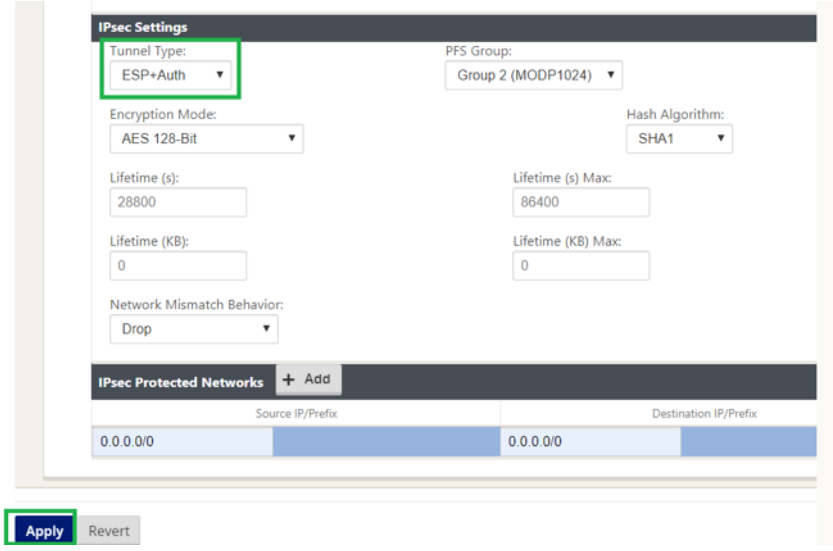


5. Configure los parámetros de IKE en función del archivo de configuración de VPN que ha descargado de AWS.

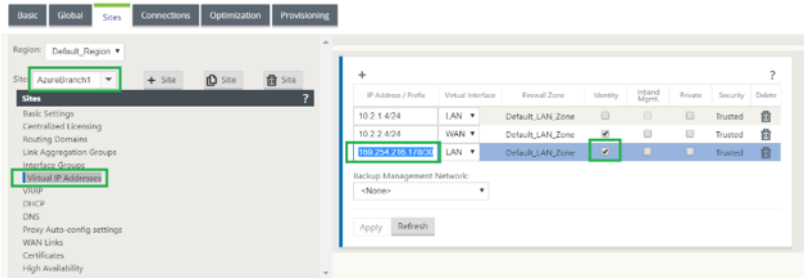


6. Configure los parámetros IPSec en función del archivo de configuración de VPN que ha descargado de AWS. Configure también **las redes protegidas IPSec** en función de la red que desea enviar a través del túnel. Puede ver que está configurado para permitir cualquier tráfico a través del túnel IPSec.

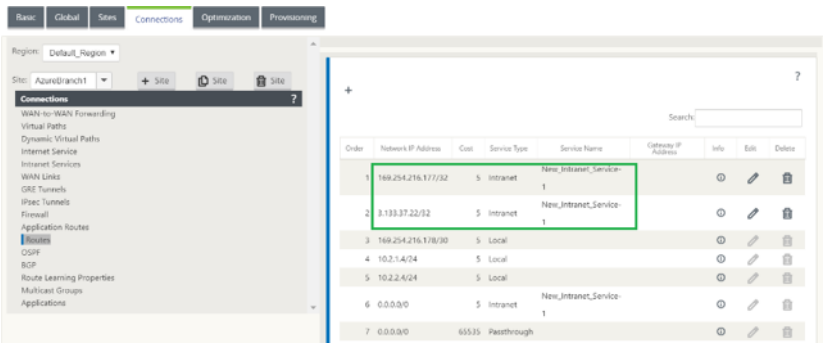
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Configure la puerta de **enlace del cliente dentro de la dirección IP** como una de las direcciones IP virtuales en SD-WAN. Desde el archivo de configuración de VPN descargado, busque la Gateway del cliente dentro de la dirección IP relacionada con Tunnel-1. Configure esta puerta de enlace de cliente dentro de la dirección IP como una de las direcciones IP virtuales en SD-WAN y active la casilla **Identity**.



8. Agregue **rutas** en SD-WAN para llegar a la **puerta de enlace privada virtual** de tránsito. Desde el archivo de configuración de VPN descargado, busque la dirección IP interna y externa de Virtual Private Gateway relacionada con Tunnel-1. Agregue rutas a la dirección IP interna y externa de Virtual Private Gateway con el **tipo de servicio** como **Intranet** y seleccione el servicio de Intranet creado en los pasos anteriores.

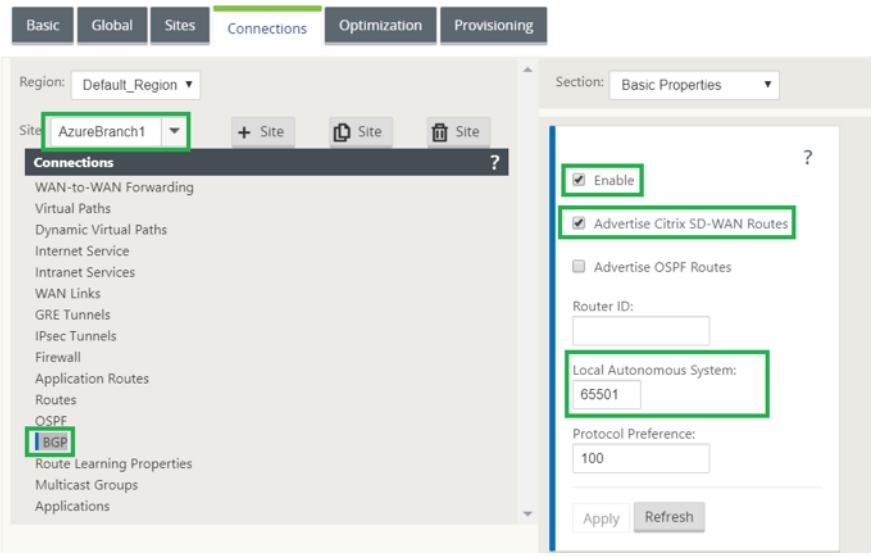


9. Configure **BGP** en SD-WAN. Habilite BGP con el número ASN adecuado. En el archivo de con-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

figuración de VPN descargado, busque las opciones de configuración de BGP relacionadas con Tunnel-1. Utilice estos detalles para agregar vecino BGP en SD-WAN.

Para habilitar BGP en SD-WAN, vaya a **Conexiones**, seleccione el sitio en la lista desplegable y, a continuación, seleccione **BGP**. **Haga clic en la casilla de verificación Habilitar para habilitar BGP.** Haga clic en la casilla de verificación **Anunciar rutas SD-WAN de Citrix** para anunciar rutas SD-WAN hacia la puerta de enlace de tránsito. Utilice el **ASN de puerta de enlace del cliente** desde las opciones de configuración de BGP y configúrelo como **Sistema Autónomo Local**.



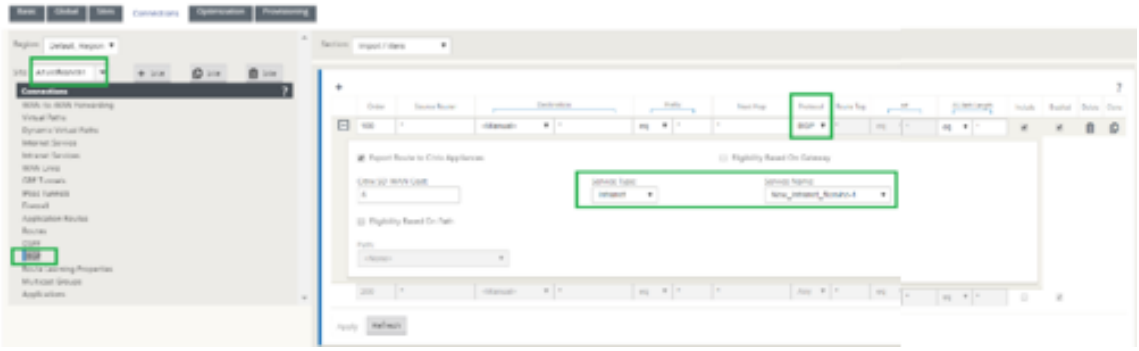
10. Para agregar **vecinos** BGP en SD-WAN, vaya a **Conexiones** seleccione el sitio en la lista desplegable y, a continuación, seleccione **BGP**. Haga clic en la sección **Vecinos** y en la opción **+**.

    Utilice **Dirección IP de vecino** y **ASN de puerta de enlace privada virtual** desde las opciones de configuración de BGP mientras agrega vecino. La **IP de origen** debe coincidir con la **puerta de enlace del cliente** dentro de la dirección IP (configurada como dirección IP virtual en SD-WAN) desde el archivo de configuración descargado de AWS. Agregar vecino BGP con **Multi Hop** habilitado en SD-WAN.

11. Para agregar **filtros de importación** para importar rutas BGP a SD-WAN, vaya a **Conexiones**, seleccione el sitio en la lista desplegable, seleccione **BGP** y haga clic en **Importar la sección Filtros**. Haga clic en la opción **+** para agregar un filtro de importación. Seleccione el **protocolo** como **BGP** y coincida con cualquiera para importar todas las rutas BGP. Seleccione el **tipo de servicio** como **Intranet** y seleccione el servicio de Intranet creado. Esto es para importar rutas

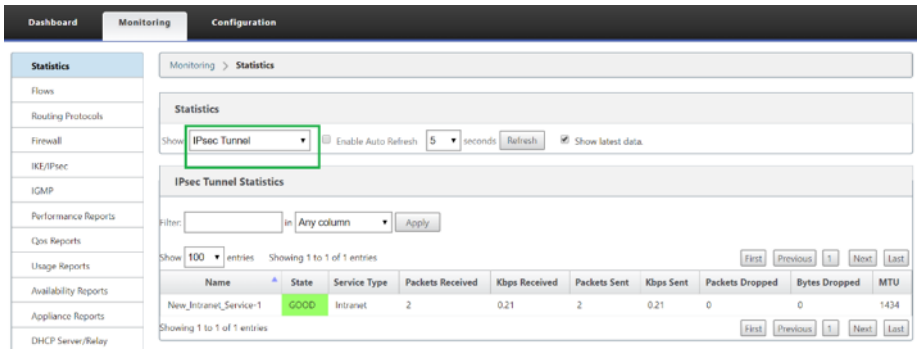
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

BGP con tipo de servicio como Intranet.



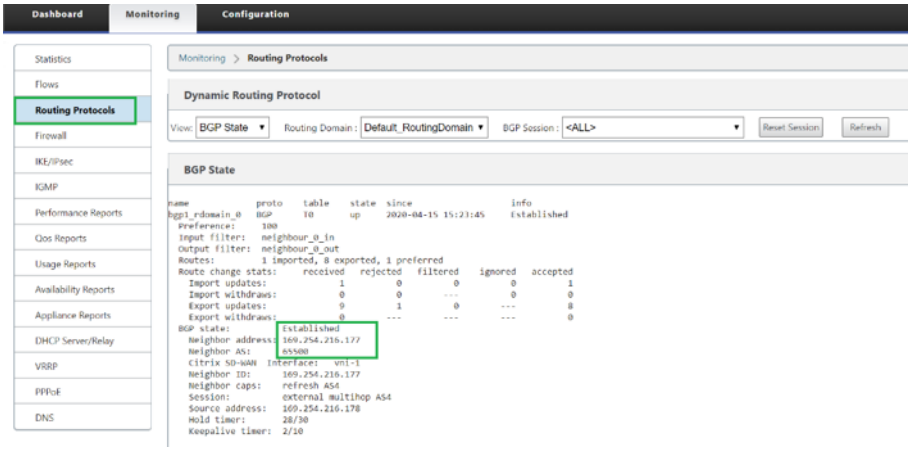
Supervisión y resolución de problemas en SD-WAN

1. Para comprobar el estado de establecimiento del túnel IPSec en SD-WAN, vaya a **Supervisión > Estadísticas > Túnel IPSec**. En la siguiente captura de pantalla, puede ver que el túnel IPSec se establece desde SD-WAN hacia AWS Transit Gateway y el estado es **BUENO**.
   Además, puede supervisar la cantidad de tráfico enviado y recibido a través de este túnel IPSec.



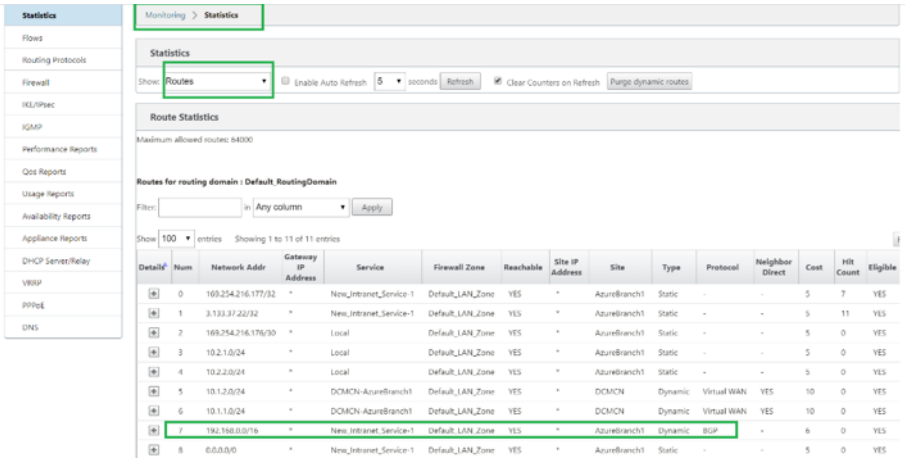
2. Para verificar el estado de **Peering BGP** en SD-WAN, vaya a **Supervisión > Protocolos de enrutamiento** y seleccione **Estado BGP**. Puede ver que el estado BGP se informó como **Establecido** y que la **dirección IP del vecino** y la **ASN de vecino** coinciden con los detalles del vecino BGP de AWS. Con esto, puede asegurarse de que el peering BGP se estableció desde SD-WAN hasta AWS Transit Gateway a través del túnel IPSec.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Una VPC (192.168.0.0) está conectada a AWS Transit Gateway. SD-WAN ha aprendido esta red VPC (192.168.0.0) desde AWS Transit Gateway a través de BGP
y esta ruta se instaló en SD-WAN con el tipo de servicio como Intranet según el filtro de importación creado en los pasos anteriores.

3. Para verificar la instalación de la ruta BGP en SD-WAN, vaya a **Supervisión > Estadísticas > Rutas** y compruebe la red 192.168.0.0/16 que se instaló como ruta BGP con el tipo de servicio como Intranet. Esto significa que puede aprender las redes conectadas a AWS Transit Gateway y puede comunicarse con esas redes a través del túnel IPSec establecido.



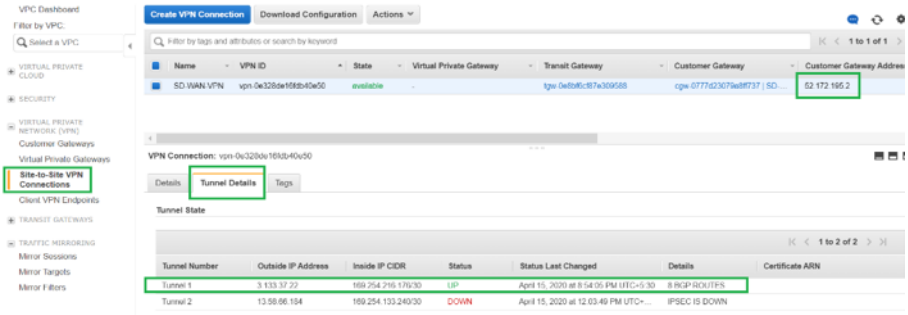
Supervisión y solución de problemas en AWS

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 Tunnel con AWS Transit

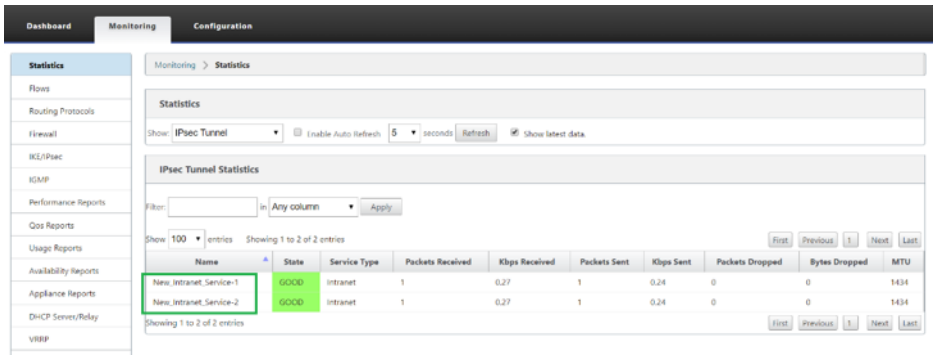
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gateway y también puede intercambiar rutas a través de BGP.

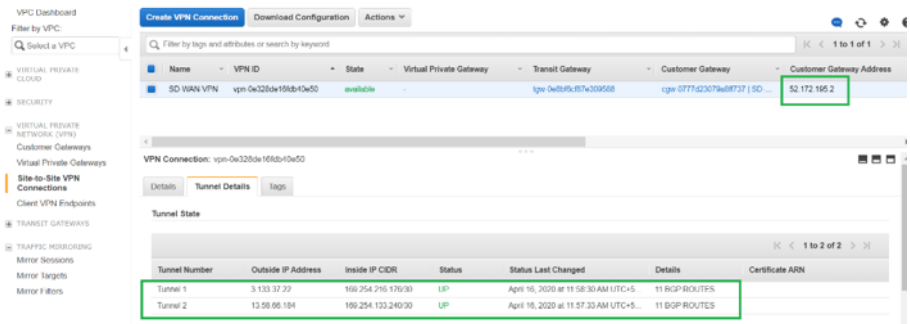


2. Configure los detalles de IPSec y BGP relacionados con el segundo túnel en función del archivo de configuración descargado en SD-WAN.

   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:



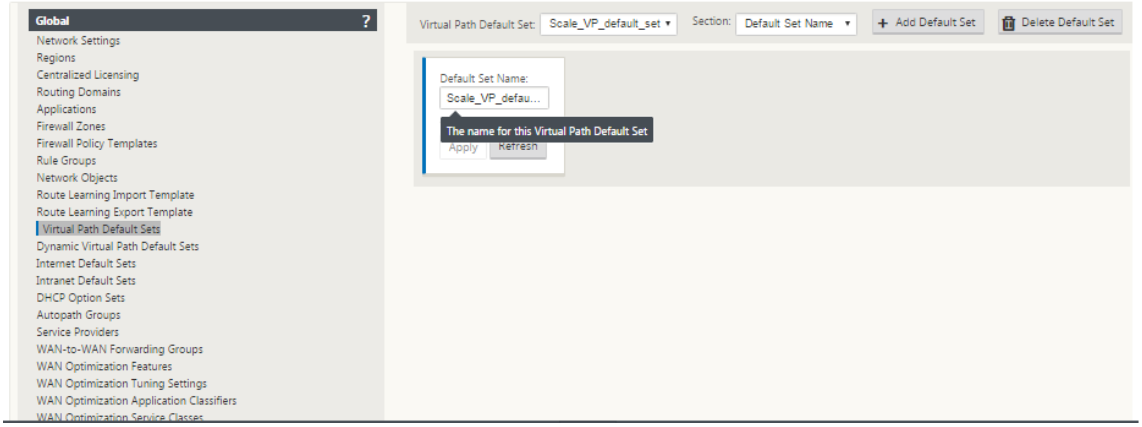
Cómo configurar túneles IPSec para rutas virtuales y dinámicas

May 7, 2021

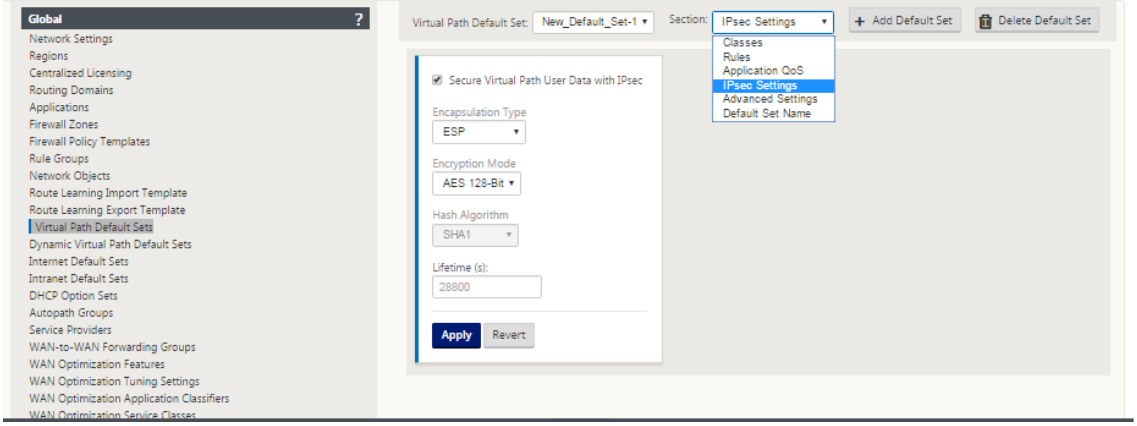
Para configurar túneles IPSec para rutas virtuales virtuales virtuales y dinámicas entre sitios de sucursal de Citrix SD-WAN:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Desplácese hasta **Global > Conjuntos predeterminados de rutas virtuales** o **Conjuntos predeterminados de rutas virtuales dinámicas**.



2. Cree un nuevo conjunto predeterminado (ruta virtual o dinámica) y habilite los **datos de usuario de ruta virtual segura con IPSec**.
3. Elija una de las opciones disponibles para el cifrado IPSec:
   - Tipos de encapsulación: ESP, AH o ESP+AH
   - Modos de cifrado: AES-CBC, AES 128 o 256 bits
   - Algoritmo hash: SHA1 o SHA-256
4. Aplique el conjunto predeterminado de ruta virtual creado al nodo MCN. Esto aplica automáticamente el mismo conjunto predeterminado a todos los nodos de cliente que tienen ruta virtual al MCN.



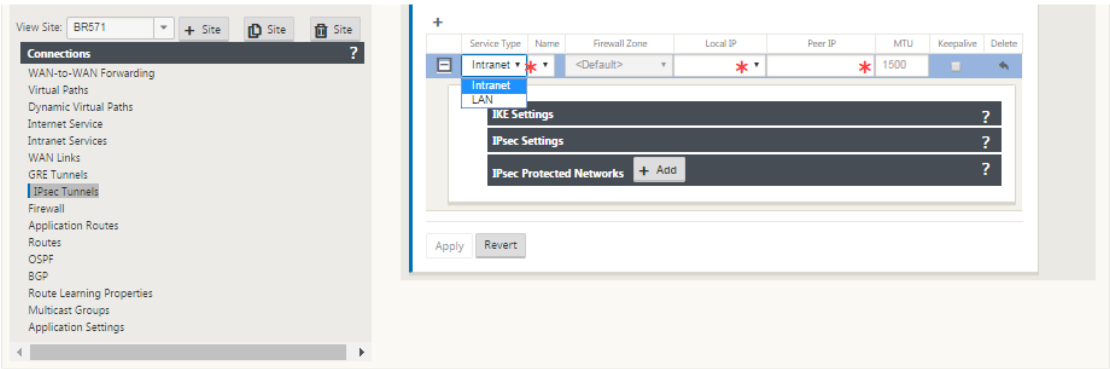
Cómo configurar túneles IPSec entre dispositivos SD-WAN y de terceros

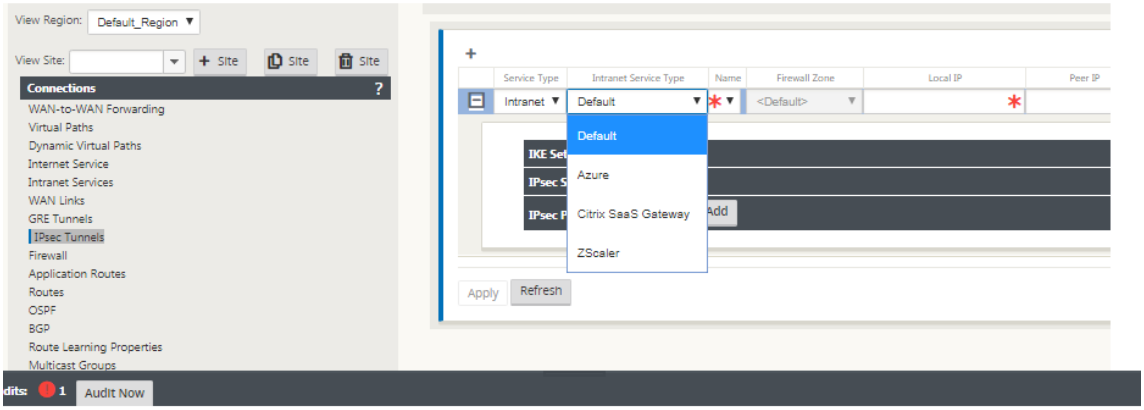
May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

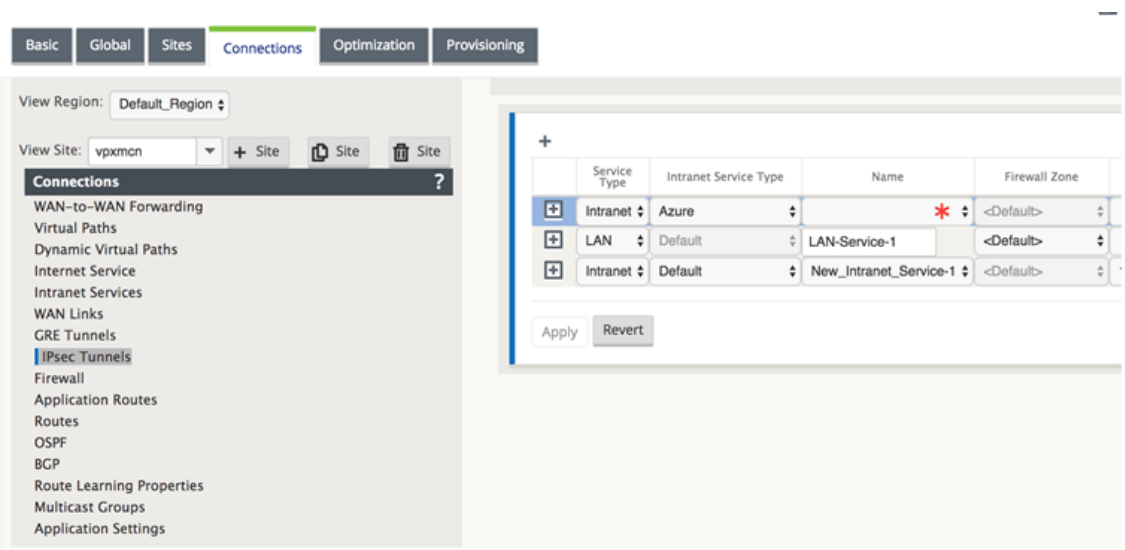
Para configurar el túnel IPSec para el servicio de intranet o LAN:

1. En el **Editor de configuración**, vaya a **Conexiones**> **Ver sitio**> **[Nombre del sitio]**> **Túneles IPSec**. Elija un **tipo de servicio** (LAN o Intranet).
2. Introduzca un **nombre** para el tipo de servicio. Para el tipo de servicio de Intranet, el servidor de Intranet configurado determina qué direcciones IP locales están disponibles.
3. Seleccione la dirección **IP local disponible e introduzca la dirección IP** del **mismo nivel** para la ruta virtual con la que se va a establecer el mismo nivel.

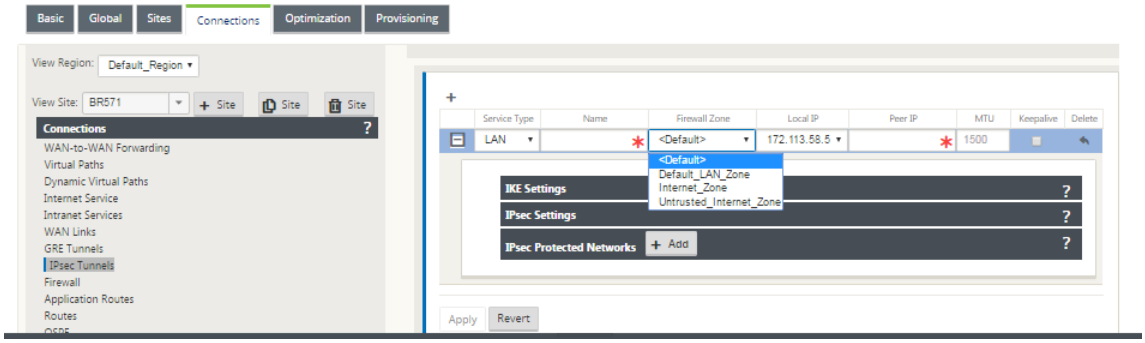




© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Si el tipo de servicio es Intranet, la dirección IP está predeterminada por el servicio de intranet seleccionado.



4. Configure la configuración de IPSec aplicando los criterios descritos en las tablas siguientes. Cuando haya terminado, haga clic en **Aplicar** para guardar la configuración.

Campo	Descripción	Valor
Tipo de servicio	Elija un tipo de servicio en el menú desplegable	Intranet, LAN
Nombre	Si el tipo de servicio es Intranet, elija en la lista de servicios de intranet configurados en el menú desplegable. Si el tipo de servicio es LAN, escriba un nombre único	Cadena de texto

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Descripción	Valor
IP local	Elija la dirección IP local del túnel IPSec en el menú desplegable de direcciones IP virtuales disponibles configuradas en este sitio	Dirección IP
IP del mismo nivel	Introduzca la dirección IP del mismo nivel del túnel IPSec	Dirección IP
MTU	Introduzca la **MTU** para fragmentar fragmentos IKE e IPSec	Predeterminado: 1500
Configuración IKE	Versión: Seleccione una versión IKE en el menú desplegable	IKEv1 IKEv2
Modo	Elija un modo en el menú desplegable	Cumple con FIPS: Principal, no compatible con FIPS: Agresivo
Identidad	Elija una identidad en el menú desplegable	Dirección IP automática Manual Dirección IP Usuario FQDN
Autenticación	Elija el tipo de autenticación en el menú desplegable	Clave previamente compartida: si está utilizando una clave previamente compartida, cópiela y péguela en este campo. Haga clic en el icono de globo ocular () para ver la clave previamente compartida. Certificado: si está utilizando un certificado de identidad, selecciónelo en el menú desplegable.
Validar identidad del mismo nivel	Active esta casilla de verificación para validar el par del IKE. Si el tipo de ID del par no es compatible, no habilite esta función	Ninguno

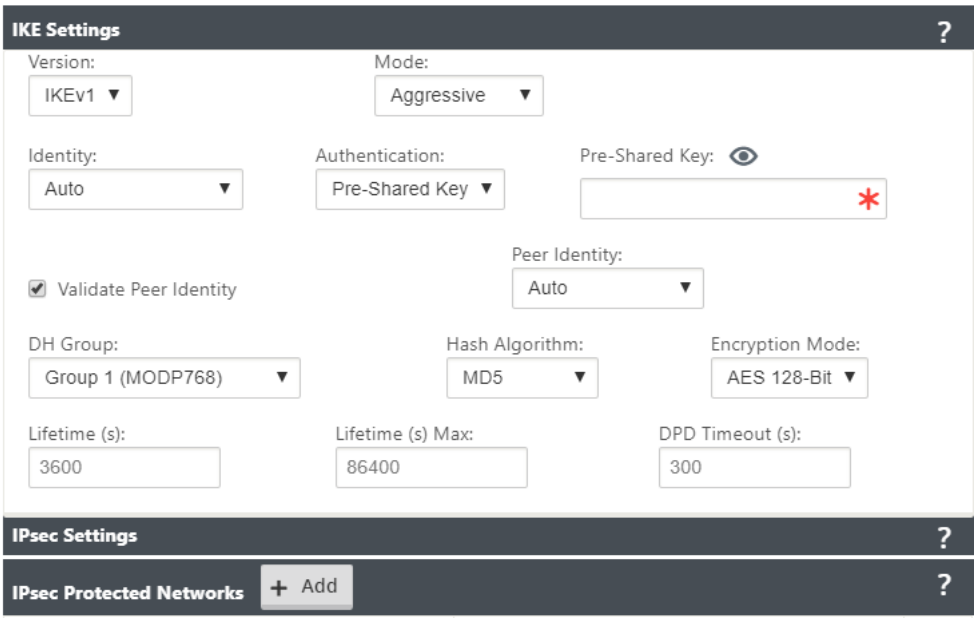
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Descripción	Valor
Grupo DH	Elija el grupo Diffie-Hellman para utilizar para la generación de claves IKE en el menú desplegable	No compatible con FIP: Grupo 1, Cumple con FIPS: Grupo 2 Grupo 5 Grupo 14 Grupo 15 Grupo 16 Grupo 19 Grupo 20 Grupo 21
Algoritmo hash	Elija un algoritmo en el menú desplegable para autenticar los mensajes IKE	No cumple con FIPS: MD5 Cumple con FIPS: SHA1 SHA-256
Modo de cifrado	Elija el **modo de cifrado** para mensajes IKE en el menú desplegable	AES de 128 bits AES de 192 bits AES de 256 bits
Vida útil (s)	Introduzca la duración preferida, en segundos, para que exista una asociación de seguridad IKE	3600 segundos (predeterminado)
Vida útil (s) máx.	Introduzca la duración máxima preferida, en segundos, para permitir que exista una asociación de seguridad IKE	86400 segundos (predeterminado)
Tiempo de espera (s) de DPD	Introduzca el tiempo de **espera de detección de pares muertos**, en segundos, para las conexiones VPN	300 segundos (predeterminado)
IKEv2	Autenticación del mismo nivel: **seleccione Autenticación** del mismo nivel en el menú desplegable	Certificado de clave precompartida reflejado
IKE2 - Clave precompartida	Clave precompartida del mismo nivel: pegue la clave precompartida del par IKEv2 en este campo para la autenticación. Haga clic en el icono con forma de ojo para ver la clave precompartida	Cadena de texto

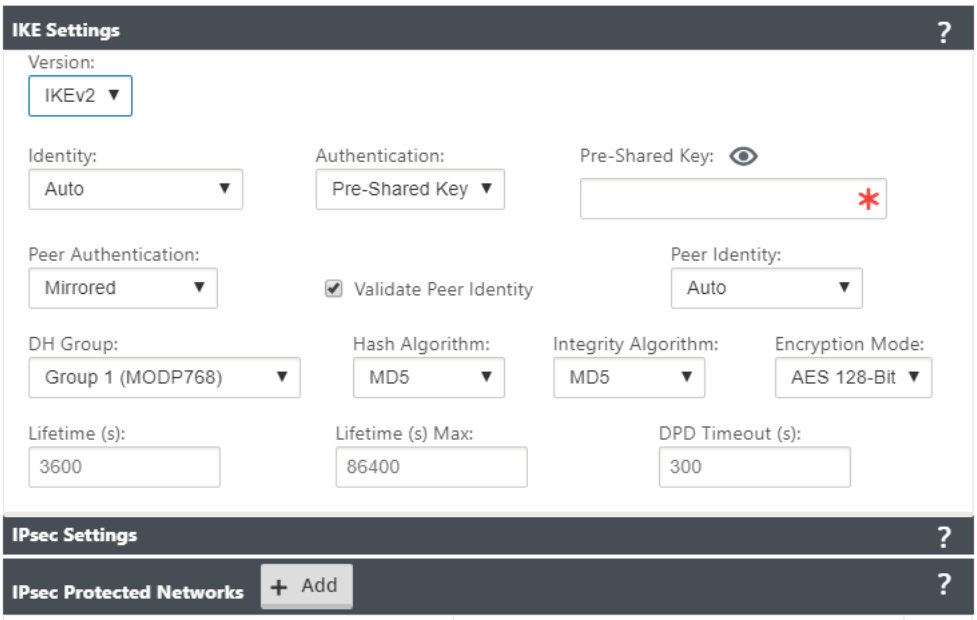
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Descripción	Valor
Algoritmo de integridad	Elija un algoritmo como algoritmo hash para usar para la verificación HMAC en el menú desplegable	No cumple con FIPS: MD5 Cumple con FIPS: SHA1 SHA-256

> **Nota:**
>
> Si el enrutador IPSec de terminación incluye código de autenticación de mensajes basado en hash (HMAC) en la configuración, cambie el modo IPSec a **Exp+Auth** con un algoritmo hash como **SHA1**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración de red protegida IPSec e IPSec:

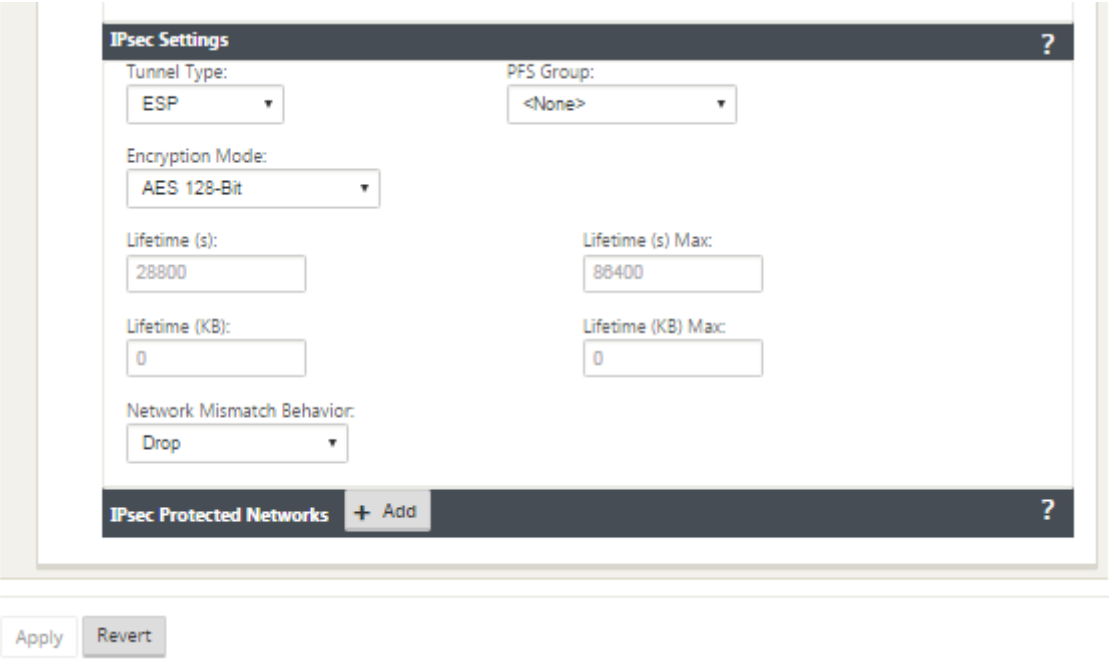
Campo	Descripción	Valor (s)
Tipo de túnel	Elija el **tipo de túnel** en el menú desplegable	ESP ESP+Auth ESP+NULL AH
Grupo PFS	Elija el grupo Diffie-Hellman para utilizar para una generación perfecta de claves de secreto directo en el menú desplegable	Grupo 1 Grupo 2 Grupo 5 Grupo 14 Grupo 15 Grupo 16 Grupo 19 Grupo 20 Grupo 21

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Descripción	Valor (s)
Modo de cifrado	Elija el **modo de cifrado** para los mensajes IPSec en el menú desplegable	Si elige ESP o ESP+ Auth, seleccione una de las siguientes opciones: AES 128 bits, AES 192 bits, AES 256 bits, AES 128 bits GCM 64 bits, AES de 128 bits GCM de 64 bits, AES de 192 bits GCM de 64 bits, AES de 128 bits GCM de 96 bits, AES de 192 bits GCM de 96 bits, AES de 192 bits GCM de 96 bits, AES de 192 bits GCM de 96 bits 96 bits, AES 128 bits GCM de 128 bits, AES de 192 bits GCM de 128 bits, AES de 256 bits GCM de 128 bits. AES 128/192/256 Bit son compatibles con CBC.
Vida útil (s)	Introduzca la cantidad de tiempo, en segundos, para permitir que exista una asociación de seguridad IPsec	28800 segundos (predeterminado)
Máx. (s) de vida útil	Introduzca la cantidad máxima de tiempo, en segundos para permitir que exista una asociación de seguridad IPsec	86400 segundos (predeterminado)
Duración (KB)	Introduzca la cantidad de datos, en kilobytes, para que exista una asociación de seguridad IPSec	Kilobytes
Duración máxima (KB)	Introduzca la cantidad máxima de datos, en kilobytes, para permitir que exista una asociación de seguridad IPSec	Kilobytes
Comportamiento de falta de coincidencia de red	Elija la acción que quiere realizar si un paquete no coincide con las redes protegidas del túnel IPSec en el menú desplegable	Soltar, enviar sin cifrar, usar ruta que no sea IPSec

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Campo	Descripción	Valor (s)
Redes protegidas IPSec	**IP/prefijo de origen**: después de hacer clic en el botón Agregar (+ Agregar), introduzca la **IP de origen** y el prefijo del tráfico de red que protegerá el túnel IPSec	Dirección IP
Redes protegidas IPSec	**IP/prefijo de destino**: introduzca la **IP de destino** y el prefijo del tráfico de red que el túnel IPSec protegerá	Dirección IP



Supervisar túneles IPSec

Desplácese hasta **Monitoring>IKE/IPSec** en la GUI del dispositivo SD-WAN para ver y supervisar la configuración del túnel IPSec.

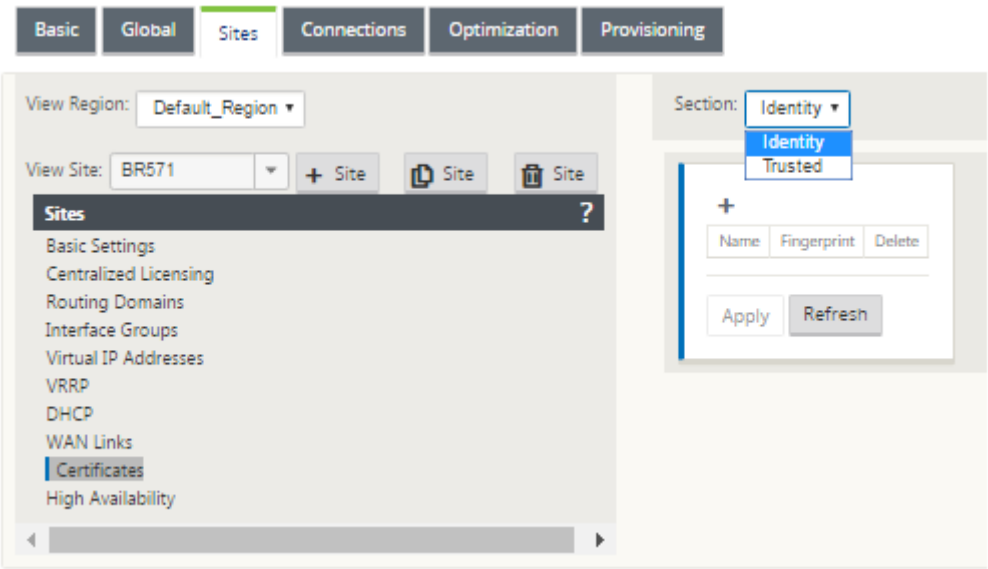
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cómo agregar certificados IKE

May 7, 2021

Para implementar certificados para la negociación IKE:

1. Vaya a **Sitios** > **Certificados** y agregue los certificados necesarios.



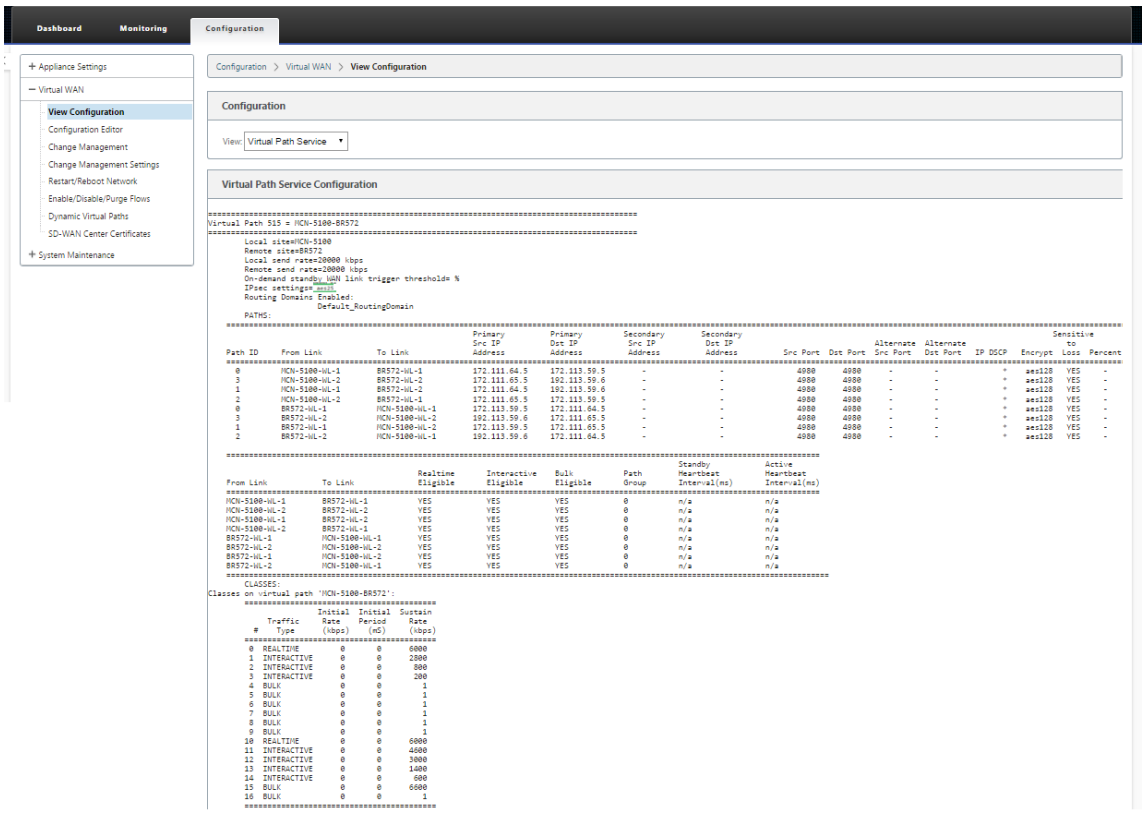
Cómo ver la configuración del túnel ipsec

May 7, 2021

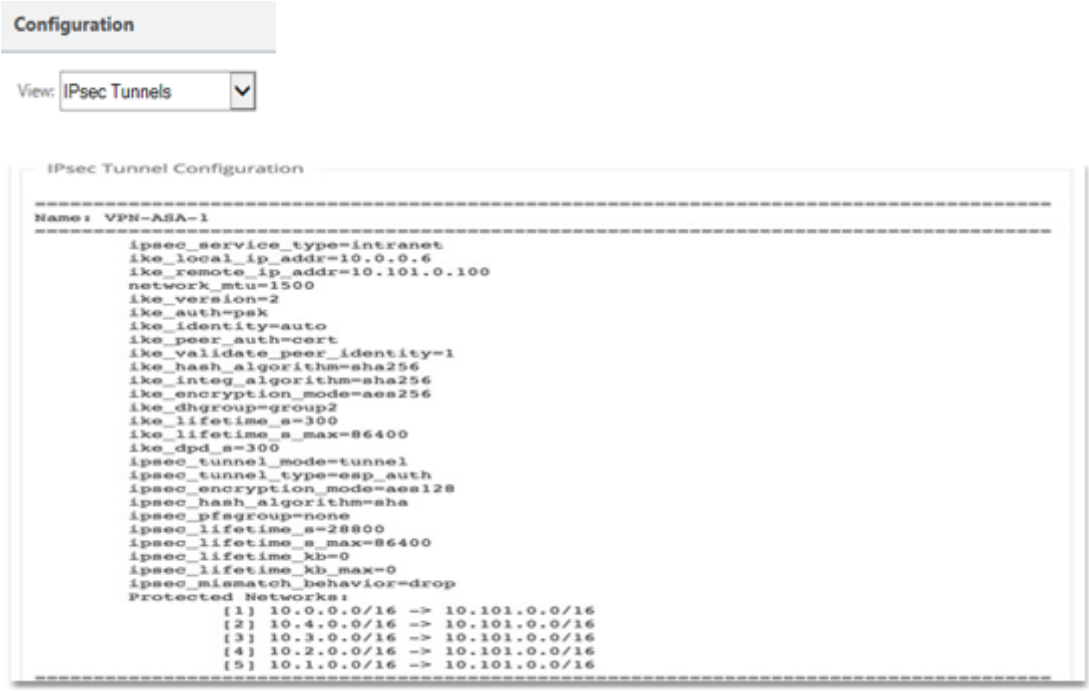
Para ver la configuración del túnel ipsec:

1. Vaya a **Configuración > WAN virtual** > **Ver configuración**.
2. Seleccione **Virtual Path Service** en el menú implementable. La configuración de IPSec se muestra si IPSec está habilitado en el editor de configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

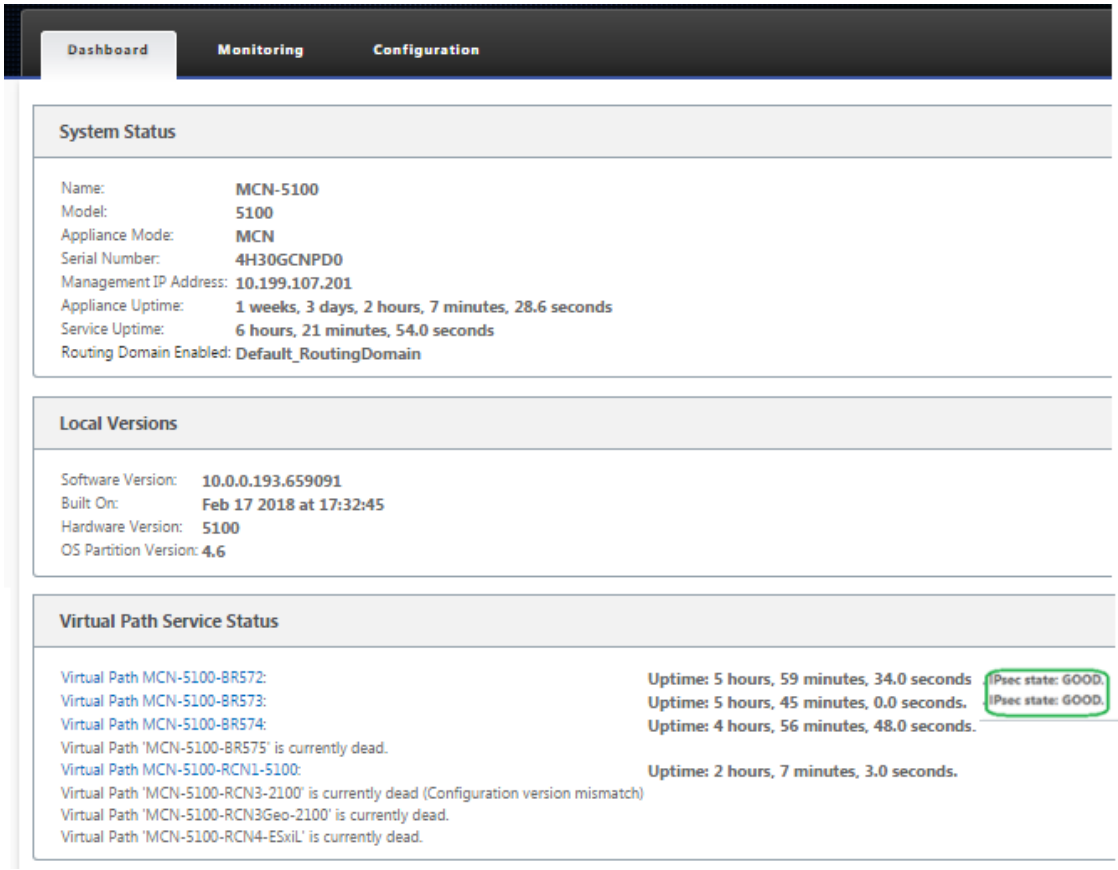


3. Seleccione **Túneles IPSec** en el menú implementable para ver la configuración del túnel IPSec.



4. Cada ruta virtual mostrará su propio estado de túnel IPSec como se muestra a continuación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

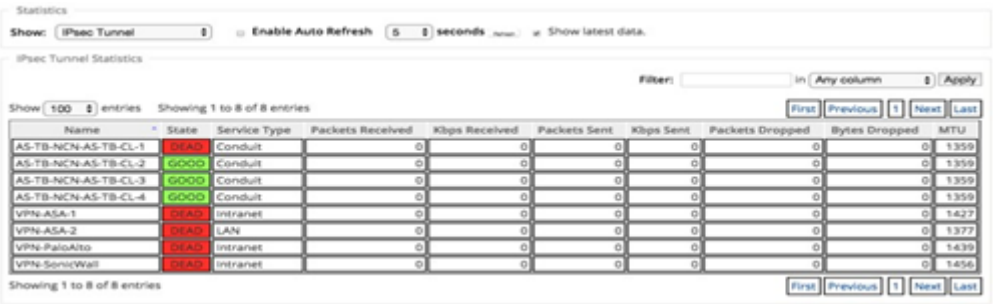


Supervisión y registro de IPSec

May 7, 2021

Para supervisar las estadísticas del túnel ipsec:

1. Desplácese hasta **Supervisar > Estadísticas**. Elija **IPSec Tunnel** en el menú implementable **Mostrar** como se muestra a continuación:



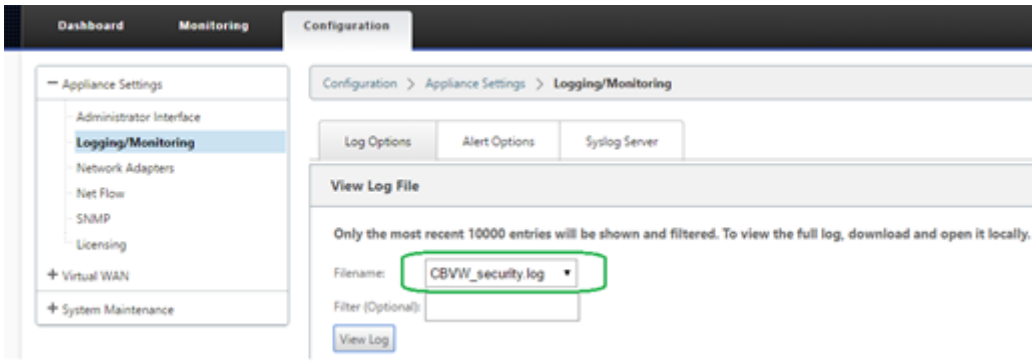
2. Vaya a **Monitor** > **IKE/IPSec**. Observe los túneles IPSec configurados, las asociaciones de servicios IKE e IPSec entre dos extremos VPN de modo o configurados dentro de la red SD-WAN.

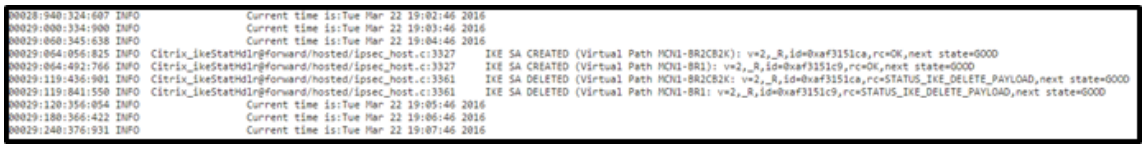
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cómo supervisar los registros de ipec

1. Vaya a **Configuración** > **Configuración del equipo** > **Registro/Supervisión**. Seleccione **Nombre de archivo** en el menú implementable y haga clic en **Ver registro**. Puede ver los siguientes detalles de registro para el túnel IPSec:

   - Creación y eliminación de túnel IPSec
   - Cambio de estado del túnel IPSec



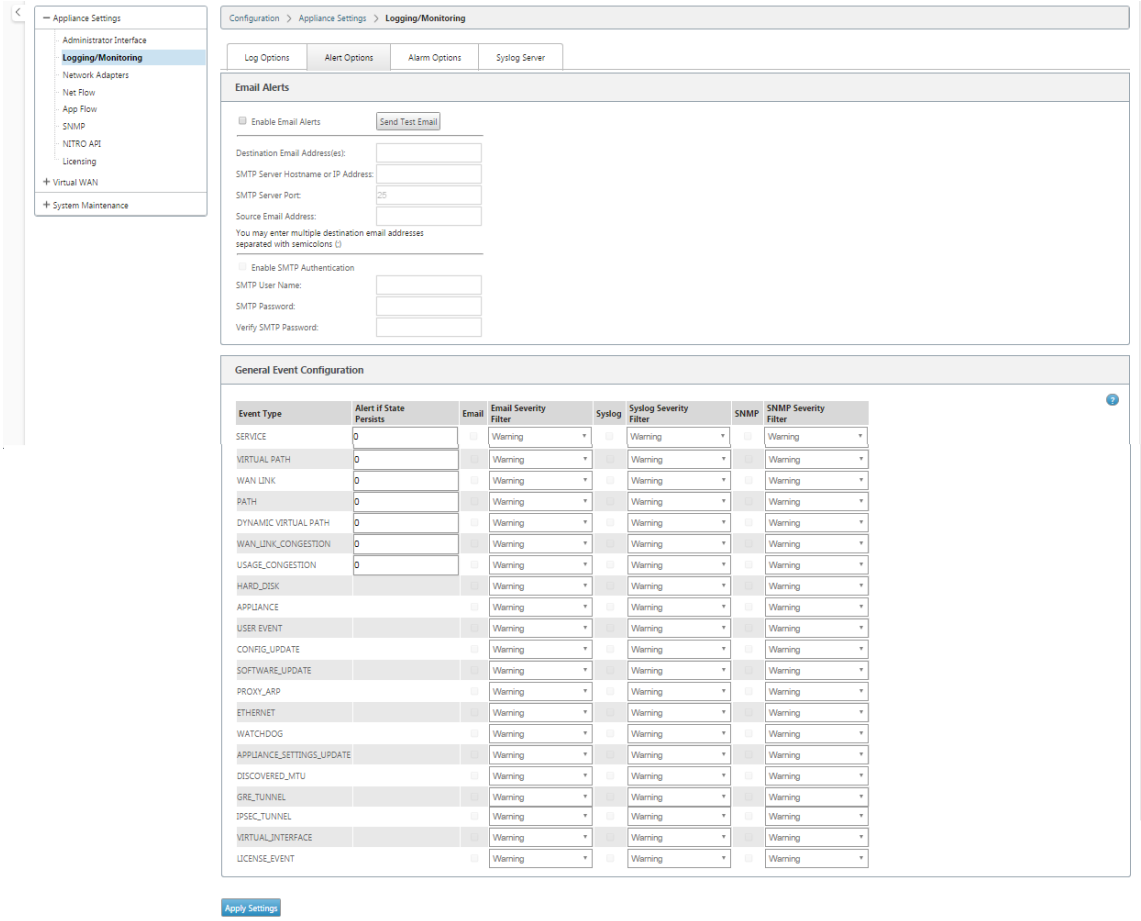


Cómo ver alertas de túnel ipsec

1. Vaya a **Configuración** > **Configuración del equipo > Registro/Supervisión** > **Opciones de alerta**.
2. Crear alertas de correo electrónico y Syslog para informes de estado de túnel IPSec.

   - Admite IPSEC_TUNNEL como uno de los tipos de eventos que le permite configurar los filtros de gravedad de correo electrónico y Syslog.

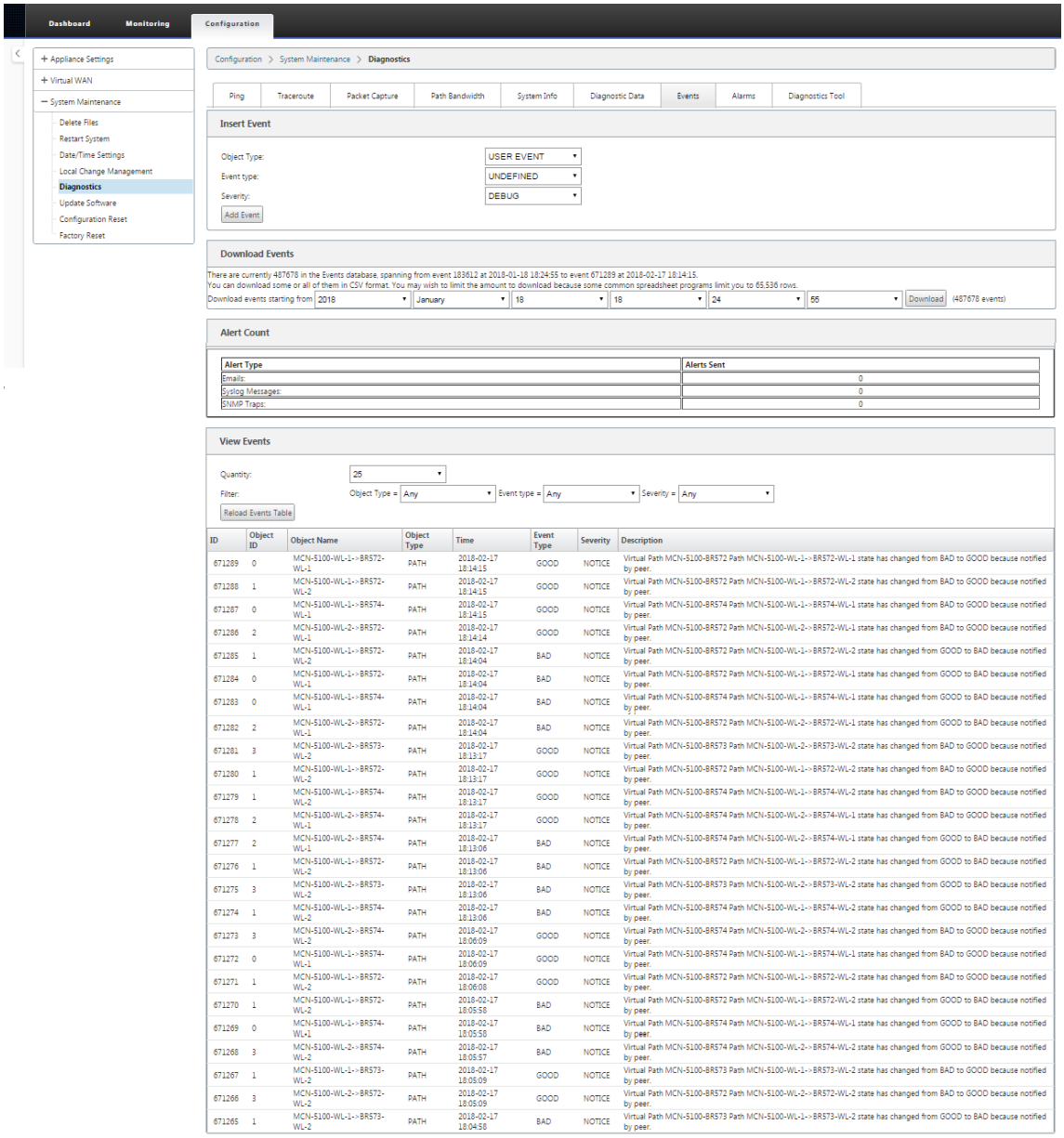
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cómo supervisar eventos de túnel ipsec

1. Vaya a **Configuración > Mantenimiento del sistema** > **Diagnósticos** > **Eventos**.
2. Agregue eventos basados en el tipo de objeto **IPSEC_TUNNEL**. Crear filtros para todos los eventos relacionados con IPSec.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

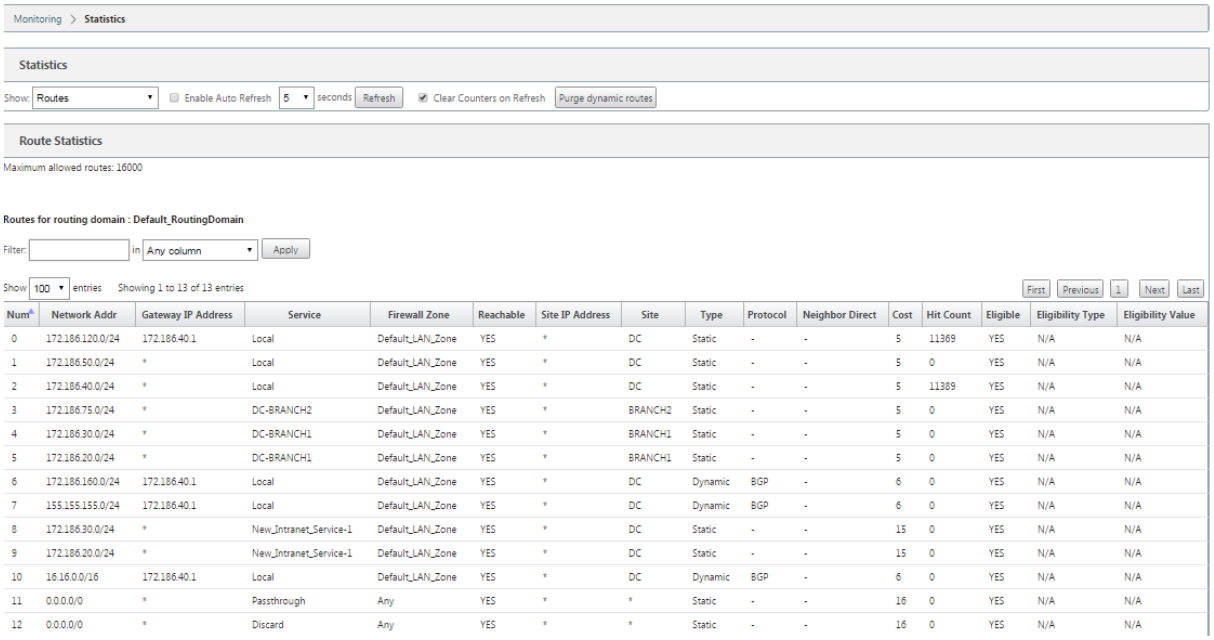


Elegibilidad para rutas de ruta no virtuales ipsec

May 7, 2021

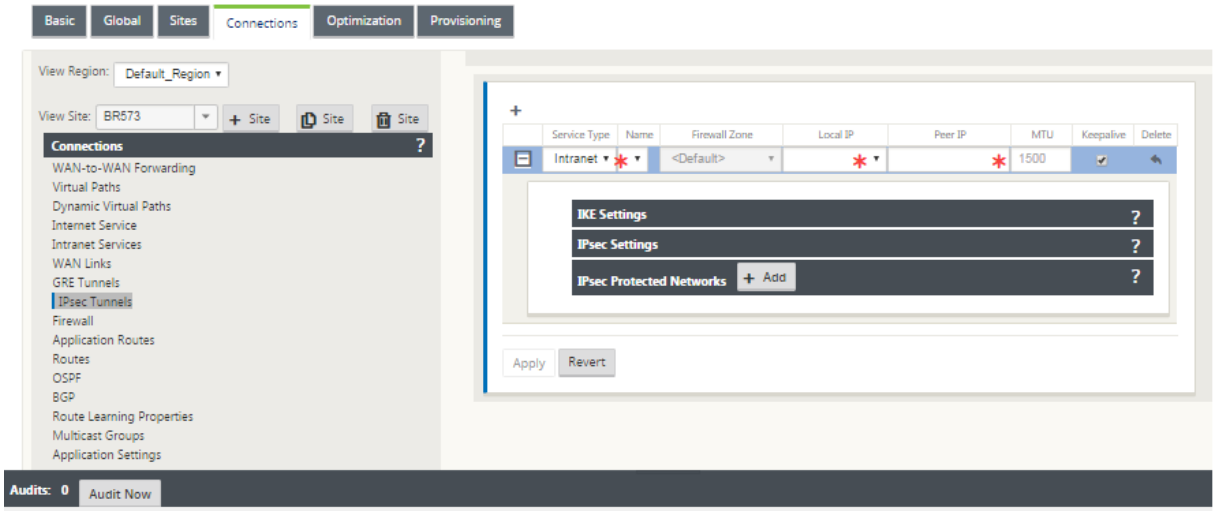
En versiones anteriores, las rutas de túnel ipsec permanecerían en la tabla de rutas, incluso si el túnel no estuviera disponible.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

El uso de la opción Keepalive en **Conexiones** > [Nombre del sitio] > **Túneles IPSec** mejora este comportamiento de modo que las rutas de ruta no virtuales IPSec se consideran ahora no aptas cuando el túnel IPSec ya no está disponible. Cuando se habilita la opción keepalive, las SA se crean automáticamente sin que se envíe ningún tráfico a través del túnel.



Cifrado nulo IPSec

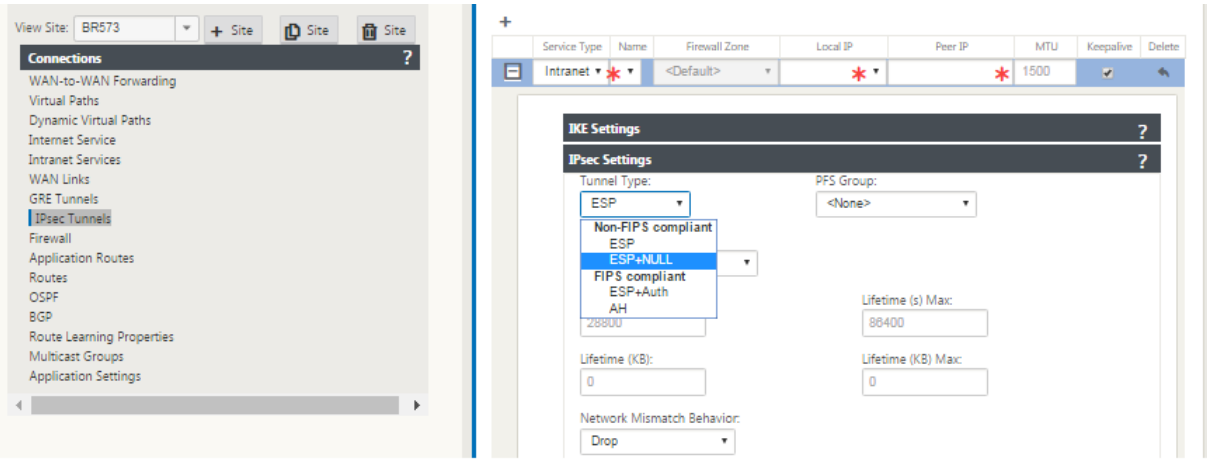
May 7, 2021

En versiones anteriores, se introdujo el tipo de túnel ESP+NULL. Cuando se utiliza el protocolo ESP IPSec, el tráfico suele estar cifrado y autenticado. Sin embargo, puede optar por no utilizar el cifrado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mediante el cifrado Nulo. En el tipo de túnel ESP + NULL, los paquetes se autentican pero no cifran.

Puede configurar el túnel IPSec con el tipo de túnel ESP+NULL en el Editor de configuración, en la sección **Configuración de IPSec**.



Cumplimiento de FIPS

May 7, 2021

En Citrix SD-WAN, el modo FIPS obliga a los usuarios a configurar las opciones 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 en 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 IPSec para rutas virtuales
- Hash IKE e modo de integridad (IKEv2), modo de autenticación IPsec.
- Realiza errores de auditoría para la configuración de vida basada en FIPS

Para habilitar el cumplimiento de FIPS mediante la GUI de Citrix SD-WAN:

1. Vaya a **Configuración** > **Virtual WAN** > **Editor de configuración** > **Global** y seleccione **Habilitar modo FIPS**.

Al habilitar el modo FIPS se aplican comprobaciones durante la configuración para garantizar que todos los parámetros de configuración relacionados con IPSec cumplan los estándares FIPS. Se le pedirá a través de errores de auditoría y advertencias que configure IPSec.

Para configurar la configuración de IPSec de ruta virtual:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Habilite los túneles IPSec de ruta virtual para todas las rutas virtuales donde se requiera el cumplimiento FIPS. La configuración IPSec para rutas virtuales se controla mediante conjuntos predeterminados.
- Configure la autenticación de mensajes cambiando el modo IPSec a AH o ESP+Auth y use una función hash aprobada por FIPS. SHA1 es aceptado por FIPS, pero SHA256 es altamente recomendable.
- La vida útil de IPsec debe configurarse durante no más de 8 horas (28.800 segundos).

La WAN virtual utiliza IKE versión 2 con claves previamente compartidas para negociar túneles IPSec a través de la ruta virtual mediante la siguiente configuración:

- Grupo DH 19: ECP256 (curva elíptica de 256 bits) para negociación de claves
- Cifrado AES-CBC de 256 bits
- Hashing SHA256 para autenticación de mensajes
- Hashing SHA256 para la integridad del mensaje
- DH Grupo 2: MODP-1024 para el secreto directo perfecto

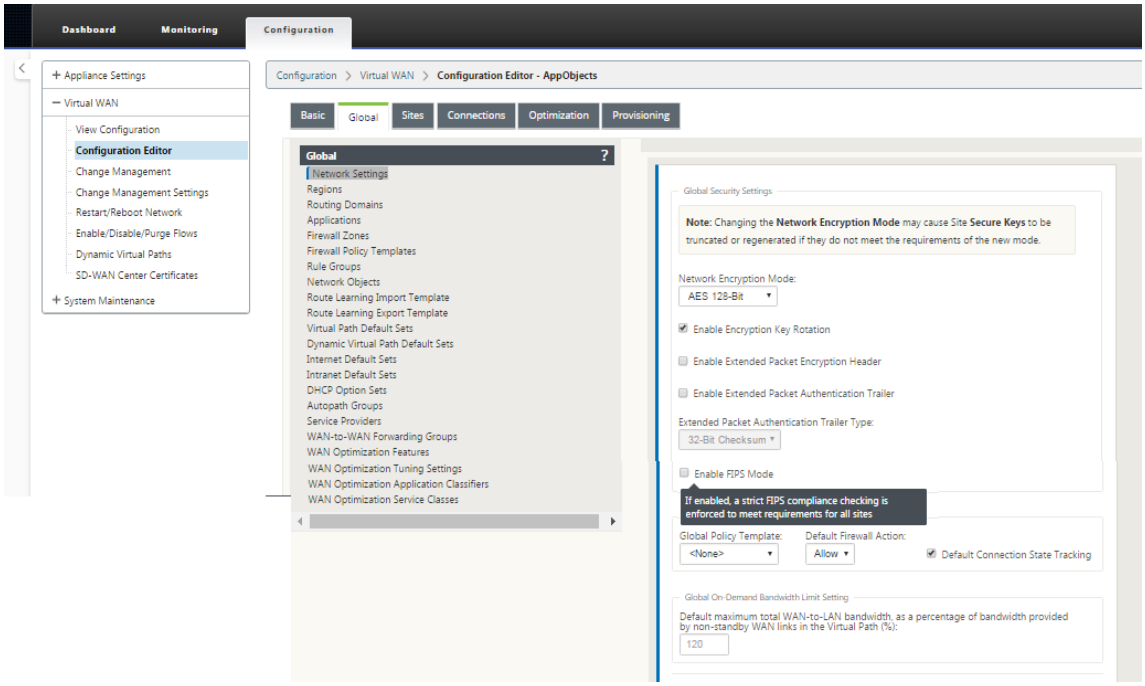
Para configurar el túnel IPSec para un tercero, utilice los valores siguientes:

1. Configure el grupo DH aprobado por FIPS. Los grupos 2 y 5 están permitidos bajo FIPS, sin embargo los grupos 14 y superiores son altamente recomendados.
2. Configure la función hash aprobada por FIPS. SHA1 es aceptado por FIPS, sin embargo SHA256 es altamente recomendable.
3. Si utiliza IKEv2, configure una función de integridad aprobada por FIPS. SHA1 es aceptado por FIPS, sin embargo SHA256 es altamente recomendable.
4. Configure una duración de IKE y una duración máxima de no más de 24 horas (86.400 segundos).
5. Configure la autenticación de mensajes IPSec cambiando el modo IPSec a AH o ESP+Auth y utilice una función hash aprobada por FIPS. SHA1 es aceptado por FIPS, pero SHA256 es altamente recomendable.
6. Configure una vida útil de IPSec y una vida útil máxima de no más de ocho horas (28.800 segundos).

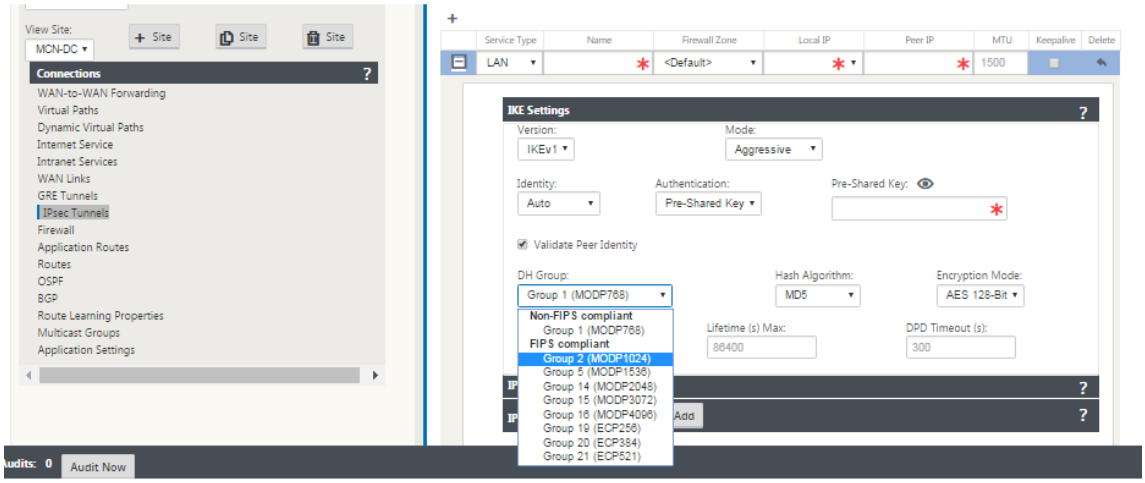
Para configurar túneles IPSec:

1. En el dispositivo MCN, vaya a **Configuración** > **Virtual WAN** > **Editor de configuración**. Abra un paquete de configuración existente. Vaya a **Conexiones** > **Túneles IPSec**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

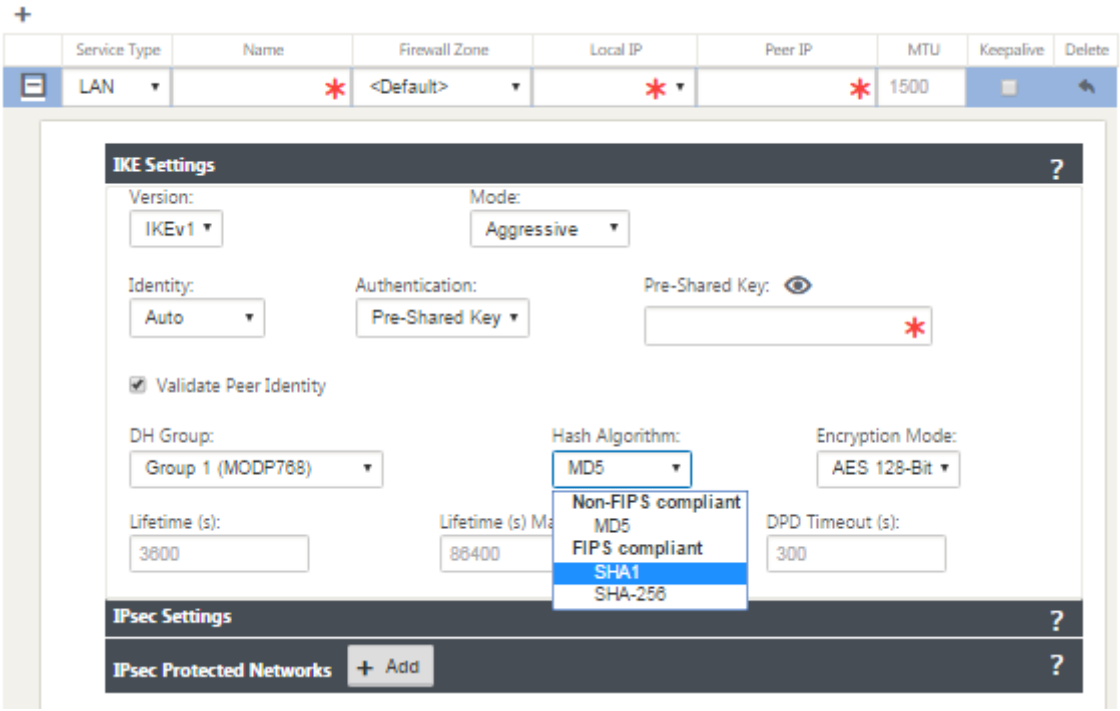


2. Vaya a **Conexiones** > **Túneles IPSec**. Con el túnel **LAN** o **Intranet** seleccionado, la pantalla distingue los grupos compatibles con FIPS en la configuración IKE de los que no son compatibles, de modo que puede configurar fácilmente el cumplimiento FIPS.

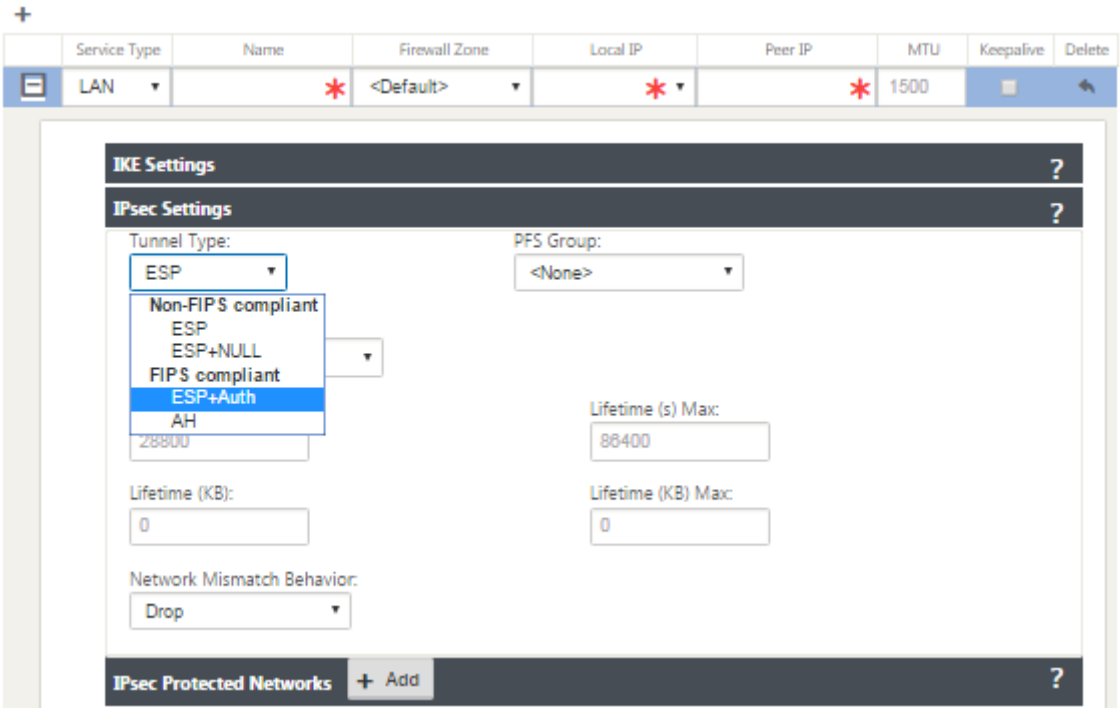


La pantalla también indica si el algoritmo hash es compatible con FIPS, como se muestra en la siguiente figura.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Opciones de cumplimiento de FIPS para la configuración de IPSec:



Si la configuración IPSec no cumple con los estándares FIPS cuando está habilitada, es posible que se desencadene un error de auditoría. A continuación se presentan el tipo de errores de auditoría que se muestran en la GUI.

- Cuando, el modo FIPS está habilitado y se selecciona la opción no compatible con FIPS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Cuando, el modo FIPS está habilitado y se introduce un valor de duración incorrecto.
- Cuando, el modo FIPS está habilitado y la configuración IPSec para la ruta virtual predeterminada también está habilitada, y se selecciona el modo túnel incorrecto (ESP vs ESP_Auth/AH).
- Cuando se habilita el modo FIPS, también se habilita la configuración IPSec para el conjunto predeterminado de ruta virtual y se introduce un valor de duración incorrecto.

Citrix SD-WAN Secure Web Gateway

May 7, 2021

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. Tal 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 omitan 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.Y si tiene muchas sucursales, la administración de costes se vuelve poco práctica.

- ¡Zscaler!

La solución ideal para imponer la seguridad sin agregar costes, complejidad ni latencia es redirigir todo el tráfico de Internet de la sucursal desde el dispositivo Citrix SD-WAN a la plataforma de seguridad de Zscaler Cloud. 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. Dado que la solución de seguridad de Zscaler está basada 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) elabora Normas Federales de Procesamiento de la Información (FIPS) en esferas 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

FIPS especifica los requisitos de seguridad para 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 redireccionamiento de firewall (proxy transparente por NAT de destino) para redirigir el tráfico de Internet (HTTP y HTTPS) desde un dispositivo SD-WAN en el borde de la empresa 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

October 27, 2021

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:

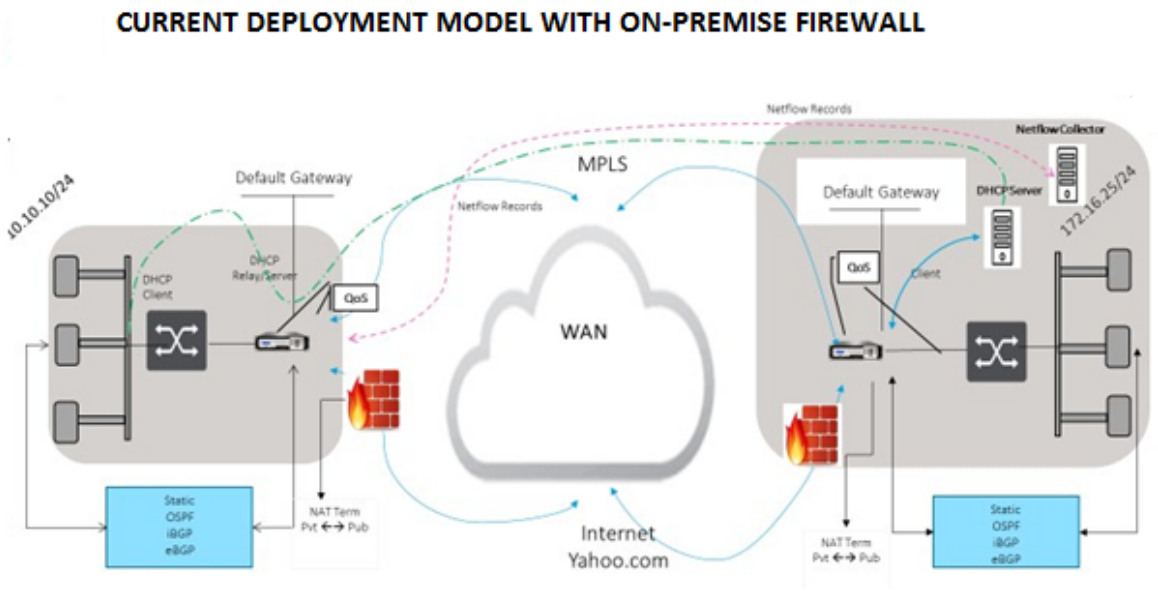
- Reenviar todo el tráfico GRE a Zscaler, lo que permite la ruptura directa de Internet.
- Acceso directo a Internet (DIA) mediante Zscaler en base a un sitio por cliente.
  - En algunos sitios, es posible que desee proporcionar a DIA equipo de seguridad local y no utilizar Zscaler.
  - En algunos sitios, 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.

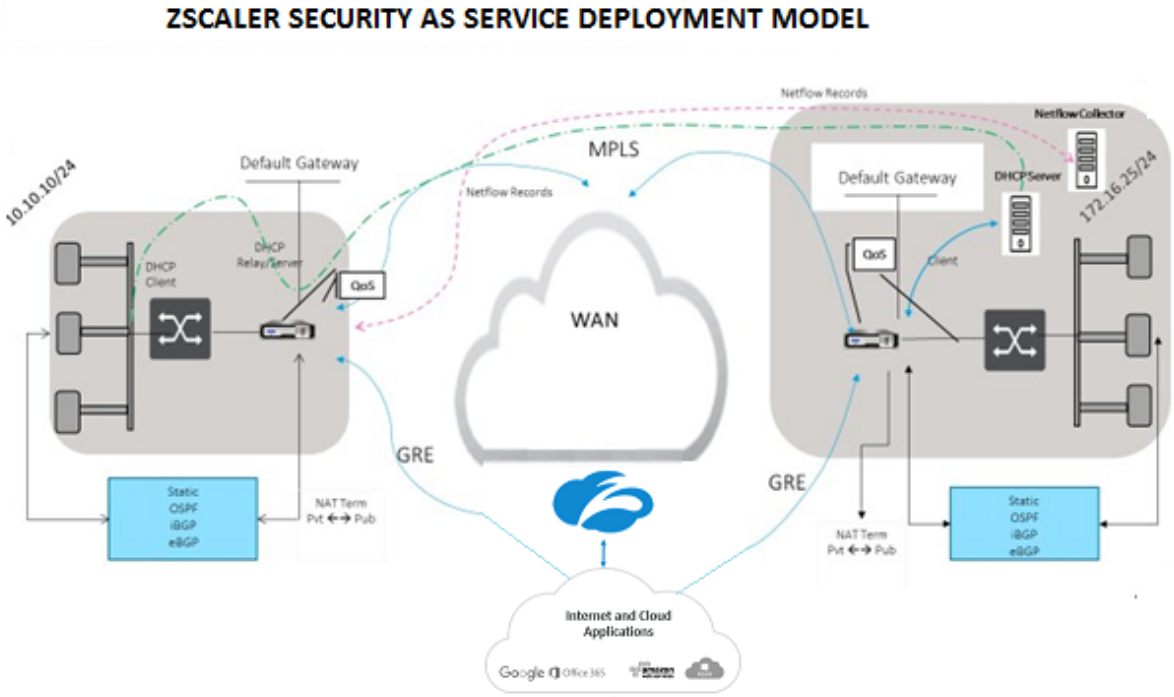
Zscaler es un servicio en la nube. Debe configurarlo como servicio y definir los vínculos WAN subyacentes:

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

1. Vaya a **Conexiones**- **Servicios de Internet**. Configure el servicio de internet.
2. Seleccione **+ Service** y habilite la configuración (configuración básica, vínculos WAN y reglas) según sea necesario.
3. Seleccione **Aplicar**.

Para obtener más información sobre cómo habilitar el servicio de Internet para un sitio, consulte Interrupción directa de Internet en una sucursal con firewall integrado.

Puede configurar los siguientes ajustes en un servicio de Internet:

- Parámetros básicos
- Enlaces WAN
- Reglas

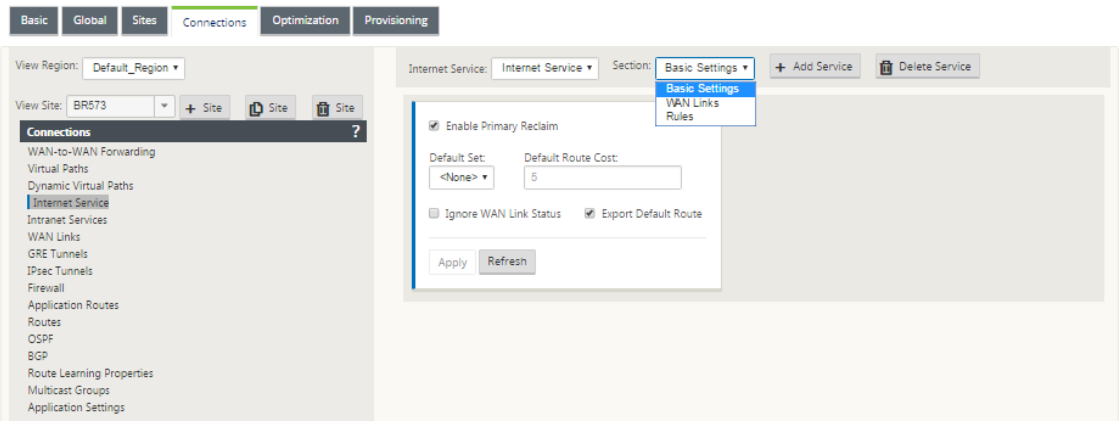
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetros básicos

La configuración de zona del firewall no se puede configurar para un servicio de Internet. Si el servicio Internet es de confianza, se asigna a **Internet_Zone**. Si el servicio Internet no es de confianza, se asigna a **Untrusted_Internet_Zone**.

Los ajustes básicos que se pueden configurar se describen a continuación:

- **Habilitar recuperación primaria**: si está habilitada, el uso (use = principal) asociado a este servicio en un enlace WAN recupera forzosamente el estado como servicio activo en ese enlace WAN.
- **Conjunto predeterminado**: Nombre del conjunto predeterminado de Internet que rellena las reglas del servicio Internet del sitio.
- Coste de**ruta predeterminado: coste**de ruta asociado a la ruta de Internet predeterminada (0.0.0.0/0).
- **Ignorar estado del enlace WAN**: si está habilitado, los paquetes destinados a este servicio seguirán eligiendo este servicio aunque no estén disponibles todos los enlaces WAN de este servicio.
- **Exportar ruta predeterminada**: si está habilitada, la ruta predeterminada del servicio de Internet, 0.0.0.0/0, se exporta a otros sitios si el reenvío de WAN a WAN está habilitado.



Enlaces WAN

La configuración del enlace WAN configurable se describe a continuación:

- **Uso**: Permitir que el servicio utilice este enlace WAN. Cuando Usar está inhabilitado, el resto de opciones no están disponibles.
- **Modo**: Modo de servicio: primario, secundario o equilibrado, para redundancia de tráfico o equilibrio de carga.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

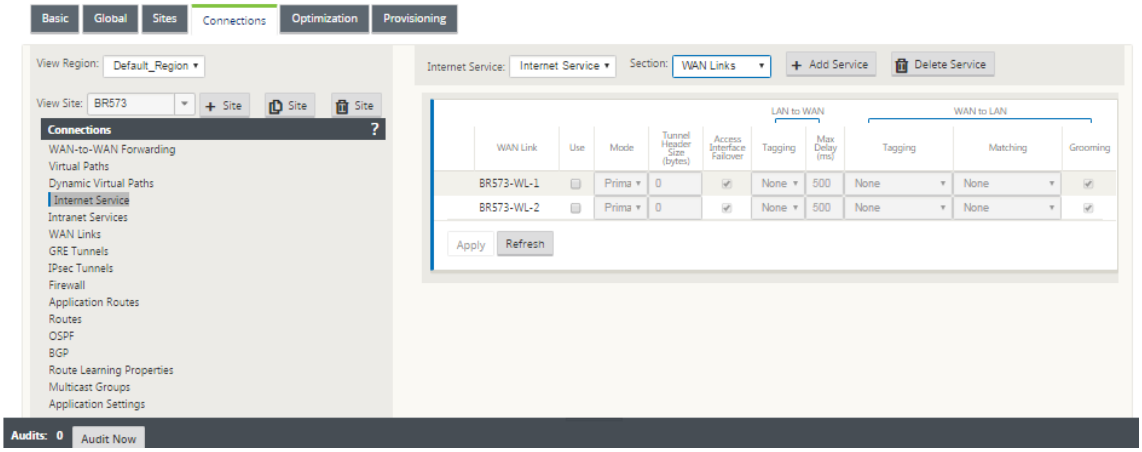
- **Tamaño del encabezado del túnel (bytes)**: tamaño del encabezado del túnel, en bytes, si procede.
- **Conmutación por error de interfaz de acceso**: si está habilitada, los paquetes de Internet o de intranet con VLAN no coincidentes pueden seguir utilizando el servicio.

LAN a WAN

- **Etiquetado**: etiqueta DSCP que se aplica a los paquetes LAN a WAN del servicio.
- **Demora máxima (ms)**: tiempo máximo, en milisegundos, para almacenar paquetes en búfer cuando se supera el ancho de banda de los enlaces WAN.

WAN a LAN

- **Etiquetado**: etiqueta DSCP que se aplica a los paquetes WAN a LAN del servicio.
- **Coincidencia**: los paquetes de Internet WAN a LAN que coinciden con esta etiqueta se asignan al servicio.
- **Grooming**: Si se habilita, los paquetes se descartan aleatoriamente para evitar que el tráfico de WAN a LAN exceda el ancho de banda aprovisionado del servicio.



Reglas

El tráfico de Internet se identifica según las reglas definidas. Se utiliza una definición de regla para hacer coincidir un flujo de tráfico específico. Una vez coincidente, debe definir la acción que se aplicará al flujo de tráfico.

La lista de reglas disponibles se describe a continuación:

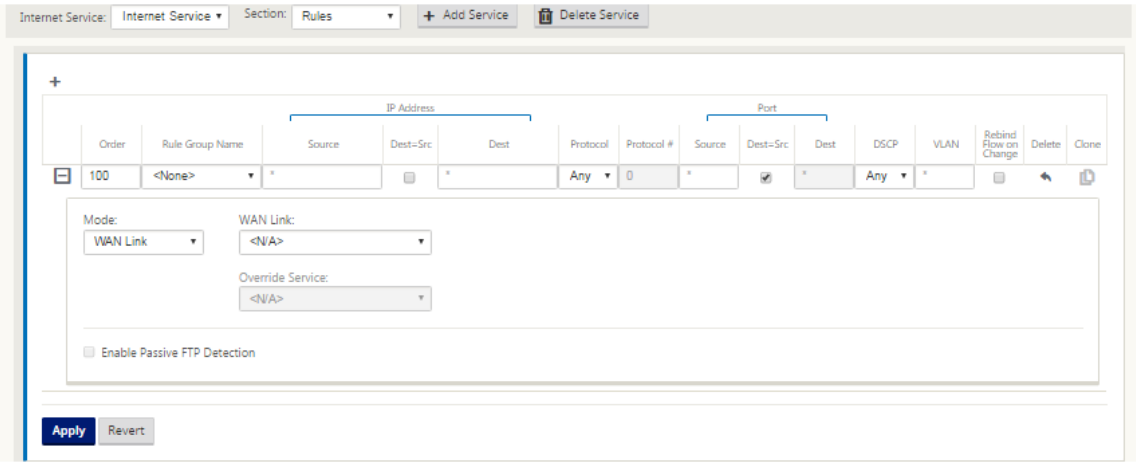
- **Orden**: secuencia en la que se aplican las reglas y se redistribuyen automáticamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nombre del grupo de reglas**: Nombre dado a una regla que permite sumar las estadísticas de reglas en grupos cuando se muestran. Todas las estadísticas de las reglas con el mismo nombre de grupo de reglas se pueden ver juntas.
- **Origen**: dirección IP de origen y máscara de subred que coinciden con la regla.
- **Dest-Src**: Si está habilitada, la dirección IP de origen también se utiliza como dirección IP de destino.
- **Dest**: La dirección IP de destino y la máscara de subred que coinciden con la regla.
- **Protocolo**: nombre del protocolo que coincide con el filtro.
- **Número de protocolo**: número de protocolo que coincide con el filtro.
- **DSCP**: etiqueta DSCP del encabezado IP que coincide con la regla.

La lista de acciones disponibles se describe a continuación:

- **Enlace WAN**: vínculo WAN que utilizarán los flujos que coinciden con la regla cuando el equilibrio de carga de Internet está habilitado.
- **Servicio de anulación**: el servicio de destino de los flujos que coinciden con la regla.
  - **Descartar**: Deja el tráfico.
  - **Passthrough**: asigne el flujo al paso y permita que el tráfico fluya por el dispositivo sin cambios.

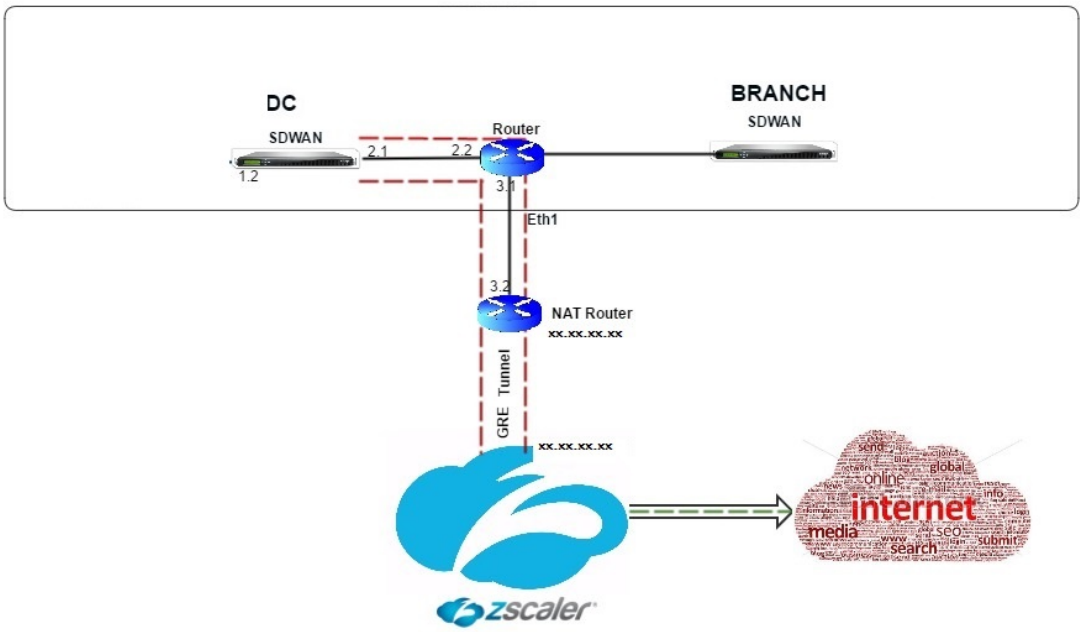


Configurar túnel GRE

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

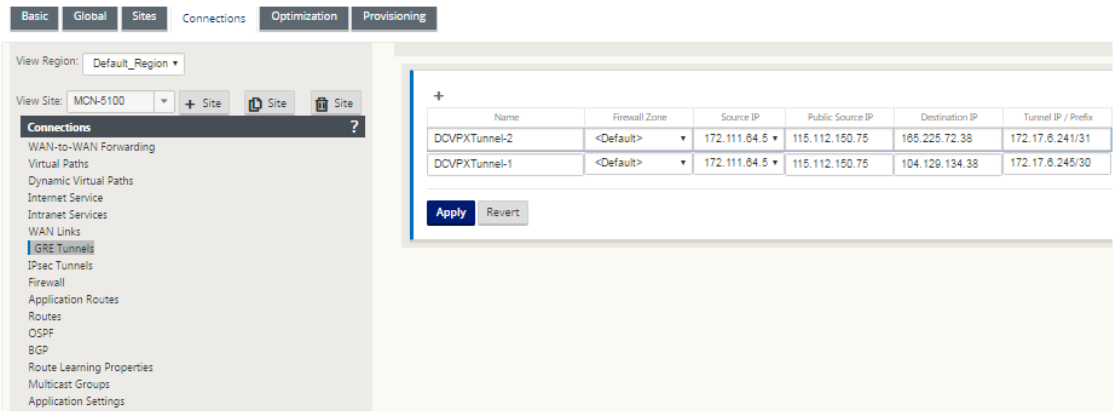
3. La dirección IP de origen y la dirección IP de destino son los encabezados GRE del router cuando se encapsula la carga útil original.
4. La dirección IP del túnel y el prefijo son las direcciones IP del propio túnel GRE. Esto resulta útil para redirigir el tráfico a través del túnel GRE. El tráfico necesita esta dirección IP como dirección de puerta de enlace.



Para configurar el túnel GRE:

1. En el editor de configuración, vaya a **Conexiones** > **Sitio** > **Túneles GRE**y configure rutas para reenviar los servicios de prefijos de Internet a los túneles GRE de Zscaler.

   La dirección IP de origen se puede elegir de la interfaz de red virtual en vínculos de confianza. Consulte Cómo configurar el túnel GRE.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

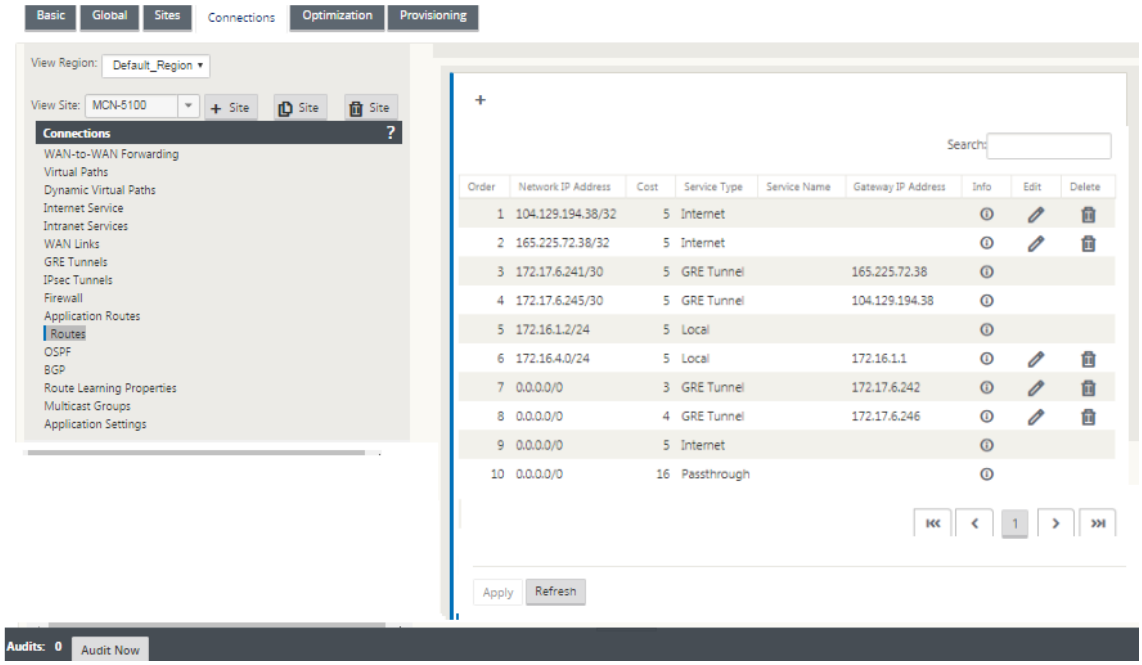
Configurar rutas para túneles GRE

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.

Para configurar rutas para el túnel GRE:

1. Vaya a **Conexiones** > **Sitio** > **Rutas**y siga los procedimientos descritos en Configuración de rutas para obtener instrucciones sobre cómo crear rutas.



> **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 desea, configure

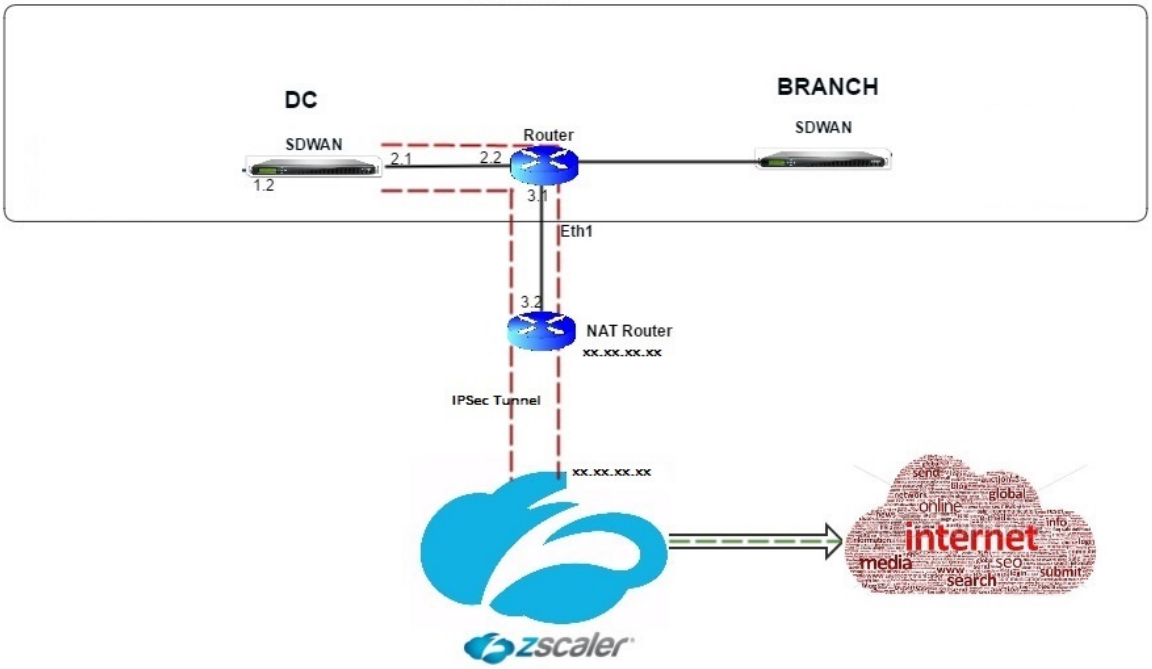
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

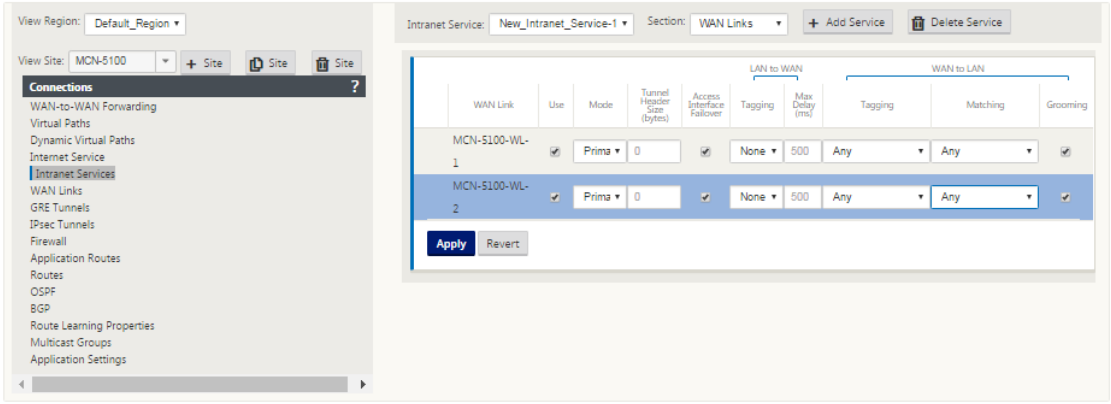
Configurar túneles IPsec

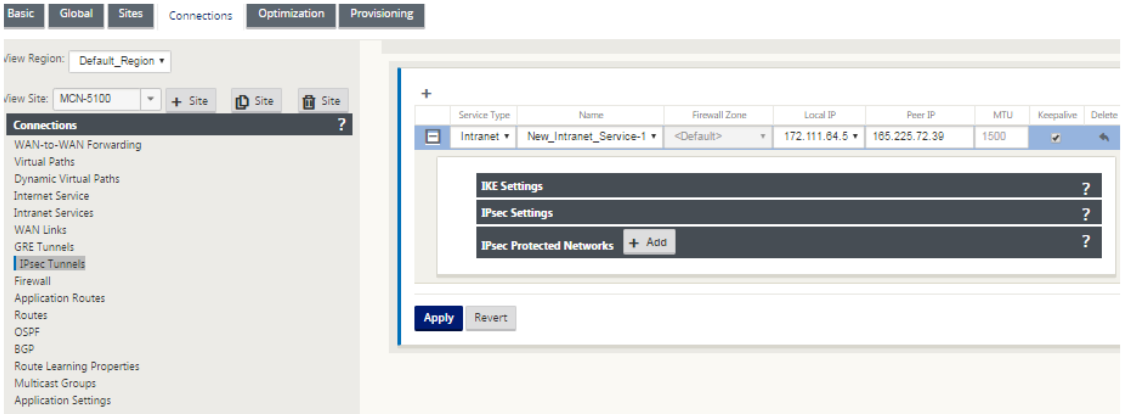


Para configurar túneles IPsec para servicios de intranet o LAN en la GUI del dispositivo Citrix SD-WAN:

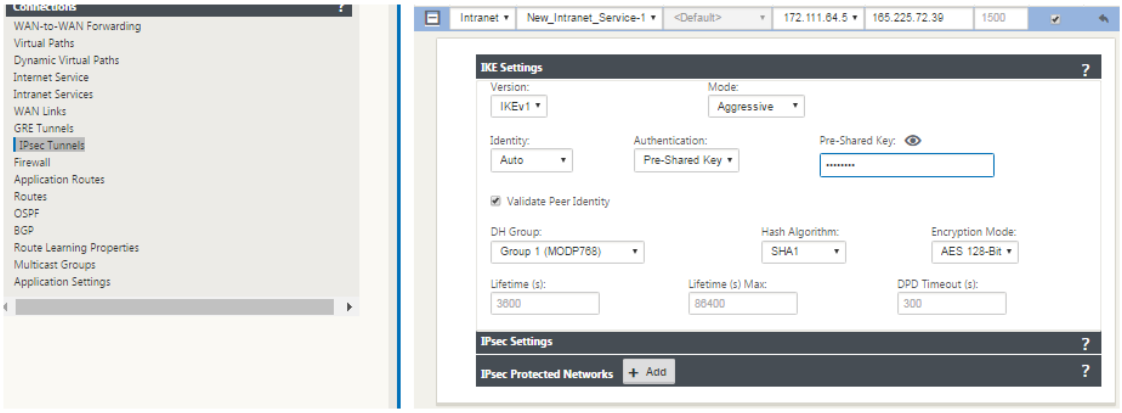
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el Editor de configuración, vaya a **Conexiones** > <**Nombre del sitio**> > **Túneles IPsec** y elija un tipo de servicio (LAN o Intranet).
2. Introduzca un nombre para el tipo de servicio. Para el tipo de servicio de intranet, el servidor de intranet configurado determina qué direcciones IP locales están disponibles.
3. Seleccione la dirección IP local disponible e introduzca la dirección IP del mismo nivel para la ruta virtual al par remoto.





4. Seleccione **IKEv1** para **Configuración de IKE**. Zscaler solo admite IKEv1.

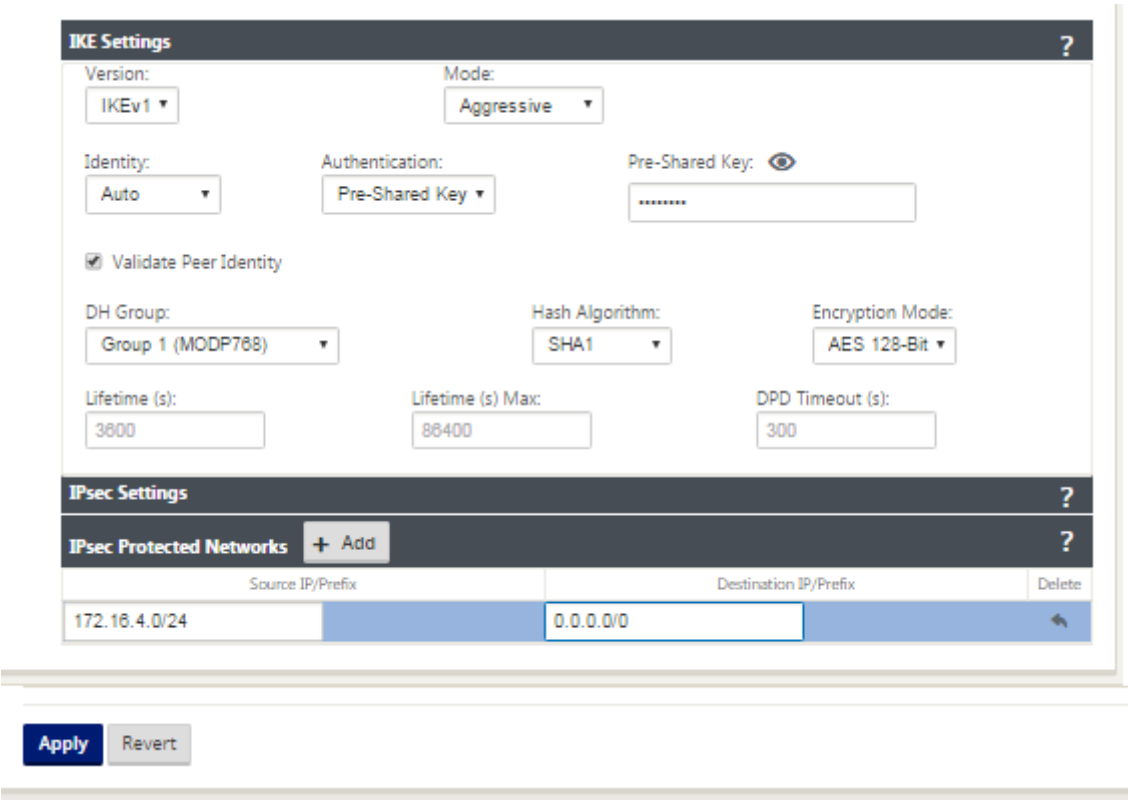


5. En Configuración de IPsec, seleccione **ESP-NULL** para **Tipo de túnel**para redirigir el tráfico a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zscaler a través del túnel IPsec. El túnel IPsec no cifra el tráfico.

6. Debido a que el tráfico de Internet se redirige, la IP/prefijo de destino puede ser cualquier dirección IP.



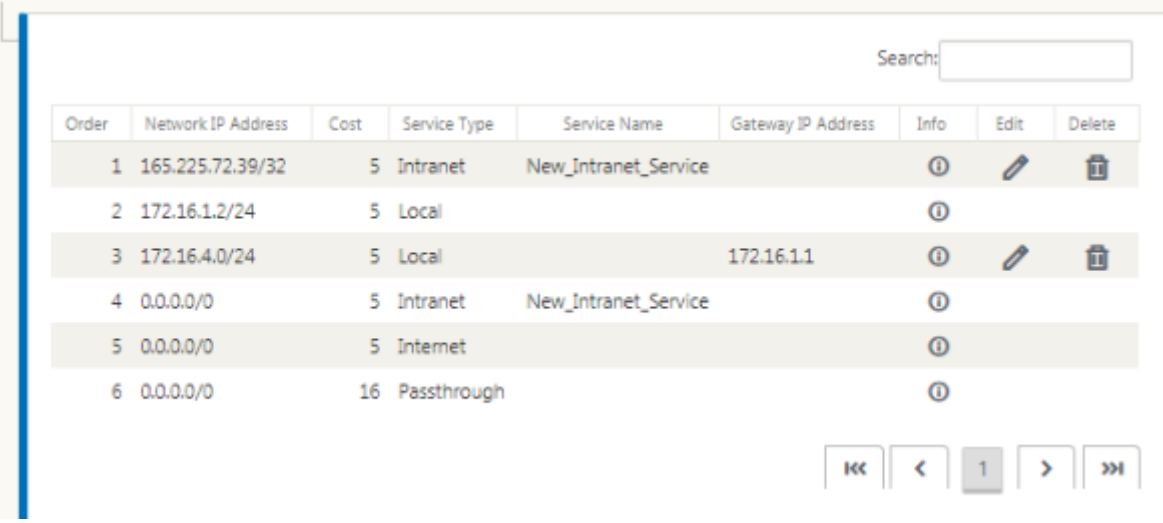
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para obtener más información sobre la configuración de túneles IPsec mediante la interfaz web de Citrix SD-WAN, consulte; el tema Túneles IPsec.

Configurar rutas para túneles IPsec

Para configurar rutas IPsec:

1. Vaya a **Conexiones** > **DC** > **Rutas** y siga los procedimientos descritos en Configuración de rutas para obtener instrucciones sobre cómo crear rutas.



Search:

Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	165.225.72.39/32	5	Intranet	New_Intranet_Service				
2	172.16.1.2/24	5	Local					
3	172.16.4.0/24	5	Local		172.16.1.1			
4	0.0.0.0/0	5	Intranet	New_Intranet_Service				
5	0.0.0.0/0	5	Internet					
6	0.0.0.0/0	16	Passthrough					

1

Para supervisar las estadísticas del túnel 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

May 7, 2021

Forcepoint admite las siguientes funciones, aunque SD-WAN solo admite la función de redirección del firewall:

- IPsec con PKI

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- IPsec con PSK
- Encadenamiento de proxy mediante la configuración del archivo PAC
- Encadenado de proxy con encabezados estándar
- Encadenamiento de proxy con encabezados propietarios que eliminan la necesidad de configurar el rango IP del cliente: Asociación/desarrollo
- Redirección de firewall (proxy transparente por NAT de destino)

La directiva NAT de destino permite a las empresas enrutar el tráfico de Internet a través del servicio de seguridad alojado en la nube mediante ForcePoint.

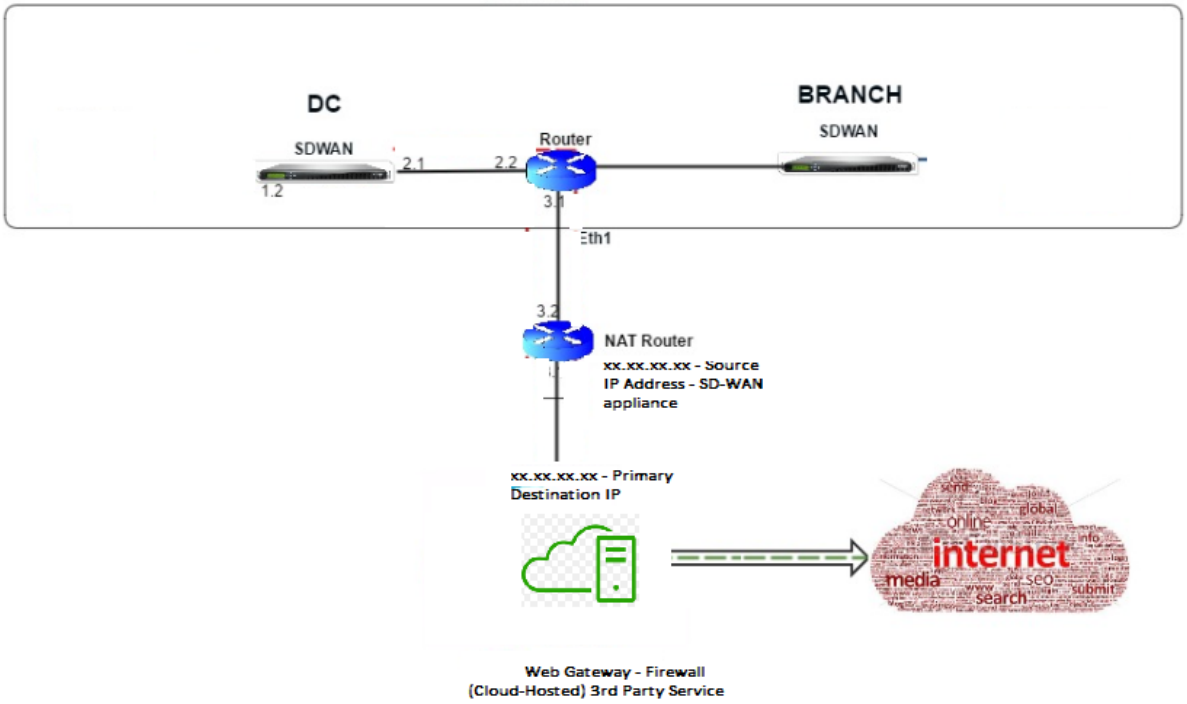
Revise el siguiente caso de uso para comprender cómo configurar NAT de destino en dispositivos SD-WAN y redirigir el tráfico de Internet a través de un servicio de firewall seguro basado en la nube.

Requisitos previos:

1. Inicie sesión en elSitio del portal 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 principales y secundarias a las que se debe redirigir el tráfico de Internet.
2. En la GUI de SD-WAN, en un dispositivo SD-WAN en el sitio de DC, configure el servicio de Internet asociado con enlaces WAN.
3. 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 Gateway 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.

Para obtener información adicional acerca de la compatibilidad con NAT en Citrix SD-WAN, consulte el tema siguiente:Configurar NAT

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración de NAT de destino (DNAT)

Utilice la GUI de Citrix SD-WAN para configurar NAT de destino (DNAT). En la configuración, agregue una o más directivas DNAT que redirijan el tráfico que coincida con una dirección IP de destino y un puerto específicos.

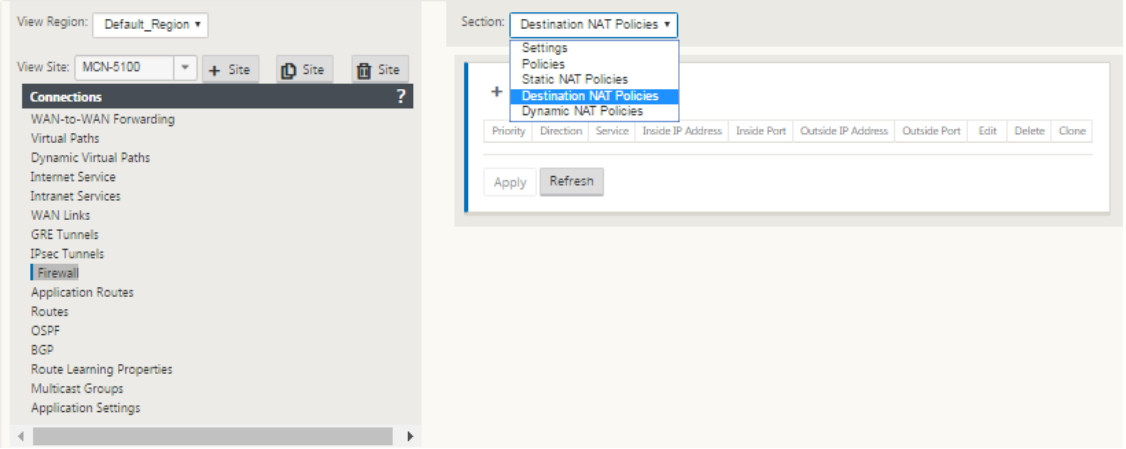
Para configurar NAT de destino:

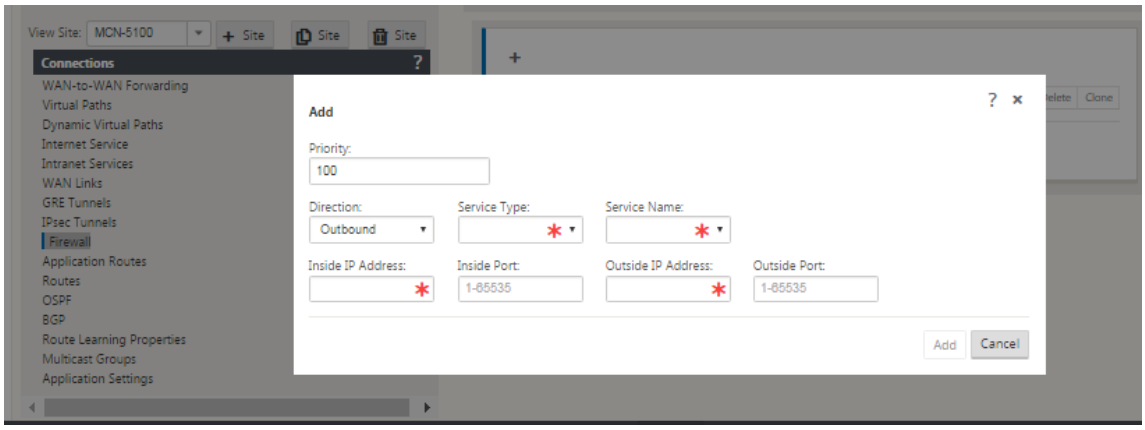
En la GUI de SD-WAN SE/VPX, vaya a **Configuración** -> **Virtual WAN** -> Configuration Editor. Haga clic en **Abrir** para abrir un paquete existente. Seleccione un paquete de configuración guardado. También puede crear reglas DNAT mientras crea la configuración de red.

1. En el DC (MCN), configure el servicio de Internet. Vaya a **Conexiones** -> **Firewall**.
2. Haga clic en **+ Agregar** para agregar una directiva DNAT.
3. En el cuadro de diálogo **Agregar directiva de NAT de destino**, proporcione la siguiente información:
    - Prioridad
    - Dirección
    - Tipo de servicio
    - Nombre del servicio
    - Dirección IP interna
    - Puerto interior

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Dirección IP externa
- Puerto exterior





4. Aprovisione reglas NAT de destino para redirigir tráfico de Firewall, similar a NAT estático.
5. Introduzca los criterios coincidentes y la IP de destino /puerto en los que se va a utilizar NAT.
6. Realice la coincidencia de conexión de la regla DNAT con las estadísticas.
7. Quitar o actualizar las reglas DNAT durante la actualización de la configuración.

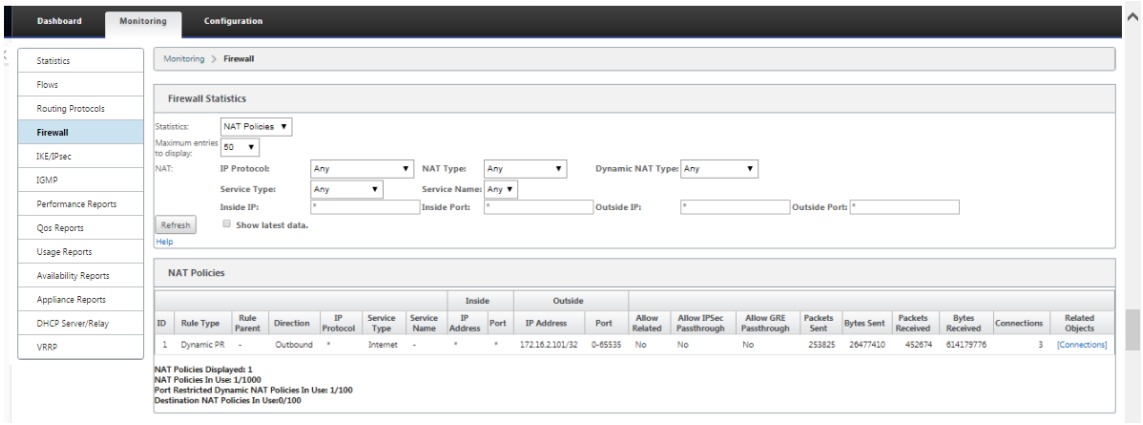
Supervisión de una directiva NAT de destino (Firewall)

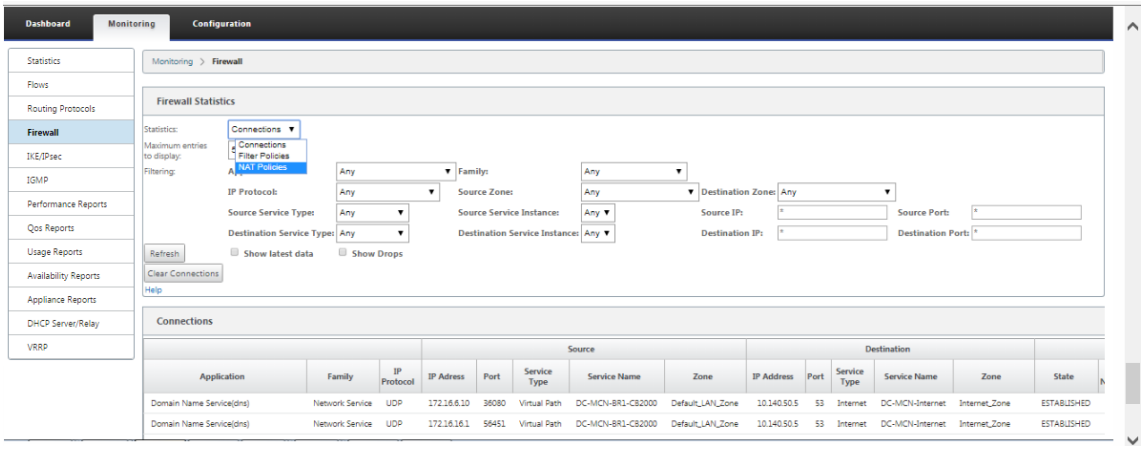
También puede utilizar la GUI de Citrix SD-WAN para supervisar la configuración actual de directivas DNAT.

Para supervisar la configuración actual de la directiva NAT de destino:

1. En la GUI de Citrix SD-WAN, vaya a **Monitoring** > **Firewall** > **NAT Policies**.
2. Seleccione la ficha que incluye las estadísticas que quiere supervisar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





Integración de Palo Alto mediante túneles IPSec

May 7, 2021

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.

El servicio Prisma Access también le permite administrar las directivas de forma centralizada desde Panorama para lograr una seguridad uniforme y optimizada para sus ubicaciones de red remotas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para conectar sus ubicaciones de red remotas al servicio Prisma Access, puede usar el firewall de última generación de Palo Alto Networks o un dispositivo compatible con IPsec de terceros, incluido SD-WAN, que puede establecer un túnel IPsec para el servicio.

- Planificar el servicio Prisma Access para redes remotas
- Configurar el servicio Prisma Access para redes remotas
- Redes remotas integradas con importación de configuración

La solución Citrix SD-WAN ya ofrecía la capacidad de eliminar el tráfico de Internet de la sucursal. Esto es fundamental para ofrecer una experiencia de usuario más confiable y de baja latencia, evitando al mismo tiempo la introducción de una costosa pila de seguridad en cada sucursal. Citrix SD-WAN y Palo Alto Networks ahora ofrecen a las empresas distribuidas una forma más confiable y segura de conectar a los usuarios de sucursales 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. Puede configurar la red Palo Alto en Citrix SD-WAN Center.

Antes de comenzar a configurar el servicio de acceso de Prisma para redes remotas, mantenga lista la siguiente configuración para asegurarse de que puede habilitar correctamente el servicio y aplicar la directiva a los usuarios de las ubicaciones de red remotas:

1. **Conexión de servicio**: Si sus ubicaciones de red remotas requieren acceso a la infraestructura de su sede corporativa para autenticar usuarios o para habilitar el acceso a activos de red críticos, debe configurar el acceso a su red corporativa para que las oficinas centrales y las ubicaciones de red remotas sean conectado.

Si la ubicación de red remota es autónoma y no necesita acceder a la infraestructura en otras ubicaciones, no es necesario configurar la conexión de servicio (a menos que los usuarios móviles necesiten acceso).

1. **Plantilla**: El servicio Prisma Access crea automáticamente una pila de plantillas (Remote_Network_Template_Stack) y una plantilla de nivel superior (Remote_Network_Template) para el servicio Prisma Access para redes remotas.

   Para configurar el servicio de acceso de Prisma para redes remotas, configure la plantilla de nivel superior desde cero o aproveche la configuración existente, si ya está ejecutando un firewall de Palo Alto Networks local.

   La plantilla requiere la configuración para establecer el túnel IPSec y la configuración de Intercambio de claves de Internet (IKE) para la negociación de protocolos entre la ubicación de red remota y el servicio Prisma Access para redes remotas, zonas a las que puede hacer referencia en la directiva de seguridad y un perfil de reenvío de registros para que puede reenviar registros desde el servicio Prisma Access para redes remotas al servicio de registro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. **Grupo de dispositivos principal**: el servicio Prisma Access para redes remotas requiere que especifique un grupo de dispositivos principal que incluya la directiva de seguridad, los perfiles de seguridad y otros objetos de directiva (como grupos de aplicaciones y objetos y grupos de direcciones), así como la directiva de autenticación, para que el servicio Prisma Access para redes remotas puede aplicar sistemáticamente directivas para el tráfico que se enruta a través del túnel IPSec al servicio Prisma Access para redes remotas. Debe definir reglas de directiva y objetos en Panorama o utilizar un grupo de dispositivos existente para proteger a los usuarios en la ubicación de red remota.

   > **Nota:**
   >
   > Si utiliza un grupo de dispositivos existente que hace referencia a zonas, asegúrese de agregar la plantilla correspondiente que define las zonas a Remote_Network_Template_Stack.

   Esto le permite completar la asignación de zonas al configurar Prisma Access Service for Remote Networks.

3. **Subredes IP**: para que el servicio Prisma Access enrute el tráfico a las redes remotas, debe proporcionar información de enrutamiento para las subredes que desea proteger mediante el servicio Prisma Access. Puede definir una ruta estática a cada subred en la ubicación de red remota o configurar BGP entre las ubicaciones de conexión de servicio y el servicio Prisma Access, o utilizar una combinación de ambos métodos.

   Si configura ambas rutas estáticas y habilita BGP, las rutas estáticas tienen prioridad. Si bien puede ser conveniente utilizar rutas estáticas si tiene solo unas pocas subredes en las ubicaciones de red remotas, en una implementación grande con muchas redes remotas con subredes superpuestas, BGP le permite escalar más fácilmente.

Red Palo Alto en SD-WAN Center

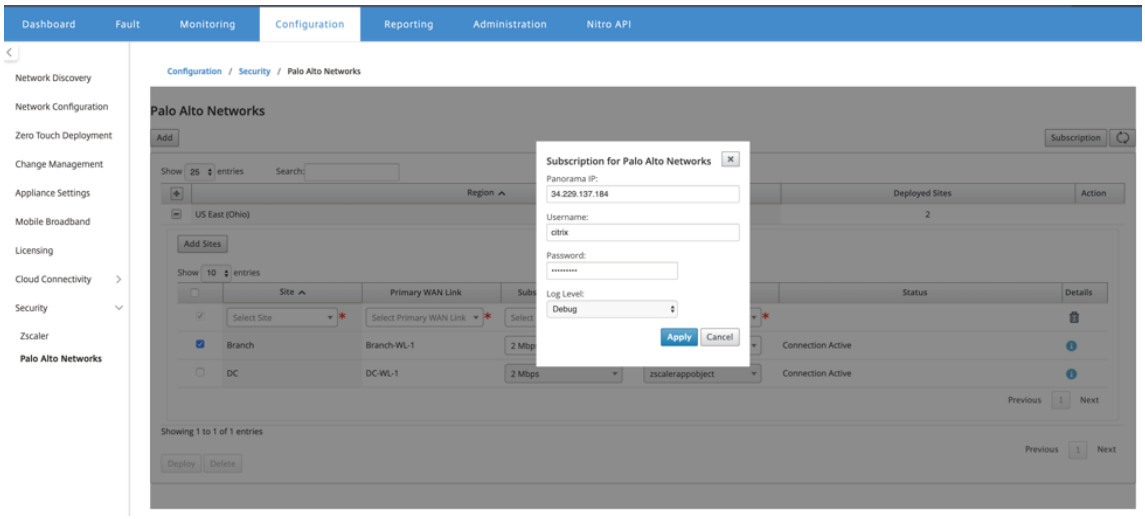
Asegúrese de que se cumplen los siguientes requisitos previos:

- Obtenga una dirección IP panorámica del servicio PRISMA ACCESS.
- Obtener nombre de usuario y contraseña de usuario en el servicio PRISMA ACCESS.
- Configure los túneles IPSec en la GUI del dispositivo SD-WAN.
- Asegúrese de que el sitio no está integrado en una Región, que ya tiene otro sitio configurado con perfiles IKE/IPSec distintos de Citrix-IKE-Crypto-Default/Citrix-IPsec-Crypto-Default.
- Asegúrese de que la configuración de Prisma Access no se cambie manualmente cuando SD-WAN Center actualice la configuración.

En la GUI de Citrix SD-WAN Center, proporcione información de suscripción a Palo Alto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configure la dirección IP panorámica. Puede obtener esta dirección IP de Palo Alto (servicio PRISMA ACCESS).
- Configure el nombre de usuario y la contraseña utilizados en el servicio PRISMA ACCESS.

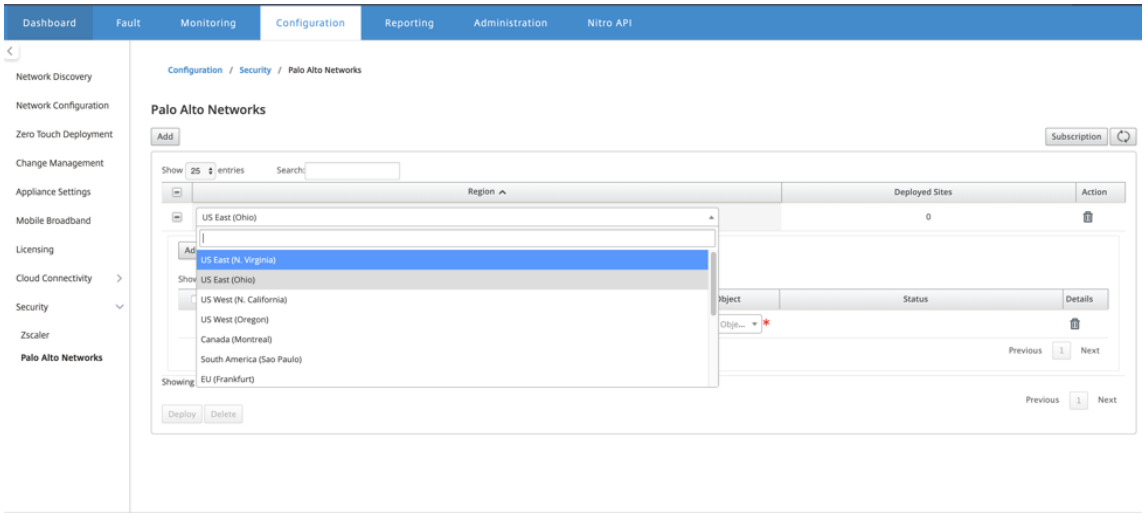


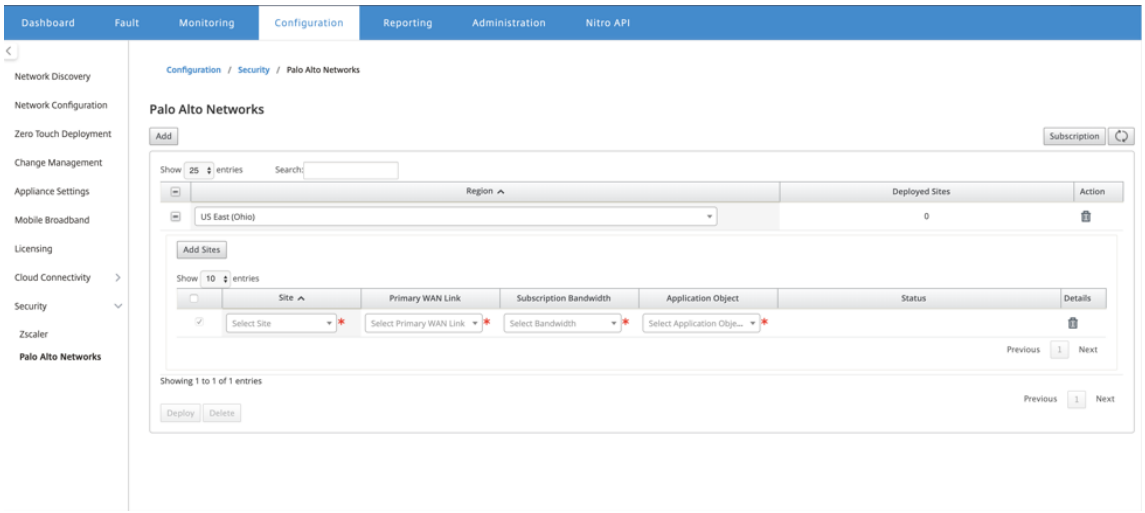
Agregar e implementar sitios

1. Para implementar los sitios, elija la región de red PRISMA ACCESS y el sitio SD-WAN que se configurará para la región Prisma Access y, a continuación, seleccione el enlace WAN del sitio, el ancho de banda y el objeto de aplicación para la selección del tráfico.

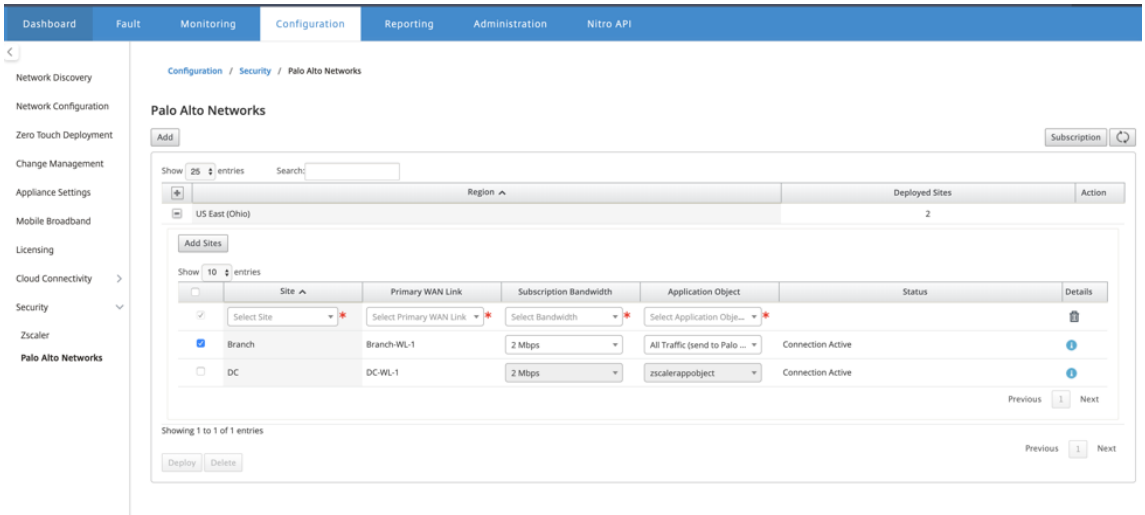
> **Nota:**
>
> El flujo de tráfico se ve afectado si el ancho de banda seleccionado supera el rango de ancho de banda disponible.
>
> Puede optar por redirigir todo el tráfico enlazado a Internet al servicio PRISMA ACCESS seleccionando la opción **Todo el tráfico** en la selección Objeto Aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





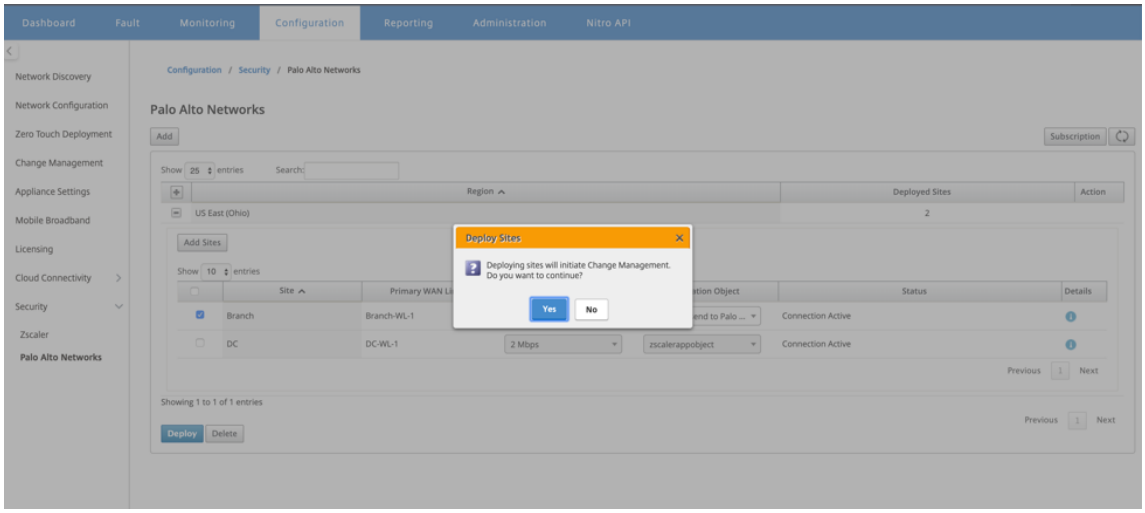
2. Puede continuar agregando más sitios de sucursales SD-WAN según sea necesario.



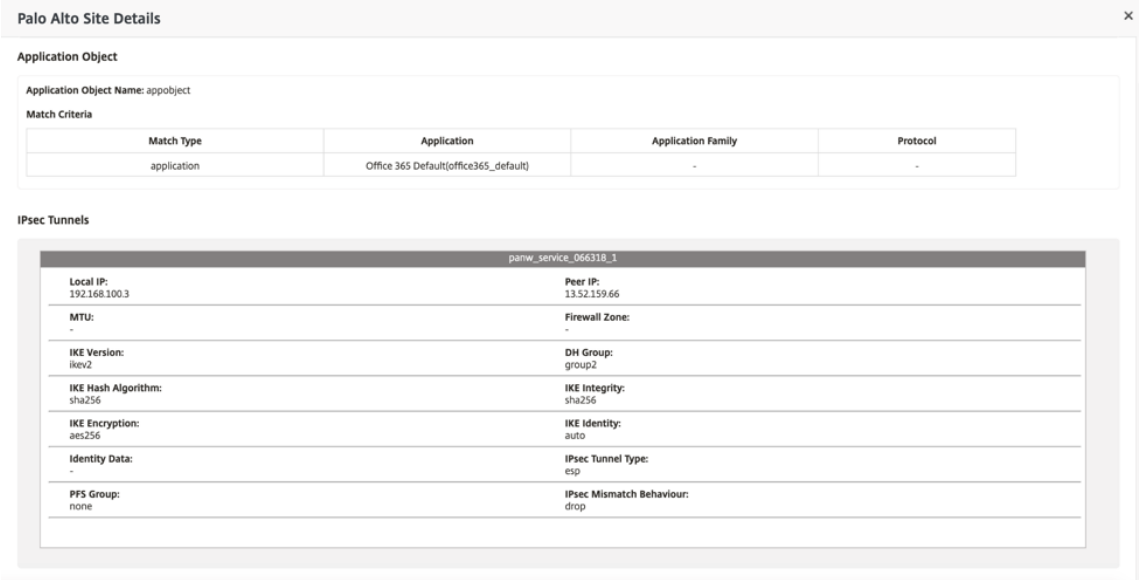
3. Haga clic en **Implementar**. Se inicia el proceso de gestión de cambios. Haga clic en **Sí** para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

continuar.

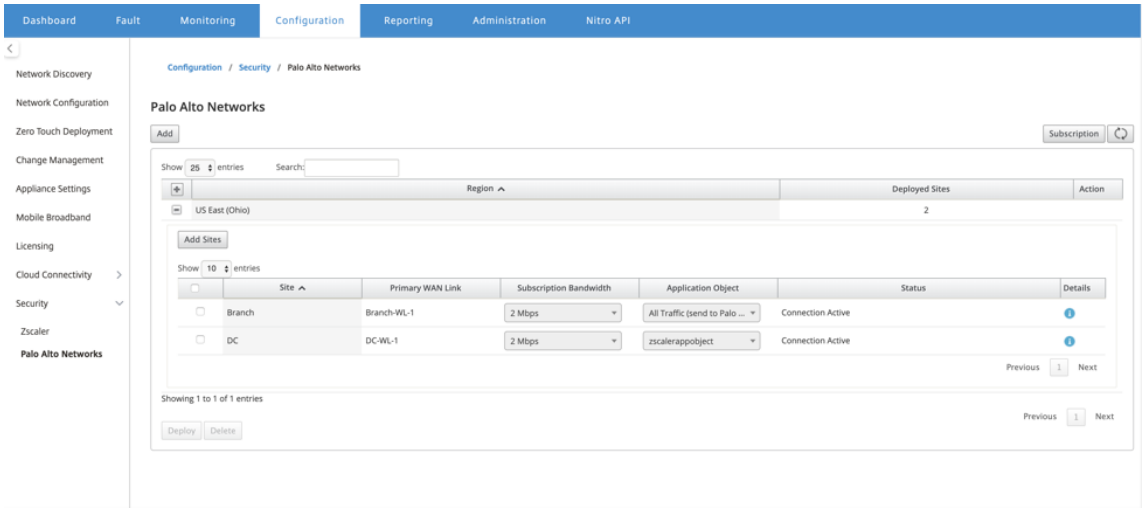


Después de la implementación, la configuración del túnel IPSec utilizada para establecer los túneles es la siguiente.



La página de destino muestra la lista de todos los sitios configurados y agrupados en diferentes regiones SD-WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Verificar la conexión de tráfico de extremo a extremo:

- Desde la subred LAN de una sucursal, acceda a los recursos de Internet.
- Compruebe que el tráfico pasa a través del túnel IPSec de Citrix SD-WAN hasta Palo Alto Prisma Access.
- Compruebe que la directiva de seguridad de Palo Alto se aplica al tráfico en la ficha Supervisión.
- Verifique que llegue la respuesta de Internet al host en una sucursal.

Integrar Citrix SD-WAN y la nube iboss

June 8, 2022

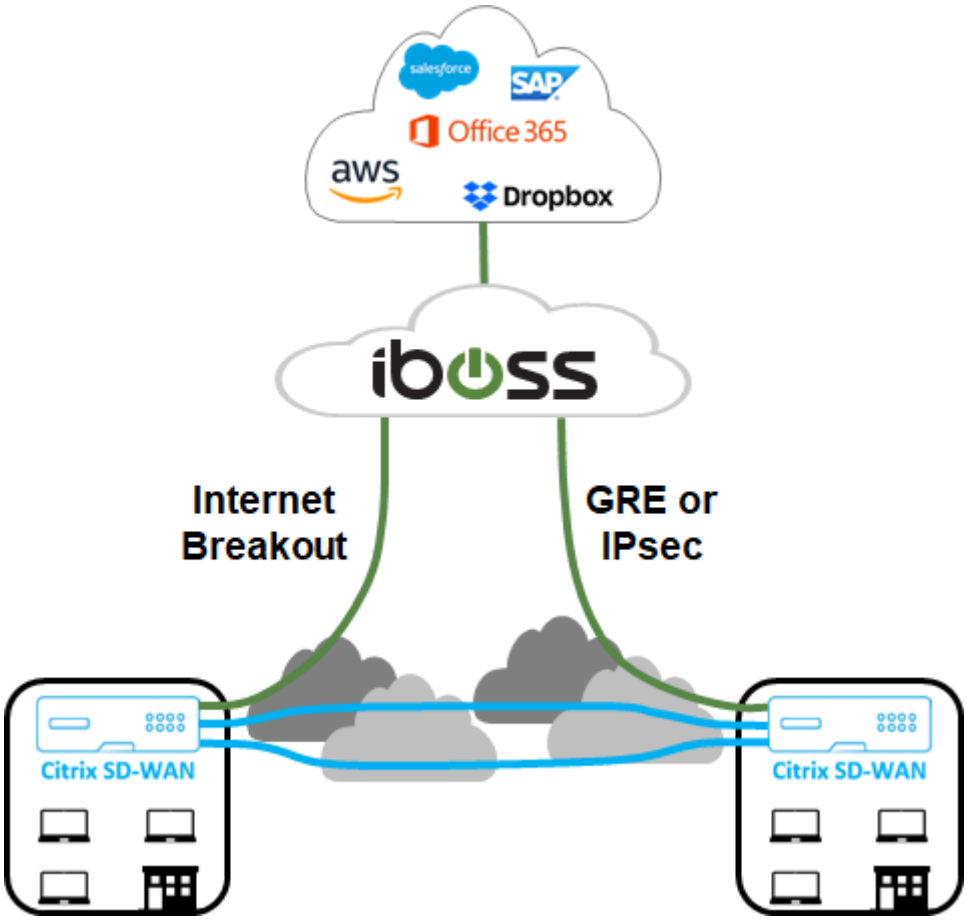
Citrix SD-WAN ayuda a las empresas a trasladarse a la nube al habilitar de forma segura las interrupciones locales de sucursal a Internet que pueden permitir o denegar el acceso a Internet directamente desde la sucursal. Citrix SD-WAN identifica aplicaciones mediante una combinación de una base de datos integrada de más de 4.500 aplicaciones, incluidas aplicaciones SaaS individuales, y utiliza tecnología de inspección profunda de paquetes para el descubrimiento y clasificación de aplicaciones en tiempo real. Utiliza este conocimiento de aplicaciones para dirigir de forma inteligente el tráfico de la sucursal a Internet, nube o SaaS.

iboss cloud asegura el acceso a Internet en cualquier dispositivo, desde cualquier ubicación, en la nube. iboss proporciona seguridad en la nube para sucursales donde el tráfico de Internet se descarga de conexiones de oficina privada a través de interrupciones de Internet. Los usuarios reciben la mejor protección de Internet que incluye cumplimiento normativo, filtrado web, inspección SSL, seguridad basada en archivos y secuencias, defensa contra malware y prevención de pérdida de datos. El tráfico

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

está protegido en la nube, con directivas de seguridad centralizadas en todas las sucursales y escalado instantáneo a medida que crece el ancho de banda.

La combinación de Citrix SD-WAN y iboss Cloud permite a las empresas transformar su WAN de forma segura. La arquitectura general de la solución se muestra en la siguiente figura.



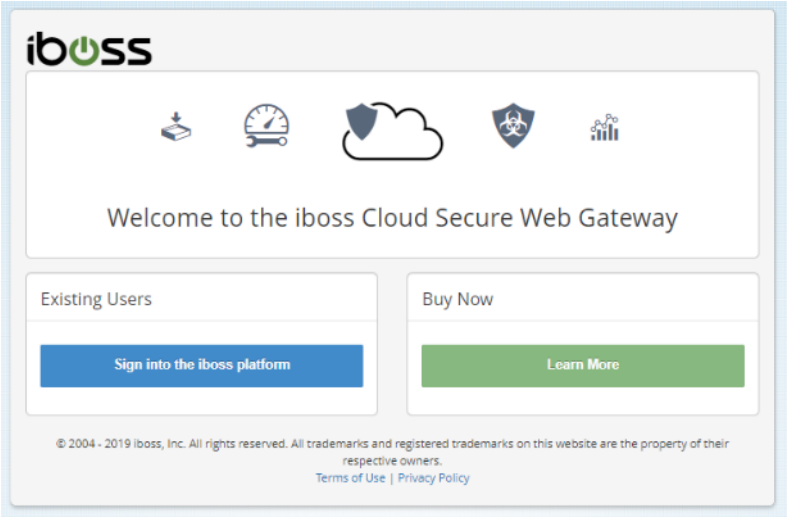
configuración de iboss

Inicio de sesión

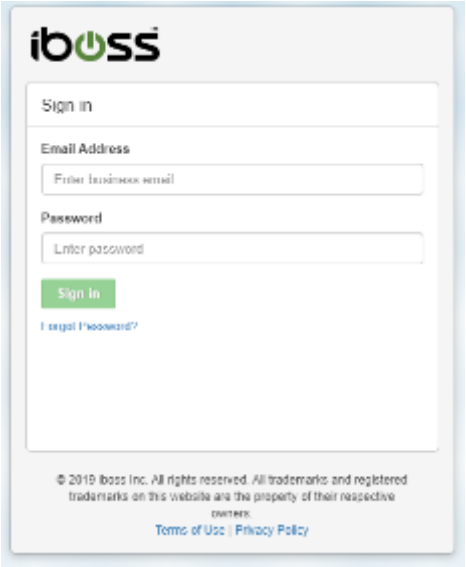
La configuración de iboss se aprovisiona a través de la interfaz gráfica de usuario del panel iboss.

Para iniciar sesión en la interfaz de administración, a través de un explorador de Internet navegue a www.ibosscloud.com.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



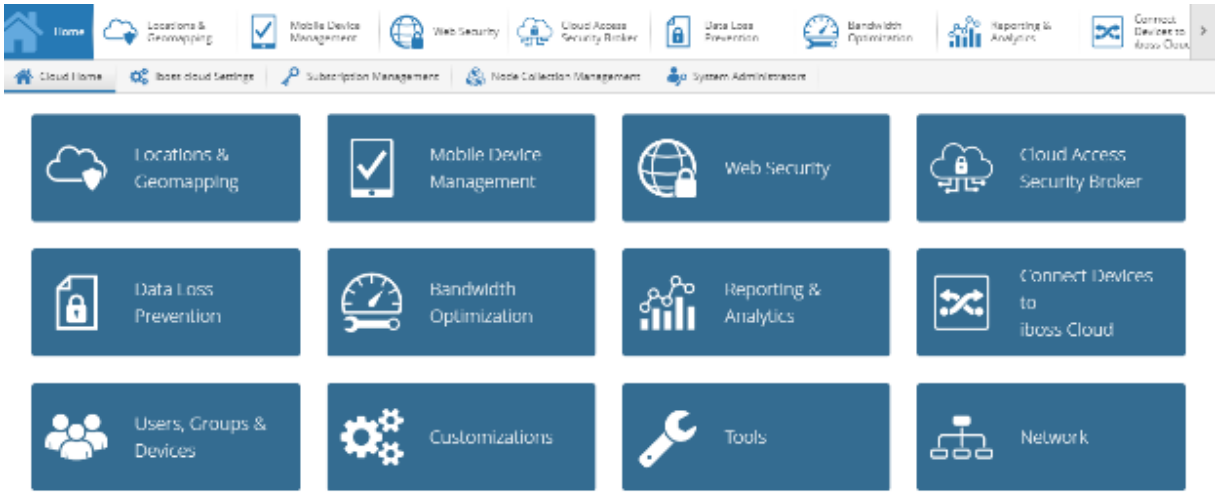
Haga clic **en Iniciar sesión en la plataforma iboss** y proporcione sus credenciales.



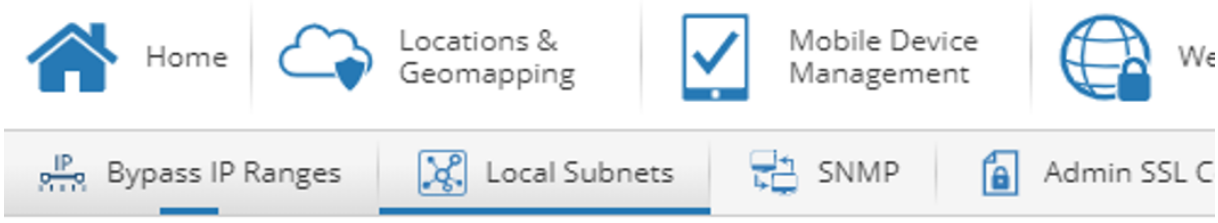
Subredes de red

Muchos clientes crean directivas para implementaciones de SD-WAN basadas en subredes de red de sucursales. Se recomienda agregar una subred abierta para cada rango privado utilizado en la red (por ejemplo 10.0.0.0/255.0.0.0) y, a continuación, crear subredes más específicas según sea necesario. Para crear una subred de red, seleccione el icono **Red** en la página principal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

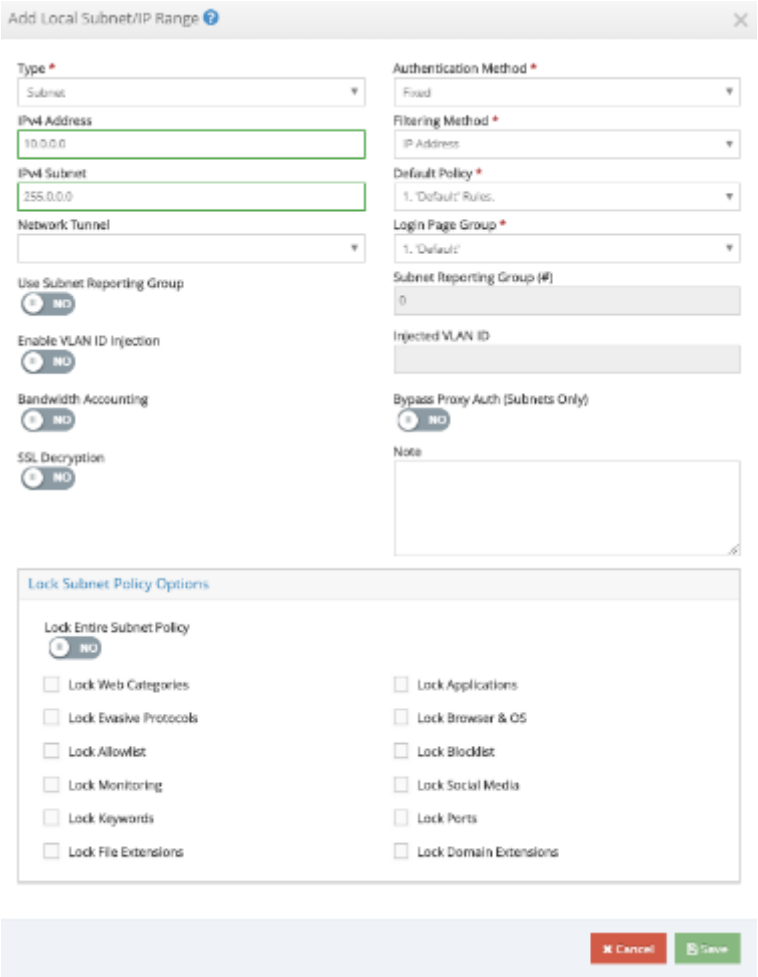


Desplácese hasta **Subredes Locales** > **+ Nueva subred local/Rango IP**.



Introduzca o seleccione valores para los campos obligatorios y haga clic en **Guardar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



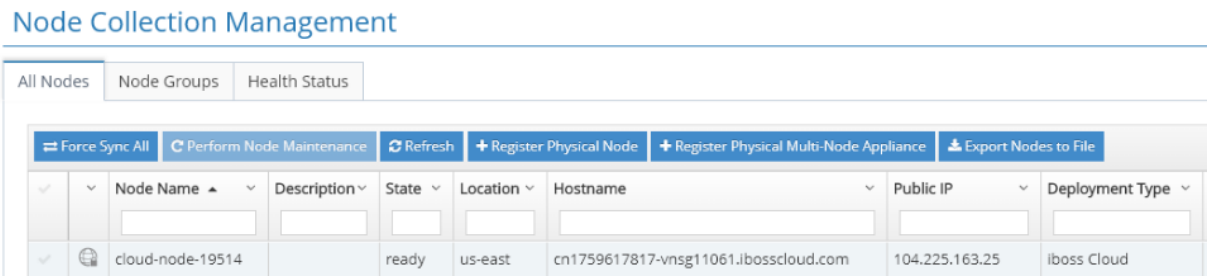
Túneles

Una vez aprovisionadas las subredes de red, se pueden utilizar túneles GRE o IPSec para conectar la sucursal a iboss Cloud si es necesario. Los siguientes pasos muestran cómo configurar un único túnel en un único nodo SWG iboss. Los pasos se pueden replicar para proporcionar varios túneles desde un solo dispositivo de sucursal o a varios nodos de Gateway iboss.

Los túneles GRE o IPSec de un dispositivo Citrix SD-WAN terminarán en la dirección IP pública de un nodo de Gateway iboss. Para identificar la dirección IP pública de un nodo de puerta de enlace iboss, vuelva a la página principal y haga clic en **Administración de colecciones de nodos**.

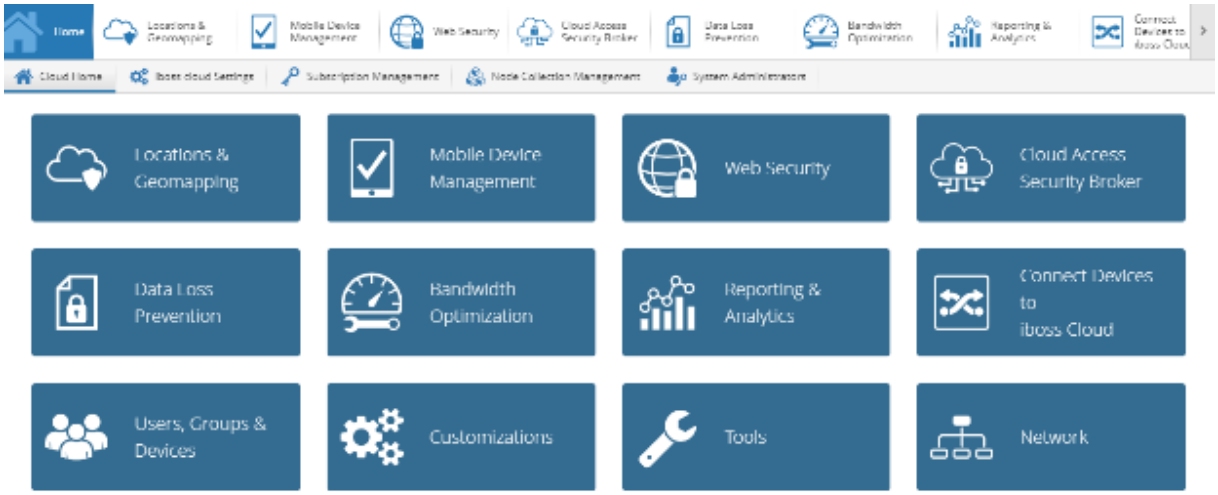
En la ficha **Todos los nodos**, la dirección **IP pública** de un nodo de puerta de enlace es la dirección IP externa del túnel. En el ejemplo siguiente, la IP externa de un túnel en el lado iboss sería 104.225.163.25.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

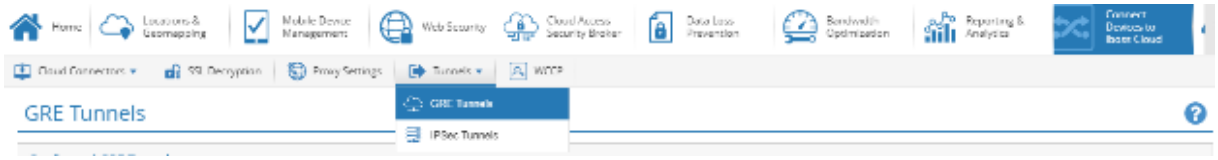


GRE

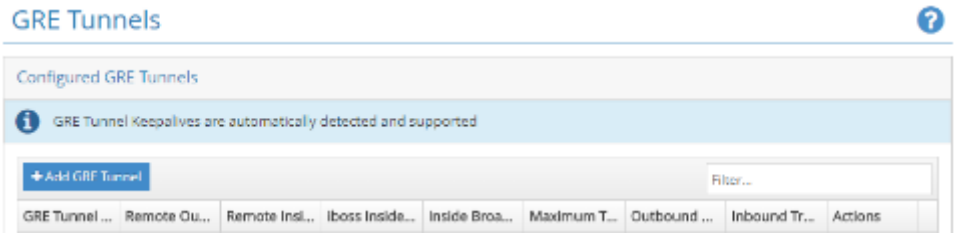
Para agregar un túnel GRE desde una ubicación específica, vuelva a la página de inicio y haga clic en **Conectar dispositivos a iboss Cloud**.



Haga clic en **Túneles** y seleccione **Túneles GRE**.



Haga clic en **+Añadir túnel GRE** e introduzca la información necesaria.

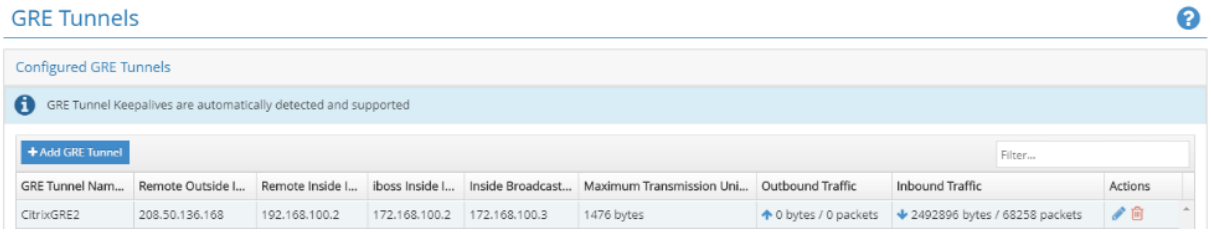


Las subredes de túnel interior deben ser únicas para cada túnel (por ejemplo, 169.254.1.0/30, 169.254.1.4/30, etc.). Los nodos iboss únicos deben utilizarse para subredes superpuestas entre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

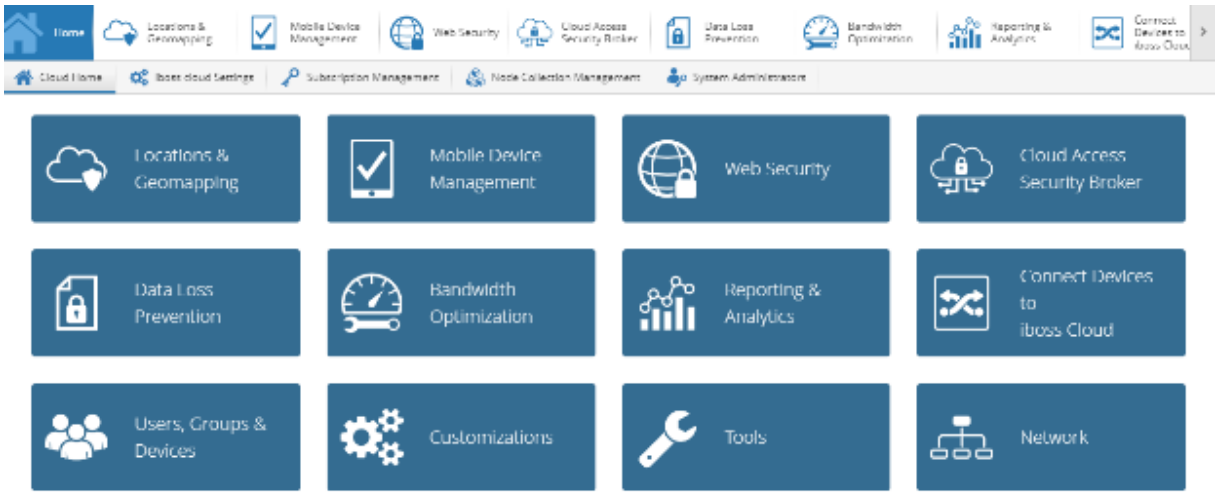
varios sitios. Por ejemplo, si el sitio 'A'y el sitio 'B'utilizan la subred 192.168.1.0/24, entonces la configuración del túnel GRE para cada uno de estos sitios debe realizarse en diferentes nodos iboss.

Haga clic en **Guardar**. La información del túnel se presenta como un resumen. Puede modificarlo si es necesario.

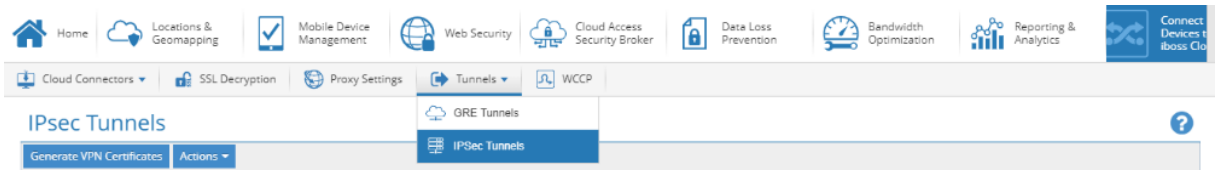


IPSec

Para agregar un túnel IPSec desde una ubicación específica, vuelva a la página principal y haga clic en **Conectar dispositivos a iboss Cloud**.



Haga clic en **Túneles** y seleccione **Túneles IPSec**.



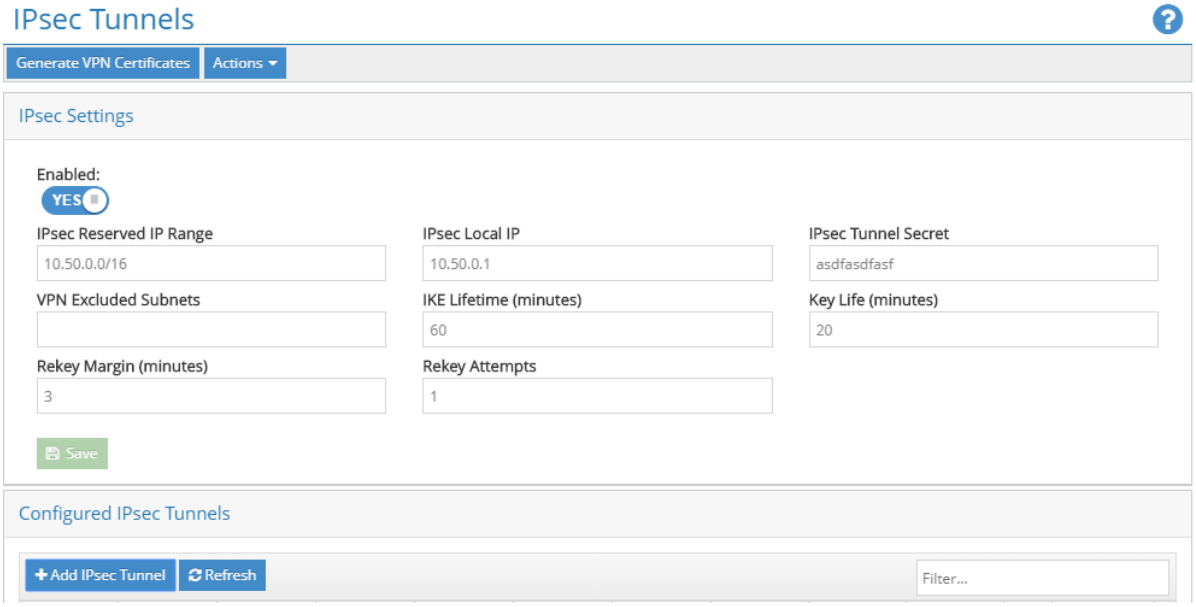
Cuando se conectan túneles desde un dispositivo Citrix SD-WAN, se recomienda la siguiente configuración de IPSec que es común en todos los túneles:

- IKE Vida útil (minutos): 60
- Vida útil de las teclas (minutos): 20

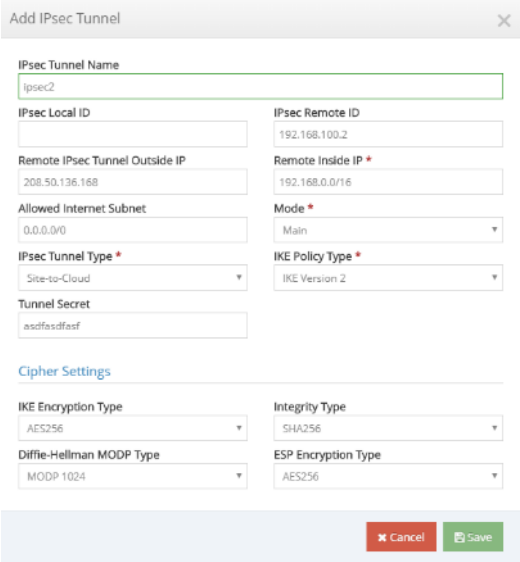
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Margen de reclave (minutos): 3
- Intentos de reclave: 1

Todas las demás configuraciones (por ejemplo, IPSec Tunnel Secret, etc.) pueden ser específicas de la implementación.



Haga clic en **+ Agregar túnel IPsec** para crear túneles según sea necesario.



Introduzca la información requerida. Para un túnel IPSec desde el dispositivo Citrix SD-WAN, recomendamos la siguiente configuración de IPsec para cada túnel:

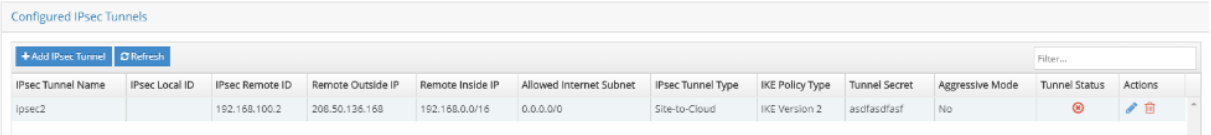
- Modo: Principal
- Tipo de túnel IPSec: de sitio a nube
- Tipo de directiva IKE: IKE versión 2

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Tipo de cifrado IKE: AES256
- Tipo de integridad: SHA256
- Diffie-Hellman MODP Tipo: MODP 1024
- Tipo de cifrado ESP: AES256

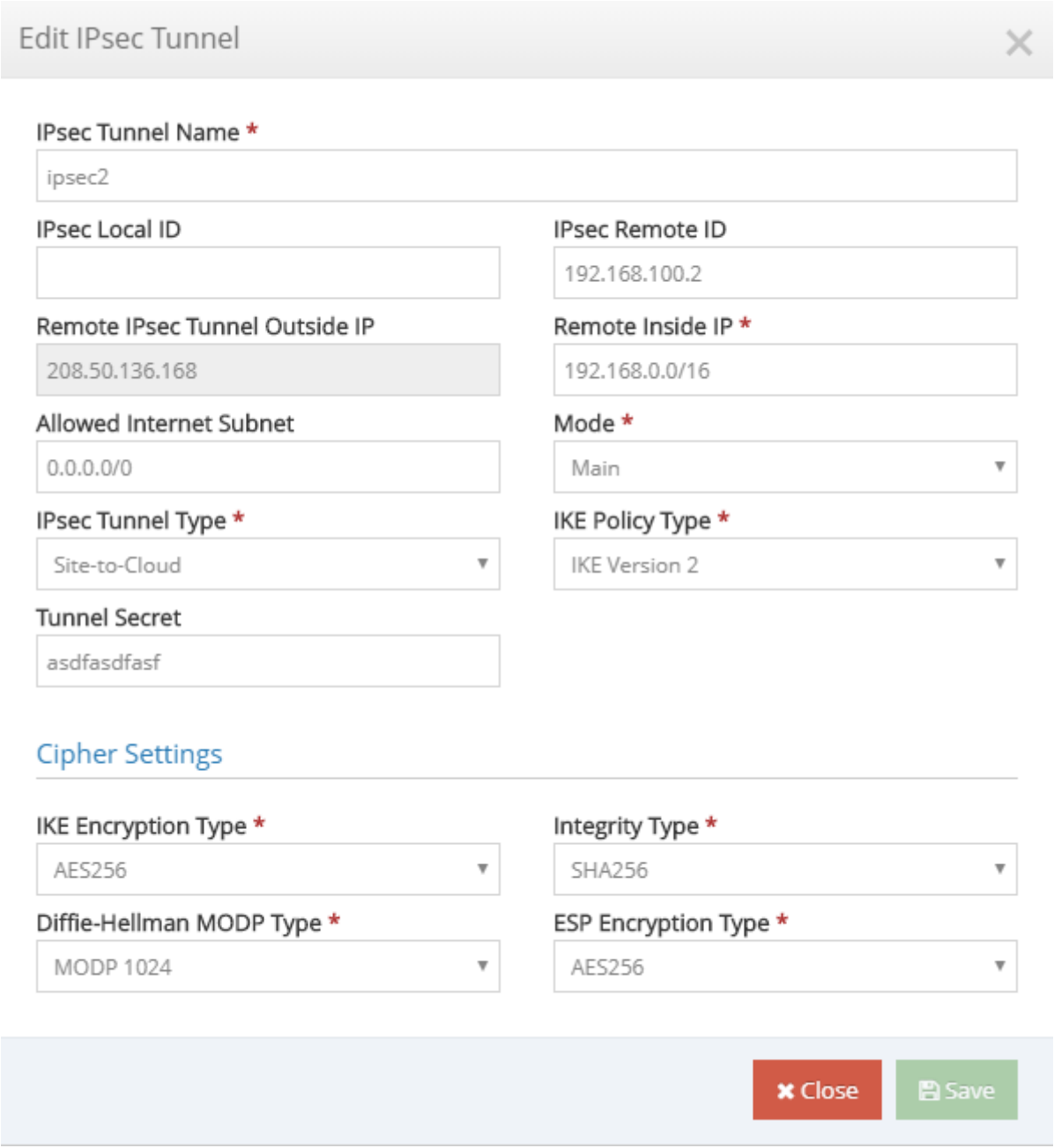
Todas las demás configuraciones (por ejemplo, IP externa del túnel IPSec remoto, etc.) pueden ser específicas de la implementación. Las subredes de túnel interior deben ser únicas para cada túnel (por ejemplo, 169.254.1.0/30, 169.254.1.4/30, etc.). Los nodos iboss únicos deben utilizarse para subredes superpuestas entre varios sitios. Por ejemplo, si el sitio 'A'y el sitio 'B'usan la subred 192.168.1.0/24, entonces la configuración del túnel para cada uno de estos sitios debe realizarse en diferentes nodos iboss.

Haga clic en **Guardar**. La información del túnel se presenta como un resumen.



Puede editar todos los parámetros de configuración del túnel, excepto Túnel IPSec **Remote IPSec Outside IP**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

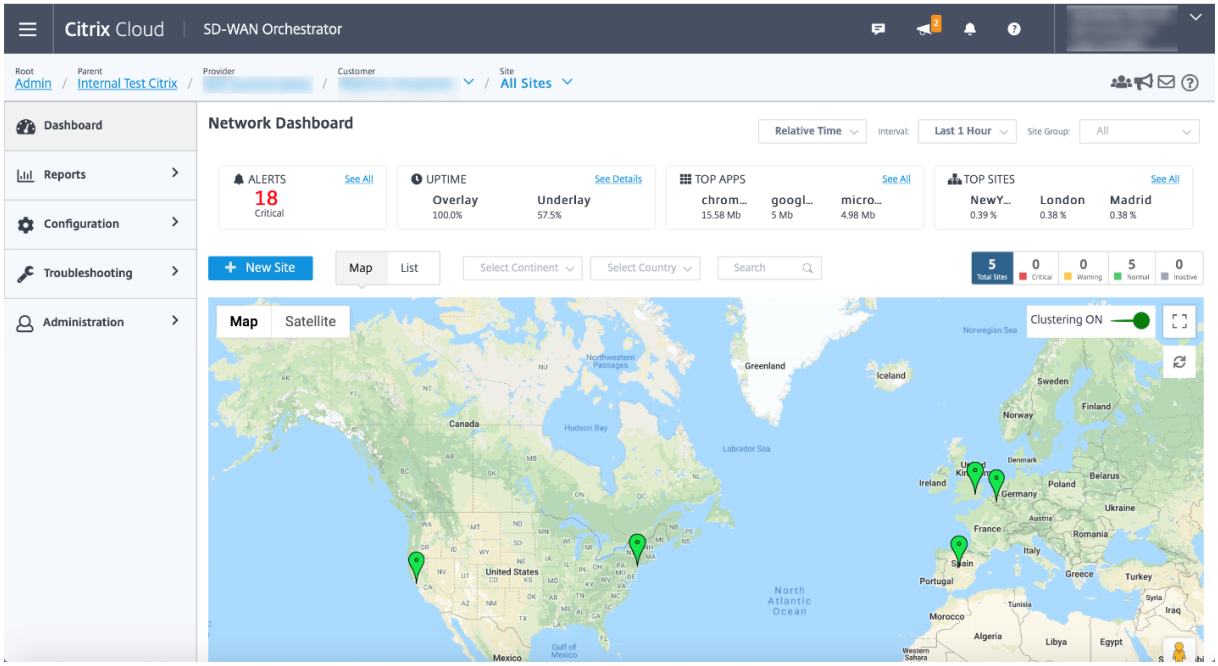


Configuración de Citrix SD-WAN

La red Citrix SD-WAN se administra a través del servicio de administración basado en Citrix Cloud Citrix SD-WAN Orchestrator. Si aún no tiene una cuenta, consulte Integración de Citrix SD-WAN Orchestrator.

Después de completar correctamente el proceso de incorporación, puede acceder a SD-WAN Orchestrator.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

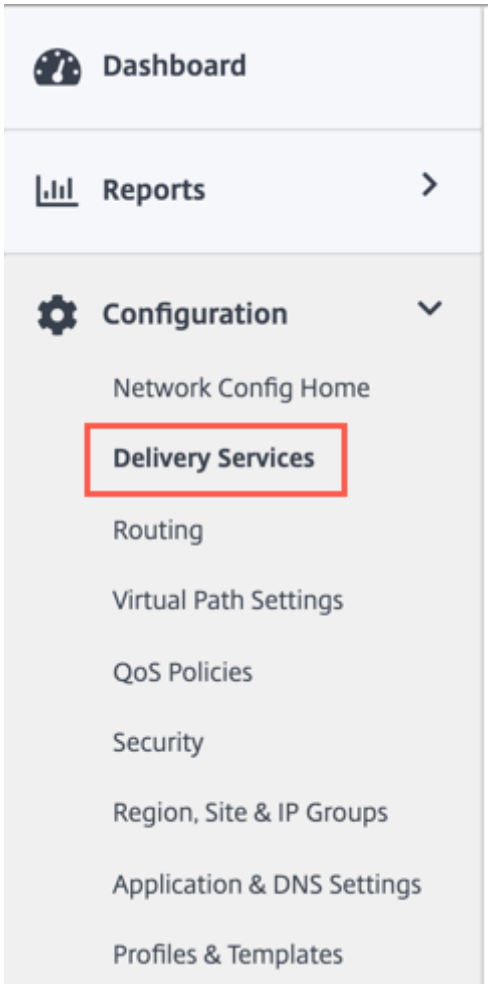


Asegúrese de que el sitio de Citrix SD-WAN ya está configurado y conectado a las sucursales y redes. Para obtener detalles sobre la configuración, consulte Configuración de red.

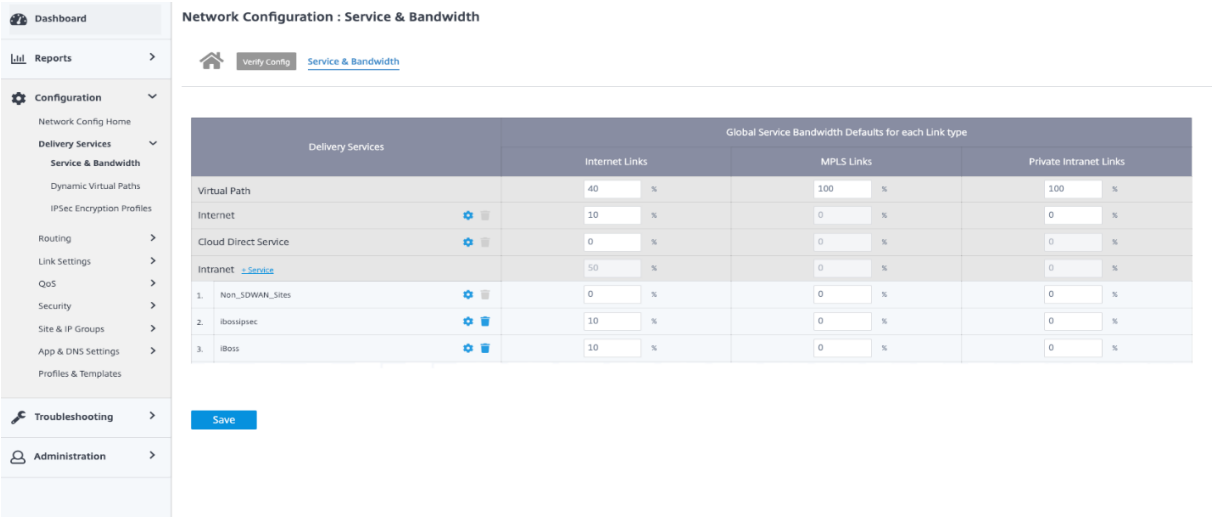
Servicios de entrega

Los servicios de entrega le permiten configurar servicios de entrega como Internet, Intranet, IPSec y GRE. Los servicios de entrega se definen globalmente y se aplican a los enlaces WAN en sitios individuales, según corresponda.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



iboss cloud se puede conectar desde Citrix SD-WAN a través de los servicios GRE o IPSec. Utiliza los ajustes recomendados por iboss en la sección anterior.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Servicio GRE

Puede configurar dispositivos SD-WAN para terminar túneles GRE. Configure los siguientes parámetros.

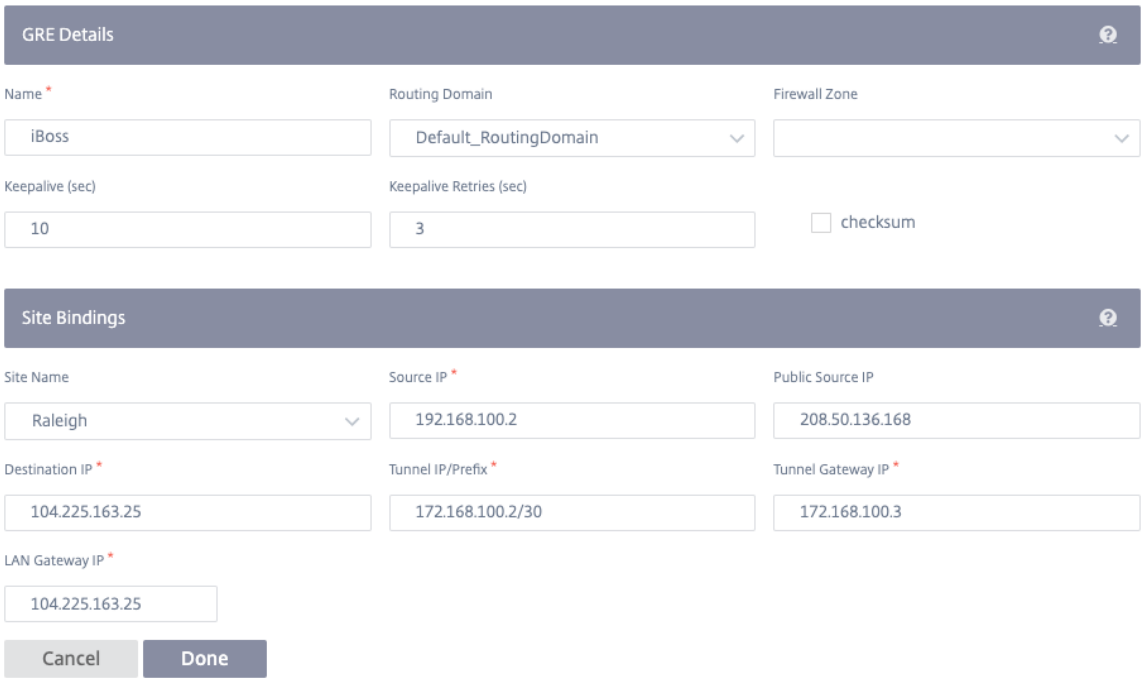
Detalles de GRE:

- **Nombre**: El nombre del servicio GRE.
- **Dominio de redirección**: Dominio de redirección del túnel GRE.
- **Zona de firewall**: Zona de firewall elegida para el túnel. De forma predeterminada, el túnel se coloca en Default_LAN_ZONE.
- **Conexión persistente**: El período entre el envío de mensajes de conexión persistente. Si se configura en 0, no se envían paquetes de mantenimiento vivo, pero el túnel permanece activo.
- **Reintentos de mantenimiento vivo**: el número de veces que el dispositivo Citrix SD-WAN envía paquetes de mantenimiento vivo sin respuesta antes de bajar el túnel.
- **Suma de comprobación**: habilite o deshabilite la suma de comprobación para el encabezado GRE del túnel.

Enlaces de sitios:

- **Nombre del sitio**: El sitio para mapear el túnel GRE.
- **IP de origen**: La dirección IP de origen del túnel. Esta es una de las interfaces virtuales configuradas en este sitio. El dominio de redirección seleccionado determina las direcciones IP de origen disponibles.
- **IP de origen público**: La IP de origen si el tráfico del túnel pasa por NAT.
- **IP de destino**: La dirección IP de destino del túnel.
- **Túnel IP/prefijo**: La dirección IP y el prefijo del túnel GRE.
- **IP de puerta de enlace de túnel**: dirección IP de salto siguiente para enrutar el tráfico del túnel.
- **IP de la puerta de enlace LAN**: dirección IP de salto siguiente para enrutar el tráfico de LAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Servicio IPSec

Los dispositivos Citrix SD-WAN pueden negociar túneles IPSec fijos con pares de terceros en el lado LAN o WAN. Puede definir los puntos finales del túnel y asignar sitios a los puntos finales del túnel.

También puede seleccionar y aplicar un perfil de seguridad IPSec que defina el protocolo de seguridad y la configuración IPSec.

Para agregar un perfil de cifrado IPSec, vaya a **Configuración** > **Servicios de entrega** > seleccione la ficha **Perfiles de cifrado IPSec**.

Los perfiles IPSec se utilizan al configurar los servicios IPSec como conjuntos de servicios de entrega. En la página de perfil de seguridad IPSec, introduzca los valores necesarios para el **perfil de cifrado IPSec**, la configuración de **IKE y la configuración**de **IPSec**.

Información del perfil de cifrado IPSec:

- **Nombre del perfil**: El nombre del perfil.
- **MTU**: El tamaño máximo de paquete IKE o IPSec en bytes.
- **Mantener vivo**: Mantenga el túnel activo y habilite la elegibilidad de la ruta.
- **Versión IKE**: La versión del protocolo IKE.

Configuración de IKE:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

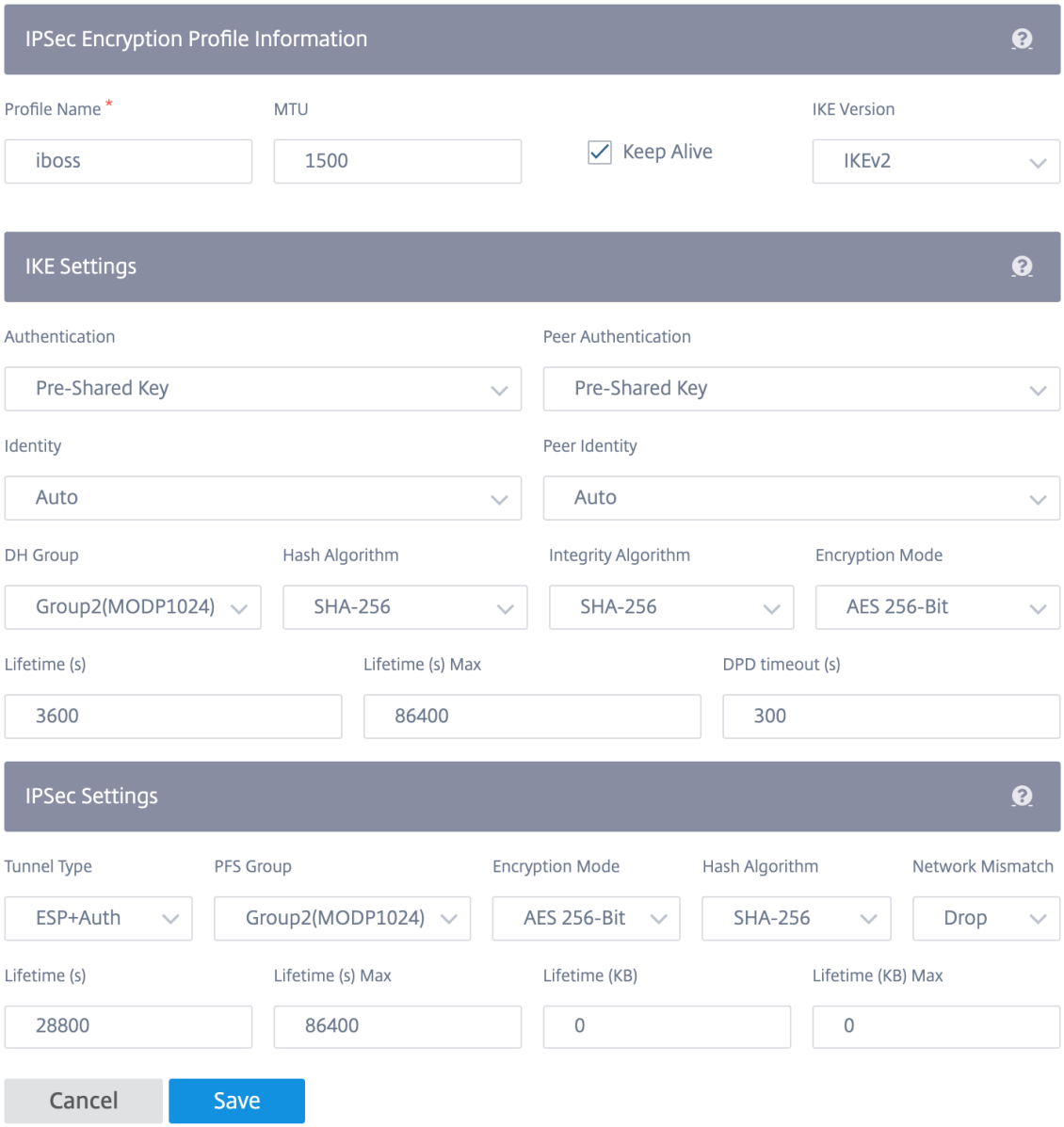
- **Modo**: Seleccione el modo principal o el modo agresivo para el modo de negociación IKE Fase 1.
  - **Principal**: No hay información expuesta a posibles atacantes durante la negociación, pero es más lenta que el modo Agresivo.
  - **Agresivo**: Cierta información (por ejemplo, la identidad de los pares negociadores) está expuesta a posibles atacantes durante la negociación, pero es más rápida que el modo Principal.
- **Autenticación**: el tipo de autenticación, Certificado o Clave precompartida.
- **Identidad**: El método de identidad.
- **Identidad de pares**: El método de identidad de pares.
- **Grupo DH: El grupo**Diffie-Hellman (DH) que están disponibles para la generación de claves IKE.
- **Algoritmo hash**: algoritmo hash para autenticar mensajes IKE.
- **Modo**de cifrado: el modo de cifrado para mensajes IKE.
- **Duración (s)**: la duración preferida (en segundos) para que exista una asociación de seguridad IKE.
- **Duración (s) Máx**(s): duración máxima preferida (en segundos) para permitir que exista una asociación de seguridad IKE.
- **Timeout (s) DPD (s)**: el tiempo de espera de detección de pares muertos (en segundos) para las conexiones VPN.

Configuración de IPSec:

- **Tipo de túnel**: El tipo de encapsulación del túnel.
  - **ESP**: Cifra únicamente los datos del usuario.
  - **ESP+Auth**: Cifra los datos del usuario e incluye un HMAC.
  - **ESP+NULL**: Los paquetes están autenticados pero no cifrados.
  - **AH**: Solo incluye un HMAC.
- Grupo**PFS: El grupo**Diffie—Hellman que se utiliza para una perfecta generación de claves de secreto hacia adelante.
- **Modo**de cifrado: el modo de cifrado para los mensajes IPSec del menú desplegable.
- **Algoritmo de hash: Los algoritmos**hash MD5, SHA1 y SHA-256 están disponibles para la verificación HMAC.
- **Discordancia de red**: acción que se debe realizar si un paquete no coincide con las redes protegidas del túnel IPsec.
- **Duración (s)**: cantidad de tiempo (en segundos) para que exista una asociación de seguridad IPSec.
- **Duración (s) Máx**(s): cantidad máxima de tiempo (en segundos) para permitir que exista una asociación de seguridad IPSec.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Vida útil (KB)**: la cantidad de datos (en kilobytes) para que exista una asociación de seguridad IPSec.
- **Vida útil (KB) Máx.**: cantidad máxima de datos (en kilobytes) para permitir que exista una asociación de seguridad IPSec.



Para configurar el túnel IPSec:

1. Especifique los detalles del servicio:

   - **Nombre del servicio**: nombre del servicio IPSec.
   - **Tipo de servicio**: servicio que utiliza el túnel IPSec.
   - **Dominio de redirección**: Para túneles IPSec a través de LAN, seleccione un dominio de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

redirección. Si el túnel IPSec utiliza un servicio de Intranet, el servicio de Intranet determina el dominio de redirección.
- **Zona de firewall**: Zona de firewall para el túnel. De forma predeterminada, el túnel se coloca en Default_LAN_ZONE.

2. Agregue el punto final del túnel.

   - **Nombre**: Cuando el tipo de servicio es Intranet, elija un servicio de intranet que el túnel proteja. De lo contrario, introduzca un nombre para el servicio.
   - **IP del mismo nivel**: La dirección IP del par remoto.
   - **Perfil IPSec**: Perfil de seguridad IPSec que define el protocolo de seguridad y la configuración IPSec.
   - **Clave precompartida**: clave previamente compartida utilizada para la autenticación IKE.
   - **Clave precompartida de par**: Clave precompartida utilizada para la autenticación IKEv2.
   - **Datos de identidad**: los datos que se utilizarán como identidad local, cuando se utiliza la identidad manual o el tipo FQDN de usuario.
   - **Datos de identidad del mismo nivel**: Los datos que se utilizarán como identidad del mismo nivel cuando se utilice la identidad manual o el tipo FQDN del usuario.
   - **Certificado**: Si elige Certificado como autenticación IKE, elija entre los certificados configurados.

3. Asigne sitios a los puntos finales del túnel.

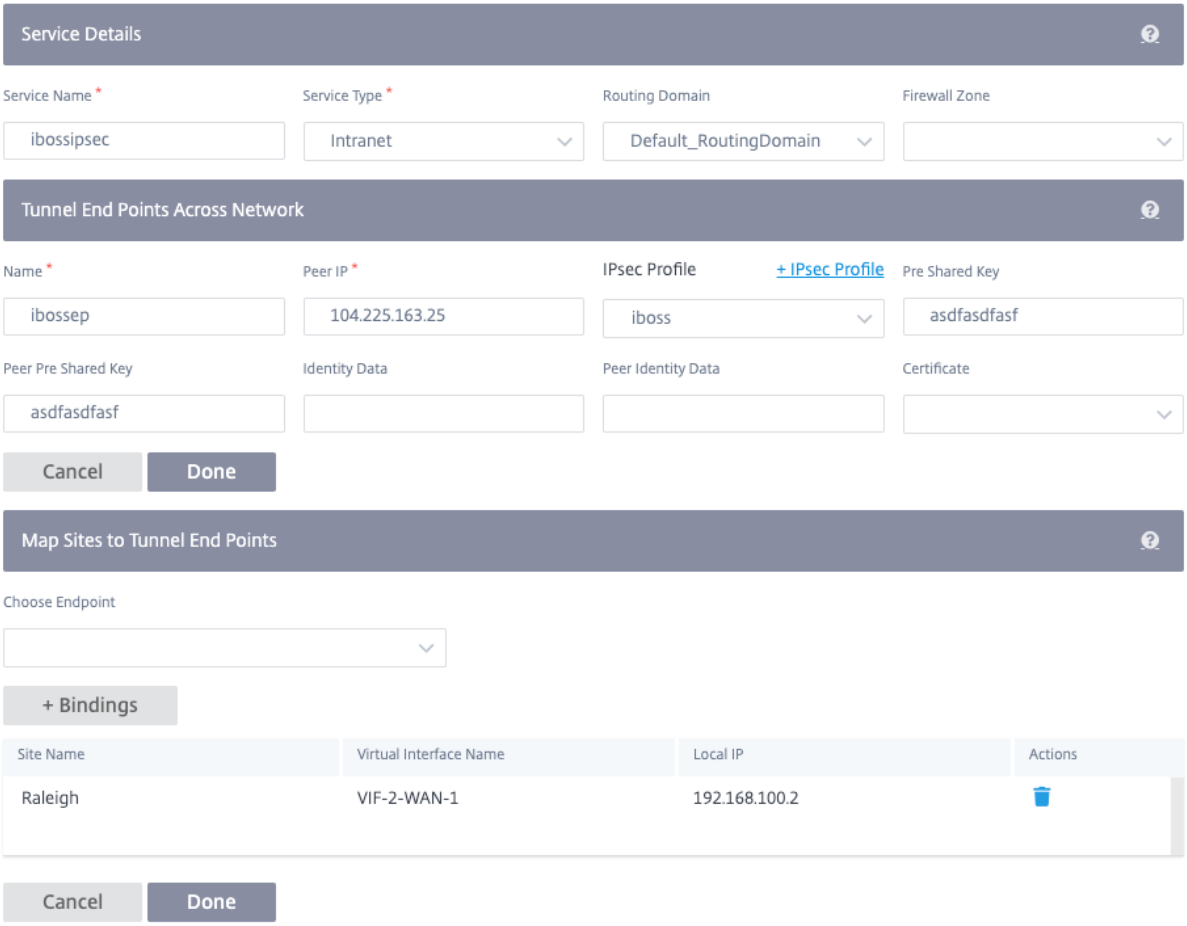
   - **Elija dispositivo de punto final**: El punto final que se va a asignar a un sitio.
   - **Nombre del sitio**: el sitio que se va a asignar al punto final.
   - **Nombre de la interfaz virtual**: Interfaz virtual en el sitio que se va a utilizar como punto final.
   - **IP local**: La dirección IP virtual local que se utilizará como punto final del túnel local.

4. Cree la red protegida.

   - **IP/Prefijo de red**de origen: Dirección IP de origen y prefijo del tráfico de red que protege el túnel IPSec.
   - **IP/Prefijo de red**de destino: Dirección IP de destino y prefijo del tráfico de red que protege el túnel IPSec.

5. Asegúrese de que las configuraciones IPSec estén reflejadas en el dispositivo del mismo nivel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



IPSec proporciona túneles seguros. Citrix SD-WAN admite rutas virtuales IPSec, lo que permite que los dispositivos de terceros terminen los 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 certificado FIPS 140-2 de nivel 1.

Citrix SD-WAN también admite tunelización IPSec resistente mediante un mecanismo de túnel de ruta virtual diferenciado.

Supervisión de túneles GRE e IPSEC

Túneles GRE

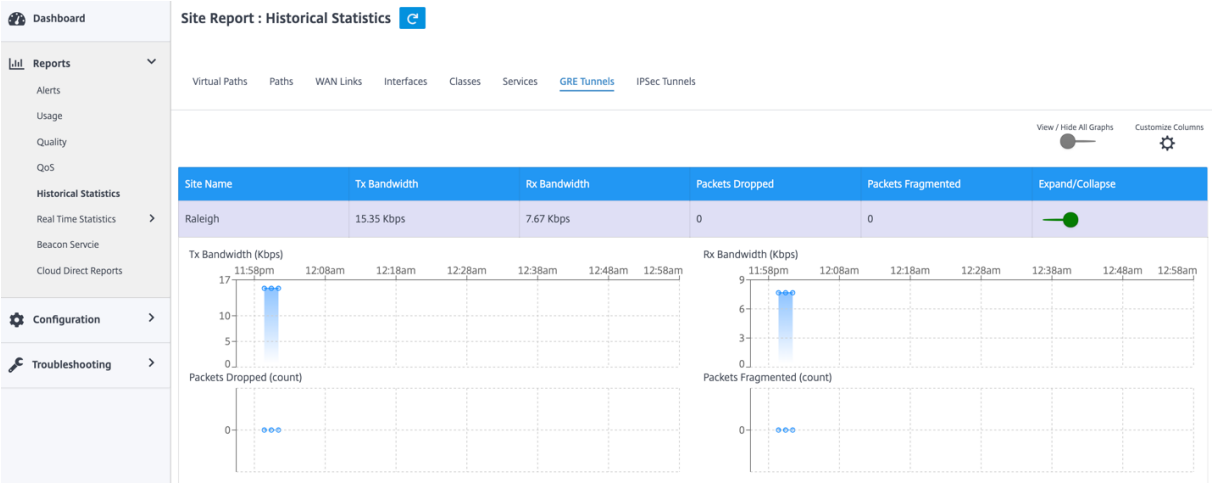
Puede utilizar un mecanismo de túnel para transportar paquetes de un protocolo dentro de otro protocolo. El protocolo que lleva el otro protocolo se denomina protocolo de transporte, y el protocolo transportado se denomina protocolo de pasajeros. La encapsulación de redirección genérica (GRE) es un mecanismo de túnel que utiliza IP como protocolo de transporte y puede transportar muchos protocolos de pasajeros diferentes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La dirección de origen del túnel y la dirección de destino se utilizan para identificar los dos extremos de los vínculos virtuales punto a punto del túnel.

Para ver las estadísticas del túnel GRE, vaya a **Informes** > **Estadísticas** > **Túneles GRE**.
Puede ver las siguientes métricas:

- **Nombre del sitio**: El nombre del sitio.
- **Ancho de banda Tx**: Ancho de banda transmitido.
- **Ancho de banda Rx**: Ancho de banda recibido.
- **Paquete eliminado**: número de paquetes descartados debido a la congestión de la red.
- **Paquetes Fragmentados**: Número de paquetes fragmentados. Los paquetes se fragmentan para crear paquetes más pequeños que pueden pasar a través de un enlace con una MTU más pequeña que el datagrama original. El host receptor vuelve a ensamblar los fragmentos.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.



Túneles IPSec

Los protocolos de seguridad IP (IPSec) proporcionan servicios de seguridad como el cifrado de datos confidenciales, la autenticación, la protección contra la reproducción y la confidencialidad de los datos para los paquetes IP. Carga útil de seguridad encapsulada (ESP) y Encabezado de autenticación (AH) son los dos protocolos de seguridad IPSec utilizados para proporcionar estos servicios de seguridad.

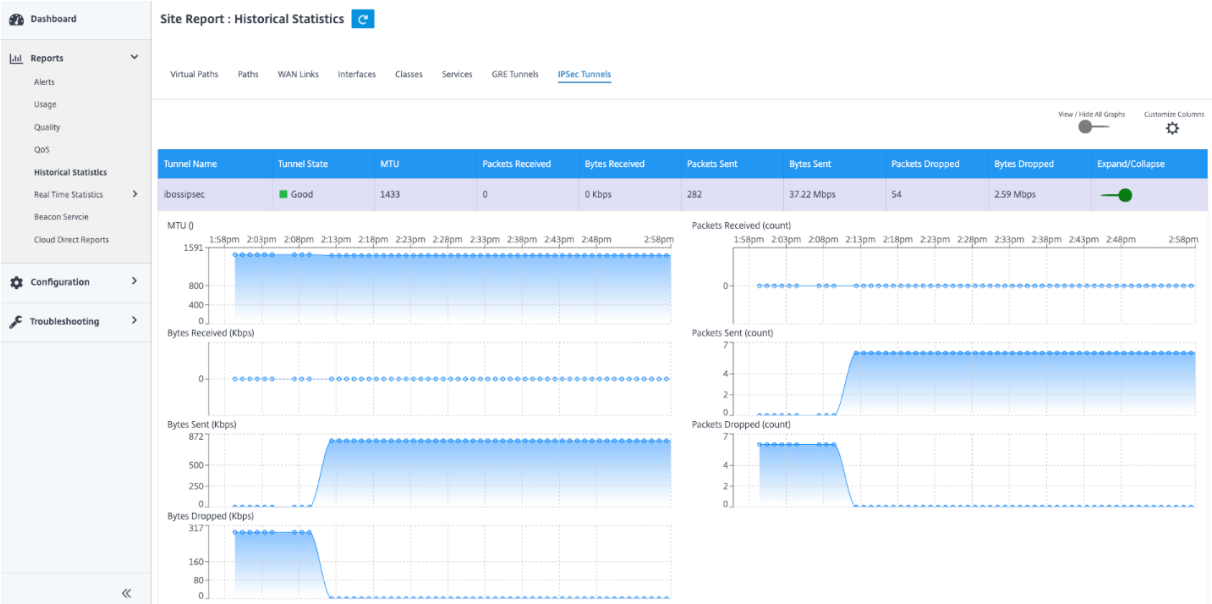
En el modo de túnel IPSec, todo el paquete IP original está protegido por IPSec. El paquete IP original está envuelto y cifrado, y se agrega un nuevo encabezado IP antes de transmitir el paquete a través del túnel VPN.

Para ver las estadísticas **del túnel IPSec**, vaya a **Informes** > **Estadísticas** > **Túneles IPSec**.

Puede ver las siguientes métricas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Nombre del túnel**: Nombre del túnel.
- **Estado del túnel**: Estado del túnel IPSec.
- **MTU**: Unidad de transmisión máxima: Tamaño del datagrama IP más grande que se puede transferir a través de un enlace específico.
- **Paquetes recibidos**: Número de paquetes recibidos.
- **Paquetes enviados**: Número de paquetes enviados.
- **Paquete eliminado**: número de paquetes descartados debido a la congestión de la red.
- **Bytes eliminados**: número de bytes eliminados.
- **Expandir/Contraer**: Puede expandir o contraer los datos según sea necesario.



Soporte de firewall con estado y NAT

May 7, 2021

Esta función proporciona un firewall integrado en la aplicación SD-WAN. El firewall permite directivas entre servicios y zonas, y admite NAT estático, NAT dinámico (PAT) y NAT dinámico con reenvío de puertos. Más funciones de firewall incluyen:

- Proporcionar seguridad para el tráfico de usuarios dentro de la red SD-WAN (Enterprise y Service Providers)
- (Potencial) Reducción del equipo externo (empresas y proveedores de servicios)
- Uso del mismo espacio de direcciones IP para varios clientes: Capacidad NAT (proveedores de servicios)
- Aplicar múltiples firewalls desde una perspectiva global (Proveedores de servicios)

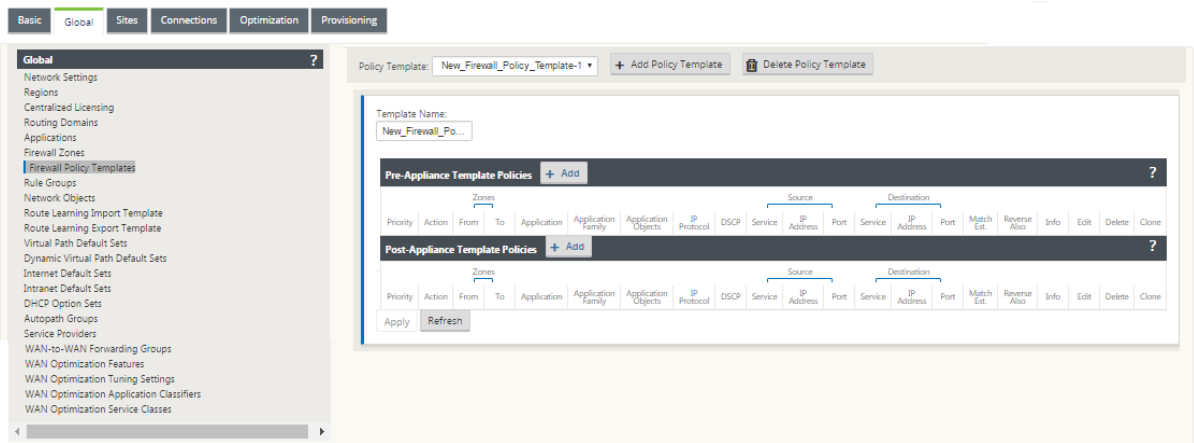
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Filtrar flujos de tráfico entre zonas
- Filtrar el tráfico entre servicios dentro de una zona
- Filtrar el tráfico entre servicios que residen en diferentes zonas
- Filtrar el tráfico entre servicios en un sitio
- Definición de directivas de filtro para permitir, denegar o rechazar flujos
- Seguimiento del estado del flujo de 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 estática (NAT estático)
- Proporcionar traducción dinámica de direcciones de red (NAT dinámico)
- Traducción de direcciones de puerto (PAT)
- Reenvío de puertos

Para simplificar el proceso de configuración, las directivas de firewall se crean en el nivel de Configuración global. Esta configuración global consta de plantillas de directivas de sitios anteriores y posteriores al appliance que se pueden aplicar a todos los sitios dentro de la red SD-WAN.

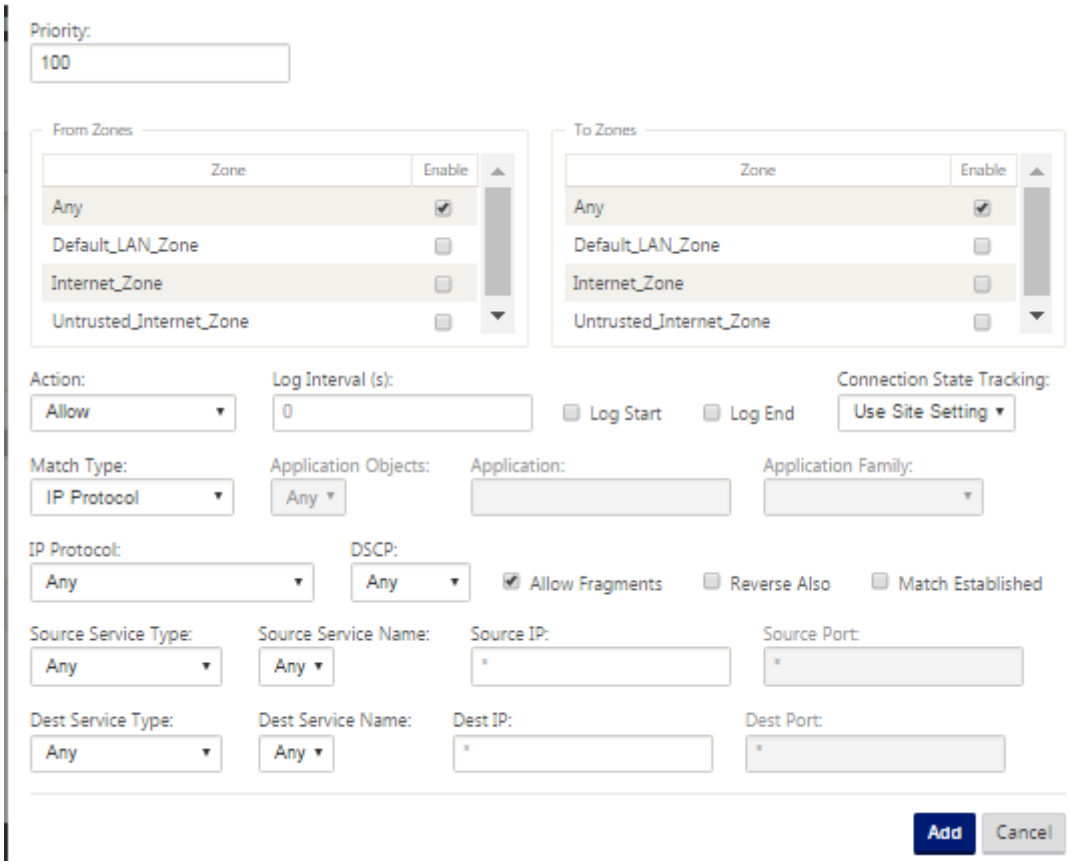
> **Nota**
>
> No se recomienda utilizar firewall en el modo en línea Fail-to-Wire debido a razones de seguridad.

Plantillas de directivas globales



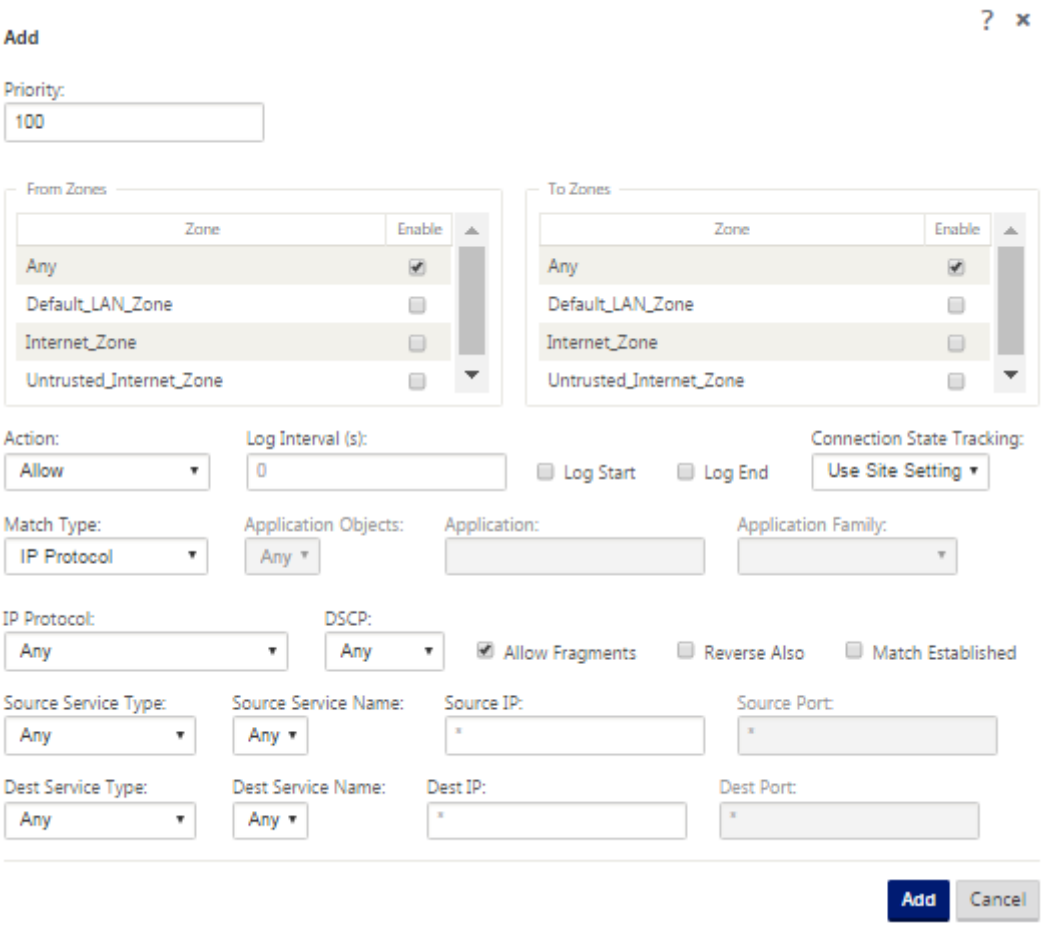
Plantilla previa a la directiva

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Plantilla posterior a la directiva

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración global del firewall

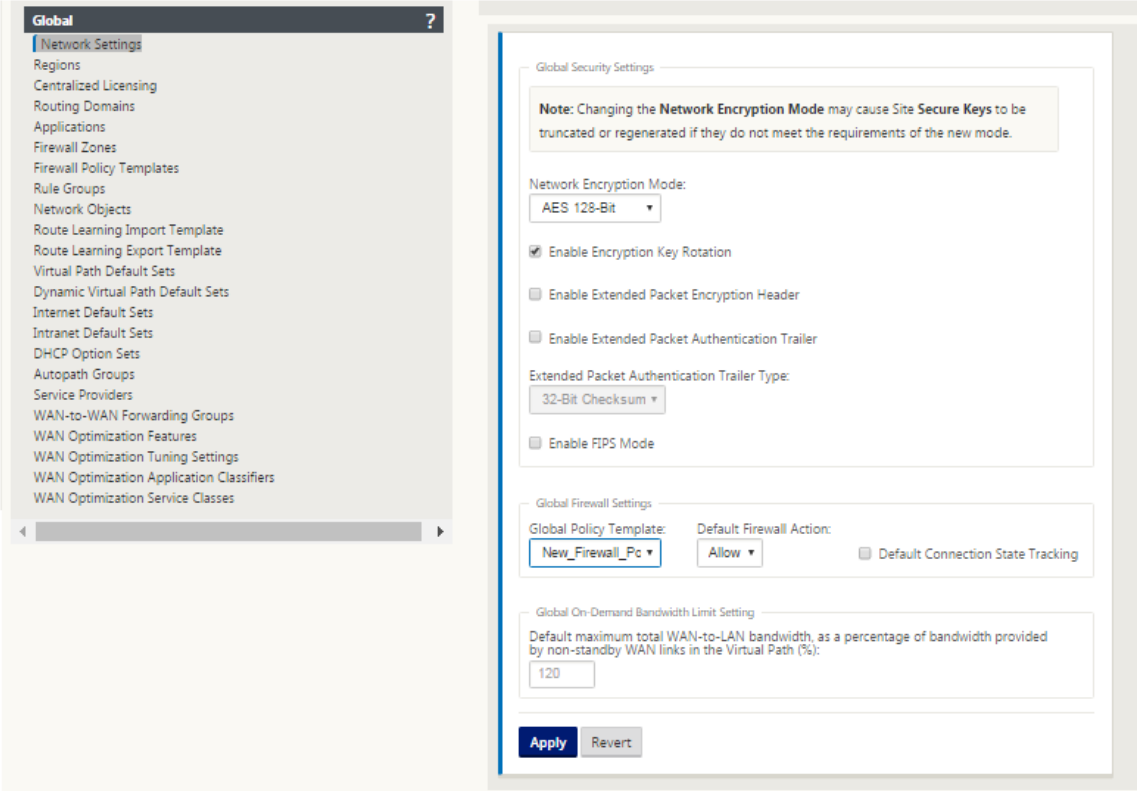
May 7, 2021

Una vez que haya creado las plantillas de directiva de firewall, puede utilizar esta directiva para configurar las opciones de firewall para NetScaler SD-WAN Network. 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.

Para configurar la configuración global del firewall:

1. En el **Editor de configuración**, vaya a **Global** > **Configuración de red** y haga clic en el icono de edición.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. En la sección **Configuración global del firewall**, seleccione valores para las siguientes opciones:
   - **Plantilla de directiva global** - Seleccione una plantilla de directiva de firewall para aplicar a todos los dispositivos de la red SD-WAN, **Acciones de cortafuegos predeterminadas** - Seleccione Permitir para permitir paquetes que no coincidan con la directiva de filtro. Seleccione Drop, para eliminar los paquetes que no coinciden con la directiva de filtro, **Rastreo de estado de conexión predeterminado** - Esto habilita el seguimiento direccional del estado de conexión para flujos TCP, UDP e ICMP que no coinciden con una directiva de filtro o una regla NAT. Esto bloquea el flujo asimétrico, incluso cuando no hay directivas de firewall definidas.
3. Haga clic en **Aplicar**.

> **Nota**
>
> También puede configurar estas opciones en el nivel del sitio, esto anulará la configuración global.

Configuración avanzada de firewalls

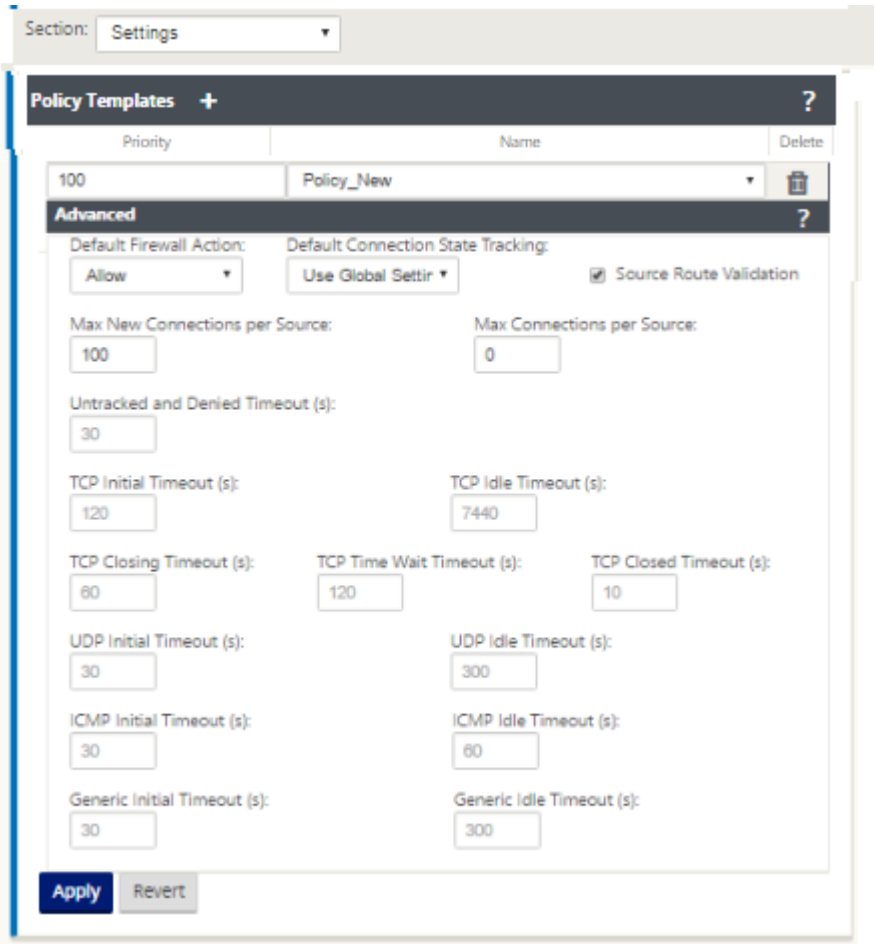
May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede configurar las opciones avanzadas de firewall para cada sitio individualmente. Esto anulará la configuración global.

Para configurar opciones avanzadas de firewall:

1. En el **Editor de configuración**, vaya a **Conexiones**> **Ver sitio**> **Firewall**> **Configuración**.



2. En la sección **Plantilla de directiva**, haga clic en **Agregar**. Introduzca valores para los siguientes parámetros.

   - **Prioridad**: Orden en el que se aplica la directiva en el sitio.
   - **Nombre: Nombre** de la plantilla de directiva que se va a utilizar en el sitio.

3. Haga clic en **Avanzadas**. Introduzca valores para los siguientes parámetros:

   - **Acción predeterminada del cortafuegos**: Seleccione una de las siguientes opciones.
     - **Usar configuración global**: Utilice la configuración global configurada en la configuración de NetScaler SD-WAN
     - **Permitir**: Se permiten paquetes que no coincidan con ninguna directiva de filtro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Drop**: Se eliminan los paquetes que no coinciden con ninguna directiva de filtro.
- **Seguimiento del estado de conexión predeterminado**: Seleccione una de las siguientes opciones.
  - **Usar configuración global**: Utilice la configuración global configurada en la configuración de NetScaler SD-WAN
  - **Sin seguimiento**: El seguimiento del estado de conexión bidireccional no se realizará en paquetes que no coincidan con ninguna directiva de filtro
  - **Seguimiento**: El seguimiento del estado de conexión bidireccional se realizará en paquetes TCP, UDP e ICMP que no coincidan con ninguna directiva de filtro o regla NAT. Esto bloquea el flujo asimétrico, incluso cuando no hay directivas de firewall definidas.
- **Validación de ruta de origen**: Si está habilitada, los paquetes se descartarán cuando se reciban en una interfaz que difiere de la ruta del paquete, según lo determinado por la dirección IP de origen. Solo se considera la ruta con la que el paquete coincidiría actualmente.
- **Máximo de conexiones nuevas por origen**: El número máximo de conexiones no establecidas que se permitirán por dirección IP de origen. 0 significa ilimitado. Utilice esta configuración para evitar ataques de denegación de servicio en el firewall.
- **Número máximo de conexiones por origen**: Número máximo de conexiones para permitir por dirección IP de origen. 0 significa ilimitado. Utilice esta configuración para evitar ataques de denegación de servicio en el firewall.

4. Configure las distintas opciones de tiempo de espera y haga clic en **Aplicar**.

Zonas

May 7, 2021

Puede configurar zonas en la red y definir directivas para controlar la forma en que el tráfico entra y sale de las zonas. De forma predeterminada, se crean las siguientes zonas:

- Zona Internet_Internet
  - Se aplica al tráfico hacia o desde un servicio de Internet mediante una interfaz de confianza.
- Zona de Internet_Untrusted_Untrust

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

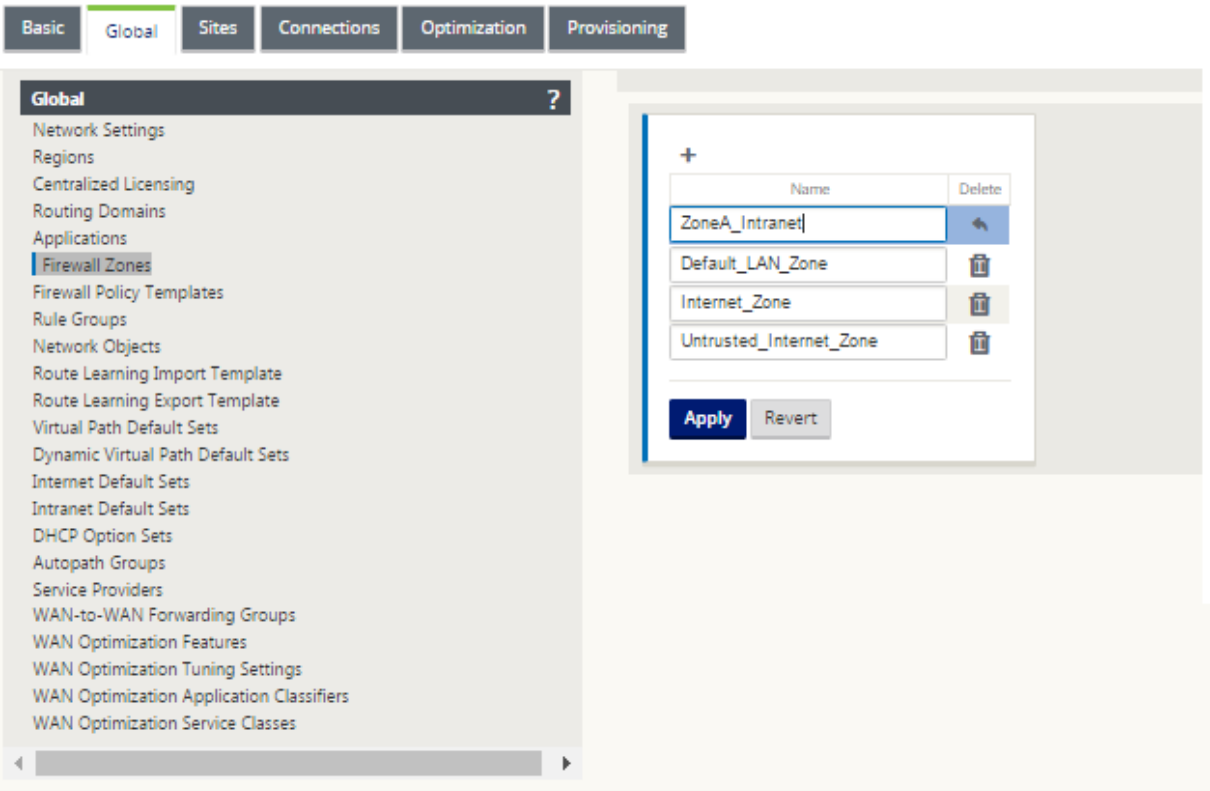
  - Se aplica al tráfico hacia o desde un servicio de Internet mediante una interfaz que no es de confianza.

- Zona DEFAULT_LAN_ZONA
  - Se aplica al tráfico hacia o desde un objeto con una zona configurable, donde no se ha establecido la zona.

Puede crear sus propias zonas y asignarlas a los siguientes tipos de objetos:

- Interfaces de red virtuales (VNI)
- Servicios de Intranet
- Túneles GRE
- Túneles IPSec de LAN

En la siguiente ilustración se muestran las tres zonas preconfiguradas. Además, puede crear sus propias zonas según sea necesario. En este ejemplo, la zona "Zonea_intranet"es una zona creada por el usuario. Se asigna a la interfaz virtual del segmento de derivación (puertos 1 y 2) del dispositivo SD-WAN.

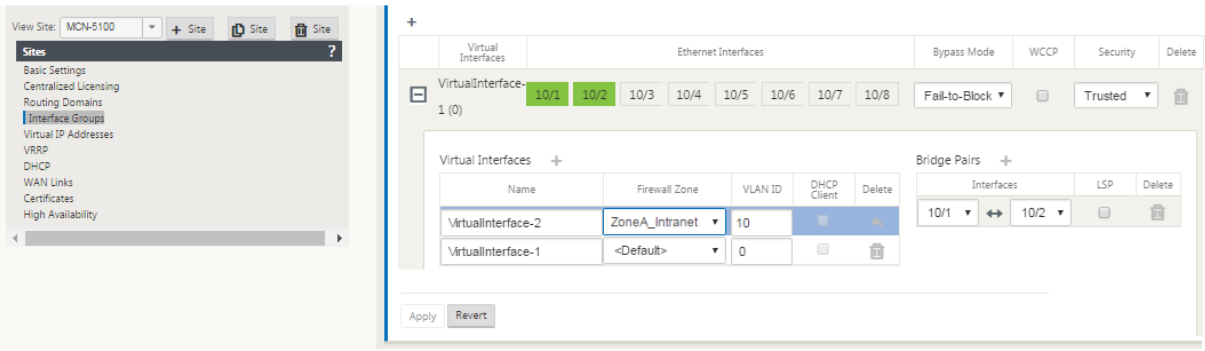


La zona de origen de un paquete viene determinada por el servicio o la interfaz de red virtual en la que se recibe el paquete. La excepción a esto es el tráfico de ruta virtual. Cuando el tráfico entra en una ruta virtual, los paquetes se marcan con la zona que originó el tráfico y esa zona de origen se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

transporta a través de la ruta virtual. Esto permite que el extremo receptor de la ruta virtual tome una decisión de directiva basada en la zona de origen original antes de entrar en la ruta virtual.

Por ejemplo, es posible que un administrador de red quiera definir directivas para que el tráfico de la VLAN 30 en el sitio A pueda introducir la VLAN 10 en el sitio B. El administrador puede asignar una zona para cada VLAN y crear directivas que permitan el tráfico entre estas zonas y bloqueen el tráfico de otras zonas. La captura de pantalla siguiente muestra cómo un usuario asignaría la zona Zonea_intranet a la VLAN 10. En este ejemplo, la zona Zonea_intranet fue definida previamente por el usuario para asignarla a la interfaz virtual VirtualInterface-2".



La zona de destino de un paquete se determina en función de la coincidencia de 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.

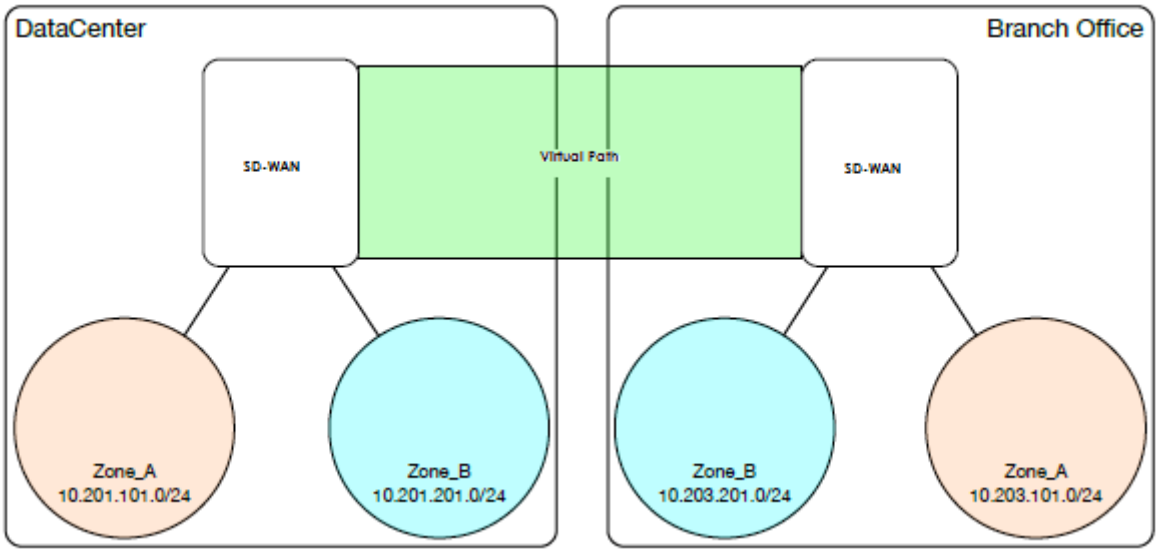
- Zona de origen
  - Ruta de acceso no virtual: Se determinó mediante el paquete de interfaz de red virtual que se recibió en.
  - Ruta virtual: Se determina a través del campo de zona de origen en el encabezado de flujo de paquetes.
  - Interfaz de red virtual: El paquete se recibió en el sitio de origen.
- Zona de destino
  - Se determina mediante la búsqueda de ruta 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). Mediante 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 a un administrador de red una forma eficiente 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 sola zona o crear directivas que se pueden aplicar entre servicios en diferentes zonas, como se muestra en

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la figura siguiente. En el siguiente ejemplo, tenemos Zone_A y Zone_B, cada una de las cuales tiene una interfaz de red virtual LAN.



La captura de pantalla siguiente muestra la herencia de zona para una IP virtual (VIP) de su interfaz de red virtual (VNI) asignada.

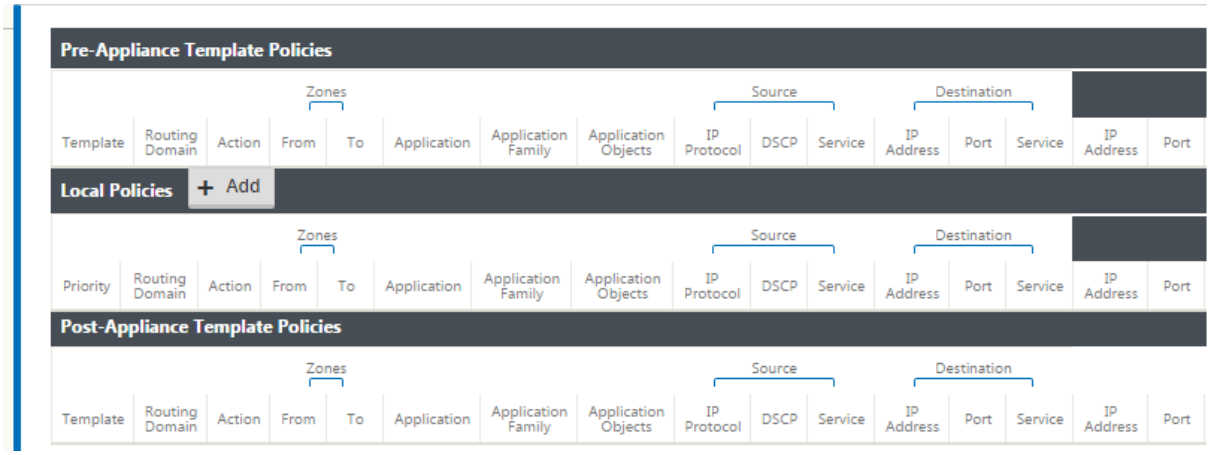
IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	✔		Trusted	🗑
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone			Trusted	

Directivas

May 7, 2021

Las directivas proporcionan la capacidad de permitir, denegar, rechazar o contar y continuar flujos de tráfico específicos. La aplicación de estas directivas de forma individual a cada sitio sería difícil a medida que crecen las redes SD-WAN. Para resolver este problema, se pueden crear grupos de filtros de firewall con una plantilla de directiva de firewall. Una plantilla de directiva de firewall se puede aplicar a todos los sitios de la red o a sitios específicos. Estas directivas se ordenan como directivas de plantilla previa al dispositivo o directivas de plantilla posterior al dispositivo. Las directivas de plantilla anterior y posterior al appliance para toda la red se configuran a nivel global. Las directivas locales se configuran en el nivel de sitio en Conexiones y se aplican únicamente a ese sitio específico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Las directivas de plantilla previa al dispositivo se aplican antes que las directivas de sitio local. Las directivas de sitio local se aplican a continuación, seguidas de las directivas de plantilla posteriores al dispositivo. El objetivo es simplificar el proceso de configuración al permitirle aplicar directivas globales al tiempo que mantiene la flexibilidad para aplicar directivas específicas del sitio.

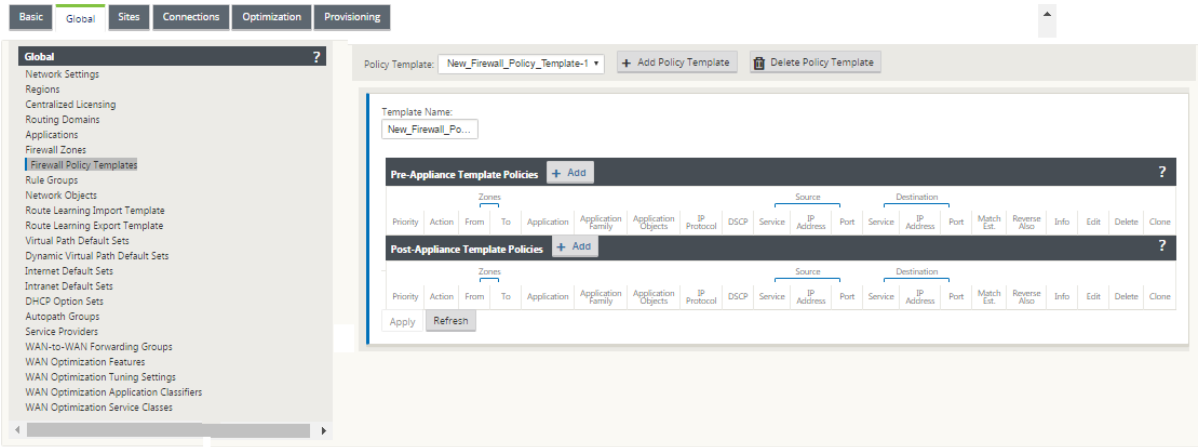
Filtrar orden de evaluación de directivas

1. Plantillas previas —directivas compiladas de todas las secciones de plantilla “PRE”.
2. Pre-Global —directivas compiladas de la sección Global “PRE”.
3. Local: Directivas de nivel de dispositivo.
4. Generación automática local: Directivas generadas automáticamente locales.
5. Post-Templates: directivas compiladas de todas las secciones “POST”de plantilla.
6. Post-Global —directivas compiladas de la sección Global “POST”.

Definiciones de directivas - Global y Local (sitio)

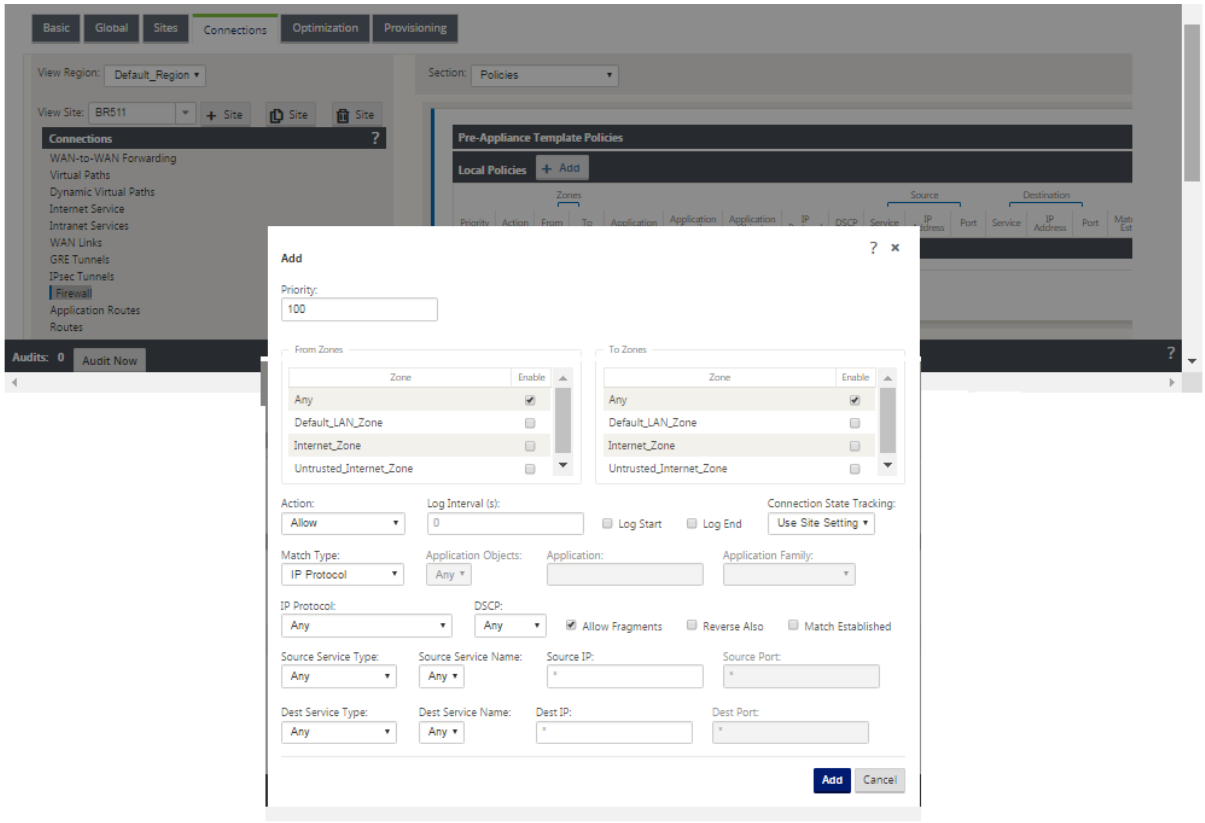
Puede configurar directivas de plantilla previa y posterior al dispositivo a nivel global. Las directivas locales se aplican en el nivel de sitio de un dispositivo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La captura de pantalla anterior muestra la plantilla de directiva que se aplicaría a la red SD-WAN globalmente. Para aplicar una plantilla a todos los sitios de la red, vaya a**Global** > **Configuración de red > Plantilla de directiva global** y seleccione una directiva específica. En el nivel del sitio, puede agregar más plantillas de directivas, así como crear directivas específicas del sitio.

Los atributos configurables específicos de una directiva se muestran en la captura de pantalla siguiente, estos son los mismos para todas las directivas.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Atributos de directiva

- **Prioridad**: Orden en el que se aplicará la directiva dentro de todas las directivas definidas. Las directivas de prioridad inferior se aplican antes que las directivas de prioridad superior.
- **Zona**: Los flujos tienen una zona de origen y una zona de destino.
  - **Desde Zona**: Zona de origen para la directiva.
  - **Zona To**: Zona de destino para la directiva.
- **Acción**: Acción que se realiza en un flujo coincidente.
  - **Permitir**: Permite el flujo a través del cortafuegos.
  - **Drop**: Denegar el flujo a través del firewall mediante la eliminación de los paquetes.
  - **Rechazar**: Deniega el flujo a través del firewall y envía una respuesta específica del protocolo. TCP enviará un reinicio, ICMP enviará un mensaje de error.
  - **Contar y continuar**: Cuente el número de paquetes y bytes para este flujo y, a continuación, continúe hacia abajo en la lista de directivas.
- **Intervalo de registro**: Tiempo en segundos entre el registro del número de paquetes que coinciden con la directiva con el archivo de registro del firewall o con el servidor syslog, si está configurado.
  - **Inicio del registro**: Si se selecciona, se crea una entrada de registro para el nuevo flujo.
  - **Fin de registro**: Registra los datos de un flujo cuando se elimina el flujo.

> **Nota**
>
> El valor predeterminado del intervalo de registro de 0 significa que no hay registro.

- **Seguimiento**: Permite que el firewall realice un seguimiento del estado de un flujo y muestre esta información en la tabla **Supervisión** > **Firewall** > **Conexiones**. Si no se realiza un seguimiento del flujo, el estado mostrará NOT_TRACKED. Consulte la tabla para el seguimiento de estado basado en el protocolo a continuación. Utilice la configuración definida en el nivel del sitio en **Firewall** > **Configuración** > **Avanzado** > **Seguimiento predeterminado**.
  - **No Track**: El estado de flujo no está habilitado.
  - **Seguimiento**: Muestra el estado actual del flujo (que coincide con esta directiva).
- **Tipo de coincidencia**: Seleccione uno de los siguientes tipos de coincidencia
  - **Protocolo IP**: Si se selecciona este tipo de coincidencia, seleccione un protocolo IP con el que coincida el filtro. Las opciones incluyen ANY, TCP, UDP ICMP y así

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Aplicación**: Si se selecciona este tipo de coincidencia, especifique la aplicación que se utiliza como criterio de coincidencia para este filtro.
  - **Familia de aplicaciones**: Si se selecciona este tipo de coincidencia, seleccione una familia de aplicaciones que se utilice como criterio de coincidencia para este filtro.
  - **Objeto de aplicación:** si se selecciona este tipo de coincidencia, seleccione una familia de aplicaciones que se utilice como criterio de coincidencia para este filtro.

Para obtener más información sobre la aplicación, la familia de aplicaciones y el objeto de aplicación, consulte Clasificación de aplicaciones.

- **DSCP**: Permite que el usuario coincida con una configuración de etiqueta DSCP.
- **Permitir fragmentos**: Permite fragmentos IP que coincidan con esta directiva de filtro.

> **Nota**
>
> El firewall no vuelve a ensamblar tramas fragmentadas.

- **Invertir también**: Agregue automáticamente una copia de esta directiva de filtro con la configuración de origen y destino invertida.
- **Coincidencia establecida**: Coincide con los paquetes entrantes para una conexión a la que se permitieron los paquetes salientes.
- **Tipo de servicio de origen**: En referencia a un servicio SD-WAN, Local (para el dispositivo), Ruta de acceso virtual, Intranet, IPHost o Internet son ejemplos de tipos de servicio.
- **Opción IPHost**: Este es un nuevo tipo de servicio para el Firewall y se utiliza para paquetes generados por la aplicación SD-WAN. Por ejemplo, ejecutar un ping desde la interfaz de usuario web de la SD-WAN da como resultado un paquete procedente de una dirección IP virtual SD-WAN. La creación de una directiva para esta dirección IP requeriría que el usuario seleccionara la opción iPHost.
- **Nombre del servicio de origen**: Nombre de un servicio vinculado al tipo de servicio. Por ejemplo, si se selecciona la ruta de acceso virtual para el tipo de servicio de origen, éste sería el nombre de la ruta de acceso virtual específica. Esto no siempre es necesario y depende del tipo de servicio seleccionado.
- **Dirección IP de origen**: Dirección IP típica y máscara de subred que utilizará el filtro para hacer coincidir.
- **Puerto de origen**: Puerto de origen que utilizará la aplicación específica.
- **Tipo de servicio de destino**: En referencia a un servicio SD-WAN: Local (para el dispositivo), Ruta de acceso virtual, Intranet, IPHost o Internet son ejemplos de tipos de servicio.
- **Nombre de servicio de destino**: Nombre de un servicio vinculado al tipo de servicio. Esto no siempre es necesario y depende del tipo de servicio seleccionado.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Dirección IP de destino**: Dirección IP típica y máscara de subred que utilizará el filtro para hacer coincidir.
- **Puerto de destino**: Puerto de destino que utilizará la aplicación específica (es decir, puerto de destino HTTP 80 para el protocolo TCP).

La opción de pista proporciona mucho más detalles sobre un flujo. La información de estado rastreada en las tablas de estado se incluye a continuación.

Tabla de estado para la opción de pista

Solo hay unos pocos estados que son consistentes:

- Conexión**INIT** creada, pero el paquete inicial no era válido.
- **O_DENIED-** paquetes que crearon la conexión son denegados por una directiva de filtro.
- **R_DENIED-** Los paquetes del respondedor son denegados por una directiva de filtro.
- **NOT_TRACKED-** la conexión no se realiza un seguimiento con estado, pero se permite de otro modo.
- **CERRADA**: La conexión ha agotado el tiempo de espera o ha sido cerrada de otro modo por el protocolo.
- **DELETED**: La conexión está en proceso de ser eliminada. El estado DELETED casi nunca se verá.

Todos los demás estados son específicos del protocolo y requieren que se habilite el seguimiento con estado.

TCP puede informar de los siguientes estados:

- **SYN_ENENT** - primer mensaje TCP SYN visto.
- **SYN_SENT2** - Mensaje SYN visto en ambas direcciones, sin SYN+ACK (también conocido como abierto simultáneo).
- **SYN_ACK_RCVD** - SYN+ACK recibido.
- **ESTABLECIDO -** segundo ACK recibido, la conexión está completamente establecida.
- **FIN_WAIT** - primer mensaje FIN visto.
- **CLOSE_WAIT** - Mensaje FIN visto en ambas direcciones.
- **TIME_WAIT** - último ACK visto en ambas direcciones. La conexión está cerrada a la espera de que se vuelva a abrir.

Todos los demás protocolos IP (especialmente ICMP y UDP) tienen los siguientes estados:

- **NUEVO**: Paquetes vistos en una dirección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **ESTABLISHED**: Paquetes vistos en ambas direcciones.

Traducción de direcciones de red (NAT)

May 7, 2021

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 direcciones de puerto PAT)
- NAT dinámico con reglas de reenvío de puertos

> **Nota**
>
> La capacidad NAT solo se puede configurar 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.

NAT estático

May 7, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

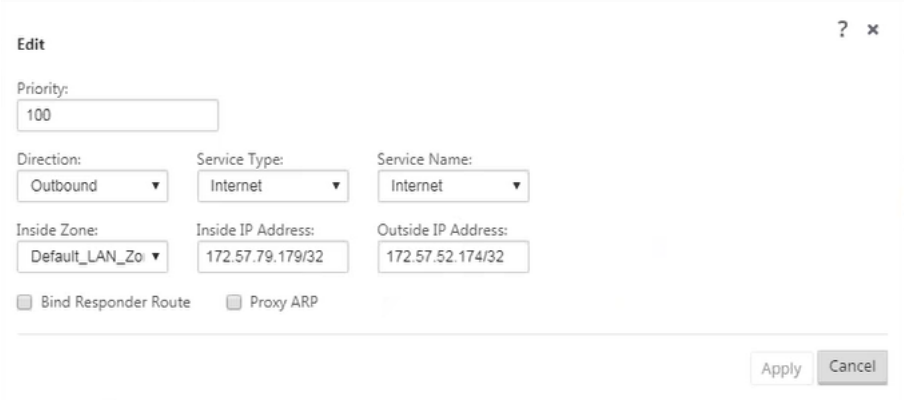
Para NAT saliente, la zona exterior se deriva automáticamente del servicio. Todos los servicios de SD-WAN están asociados a una zona de forma predeterminada. Por ejemplo, el servicio de Internet en un vínculo de Internet de confianza está asociado a la zona de Internet de confianza. Del mismo modo, para 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.

Configurar directivas NAT estáticas

Para configurar directivas NAT estáticas, en el Editor de configuración, vaya a **Conexiones** > **Firewall** > **Directivas NAT estáticas**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

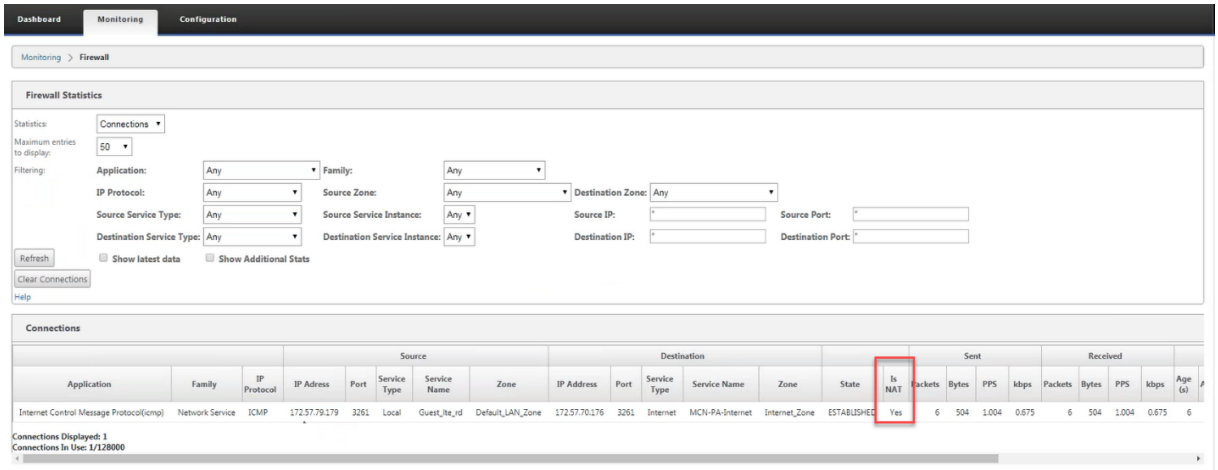


- **Prioridad**: orden en que se aplicará la política dentro de todas las políticas definidas. Las directivas de menor prioridad se aplican antes que las directivas de mayor prioridad.
- **Dirección**: La dirección en la que fluye el tráfico, desde la perspectiva de la interfaz virtual o servicio. Puede ser tráfico entrante o saliente.
- **Tipo de Servicio**: Los tipos de servicio SD-WAN en los que se aplica la directiva NAT. Para NAT estático, los tipos de servicio admitidos son Local, Rutas virtuales, Internet, Intranet y servicios de dominio de interredirección
- **Nombre de servicio**: seleccione un nombre de servicio configurado que corresponda al tipo de servicio.
- **Zona interior**: el tipo de coincidencia de la zona del firewall interior del que debe ser el paquete para permitir la traducción.
- **Zona exterior**: tipo de coincidencia de zona de cortafuegos exterior del que debe ser el paquete para permitir la traducción.
- **Dirección IP interna: la dirección**IP interna y el prefijo a los que se debe traducir si se cumplen los criterios de coincidencia.
- **Dirección IP externa: la dirección**IP externa y el prefijo a los que se traduce la dirección IP interna si se cumplen los criterios de coincidencia.
- **Enlazar ruta del respondedor**: asegura que el tráfico de respuesta se envía a través del mismo servicio en el que se recibe, para evitar el enrutamiento asimétrico.
- **ARP proxy**: garantiza que el dispositivo responda a las solicitudes ARP locales para la dirección IP externa.

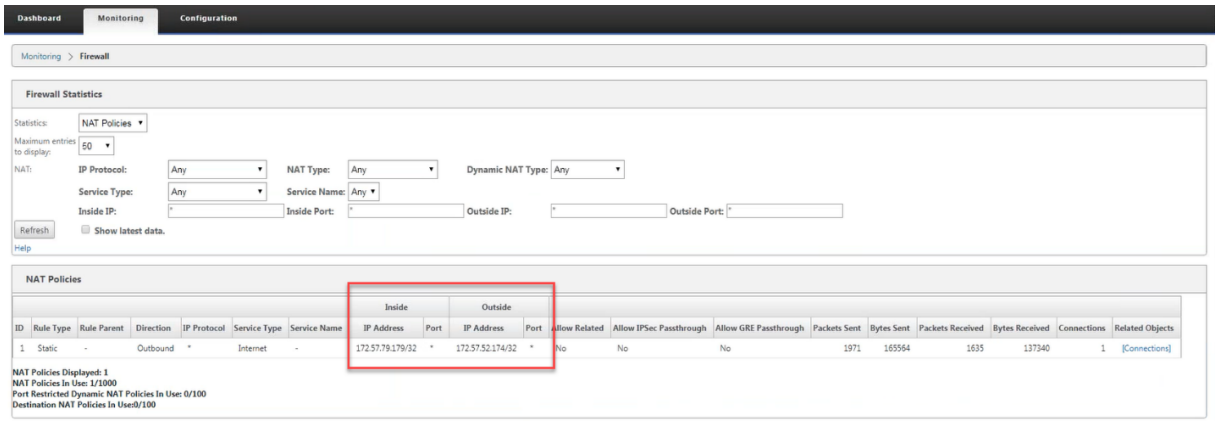
Supervisión

Para supervisar NAT, vaya a **Supervisión** > **Estadísticas del cortafuegos** > **Conexiones**. Para una conexión, puede ver si NAT está hecho o no.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



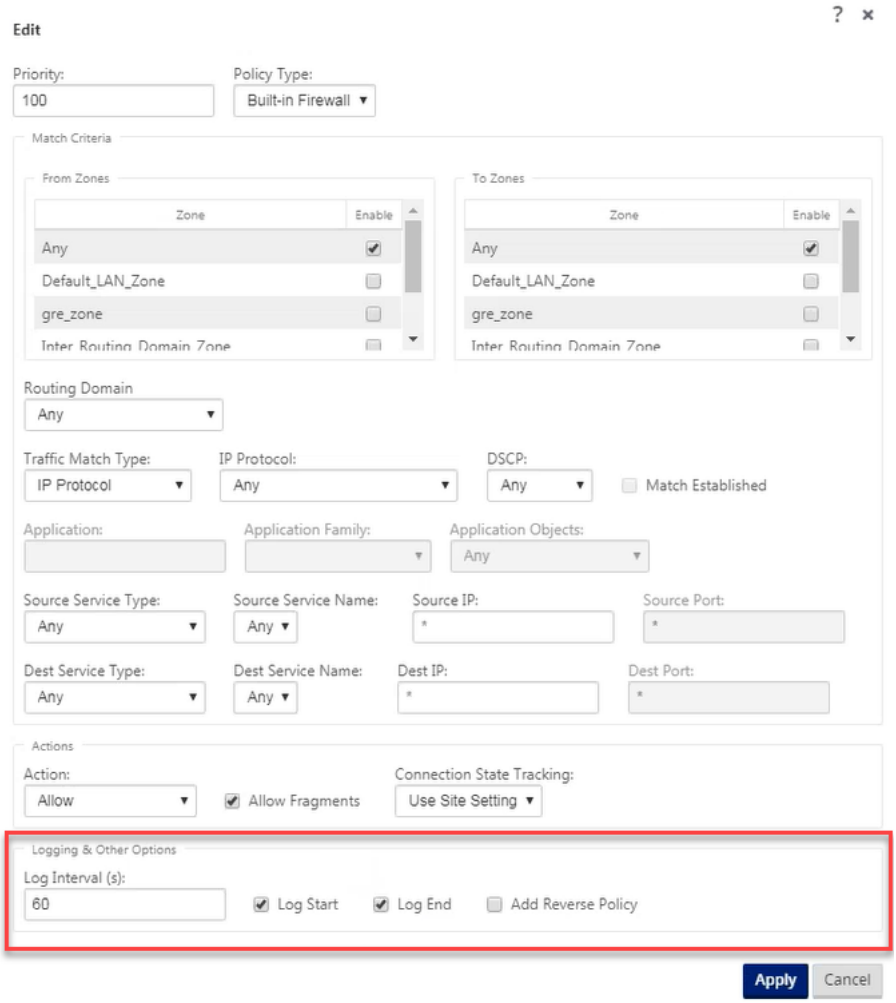
Para ver más a fondo la asignación de direcciones IP internas a direcciones IP externas, haga clic en **NAT posterior al enrutamiento** en **Objetos relacionados** o vaya a **Supervisión** > **Estadísticas del cortafuegos** > **Políticas NAT**.



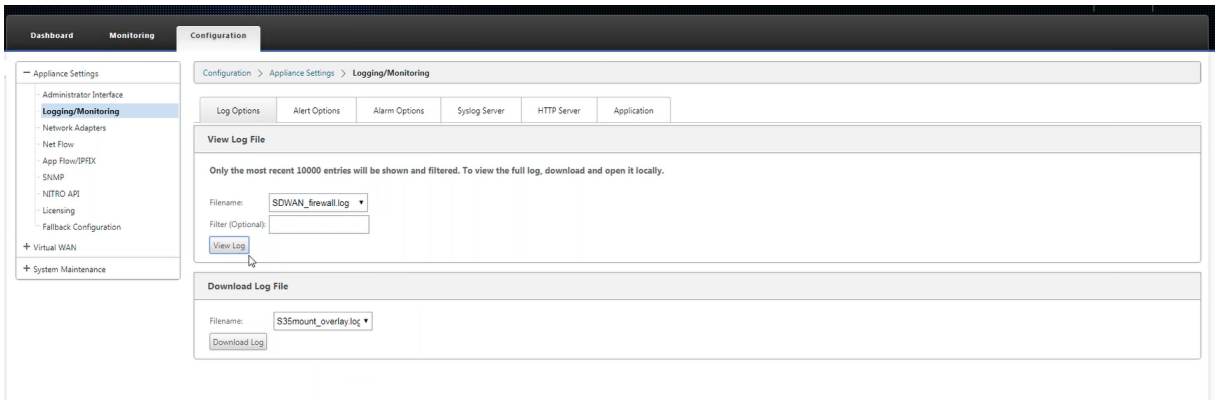
Registros

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vaya a **Registro/Supervisión** > **Opciones de registro**, seleccione **SDWAN_firewal.log**y haga clic en **Ver registro**.



Los detalles de conexión NAT se muestran en el archivo de registro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8704:      Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

NAT dinámico

May 7, 2021

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

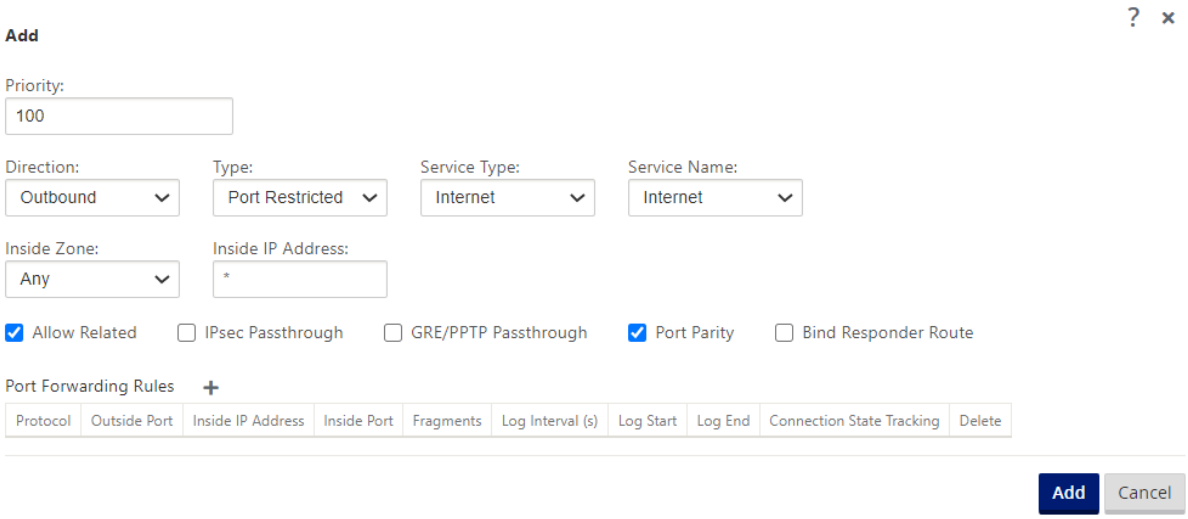
La dirección de una conexión puede ser de interior a exterior o de exterior a interior. Cuando se crea una regla NAT, se aplica a ambas direcciones según el tipo de coincidencia de dirección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

Configurar directivas NAT dinámicas

Para configurar directivas NAT dinámicas, en el Editor de configuración, vaya a **Conexiones** > **Firewall** > **Directivas NAT dinámicas**.



- **Prioridad**: orden en que se aplica la política dentro de todas las directivas definidas. Las directivas de menor prioridad se aplican antes que las directivas de mayor prioridad.
- **Dirección**: La dirección en la que fluye el tráfico, desde la perspectiva de la interfaz virtual o servicio. Puede ser tráfico entrante o saliente.
- **Tipo**: Tipo de NAT dinámico que se va a realizar, con restricción de puerto o simétrica.

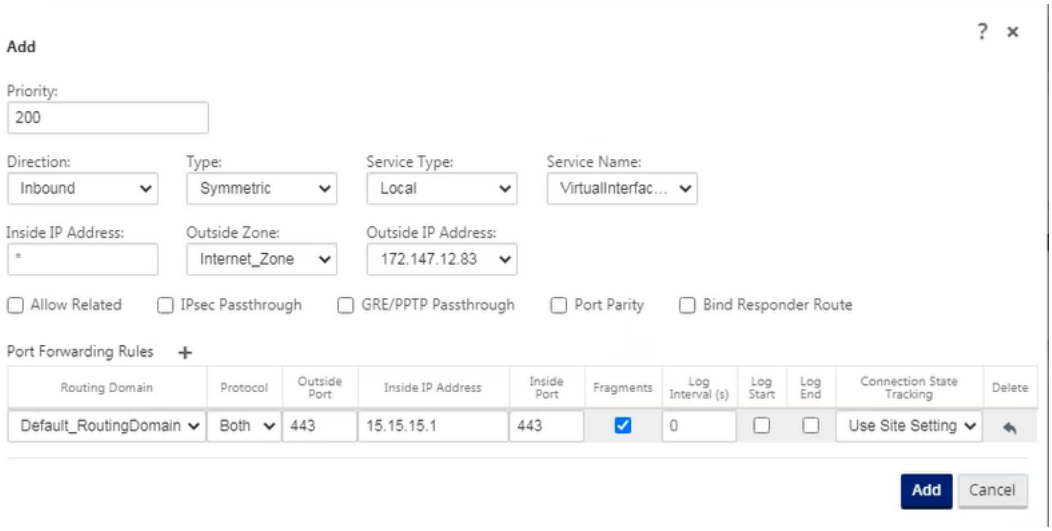
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Tipo de Servicio**: Los tipos de servicio SD-WAN en los que se aplica la directiva NAT dinámica. NAT dinámico entrante es compatible con los servicios de dominio local e interredirección. La NAT dinámica saliente es compatible con los servicios de dominio local, de Internet, de Intranet y interredirección
- **Nombre de servicio**: seleccione un nombre de servicio configurado que corresponda al tipo de servicio.
- **Zona interior**: el tipo de coincidencia de la zona del firewall interior del que debe ser el paquete para permitir la traducción.
- **Zona exterior**: para el tráfico entrante, especifique el tipo de coincidencia de zona de firewall exterior del que debe ser el paquete para permitir la traducción.
- **Dirección IP interna: la dirección**IP interna y el prefijo a los que se debe traducir si se cumplen los criterios de coincidencia. Introduzca '*'para indicar cualquier dirección IP interna.
- **Dirección IP externa: la dirección**IP externa y el prefijo a los que se traduce la dirección IP interna si se cumplen los criterios de coincidencia. Para el tráfico saliente que utiliza servicios de Internet e Intranet, la dirección IP del vínculo WAN configurada se elige dinámicamente como la dirección IP externa.
- **Permitir Relacionado**: Permitir tráfico relacionado con el flujo que coincide con la regla. Por ejemplo, la redirección ICMP relacionada con el flujo específico que coincide con la directiva, si hubo algún tipo de error relacionado con el flujo.
- **Pase IPSec**: Permitir que se traduzca una sesión IPSec (AH/ESP).
- **GRE/PPTP Pase through**: Permitir que una sesión GRE/PPTP sea traducida.
- **Paridad de puertos**: Si está habilitado, los puertos externos para las conexiones NAT mantienen la paridad (incluso si el puerto interior es par, impar si el puerto exterior es impar).
- **Enlazar ruta del respondedor**: asegura que el tráfico de respuesta se envía a través del mismo servicio en el que se recibe, para evitar el enrutamiento asimétrico.

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, Explicación del NAT dinámico de Citrix SD-WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Protocolo**: TCP, UDP o ambos.
- **Puerto exterior**: El puerto exterior que es el puerto de reenvío hacia el puerto interior.
- **Dirección IP interna**: la dirección interna para reenviar paquetes coincidentes.
- **Puerto interior**: El puerto interior al que se reenviará el puerto exterior.
- **Fragmentos**: permite el reenvío de paquetes fragmentados.
- **Intervalo de registro**: Tiempo en segundo entre registrar el número de paquetes que coinciden con la directiva en un servidor syslog.
- **Inicio del registro**: Si se selecciona, se crea una nueva entrada de registro para el nuevo flujo.
- **Final**de registro: Registre los datos de un flujo cuando se elimina el flujo.

  > **Nota**
  >
  > El valor predeterminado del intervalo de registro de 0 significa que no hay registro.

- **Seguimiento**: El seguimiento del estado de conexión bidireccional se realiza en paquetes TCP, UDP e ICMP que coinciden con la regla. Esta función bloquea flujos que parecen ilegítimos, debido al enrutamiento asimétrico o al fallo de la suma de comprobación, validación específica del protocolo. Los detalles del estado se muestran en **Supervisión** > **Firewall** > **Conexiones**.
- **Sin seguimiento**: el seguimiento del estado de conexión bidireccional no se realiza en paquetes que coincidan con la regla.

Cada regla de reenvío de puertos tiene una regla NAT principal. La dirección IP externa se toma de la regla NAT principal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

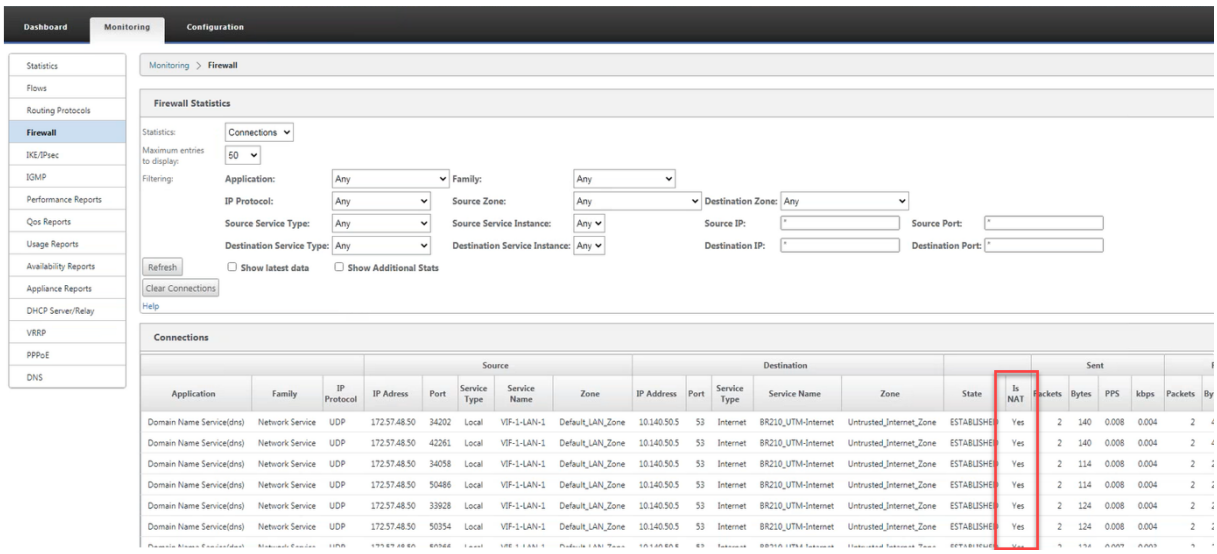
Directivas NAT dinámicas creadas automáticamente

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 único enlace WAN. Para obtener más información detallada, consulte Configurar la segmentación del firewall.
- Configuración de reenviadores DNS o proxy DNS en SD-WAN. Para obtener más información detallada, consulte Sistema de nombres de dominio.

Supervisión

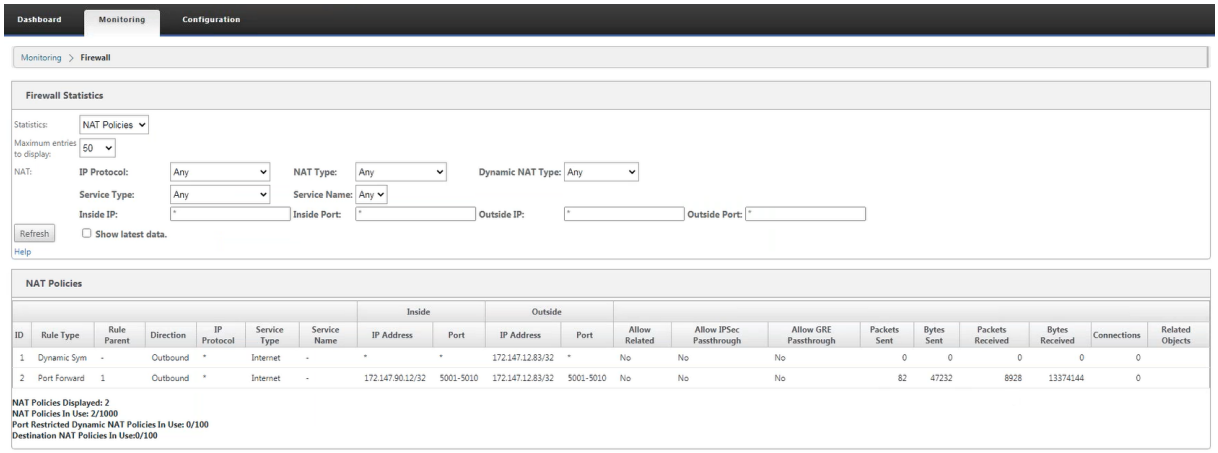
Para supervisar NAT dinámico, vaya a **Supervisión** > **Estadísticas del cortafuegos** > **Conexiones**. Para una conexión, puede ver si NAT está hecho o no.



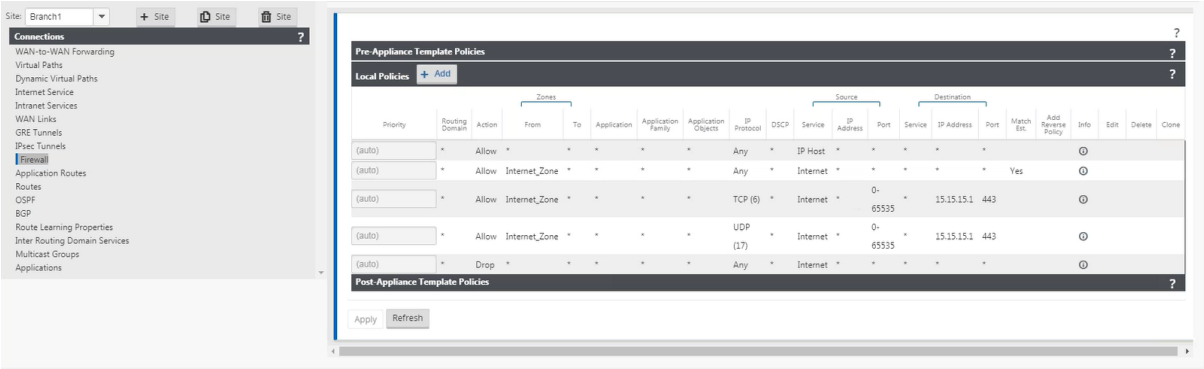
Para ver más a fondo la asignación de direcciones IP internas a direcciones IP externas, haga clic en **NAT previo al enrutamiento o NATposterior al enrutamiento**en**Objetos relacionados**o vaya a**Supervisión**>**Estadísticas del cortafuegos**>**Políticas NAT**.

La siguiente captura de pantalla muestra las estadísticas de la regla NAT dinámica de tipo simétrico y su regla de reenvío de puertos correspondiente.

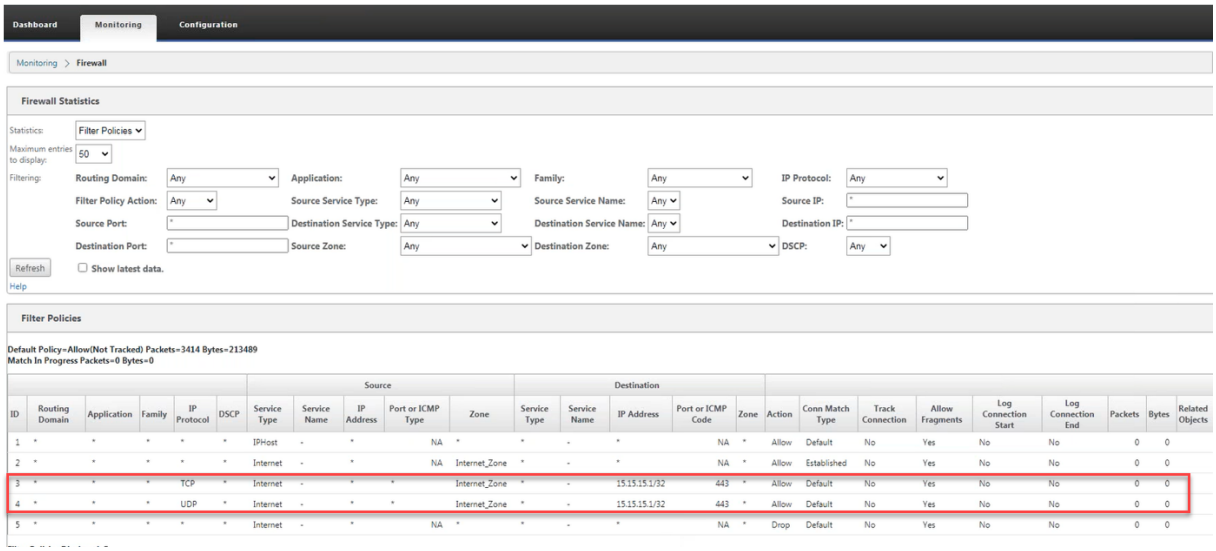
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Cuando se crea una regla de reenvío de puertos, también se crea una regla de firewall correspondiente.



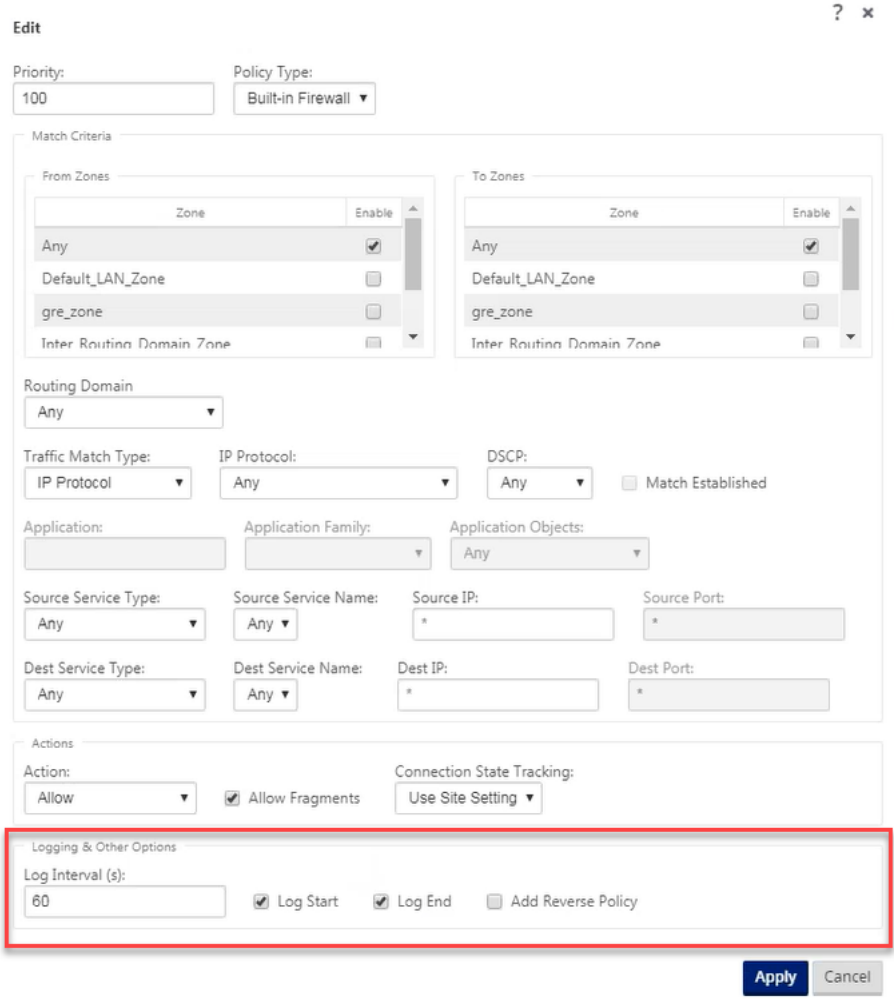
Para ver las estadísticas de directivas de filtro, vaya a **Supervisión** > **Estadísticas del cortafuegos** > **Directivas de filtro**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

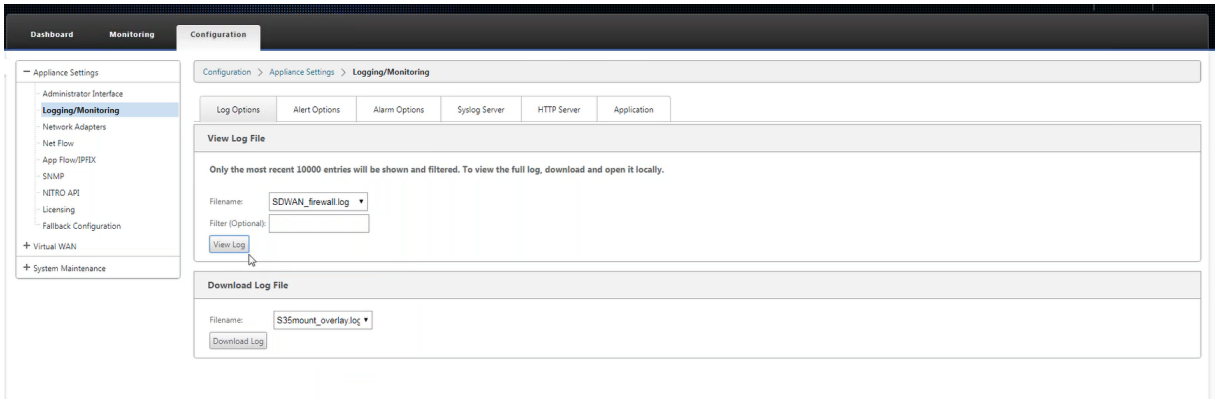
Registros

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.



Vaya a **Registro/Supervisión** > **Opciones de registro**, seleccione **SDWAN_firewal.log**y haga clic en **Ver registro**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Los detalles de conexión NAT se muestran en el archivo de registro.

```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8704        Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

Configurar el servicio WAN virtual

May 7, 2021

La configuración de Citrix SD-WAN describe y define la topología de su red Citrix SD-WAN. Antes de poder implementar una red SD-WAN, debe definir la configuración de WAN virtual. Para ello, utilice el Editor de configuración en la interfaz web de administración de Citrix SD-WAN en el dispositivo MCN.

Seguridad y cifrado

Habilitar el cifrado para SD-WAN (para las rutas virtuales) es opcional. Las instrucciones para configurar esta función se proporcionan en la sección Habilitación y configuración de la seguridad y el cifrado de la WAN virtual (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 los de 256 bits (tamaños de clave) y son opciones configurables. Puede seleccionar, habilitar y configurar estas y otras opciones de cifrado mediante el Editor de configuración de la Interfaz Web

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de administración en el Nodo de control de administración (MCN). Debe tener acceso administrativo en el MCN para modificar la configuración y distribuir los cambios a través de la red SD-WAN. Una vez asegurado el MCN, la configuración de cifrado y su distribución también son seguros.

La autenticación entre sitios funciona con la configuración 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.

Habilitación del servicio WAN virtual

Si se trata de una instalación y configuración iniciales, como paso final deberá habilitar manualmente el servicio WAN virtual en cada dispositivo SD-WAN de la red. Al habilitar el servicio, se habilita e inicia el demonio WAN virtual.

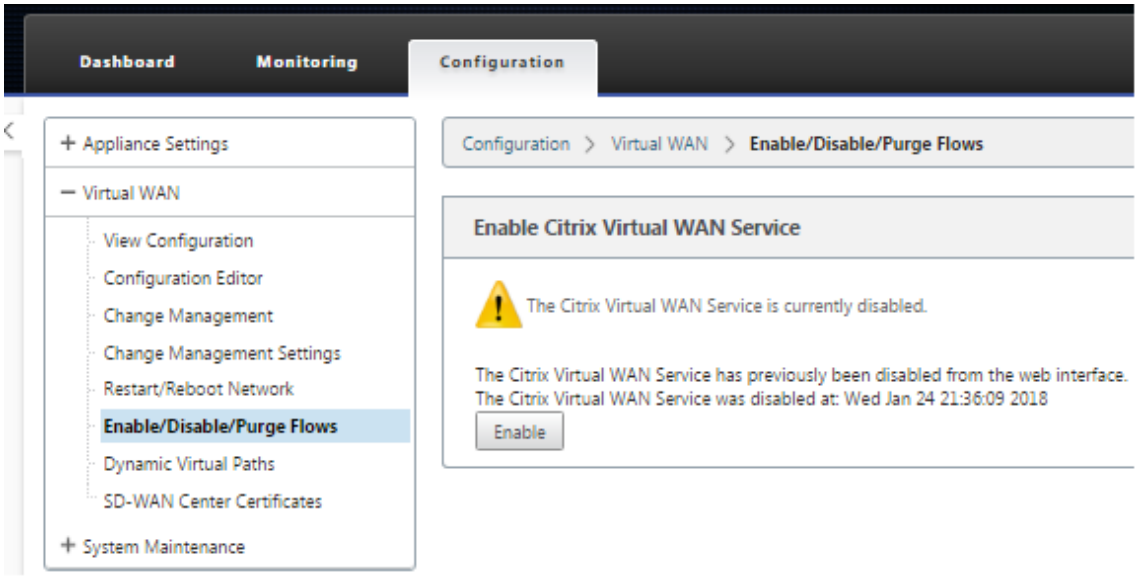
> **Nota**
>
> Si está reconfigurando una implementación existente, el MCN activa automáticamente el servicio cuando distribuye los paquetes de dispositivos actualizados a los sitios cliente. En este caso, puede omitir este paso final.

Para habilitar manualmente el servicio WAN virtual en un dispositivo, haga lo siguiente:

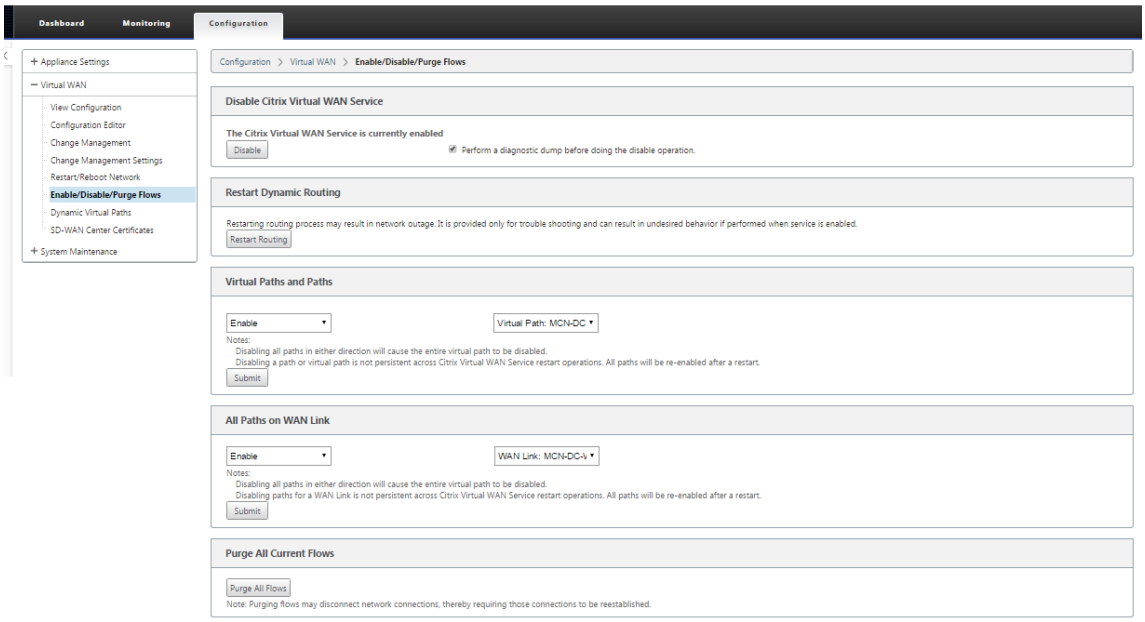
1. Inicie sesión en la Interfaz Web de administración del dispositivo que quiere activar.
2. Seleccione **la ficha Configuración**.
3. En el panel de navegación, abra la sucursal WAN virtual y seleccione **Activar/Desactivar/depurar flujos**.

   Si el servicio WAN virtual está inhabilitado, se mostrará la página Habilitar servicio WAN virtual, como se muestra a continuación. Si el servicio ya está habilitado, se mostrará la página Activar/Desactivar/Depurar Flujos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Haga clic en **Habilitar**. Esto habilita el servicio y muestra la página **Activar/Desactivar/Depurar Flujos**.



Cuando el servicio WAN virtual está habilitado, aparece un mensaje de estado a tal efecto en la sección superior de la página.

> **Nota**
>
> Esta página también presenta opciones para habilitar/inhabilitar rutas específicas y rutas virtuales en la red, así como una opción para purgar todos los flujos.

Esto completa la instalación y activación de SD-WAN en los dispositivos cliente de MCN y sitio de sucur-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sal. Ahora puede utilizar las páginas Supervisión para verificar la activación y diagnosticar cualquier problema de configuración existente o potencial.

Configurar la segmentación del firewall

May 7, 2021

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 ningún acceso al tráfico del otro.

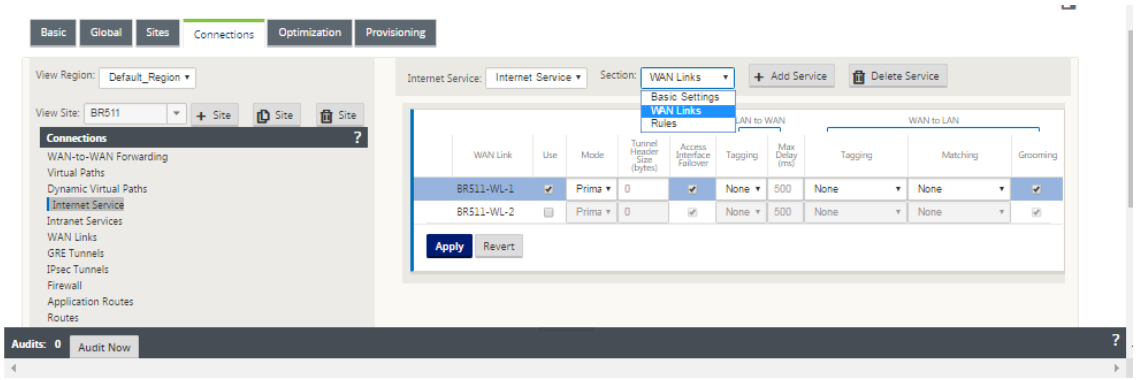
- Acceso a Internet del usuario invitado local
- Acceso a Internet entre empleados y usuarios para aplicaciones definidas
- Los usuarios de empleados pueden continuar con el bloqueo de cualquier otro tráfico al MCN
- Permitir al usuario agregar rutas específicas para dominios de redirección específicos.
- 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.

> **Nota**
>
> Para obtener más información, consulte cómo configurar VRF.

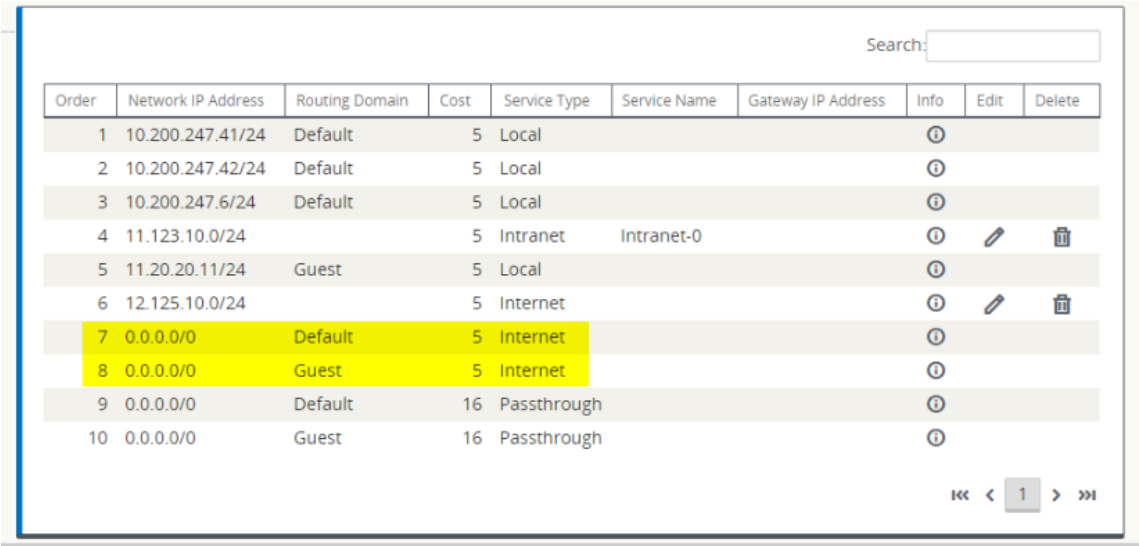
Para configurar servicios de Internet para todos los dominios de enrutamiento:

1. Crear servicio de Internet para un sitio. Vaya a **Conexiones** > **Ver región** > **Ver sitio** > [Nombre del sitio] > **Servicio Internet > Sección > Vínculos WAN** y, en Vínculos WAN, active la casilla de verificación **Usar**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> Debería ver que las rutas 0.0.0.0/0 agregadas, una por dominio de enrutamiento, en **Conexiones** > **Ver región** > **Ver sitio** >[Nombre del sitio] > **Rutas**.



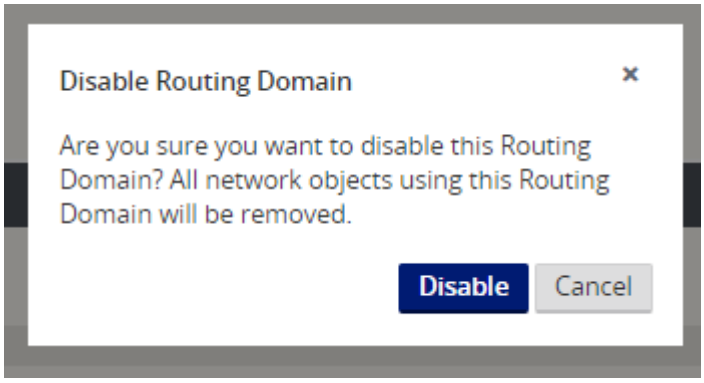
Search:

Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local					
2	10.200.247.42/24	Default	5	Local					
3	10.200.247.6/24	Default	5	Local					
4	11.123.10.0/24		5	Intranet	Intranet-0				
5	11.20.20.11/24	Guest	5	Local					
6	12.125.10.0/24		5	Internet					
7	0.0.0.0/0	Default	5	Internet					
8	0.0.0.0/0	Guest	5	Internet					
9	0.0.0.0/0	Default	16	Passthrough					
10	0.0.0.0/0	Guest	16	Passthrough					

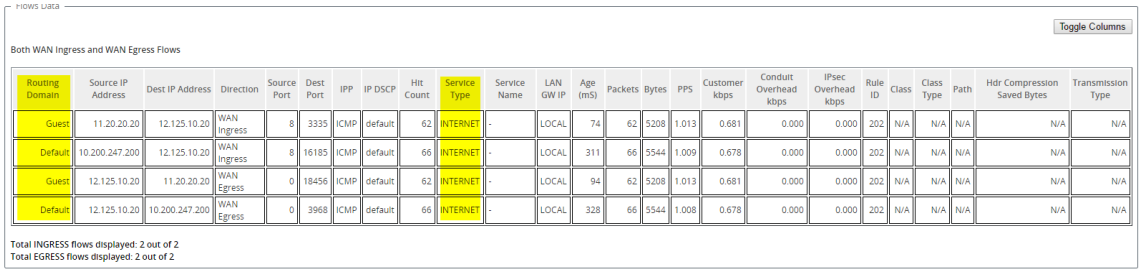
1

Ya no es necesario tener todos los dominios de redirección habilitados en el MCN.

2. Si inhabilita los dominios de redirección en el MCN, aparecerá el siguiente mensaje si los dominios están en uso en un sitio de sucursal:



3. Para confirmar que cada dominio de enrutamiento está utilizando el servicio de Internet, compruebe la columna Dominio de enrutamiento de la tabla Flujos de la interfaz de administración web en **Monitor** > **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. También puede comprobar la tabla de enrutamiento para cada dominio de enrutamiento en **Monitor** > **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, el enrutamiento y reenvío virtuales tenían 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 manera 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:

- Proporcione una infraestructura, en el sitio de 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 ruteo,
  - Se requiere una interfaz de acceso común y aceptable
  - Una interfaz de acceso para cada grupo con direcciones IP públicas independientes
- El tráfico para el empleado se puede enrutar directamente a Internet local (aplicaciones específicas)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

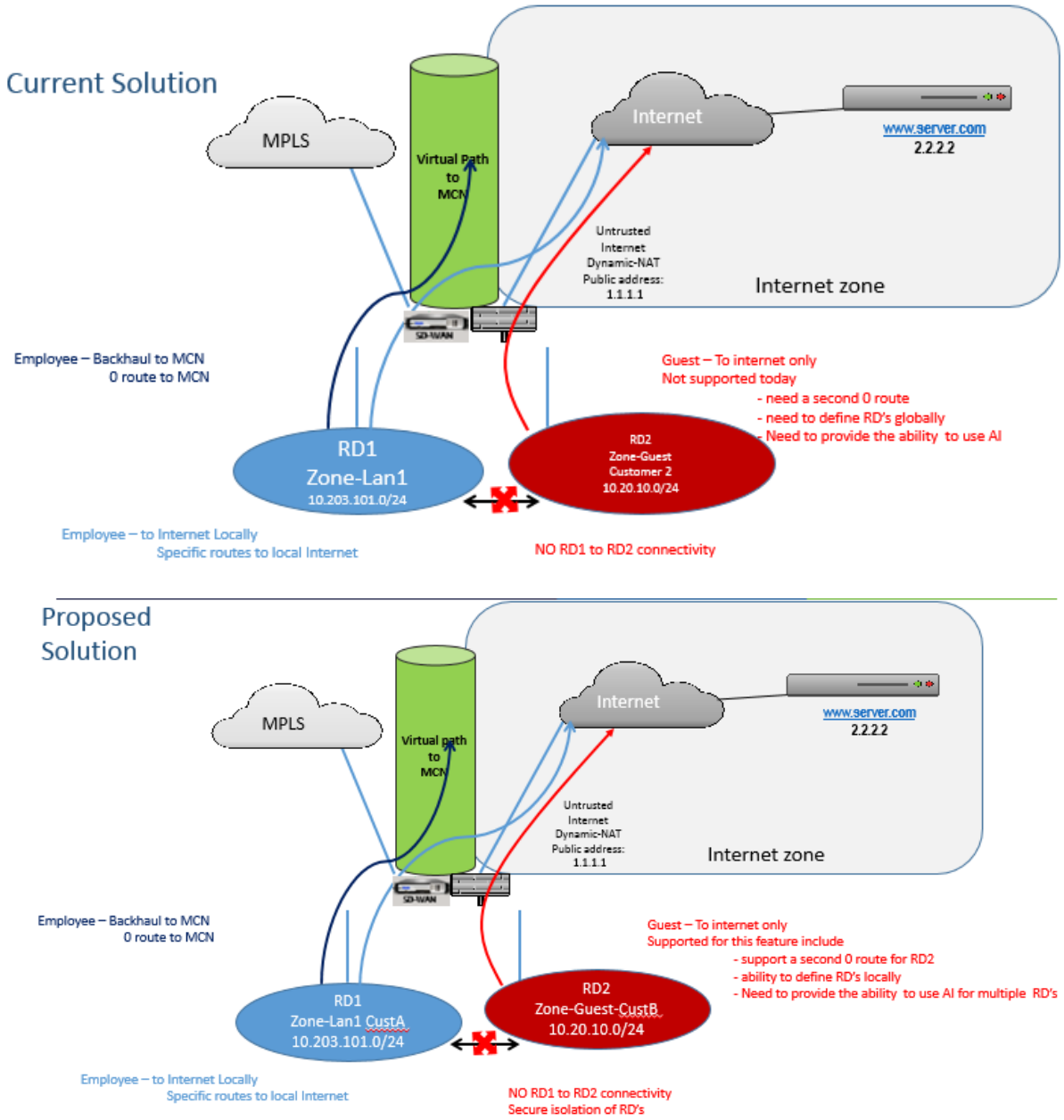
- El tráfico del empleado se puede enrutar o volver a enviar al MCN para un filtrado extenso (ruta 0)
- El tráfico para el dominio de redirección se puede enrutar directamente a Internet local (ruta 0)
- Admite rutas específicas por dominio de redirección, si es necesario
- Los dominios de redirección 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
- Le 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 RD diferente salga a Internet mediante la misma interfaz de acceso
- Permite configurar una interfaz de acceso diferente para cada RD
- Deben ser subredes únicas (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 de la cabecera de 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 enrutamiento agregado a un sitio.
- En **Sitios** > Nombre del sitio > **Enlaces WAN** > WL2[nombre] > **Interfaz de acceso**, asegúrese de que la casilla de verificación esté disponible y de que el servicio de Internet se haya definido correctamente. Si no puede activar la casilla de verificación, el servicio de Internet no está definido ni asignado a un enlace WAN para el sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Hasta 16 dominios de redirección por sitio.
- Interfaz de acceso (AI): IA única por subred.
- Las IA múltiples 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 enrutarse 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 enlaces WAN se comparten para el acceso a Internet.
- Sin QoS por dominio de enrutamiento; primero en llegar primero en servir.

Autenticación con certificados

May 7, 2021

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.

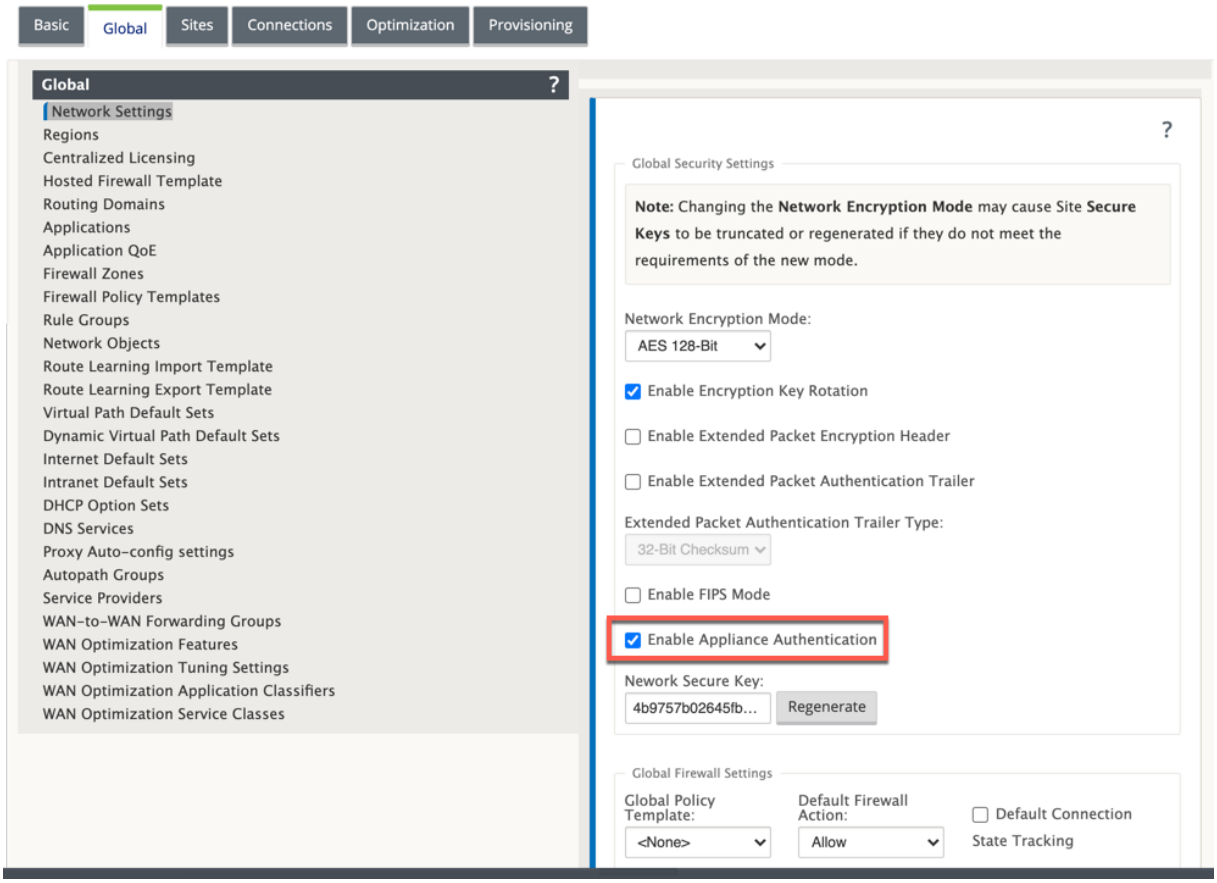
La autenticación de certificados permite a las organizaciones utilizar certificados emitidos por su entidad emisora de certificados (CA) privada para autenticar dispositivos. Los dispositivos se autentican antes de establecer las rutas virtuales. Por ejemplo, si un dispositivo de sucursal intenta conectarse 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 de acceso virtual.

El certificado emitido por la CA 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.

> **Nota**
>
> En la versión actual, los certificados de CA deben cargarse manualmente en todos los dispositivos de la red. La versión futura incluirá la distribución automática de los certificados de red.

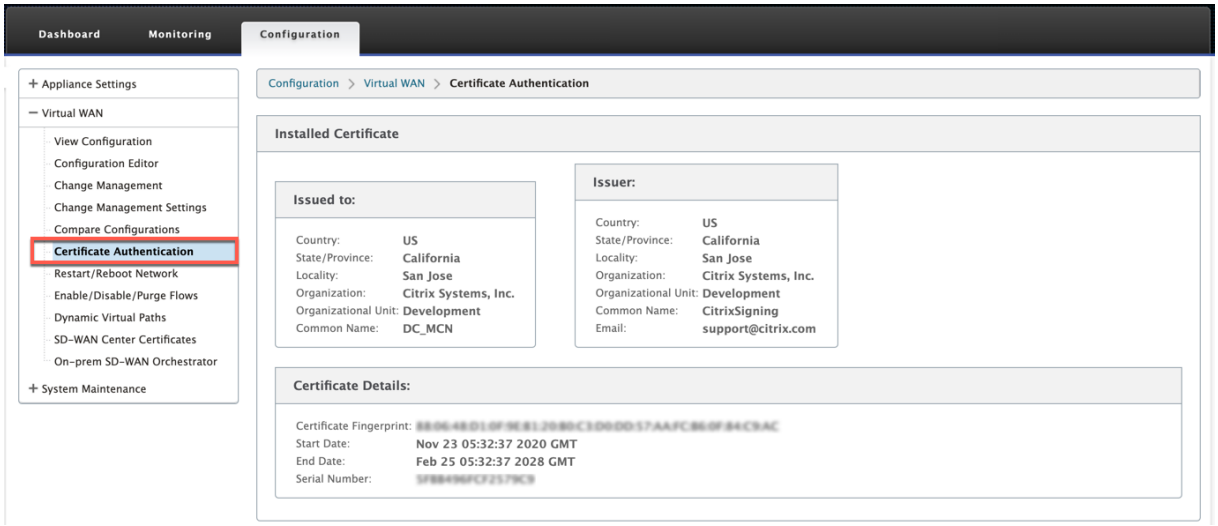
Para habilitar la autenticación del dispositivo, en el editor de configuración, vaya a **Global** > **Network Settings (Configuración de red**) y seleccione **Habilitar autenticación del dispositivo**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Una vez finalizada y aplicada la configuración, aparece una nueva opción de **autenticación de certificado** en **Configuración** > **WAN virtual**.

Puede administrar todos los certificados utilizados para la autenticación de rutas virtuales desde la página **Autenticación de certificados**.

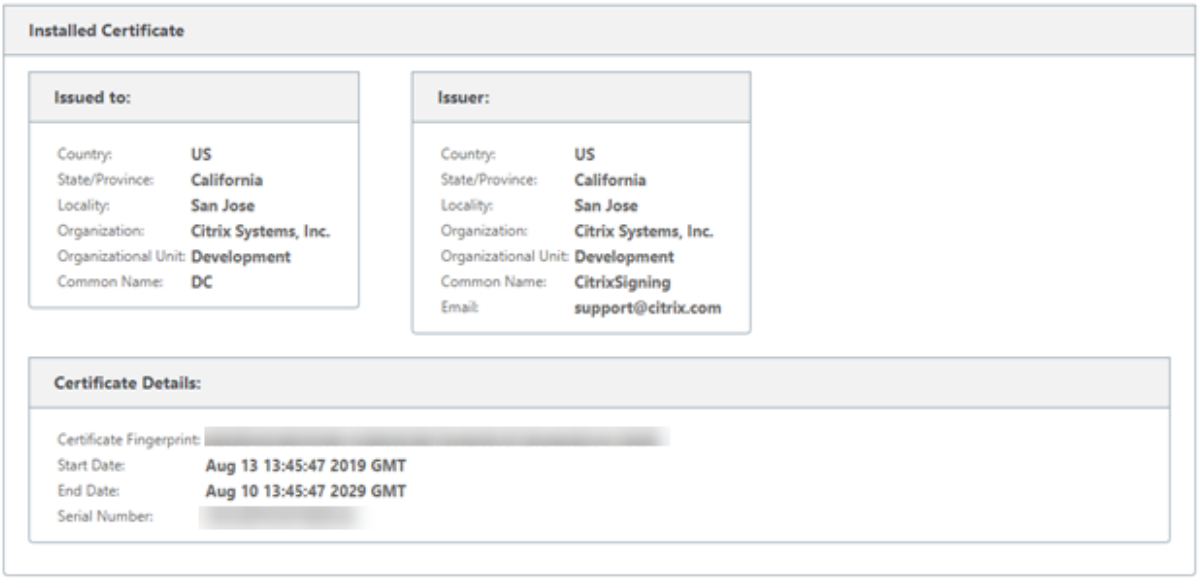


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Certificado instalado

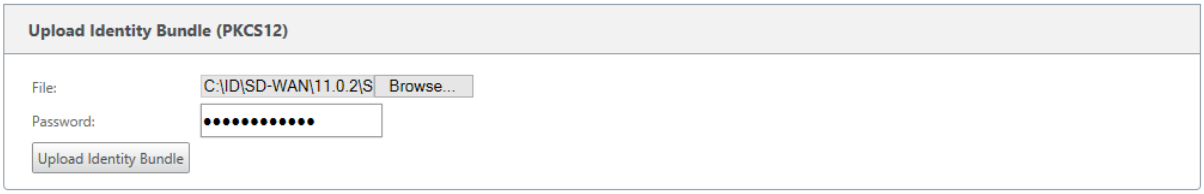
La sección **Certificado instalado** proporciona un resumen del certificado que está instalado en el dispositivo. El dispositivo utiliza este certificado para identificarse en la red.

La sección **Emitido a** proporciona detalles sobre a quién se le ha enviado el certificado. El **nombre común** del certificado coincide con el nombre del dispositivo, ya que el certificado está enlazado al nombre del dispositivo. La sección **Emisor** proporciona los detalles de la autoridad de firma de certificados, que firmó el certificado. Los detalles del certificado incluyen la huella digital del certificado, el número de serie y el período de validez del certificado.



Cargar paquete de identidad

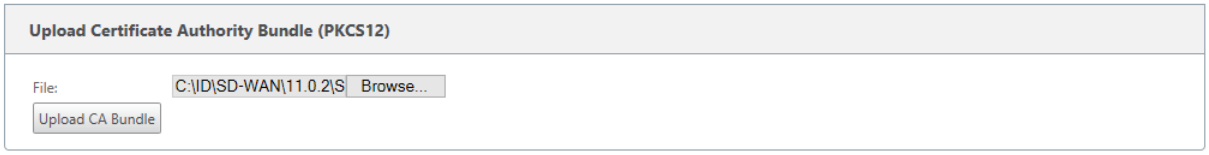
El paquete Identity incluye una clave privada y el certificado asociado a la clave privada. Puede cargar el certificado de dispositivo emitido por la CA en el dispositivo. El paquete de certificados es un archivo PKCS 12, con extensión.p12. Puede elegir protegerlo con una contraseña. Si deja el campo de contraseña en blanco, se tratará como sin protección con contraseña.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cargar paquete de entidad de certificación

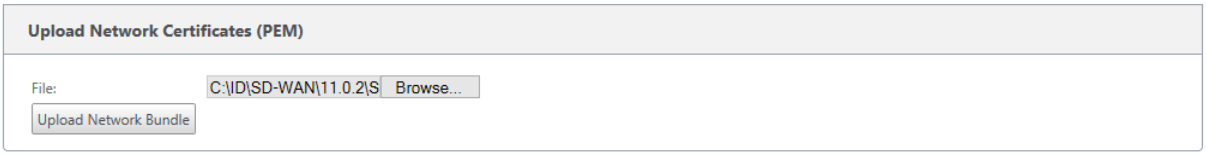
Cargue el paquete PKCS 12 que corresponde a la autoridad de firma de certificados. El paquete de la entidad emisora de certificados incluye la cadena completa de firmas, la raíz y toda la autoridad signataria intermedia.



Cargar certificados de red

Cargue todos los certificados de red concatenados juntos en un solo archivo.PEM. Los certificados de red deben cargarse en cada uno de los dispositivos de la red. Cuando un sitio inicia una conexión de ruta virtual, se envía al respondedor un mensaje que incluye su certificado. El respondedor comprueba el certificado del iniciador con el archivo PEM de certificados de red. Si el certificado del iniciador coincide con un certificado de la base de datos, se establece la conexión de ruta virtual.

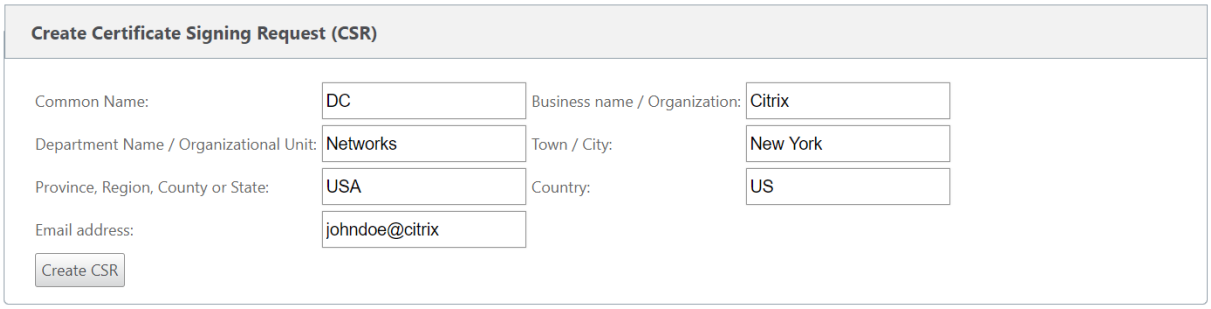
> **Nota**
>
> En la versión actual, los certificados de CA deben cargarse manualmente en todos los dispositivos de la red. La versión futura incluirá la distribución automática de los certificados de red.



Crear solicitud de firma de certificación

El dispositivo puede generar un certificado sin firmar y crear una solicitud de firma de certificado (CSR). A continuación, la entidad emisora de certificados puede descargar la CSR desde el dispositivo, firmarla y cargarla de nuevo en el dispositivo en formatos PEM o DER. Se utiliza como certificado de identidad para el dispositivo. Para crear una CSR para un dispositivo, proporcione el nombre común del dispositivo, los detalles de la organización y la dirección.

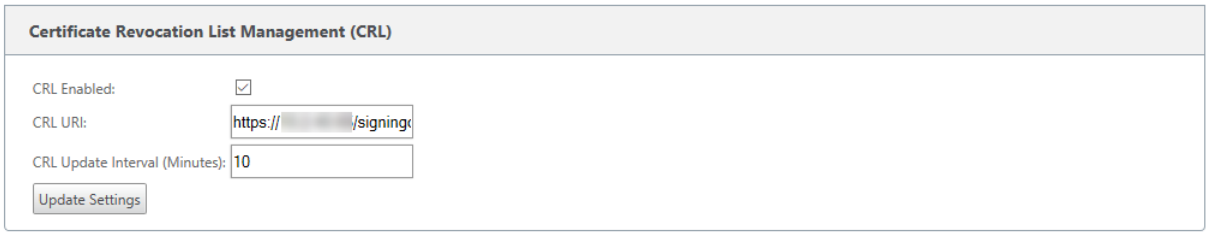
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Administrador de listas de revocación de certificados

Una lista de revocación de certificados (CRL) es una lista publicada de números de serie de certificados que ya no son válidos en la red. El archivo CRL se descarga periódicamente y se almacena localmente en todo el dispositivo. Cuando se autentica un certificado, el respondedor examina la CRL para ver si el certificado de iniciadores ya se revocó. Citrix SD-WAN admite actualmente CRL de la versión 1 en formato PEM y DER.

Para habilitar CRL, seleccione la opción CRL habilitada. Proporcione la ubicación en la que se mantiene el archivo CRL. Las ubicaciones HTTP, HTTPS y FTP son compatibles. Especifique el intervalo de tiempo para comprobar y descargar el archivo CRL, el intervalo es de 1 a 1440 minutos.



> **Nota**
>
> El período de reautenticación para una ruta de acceso virtua1 puede ser de 10 a 15 minutos, si el intervalo de actualización de CRL se establece en una duración más corta, la lista de CRL actualizada puede incluir un número de serie activo actualmente. Hacer que un certificado revocado activamente esté disponible en la red durante un corto período de tiempo.

AppFlow e IPFIX

September 26, 2023

AppFlow e IPFIX son estándares de exportación de flujo 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los datos recopilados, llamados registros de flujo, se transmiten a uno o más recopiladores IPv4. Los recopiladores agregan los registros de flujo y generan informes históricos o en tiempo real.

AppFlow

AppFlow exporta datos de nivel de flujo solo para conexiones HDX/ICA. Puede habilitar el TCP solo para la plantilla de conjunto de datos HDX o la plantilla de conjunto de datos HDX. El TCP para el conjunto de datos HDX proporciona.datos de salto múltiple El conjunto de datos HDX proporciona.Datos de información HDX

> **Nota**
>
> La plantilla HDX solo está disponible para Citrix SD-WAN PE edition y dispositivos de dos cajas. Debe habilitarse en el dispositivo del centro de datos.

AppFlow Collectors 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.

IPFIX versión 10 es compatible con Citrix SD-WAN versión 10 versión 2 y superior.

Hay algunos cambios en la arquitectura, lo que resulta en un bajo impacto en el rendimiento cuando Net Flow, AppFlow e IPFIX se habilitan juntos a medida que estos recursos de protocolo reutilizan.

Limitaciones

- 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 todos los datos se vuelven a transmitir. Si el intervalo de exportación se establece en X minutos, el dispositivo solo almacena X minutos de datos. Que se retransmite después de X minutos de pérdida de conexión.
- En Citrix SD-WAN, versión 10 2, la configuración de **AppFlow** se hace local para cada dispositivo, mientras que en las versiones anteriores era una configuración global. Si la versión del software

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

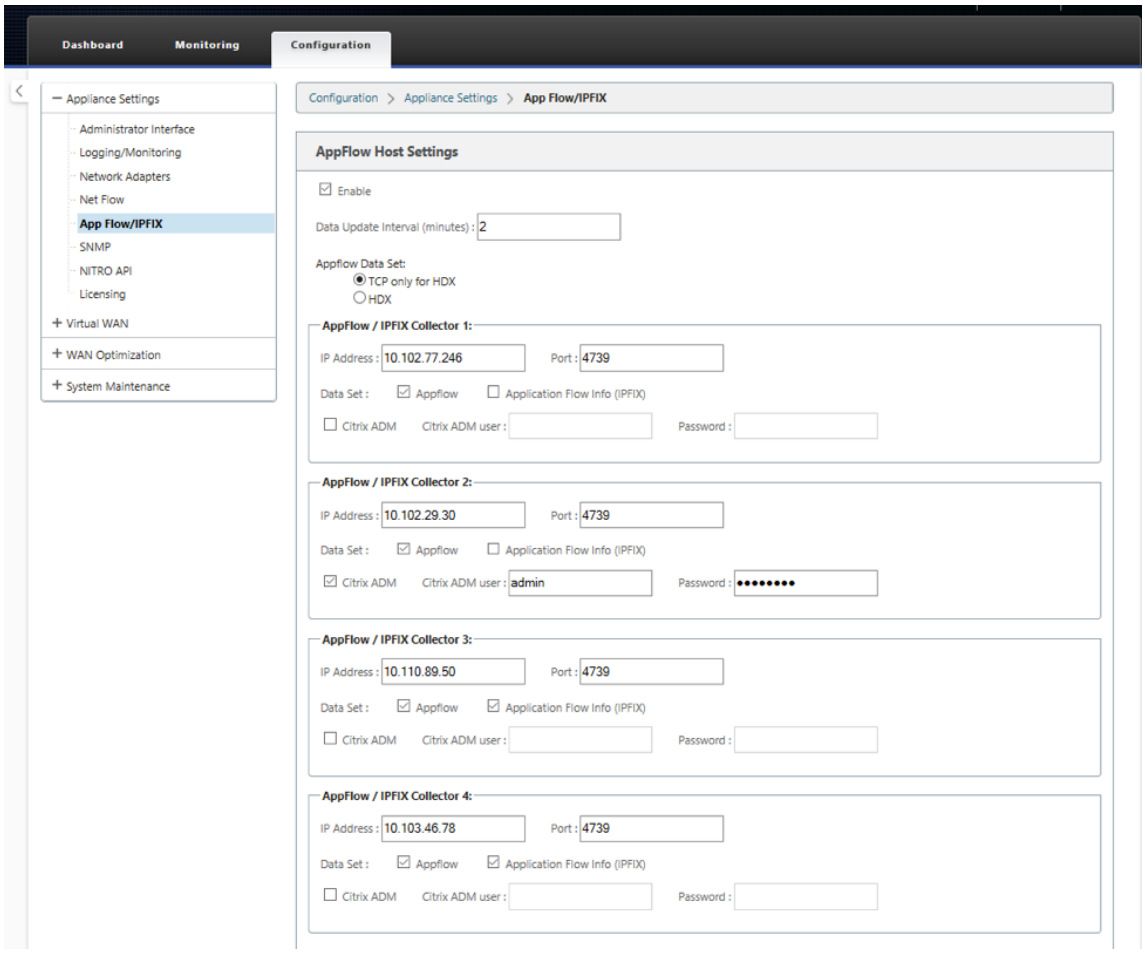
SD-WAN se rebaja a cualquiera de las versiones anteriores y si AppFlow está configurado en cualquiera de los dispositivos, se aplicará globalmente a todas las alianzas.

Configuración de AppFlow/IPFix

Puede configurar AppFlow/IPFIX en dispositivos SD-WAN individuales o configurarlo en SD-WAN Center e insertar la configuración en un grupo de dispositivos.

Para configurar AppFlow/IPFIX en dispositivos SD-WAN:

1. En la interfaz web SE/PE de Citrix SD-WAN, vaya a **Configuración > AppFlow/IPFix**.
2. Haga clic en **Habilitar**.



3. En el campo **Intervalo de actualización de datos**, especifique el intervalo de tiempo, en minutos, en el que se exportan los informes de flujo al recopilador AppFlow/IPFix. El intervalo máximo es de 10 minutos.
4. Seleccione la plantilla de **conjunto de datos de AppFlow**, puede elegir una de las siguientes plantillas de conjunto de datos:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **TCP solo para HDX (AppFlow)**: La plantilla de conjunto de datos de AppFlow para recopilar y enviar datos de varios saltos de conexiones ICA al recopilador AppFlow.
- **HDX (AppFlow)**: La plantilla de conjunto de datos de AppFlow para recopilar y enviar datos de información HDX de conexiones ICA al recopilador AppFlow.

> **Nota**
>
> La plantilla **HDX** solo está disponible para dispositivos Citrix SD-WAN PE y Two Box.

5. Puede configurar hasta cuatro colectores AppFlow/IPFIX. Para cada selector, especifique los parámetros siguientes:

   - **Dirección IP**: Dirección IP del sistema colector AppFlow/IPFIX externo.
   - **Puerto**: Número de puerto en el que escucha el sistema recopilador AppFlow/IPFIX externo. El valor predeterminado es 4739.
   - **Información de flujo de aplicaciones (IPFIX)**: La plantilla IPFIX para recopilar y enviar registros de flujo de todas las conexiones al recopilador IPFIX.
   - **Citrix ADM**: Seleccione esta opción para usar Citrix ADM como recopilador de AppFlow.

   > **Nota**
   >
   > Actualmente, Citrix ADM no admite la recopilación IPFIX.

   - **Usuario de Citrix ADM**: Nombre de usuario del recopilador de Citrix ADM
   - **Contraseña**: Contraseña del recopilador Citrix ADM.

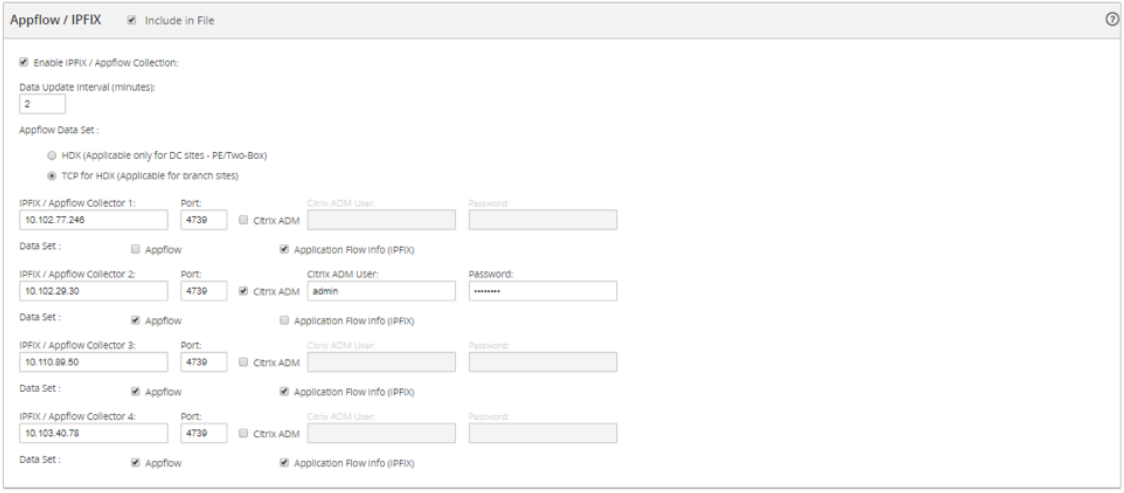
   El nombre de usuario y la contraseña se utilizan para iniciar sesión sin problemas en Citrix ADM y almacenar datos de flujo.

6. Haga clic en **Aplicar configuración**.

Para configurar el recopilador **AppFlow/IPFIX** mediante Citrix SD-WAN Center:

1. En la interfaz de usuario de administración de Citrix SD-WAN Center, vaya a **Configuración > Configuración > Configuración del equipo**.
2. Vaya a la sección **AppFlow/IPFIX** y elija **Incluir en archivo**.
3. Seleccione **Habilitar colección IPFIX/AppFlow**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. En el campo **Intervalo de actualización de datos**, especifique el intervalo de tiempo, en minutos, en el que se exportan los informes de AppFlow al recopilador AppFlow/IPFIX.

5. Seleccione la plantilla de **conjunto de datos de AppFlow**, puede elegir una de las siguientes plantillas de conjunto de datos:

   - **TCP solo para HDX**: La plantilla de conjunto de datos de AppFlow para recopilar y enviar datos de varios saltos de conexiones ICA al recopilador AppFlow.
   - **HDX**: La plantilla de conjunto de datos de AppFlow para recopilar y enviar datos de información HDX de conexiones ICA al recopilador AppFlow.

   > **Nota**
   >
   > La plantilla **HDX** solo está disponible para dispositivos Citrix SD-WAN PE y Two Box.

6. Puede configurar hasta cuatro colectores AppFlow/IPFIX. Para cada selector, especifique los parámetros siguientes:

   - **IPFIX/AppFlow Collector**: La dirección IP del sistema externo AppFlow/IPFIX.
   - **Puerto**: Número de puerto en el que escucha el sistema recopilador AppFlow/IPFIX externo. El valor predeterminado es 4739.
   - **Información de flujo de aplicaciones**: La plantilla IPFIX para recopilar y enviar registros de flujo de todas las conexiones al recopilador IPFIX.
   - **Citrix ADM**: Seleccione esta opción para usar Citrix ADM como recopilador de AppFlow.

     > **Nota**
     >
     > Actualmente, Citrix ADM no admite la recopilación IPFIX.

   - **Usuario de Citrix ADM**: Nombre de usuario del recopilador de Citrix ADM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Contraseña**: Contraseña del recopilador Citrix ADM.

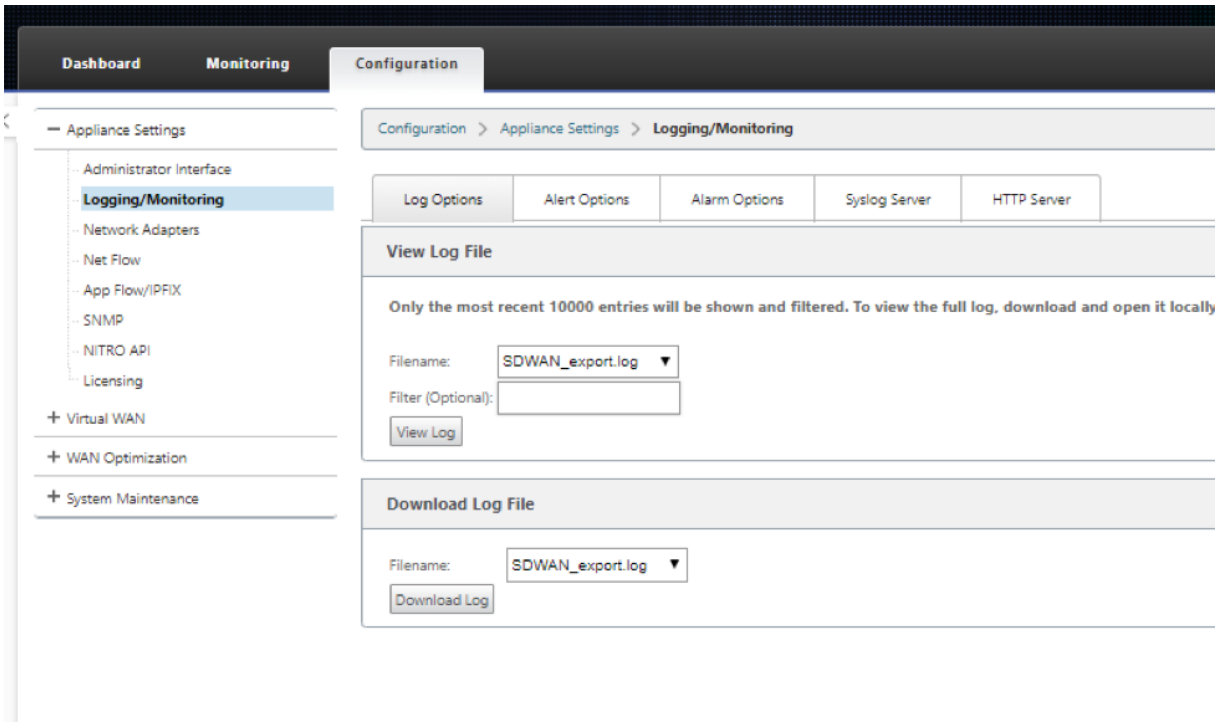
  El nombre de usuario y la contraseña se utilizan para iniciar sesión sin problemas en Citrix ADM y almacenar datos de flujo.

7. **Guarde** y **exporte** la configuración a los dispositivos administrados.

> **Nota**
>
> Si la versión SD-WAN Center es inferior a 10.2 y la versión de dispositivos SD-WAN es 10.2 o superior, puede observar las siguientes condiciones.
>
> - Si los recopiladores locales están habilitados en los dispositivos, la configuración AppFlow/IPFIX introducida desde SD-WAN Center no afecta a la configuración existente.
> - Si los recopiladores locales no están habilitados en los dispositivos, la configuración de AppFlow/IPFix introducida desde SD-WAN Center se aplicará al dispositivo.
> - Si la configuración global AppFlow/IPFix está habilitada en la configuración SD-WAN Center, todos los recopiladores locales están habilitados en los dispositivos.

Archivos de registros

Para solucionar problemas relacionados con los protocolos de exportación 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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SNMP

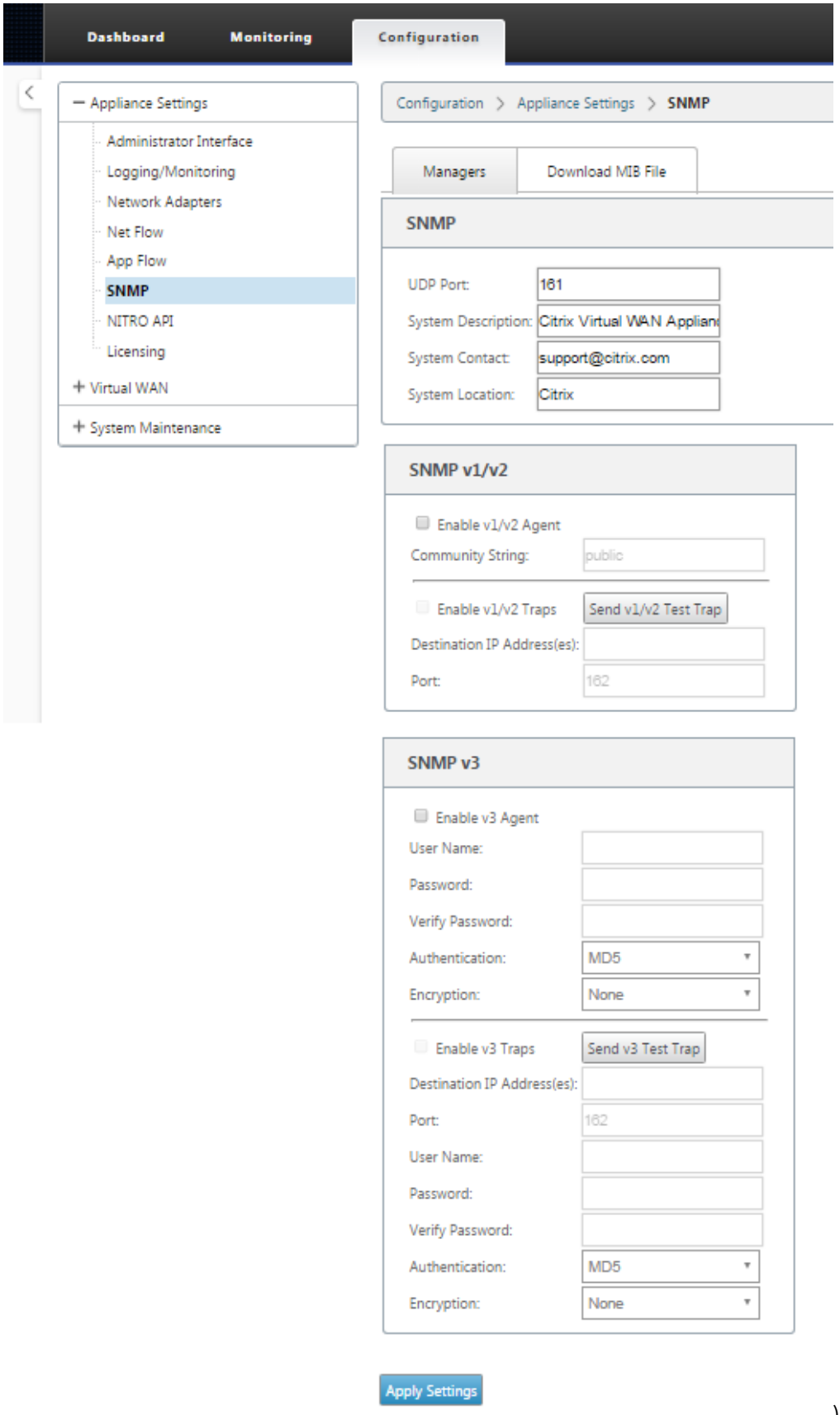
November 16, 2022

Citrix SD-WAN admite la capacidad SNMPV1/V2 y solo una cuenta de usuario única para cada función SNMPv3. Esta restricción proporciona las siguientes ventajas:

- Garantizar la conformidad con SNMPv3 para 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 equipo** -> **SNMP** y rellene los campos según sea necesario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Compatibilidad con MIB estándar

Los dispositivos SD-WAN admiten las siguientes MIB estándar.

MIB	RFC (Enlace de definición)
DISMAN-EVENT-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:

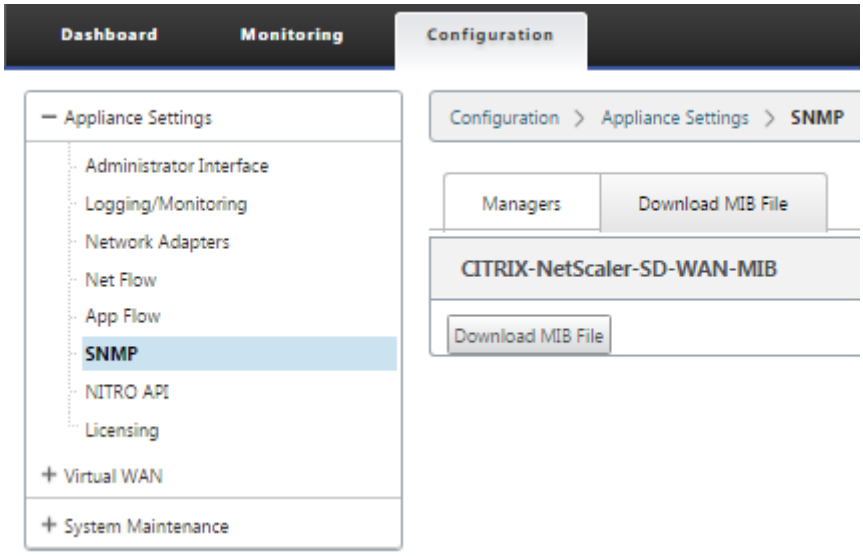
- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

Los administradores SNMPv3 y los detectores de capturas 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Vaya a **la página Configuración** > **Configuración del equipo** > **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 de daemon snmpd **net-snmp snmpd** proporciona soporte para estos MIB de forma predeterminada en sistemas Linux. Los MIB proporcionan la base para admitir aplicaciones de administración de red.
> - Los contadores de bytes y paquetes de puerto Ethernet están en **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.

Para obtener información adicional sobre cómo agregar el administrador SNMP, configurar SNMP View/Alarm y agregar servidor SNMP, consulte la documentación de CloudBridge 7.4 en:CloudBridge

Optimización WAN

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El dispositivo Citrix SD-WAN WANOP optimiza los vínculos WAN, lo que garantiza la máxima capacidad de respuesta y rendimiento. Los dispositivos WANOP de Citrix SD-WAN funcionan en pares, uno en cada extremo de un enlace, para acelerar el tráfico a través del enlace. Las siguientes son algunas de las funciones de Citrix SD-WAN WANOP:

- Compresión
- Aceleración del protocolo TCP
- Administración del tráfico
- Aceleración de aplicaciones
- Aceleración de Citrix XenApp/XenDesktop (HDX)
- Integración
- Supervisión y Gestión

Para obtener información acerca de la instalación, implementación y configuración de características de Citrix SD-WAN WANOP 10.2, consulte la Citrix SD-WAN WANOP documentación. Las funciones y procedimientos de Citrix SD-WAN WANOP 10.2 son similares a los procedimientos documentados en la versión WANOP de Citrix SD-WAN.

Puede habilitar y configurar la función de optimización de WAN en su Citrix SD-WAN Premium Edition. Para obtener más información, consulte Citrix SD-WANPremium Edition.

Puede lograr la aceleración de la red en cualquier portátil o estación de trabajo remoto con Windows mediante el software WANOP Client Plug-in. Para obtener más información, consulte Plug-in de cliente WANOP.

Citrix SD-WAN Premium Edition

May 7, 2021

La sección proporciona instrucciones paso a paso para habilitar y configurar las funciones de optimización WAN de SD-WAN Premium (Enterprise) Edition para su WAN virtual. Para ello, utilice los formularios de sección **Optimización** en el **Editor de configuración** de la Interfaz de administración Web en el MCN.

> **Nota**
>
> Debe tener instalada una licencia SD-WAN Premium (Enterprise) Edition para acceder, habilitar, configurar y activar las funciones de optimización WAN en su WAN virtual. SD-WAN Standard Edition no admite estas funciones.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hay dos pasos de nivel superior para configurar los conjuntos y parámetros de la sección **Optimización**. Estos son los siguientes, enumerados en orden de dependencia:

1. Habilite la optimización WAN y personalice la configuración **predeterminada** o acepte los valores predeterminados.

   La configuración **predeterminada** se utiliza como la configuración de **optimización** base para todos los sitios aptos para la optimización WAN. La configuración **predeterminada** viene preconfigurada y se puede personalizar.

   > **Nota**
   >
   > Para obtener instrucciones, consulte Habilitación de Optimización y Configuración de Valores por Defecto.

2. (Opcional) Personalice la configuración de optimización WAN para cada uno de los sitios de sucursal individuales o acepte los **conjuntos y valores predeterminados para cada uno de ellos.**

   De forma predeterminada, la configuración **predeterminada** se aplica inicialmente a cada sitio de sucursal que sea elegible para la optimización WAN. La optimización WAN solo se admite para dispositivos de hardware 1000-EE (edición premium) y 2000-EE (edición premium). Para cada sitio de sucursal admitido, puede optar por aceptar o modificar cualquier combinación de los conjuntos y **valores predeterminados**, o cualquier subconjunto de estos. Para obtener instrucciones, consulte Configuración de Optimización para un Sitio de Sucursal.

   Para completar estos pasos, utilice los formularios de configuración de la sección **Optimización** del **Editor de configuración**. La sección **Optimización** se organiza de la siguiente manera:

   - **Valores predeterminados**: La sucursal **Valores predeterminados** contiene las siguientes sucursales secundarias, que a su vez contienen uno o más formularios para configurar sus respectivos conjuntos y configuraciones:
     - **Funciones por defecto**
     - **Valores predeterminados Configuración de ajuste**
     - **Valores predeterminados Clasificadores de aplicaciones (conjunto)**
     - **Clases de servicio predeterminadas** (set)
   - **<Client Site Name>**: El árbol de configuración de la sección **Optimización** contiene una sucursal para cada nodo cliente (sitio de sucursal) que admite la optimización WAN. Si un nodo de cliente es un modelo de dispositivo no compatible, el sitio no se incluirá en el árbol de configuración de la sección **Optimización**. Cada sucursal del árbol contiene las siguientes sucursales secundarias, que a su vez contienen una o más formas para configurar sus respectivos conjuntos y configuraciones:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Funciones por defecto**
- **Valores predeterminados Configuración de ajuste**
- **Clasificadores de aplicaciones predeterminados** (conjunto)
- **Clases de servicio predeterminadas** (set)

La siguiente sección proporciona instrucciones para habilitar la optimización WAN para su WAN virtual y configurar los conjuntos y **valores predeterminados**.

Habilitar la optimización y configurar los ajustes de entidad predeterminados

May 7, 2021

Habilitar la optimización WAN en su WAN virtual implica los siguientes procedimientos:

1. Habilite la optimización WAN en la configuración de **Funciones** de la **sección Optimización.**

   En esta sección se proporcionan instrucciones para esta parte del proceso.

2. Configure la configuración de directiva **Aceleración** para cada clase de servicio aplicable en la tabla **Clases de servicio**.

   Este procedimiento se produce más adelante, después de haber completado el resto de la configuración de **Optimización**. Las instrucciones se proporcionan en la sección.Configuración de Clases de Servicio Predefinidas de Optimización En este punto, la optimización WAN se ha habilitado en su configuración, pero aún no se ha activado ni activado en su WAN virtual. Para habilitar y activar la Optimización de WAN en su WAN virtual, debe completar la configuración de WAN virtual y, a continuación, generar, organizar y activar los Paquetes de Virtual WAN Appliance en los sitios aptos de su implementación, como se describe en los capítulos siguientes de esta guía.

   Para habilitar la optimización WAN y configurar la sección **Valores predeterminados** Configuración de **funciones**, haga lo siguiente:

   a) Si es necesario, vuelva a iniciar sesión en la Interfaz Web de administración y abra el **Editor de configuración.**

      Para abrir el **Editor de configuración**, haga lo siguiente:

      i. Seleccione la ficha **Configuración** en la parte superior de la página para abrir el árbol de navegación **Configuración** (panel izquierdo).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ii. En el árbol de navegación, haga clic en **+** a la izquierda de la sucursal **WAN virtual** para abrir esa sucursal.

iii. En la rama **WAN virtual**, seleccione **Editor de configuración.**

b) Abra el paquete de configuración que quiera modificar.

Haga clic en **Abrir** para mostrar el cuadro de diálogo **Abrir paquete de configuración** y seleccione el paquete en el menú implementable **Paquetes guardados**.

Esto carga el paquete seleccionado en el **Editor de configuración** y lo abre para su edición.
Si tiene una licencia válida y actual que incluye funciones de Optimización de WAN, la sección **Optimización** está disponible en el **Editor de configuración**.

> **Nota**
>
> Si la sección **Optimización** no está disponible, compruebe que ha instalado una licencia SD-WAN Premium (Enterprise) Edition en su Virtual WAN. SD-WAN Standard Edition no admite las funciones de optimización WAN.

Para obtener más información e instrucciones, consulte las siguientes secciones:

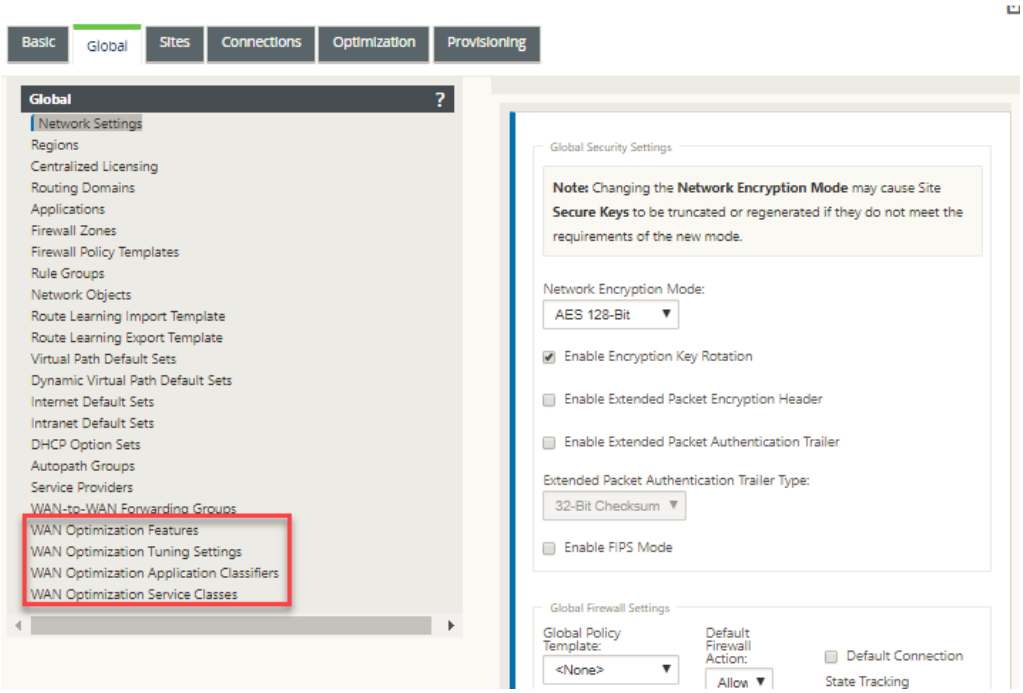
- Las ediciones SD-WAN
- Licencias

c) Haga clic en la ficha **Global**.

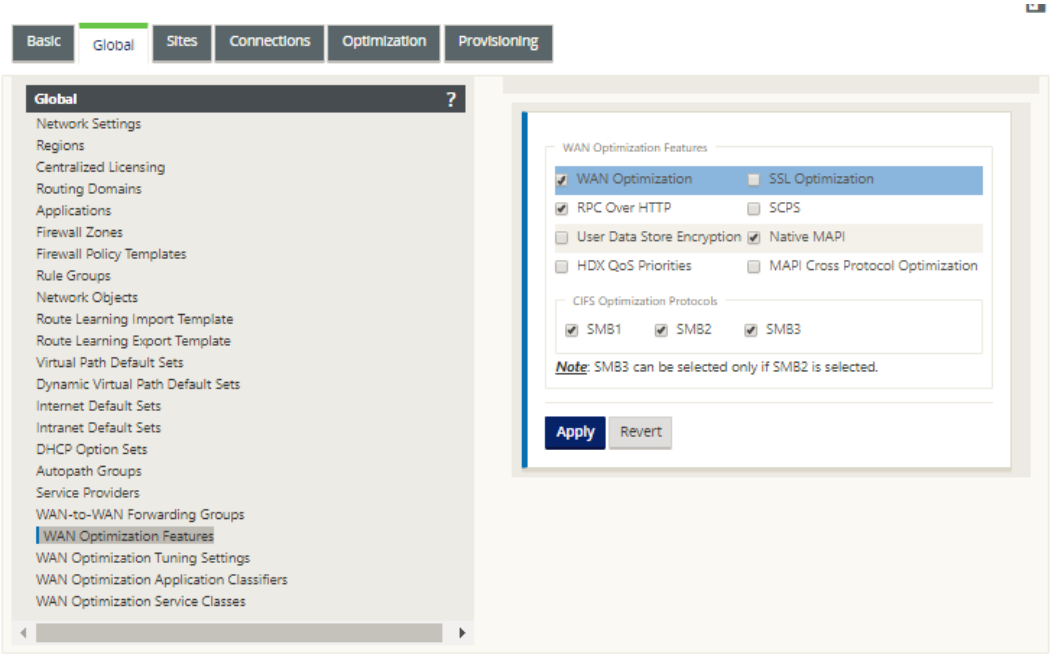
Puede configurar los siguientes valores predeterminados para la optimización WAN desde la ficha **Global**.

- Funciones de optimización WAN
- Configuración de optimización WAN
- Clasificadores de aplicaciones de optimización WAN
- Clase de servicio de optimización WAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



d) Haga clic en **Funciones de optimización WAN**.



e) Active la casilla de verificación **Optimización de WAN**.

La casilla de verificación **Optimización de WAN** se encuentra en la esquina superior izquierda de la sección **Funciones** de **optimización de WAN**. Esto habilita la edición del formulario y revela los botones **Aplicar** y **Revertir**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> Esto selecciona esta función para habilitar. La optimización WAN no se habilitará en la sección **Optimización** o en el paquete de configuración hasta que haga clic en **Aplicar,** después de completar la configuración de **funciones**. Además, también debe configurar la opción **Aceleración** para cada clase de servicio aplicable en la tabla Clases de servicio, como se indica más adelante en el proceso de configuración de **Optimización**. (Las instrucciones se proporcionan en la sección Configuración de Clases de Servicio Predefinidas de Optimización) Finalmente, la optimización de WAN no se activará ni activará en su WAN virtual hasta que haya completado toda la configuración de WAN virtual y, a continuación, generado, organizado, distribuido y activado los paquetes de Virtual WAN Appliance en los sitios elegibles de su WAN Virtual.

f) Configure los ajustes de **Funciones**.

Haga clic en una casilla de verificación para seleccionar o anular la selección de una opción. Puede aceptar la configuración predeterminada preseleccionada en el formulario o personalizar la configuración.

> **Nota**
>
> De forma predeterminada, la configuración que configure en la ficha **Global** se aplica automáticamente a cada sitio de sucursal incluido en el árbol. Sin embargo, puede personalizar la configuración de **Optimización** para una sucursal específica, como se describe en la sección Configuración de Optimización para un Sitio de Sucursal.

El formulario de configuración de **funciones** contiene dos secciones:

- **Funciones de optimización WAN**
- **Protocolos de optimización CIFS**

La configuración de **las funciones de optimización WAN** es la siguiente:

- **Optimización de WAN** : active la casilla de verificación para habilitar Optimización de WAN para esta configuración. Esto también permite la compresión, la deduplicación y la optimización del protocolo TCP.

  > **Nota**
  >
  > Se debe seleccionar la opción Optimización WAN para que las demás opciones de la sección Optimización estén disponibles.

- **SCPS** : active la casilla de verificación para habilitar la optimización del protocolo TCP para los vínculos de satélite.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Prioridades de QoS de HDX** : active la casilla de verificación para habilitar la optimización del tráfico ICA en función de la priorización de subcanales HDX.
- **Optimización de protocolo cruzado MAPI** : active la casilla de verificación para habilitar la optimización cruzada del tráfico de Microsoft Outlook (MAPI).
- **Optimización SSL** : active la casilla de verificación para habilitar la optimización de flujos de tráfico con cifrado SSL.
- **RPC sobre HTTP:** active la casilla de verificación para habilitar la optimización del tráfico de Microsoft Exchange que utiliza RPC a través de HTTP.
- **Cifrado de almacén de datos de usuario:** active la casilla de verificación para habilitar la seguridad mejorada de los datos mediante el cifrado del historial de compresión de optimización de WAN.
- **MAPI nativo** : active la casilla de verificación para habilitar la optimización del tráfico de Microsoft Exchange.

  Las opciones de **los protocolos de optimización CIFS** son las siguientes:

  - **SMB1** : active la casilla de verificación para habilitar Optimización del uso compartido de archivos de Windows (SMB1)
  - **SMB2** : active la casilla de verificación para habilitar Optimización del uso compartido de archivos de Windows (SMB2)
  - **SMB3** : active la casilla de verificación para habilitar Optimización del uso compartido de archivos de Windows (SMB3). Primero debe seleccionar la opción **SMB2** para poder seleccionar **SMB3**.

g) Haga clic en **Aplicar** para activar y agregar las **características predeterminadas** seleccionadas al paquete de configuración.

El siguiente paso es configurar los **ajustes** predeterminados de **optimización**.

Configurar los ajustes predeterminados de optimización

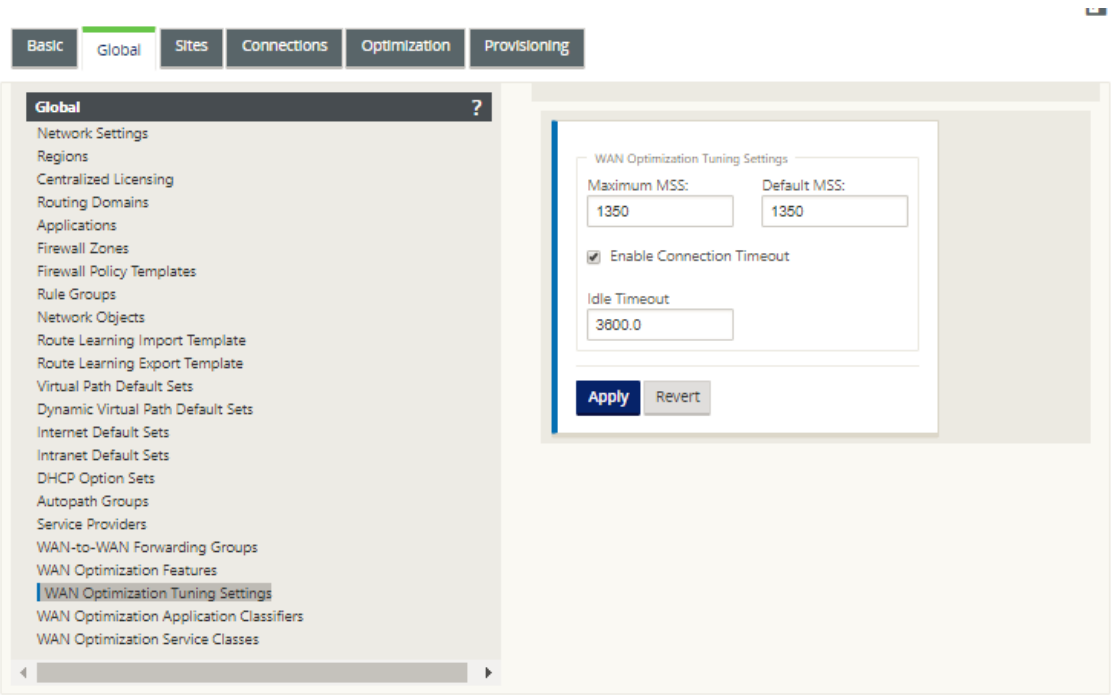
May 7, 2021

Puede configurar los ajustes predeterminados de optimización WAN en la ficha **Global**.

Para configurar los **ajustes**predeterminados de optimización WAN, haga lo siguiente:

1. En la ficha **Global**, haga clic en **Configuración de optimización WAN**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Seleccione y configure los **ajustes de ajuste**.

   Las opciones **Ajustes de ajuste** son las siguientes:

   - **MSS máximo**: Introduzca el tamaño máximo (en bytes) para el tamaño máximo de segmento (MSS) de un segmento TCP.
   - **MSS predeterminado**: Introduzca el tamaño predeterminado (en octetos) para el MSS para los segmentos TCP.
   - **Activar tiempo de espera de conexión**: Seleccione esta opción para habilitar la terminación automática de una conexión cuando se supere el umbral inactivo.
   - **Tiempo de espera inactivo**: Introduzca un valor de umbral (en segundos) para especificar la cantidad de tiempo de inactividad permitido antes de que finalice una conexión inactiva. Primero debe seleccionar **Activar tiempo de espera de conexión** para poder configurar este campo.

3. Haga clic en **Aplicar**.

   Esto aplica los **ajustes de ajuste** modificados a la configuración global.

   El siguiente paso es configurar el conjunto predeterminado de Clasificadores de aplicaciones de optimización WAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurar los clasificadores de aplicaciones predeterminados de optimización

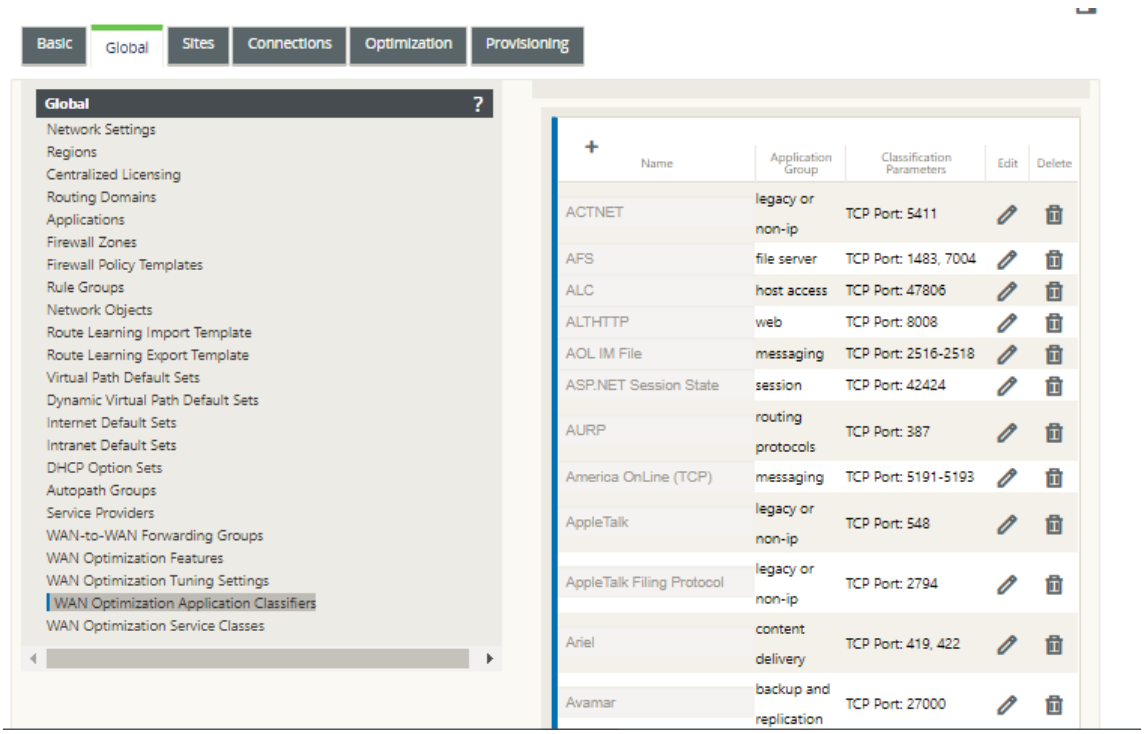
May 7, 2021

Puede configurar la configuración predeterminada del clasificador de aplicaciones de optimización WAN en la ficha **Global**.

Para configurar el conjunto predeterminado de Clasificadores de aplicaciones de optimización WAN, haga lo siguiente:

1. En la ficha **Global**, haga clic en **Clasificadores de aplicaciones de optimización WAN**.

   Esto abre la tabla **Clasificadores de aplicaciones**, que muestra el conjunto predeterminado de Clasificadores de aplicaciones.



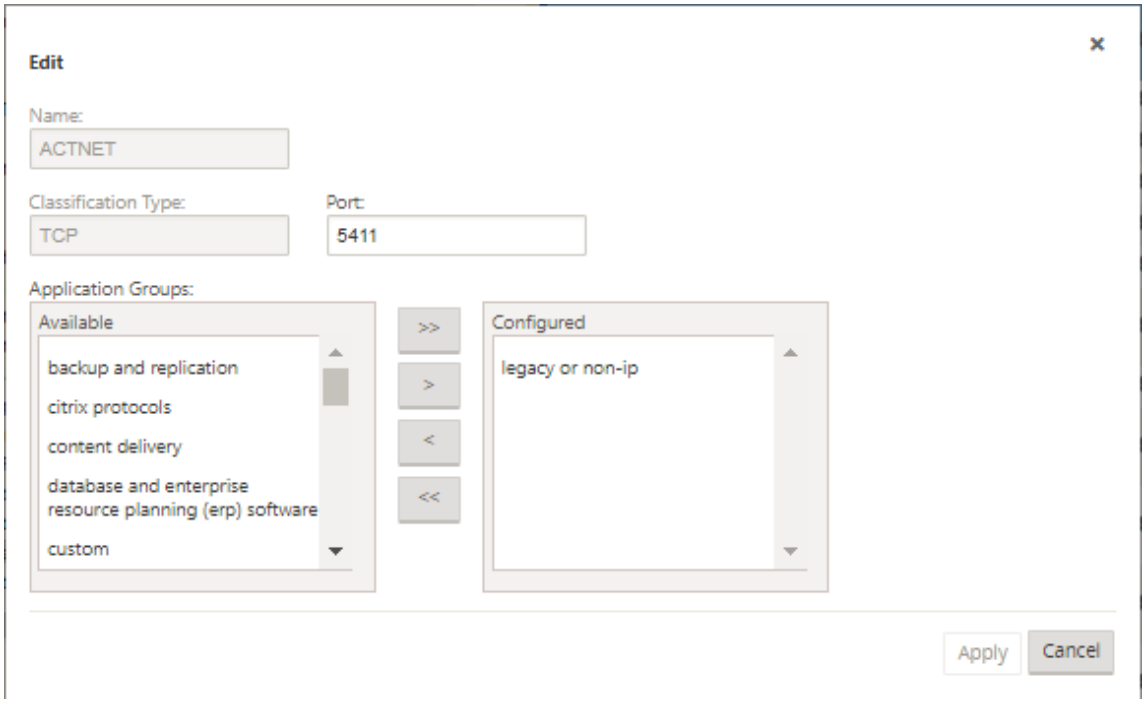
   Esta tabla es también un formulario de configuración. Puede utilizar este formulario para configurar (modificar), eliminar y agregar clasificadores de aplicaciones para crear un conjunto predeterminado personalizado. El conjunto de **Clasificadores de aplicaciones** predeterminado modificado y la configuración del Clasificador de aplicaciones individual que configure se aplican automáticamente como valores predeterminados a cualquier sitio de sucursal incluido en el árbol de sección **Optimización**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> También puede personalizar el conjunto de **Clasificadores de aplicaciones** y la configuración de cada sitio de sucursal específico. Para obtener instrucciones, consulte la sección Configuración de Optimización para un Sitio de Sucursal.

2. Para configurar un Clasificador de aplicaciones existente, haga clic en Modificar (icono de lápiz), en la columna **Modificar** de esa entrada del clasificador.

   Esto abre un formulario emergente **Modificar** configuración para configurar el Clasificador de aplicaciones seleccionado.



3. En el campo **Puerto**, introduzca el número de puerto para el Clasificador de aplicaciones o acepte el valor predeterminado.

4. Agregue o quite grupos de aplicaciones en la lista **Configurado** o acepte los valores predeterminados.

   - **Para agregar un grupo de aplicaciones a la lista**: Selecciónelo en la lista **Grupos de aplicaciones**de la izquierda y, a continuación, haga clic en la flecha Agregar a la derecha (>) para agregar el grupo a la lista **Configurado**de la derecha. Para agregar todos los **grupos de aplicaciones** a la lista a la vez, haga clic en la flecha doble derecha Agregar todo (»).

   - **Para quitar un grupo de aplicaciones de la lista**: Selecciónelo en la lista **Configurado**de la derecha y, a continuación, haga clic en Eliminar flecha izquierda (<). Para quitar todos los **grupos de aplicaciones** de la lista a la vez, haga clic en la flecha izquierda doble Eliminar todo («).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Haga clic en **Aplicar**.

   Esto aplica los cambios en el Clasificador de aplicaciones y descarta el formulario **Modificar** configuración.

6. (Opcional) Personalice el conjunto de **clasificadores de aplicaciones** predeterminado.

   Puede agregar o eliminar clasificadores de aplicaciones para personalizar el conjunto predeterminado, como se indica a continuación:

   - **Para quitar un Clasificador de Aplicaciones del conjunto**:

   Haga clic en el icono de papelera de la columna **Eliminar** de una entrada del **Clasificador de aplicaciones** para eliminar esa entrada de la tabla.

   - **Para agregar un Clasificador de aplicaciones al conjunto:**

     a) Haga clic en **+** a la derecha de la etiqueta de sucursal **Clasificador de aplicaciones**.

        Muestra el formulario **Agregar** configuración.

     b) Introduzca el nombre y el número de puerto del Clasificador de aplicaciones en los campos **Nombre** y **Puerto**, respectivamente.

     c) Agregar o quitar grupos de aplicaciones en la lista **Configurado**.

        Para agregar un grupo de aplicaciones a la lista: Selecciónelo en la lista **Grupos de aplicaciones**de la izquierda y, a continuación, haga clic en la flecha Agregar a la derecha (>) para agregar el grupo a la lista **Configurado**de la derecha. Para agregar todos los **grupos de aplicaciones** a la lista a la vez, haga clic en la flecha doble derecha Agregar todo (»).

        Para quitar un grupo de aplicaciones de la lista: Selecciónelo en la lista **Configurado**de la derecha y, a continuación, haga clic en Eliminar flecha izquierda (<). Para quitar todos los **grupos de aplicaciones** de la lista a la vez, haga clic en la flecha izquierda doble Eliminar todo («).

     d) Haga clic en **Aplicar**.

        Esto agrega el nuevo Clasificador de aplicaciones al conjunto y descarta el formulario **Agregar** configuración.

        El siguiente paso es configurar el conjunto predeterminado de clases de servicio de optimización WAN.

Configurar clases de servicio predeterminadas de optimización

May 7, 2021

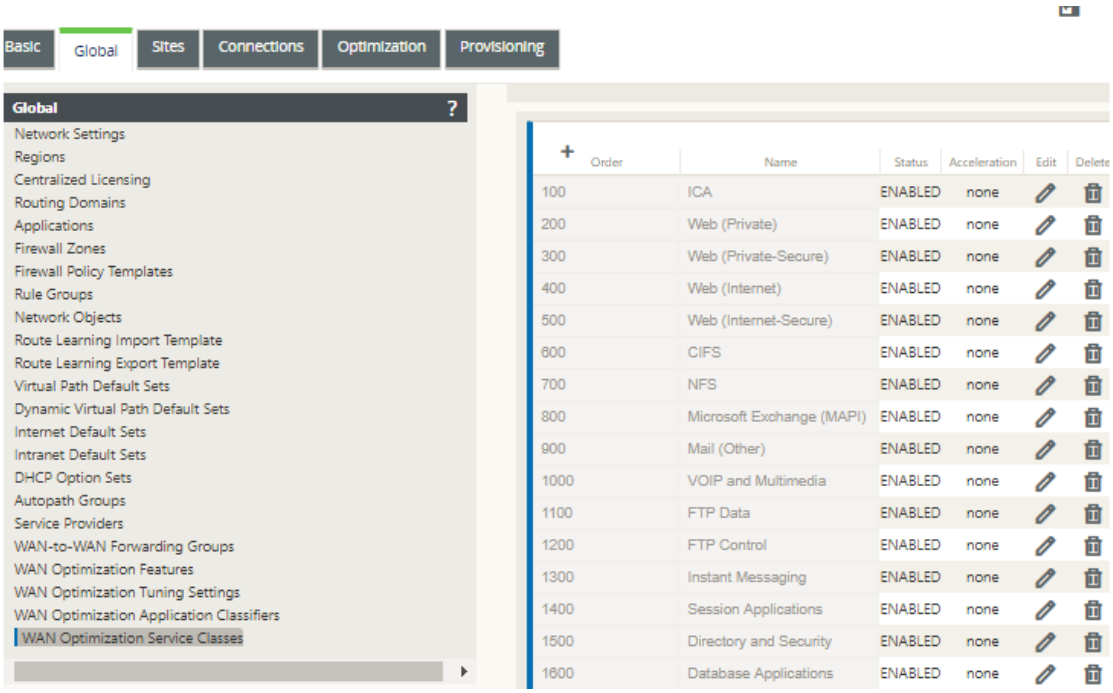
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede configurar la configuración predeterminada de la clase de servicio de optimización WAN en la ficha **Global**.

Para configurar el conjunto predeterminado de clases de servicio de optimización de WAN, haga lo siguiente:

1. En la ficha **Global**, haga clic en **Clases de servicio de optimización WAN.**

   Esto abre la tabla **Clases de servicio**, que muestra el conjunto predeterminado de Clases de servicio.



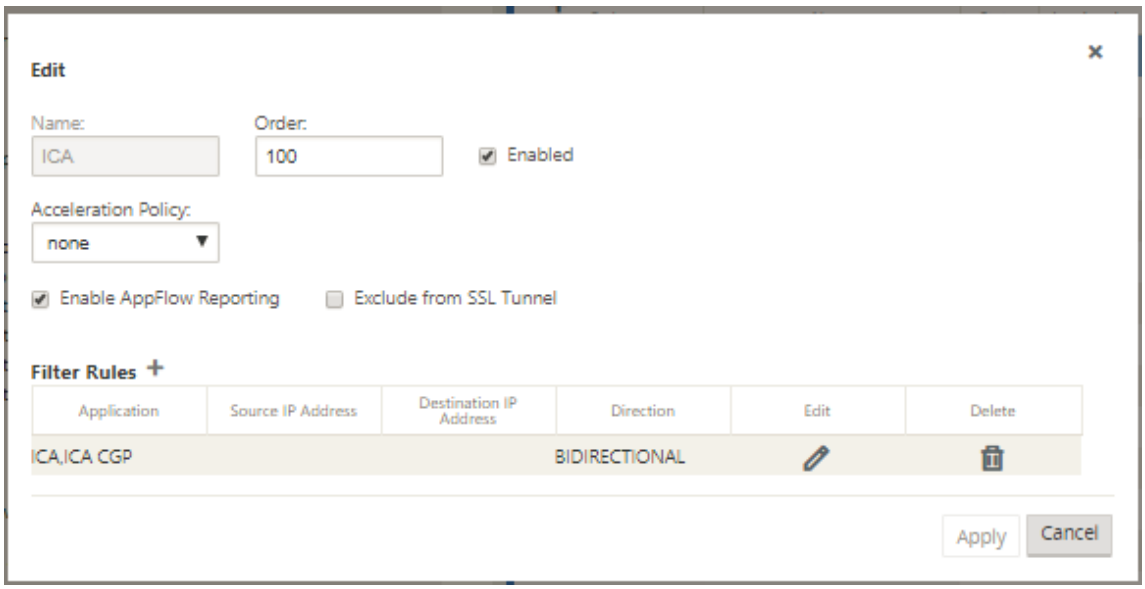
   Esta tabla es también un formulario de configuración. Puede utilizar este formulario para configurar (modificar), eliminar y agregar clases de servicio para crear un conjunto predeterminado personalizado. El conjunto de **Clases de Servicio** predeterminado modificado y los valores de Clase de Servicio individuales que configure se aplican automáticamente como valores predeterminados a cualquier sitio de sucursal incluido en el árbol de sección **Optimización**.

   > **Nota**
   >
   > También puede personalizar el conjunto de **clases de servicio** y la configuración de cada sitio de sucursal específico. Para obtener instrucciones sobre cómo personalizar la configuración de **Optimización** para un sitio de sucursal, consulte la sección,Configuración de Optimización para un Sitio de Sucursal.

2. Para configurar una clase de servicio existente, haga clic en Modificar (icono de lápiz), en la columna **Modificar** de esa entrada de clase de la tabla Clases de servicio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Esto abre un formulario emergente **Modificar** configuración para configurar la clase de servicio seleccionada



3. Configure las opciones básicas para la clase de servicio.

   Los ajustes básicos son los siguientes:

   - **Habilitado**: Seleccione esta opción para habilitar la nueva clase de servicio. La clase está habilitada de forma predeterminada.
   - **Directiva de aceleración**: Seleccione una directiva en el menú implementable **Directiva de aceleración**. Las opciones son:
     - **disk** : seleccione esta directiva para especificar el disco del dispositivo como ubicación para almacenar el historial de tráfico utilizado para la compresión. Esto habilita la directiva de compresión basada en disco (DBC) para esta clase de servicio. En términos generales, una directiva de **disco** suele ser la mejor opción, ya que el dispositivo selecciona automáticamente el **disco** o la **memoria** como ubicación de almacenamiento, dependiendo de cuál sea más apropiado para el tráfico.
     - **none** : seleccione esta opción si no desea habilitar una directiva de aceleración para esta clase de servicio. Por lo general, una directiva de **none** se usa solo para el tráfico cifrado no compresible y el vídeo en tiempo real.
     - **Solo control de flujo**: Seleccione esta directiva para inhabilitar la compresión pero habilitar la aceleración de control de flujo. Seleccione esta opción para los servicios que siempre están cifrados y para el canal de control FTP.
     - **memoria**: Seleccione esta directiva para especificar la memoria como ubicación para almacenar el historial de tráfico utilizado para la compresión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Habilitar informes de AppFlow**: Seleccione esta opción para habilitar los informes de AppFlow para esta clase de servicio. AppFlow es un estándar de la industria para desbloquear datos transaccionales de aplicaciones procesados por la infraestructura de red. La interfaz de AppFlow de optimización de WAN funciona con cualquier colector de AppFlow para generar informes. El recopilador recibe información detallada del dispositivo mediante el estándar abierto de AppFlow (`http://www.appflow.org`).

  Para obtener más información sobre AppFlow, consulte la documentación del producto Citrix CloudBridge 7.4 disponible en el portal de documentación de citrix `http://docs.citrix.com/`.

  > **Nota**
  >
  > Para ver los informes de AppFlow de optimización de WAN, seleccione la ficha **Supervisión** **y** , a continuación, en el árbol de navegación (panel izquierdo), abra la rama **Optimización de WAN** y seleccione **AppFlow.** También puede consultar Supervisión de WAN Virtual.

- **Excluir del túnel SSL**: Seleccione esta opción para excluir el tráfico asociado a la clase de servicio del túnel SSL.

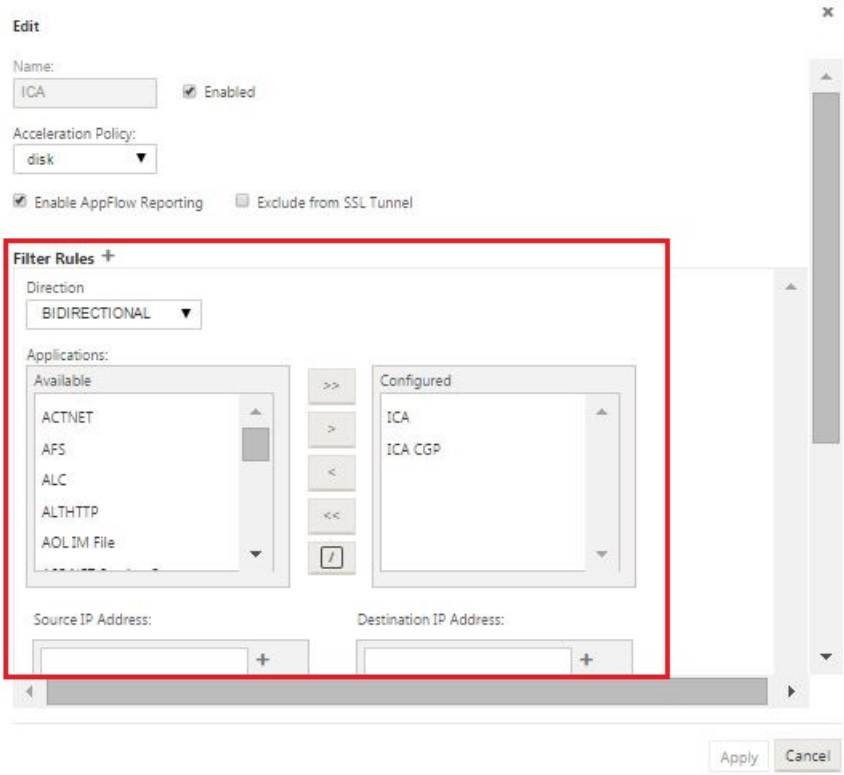
4. Configure las **reglas de filtro** para la clase de servicio.

   Para modificar una regla existente, haga lo siguiente:

   a) En la tabla Reglas de filtro (parte inferior del formulario), haga clic en Modificar (icono de lápiz) en la columna Modificar de la regla que quiere modificar.

      Esto revela la configuración de Reglas de filtro para la Regla de filtro seleccionada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) Seleccione la dirección del filtro en el menú desplegable Dirección.

Seleccione una de estas opciones:

- **BIDIRECCIONAL**
- **UNIDIRECCIONAL**

c) Agregar o quitar aplicaciones en la lista **Configurado**.

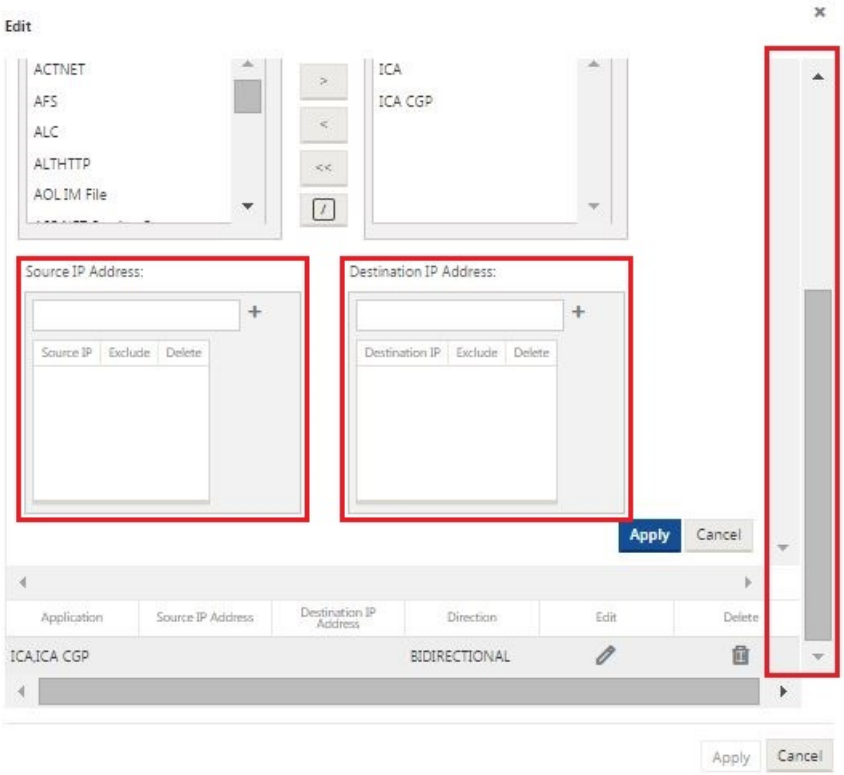
Para agregar una aplicación a la lista: Selecciónela en la lista **Aplicaciones**de la izquierda y, a continuación, haga clic en la flecha Agregar a la derecha (**>**) para agregar el grupo a la lista **Configurada**de la derecha. Para agregar todas las **aplicaciones** a la lista a la vez, haga clic en la flecha doble derecha Agregar todo (**»**).

Para eliminar una aplicación de la lista: Selecciónela en la lista Configurada de la derecha y, a continuación, haga clic en Eliminar flecha izquierda **(<**). Para eliminar todas las **aplicaciones** de la lista a la vez, haga clic en la flecha izquierda doble Eliminar todo (**«**).

d) Desplácese hacia abajo para mostrar la parte truncada del formulario.

La sección de configuración de **Reglas de filtro** es algo larga, por lo que deberá usar las barras de desplazamiento para mostrar la parte truncada del formulario.

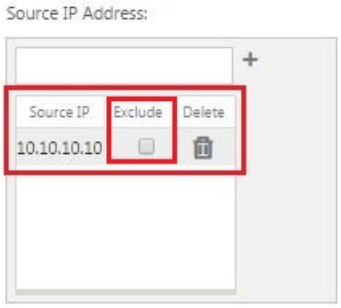
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



e) Introduzca la dirección IP de origen en el campo **Dirección IP de origen**.

f) Haga clic en **+** a la derecha de la dirección IP de origen que acaba de introducir.

Esto agrega la dirección IP especificada a la tabla **Dirección IP de origen**.



g) Especifique si quiere incluir o excluir la dirección IP de origen para esta regla de filtro.

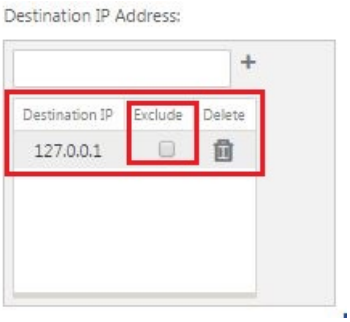
Active la casilla de verificación Excluir para excluir la dirección IP de origen especificada de esta regla de filtro. Anule la selección de la casilla de verificación para incluir la dirección.

h) Introduzca la dirección IP de destino en el campo **Dirección IP de destino**.

i) Haga clic en **+** a la derecha de la dirección IP de destino que acaba de introducir.

Esto agrega la dirección IP especificada a la tabla **Dirección IP de origen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



j) Especifique si quiere incluir o excluir la dirección IP de destino para esta regla de filtro.

Active la casilla de verificación Excluir para excluir la dirección IP de destino especificada de esta regla de filtro. Anule la selección de la casilla de verificación para incluir la dirección.

k) Haga clic en **Aplicar**.

Esto aplica las modificaciones a la regla y oculta la sección Configuración de **reglas de filtro**.

5. (Opcional) Personalice el conjunto predeterminado **de clases de servicio**.

Puede agregar o eliminar clases de servicio para personalizar el conjunto predeterminado, de la siguiente manera:

- **Para eliminar una clase de servicio del conjunto:**

  Haga clic en el icono de papelera de la columna **Eliminar** de una entrada de clase de servicio de la tabla para eliminar esa entrada.

- **Para agregar una clase de servicio al conjunto**:

  a) Haga clic en **+** a la derecha de la etiqueta de sucursal **de clase de servicio**.

  Muestra el formulario **Agregar** configuración.

  b) Introduzca el nombre de la nueva Clase de Servicio en el **campo Nombre.**

  c) Configure la nueva clase de servicio.

  Los pasos para configurar una nueva Clase de Servicio son los mismos que para modificar una Clase de Servicio existente. Para obtener instrucciones, consulte los pasos siguientes, anteriormente en esta sección:

  "3. Configure las opciones básicas para la clase de servicio.

  "4. Configure las reglas de filtro para la clase de servicio.

  d) Haga clic en **Agregar** para agregar la nueva clase de servicio al conjunto predeterminado y deseche el formulario **Agregar** configuración.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. (Opcional, recomendado) **Guarde** el paquete de configuración.

   Ya ha completado la configuración global de optimización de WAN y puede comenzar a configurar los conjuntos de **optimización** y la configuración de los sitios de sucursal.

Configurar la optimización para un sitio de sucursal

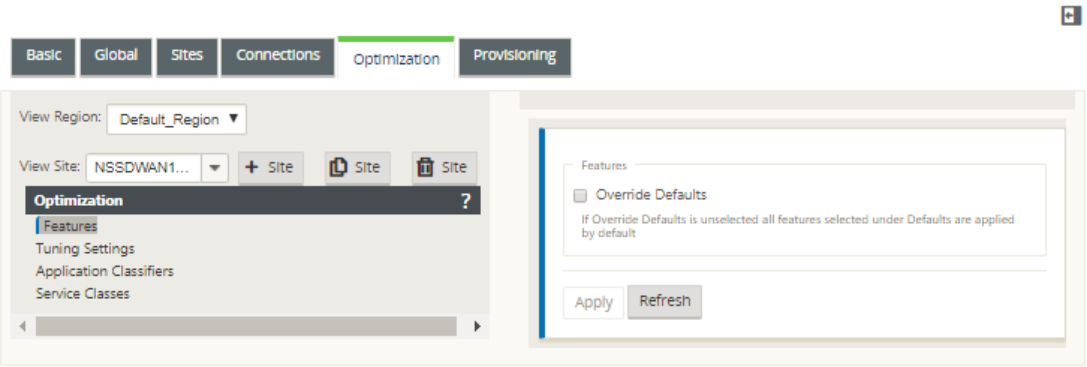
May 7, 2021

Después de completar la configuración global predeterminada, tiene la opción de personalizar los conjuntos y configuraciones para cada uno de los sitios de sucursal.

La configuración global que acaba de configurar se aplica automáticamente a cada sitio de sucursal incluido en la sección **Optimización**. Puede optar por aceptar los valores predeterminados o personalizar la configuración de cualquier sucursal determinada. Los procedimientos para configurar los conjuntos de **optimización** y la configuración de un sitio de sucursal son los mismos que para configurar los valores predeterminados globales, con algunas diferencias menores.

Para personalizar la configuración **de Optimización** para un sitio de sucursal, haga lo siguiente:

1. Haga clic en la ficha **Optimización**, en el campo Ver sitio, seleccione un sitio.

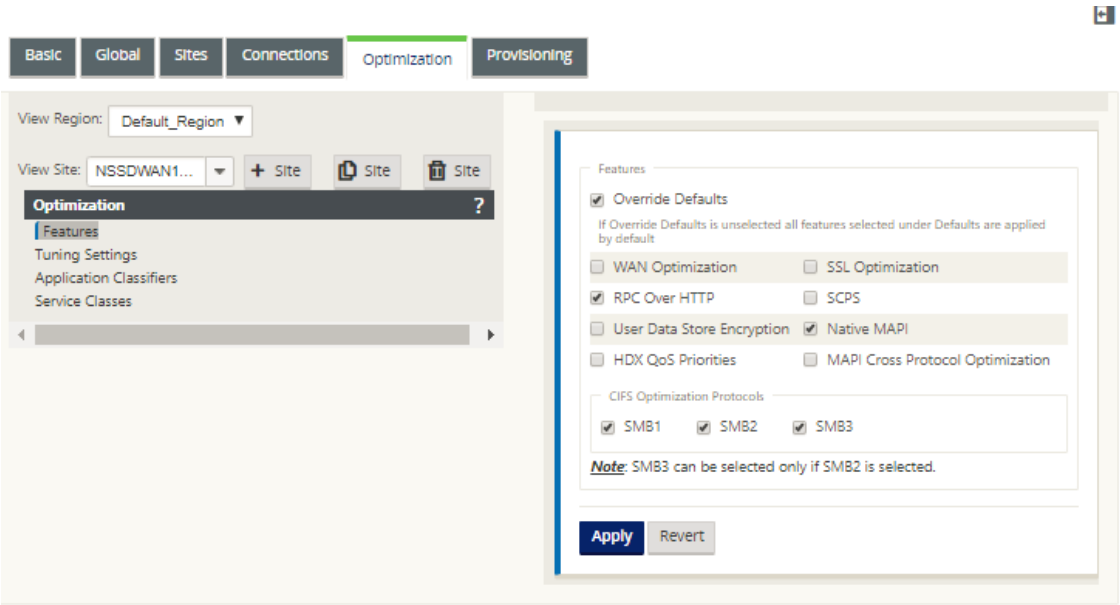


2. Active la casilla de verificación **Modificar valores predeterminados**.

   Esto revela el formulario de configuración de nivel superior para esa categoría de configuración y lo abre para su edición.

   La siguiente imagen muestra un ejemplo de configuración de configuración de nivel superior, en este caso para el conjunto de **funciones**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Introduzca los cambios de configuración.

   A partir de este punto, el proceso de configuración de cada categoría **Optimización** de sitio de sucursal es el mismo que para la categoría de sección global correspondiente. Para obtener instrucciones sobre cómo configurar una categoría concreta de conjuntos o configuraciones, consulte la sección correspondiente que se muestra a continuación:

   - Activación de la optimización y configuración de los ajustes de las funciones por defecto.
   - Configuración de ajustes predeterminados de optimización.
   - Configuración de Clasificadores de Aplicaciones Predeterminados de Optimización.
   - Configuración de Clases de Servicio Predefinidas de Optimización.

4. (Opcional, recomendado) **Guarde** el paquete de configuración.

   Ya ha completado la configuración de los conjuntos de secciones de **Optimización** y configuración para su WAN virtual.

Configurar perfiles SSL

May 7, 2021

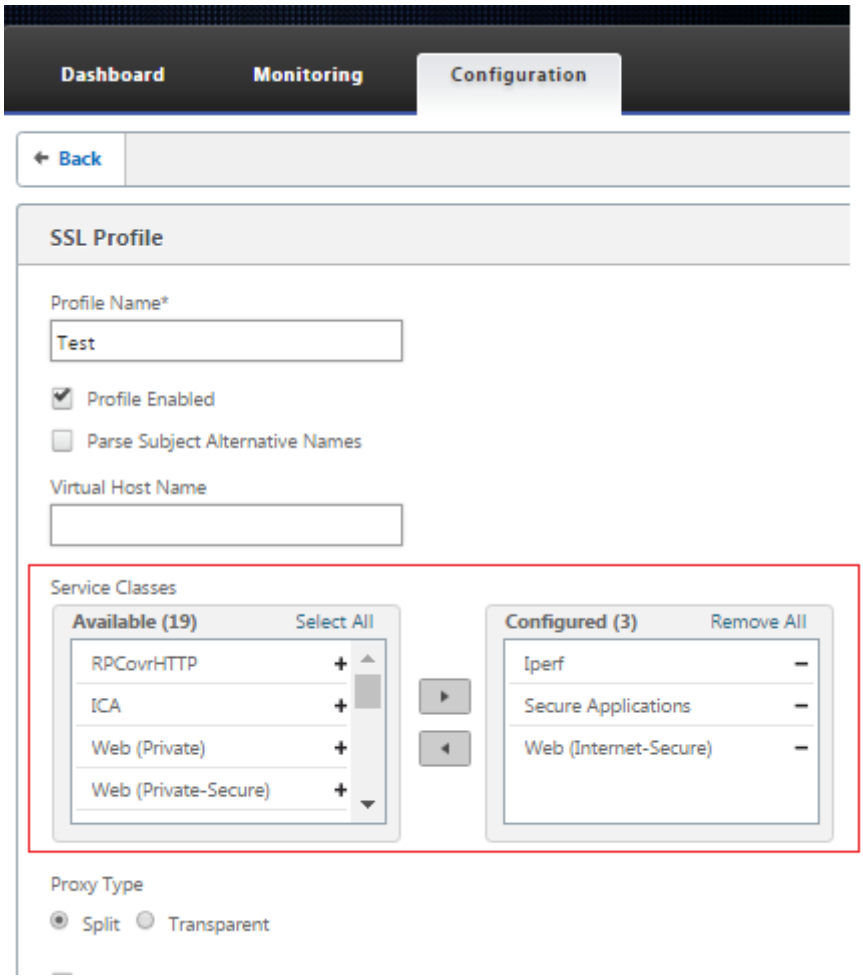
Toda la configuración relacionada con SSL está disponible a través del nuevo editor de configuración del dispositivo para mayor seguridad y facilidad de uso. En las implementaciones de SD-WAN Premium (Enterprise) Edition y en las implementaciones de dos cajas, las clases de servicio se configuran desde el editor de configuración y, por lo tanto, no se pueden adjuntar perfiles SSL. Para acomodar la

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

expresión de la asignación de perfiles SSL a una clase de servicio, el flujo de trabajo para los perfiles SSL se cambia para permitir la conexión de clases de servicio en el nodo de perfil.

Una de las limitaciones es que el perfil SSL se adjuntará a todas las reglas de una clase de servicio. Si necesita adjuntar el perfil SSL selectivamente a una regla particular, la configuración de la clase de servicio se divide en reglas detalladas para su posterior selección.

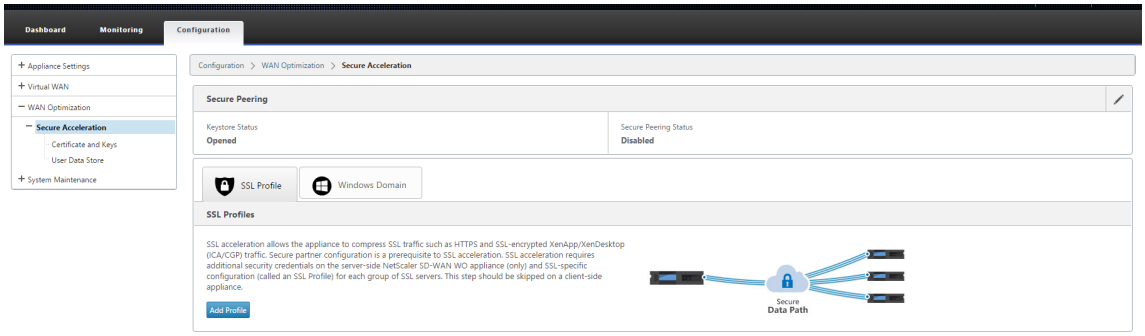
> **Nota**
>
> Solo las clases de servicio que tienen la dirección de las reglas de filtro establecida en unidireccional se pueden asociar a los perfiles SSL.

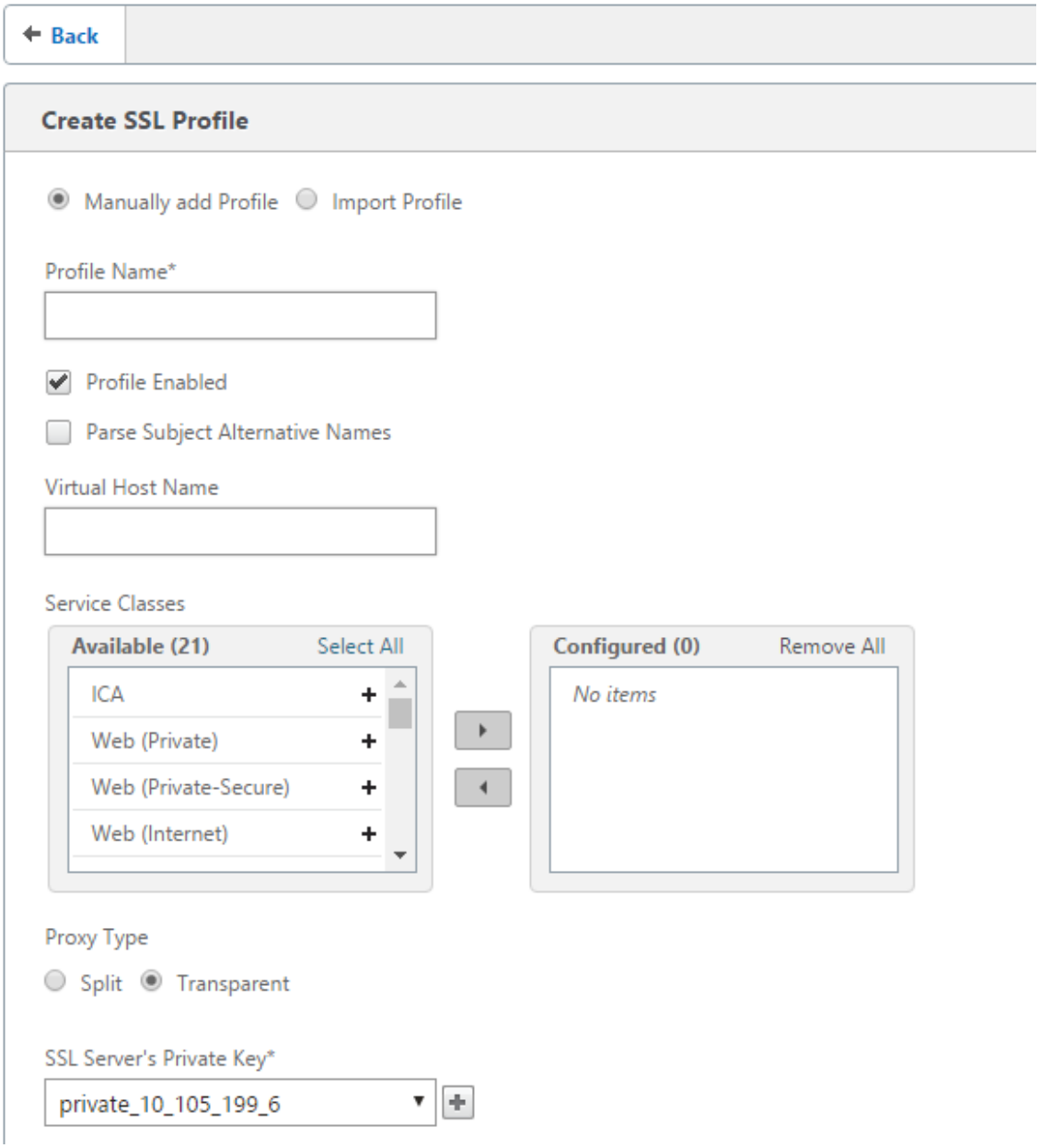


Para crear un perfil SSL en el nuevo dispositivo Premium (Enterprise) Edition en el centro de datos:

1. En la GUI web de SD-WAN, vaya a la página **Configuración** > **Aceleración segura**. Haga clic en **Agregar perfil**. Cree el **perfil SSL**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

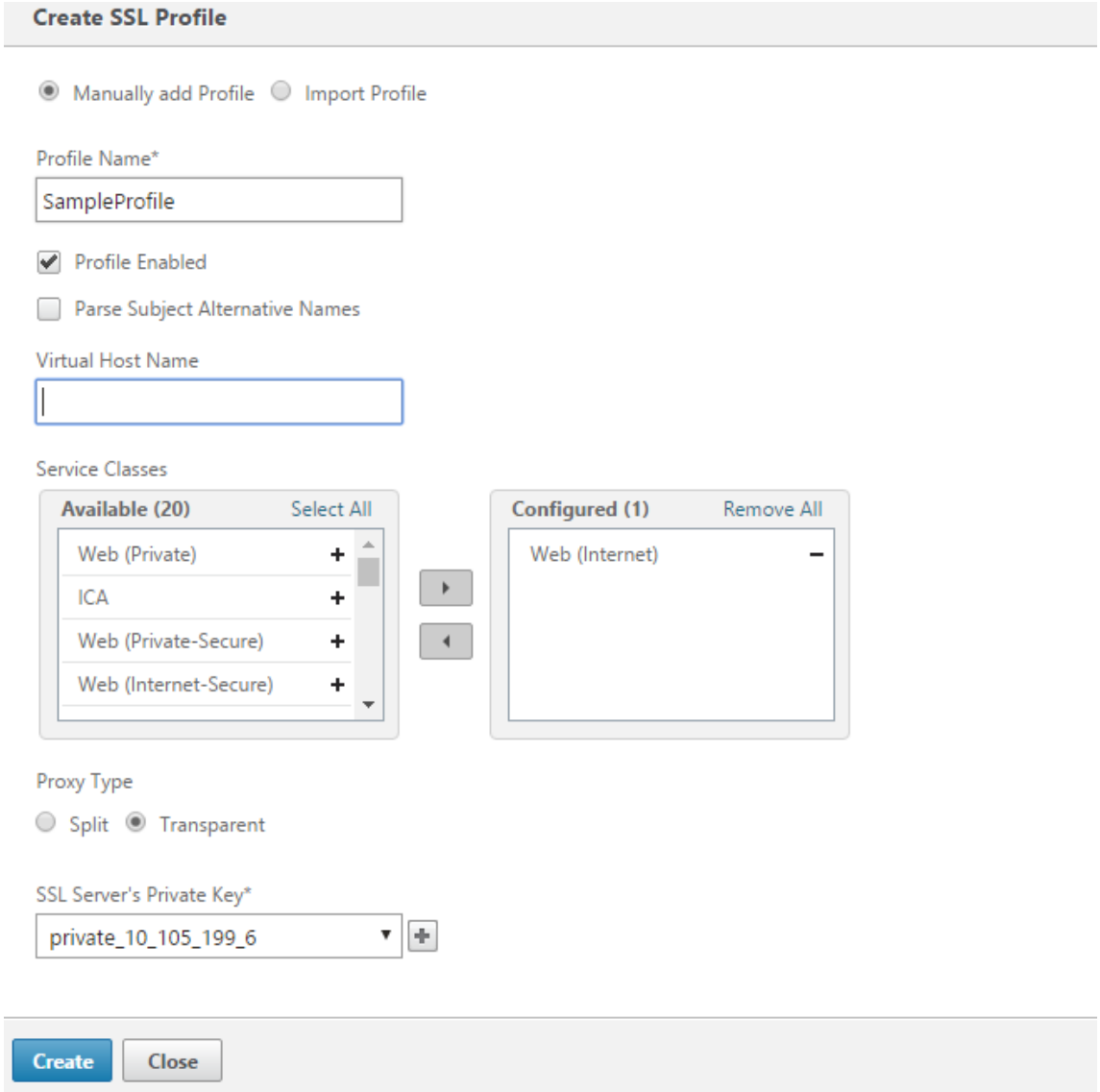




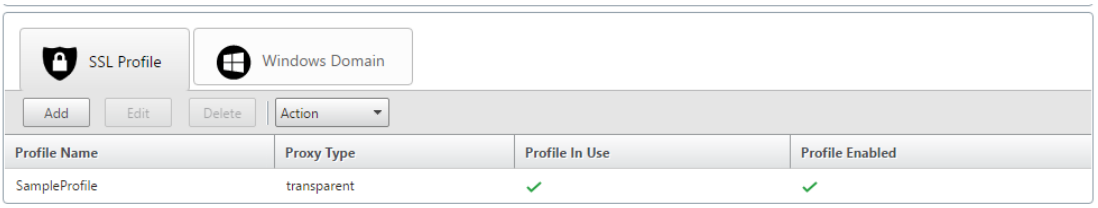
2. En la página **Crear Perfil SSL**, proporcione un nombre de perfil y seleccione **Clases de Servicio** que se asociarán a este perfil. Elija **Tipo de proxy** y proporcione los datos pertinentes y haga

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

clic en **Crear**.



3. Después de que el perfil SSL se crea correctamente y la clase de servicio se asocia, ver la información del perfil SSL como se muestra a continuación.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plug-in del cliente de la optimización WAN de Citrix

May 7, 2021

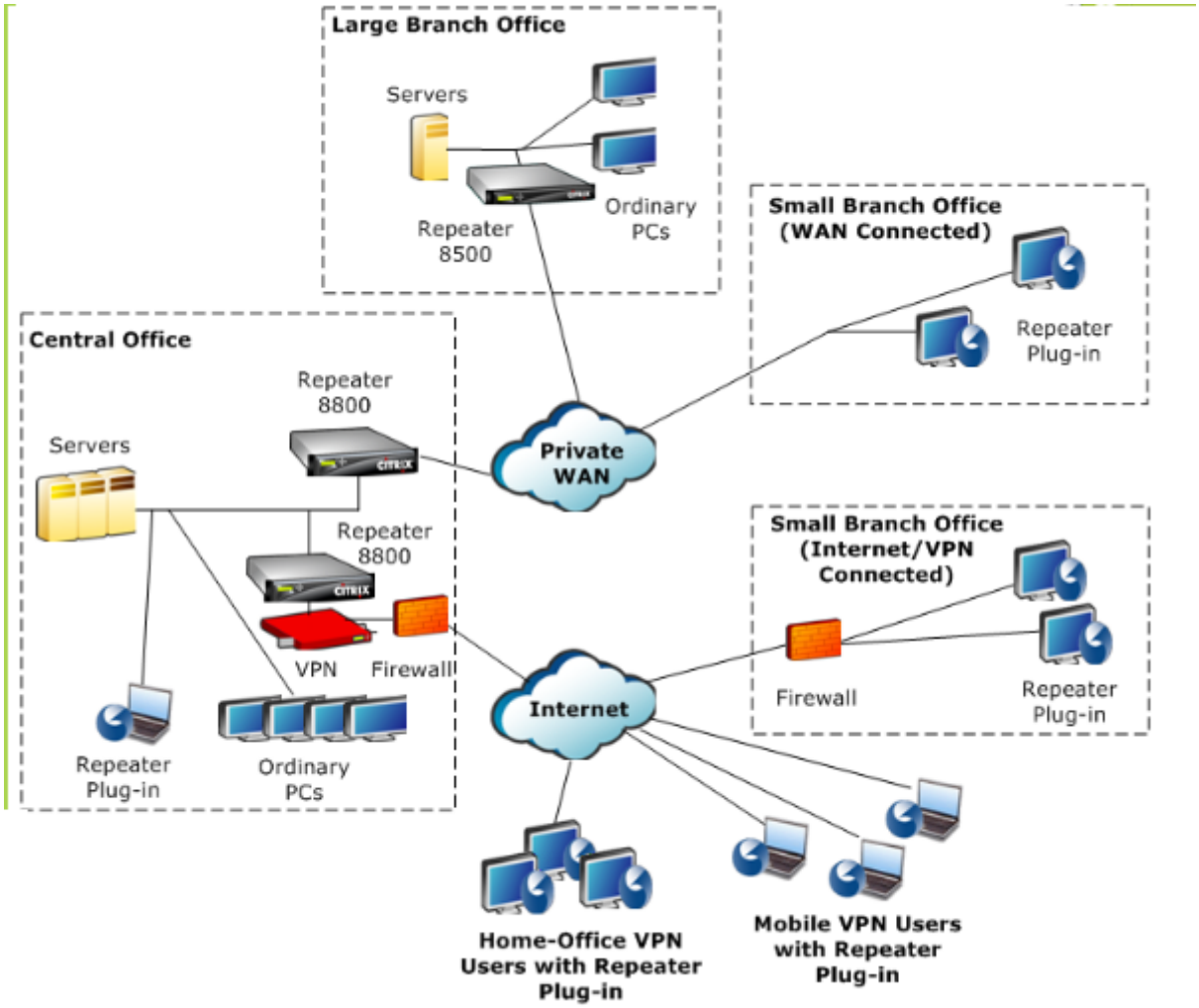
El complemento cliente de Citrix WANOP es un acelerador de red basado en software que se ejecuta en portátiles y estaciones de trabajo Windows, lo que proporciona aceleración en cualquier lugar, no solo en oficinas con dispositivos WANOP Client Plug-in. Se conecta a un dispositivo Citrix WANOP Client Plug-in en el otro extremo del vínculo.

Los principios de funcionamiento de WANOP Client Plug-in suelen ser los mismos que los de un dispositivo WANOP Client Plug-in. Para los temas no incluidos en la documentación del complemento, consulte el conjunto de documentación más grande.

El complemento se distribuye como un archivo de instalación estándar de Microsoft (MSI). La implementación de complementos requiere alguna configuración específica de complementos de los dispositivos WANOP Client Plug-in en los otros extremos de los vínculos. Si personaliza el archivo MSI con las direcciones DNS o IP de los dispositivos WANOP Client Plug-in y algunos otros parámetros, los usuarios no tendrán que introducir ninguna información de configuración al instalar el complemento en sus equipos Windows.

Ilustración 1. Red típica de complementos de cliente WANOP que muestra el complemento de cliente WANOP

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Citrix Receiver 1.2 o posterior admite el complemento, y Citrix Receiver puede distribuirlo y administrarlo.

Requisitos de hardware y software

May 7, 2021

En el lado del cliente del enlace acelerado, el complemento cliente
WANOP es compatible con sistemas de escritorio y portátiles Windows, pero no en netbooks o thin clients. Citrix recomienda las siguientes especificaciones mínimas de hardware para el equipo que ejecuta el complemento cliente WANOP:

- CPU Pentium 4 clase

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 2 GB de RAM
- 2 GB de espacio libre en disco

WANOP Client Plug-in es compatible con la plataforma Windows 10 y necesita los siguientes requisitos del sistema:

- 4 GB DE RAM
- 10 GB de espacio libre en disco

El complemento cliente WANOP es compatible con los siguientes sistemas operativos:

- Inicio de Windows XP
- Windows XP Professional
- Windows Vista (todas las versiones de 32 bits de Home Basic, Home Premium, Business, Enterprise y Ultimate)
- Windows 7 (todas las versiones de 32 y 64 bits de Home Basic, Home Premium, Professional, Enterprise y Ultimate)
- Windows 8 (versiones de 32 y 64 bits de Premium Edition)
- Windows 10 (versiones de 32 y 64 bits de Premium Edition)

En el lado del servidor, los siguientes dispositivos admiten actualmente implementaciones de WANOP Client Plug-in:

- Repetidor Serie 8500
- Repetidor Serie 8800
- Plug-in de cliente WANOP VPX
- Plug-in de cliente WANOP 2000
- Plug-in de cliente WANOP 3000
- Plug-in de cliente WANOP 4000
- Plug-in de cliente WANOP 5000

Cómo funciona el complemento WANOP

May 7, 2021

Los productos WANOP Client Plug-in utilizan su infraestructura WAN/VPN existente. Un equipo en el que está instalado el complemento continúa accediendo a la LAN, WAN e Internet como lo hacía

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

antes de la instalación del complemento. No se requieren cambios en las tablas de redirección, la configuración de red, las aplicaciones cliente o las aplicaciones de servidor.

Las VPN de Citrix Access Gateway requieren una pequeña cantidad de configuración específica del complemento de cliente WANOP.

Hay dos variaciones en la forma en que las conexiones son manejadas por el plug-in y el dispositivo: el *modo transparente y el modo* de *redirector.* Redirector es un modo heredado que no se recomienda para nuevas implementaciones.

- **El modo transparente** para la aceleración de conexión a dispositivo es muy similar a la aceleración de dispositivo a dispositivo. El dispositivo WANOP Client Plug-in debe estar en la ruta de acceso que toman los paquetes al viajar entre el complemento y el servidor. Al igual que ocurre con la aceleración de dispositivo a dispositivo, el modo transparente funciona como un proxy transparente, preservando la dirección IP de origen y destino y los números de puerto desde un extremo de la conexión al otro.
- **El modo de redirector** (no recomendado) utiliza un proxy explícito. El complemento lee los paquetes salientes a la dirección IP del redirector del dispositivo. El dispositivo a su vez readapta los paquetes al servidor, mientras cambia la dirección de retorno para que apunte a sí mismo en lugar del complemento. En este modo, el dispositivo no tiene que estar físicamente en línea con la ruta entre la interfaz WAN y el servidor (aunque esta es la implementación ideal).

  Práctica recomendada: Utilice el modo transparente cuando pueda y el modo de redirección cuando sea necesario.

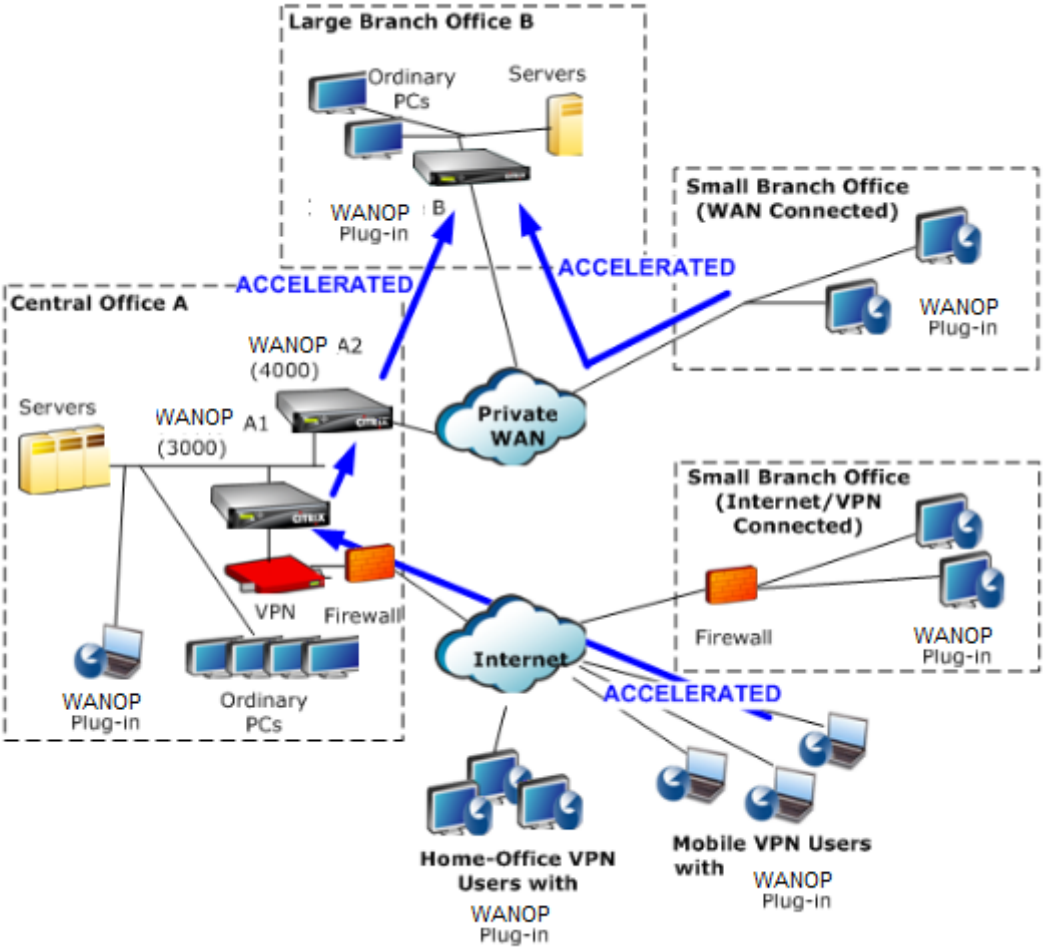
Modo transparente

En el modo transparente, los paquetes para conexiones aceleradas deben pasar por el dispositivo de destino, al igual que lo hacen en la aceleración de dispositivo a dispositivo.

El plug-in está configurado con una lista de dispositivos disponibles para la aceleración. Intenta ponerse en contacto con cada dispositivo, abriendo una conexión de señalización. Si la conexión de señalización se realiza correctamente, el complemento descarga las reglas de aceleración del dispositivo, que envía las direcciones de destino para las conexiones que el dispositivo puede acelerar.

Ilustración 1. Modo transparente, resaltando tres trayectorias de aceleración

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nota

- Flujo de tráfico: El modo transparente acelera las conexiones entre un complemento cliente WANOP y un dispositivo habilitado para el complemento.
- Licencias: Los dispositivos necesitan una licencia para admitir el número quieredo de complementos. En el diagrama, el repetidor A2 no necesita tener licencia para la aceleración del plug-in, ya que el repetidor A1 proporciona la aceleración del plug-in para el sitio A.
- Conexión en serie: Si la conexión pasa a través de varios dispositivos en el ruta al dispositivo de destino, los dispositivos en el medio deben tener activada la conexión en cadena o la aceleración se bloquea. En el diagrama, el tráfico de los usuarios VPN móviles y de la oficina doméstica destinados a la sucursal grande B se acelera con el repetidor B. Para que esto funcione, los repetidores A1 y A2 deben tener habilitado el encadenamiento en margarita.

Cada vez que el complemento abre una nueva conexión, consulta las reglas de aceleración. Si la dirección de destino coincide con alguna de las reglas, el complemento intenta acelerar la conexión adjuntando opciones de aceleración al paquete inicial de la conexión (el paquete SYN). Si algún dis-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

positivo conocido por el plug-in conecta opciones de aceleración al paquete de respuesta SYN-ACK, se establece una conexión acelerada con ese dispositivo.

La aplicación y el servidor no saben que se ha establecido la conexión acelerada. Solo el software del plug-in y el dispositivo saben que se está produciendo la aceleración.

El modo transparente se asemeja a la aceleración de dispositivo a dispositivo, pero no es idéntico al mismo. Las diferencias son:

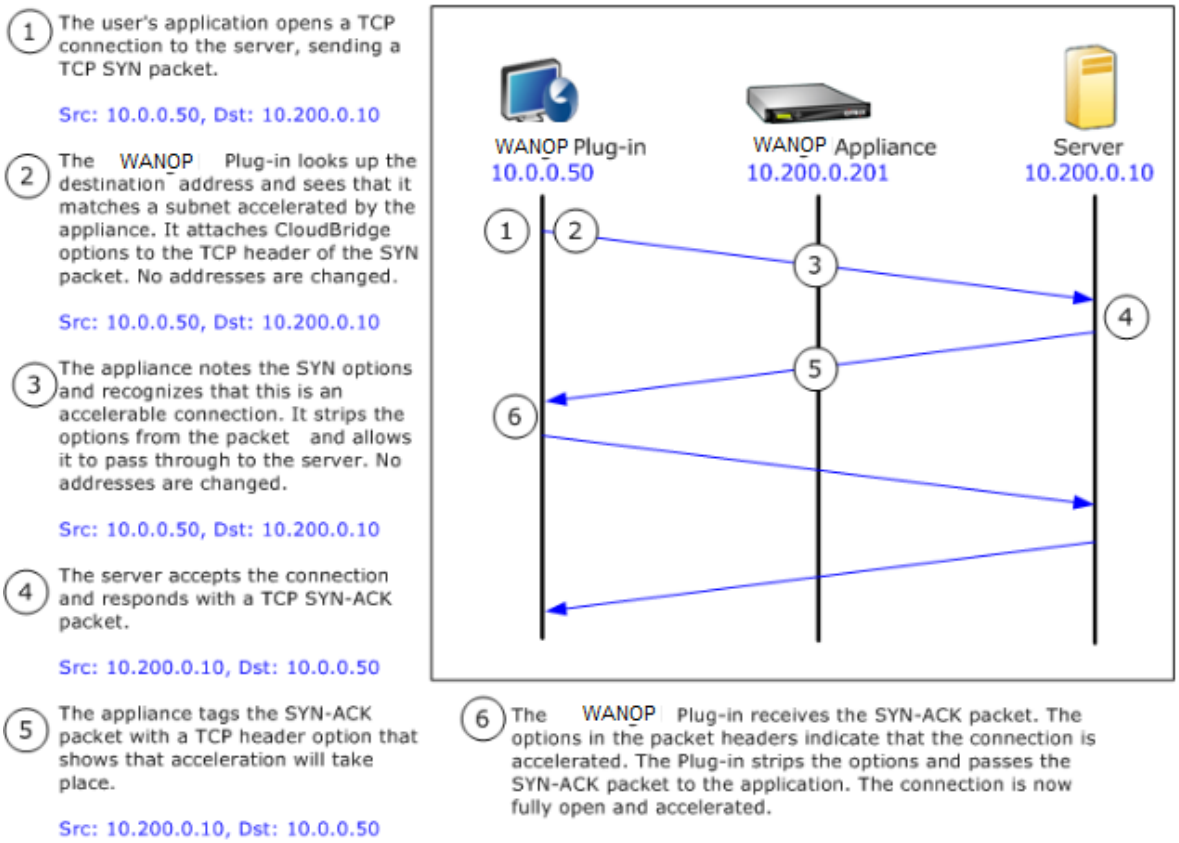
- Solo conexiones iniciadas por el cliente: El modo transparente acepta conexiones iniciadas por el sistema equipado con un complemento. Si utiliza un sistema equipado con un complemento como servidor, las conexiones del servidor no se aceleran. Por otro lado, la aceleración de dispositivo a dispositivo funciona independientemente de qué lado es el cliente y cuál es el servidor. (FTP en modo activo se trata como un caso especial, porque el servidor abre la conexión que inicia la transferencia de datos solicitada por el complemento.)
- Conexión de señalización: El modo transparente utiliza una conexión de señalización entre el plug-in y el dispositivo para la transmisión de información de estado. La aceleración de dispositivo a dispositivo no requiere una conexión de señalización, excepto para las relaciones de pares seguras, que están inhabilitadas de forma predeterminada. Si el complemento no puede abrir una conexión de señalización, no intentará acelerar las conexiones a través del dispositivo.
- Cadena en serie: Para un dispositivo que se encuentra en la ruta entre un complemento y su dispositivo de destino seleccionado, debe habilitar la conexión en cadena en el menú **Configuración: Ajuste**.

El modo transparente se usa a menudo con VPN. El complemento de cliente WANOP es compatible con la mayoría de VPN IPSec y PPTP, y con VPN de Citrix Access Gateway.

La siguiente imagen muestra el flujo de paquetes en modo transparente. Este flujo de paquetes es casi idéntico a la aceleración de dispositivo a dispositivo, excepto que la decisión de intentar o no acelerar la conexión se basa en las reglas de aceleración descargadas a través de la conexión de señalización.

Imagen 2. Flujo de paquetes en modo transparente

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Modo Redirector

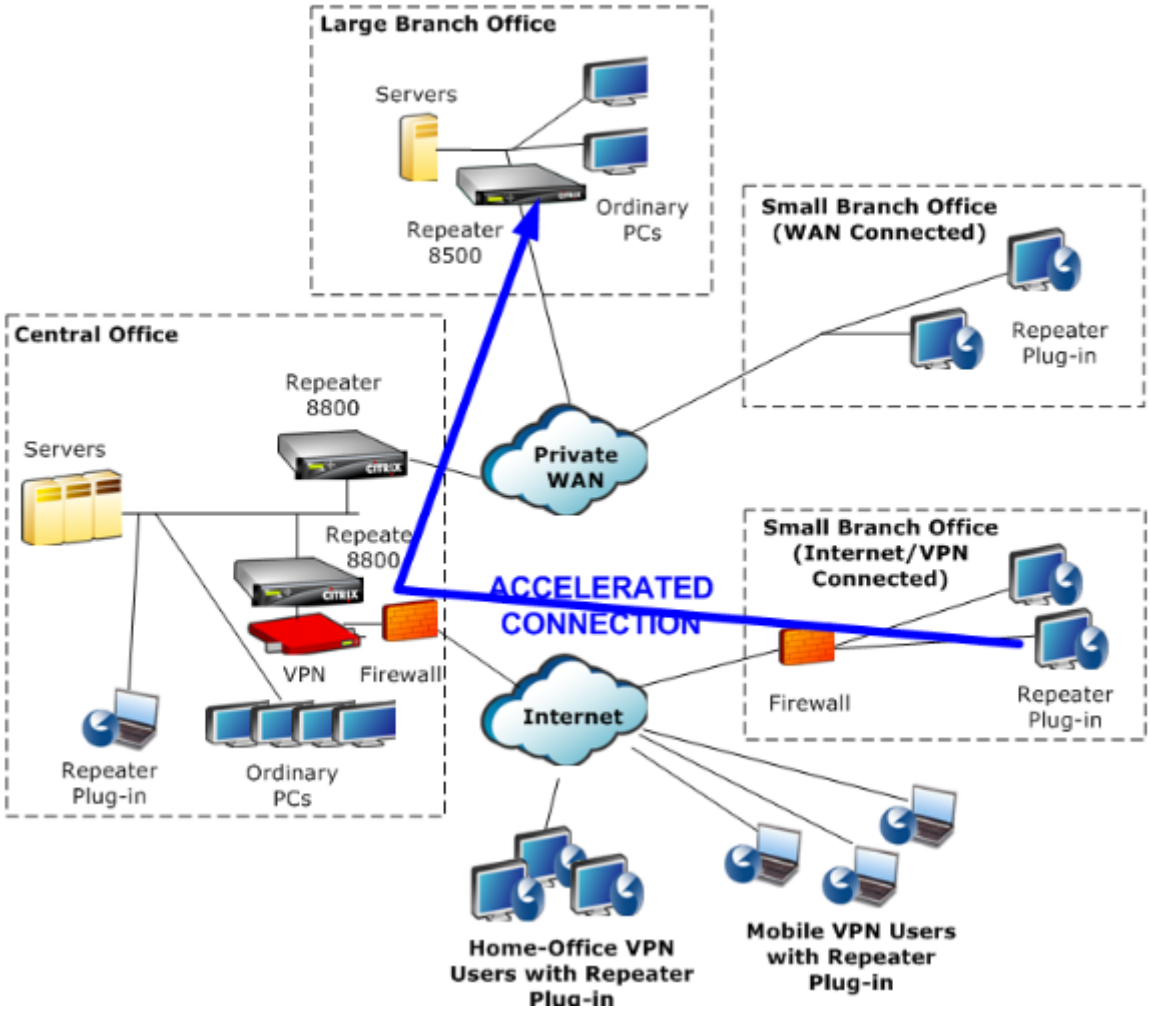
El modo Redirector funciona de manera diferente al modo transparente de las siguientes maneras:

- El software WANOP Client Plug-in redirige los paquetes dirigiéndolos explícitamente al dispositivo.
- Por lo tanto, el dispositivo en modo de redirector no tiene que interceptar todo el tráfico de enlace WAN. Debido a que las conexiones aceleradas se dirigen directamente a él, se puede colocar en cualquier lugar, siempre y cuando sea accesible tanto por el plug-in como por el servidor.
- El dispositivo realiza sus optimizaciones y, a continuación, redirige los paquetes de salida al servidor, reemplazando la dirección IP de origen de los paquetes por su propia dirección. Desde el punto de vista del servidor, la conexión se origina en el dispositivo.
- El tráfico de retorno del servidor se dirige al dispositivo, que realiza optimizaciones en la dirección de retorno y reenvía los paquetes de salida al complemento.
- Los números de puerto de destino no se cambian, por lo que las aplicaciones de supervisión de red aún pueden clasificar el tráfico.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La siguiente imagen muestra cómo funciona el modo Redirector.

Ilustración 1. Modo Redirector



La siguiente imagen muestra el flujo de paquetes y la asignación de direcciones en *modo de redirector*.

Imagen 2. Flujo de paquetes en modo de redirector

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. The user's application opens a TCP connection to the server, sending a TCP SYN packet.

   Src: 10.0.0.50, Dst: 10.200.0.10

2. The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

   Src: 10.0.0.50, Dst: 10.200.0.201

   (10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

3. The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

   Src: 10.200.0.201, Dst: 10.200.0.10

4. The server accepts the connection and responds with a TCP SYN-ACK packet.

   Src: 10.200.0.10, Dst: 10.200.0.201

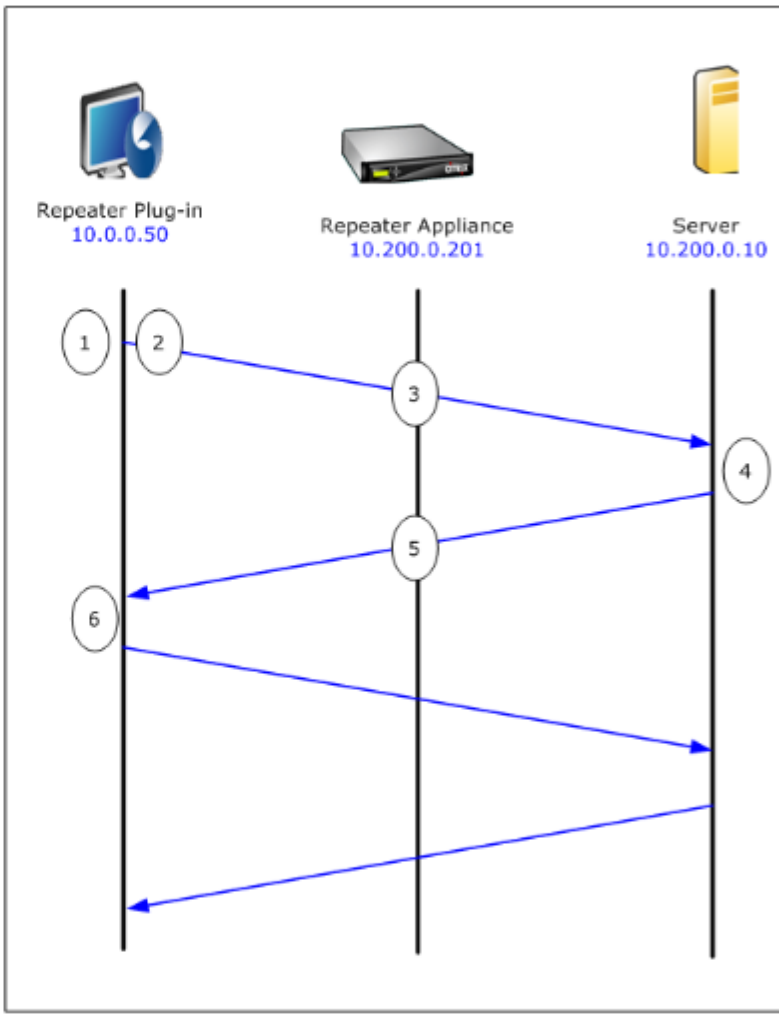
5. The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

   Src: 10.200.0.201, Dst: 10.0.0.50

6. The connection is now fully open. The client and server send packets back and forth via the appliance.

   While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

   There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cómo selecciona el complemento un dispositivo

Cada complemento está configurado con una lista de dispositivos con los que puede ponerse en contacto para solicitar una conexión acelerada.

Cada uno de los dispositivos tiene una lista de *reglas de aceleración*, que es una lista de direcciones o puertos de destino a los que el dispositivo puede establecer conexiones aceleradas. El complemento descarga estas reglas de los dispositivos y hace coincidir la dirección de destino y el puerto de cada conexión con el conjunto de reglas de cada dispositivo. Si solo un dispositivo ofrece acelerar una conexión determinada, la selección es fácil. Si más de un dispositivo ofrece acelerar la conexión, el complemento debe elegir uno de los dispositivos.

Las reglas para la selección de dispositivos son las siguientes:

- Si todos los dispositivos que ofrecen acelerar la conexión son dispositivos en modo de redirector, se selecciona el dispositivo situado más a la izquierda de la lista de dispositivos del complemento. (Si los dispositivos se especificaron como direcciones DNS y el registro DNS tiene varias direcciones IP, éstas también se analizan de izquierda a derecha.)
- Si algunos de los dispositivos que ofrecen acelerar la conexión utilizan el modo de redirector y otros utilizan el modo transparente, los dispositivos de modo transparente se ignoran y la selección se realiza desde los dispositivos de modo redirector.
- Si todos los dispositivos que ofrecen acelerar la conexión utilizan el modo transparente, el plug-in no selecciona un dispositivo específico. Inicia la conexión con las opciones SYN del complemento cliente WANOP y se utiliza el dispositivo candidato que conecte las opciones adecuadas al paquete SYN-ACK devuelto. Esto permite que el dispositivo que está en línea con el tráfico se identifique en el complemento. Sin embargo, el complemento debe tener una conexión de señalización abierta con el dispositivo que responde, de lo contrario, no se produce la aceleración.
- Parte de la información de configuración se considera global. Esta información de configuración se toma del dispositivo situado más a la izquierda de la lista para el que se puede abrir una conexión de señalización.

Implementación de dispositivos para su uso con complementos

May 7, 2021

La aceleración del cliente requiere una configuración especial en el dispositivo WANOP Client Plug-in. Otras consideraciones incluyen la ubicación del dispositivo. Por lo general, los complementos se implementan para conexiones VPN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Utilizar un dispositivo dedicado cuando sea posible

Intentar utilizar el mismo dispositivo tanto para la aceleración de complementos como para la aceleración de vínculos suele ser difícil, ya que los dos usos a veces exigen que el dispositivo se encuentre en diferentes puntos del centro de datos, y los dos usos pueden solicitar reglas de clase de servicio diferentes.

Además, un único dispositivo puede servir como punto final para la aceleración de complementos o como punto final para la aceleración de sitio a sitio, pero no puede servir a ambos fines para la misma conexión al mismo tiempo. Por lo tanto, cuando utiliza un dispositivo tanto para la aceleración de complementos para la VPN como para la aceleración de sitio a sitio en un centro de datos remoto, los usuarios de complementos no reciben aceleración de sitio a sitio. La gravedad de este problema depende de la cantidad de datos utilizados por los usuarios de complementos proviene de sitios remotos.

Por último, dado que los recursos de un dispositivo dedicado no se dividen entre las demandas de plug-in y sitio a sitio, proporcionan más recursos y, por lo tanto, un mayor rendimiento para cada usuario del complemento.

Utilizar el modo en línea cuando sea posible

Se debe implementar un dispositivo en el mismo sitio que la unidad VPN que admite. Normalmente, las dos unidades están en línea entre sí. Una implementación en línea proporciona la configuración más simple, la mayor cantidad de funciones y el mayor rendimiento. Para obtener los mejores resultados, el dispositivo debe estar directamente en línea con la unidad VPN.

Sin embargo, los dispositivos pueden utilizar cualquier modo de implementación, excepto el modo de grupo o el modo de alta disponibilidad. Estos modos son adecuados tanto para la aceleración de dispositivo a dispositivo como de cliente a dispositivo. Se pueden utilizar solos (*modo transparente*) o en combinación con el modo redirector.

Coloque los dispositivos en una parte segura de la red

Un dispositivo depende de la infraestructura de seguridad existente del mismo modo que los servidores. Debe colocarse en el mismo lado del firewall (y de la unidad VPN, si se utiliza) que los servidores.

Evite los problemas de NAT

La traducción de direcciones de red (NAT) en el lado del plug-in se maneja de forma transparente y no es una preocupación. En el lado del dispositivo, NAT puede ser problemático. Aplique las siguientes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

directrices para garantizar una implementación sin problemas:

- Coloque el dispositivo en el mismo espacio de direcciones que los servidores, de modo que las modificaciones de dirección que se utilicen para llegar a los servidores también se apliquen al dispositivo.
- Nunca acceda al dispositivo mediante una dirección que el dispositivo no se asocie a sí mismo.
- El dispositivo debe poder acceder a los servidores mediante las mismas direcciones IP en las que los usuarios del complemento tienen acceso a los mismos servidores.
- En resumen, no aplique NAT a las direcciones de servidores o dispositivos.

Seleccionar modo softboost

En la página Configurar Configuración: Gestión de Ancho de Banda, seleccione Modo Softboost. Softboost es el único tipo de aceleración compatible con WANOP Client Plug-in.

Definir reglas de aceleración de complementos

El dispositivo mantiene una lista de reglas de aceleración que indican a los clientes qué tráfico se debe acelerar. Cada regla especifica una dirección o subred y un intervalo de puertos que el dispositivo puede acelerar.

Qué acelerar: La elección del tráfico que se va a acelerar depende del uso al que se esté haciendo el dispositivo:

- Acelerador VPN: Si el dispositivo se utiliza como acelerador VPN, con todo el tráfico VPN pasando por el dispositivo, todo el tráfico TCP debe acelerarse, independientemente del destino.
- Modo de redirector: A diferencia del modo transparente, un dispositivo en modo de redirector es un proxy explícito, lo que hace que el complemento reenvíe su tráfico al dispositivo en modo de redirector incluso cuando lo haga no es quiereble. La aceleración puede ser contraproducente si el cliente reenvía el tráfico a un dispositivo distante del servidor, especialmente si esta ruta triangular introduce un vínculo lento o poco fiable. Por lo tanto, Citrix recomienda configurar reglas de aceleración para permitir que un dispositivo determinado acelere únicamente su propio sitio.
- Otros usos: Cuando el complemento no se utiliza como acelerador VPN ni en modo redirector, las reglas de aceleración deben incluir direcciones remotas para los usuarios y locales para los centros de datos.

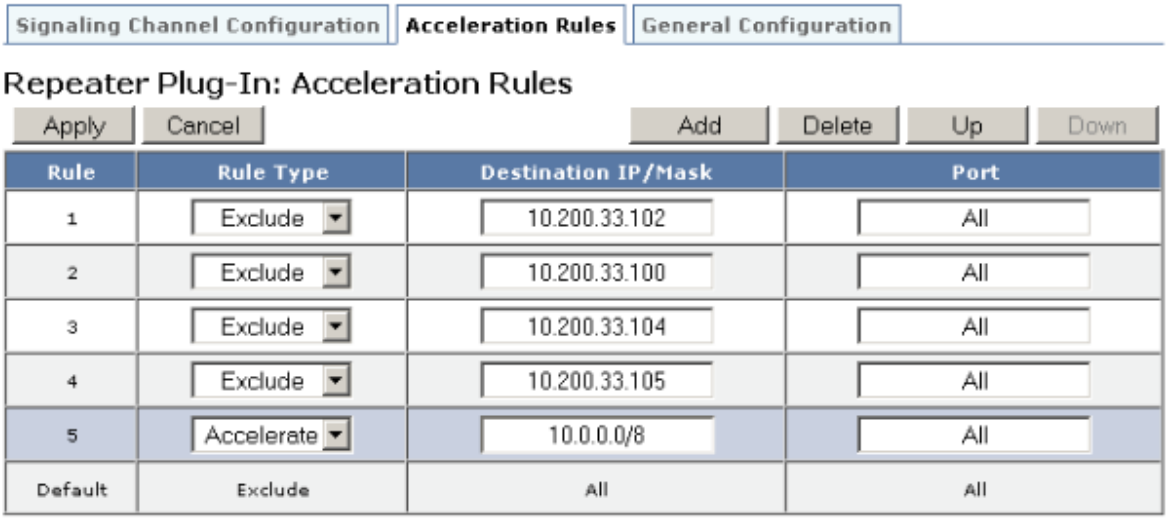
Definir las reglas: Definir reglas de aceleración en el dispositivo, en la ficha **Configuración: WANOP Client Plug-in: Reglas de aceleración**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Las reglas se evalúan en orden y la acción (Acelerar o Excluir) se toma desde la primera regla coincidente. Para que una conexión se acelere, debe coincidir con una regla Acelerar.

La acción predeterminada es no acelerar.

Ilustración 1. Configuración de reglas de aceleración



1. En la ficha Configuración: WANOP Plug-in: Reglas de aceleración:
   - Agregue una regla acelerada para cada subred local de LAN a la que pueda llegar el dispositivo. Es decir, haga clic en **Agregar**, seleccione **Acelerar**y escriba la dirección IP y la máscara de la subred.
   - Repita esta operación para cada subred que sea local en el dispositivo.
2. Si necesita excluir alguna parte del rango incluido, agregue una regla Excluir y muévalo por encima de la regla más general. Por ejemplo, 10.217.1.99 parece una dirección local. Si realmente es el punto final local de una unidad VPN, cree una regla Excluir para ella en una línea por encima de la regla Acelerar para 10.217.1.0/24.
3. Si quiere utilizar la aceleración para un solo puerto (no recomendado), como el puerto 80 para HTTP, reemplace el carácter comodín del campo Puertos por el número de puerto específico. Puede admitir puertos adicionales agregando reglas adicionales, una por puerto.
4. En general, haga una lista de reglas estrechas (generalmente excepciones) antes de las reglas generales.
5. Haga clic en **Aplicar**. Los cambios no se guardan si se desplaza fuera de esta página antes de aplicarlos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Uso del puerto IP

Utilice las siguientes directrices para el uso del puerto IP:

- **Puertos utilizados para la comunicación con el Plug-in de cliente WANOP**: El complemento mantiene un diálogo con el dispositivo a través de una conexión de señalización, que de forma predeterminada está en el puerto 443 (HTTPS), que se permite a través de la mayoría de los firewalls.
- **Puertos utilizados para la comunicación con servidores**: La comunicación entre el complemento cliente WANOP y el dispositivo utiliza los mismos puertos que el cliente utilizaría para la comunicación con el servidor si el complemento y el dispositivo no estuvieran presentes. Es decir, cuando un cliente abre una conexión HTTP en el puerto 80, se conecta al dispositivo en el puerto 80. El dispositivo, a su vez, se pone en contacto con el servidor en el puerto 80.

  En el modo de redirector, se conserva el puerto conocido (es decir, el puerto de destino en el paquete TCP SYN). El puerto efímero no se conserva. En modo transparente, ambos puertos se conservan.

  El dispositivo supone que puede comunicarse con el servidor en cualquier puerto solicitado por el cliente, y el cliente asume que puede comunicarse con el dispositivo en cualquier puerto quieredo. Esto funciona bien si el dispositivo está sujeto a las mismas reglas de firewall que los servidores. Cuando tal es el caso, cualquier conexión que tenga éxito en una conexión directa tendrá éxito en una conexión acelerada.

Uso de opciones TCP y firewalls

Los parámetros de WANOP Client Plug-in se envían en las opciones TCP. Las opciones TCP pueden ocurrir en cualquier paquete y se garantiza que estarán presentes en los paquetes SYN y SYN-ACK que establecen la conexión.

El firewall no debe bloquear las opciones TCP en el rango de 24-31 (decimal), o la aceleración no puede tener lugar. La mayoría de los firewalls no bloquean estas opciones. Sin embargo, un firewall Cisco PIX o ASA con firmware de la versión 7.x podría hacerlo de forma predeterminada y, por lo tanto, es posible que tenga que ajustar su configuración.

Personalizar el archivo MSI del complemento

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede cambiar los parámetros en el archivo de distribución
WANOP Client Plug-in, que está en el formato estándar de Microsoft Installer (MSI). La personalización requiere el uso de un editor MSI.

> **Nota**
>
> Los parámetros modificados en su edición. El archivo MSI se aplica a las instalaciones nuevas. Cuando los usuarios de complementos existentes se actualizan a una nueva versión, se conserva la configuración existente. Por lo tanto, después de cambiar los parámetros, debe aconsejar a sus usuarios que desinstalen la versión anterior antes de instalar la nueva.

Prácticas recomendadas:

Cree una entrada DNS que se resuelva al dispositivo habilitado para el complemento más cercano. Por ejemplo, defina Repeater.MyCompany.com y haga que se resuelva en su dispositivo, si tiene un dispositivo. O bien, si tiene, digamos, cinco dispositivos, haga que Repeater.MyCompany.Com resuelva a uno de sus cinco dispositivos, con el dispositivo seleccionado sobre la base de la cercanía al cliente o a la unidad VPN. Por ejemplo, un cliente que utilice una dirección asociada a una VPN determinada debería ver Repeater.MyCompany.COM resolver en la dirección IP del dispositivo WANOP Client Plug-in conectado a esa VPN. Cree esta dirección en su binario de plug-in con un editor MSI, como Orca. Al agregar, mover o quitar dispositivos, al cambiar esta única definición de DNS en el servidor DNS se actualiza automáticamente la lista de dispositivos en los complementos.

También puede hacer que la entrada DNS se resuelva en varios dispositivos, pero esto no es quiereble a menos que todos los dispositivos estén configurados de manera idéntica, ya que el complemento toma algunas de sus funciones del dispositivo situado más a la izquierda de la lista y las aplica globalmente (incluidas las funciones de compresión SSL). Esto puede dar lugar a resultados inquierebles y confusos, especialmente si el servidor DNS gira el orden de las direcciones IP para cada solicitud.

Instale Orca MSI Editor:

Hay muchos editores MSI como Orca, que es parte del SDK gratuito de plataforma de Microsoft y se puede descargar desde Microsoft.

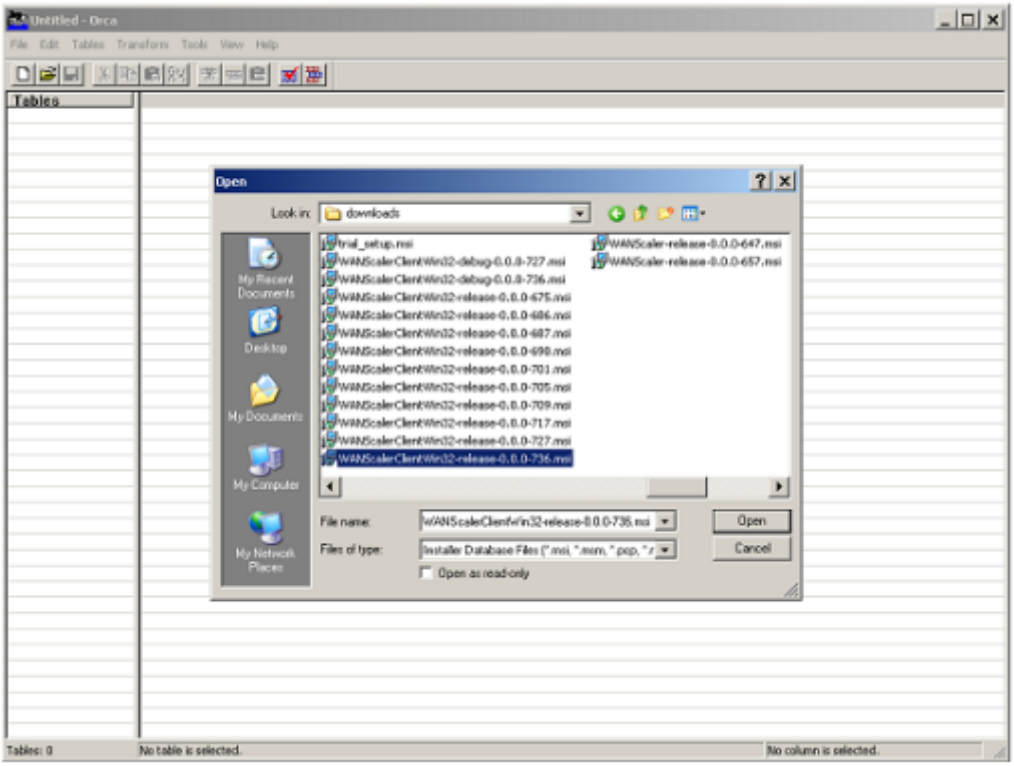
- Para instalar Orca MSI Editor

  1. Descargue la versión PSDK-x86.exe del SDK y ejecútelo. Siga las instrucciones de instalación.
  2. Una vez instalado el SDK, se debe instalar el editor Orca. Estará en Microsoft Platform SDK\Bin\Orca.Msi. Inicie Orca.msi para instalar el editor Orca real (orca.exe).
  3. **Ejecución de Orca**: Microsoft proporciona la documentación de Orca en línea. La siguiente información describe cómo modificar los parámetros más importantes del complemento de cliente WANOP.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Inicie Orca con **Inicio > Todos los programas > Orca.** Cuando aparezca una ventana Orca en blanco, abra el archivo MSI del complemento WANOP Client Plug-in con **Archivo > Abrir**.

Ilustración 1. Uso de Orca



5. En el menú **Tablas** , haga clic en **Propiedad**. Aparecerá una lista de todas las propiedades modificables del archivo MSI. Modifique los parámetros que se muestran en la tabla siguiente. Para modificar un parámetro, haga doble clic en su valor, escriba el nuevo valor y pulse **Intro**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Descripción	Predeterminado	Comentarios
WSAPPLIANCES	Lista de dispositivos	Ninguno	Introduzca aquí las direcciones IP o DNS de sus dispositivos WANOP, en una lista separada por comas en forma de {appliance1, appliance2, appliance3}. Si el puerto utilizado para las conexiones de señalización es diferente del predeterminado (443), especifique el puerto con el formato Appliance1:Port_Number.
DBCMINSIZE	Cantidad mínima de espacio en disco que se utilizará para la compresión, en megabytes	250	Cambiar esto a un valor mayor (por ejemplo, 2000) mejora el rendimiento de compresión, pero impide la instalación si no hay suficiente espacio en disco. El complemento no se instalará a menos que haya al menos 100 MB de espacio libre en disco además del valor especificado para DBCMINSIZE.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Descripción	Predeterminado	Comentarios
EKEYPEM	Clave privada para el complemento. Parte del par de certificados/claves utilizado con compresión SSL	Ninguno	Utilice el comando Pegar celda de Orca. La función Pegar normal no conserva el formato de la clave. Debería ser una clave privada en formato PEM (comenzando con —BEGIN RSA PRIVATE KEY—)
X509CERTPEM	Certificado para el complemento. Parte del par de certificados/claves utilizado con compresión SSL	Ninguno	Utilice el comando Pegar celda de Orca. La función Pegar normal no conserva el formato de la clave. Debe ser un certificado en formato PEM (empezando por — BEGIN CERTIFICATE —)
CACERTPEM	Certificado de entidad emisora de certificados para el complemento. Utilizado con compresión SSL	Ninguno	Utilice el comando Pegar celda de Orca. La función Pegar normal no conserva el formato de la clave. Debe ser un certificado en formato PEM (empezando por — BEGIN CERTIFICATE —)

6. En el menú Tablas, haga clic en Propiedad. Aparecerá una lista de todas las propiedades modificables del archivo MSI. Modifique los parámetros que se muestran en la tabla siguiente. Para modificar un parámetro, haga doble clic en su valor, escriba el nuevo valor y pulse **Intro**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Descripción	Predeterminado	Comentarios
WSAPPLIANCES	Lista de dispositivos	Ninguno	Introduzca aquí las direcciones IP o DNS de sus dispositivos WANOP Client Plug-in, en una lista separada por comas en forma de *{appliance1, appliance2, appliance3}*. Si el puerto utilizado para las conexiones de señalización es diferente del predeterminado (443), especifique el puerto con el formato *Appliance1:número_puerto*.
DBCMINSIZE	Cantidad mínima de espacio en disco que se utilizará para la compresión, en megabytes	250	Cambiar esto a un valor mayor (por ejemplo, 2000) mejora el rendimiento de compresión, pero impide la instalación si no hay suficiente espacio en disco. El complemento no se instalará a menos que haya al menos 100 MB de espacio libre en disco además del valor especificado para DBCMINSIZE.

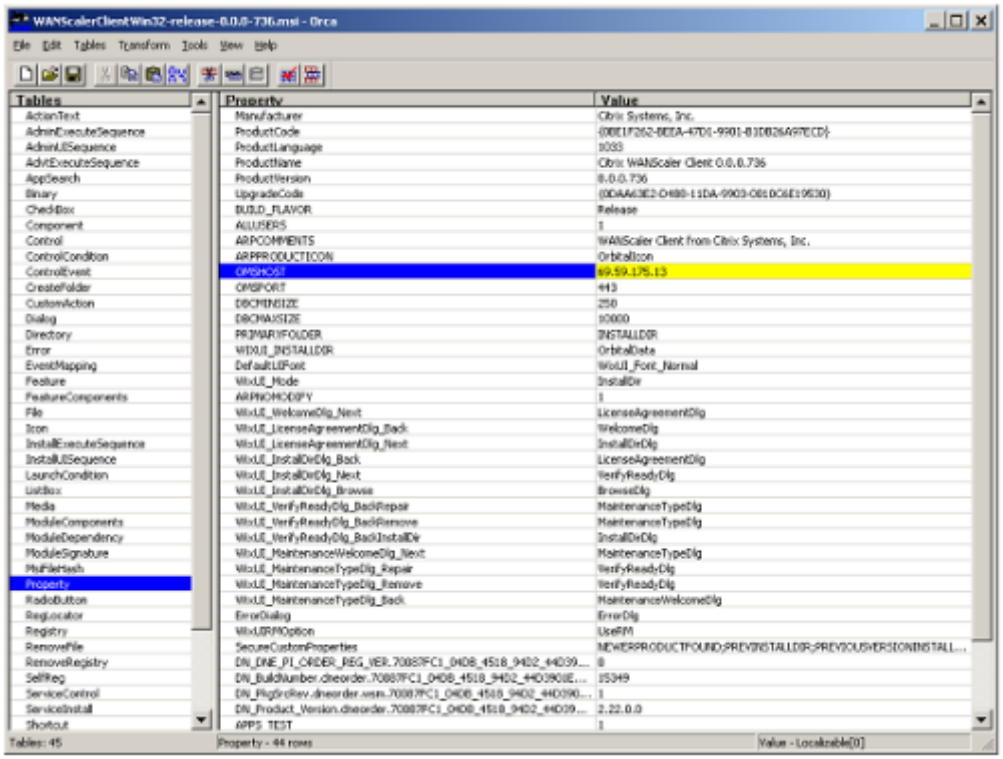
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro	Descripción	Predeterminado	Comentarios
PRIVATEKEYPEM	Clave privada para el complemento. Parte del par de certificados/claves utilizado con compresión SSL	Ninguno	Utilice el comando Pegar celda de Orca. La función Pegar normal no conserva el formato de la clave. Debería ser una clave privada en formato PEM (comenzando con —BEGIN RSA PRIVATE KEY—)
X509CERTPEM	Certificado para el complemento. Parte del par de certificados/claves utilizado con compresión SSL	Ninguno	Utilice el comando Pegar celda de Orca. La función Pegar normal no conserva el formato de la clave. Debe ser un certificado en formato PEM (empezando por — BEGIN CERTIFICATE —)
CACERTPEM	Certificado de entidad emisora de certificados para el complemento. Utilizado con compresión SSL	Ninguno	Utilice el comando Pegar celda de Orca. La función Pegar normal no conserva el formato de la clave. Debe ser un certificado en formato PEM (empezando por — BEGIN CERTIFICATE —)

7. Cuando termine, utilice el comando **Archivo: Guardar como** para guardar el archivo modificado con un nuevo nombre de archivo; por ejemplo, test.msi.

   Figura 2: Modificar parámetros en Orca:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Cuando termine, utilice el comando **Archivo: Guardar como** para guardar el archivo modificado con un nuevo nombre de archivo; por ejemplo, test.msi.

   Su software de plug-in ya ha sido personalizado.

   > **Nota**
   >
   > Algunos usuarios han visto un error en orca que hace que trunque los archivos a 1 MB. Compruebe el tamaño del archivo guardado. Si se ha truncado, realice una copia del archivo original y utilice el comando Guardar para sobrescribir el original.

   Una vez que haya personalizado la lista de dispositivos con Orca y distribuido el archivo MSI personalizado a los usuarios, el usuario no necesita escribir ninguna información de configuración al instalar el software.

Implementar complementos en sistemas Windows

May 7, 2021

WANOP Client Plug-in es un archivo ejecutable de Microsoft Installer (MSI) que se descarga e instala como ocurre con cualquier otro programa distribuido por Internet. Obtenga este archivo desde la sección MyCitrix del sitio web de Citrix.com.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La interfaz de usuario de WANOP Client Plug-in se denomina **Citrix Acceleration Plug-in Manager**.

La única configuración de usuario que necesita el complemento es la lista de direcciones del dispositivo. Esta lista puede consistir en una lista separada por comas de direcciones IP o DNS. Las dos formas se pueden mezclar. Puede personalizar el archivo de distribución para que la lista señale al dispositivo de forma predeterminada. Una vez instalado, el funcionamiento es transparente. El tráfico a las subredes aceleradas se envía a través de un dispositivo adecuado y el resto del tráfico se envía directamente al servidor. La aplicación de usuario no sabe que nada de esto está sucediendo.

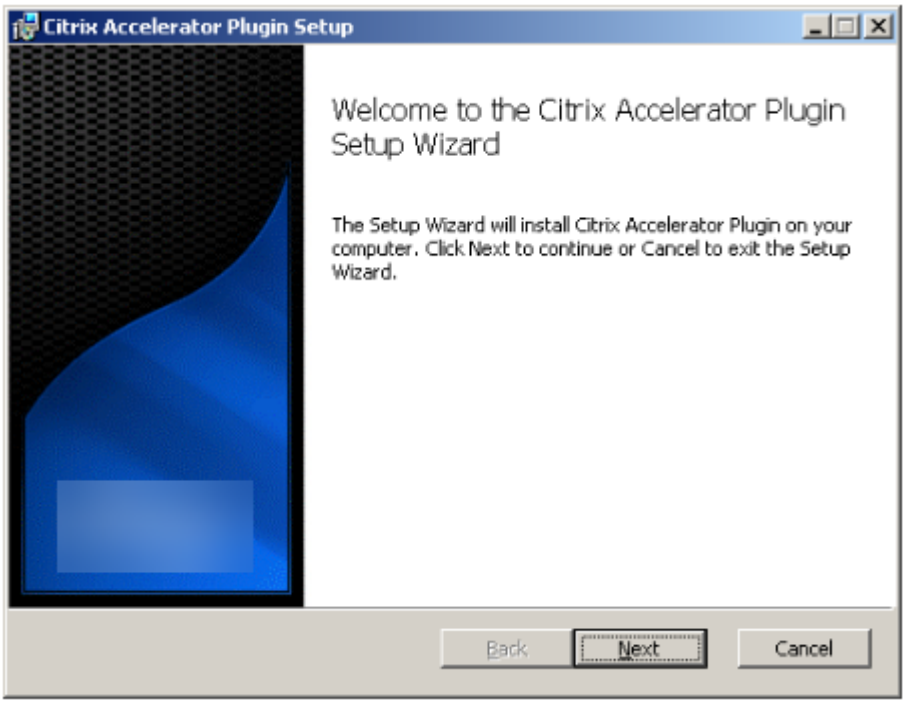
Instalación

> **Requisitos previos:**
>
> Windows 10 requiere que todos los controladores tengan una firma digital válida para realizar la instalación sin ningún error.

Para instalar WANOP Client Plug-in acelerador en el sistema Windows:

1. El archivo Repeater*.msi es un archivo de instalación. Cierre todas las aplicaciones y cualquier ventana que pueda estar abierta y, a continuación, inicie el instalador de la manera habitual (haga doble clic en una ventana de archivo o utilice el comando run).

   Ilustración 1. Pantalla de instalación inicial:



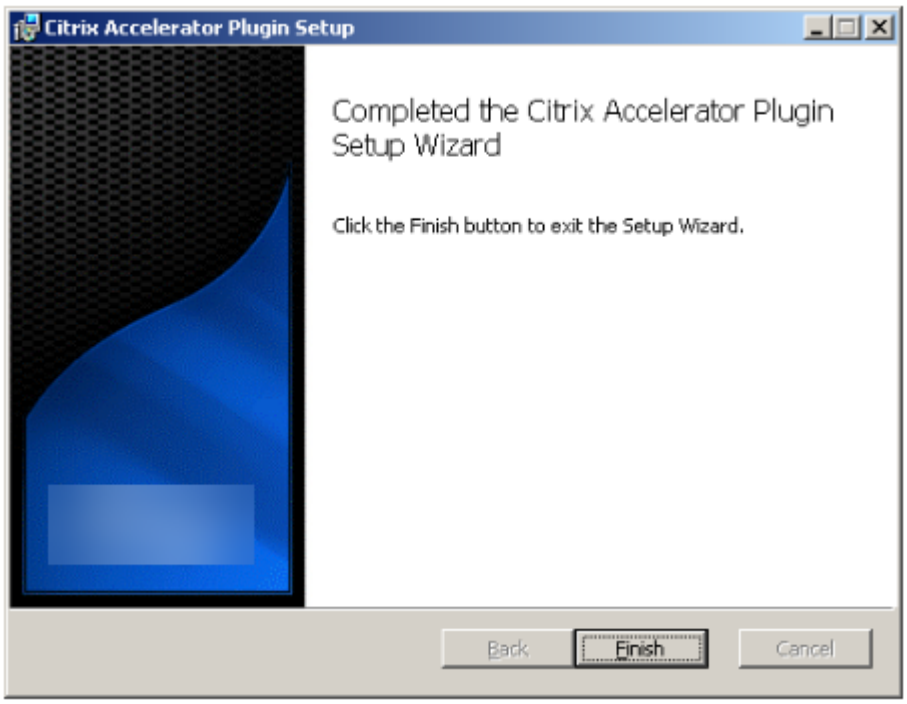
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los pasos que se indican a continuación son para una instalación interactiva. Se puede realizar una instalación silenciosa con el comando:

msiexec /i client_msi_file /qn

2. El programa de instalación solicita la ubicación en la que quiere instalar el software. El directorio que especifique se utiliza tanto para el software cliente como para el historial de compresión basado en disco. Juntos, requieren un mínimo de 500 MB de espacio en disco.
3. Cuando finalice el instalador, es posible que le pida que reinicie el sistema. Después de reiniciar, el complemento cliente WANOP se inicia automáticamente.

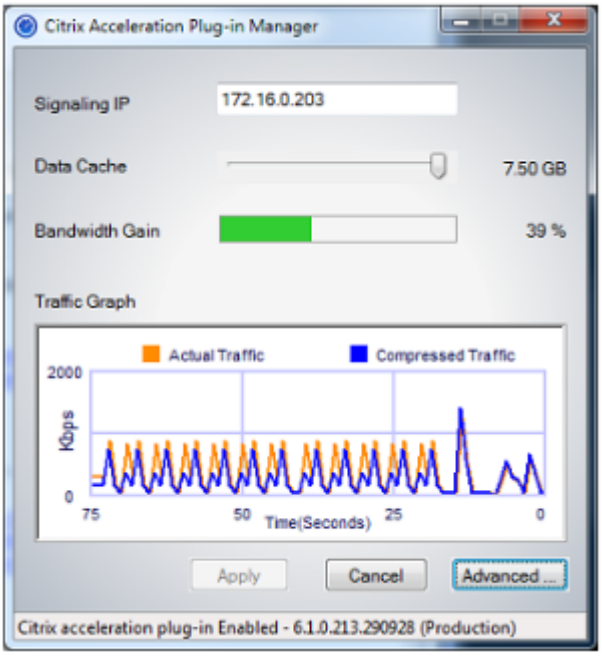
Ilustración 2. Pantallade instalación final



4. Haga clic con el botón derecho en el icono Acelerador de la barra de tareas y seleccione **Administrar aceleración** para iniciar Citrix Plug-in Accelerator Manager.

Imagen 3. Citrix Accelerator Plug in Manager, pantallainicial (básica)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Si el archivo.MSI no se ha personalizado para los usuarios, especifique la dirección de señalización y la cantidad de espacio en disco que se utilizará para la compresión:

   - En el campo Dispositivos: Direcciones de señalización, escriba la dirección IP de señalización del dispositivo. Si tiene más de un dispositivo habilitado para Plug-in, enumérelos todos, separados por comas. Las direcciones IP o DNS son aceptables.
   - Con el control deslizante Caché de datos, seleccione la cantidad de espacio en disco que se va a utilizar para la compresión. Más es mejor. 7.5 GB no es demasiado, si tiene tanto espacio en disco disponible.
   - Pulse Aplicar.

     Ahora se está ejecutando el acelerador WANOP Client Plug-in. Todas las conexiones futuras a subredes aceleradas se acelerarán

     En la ficha Reglas avanzadas del complemento, la lista Reglas de aceleración debe mostrar cada dispositivo como Conectado y las subredes aceleradas de cada dispositivo como Acelerado. Si no es así, compruebe el campo IP de Direcciones de señalización y la conectividad de red en general.

Solucionar problemas de complementos

La instalación del plug-in generalmente se realiza sin problemas. Si no es así, compruebe los siguientes problemas:

Problemas comunes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si no reinicia el sistema, el complemento cliente WANOP no se ejecutará correctamente.
- Un disco muy fragmentado puede resultar en un rendimiento de compresión deficiente.
- Un error de aceleración (no hay conexiones aceleradas enumeradas en la ficha **Diagnóstico**) suele indicar que algo impide la comunicación con el dispositivo. Compruebe la lista **Configuración: Reglas de aceleración** del complemento para asegurarse de que se está contactando correctamente con el dispositivo y de que la dirección de destino está incluida en una de las reglas de aceleración. Las causas típicas de fallas de conexión son:
  - El dispositivo no se está ejecutando o la aceleración se ha desactivado.
  - Un firewall está quitando las opciones TCP del complemento de cliente WANOP en algún punto entre el complemento y el dispositivo.
  - El complemento utiliza una VPN no compatible.

Error de bloqueo del potenciador de red determinista

En raras ocasiones, después de instalar el complemento y reiniciar el equipo, aparece el siguiente mensaje de error dos veces:

La instalación Deterministic Network Enhancer requiere un reinicio primero, para liberar recursos bloqueados. Vuelva a ejecutar esta instalación después de reiniciar el equipo.

Si esto ocurre, haga lo siguiente:

1. Vaya a **Agregar o quitar programas** y quite el complemento de cliente WANOP, si está presente.
2. Vaya a **Panel de control** > **Adaptadores de red** > **Conexión de área local** > **Propiedades**, busque la entrada de Deterministic Network Enhancer, desactive su casilla de verificación y haga clic en **Aceptar**. (Es posible que se llame al adaptador de red con un nombre distinto de Conexión de área local.)
3. Abra una ventana de comandos y vaya a c:windowsinf (o el directorio equivalente si ha instalado Windows en una ubicación no estándar).
4. Escriba el siguiente comando:

   find dne2000.cat oem*.inf
5. Busque el archivo oem*.inf con mayor número que devolvió una línea coincidente (la línea coincidente es catalogFile= dne2000.cat) y edítelo. Por ejemplo:

   bloc de notas oem13.inf
6. Elimine todo excepto las tres líneas de la parte superior que comienzan con punto y coma y, a continuación, guarde el archivo. Esto borrará cualquier configuración inapropiada u obsoleta y la siguiente instalación utilizará valores predeterminados.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Vuelva a intentar la instalación.

Otros problemas de instalación

Cualquier problema con la instalación de WANOP Client Plug-in suele ser el resultado de una red existente, firewall o software antivirus que interfiere con la instalación. Por lo general, una vez que la instalación se completa, no hay más problemas.

Si se produce un error en la instalación, pruebe los siguientes pasos:

1. Asegúrese de que el archivo de instalación del complemento se haya copiado en el sistema local.
2. Desconecte cualquier cliente de red VPN/remota activa.
3. Inhabilite temporalmente cualquier firewall y software antivirus.
4. Si algo de esto es difícil, haga lo que puedas.
5. Vuelva a instalar el complemento cliente WANOP.
6. Si esto no funciona, reinicie el sistema e inténtelo de nuevo.

Comandos de GUI del plug-in WANOP

May 7, 2021

La interfaz gráfica de usuario de WANOP Client Plug-in aparece cuando hace clic con el botón derecho en el icono **Citrix Accelerator Plug-in** y selecciona **Administrar aceleración**. La pantalla básica de la GUI aparece primero. También hay una pantalla avanzada que se puede utilizar si lo quiere.

Pantalla básica

En la página Básico, puede establecer dos parámetros:

- El campo Direcciones de señalización especifica la dirección IP de cada dispositivo al que se puede conectar el complemento. Citrix recomienda incluir un dispositivo, pero puede crear una lista separada por comas. Esta es una lista ordenada, con los dispositivos más a la izquierda tienen prioridad sobre los demás. Se intenta acelerar con el dispositivo situado más a la izquierda para el que se puede establecer una conexión de señalización. Puede utilizar direcciones DNS y direcciones IP.

  Ejemplos: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

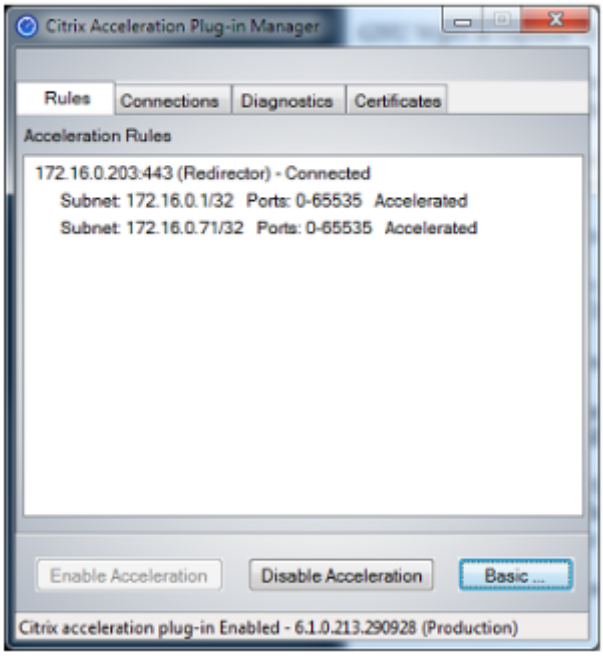
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- El control deslizante Caché de datos ajusta la cantidad de espacio en disco asignado al historial de compresión basado en disco del complemento. Más es mejor.

  Además, hay un botón para mover a la pantalla Avanzada.

Pantalla avanzada

La página Avanzadas contiene cuatro fichas: Reglas, Conexiones, Diagnósticos y Certificados.



En la parte inferior de la pantalla hay botones para activar la aceleración, desactivar la aceleración y volver a la página Básica.

Ficha Reglas

La ficha Reglas muestra una lista abreviada de las reglas de aceleración descargadas de los dispositivos. Cada elemento de la lista muestra la dirección y el puerto de señalización del dispositivo, el modo de aceleración (redirector o transparente) y el estado de conexión, seguido de un resumen de las reglas del dispositivo.

Ficha Conexiones

La ficha **Conexiones** muestra el número de conexiones abiertas de diferentes tipos:

- **Conexiones aceleradas**: Número de conexiones abiertas entre el Plug-in de cliente WANOP y los dispositivos. Este número incluye una conexión de señalización por dispositivo, pero no

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

incluye conexiones CIFS aceleradas. Al hacer clic en Más, se abre una ventana con un breve resumen de cada conexión. (Todos los botones Más le permiten copiar la información de la ventana en el portapapeles, si quiere compartirla con Soporte).

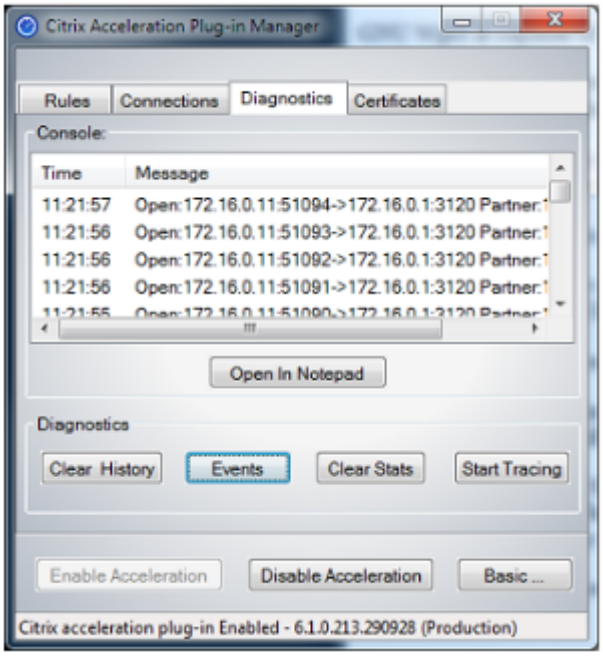
- **Conexiones CIFS aceleradas**: Número de conexiones abiertas y aceleradas con servidores CIFS (sistema de archivos de Windows). Esto suele ser el mismo que el número de sistemas de archivos de red montados. Al hacer clic en Más, se muestra la misma información que con las conexiones aceleradas, además de un campo de estado que indica Activo si la conexión CIFS se ejecuta con las optimizaciones CIFS especiales de WANOP Client Plug-in.
- Conexiones**MAPI aceleradas: Número de conexiones**abiertas y aceleradas de Outlook/Exchange.
- **Conexiones ICA aceleradas**: Número de conexiones abiertas y aceleradas de XenApp y XenDesktop que utilizan los protocolos ICA o CGP.
- **Conexiones no aceleradas**: Abre conexiones que no se están acelerando. Puede hacer clic en Más para mostrar una breve descripción de por qué no se aceleró la conexión. Normalmente, el motivo es que ningún dispositivo acelera la dirección de destino, que se notifica como regla de directiva de servicio.
- **Abrir/cerrar conexiones**: Conexiones que no están completamente abiertas, pero que están en proceso de apertura o cierre (conexiones TCP semiabiertas o semicerradas). El botón Más muestra información adicional sobre estas conexiones.

Ficha Diagnóstico

La página Diagnósticos indica el número de conexiones en diferentes categorías y otra información útil.

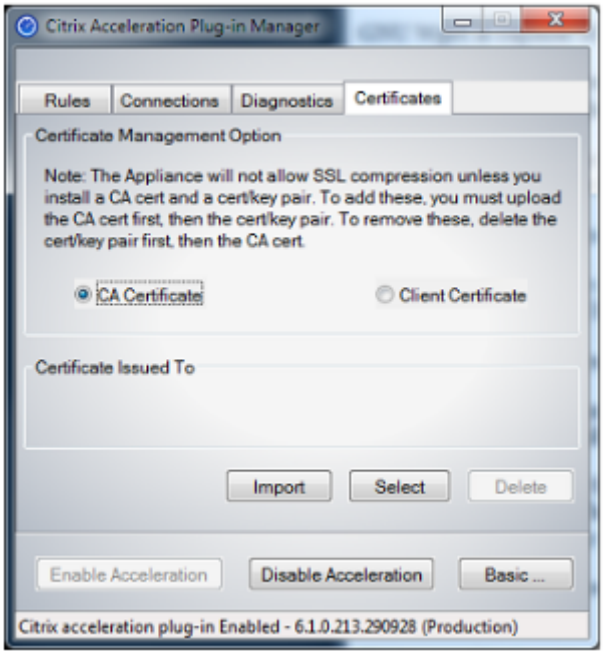
- **Iniciar seguimiento/detención de seguimiento**: Si informa de un problema, es posible que su representante de Citrix le pida que realice un seguimiento de conexión para identificar los problemas. Este botón inicia y detiene el seguimiento. Cuando se detiene el seguimiento, una ventana emergente muestra los archivos de seguimiento. Envíelos a su representante de Citrix por los medios que le recomiende.
- **Borrar historial**: No se debe utilizar esta función.
- **Borrar estadísticas**: Al pulsar este botón se borran las estadísticas de la ficha Rendimiento.
- **Consola**: Ventana desplazable con mensajes de estado recientes, principalmente mensajes de apertura de conexión y cierre de conexión, pero también mensajes de error y de estado varios.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ficha Certificados

En la ficha Certificados, puede instalar credenciales de seguridad para la función opcional de interconexión segura. El propósito de estas credenciales de seguridad es permitir que el dispositivo compruebe si el complemento es un cliente de confianza o no.



Para cargar el certificado de CA y el par de claves de certificado:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Seleccione **Administración de certificados de**CA.
2. Haga clic en **Importar**.
3. Cargue un certificado de CA. El archivo de certificado debe utilizar uno de los tipos de archivo admitidos (.pem,.crt.,.cer o.spc). Puede aparecer un cuadro de diálogo en el que se le pida que seleccione el almacén de certificados que quiere utilizar y se le presente una lista de palabras clave. Seleccione la primera palabra clave de la lista.
4. Seleccione **Administración de certificados de cliente**.
5. Haga clic en **Importar**.
6. Seleccione el formato del par de claves de certificado (PKCS12 o PEM/DER).
7. Haga clic en **Enviar**.

> **Nota**
>
> En el caso de PEM/DER, hay cajas de carga separadas para el certificado y la clave. Si el par de claves de certificado se combina en un solo archivo, especifique el archivo dos veces, una vez para cada cuadro.

Actualizar el complemento WANOP

May 7, 2021

Para instalar una versión más reciente del complemento cliente WANOP, siga el mismo procedimiento que utilizó al instalar el complemento por primera vez.

Desinstalar el complemento cliente WANOP

Para desinstalar el complemento WANOP Client, utilice la utilidad Agregar o quitar programas de Windows. WANOP Client Plug-in aparece como **Citrix Acceleration Plug-in** en la lista de programas instalados actualmente. Selecciónelo y haga clic en **Quitar**.

Debe reiniciar el sistema para terminar de desinstalar el cliente.

Solucionar problemas del complemento WANOP

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Problema**: Me enfrento a problemas de conectividad del canal de señalización. ¿Cómo puedo resolver estos problemas?

  Resolución: Para resolver problemas de conectividad del canal de señalización, lleve a cabo los siguientes pasos de solución de problemas:

  - Compruebe que ha configurado correctamente la dirección IP de señalización. Puede hacerlo haciendo ping a la dirección IP de señalización y verificando la respuesta.
  - Compruebe que el estado de señalización esté habilitado en el dispositivo WANOP.
  - Compruebe que el firewall instalado en la red no elimina las opciones TCP WANOP.
  - Compruebe que hay instalada una licencia de complemento WANOP válida en el dispositivo WANOP.
  - Compruebe que la configuración de Filtrado de Origen de Canal de Señalización no bloquee la dirección IP de Origen del Cliente.
  - Si ha habilitado la detección de LAN, compruebe que el tiempo de ida y vuelta entre el complemento WANOP y el dispositivo WANOP sea un valor aceptable.

- **Problema**: En un dispositivo WANOP 4000, no puedo inhabilitar el complemento WANOP.

  Causa: Se trata de un problema conocido.

  Resolución: Ninguna. No se puede inhabilitar el complemento WANOP en un dispositivo WANOP 4000.

- **Problema**: Al conectarse al dispositivo WANOP mediante el complemento WANOP, se registra la siguiente entrada de mensaje de error en la ficha Alertas:

  Más plug-ins WANOP que el límite actual de <Number> han intentado conectarse a este dispositivo.

  Causa: El número de conexiones al dispositivo WANOP ha superado el límite de usuarios con licencia.

  Resolución: Espere a que un usuario se desconecte o termine una conexión.

- **Problema**: La dirección IP de señalización incorrecta está configurada en un dispositivo WANOP 4000 o 5000.

  Resolución: Para actualizar la dirección IP de señalización en un dispositivo WANOP 4000 o 5000, siga el procedimiento siguiente:

  1. Inicie sesión en la instancia de NetScaler del dispositivo WANOP.
  2. Acceda a la página Gestión del tráfico > Equilibrio de carga > Servidores virtuales > BR_LB_VIP_SIG.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Actualice la dirección IP de señalización.
4. Guarde la configuración.

- **Problema**: El tráfico CIFS e ICA no se está acelerando.

  Solución: Para resolver este problema, realice los siguientes pasos de solución de problemas:

  - Compruebe que las reglas de aceleración para la dirección IP y los números de puerto estén correctamente definidas para el complemento WANOP.
  - Compruebe que las conexiones CIFS o ICA se establecen después de que la conexión de señalización sea correcta.
  - Verifique la directiva de aceleración para la clase de servicio que se está utilizando.

Conexión SMB 3.1.1

May 7, 2021

El protocolo de bloque de mensajes de servidor (SMB) es un protocolo de uso compartido de archivos de red. Los paquetes de mensajes que definen una versión concreta del protocolo se denominan dialecto. El protocolo del sistema común de archivos de Internet (CIFS) es un dialecto de SMB.

En Citrix SD-WAN versión 10 versión 1, el protocolo SMB 3.1.1 se introduce en las plataformas Citrix SD-WAN WANOP y Premium Edition.

Citrix SD-WAN WANOP admite conexiones SMB 3.1.1. Las conexiones SMB 3.1.1 son aplicables cuando el cliente es Windows 10 y el servidor es Windows Server 2016.

Cuando el tráfico SMB 3.1.1 pasa a través del módulo WANOP:

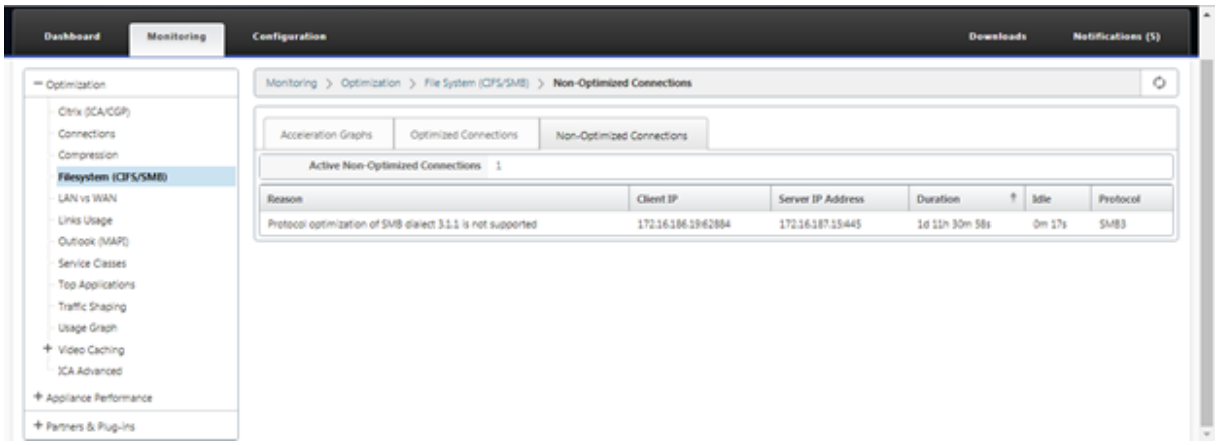
- Es contado/visible como parte de las conexiones CIFS no optimizadas SMB 3.1
- Se muestra el siguiente mensaje de seguimiento, “Pasar a través de esta conexión como SMB 3.1.1 no es compatible”.

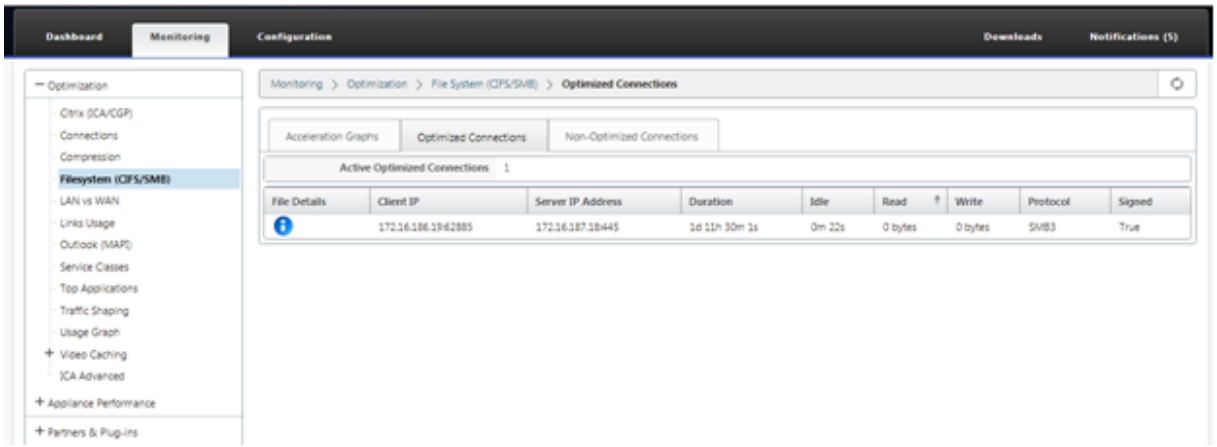
Cliente	Servidor	Versión SMB
Windows 10	Win 2016, 2012R2	SMB 3.1.1, 3.0.2
Windows 8.1	SMB 3,0	SMB 3,0
Windows 7	SMB 3,0	SMB 3,0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para conexiones no optimizadas, la GUI del dispositivo WANOP de Citrix SD-WAN muestra un mensaje para SMB 3.1.1.

En la GUI del dispositivo WANOP de Citrix SD-WAN, vaya a **Monitoring** > **Filesystem (CIFS/SMB)**. Haga clic en la ficha **Conexiones no optimizadas**, aparece el siguiente mensaje: *Optimización de protocolo del dialecto SMB 3.1.1 no es compatible*. No hay entradas de registro disponibles y no se requiere ninguna nueva configuración en SD-WAN WANOP para admitir esto.





Artículos prácticos

May 7, 2021

Los Artículos prácticos 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 un nombre de función a continuación para ver la lista de artículos de procedimientos para esa función.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Redirección y reenvío virtuales
- Habilitación de RED para la equidad de QoS
- Configuración
- Redirección dinámica
- Servidor DHCP y retransmisión DHCP
- Filtros de ruta
- Terminación y supervisión de IPSec
- Secure Web Gateway
- QoS
- Operación compatible con FIPS - Túnel IPSec
- Configuración NAT dinámica
- Detección de ancho de banda adaptable
- Pruebas de ancho de banda activo
- Mejoras de BGP
- Asociación de clases de servicio con perfiles SSL
- Emparejamiento seguro y Emparejamiento seguro manual
- Implementación sin contacto
- Implementación en modo de dos cajas

Grupos de interfaz

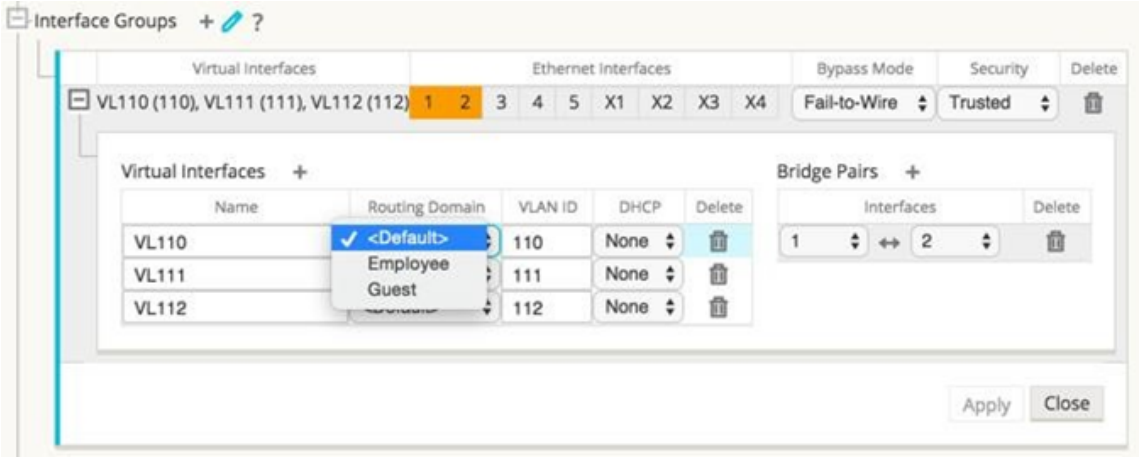
May 7, 2021

Para configurar grupos de interfaces:

1. En el **Editor de configuración**, vaya a **Sitios**> **[Nombre del sitio del cliente]**> **Grupos de interfaz**, elija un **dominio de enrutamiento**en el menú implementable al configurar interfaces virtuales. Para obtener instrucciones detalladas, consulte configurar grupos de interfaces.

   > **Nota**
   >
   > Una vez que las interfaces virtuales se asocian a un dominio de redirección específico, solo estarán disponibles esas interfaces cuando se utilice ese dominio de redirección.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



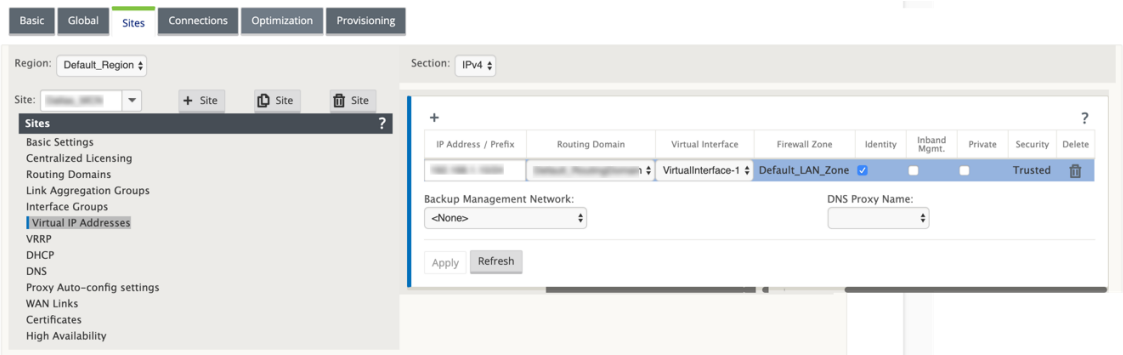
Configurar la identidad de la dirección IP virtual

May 7, 2021

La interfaz de red virtual puede alojar varias direcciones IP en las mismas subredes o diferentes. Sin embargo, solo puede seleccionar una IP virtual con la identidad establecida en true que se puede utilizar para protocolos de redirección dinámica como BGP/OSPF, servidor/relé DHCP y administración en banda.

Para configurar la identidad de la dirección IP virtual:

1. En el **Editor de configuración**, vaya a **Sitios** > **[Nombre del sitio]** > **Direcciones IP virtuales**.
2. Haga clic en la casilla **Identidad** de una dirección IP virtual para utilizarla para servicios IP.



Configurar la interfaz de acceso

September 26, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para configurar la interfaz de acceso:

1. En el **Editor de configuración**, vaya a **Sitios** > **[Nombre del sitio del cliente]** > **Vínculos WAN** > **[Nombre de vínculo WAN]** > **Interfaces de acceso**.
2. Seleccione un **dominio de enrutamiento** en el menú implementable al configurar una interfaz de acceso.

   Para obtener instrucciones detalladas, consulte la sección **Cómo configurar la interfaz de acceso** en el Configurar MCN tema.

Configurar direcciones IP virtuales

May 7, 2021

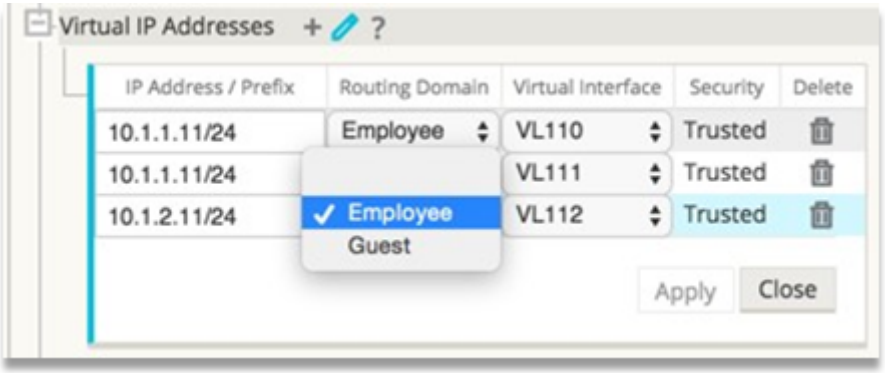
Para configurar direcciones IP virtuales:

1. En el **Editor de configuración**, vaya a **Sitios > [Nombre del sitio del cliente] > Direcciones IP virtuales**.
2. Elija un **dominio de enrutamiento** en el menú implementable al configurar direcciones IP virtuales.

   Para obtener instrucciones detalladas, consulte configurar direcciones IP virtuales.

El dominio de enrutamiento que elija determina qué interfaces virtuales están disponibles en el menú implementable.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



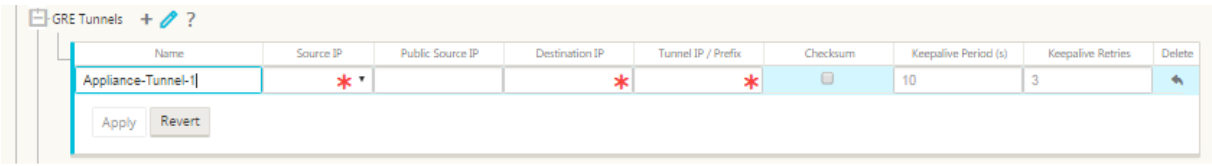
Configurar túneles GRE

May 7, 2021

Para configurar túneles GRE:

1. En el editor de configuración, vaya a **Conexiones**> **Sitio**> **Túneles GRE**. La dirección IP de origen se puede elegir de la interfaz de red virtual en vínculos de confianza.
2. Escriba un nombre para el túnel GRE.
3. Seleccione la dirección **IP de origen** disponible en el menú implementable. El dominio de redirección determina qué direcciones IP de origen están disponibles en el menú desplegable.
4. (Opcional) Seleccione la **IP de origen público**. Este campo puede estar vacío si esta dirección es la misma que la IP de origen.
5. Introduzca la dirección **IP de destino** del túnel GRE.
6. Introduzca la dirección **IP/prefijo del túnel** del túnel GRE.
7. Haga clic en **Suma de comprobación**, si quiere utilizar suma de comprobación en el encabezado del túnel GRE.
8. Introduzca un valor para el **Período Keepalive** en segundos. Si configura 0, no se transmite ningún paquete keepalive, pero el túnel GRE estará activo.
9. Introduzca un valor para los **reintentos de Keepalive**. Este valor determina el número de veces que se intentan reintentos keepalive antes de que el dispositivo SD-WAN desactive el túnel GRE.

Consulte elconfiguración de túneles GREen el sitio de MCN para obtener más información.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para obtener más información sobre cómo proteger la Gateway web mediante túneles GRE, consulte;Secure Web Gateway

Configurar rutas dinámicas para la comunicación de bifurcación a bifurcación

May 7, 2021

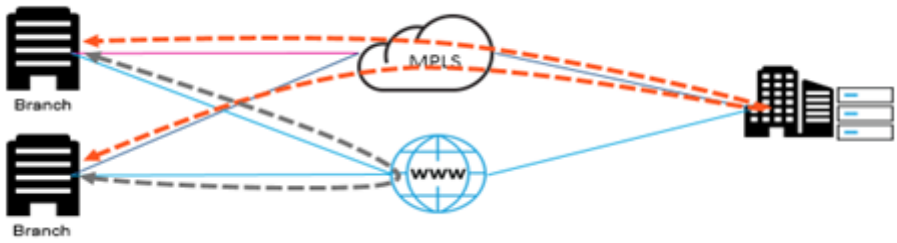
Con la demanda de VoIP y videoconferencias, el tráfico se mueve cada vez más entre oficinas. Es ineficiente configurar conexiones de malla completas a través de centros de datos, lo que puede llevar mucho tiempo.

Con Citrix SD-WAN, no es necesario configurar rutas entre cada oficina. Puede habilitar la función Ruta dinámica y la solución SD-WAN crea automáticamente rutas entre oficinas bajo demanda. La sesión utiliza inicialmente una ruta fija existente. Y a medida que se alcanzan 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 da como resultado 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:

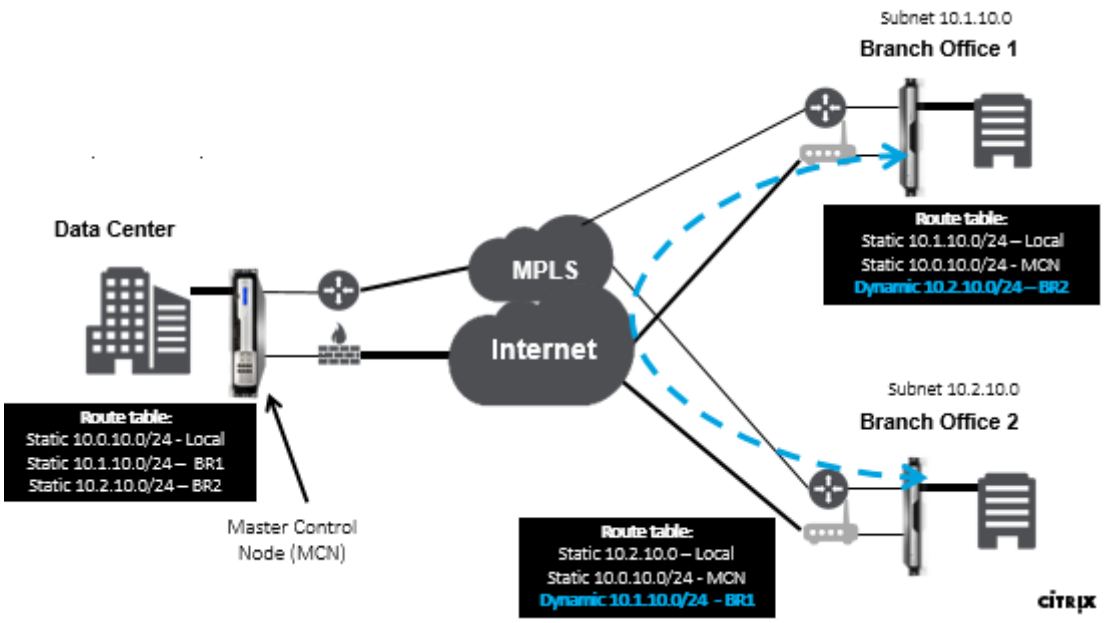
- Umbrales de ancho de banda y PPS para permitir conexiones de sucursal a sucursal
- Reduzca los requisitos de ancho de banda dentro y fuera del centro de datos al tiempo que minimiza la latencia
- Las rutas creadas a petición dependen de umbrales establecidos
- Liberar dinámicamente recursos de red cuando no sea necesario
- Reduzca la carga en el nodo principal de control y la latencia

Comunicación de bifurcación a bifurcación mediante rutas virtuales dinámicas:



Red SD-WAN con ruta dinámica:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



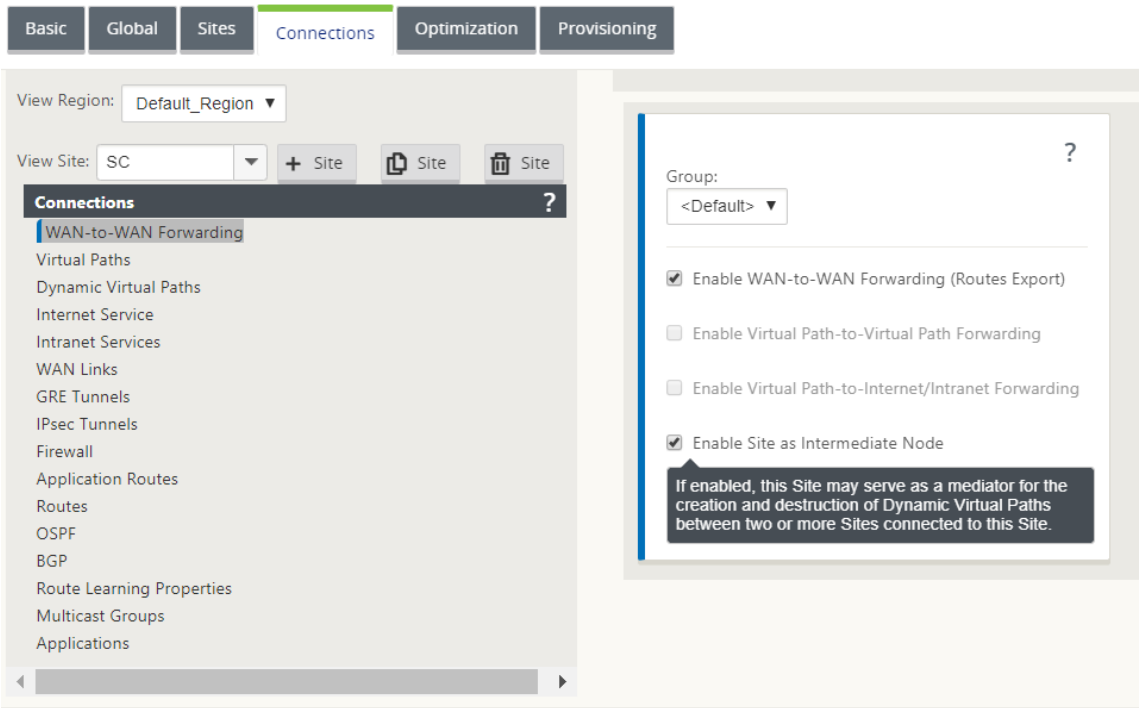
- Las rutas virtuales dinámicas se utilizan para implementaciones a gran escala, como Empresas
- Las implementaciones más pequeñas usan rutas virtuales estáticas y rutas virtuales de cualquier a cualquier
- Utilice siempre rutas virtuales estáticas entre dos centros de datos (DC a DC)
- No es necesario configurar todas las rutas WAN para utilizar la ruta virtual dinámica
- Cada dispositivo SD-WAN tiene un número limitado de rutas virtuales dinámicas (8 límite dinámico más bajo, 8 límite estático más bajo = 16 total) que se pueden configurar.

Cómo habilitar la ruta virtual dinámica en la GUI de SD-WAN

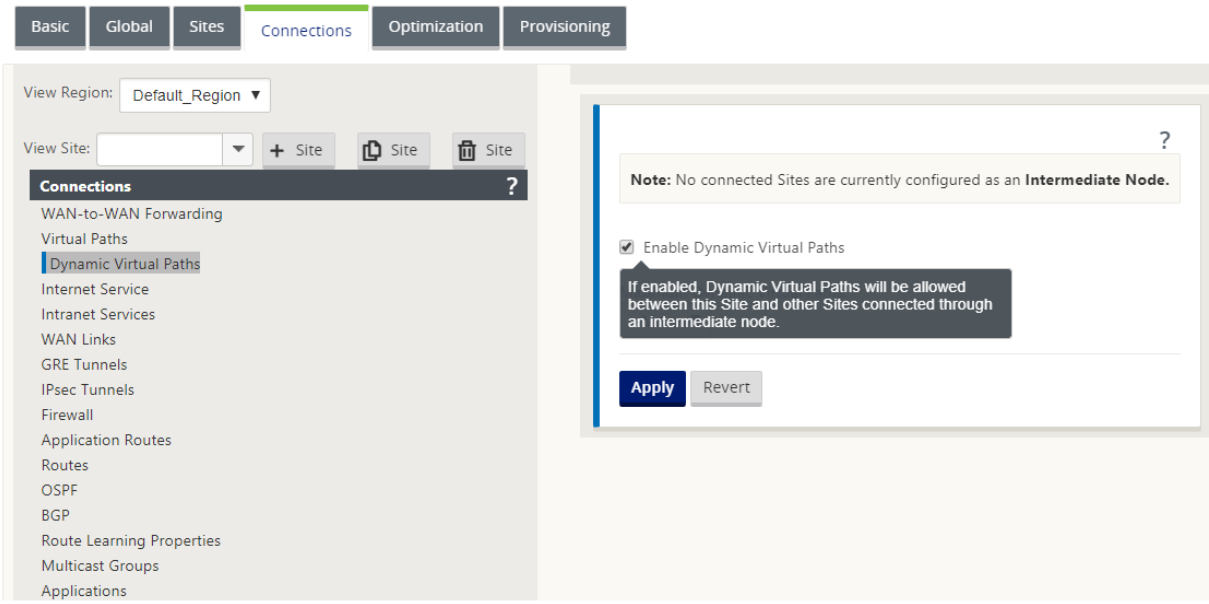
Para habilitar rutas virtuales dinámicas:

1. En la GUI de Citrix SD-WAN, en el panel **Conexiones**, cree un grupo de reenvío de WAN a WAN.
2. Desplácese hasta **Conexiones > [Nombre del sitio del cliente] > Reenvío de WAN a WAN**.
3. Habilite el **reenvío de WAN a WAN** para permitir que el sitio sirva como proxy para sitios múltiples saltos a sitio.
4. Habilitar **el sitio como nodo intermedio**
5. Vaya a **Conexiones > Sitio remoto > Reenvío WAN a WAN**.
6. Habilite el reenvío de WAN a WAN para permitir que el sitio sirva como proxy para el sitio de salto múltiple a sitio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Vaya a **Conexiones > Sitio remoto > Ruta virtual > Ruta virtual dinámica**.
8. Habilite **rutas virtuales dinámicas**.
9. Establezca el número máximo de rutas dinámicas.

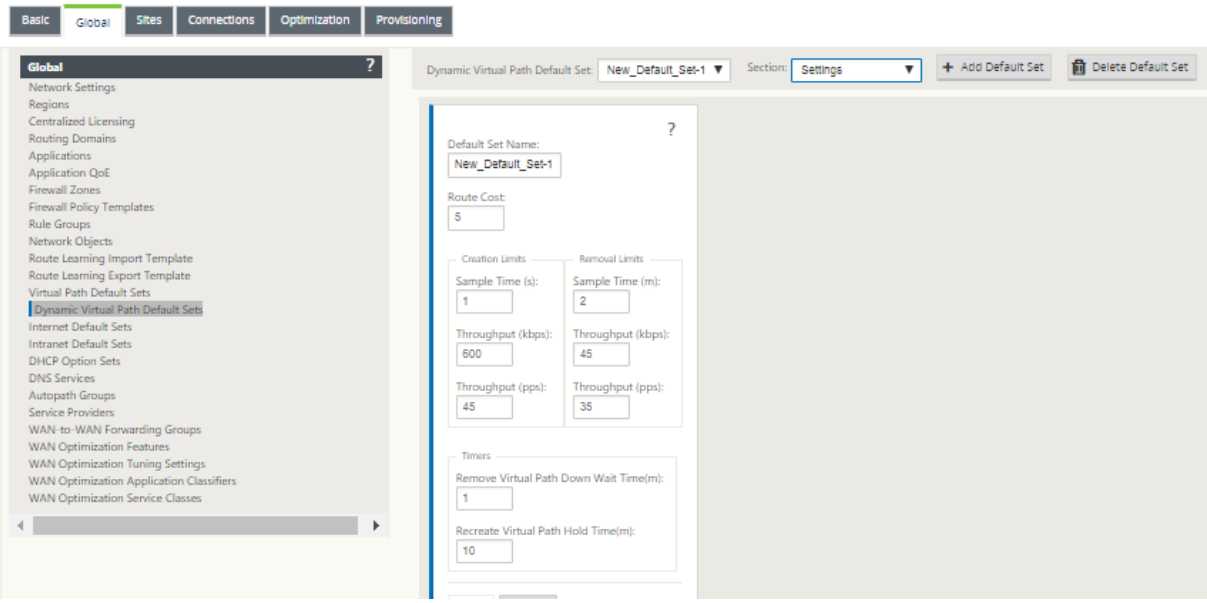


Cómo crear una ruta virtual dinámica

- La configuración determina cuándo una ruta virtual dinámica está activa o inactiva.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Configure el recuento de paquetes de muestra (pps) o el ancho de banda (kbps) dentro de un período de tiempo.
- Se puede establecer globalmente o con WAN Link configurado en el nodo intermedio.



Reenvío Wan-to-WAN

May 7, 2021

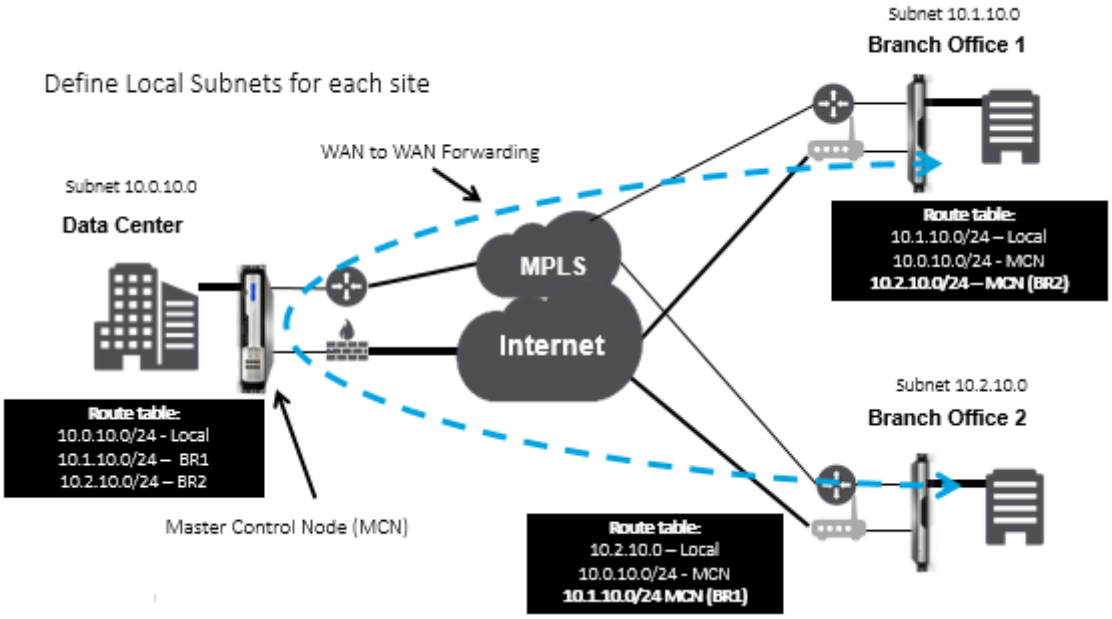
Al habilitar el reenvío Wan-to-WAN en el MCN, el MCN puede anunciar rutas de sitios remotos.

- 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 Wan-to-WAN está habilitado en el MCN. Al habilitar esta opción, los nodos SD-WAN de la rama conocen otras subredes de sucursal. El tráfico destinado a otras sucursales se reenvía a MCN. MCN lo enruta al destino correcto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supervisión y solución de problemas

May 7, 2021

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

Visualización de información estadística

Visualización de información de flujo

Ver informes

Visualización de estadísticas del firewall

Herramienta de diagnóstico

Asignación y ancho de banda mejorados

Resolución de problemas de IP de administración

Pruebas de ancho de banda activo

Detección de ancho de banda adaptable

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Supervisión de WAN Virtual

May 7, 2021

Visualización de la 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 información básica de dicho dispositivo.

La página **Panel** muestra la siguiente información básica para el dispositivo local:

Estado del sistema:

- **Nombre**: Es el nombre que asignó al dispositivo cuando lo agregó al sistema.
- **Modelo**: Es el número de modelo del dispositivo WAN virtual.
- **Modo de dispositivo**: Indica si este dispositivo se ha configurado como MCN principal o secundario, o como dispositivo cliente.
- **Dirección IP de administración**: Es la dirección IP de administración del dispositivo.
- **Tiempo de actividad del equipo**: 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:

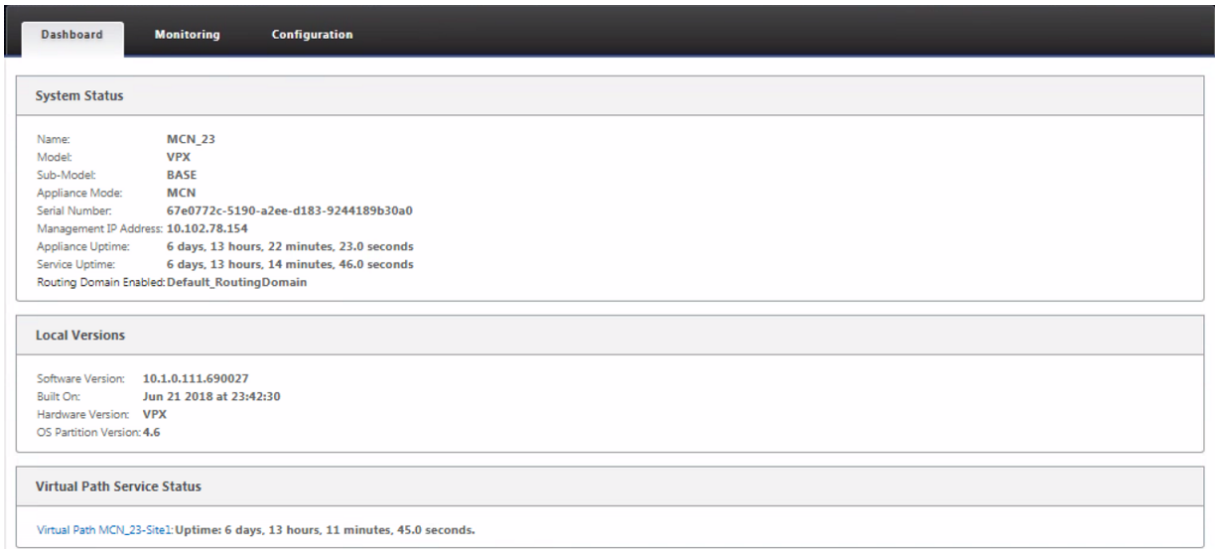
[Nombre del sitio] de ruta virtual: Muestra el estado de todas las rutas virtuales asociadas a este dispositivo. Si el servicio WAN virtual está habilitado, esta sección se incluye en la página. Si el servicio WAN virtual está inhabilitado, se mostrará un icono de alerta (delta de vara dorada) y un mensaje de alerta a tal efecto en lugar de esta sección.

Información de la versión local:

- **Versión de software**: Es la versión del paquete de software CloudBridge Virtual Path activado actualmente en el dispositivo.
- **Crear**: Es la fecha de compilación de la versión del producto que se está ejecutando actualmente en el dispositivo local.
- **Versión de hardware**: Es el número de modelo de hardware y la versión del dispositivo.
- **Versión de la partición del sistema operativo**: Es la versión de la partición del sistema operativo actualmente activa en el dispositivo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La siguiente figura muestra una página de panel de ejemplo.



Visualización de información estadística

May 7, 2021

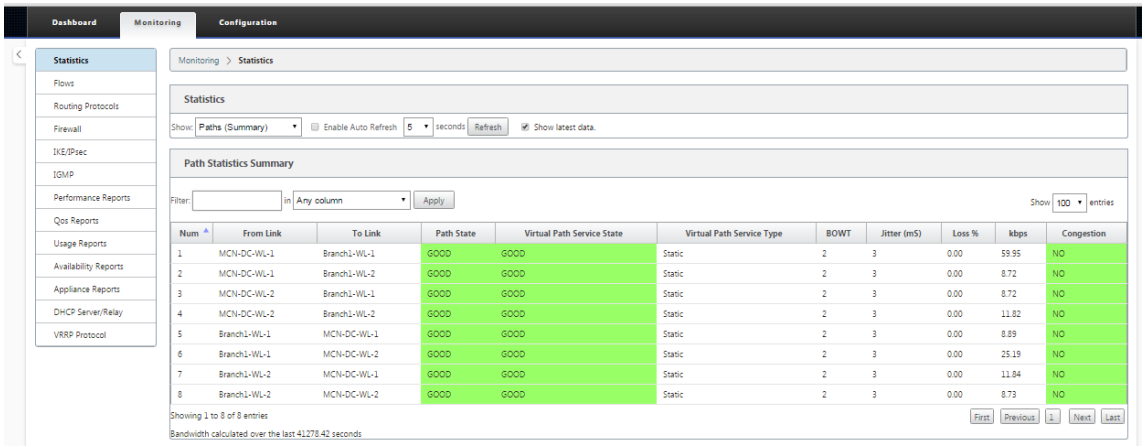
En esta sección se proporcionan instrucciones básicas para ver la información de estadísticas de WAN virtual.

1. Inicie sesión en la Interfaz Web de administración para el MCN.
2. Seleccione la ficha **Supervisión**.

   Esto abre el árbol de navegación **Supervisión** en el panel izquierdo. De forma predeterminada, también muestra la página **Estadísticas** con **Rutas preseleccionadas** en el campo **Mostrar**. Contiene una tabla detallada de estadísticas de ruta.

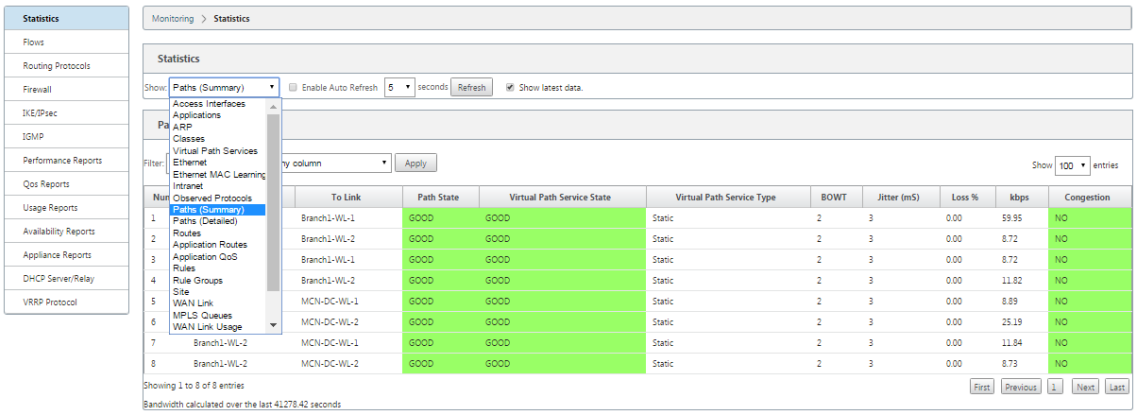
   > **Nota**
   >
   > Si accede a otra página **Supervisión** (por ejemplo, **Flujos**), puede volver a esta página seleccionando **Estadísticas** en el árbol de navegación **Supervisión** (panel izquierdo).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Abra el menú implementable **Mostrar** junto al campo **Mostrar**.

   Además de las estadísticas de **rutas**, el menú **Mostrar** también ofrece varias opciones más para filtrar y ver información estadística.



4. Seleccione un filtro en el menú **Mostrar** para ver una tabla de información estadística para ese tema.

Visualización de información de flujo

January 10, 2022

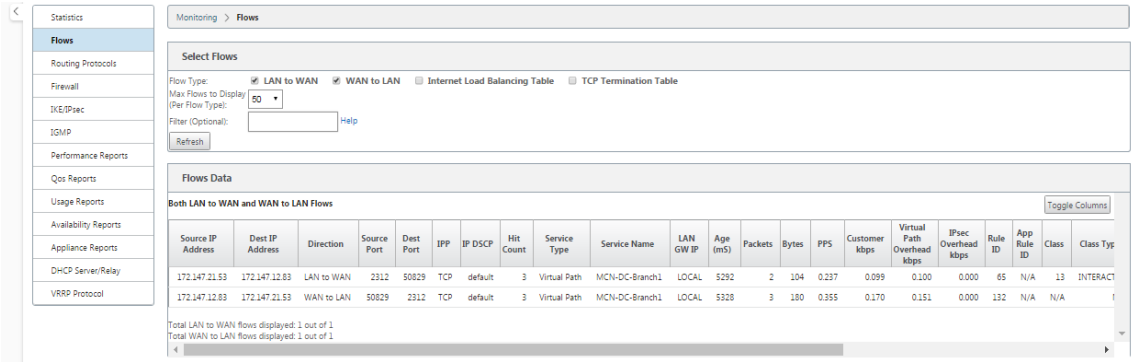
En esta sección se proporcionan instrucciones básicas para ver la información de flujo de WAN virtual.

Para ver la información de 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 desea 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.

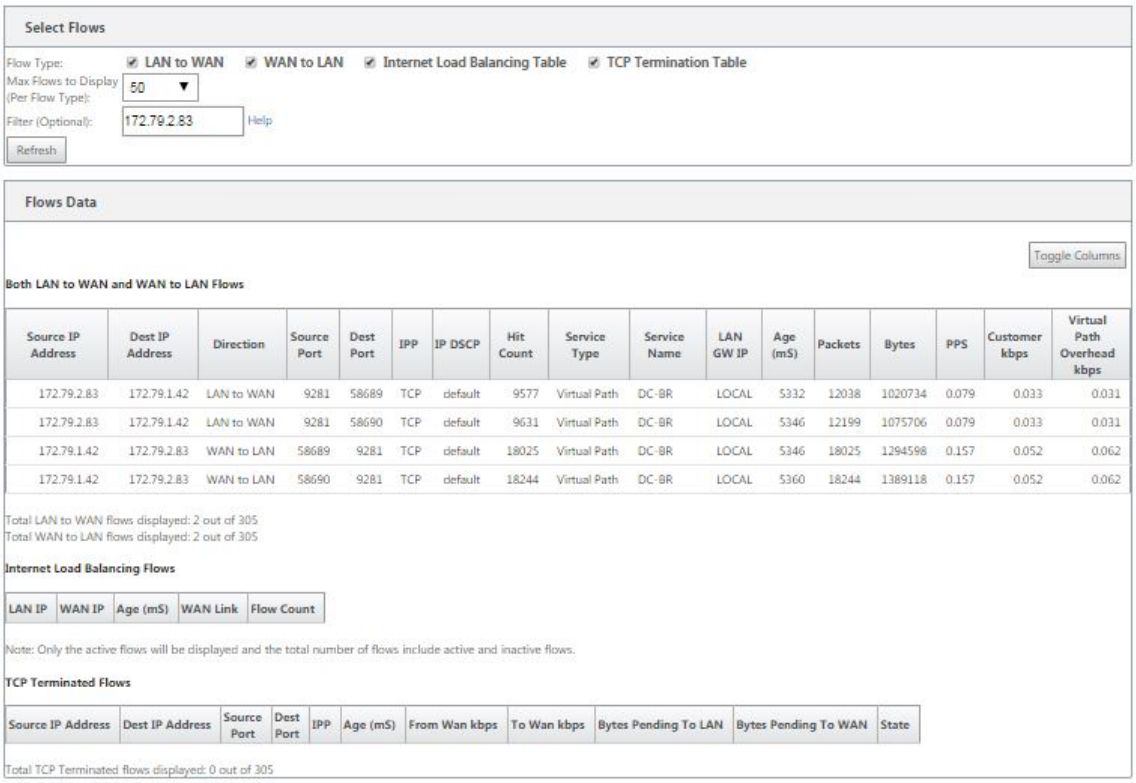
5. Determina el número de entradas que se mostrarán en la tabla **Flujos**. Las opciones son: **50**, **100**, **1000**.

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 **flujo**, 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 figura muestra una muestra filtrada de página **Flujos** con todos los tipos de flujo seleccionados.

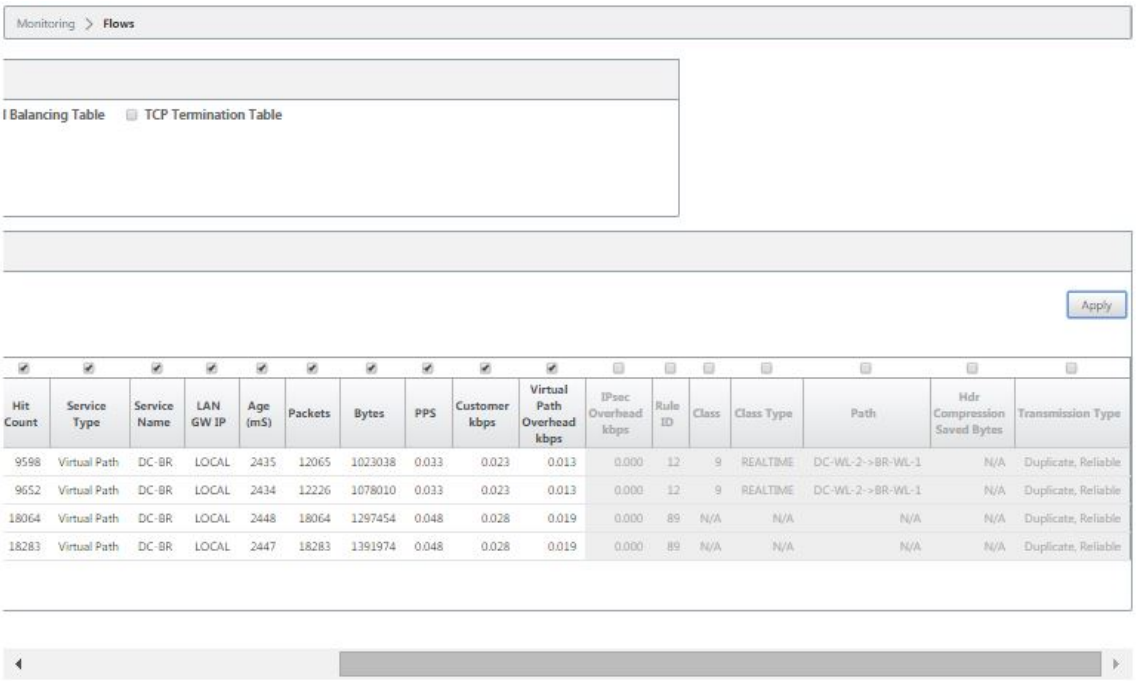
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. (Opcional) Seleccione las columnas que quiere incluir en la tabla. Haga lo siguiente:
9. Haga clic en **Alternar** columnas. El botón **Alternar columnas** está justo encima de la esquina superior derecha de la tabla **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 figura.

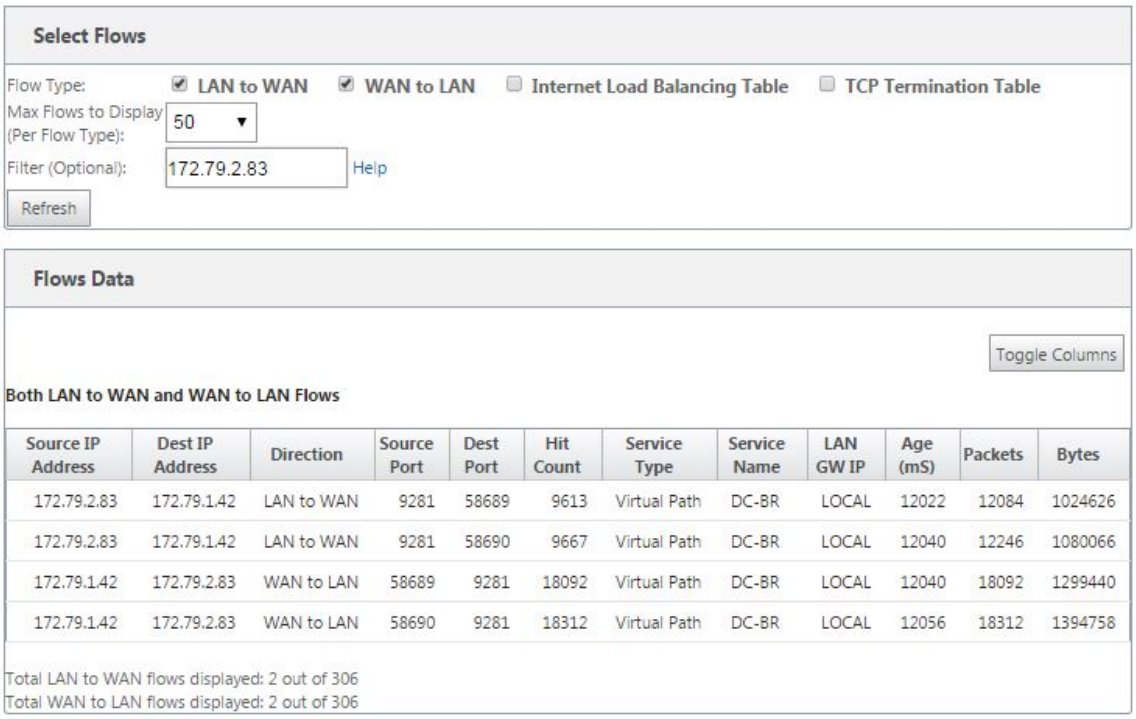
> **Nota**
>
> De forma predeterminada, se seleccionan todas las columnas, lo que puede hacer que la tabla se trunque en la pantalla, oscureciendo el botón **Alternar columnas**. Si es así, se muestra una barra de desplazamiento horizontal debajo de la tabla. Deslice la barra de desplazamiento hacia 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1297454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

10. Haga clic en una casilla de verificación para seleccionar o anular la selección de una columna.
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.



Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aplicaciones DPI en SD-WAN Center

En versiones anteriores, se pueden identificar alrededor de 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.

Asignación de rutas y uso de ancho de banda mejorados

May 7, 2021

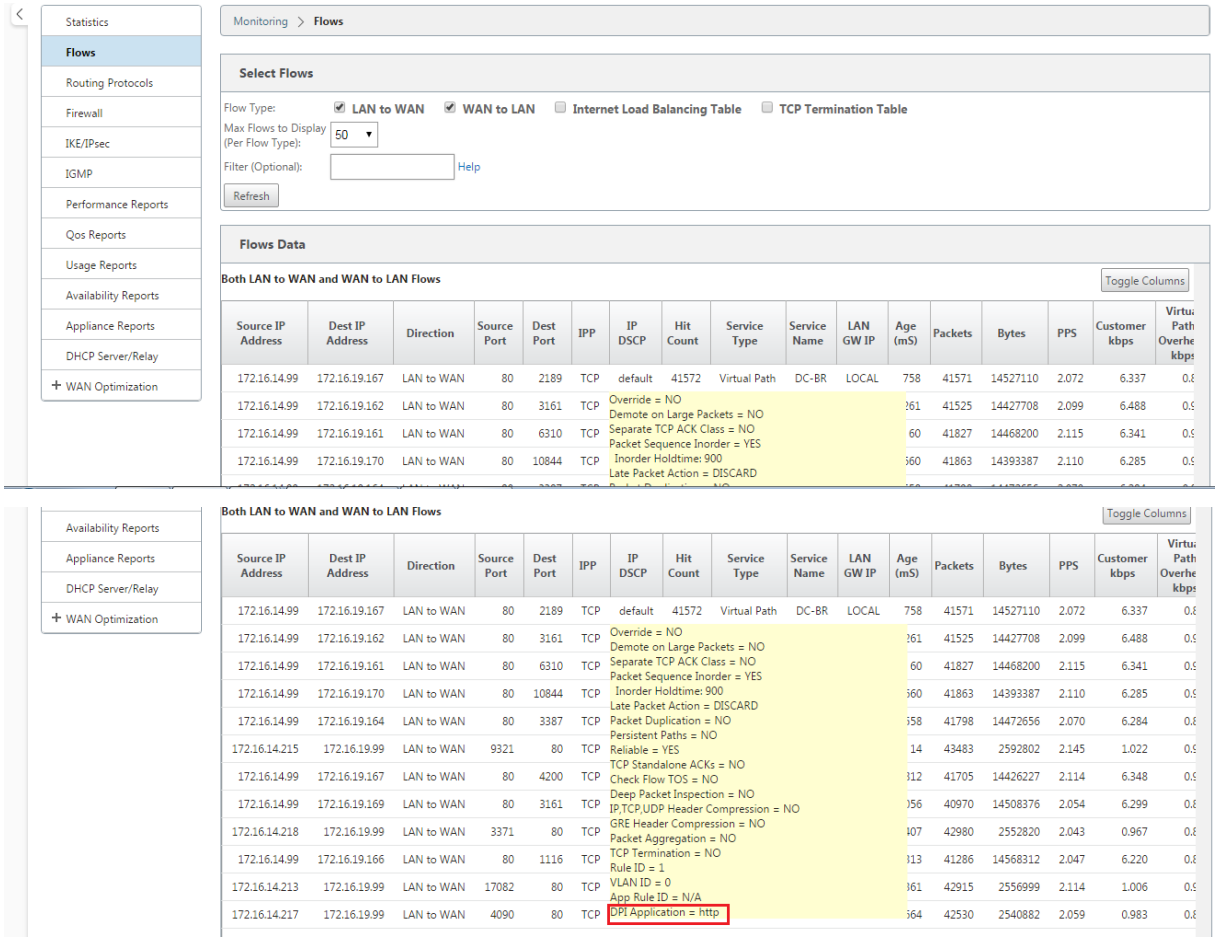
Las mejoras de asignación de rutas y uso de ancho de banda se implementan en la ficha Supervisión para mostrar los flujos de tráfico. Por ejemplo, cuando una ruta virtual está sirviendo una conexión de red, y si esa ruta virtual se vuelve inactiva, se elige una nueva mejor ruta y la ruta inicial se convierte en la última mejor ruta. Este caso se implementa cuando la demanda de ancho de banda es menor y cuando solo se elige un path

Cuando hay más de una ruta virtual que sirve una conexión, observa una mejor ruta actual y la siguiente mejor ruta, si está disponible. Si existe una ruta para procesar el tráfico, suponiendo que hay más de dos rutas procesando el 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 hay una necesidad de más paths con demanda de ancho de banda.

Supervisión de la información de aplicaciones DPI en la GUI SD-WAN

El nombre del objeto de aplicación DPI en el flujo de supervisión se almacena y muestra en la página SD-WAN GUI **Monitoring** -> **Flujos**. Se muestra una información sobre herramientas para identificar la aplicación DPI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supervisión de la información de ruta para el flujo de tráfico en la GUI de SD-WAN

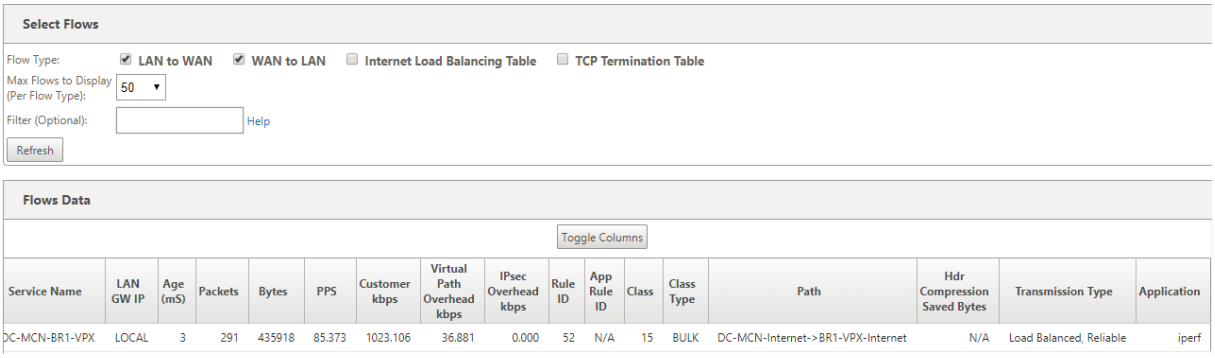
Es posible que, según la tasa de tráfico entrante que exige ancho de banda, se requieran uno o más paths para procesar el tráfico.

Para determinar cómo se realiza la asignación de rutas, revise los siguientes casos:

Modo de transmisión equilibrada de carga:

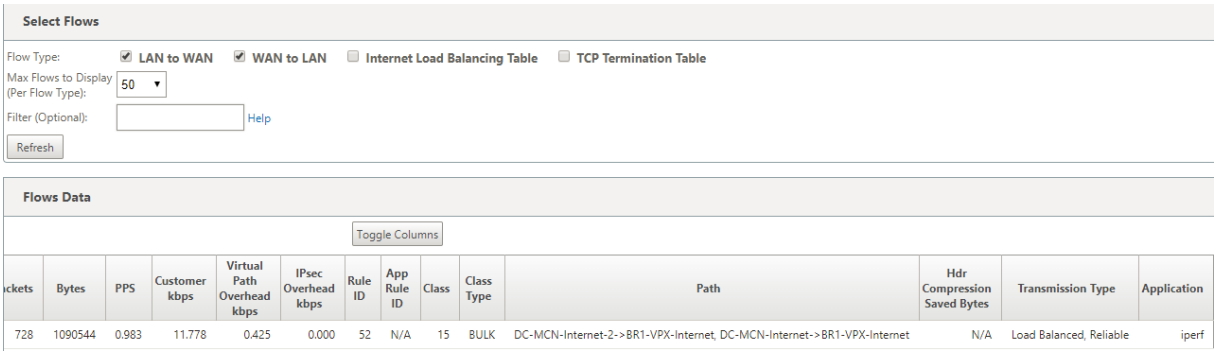
La siguiente figura ilustra el caso en el que se inicia el tráfico y todos los paths son buenos, se elige una mejor ruta, ya que la demanda de ancho de banda es suficiente para ser atendida por un path. Observe que solo se elige una ruta **DC-McN-Internet** -> **BR1** -**VPX-Internet** y el tipo de transmisión se muestra como **Equilibrado de carga.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La siguiente figura ilustra cuándo fluye el tráfico y los atributos WAN de la ruta se degradan, 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 en este ejemplo es un indicador de la ruta que sirvió a la conexión anteriormente.

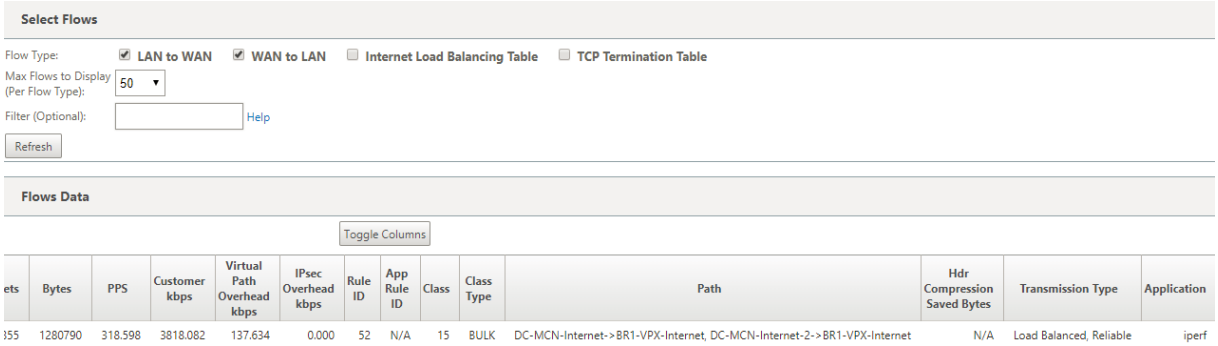


La siguiente figura ilustra que cuando el tráfico está en curso y se elige más de una ruta para el procesamiento del tráfico debido a la demanda de ancho de banda, como se muestra a continuación, se elige más de una ruta cuando se envía el tráfico. A diferencia del caso anterior, aquí puede haber más de dos rutas que también sirven al tráfico, pero en la GUI solo se muestran las dos mejores rutas que actualmente están sirviendo 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 **Flows Data**.

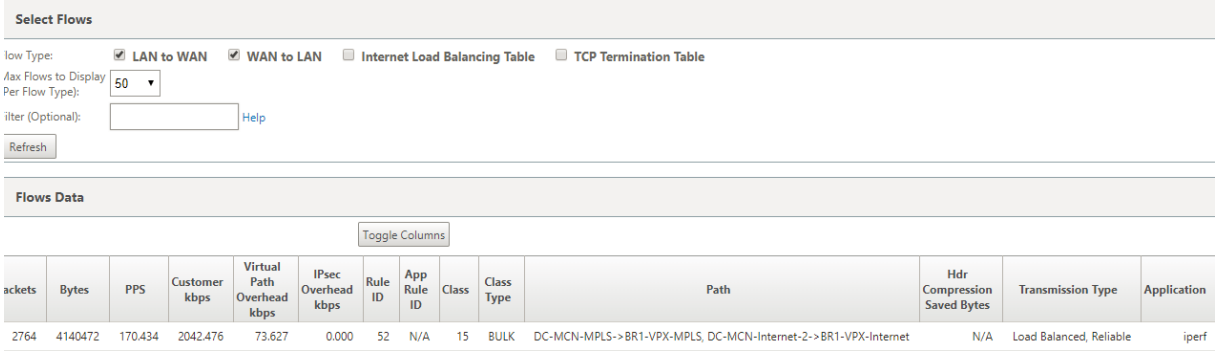
> **Nota**
>
> Como se indica, se muestran un máximo de dos rutas en la tabla de flujos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



La siguiente figura ilustra que cuando el tráfico sigue fluyendo, si la mejor ruta actual que es **DC-McN-Internet->br1-VPX-Internet** no está disponible/inactivo/degradado en atributos WAN, la mejor ruta actual elegida aparecerá primero en la sección ruta de acceso de la tabla **Flows Data** seguido de la última mejor ruta que sirve el tráfico.

Dado que el **DC-McN-Internet->BR1-VPX-Internet** ya no era 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** como ambos son necesarios para la demanda actual de tráfico de ancho de banda.



Modo de transmisión duplicado

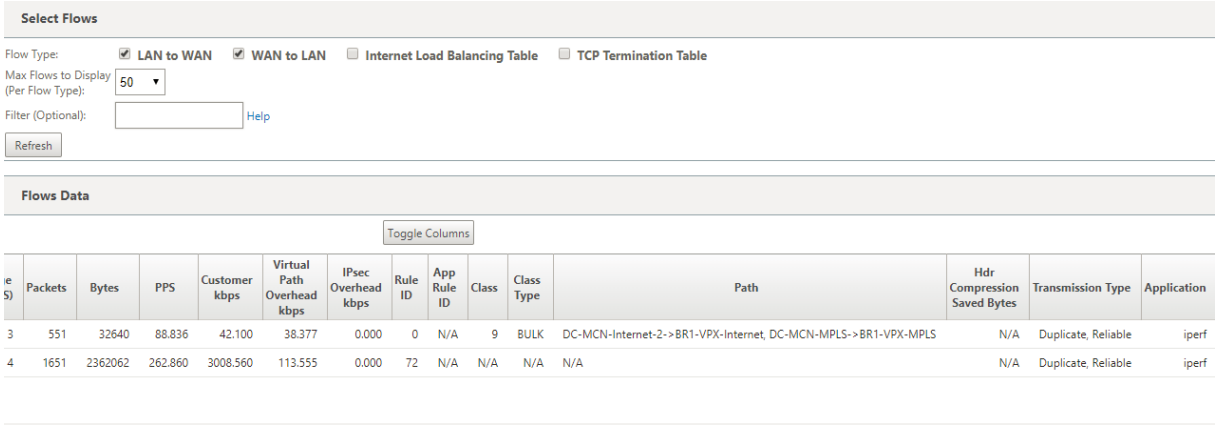
El modo general de duplicación de paquetes garantiza que se tomen inicialmente dos paths para procesar paquetes de la misma conexión a fin de garantizar una entrega confiable duplicando paquetes en dos paths independientes.

En Asignación de rutas, observe que se toman dos rutas en la sección de rutas de la tabla de flujo siempre que existan dos rutas para procesar flujos duplicando.

La siguiente imagen ilustra que, cuando hay tráfico, aparecen dos rutas que procesan el tráfico. A diferencia de cualquier otro modo, incluso si el tráfico requiere menos ancho de banda que puede ser proporcionado por un solo path, este modo siempre duplicará el tráfico a través de dos paths para una entrega fiable de aplicaciones.

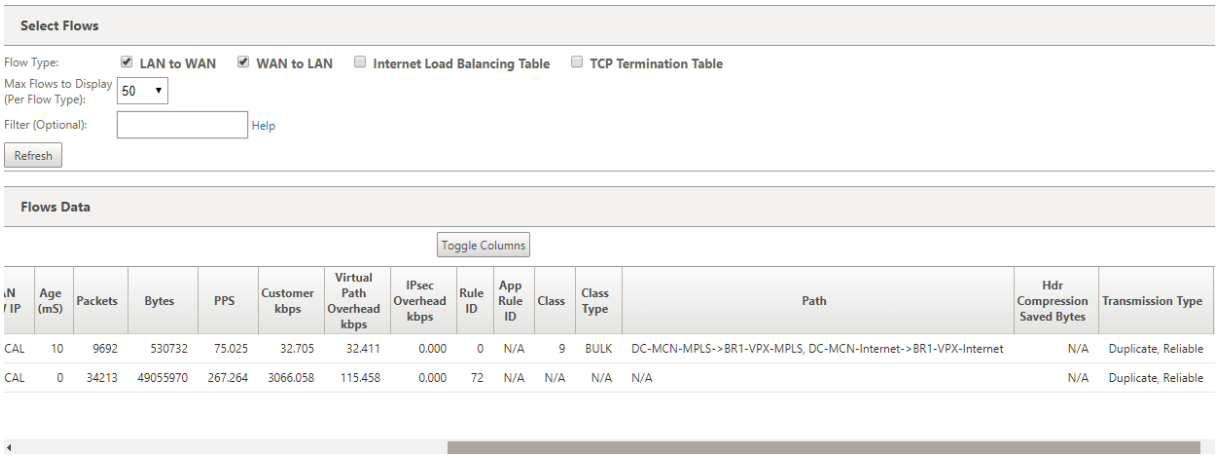
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Observe en la figura siguiente, dos rutas en la sección de ruta de la tabla **Flows Data** ; **DC-McN-Internet2->BR-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS**.



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
551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

La siguiente figura ilustra que cuando el tráfico fluye, si uno de los mejores paths actuales se vuelve inactivo, se elige otro path y todavía hay dos paths como parte de la sección path en la tabla **Flows Data**.

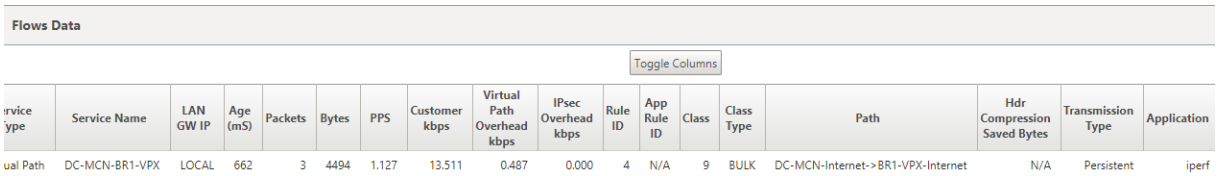


Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

Modo de transmisión de ruta persistente

El modo de transmisión de ruta persistente ayuda a retener paquetes de un flujo basado en la impedancia de latencia de ruta.

La siguiente figura ilustra una ruta que es la mejor ruta que maneja actualmente los flujos y sus paquetes. No hay demanda de ancho de banda y un path lo sirve todo. Actualmente solo hay una mejor ruta que es **DC-McN-Internet->BR1-VPX-Internet.**



Service Name	LAN GW IP	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
DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

La siguiente figura ilustra que si la ruta de acceso **DC-McN-Internet->br1-VPX-Internet** se convierte en propenso a la latencia o está inhabilitada, observará que la ruta de acceso nueva tiene efecto y la ruta de acceso actual **DC-McN-Internet->br1-VPX-Internet** se convierte en la última ruta mejor.

Así que la nueva sección de ruta muestra **DC-MCN-MPLS->BR1-VPX-MPLS, DC-McN-Internet->BR1-VPX-Internet**.

Flows Data

Toggle Columns

N / IP	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
CAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

En modo persistente, puede haber más de una ruta elegida para procesar el tráfico. En ese caso, la GUI muestra las rutas con mejor y siguiente mejor en la sección de ruta de la tabla de flujo desde el comienzo del flujo de tráfico.

La siguiente figura ilustra que el flujo inicialmente solo necesita más de dos rutas y permanecen persistentes mientras no haya cruce de impedancia de latencia de 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

Suponga que una de las mejores rutas de **DC-McN-Internet** entra en alta latencia o está inhabilitada. Esto hace que aparezca una nueva ruta y la nueva ruta puede ser la mejor ruta o podría ser la segunda mejor ruta basada en la decisión de la selección de ruta en ese instante.

Flows Data

Toggle Columns

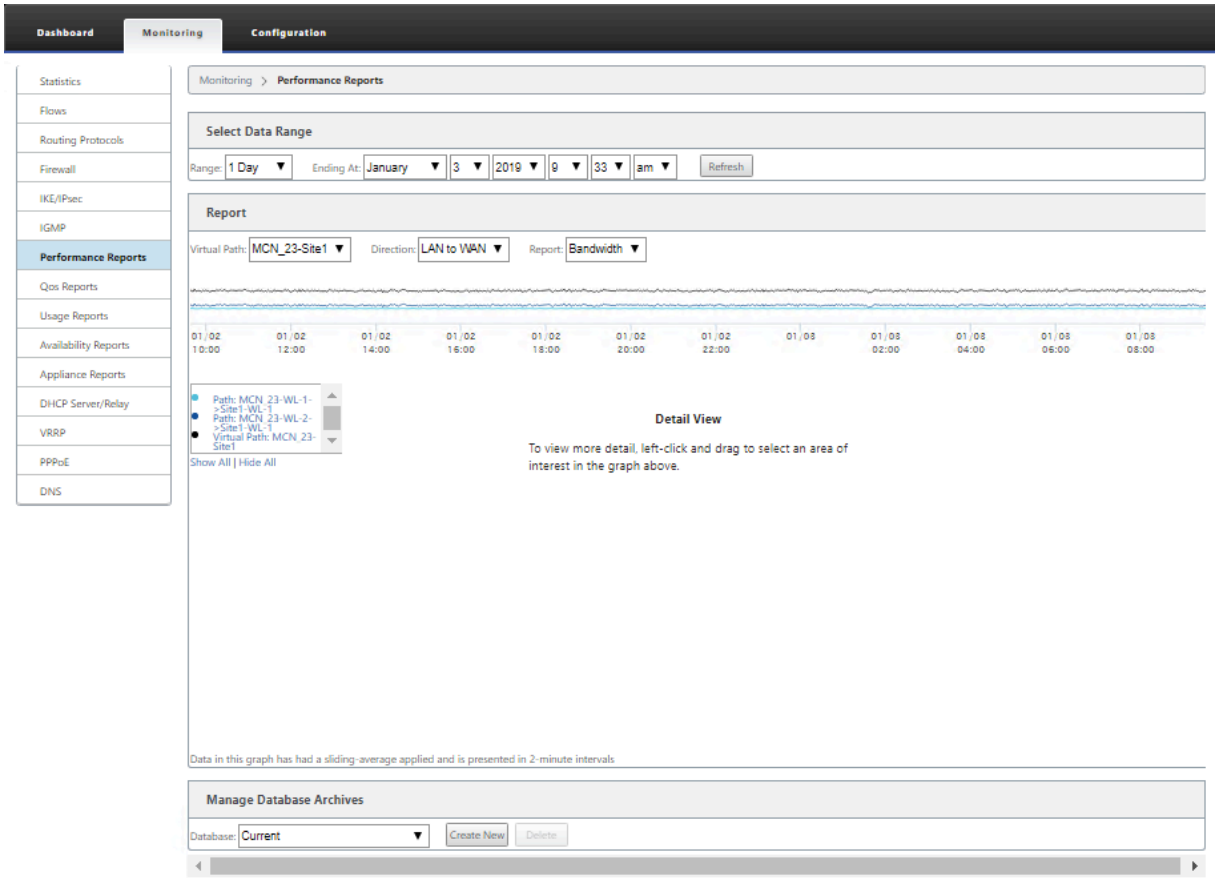
Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	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

Ver informes

May 7, 2021

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Nota**
>
> Los informes generados en la Interfaz Web de administración se aplican al dispositivo local. Para generar y ver informes para la WAN virtual, utilice Virtual WAN Center Web Interface.

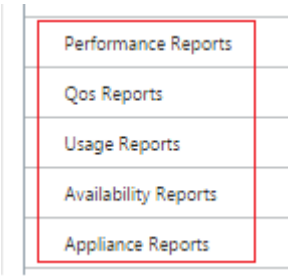
Para generar y ver informes de WAN virtual, haga lo siguiente:

1. Inicie sesión en la Interfaz Web de administración del MCN y seleccione la ficha **Supervisión**.

   Esto abre el árbol de navegación **Supervisión** en el panel izquierdo.

2. Seleccione un tipo de informe en el árbol de navegación.

   Los tipos de informe aparecen como sucursales en el árbol de navegación, justo debajo de la sucursal **Flujos**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los tipos de informe disponibles son los siguientes:

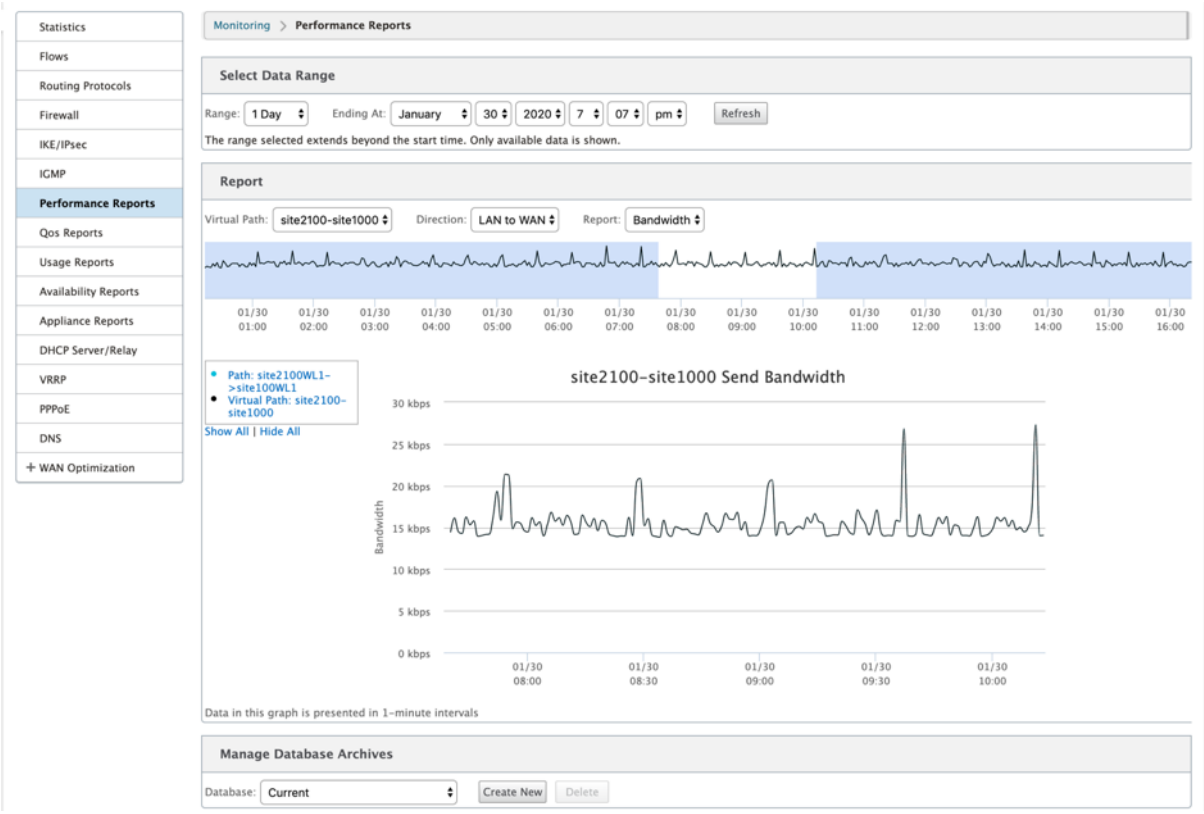
- **Informes de rendimiento**
- **Informes de QoS**
- **Informes de uso**
- **Informes de disponibilidad**
- **Informes de dispositivos**

3. Seleccione las opciones del 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 ejecución

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 izquierdo del ratón y seleccione un área específica de trazado o marco de tiempo en la línea del gráfico.



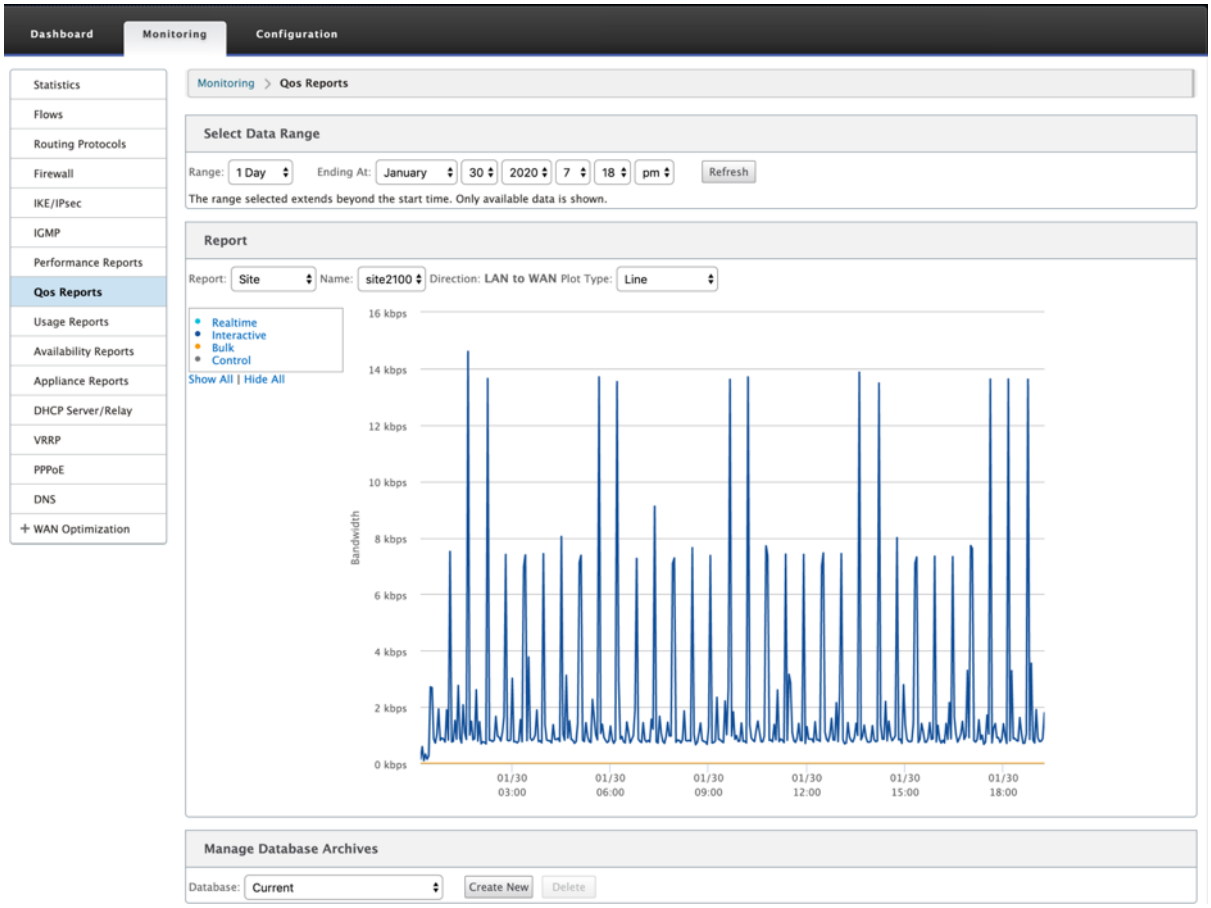
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



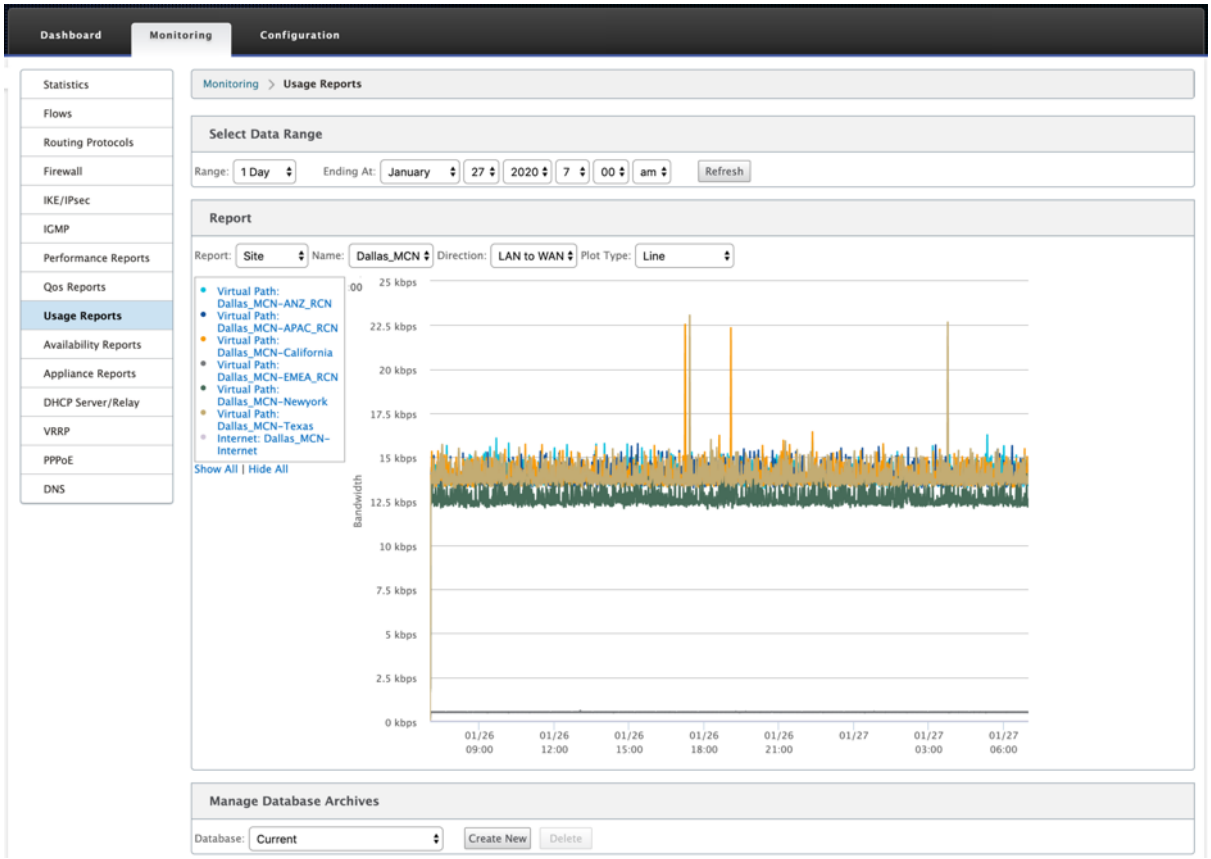
Puede ver las siguientes métricas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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 enrutamiento, programación y estadísticas de vínculos.

Informes de uso

Los informes de uso proporcionan la información de uso de rutas virtuales.



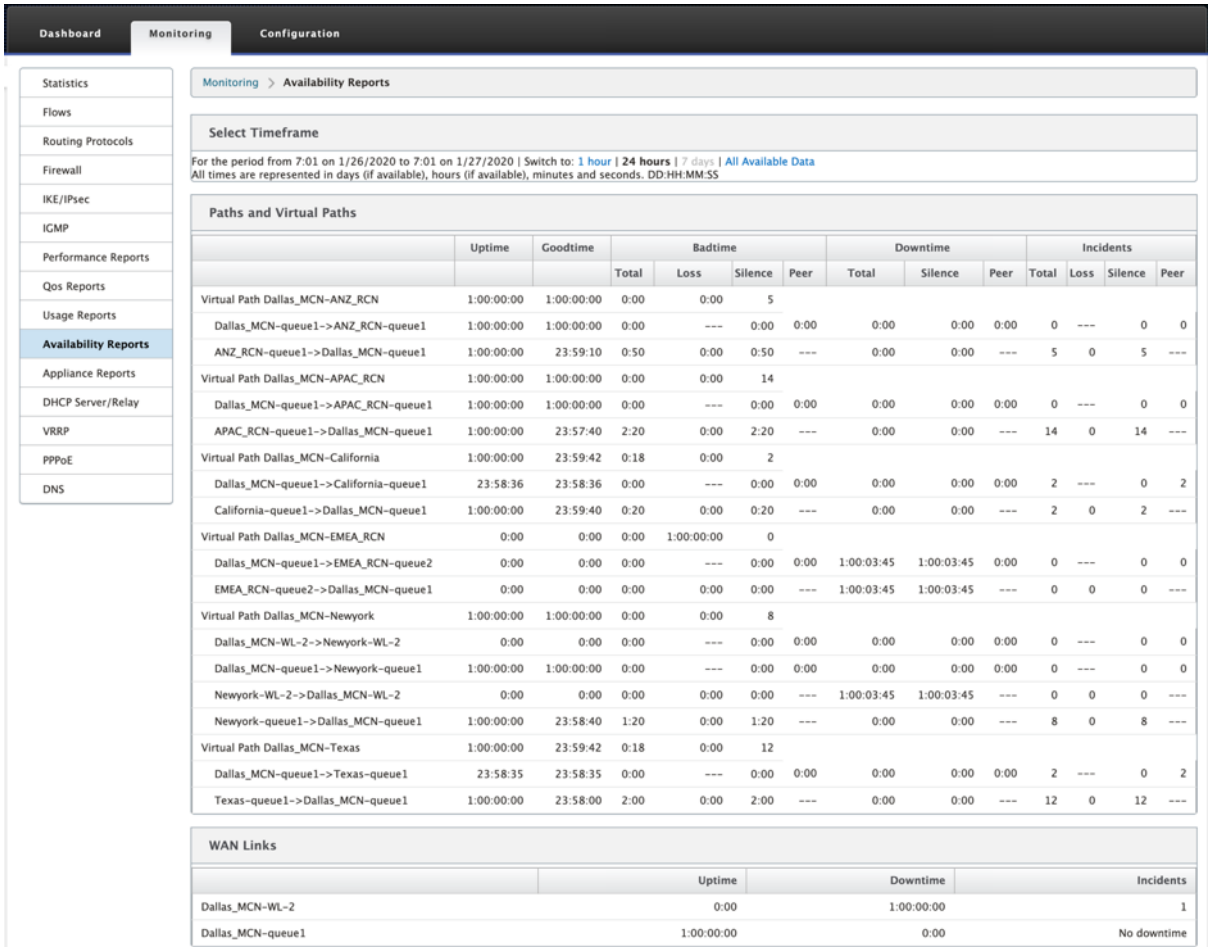
- **Informe:** Seleccione **Sitio** o **Enlace WAN** en la lista desplegable para ver el informe.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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

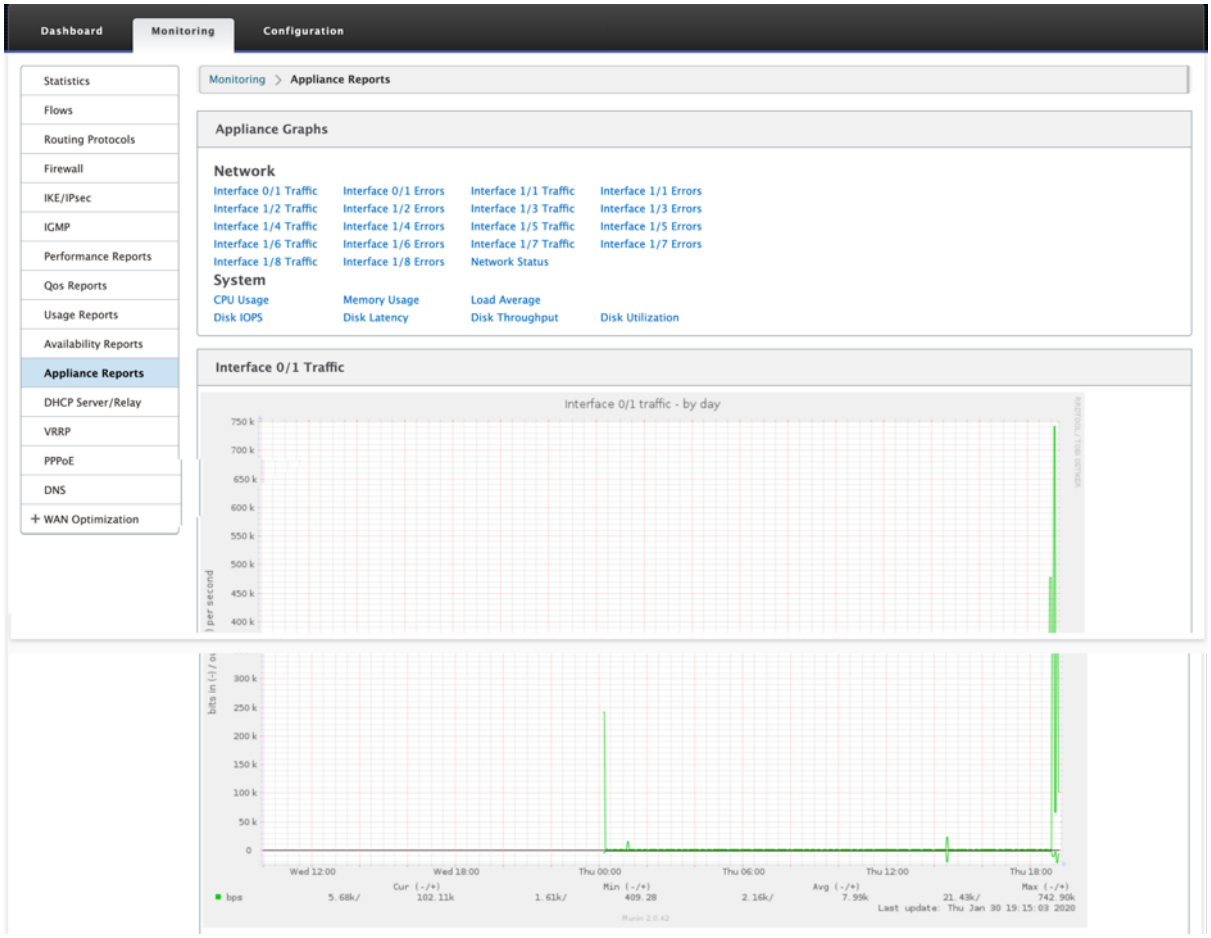
En este informe, puede ver los datos de disponibilidad de Vínculos WAN, Rutas de acceso y Rutas virtuales. También puede cambiar o elegir un período de tiempo específico, como 1 hora, 24 horas y 7 días para ver los datos disponibles. Los datos Rutas y Rutas virtuales se representan en formato **DD:HH:MM:SS**.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Visualización de estadísticas del firewall

May 7, 2021

Una vez que haya configurado las directivas de firewall y NAT, puede ver las estadísticas de las conexiones, las directivas de firewall y las directivas de NAT como informes. Puede filtrar los informes mediante los distintos parámetros de filtrado.

Para obtener información sobre la configuración de las directivas de firewall y NAT, consulte Soporte de firewall con estado y NAT.

Conexiones

Puede comprobar las estadísticas de Aplicaciones para la directiva de firewall. Esto le permite ver todas las conexiones que coinciden con la aplicación seleccionada, de dónde vienen, a dónde van y

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

cuánto tráfico están generando. 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 criterios de filtro para la conexión.
- Familia: Familia de aplicaciones utilizada como criterios de filtro para la conexión.
- Protocolo IP: Protocolo IP utilizado por la conexión.
- Zona de origen: La 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 los que se originó la conexión. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.
- Tipo de servicio de destino: El servicio desde el que se origina el tráfico de respuesta.
- Instancia de 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 utilizados por el dispositivo de respuesta. 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. Grupo de filtros de firewall se crean mediante plantillas de directiva de firewall y se pueden aplicar a todos los sitios de la red o 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 de firewall.
- Aplicación: Aplicación utilizada como criterio de filtro en la directiva de firewall
- Familia: Familia de aplicaciones utilizada como criterios de filtro en la directiva de firewall.
- Protocolo IP: Protocolo IP que coincide con la directiva de filtro.
- DSCP: La etiqueta DSCP que coincide con la directiva de filtro.
- Acción de directiva de filtro: La 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 los que se originó la conexión. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.
- Tipo de servicio de destino: El servicio al que está destinado el tráfico de respuesta.
- Nombre del servicio de destino: Cuando corresponda, el servicio al que está destinado 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 utilizados por el dispositivo de respuesta. 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

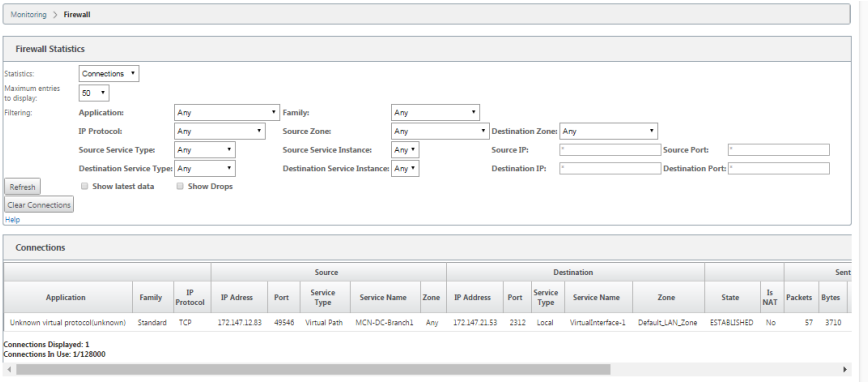
Puede ver las estadísticas de todas las directivas de traducción de direcciones de red (NAT) y filtrar el informe mediante los siguientes parámetros.

- Protocolo IP: Protocolo IP que coincide con la directiva NAT.
- Tipo de NAT: El tipo de NAT que utiliza la directiva de NAT.
- Tipo de NAT dinámico: El tipo de NAT dinámico que utiliza la directiva NAT.
- Tipo de servicio: El tipo de servicio utilizado por la directiva NAT.
- Nombre del servicio: Instancia del servicio utilizado por la directiva NAT.
- Inside IP - La dirección IP interna, entrada en notación decimal punteada con una máscara de subred opcional.
- Puerto interior: Rango de puertos interiores 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, entrada en notación decimal punteada 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 -.

Para ver las estadísticas del firewall:

1. Vaya a **Supervisión** > **Firewall.**
2. En el campo Estadísticas, seleccione **Conexiones**, Directivas de **filtro o Directivas NAT**según sea necesario.
3. Establezca los criterios de filtrado según sea necesario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Haga clic en **Actualizar**.

Diagnóstico

September 26, 2023

Las utilidades de **diagnóstico de Citrix SD-WAN** ofrecen las siguientes opciones para probar e investigar problemas de conectividad:

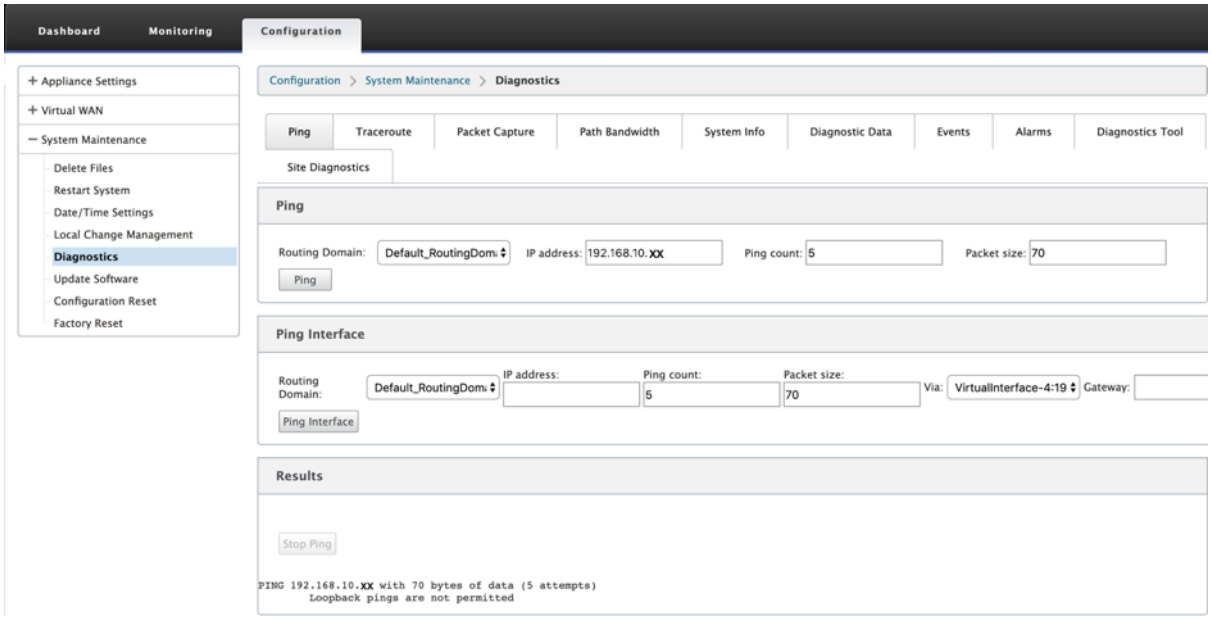
- Ping
- Traceroute
- Captura de paquetes
- Ancho de banda path
- Información del sistema
- Datos de diagnóstico
- Eventos
- Alarmas
- Herramienta de diagnóstico
- Diagnóstico del sitio

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

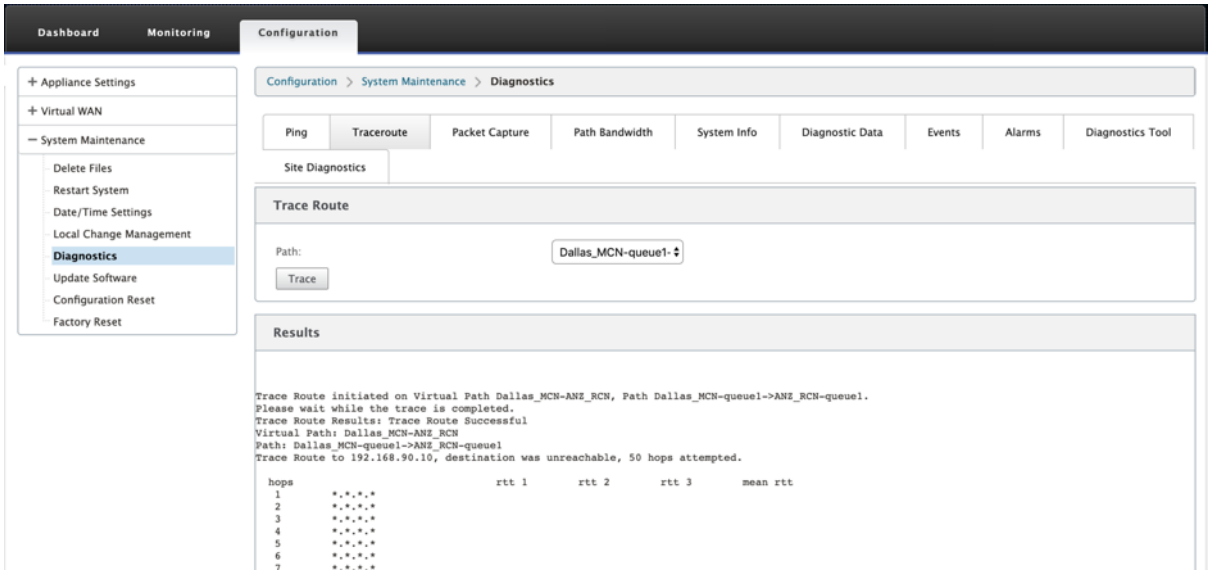


Seleccione el dominio de redirección. Proporcione una dirección IP válida, el número de recuentos de ping (número de veces que se envía la solicitud de ping) y el tamaño del paquete (número de bytes de datos). Haga clic en **Detener ping** para detener una búsqueda de ping en curso.

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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

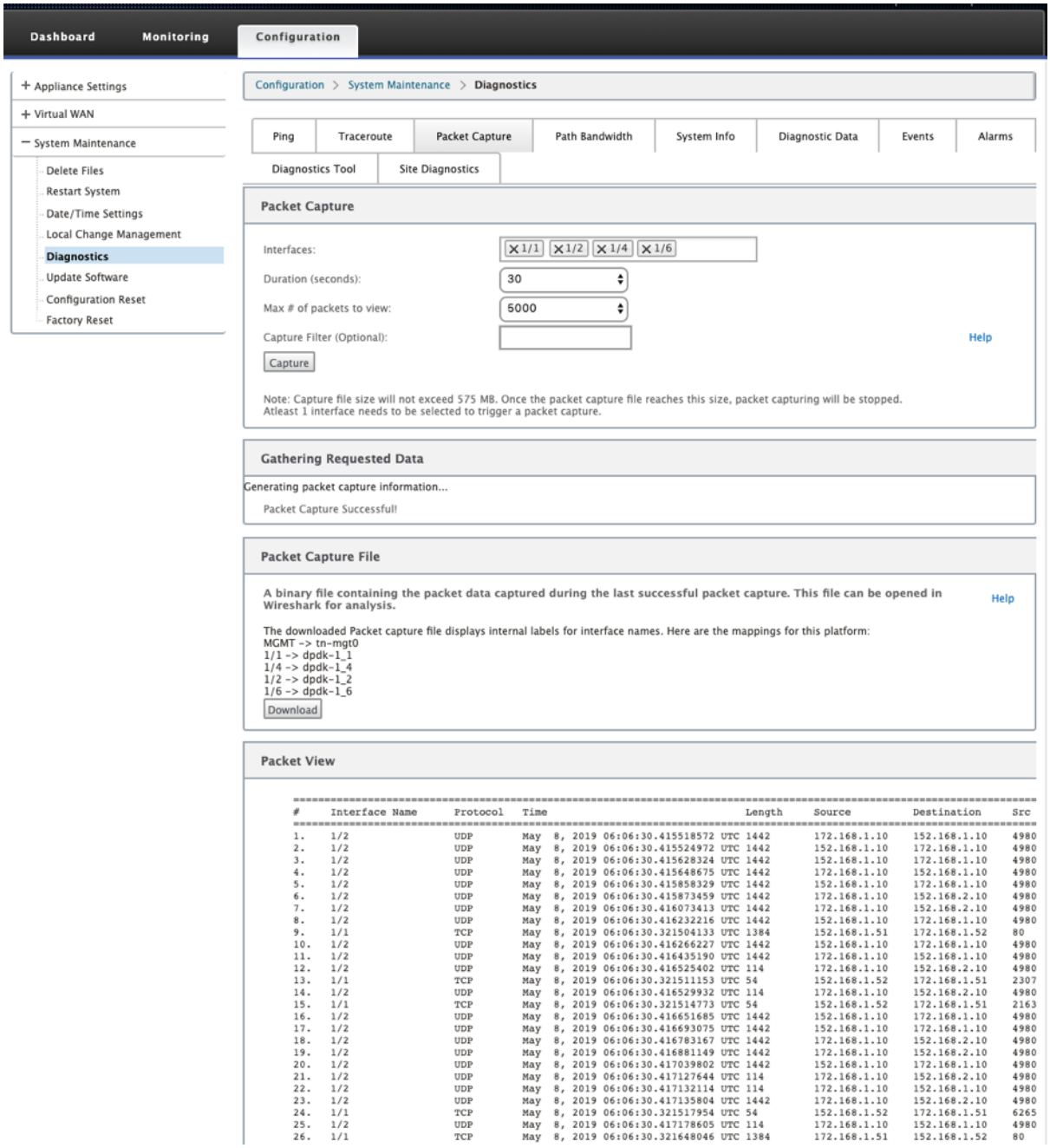
Traceroute ayuda a descubrir y mostrar la ruta o ruta a un servidor remoto. Utilice la opción **Traceroute** como herramienta de depuración para detectar los puntos de fallo de una red.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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. Se debe seleccionar 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

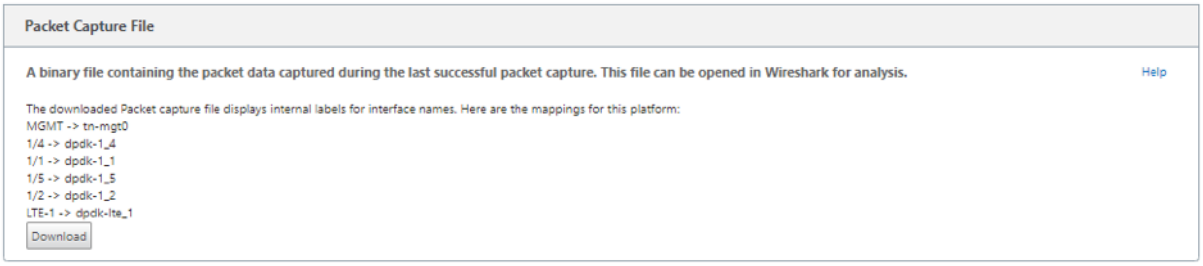
Recopilación de datos solicitados

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.

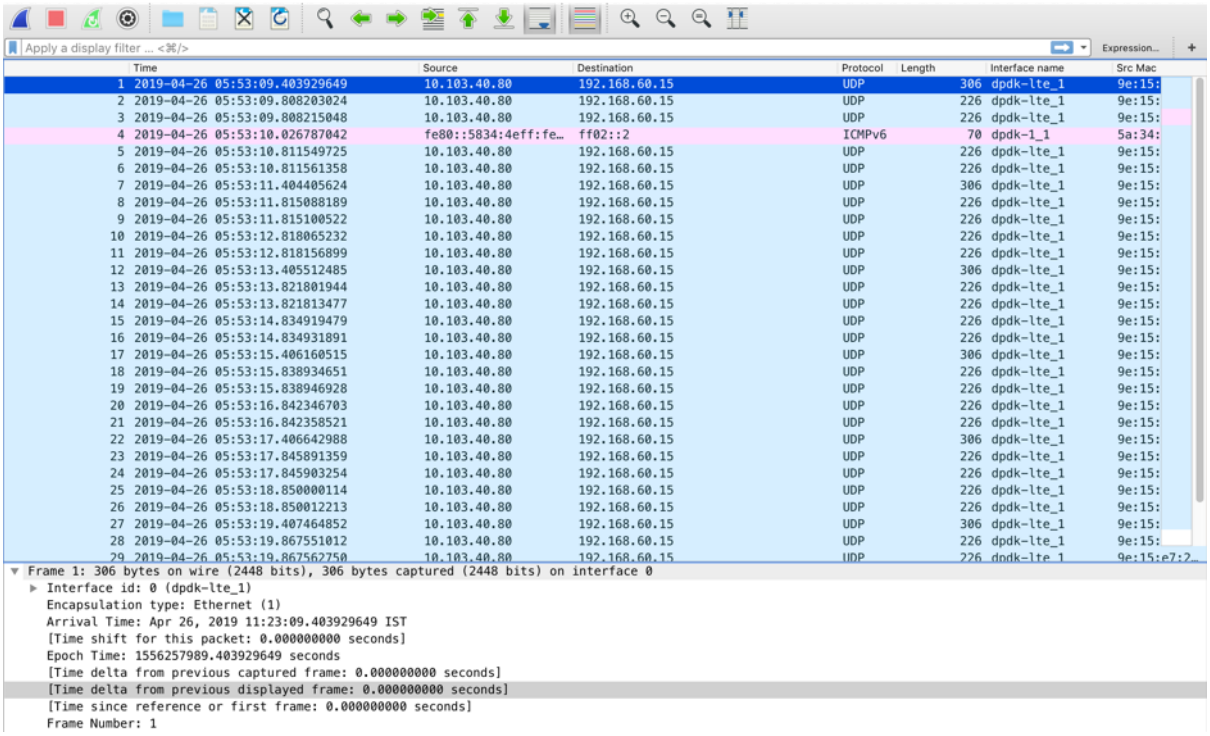
Archivo de captura de paquetes

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Necesita la versión 2.4.13 del software **Wireshark** o superior para abrir y leer el archivo binario.



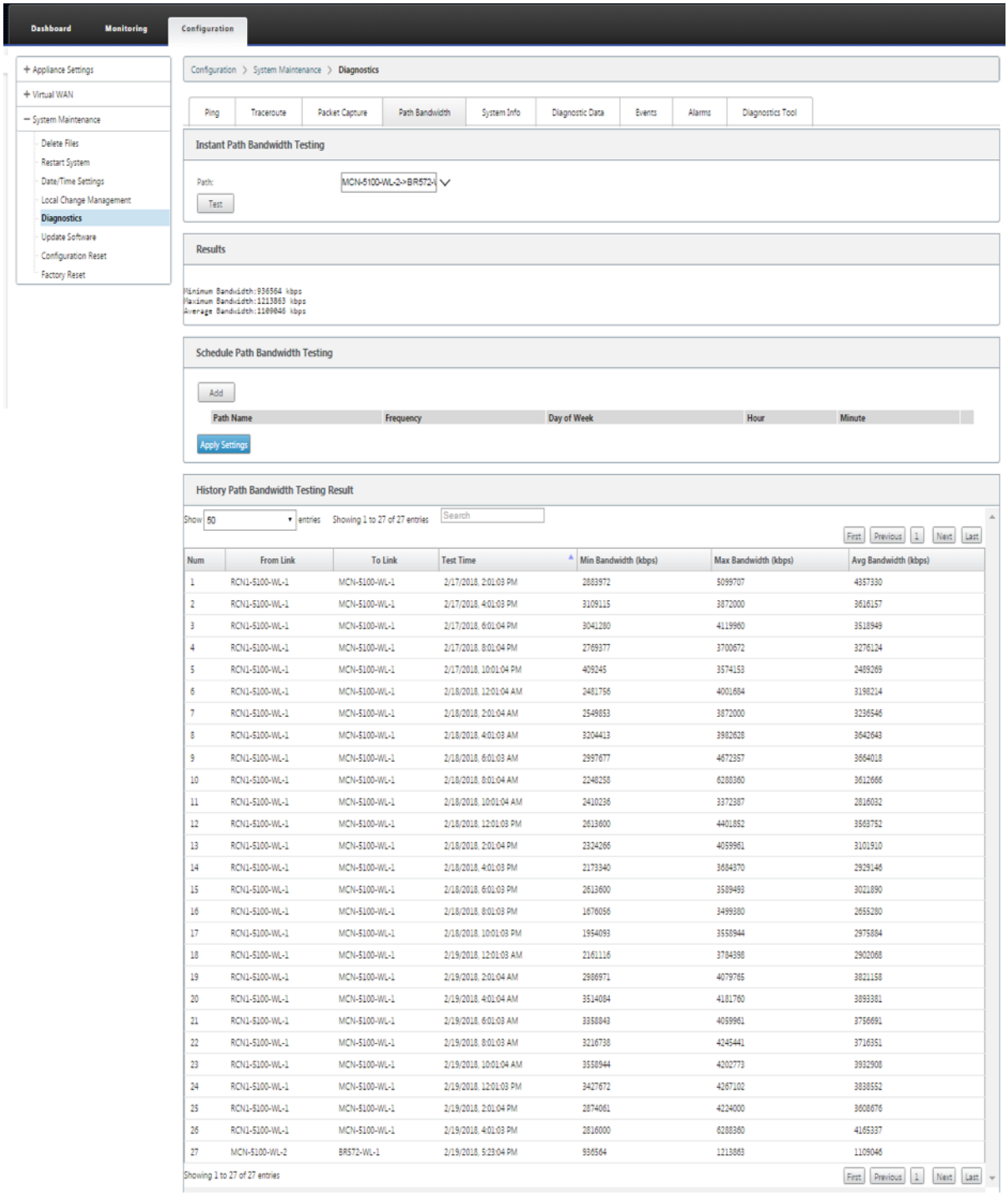
Vista de paquetes

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

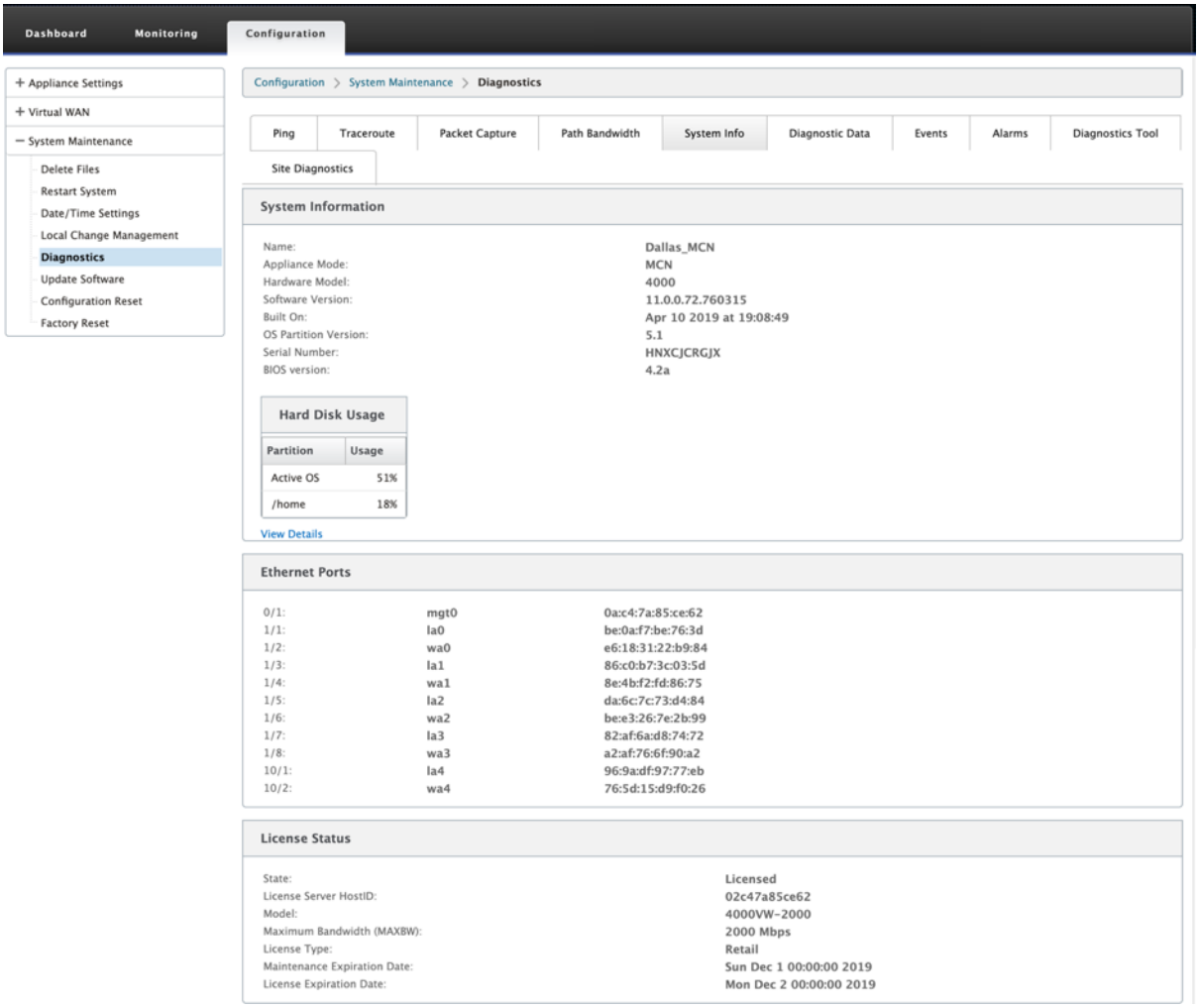
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

entre dos ubicaciones durante instalaciones nuevas y existentes. También 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 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.

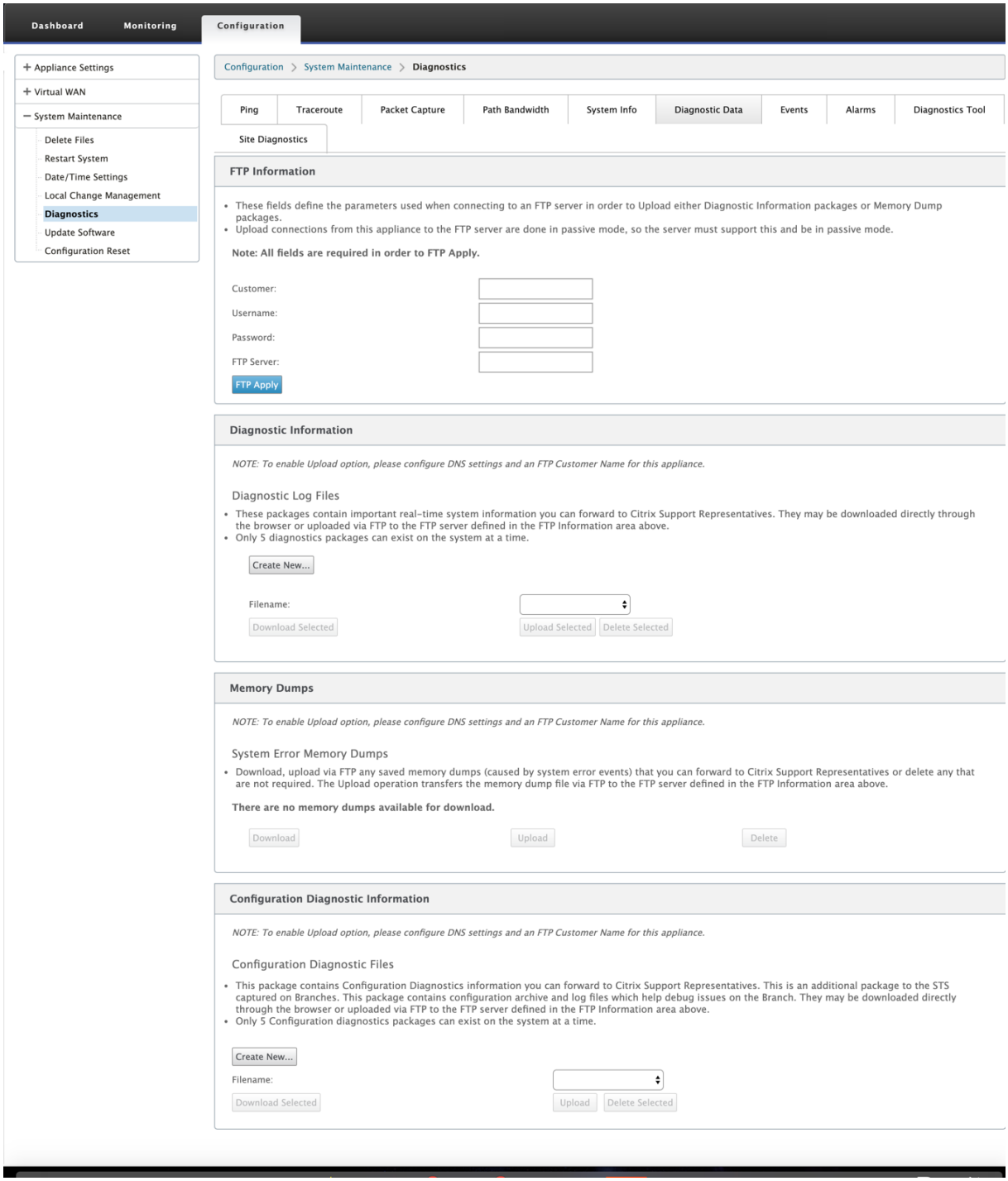
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datos diagnósticos

Los **datos de diagnóstico** le permiten generar el 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-

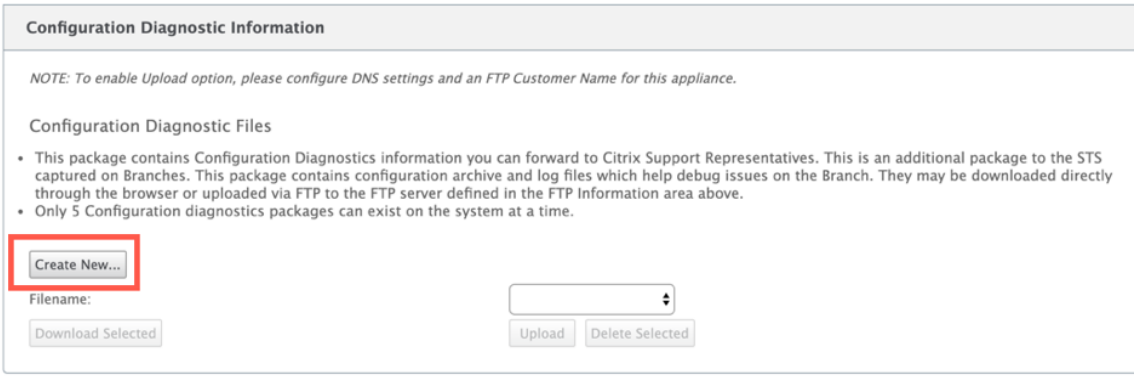
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

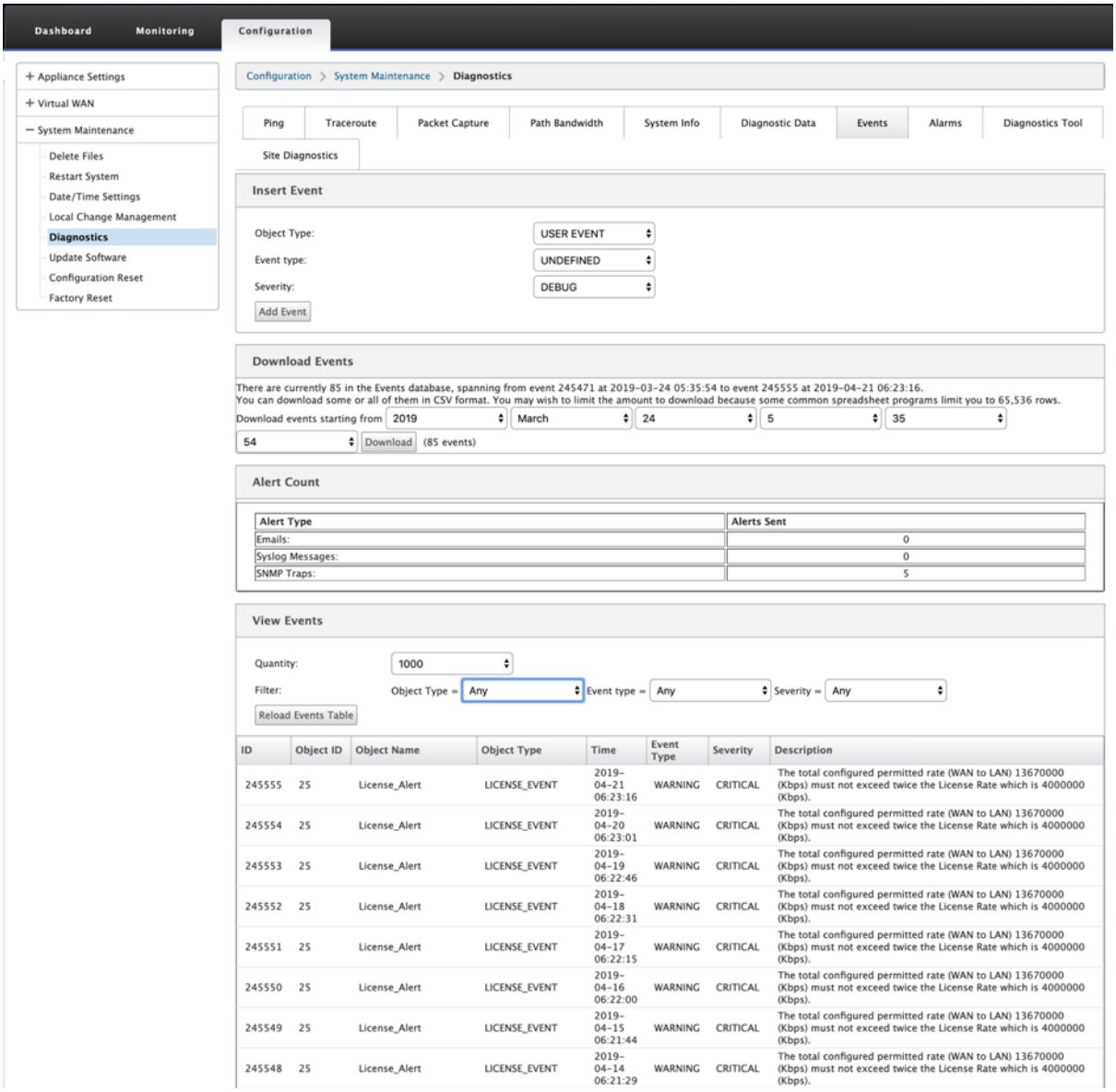
Utilice la función **Eventos** para agregar, supervisar y administrar los eventos generados. Ayuda a identificar eventos en tiempo real, lo que le ayuda a solucionar los problemas de inmediato y a mantener

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

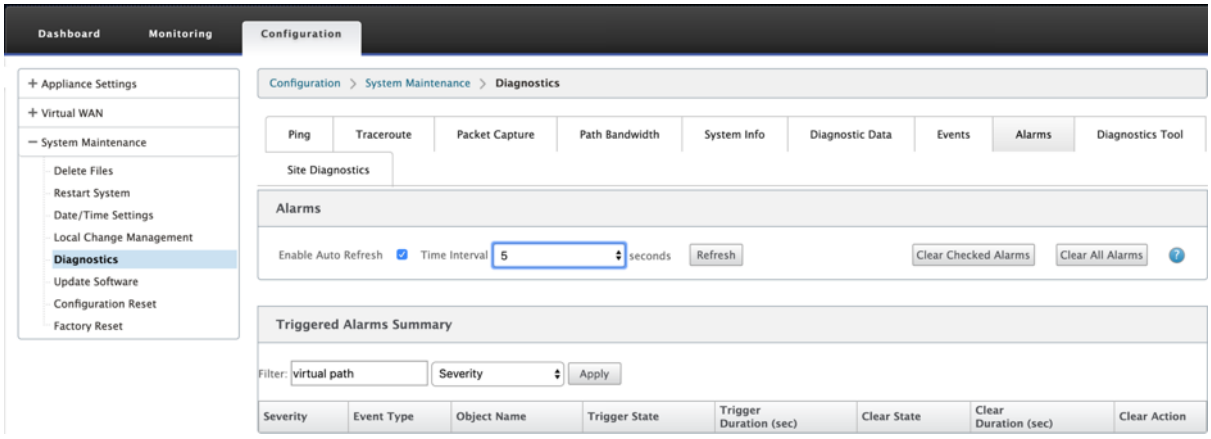
Las notificaciones se generan para eventos iguales o superiores al nivel de gravedad especificado para el tipo de evento.

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 desee 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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:

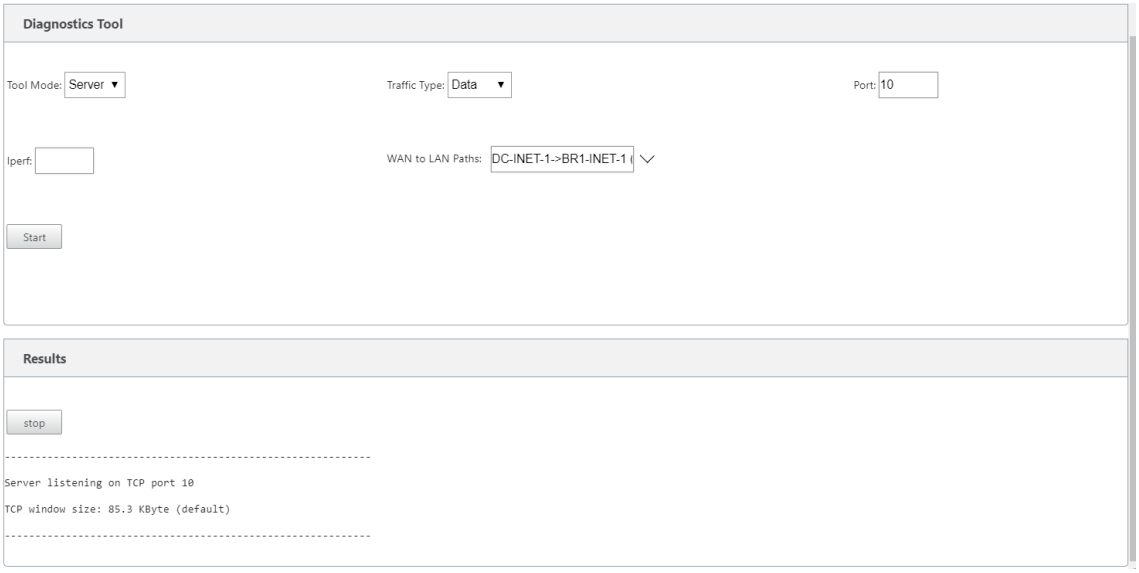
- **Control**: Genera tráfico sin que se aplique la calidad de servicio/programación a los paquetes. Como resultado, los paquetes se envían a través de la ruta seleccionada en la interfaz de usuario, incluso si la ruta no es la mejor en ese momento. Este tráfico se utiliza para probar rutas específicas 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

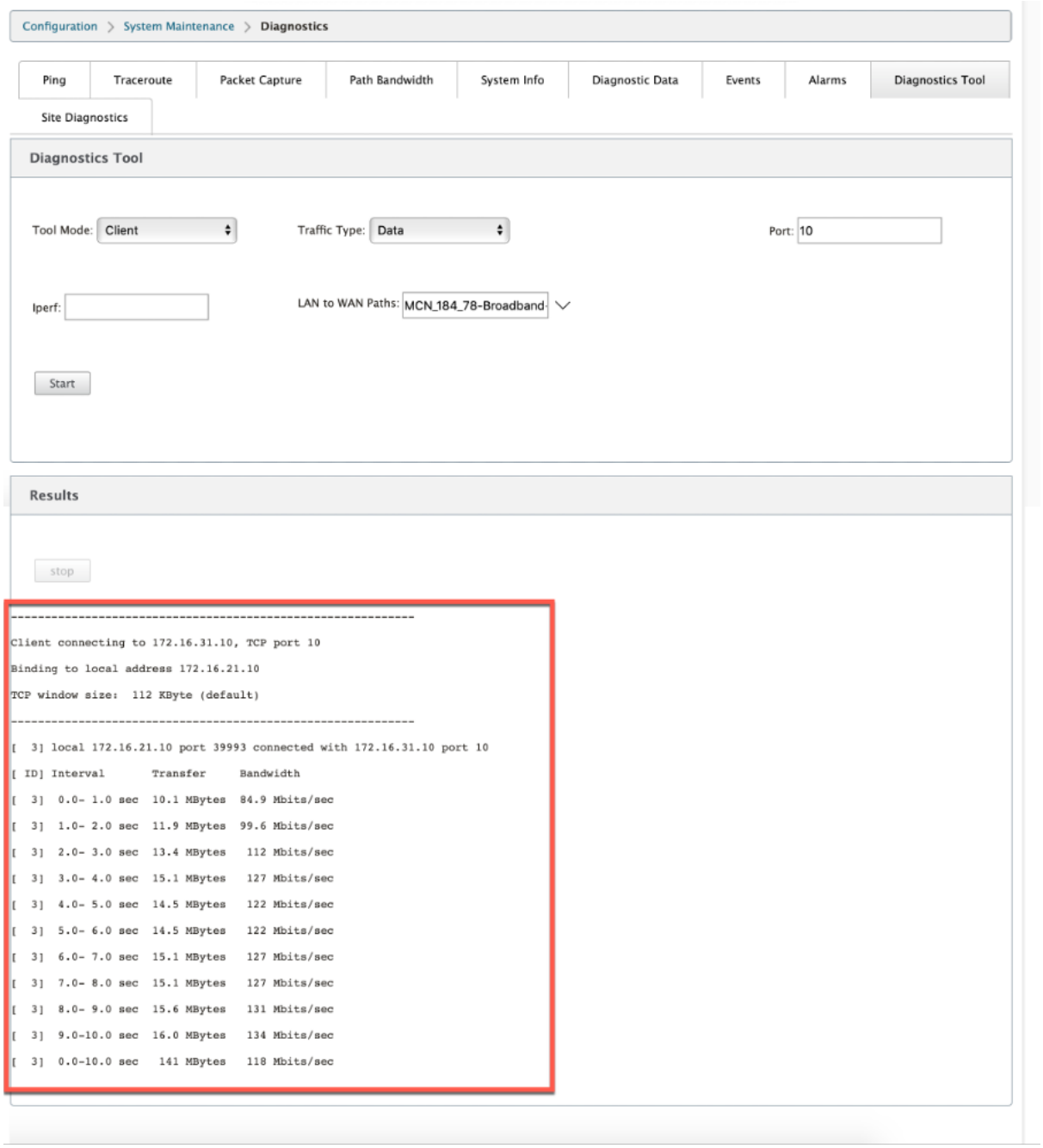
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - -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 desea 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

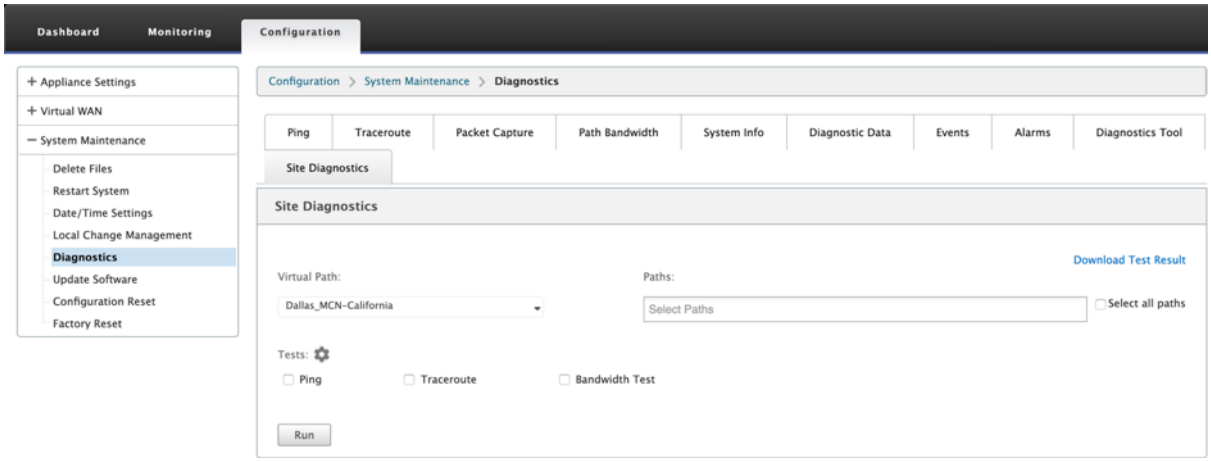


Diagnóstico del sitio

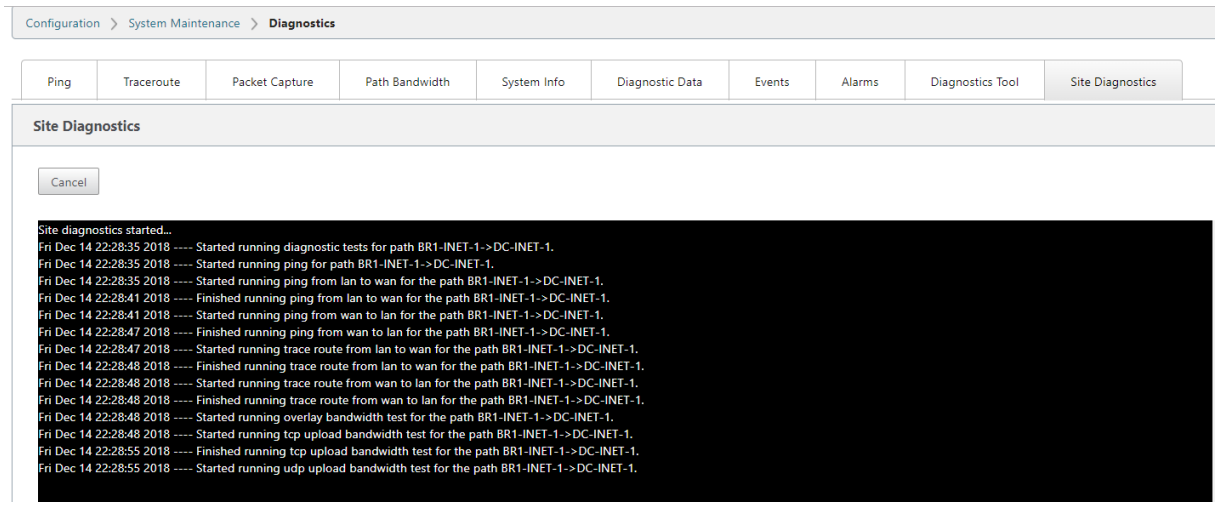
Puede probar el uso del ancho de banda, hacer ping y realizar traceroute para los vínculos WAN configurados en diferentes sitios de la red Citrix SD-WAN. Proporciona información que ayuda a solucionar problemas en la configuración existente.

Para utilizar **Diagnóstico del sitio**, vaya a **Configuración >** expanda **Mantenimiento del sistema > Diagnóstico** y seleccione **Herramienta de diagnóstico**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Resolución de problemas de IP de administración

May 7, 2021

Los siguientes son los casos posibles que puede encontrar al configurar la dirección IP 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 dispositivos SD-WAN; Standard Edition, WANOP y Premium (Enterprise) Edition - Físicos y virtuales.

> **Nota**
>
> Todos los modelos de hardware de dispositivos SD-WAN se envían con una dirección IP de administración predeterminada de fábrica. Asegúrese de configurar la dirección IP DHCP necesaria para el dispositivo durante el proceso de instalación.
>
> 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 encienden 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 reintentarán la solicitud DHCP cada 300 segundos (valor predeterminado). El intervalo real es de aproximadamente 7 minutos
  - Por lo tanto, los dispositivos con servicio DHCP habilitado adquirirán direcciones DHCP en un plazo de 7 minutos después de que los servidores DHCP estén disponibles. El retardo oscila entre 0 y 7 minutos

La dirección DHCP asignada caduca:

- Comportamiento esperado:
  - Los dispositivos con servicio DHCP habilitado intentarán renovar la concesión antes de que caduque la dirección
  - Los dispositivos comienzan con el descubrimiento de DHCP nuevo, si falla la renovación

Los dispositivos con el servicio DHCP habilitado se mueven de una subred habilitada para DHCP a otra subred:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 que se reinicien los dispositivos para adquirir una dirección IP del nuevo servidor DHCP.
  - Tras la expiración de la concesión 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 Gateway no se modifica en la GUI y la CLI. Se actualiza después de completar el proceso de reinicio.

Recomendación:

- Asigne siempre la concesión permanente para las direcciones DHCP asignadas a dispositivos Citrix SD-WAN (físico/virtual). Esto permite que los dispositivos tengan una dirección IP de administración predecible.

Notificaciones HTTP basadas en sesiones

May 7, 2021

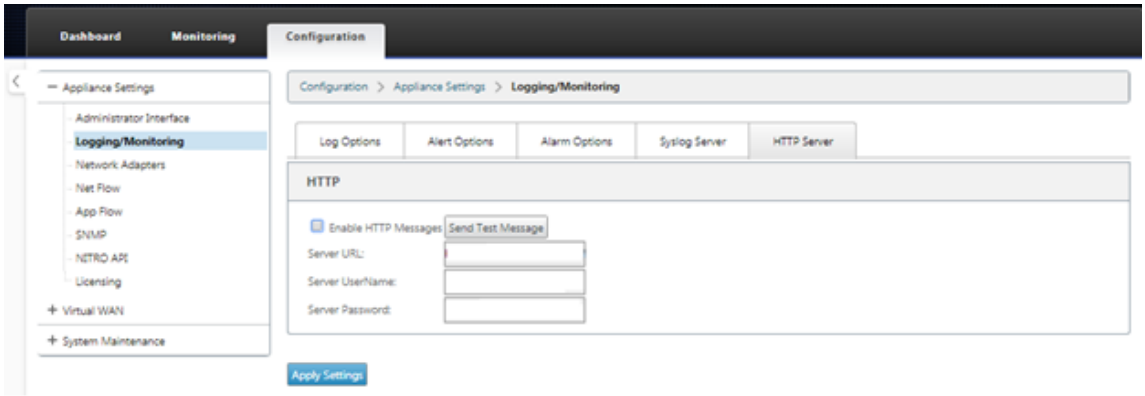
Ahora puede configurar los informes de eventos y alarmas para las solicitudes genéricas de servicio HTTP POST API en la GUI del dispositivo Citrix SD-WAN. La configuración de alarma y notificación de eventos HTTP son similares a los eventos de correo electrónico y SNMP para eventos y alarmas compatibles con SD-WAN.

La notificación HTTP Post basada en sesión se envía a un servicio externo, como Service Now. Las notificaciones de eventos para el servidor HTTP se pueden configurar en la GUI del dispositivo Citrix SD-WAN y Citrix SD-WAN Center.

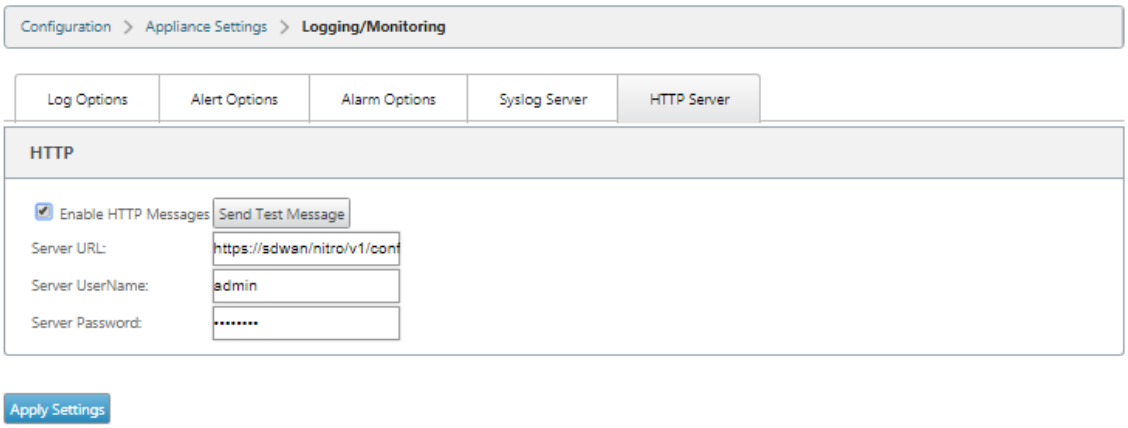
Para configurar las notificaciones HTTP POST en la GUI del dispositivo Citrix SD-WAN:

1. Vaya a **Configuración** > **Registro/Supervisión** > **Servidor HTTP**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Haga clic en **Habilitar mensajes HTTP**.
3. Introduzca la **dirección URL** del servidor HTTP del que quiere recibir notificaciones. Introduzca el nombre de **usuario del servidor** y la **contraseña del servidor**.



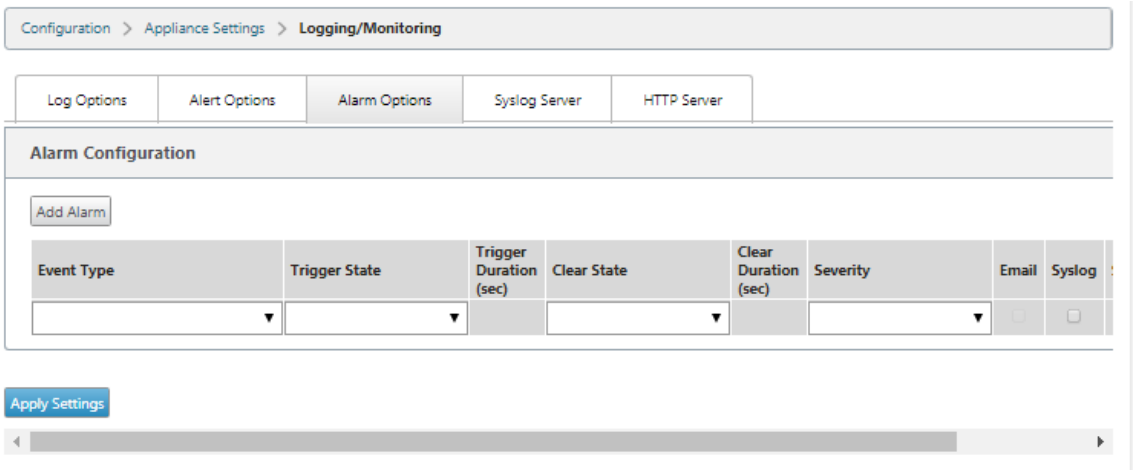
4. Haga clic en **Aplicar configuración**. La página se actualiza después de aplicar la configuración de notificaciones del servidor HTTP.

> **Nota**
>
> Utilice la opción **Enviar mensaje de prueba** para comprobar que la conexión del servidor HTTP es correcta.

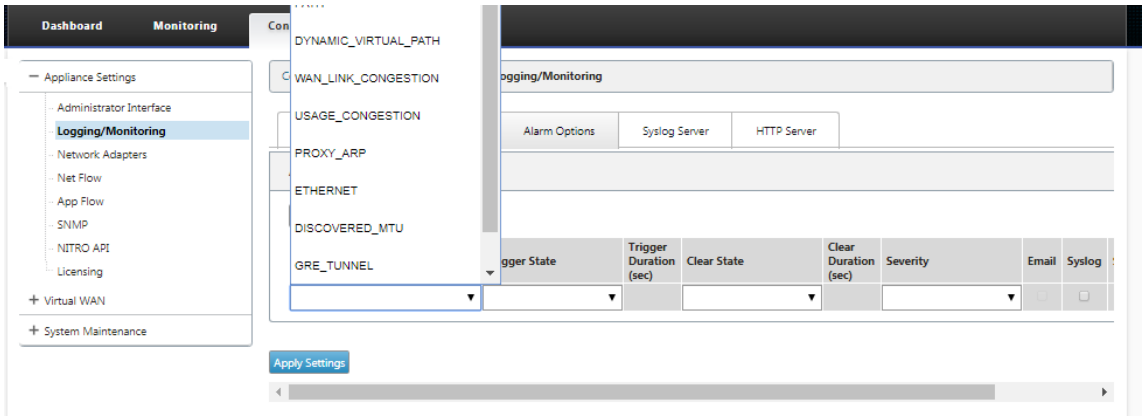
Para agregar una notificación de alarma para la sesión del servidor HTTP:

1. En la página **Registro/Monitoring**, vaya a la página de la ficha **Opciones de alarma**.
2. Haga clic en **Agregar alarma**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



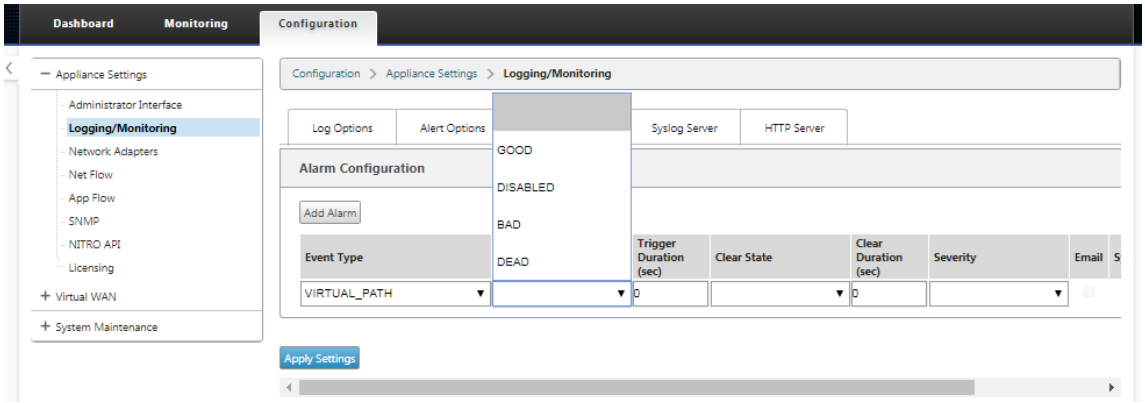
3. Seleccione un **tipo de evento** en la lista implementable.

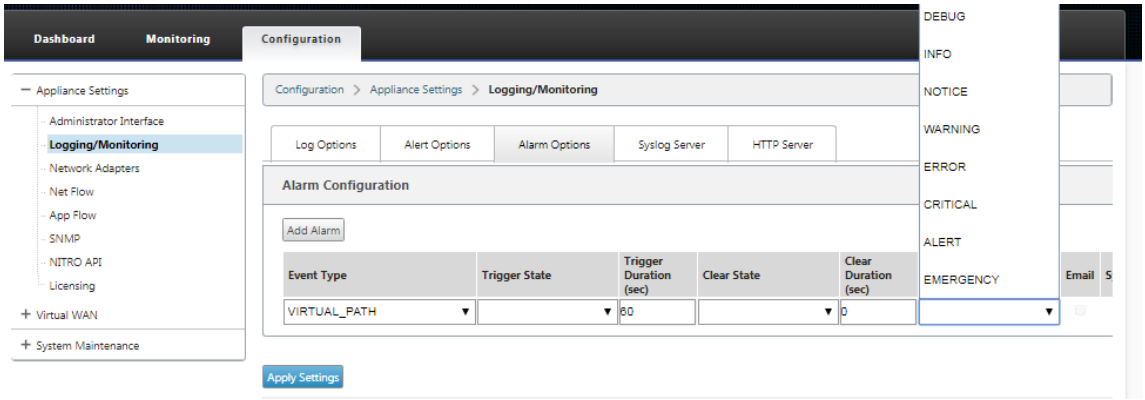


4. Seleccione los siguientes estados de notificación de alarma para el **tipo de evento**seleccionado. El estado de activación y el estado de borrado cambian según el tipo de evento seleccionado.

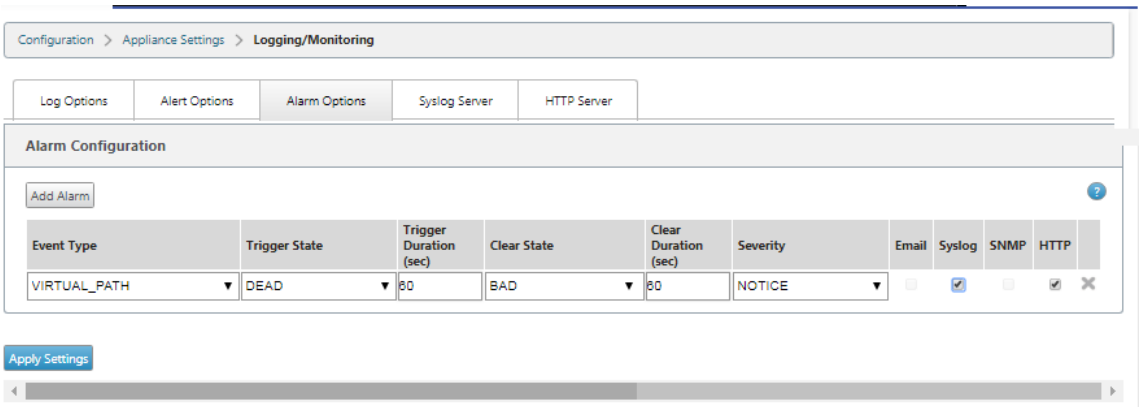
   - Estado de activación: BUENO, INHABILITADO, INCORRECTO, DESCONECTADO
   - Duración del disparo: Tiempo en segundos
   - Estado despejado: BUENO, INHABILITADO, INCORRECTO, DESCONECTADO
   - Duración clara: Tiempo en segundos
   - Severidad: Depuración, información, aviso, advertencia, error, crítico, evento, emergencia

© 1999–2024 Cloud Software Group, Inc. All rights reserved.





5. Active las casillas de verificación **Syslog** y **HTTP** para recibir notificaciones específicas de los eventos del servidor Syslog y HTTP. Haga clic en **Aplicar configuración**.

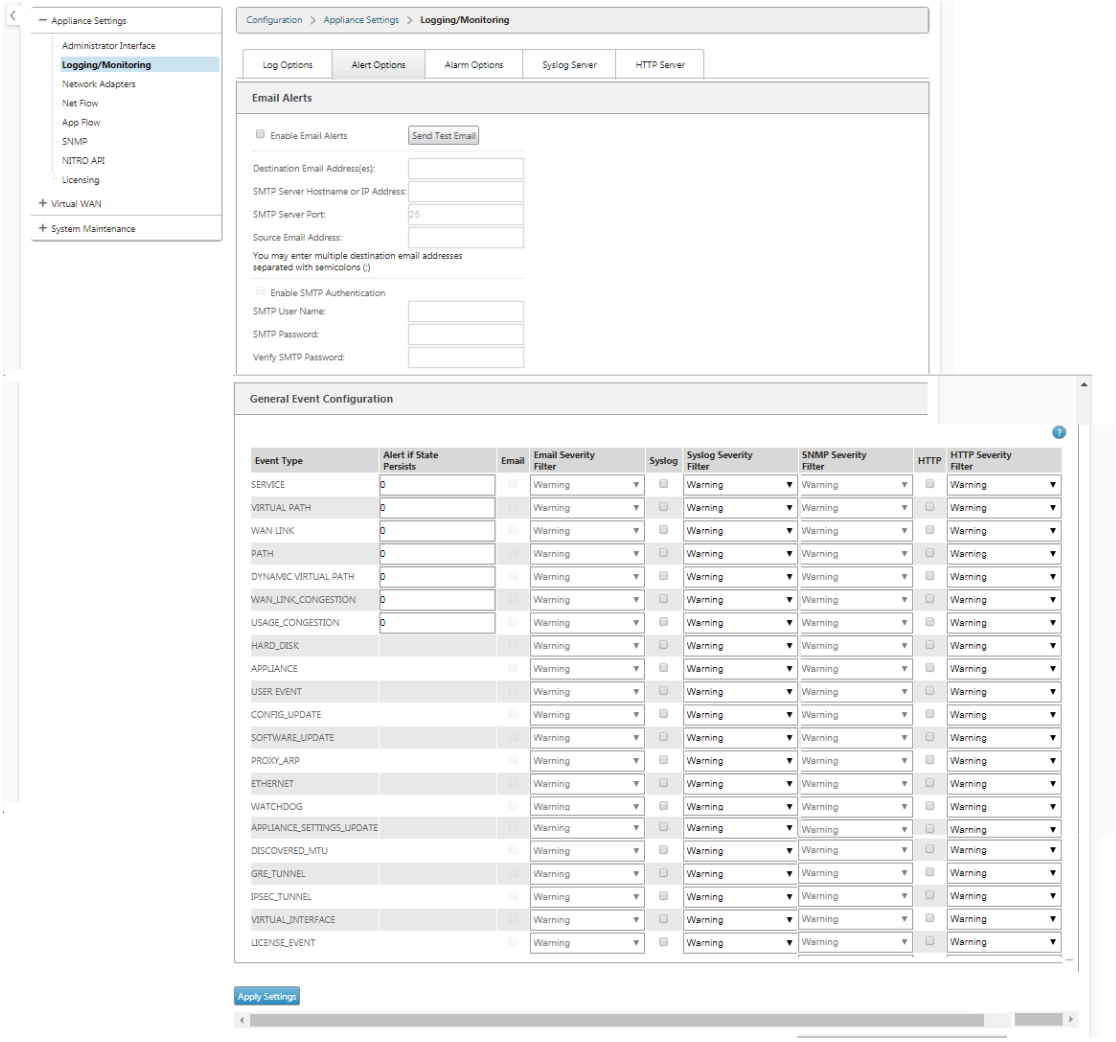


Para configurar las opciones de eventos:

Vaya a la página de la ficha **Opciones de alerta**. En **la página Configuración general de eventos**, seleccione el filtro de notificación del servidor HTTP para un **tipo de evento** y haga clic en **Aplicar configuración**.

- HTTP
- Filtro de gravedad HTTP

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

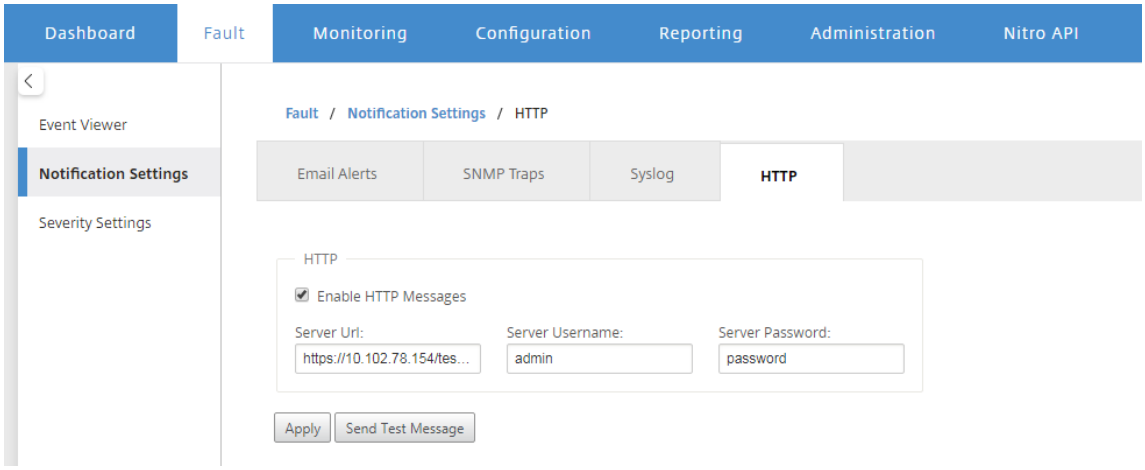


Configurar notificaciones HTTP en Citrix SD-WAN Center

Para configurar notificaciones HTTP:

1. Desplácese hasta **Fallo** > **Configuración de notificaciones** > **HTTP**.

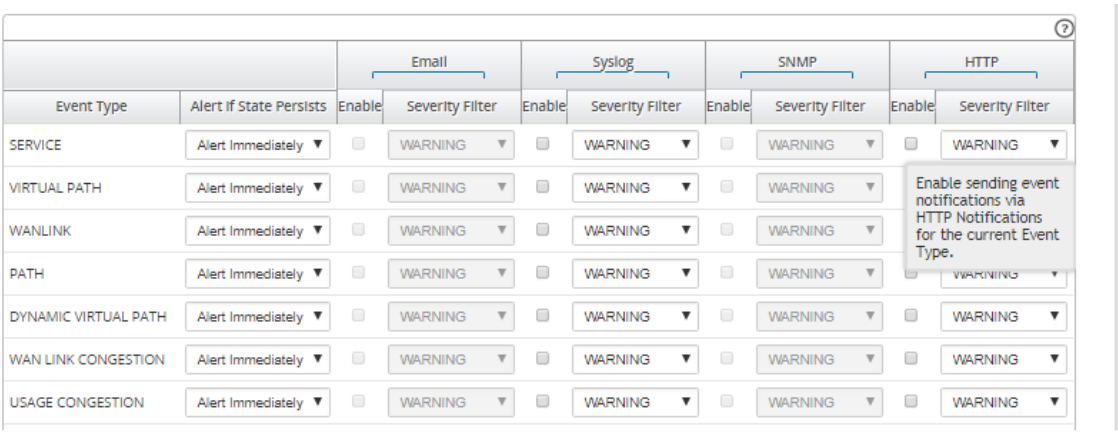
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**

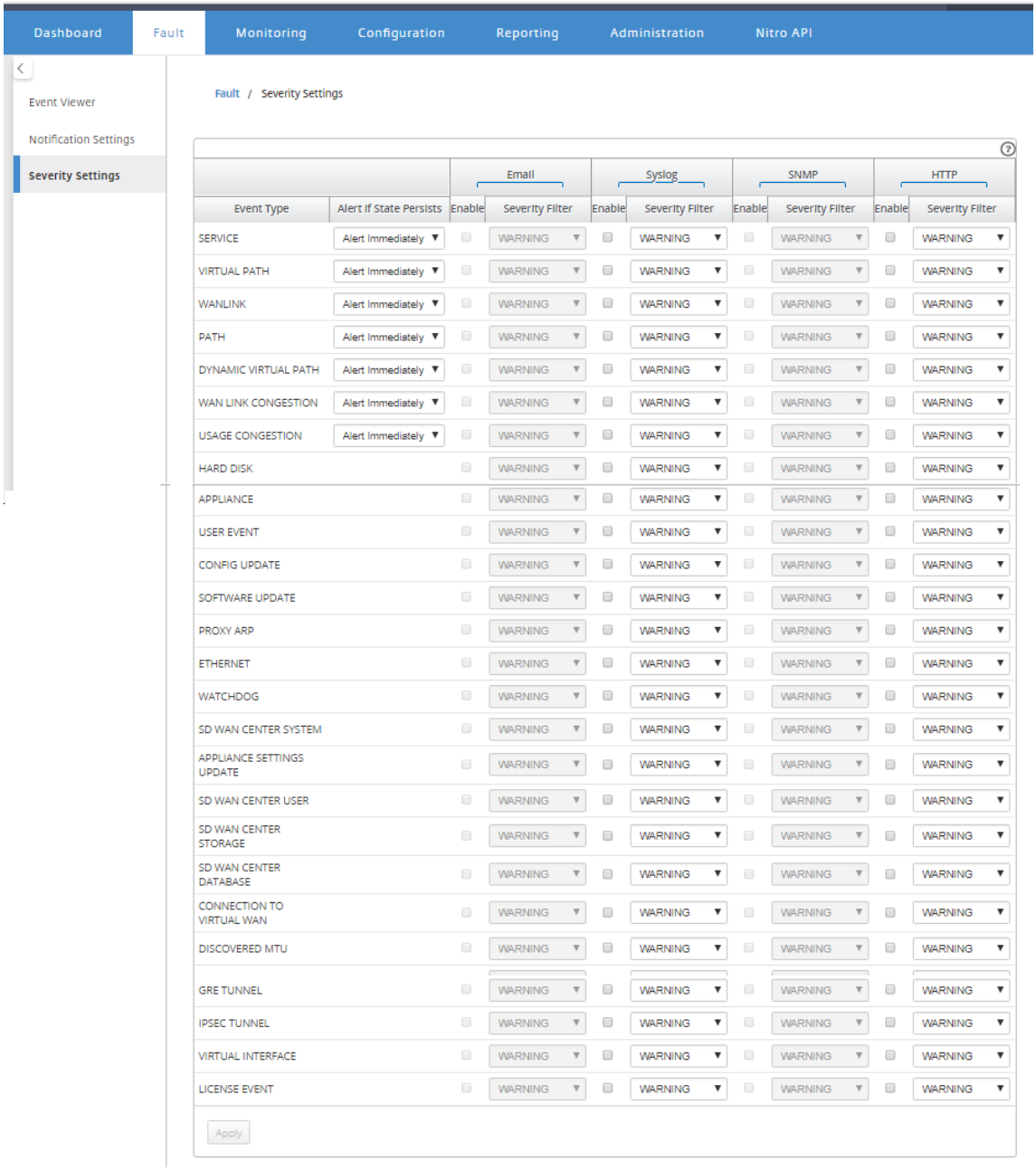
Para configurar los valores de gravedad:

1. Vaya a la página **Configuración de gravedad**. Haga clic en **Habilitar** para comenzar 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 eventos. Haga clic en **Aplicar**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pruebas de ancho de banda activo

May 7, 2021

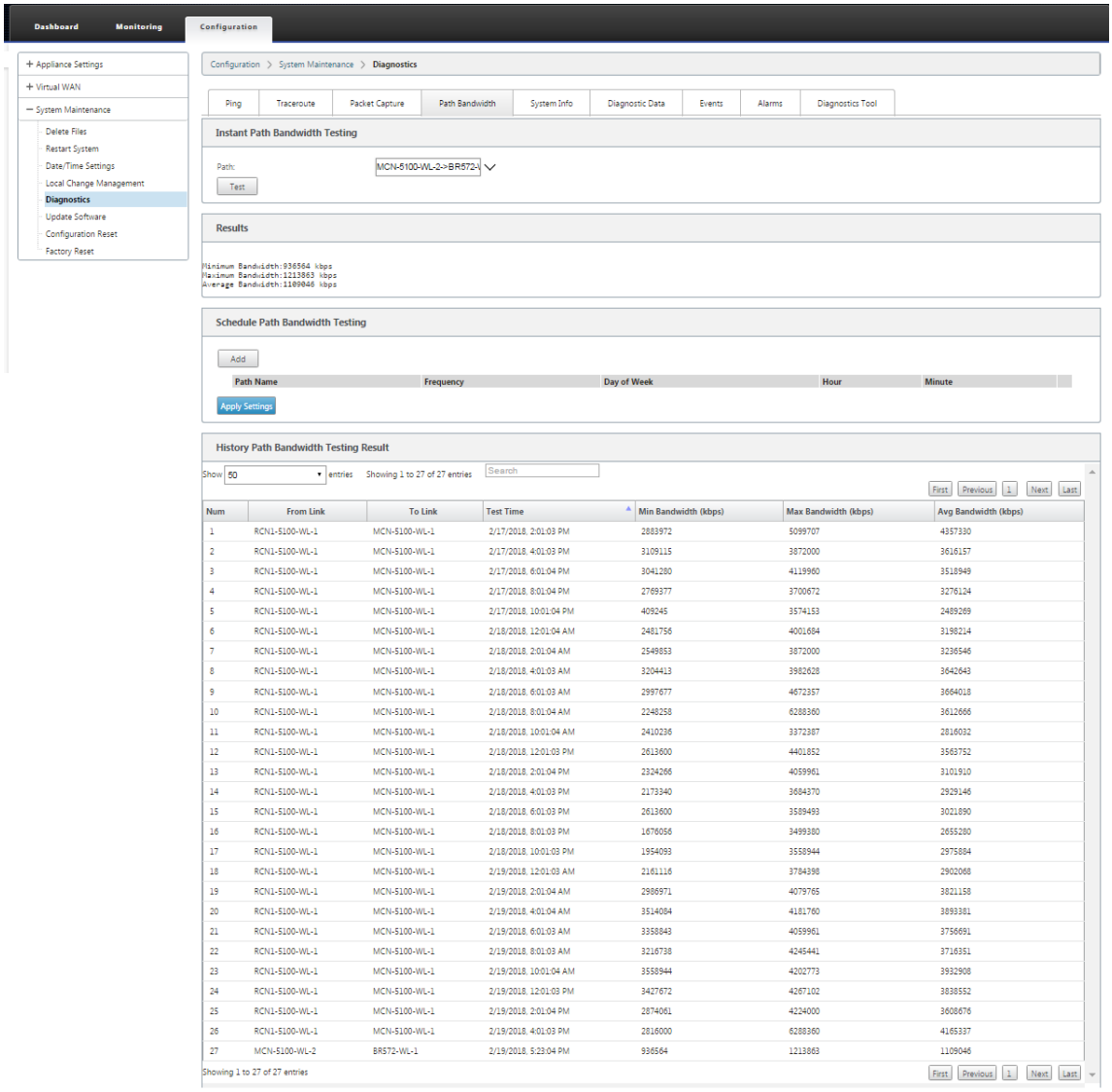
Las pruebas activas de ancho de banda le permiten realizar una prueba instantánea de ancho de banda de path a través de un enlace público de Internet WAN, o programar pruebas de ancho de banda de enlace público de Internet WAN para que se completen en momentos específicos de forma

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

periódica. Esta función es útil para demostrar cuánto ancho de banda está disponible entre dos ubicaciones durante instalaciones nuevas y existentes, también 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** > **Diagnósticos** > **Ancho de banda de ruta**.
2. Seleccione la **ruta** deseada y haga clic en **Probar**.

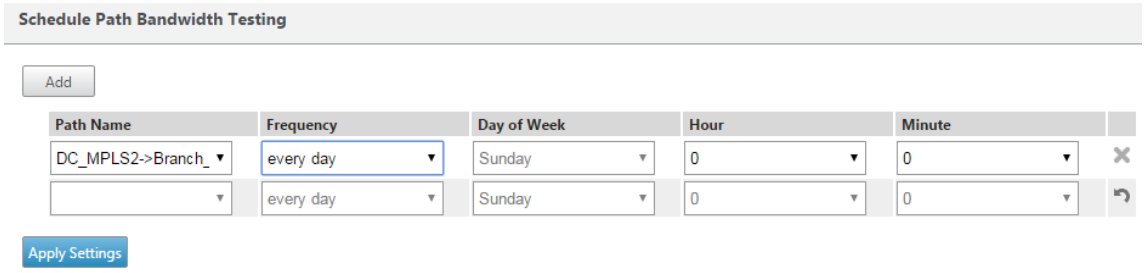


La salida muestra el ancho de banda medio utilizado como valor para establecer como la velocidad permitida para los resultados de ancho de banda mínimo y máximo de enlace WAN de la prueba. Junto con la capacidad de probar el ancho de banda, ahora puede cambiar el archivo de configuración para usar el ancho de banda aprendido. Esto se logra a través de la opción Aprendizaje automático que se encuentra en **Sitio** > [Nombre del sitio] > **Vínculos WAN**> [Nom-

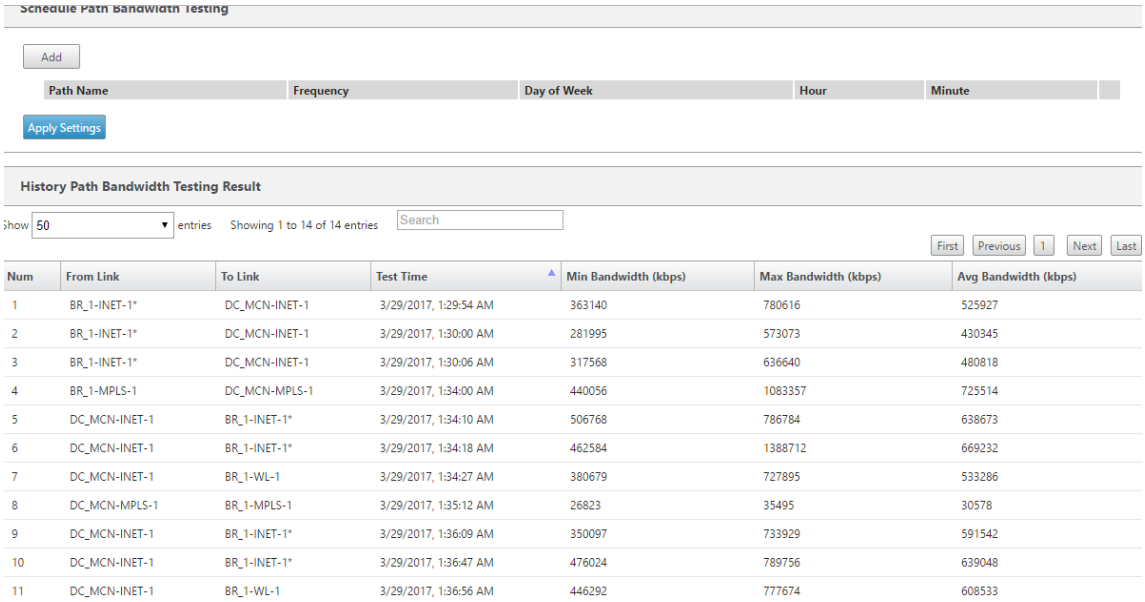
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

bre 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.



Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	480818
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM	440056	1083357	725514
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM	506768	786784	638673
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM	462584	1388712	669232
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM	380679	727895	533286
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM	26823	35495	30578
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM	350097	733929	591542
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM	476024	789756	639048
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM	446292	777674	608533

Detección de ancho de banda adaptable

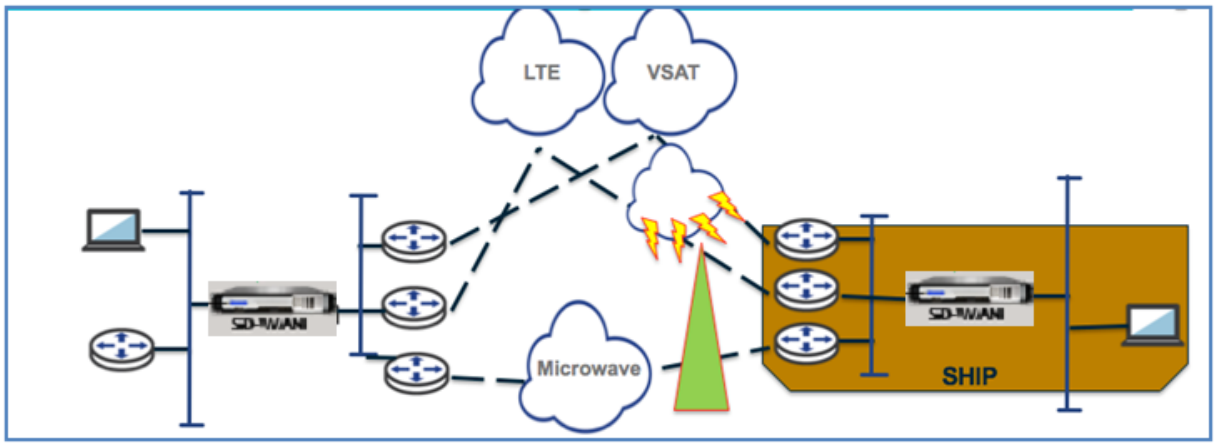
May 7, 2021

Esta función es aplicable a redes con VSAT, LOS, Microondas, 3G/4G/LTE WAN Links, para las que el ancho de banda disponible varía según las condiciones climáticas y atmosféricas, la ubicación y las obstrucciones de línea de sitio. Permite a los dispositivos SD-WAN ajustar la velocidad de ancho de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

banda en el enlace WAN dinámicamente en función de un rango de ancho de banda definido (velocidad de enlace WAN mínima y máxima) para utilizar la cantidad máxima de ancho de banda disponible sin marcar las rutas INCORRECTA.

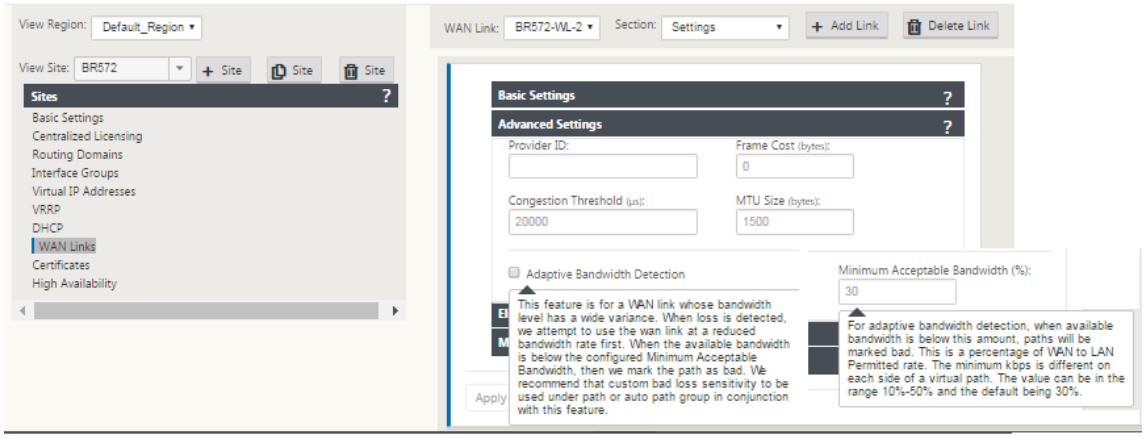
- Mayor fiabilidad del ancho de banda (a través de VSAT, microondas, 3G/4G y LTE)
- Mayor previsibilidad del ancho de banda adaptativo sobre la configuración configurada por el usuario



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. Puede habilitarlo en **Global** >**Grupos de ruta automática** > [**Nombre de grupo de rutas automáticas**] > **Sensible a pérdidas incorrectas**.

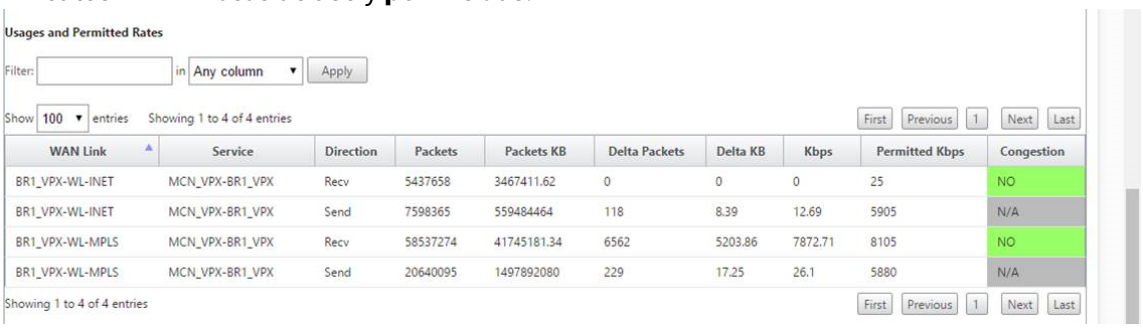
1. Enable **Adaptive Bandwidth Detection** under **Global** >**Autopath Groups** > [**Nombre de grupo de rutas automáticas**] >**Bad Loss Sensitive**.
2. Vaya al **Configuration Editor** > **Sites** > [**Nombre del sitio**] > **WAN Links** > [**Nombre del enlace WAN**] > **Settings** > **Advanced Settings**.



3. Active la casilla **Detección de ancho de banda adaptable** e introduzca un valor en el campo **Ancho de banda mínimo aceptable**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Consulte la tabla **Uso y Tarifas Permitidas**. Para ello, vaya a **Monitor** > **Estadísticas** > **Uso de vínculos WAN** > Tasas de **uso** y **permitidas**.



Usages and Permitted Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

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

Showing 1 to 4 of 4 entries First Previous 1 Next Last

Prácticas recomendadas

May 7, 2021

Los temas siguientes proporcionan las prácticas recomendadas que deben seguirse cuando se diseña, planifica y ejecuta la solución Citrix SD-WAN en la red.

Seguridad

Redirección

QoS

Enlaces WAN

Seguridad

May 7, 2021

En este artículo se describen las prácticas recomendadas de seguridad para la solución Citrix SD-WAN. Proporciona orientación general de seguridad para las implementaciones de Citrix SD-WAN.

Directrices de implementación de Citrix SD-WAN

Para mantener la seguridad durante el ciclo de vida de la implementación, Citrix recomienda la siguiente consideración de seguridad:

- Seguridad física
- Seguridad del dispositivo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Seguridad de red
- Administración y Gestión

Seguridad física

Implementar dispositivos Citrix SD-WAN en una sala de servidores seguros: El dispositivo o servidor en el que está instalado Citrix SD-WAN debe colocarse en una sala de servidores seguros o en un centro de datos restringido, que proteja al dispositivo del acceso no autorizado. Como mínimo, el acceso debe ser controlado por un lector electrónico de tarjetas. El acceso al dispositivo es supervisado por CCTV, que registra continuamente toda la actividad con fines de auditoría. Si un robo, el sistema de vigilancia electrónica debe enviar una alarma al personal de seguridad para una respuesta inmediata.

Proteja los puertos del panel frontal y de la consola del acceso no autorizado: Asegure el dispositivo en una jaula grande o rack con control de acceso con llave física.

Proteger la fuente de alimentación: Asegúrese de que el dispositivo está protegido con un sistema de alimentación ininterrumpida (UPS).

Seguridad del dispositivo

Para la seguridad del dispositivo, proteja el sistema operativo de cualquier servidor que aloje un dispositivo virtual SD-WAN (VPX) de Citrix, realice actualizaciones de software remotas y siga las 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 dispositivo virtual en un servidor estándar. El acceso al servidor estándar debe protegerse con un control de acceso basado en roles y una administración segura de contraseñas. Además, Citrix recomienda actualizaciones periódicas en el servidor con las revisiones 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 de Boletines de seguridad para registrarse y recibir alertas de seguridad actualizadas.
- Siga las prácticas de administración del ciclo de vida seguro: Para administrar un dispositivo al volver a implementar o iniciar RMA y retirar datos confidenciales, complete las contramedidas de recuerdos de datos eliminando los datos persistentes del dispositivo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Seguridad de red

Para la seguridad de la red, no utilice el certificado SSL predeterminado. Utilice la seguridad de la capa de transporte (TLS) al acceder a la interfaz de administrador, proteja la dirección IP de administración no enrutable del dispositivo, configure una configuración de alta disponibilidad e implemente las salvaguardias de administración y administración según corresponda para la implementación.

- No utilice el certificado SSL predeterminado: Un certificado SSL de una entidad de certificación reputada simplifica la experiencia del usuario para aplicaciones Web orientadas a Internet. A diferencia de lo que ocurre con un certificado autofirmado o un certificado de la entidad de certificación reputada, los exploradores web no requieren que los usuarios instalen el certificado de la entidad de certificación reputada para iniciar una comunicación segura con el servidor Web.
- Utilizar la seguridad de la capa de transporte al acceder a la interfaz de administrador: Asegúrese de que la dirección IP de administración no sea accesible desde Internet o esté protegida por un firewall seguro. Asegúrese de que la dirección IP LOM no sea accesible desde Internet o esté protegida por un firewall seguro.
- Cuentas de administración y administración seguras: Cree una cuenta de administrador alternativa, establezca contraseñas seguras para cuentas de administrador y visor. Al configurar el acceso remoto a cuentas, considere la posibilidad de configurar la administración administrativa autenticada externamente de cuentas mediante RADIUS y TACAS. Cambie la contraseña predeterminada para 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 de superposición Citrix SD-WAN protege los datos que atraviesan la red de superposición 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 la contraseña de usuario local
- Administrar usuarios

Certificados HTTPS:

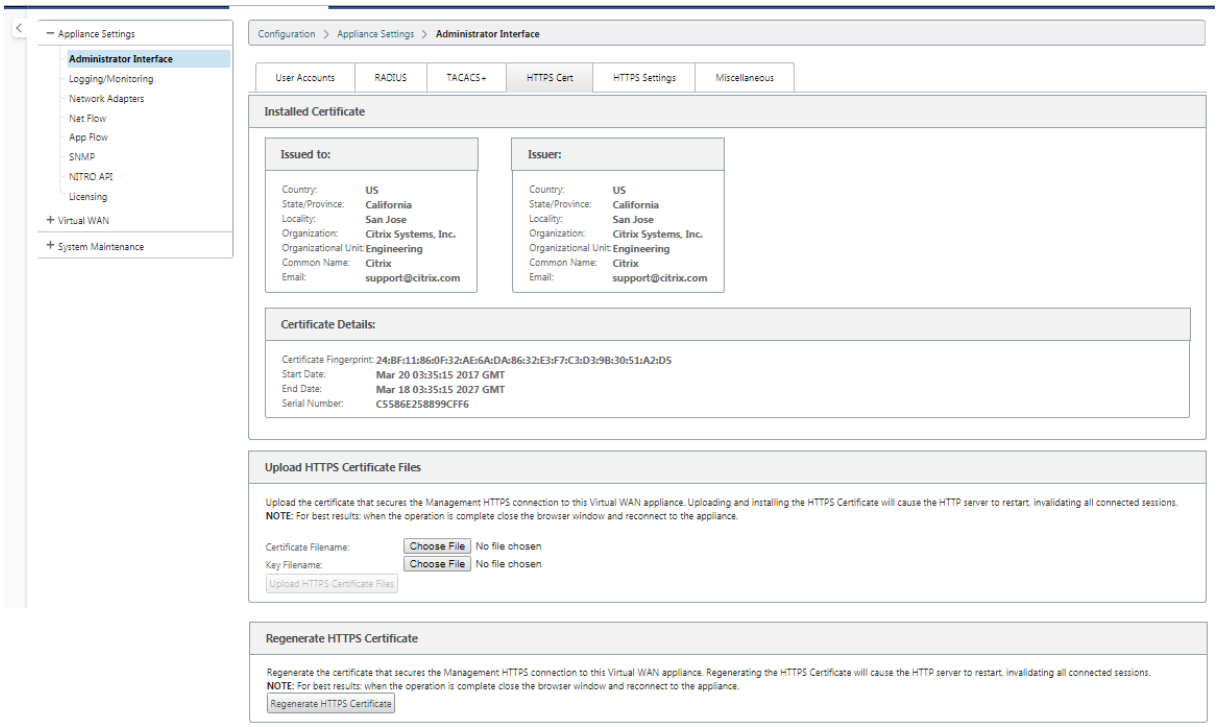
- Certificado

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Tecla

Varios:

- Tiempo de espera de la consola Web



Editor de configuración > **Global** > **Configuración de red**

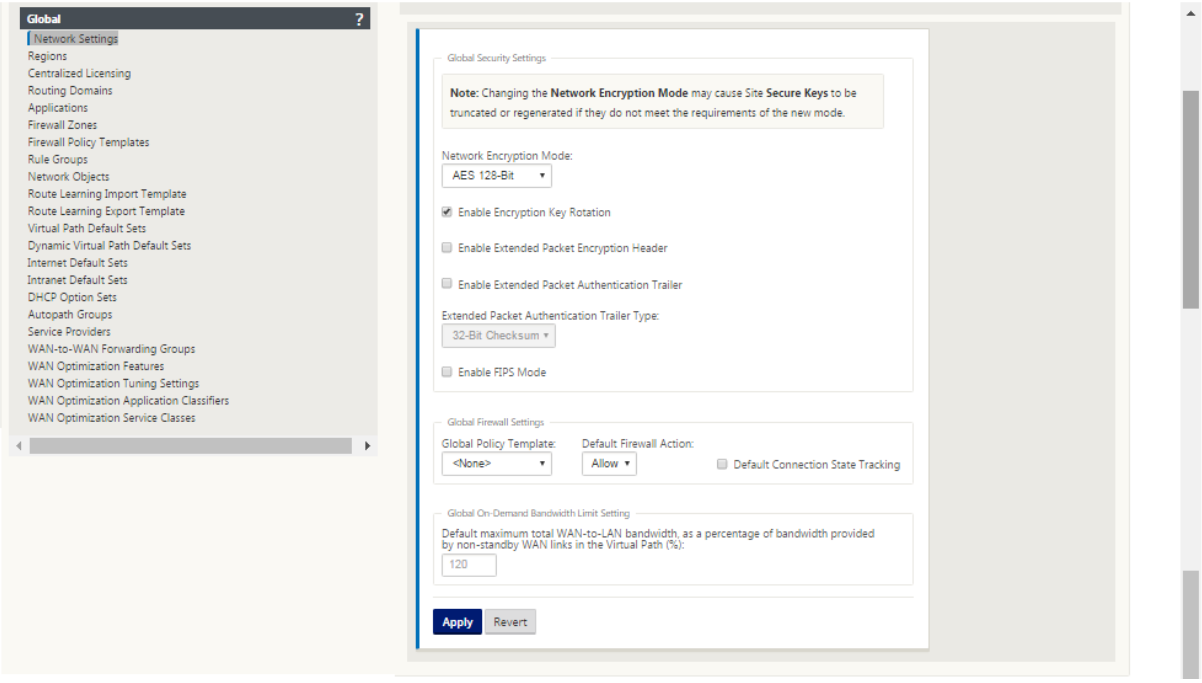
Configuración global del firewall:

- Plantilla de directiva global
- Acciones predeterminadas del firewall
- Seguimiento del estado de conexión predeterminado

Configuración de cifrado de ruta virtual global:

- AES de 128 bits (predeterminado)
- Rotación de clave de cifrado (valor predeterminado)
- Encabezado de cifrado de paquetes extendido
- Tráiler de autenticación de paquetes extendidos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuración de cifrado de rutas virtuales globales

- 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 “habilitar la rotación de claves de cifrado”esté configurado 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 10-15 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.

- Encabezado de cifrado de paquetes extendido permite que un contador predefinido aleatoriamente se antepone al principio de cada mensaje cifrado. Cuando se cifra, este contador sirve como un vector de inicialización aleatoria, determinista solo con la clave de cifrado. Esto aleatoriza la salida del cifrado, proporcionando mensajes fuertes indistinguibles. Tenga en cuenta que cuando está habilitada esta opción aumenta la sobrecarga del paquete en 16 bytes
- El Trailer de autenticación de paquetes extendido agrega un código de autenticación al final de cada mensaje cifrado. Este remolque permite verificar que los paquetes no se modifican en tránsito. Tenga en cuenta que esta opción aumenta la sobrecarga del paquete.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Seguridad del firewall

La configuración recomendada de Firewall es con una acción predeterminada de Firewall como deny all al principio y, a continuación, agregue 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 realice un seguimiento y permita revisar los cambios en la configuración del **firewall**. Configure el Firewall para todos los dispositivos para realizar un seguimiento de las conexiones a través del dispositivo mediante la configuración global. El seguimiento de las conexiones verifica que los paquetes estén correctamente formados y sean apropiados para el estado de conexión. Crear zonas adecuadas a la jerarquía lógica de la red o áreas funcionales de la organización. Tenga en cuenta que las zonas son globalmente significativas 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 las reglas Cualquiera en 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 directiva basadas en roles funcionales de los dispositivos en la red y aplíquelas cuando proceda. Defina directivas en sitios individuales solo cuando sea necesario.

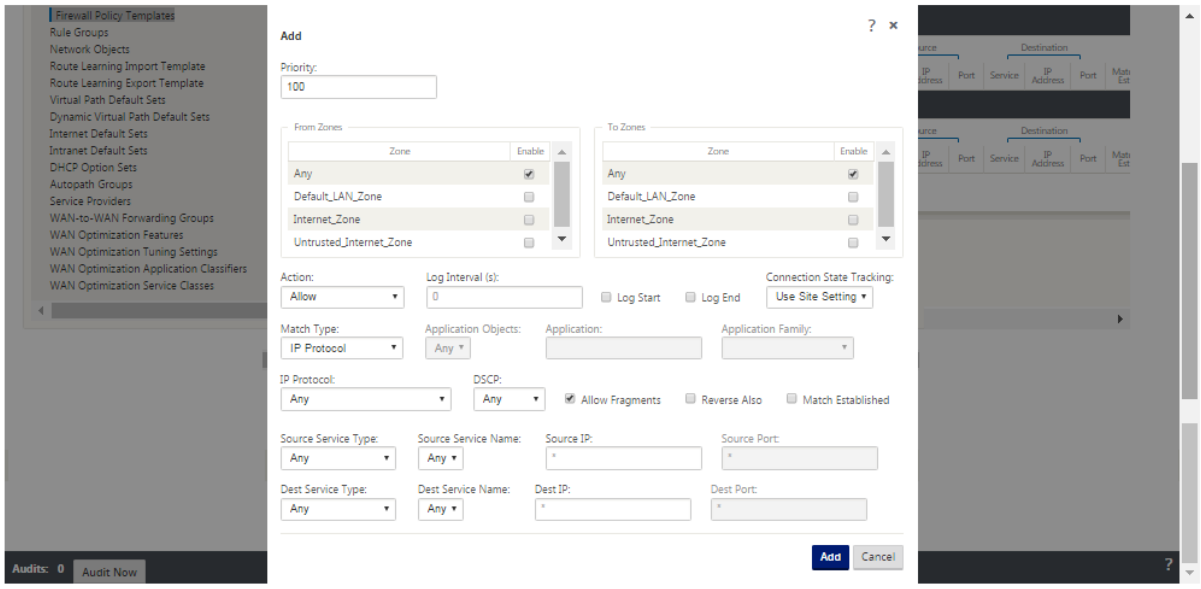
Plantillas de firewall globales: Las plantillas de firewall permiten la configuración de parámetros globales que afectan el funcionamiento del firewall en dispositivos individuales que operan en el entorno de superposición SD-WAN.

Acciones predeterminadas del firewall: Permite permitir paquetes que no coincidan con ninguna directiva de filtro. Denegar permite que se eliminen los paquetes que no coinciden con ninguna directiva de filtro.

Seguimiento del estado de conexión predeterminado: Habilita 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 se habilita incluso cuando no hay directivas de firewall definidas. La configuración se puede definir en el nivel del sitio, lo que anulará 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 globalmente.

Zonas: Las zonas de firewall definen la agrupación de seguridad lógica de redes conectadas a Citrix SD-WAN. Las zonas se pueden aplicar a interfaces virtuales, servicios de intranet, túneles GRE y túneles IPsec LAN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Zona de seguridad de enlace WAN

La zona de seguridad no confiable debe configurarse en enlaces WAN conectados directamente a una red pública (no segura). La opción no confiable establecerá el enlace WAN en su estado más seguro, permitiendo que solo se acepte tráfico cifrado, autenticado y autorizado en el grupo de interfaz. ARP e ICMP a la dirección IP virtual son el único otro tipo de tráfico permitido. Esta configuración también garantizará que solo el tráfico cifrado se envíe fuera de 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.

Editor de configuración > **Global**

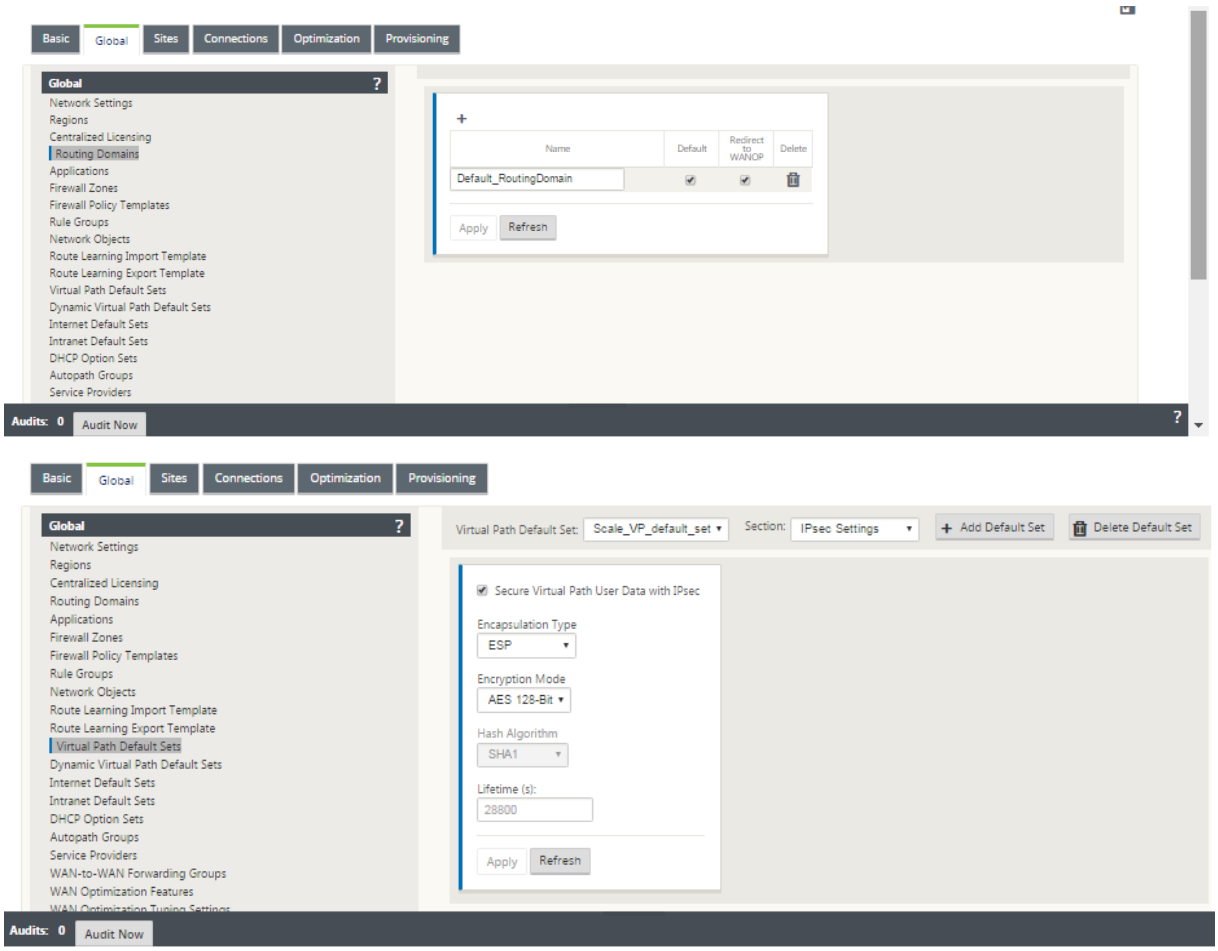
Dominios de redirección

- Default_RoutingDomain

Túneles IPSec

- Conjuntos predeterminados
- Datos de usuario de ruta virtual segura con IPSec

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Túneles IPSec

Los túneles IPSec protegen tanto los datos de usuario como la información de 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 a través de la ruta virtual antes de que los datos puedan fluir a través de la red de superposición SD-WAN.

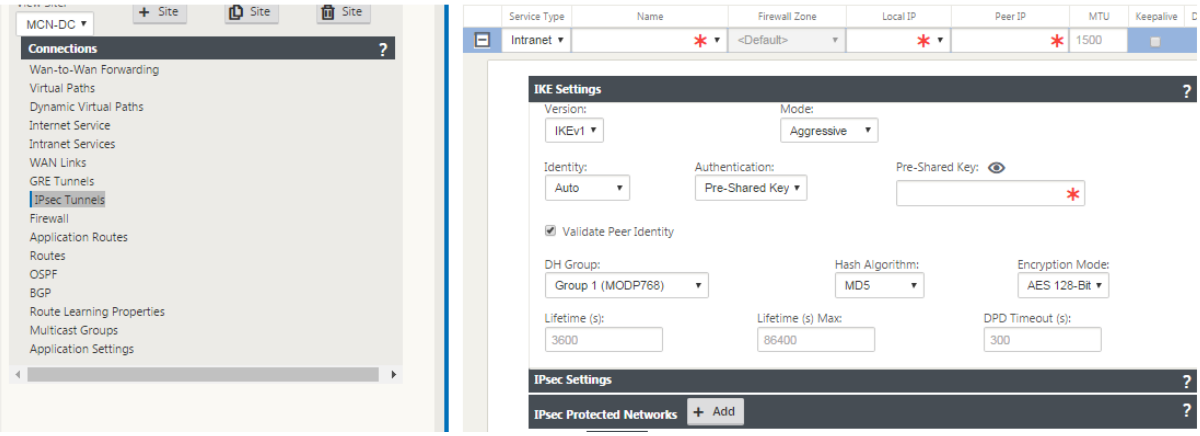
- Las opciones de tipo de encapsulación incluyen ESP: Los datos se encapsulan y cifran, ESP+Auth: Los datos se encapsulan, cifran y validan con un HMAC, AH: Los datos se validan con un HMAC.
- El modo de cifrado es el algoritmo de cifrado utilizado cuando ESP está habilitado.
- Algoritmo hash se utiliza para generar un HMAC.
- La duración es la duración preferida, en segundos, para que exista una asociación de seguridad IPSec. 0 se puede utilizar de forma ilimitada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración IKE

Intercambio de claves de Internet (IKE) es un protocolo IPSec utilizado para crear una asociación de seguridad (SA). Los dispositivos Citrix SD-WAN admiten los protocolos IKEv1 e IKEv2.

- El modo puede ser el modo principal o el modo agresivo.
- La identidad puede ser automática para identificar el par, o una dirección IP se puede utilizar para especificar manualmente la dirección IP del par.
- La autenticación habilita la autenticación de clave previamente compartida o el certificado como método de autenticación.
- Validar identidad del mismo nivel permite la validación de la identidad del mismo nivel del IKE si se admite el tipo de ID del mismo nivel; 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.
- 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 están disponibles para los mensajes IKE.
- La configuración de IKEv2 incluye Autenticación del mismo nivel y Algoritmo de Integridad.



Configuración del firewall

Los siguientes problemas comunes se pueden identificar comprobando la configuración de Router y Firewall de subida:

- Configuración de colas MPLS y QoS: Compruebe que el tráfico encapsulado UDP entre direcciones IP virtuales SD-WAN no se vea afectado debido a la configuración de **QoS** en los dispositivos intermedios de la red.
- Todo el tráfico de los enlaces WAN configurados en la red SD-WAN debe ser procesado por el dispositivo Citrix SD-WAN mediante el tipo de servicio correcto (Ruta de acceso virtual, Internet, Intranet y Local).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si el tráfico tiene que omitir el dispositivo Citrix SD-WAN y utilizar el mismo vínculo 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 SD-WAN.
- Verifique que el Router/Firewall intermedio no tenga ningún límite de inundación UDP y/o PPS impuesto. Esto limita el tráfico cuando se envía a través de la ruta virtual (encapsulado UDP).

Redirección

May 7, 2021

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 enruta a través de la ruta virtual a MCN.

Prioridad de redirección

El orden de prioridad de redirección:

- Coincidencia de prefijo: Coinciden los prefijos más largos.
- Servicio: Local, Servicio de ruta virtual, Internet, Intranet, Passthrough
- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

QoS

May 7, 2021

Tenga en cuenta lo siguiente al configurar QoS:

- Comprenda los patrones y requisitos de tráfico de red. Es posible que tenga que observar las **estadísticas de clase QoS**y cambiar las profundidades de la cola, y/o cambiar el porcentaje de cuota de clase QoS predeterminado para evitar caídas de cola como se muestra en las estadísticas 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 concretas. Agregar una subred completa a una regla 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

May 7, 2021

En este artículo se describen las prácticas recomendadas de configuración de enlaces WAN para la solución Citrix SD-WAN.

Puntos a recordar al configurar enlaces WAN:

- Configure la velocidad **permitida y física** como ancho de banda de enlace WAN real. En los casos en que el dispositivo SD-WAN no debe utilizar toda la capacidad de enlace WAN, cambie la velocidad **permitida** en consecuencia.
- Si no está seguro del ancho de banda y si los vínculos no son confiables, puede habilitar la función **Aprendizaje automático**. La función **Aprendizaje automático** sólo aprende la capacidad del vínculo subyacente y utiliza el mismo valor en el futuro.
- Si el enlace subyacente no es estable y no garantiza 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.
- Si el vínculo subyacente no es estable, cambie la siguiente configuración de ruta:
  - Configuración de pérdida

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Desactivar Sensible a la Inestabilidad
  - Tiempo de silencio
- Utilice la **herramienta de diagnóstico** para comprobar el estado y la capacidad del vínculo.
- Si SD-WAN se implementa en modo de **un brazo**, asegúrese de que no exceda la capacidad física del vínculo subyacente.

Verificación del estado del enlace de ISP

Para implementaciones nuevas, antes de la implementación de SD-WAN y al agregar un nuevo vínculo de ISP a la implementación de SD-WAN existente:

- Verifique el tipo de vínculo. 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

Generalmente se observa que el tráfico de red específico omite los dispositivos Citrix SD-WAN y utiliza el mismo vínculo subyacente configurado en la red SD-WAN. Debido a que SD-WAN no tiene visibilidad completa sobre la utilización del enlace, es probable que SD-WAN sobresuscriba el enlace, lo que lleva a problemas de rendimiento y PATH.

Provisioning

Puntos a tener en cuenta al Provisioning SD-WAN:

- De forma predeterminada, todas las sucursales y servicios WAN (Ruta virtual/Internet/Intranet) reciben la misma parte 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 que se conectan.
- 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

May 7, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Alta disponibilidad

¿Cuál es la diferencia entre el dispositivo High Availability y el dispositivo secundario (Geo)?

- La alta disponibilidad garantiza la tolerancia a fallos. El dispositivo secundario (Geo) permite la recuperación ante desastres.
- La alta disponibilidad se puede configurar para los dispositivos MCN, RCN y sucursales. El dispositivo secundario (geo) 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 (Geo).
- El dispositivo primario y secundario de alta disponibilidad deben ser los mismos modelos de plataforma. El dispositivo secundario (geo) puede o no ser el mismo modelo de plataforma que el MCN/RCN principal.
- La alta disponibilidad tiene mayor prioridad sobre la secundaria (Geo). Si un dispositivo (MCN/RCN) está configurado con dispositivos High Availability y Secondary (Geo), cuando el dispositivo falla, el dispositivo secundario de alta disponibilidad se activa. Si los dispositivos de alta disponibilidad fallan o si el sitio del centro de datos se bloquea, el dispositivo secundario (Geo) se activa.
- En Alta disponibilidad, la conmutación primaria/secundaria ocurre instantáneamente o dentro de 10-12 segundos, dependiendo de la implementación de alta disponibilidad. El cambio de MCN/RCN primario a MCN/RCN secundario (Geo) se produce después de 15 segundos de que el primario esté inactivo.
- La configuración de alta disponibilidad le permite configurar la recuperación primaria. No se puede configurar la recuperación primaria para el dispositivo secundario (Geo), la recuperación primaria se produce automáticamente después de que el dispositivo principal haya vuelto y expire el temporizador de retención.

Actualización de un solo paso

> **Nota**
>
> Los componentes del sistema operativo WANOP, SVM y XenServer Supplemental/HFS se ven como componentes del sistema operativo.

¿Debo usar.*tar.gz,* o actualizar el *paquete.zip* de un solo paso para actualizar a 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 SD-WAN a la versión 9.3.x, realice la administración de cambios mediante el *paquete.zip* para transferir/organizar paquetes de software de componentes del

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 será atendida por el paquete de actualización de un solo paquete.*zip* y se instala según los detalles de programación proporcionados por usted en la configuración de administración de cambios de los sitios respectivos.

¿Por qué debería usar.*tar.gz* seguido de un paquete.*zip* para actualizar de anteriores a 9.3 a 9.3.x, y por qué no usar directamente el paquete.*zip* de 9.3.x?

El paquete de actualización de un solo paso se admite a partir de 9.3.0.161 y en versiones anteriores (anteriores a la versión 9.3) este paquete no se reconoce. *Cuando el paquete de actualización de un solo paso se carga en la bandeja de entrada de Administración de cambios, el sistema genera un error que indica que el paquete no se reconoce.* Por lo tanto, primero actualice el software SD-WAN a la versión 9.3 o superior 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 pondrá en fase intermedia paquetes de software de componentes del sistema operativo basados en el modelo del dispositivo, una vez completada la administración de cambios mediante el paquete.*zip* de actualización de un solo paso. Después de la activación, el MCN comienza a transferir/organizar los paquetes de software de componentes del sistema operativo para las sucursales que los necesitan para la actualización/actualización programada.

¿Cómo instalo 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 solo se inicia cuando el dispositivo ha recibido todo el paquete necesario para el sitio, incluso cuando el valor de la **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 es aplicable únicamente a los componentes del sistema operativo y no a la actualización del software de VW. Con la actualización de 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de los componentes del sistema operativo en un momento diferente a la actualización de la versión del software de VW.

¿Por qué la información de programación de la página Configuración de administración de cambios aparece de forma predeterminada la fecha de programación anterior y qué significa?

La página **Configuración de Gestión de cambios** muestra la información de programación predeterminada que es, *"'start: 2016-05-21 21:20:00, window: 1, repeat: 1, unit: Days'"*. Si la fecha es una fecha pasada, significa que, la instalación programada se basa en la hora y otros parámetros como ventana de mantenimiento, ventana de repetición y unidad y no en la fecha.

¿Cuál es la fecha y hora de instalación de la programación predeterminada establecida en, depende del dispositivo genérico o local?

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) '*. Este detalle depende del sitio del dispositivo local.

¿Cómo puedo instalar componentes del sistema operativo inmediatamente sin esperar el mantenimiento o la ventana programada?

Establezca el valor de la **ventana de mantenimiento** en '**0** 'en la página **Configuración de administración de cambios**, esto anula el tiempo de instalación programado.

¿Qué paquete debo usar para actualizar cuando la versión actual del software es 9.3.x o superior?

Utilice el paquete de actualización *de un* solo paso para actualizar a cualquier versión superior cuando la versión actual del software 9.3.x o superior.

¿Cuándo se transfieren o ponen en escena 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 Hypervisor, como **SD-WAN —400, 800, 1000, 2000 SE** y sin sistema operativo **SD-WAN - 2100** que se ejecutan con licencia EE recibirán componentes del sistema operativo para actualizar.

¿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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

establece en **1 día** 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 **Actualizar es correcta**.

¿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 Gestión de cambios de** MCN. Para las sucursales de RCN, debe iniciar sesión en el RCN respectivo y establecer los detalles de la programación.

¿Desde dónde puedo obtener el estado de la instalación programada?

El estado de la instalación programada para 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 respectivo 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scheduling Information

Show 100 entries Search: Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries Previous 1 Next

¿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. Desde la versión 9.3 versión 1, la página **Actualizar software del sistema operativo** está depreciada. 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 u obtener STS para ver esta información.

¿Qué diferencia haría si tengo dispositivos sin sistema operativo en mi red? ¿La programación afecta a los dispositivos virtuales o sin sistema operativo?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los dispositivos sin sistema operativo como **SD-WAN: 410,2100,4100,5100 SD-WAN** solo ejecutan software SD-WAN. Los dispositivos sin sistema operativo no necesitan paquetes de componentes del sistema operativo. Estas plataformas se tratan a la par con los dispositivos SD-WAN VPX-SE en términos de necesidad de software. El MCN no transferirá paquetes de componentes del sistema operativo a estos dispositivos. La configuración de la información de programación no surtirá efecto para estos dispositivos, ya que no tienen ningún componente del sistema operativo que necesite actualizar.

¿Cómo funciona SSU en entornos de alta disponibilidad/implementación?

En la implementación de alta disponibilidad en MCN, tenemos una limitación, donde el switch MCN activo o alterna el rol de MCN primario durante la administración de cambios y el MCN Standby/Secondary asume 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 de un solo paso en entornos/implementación de alta disponibilidad?

Mientras se realiza la actualización de un solo paso en la implementación de alta disponibilidad, se activa la función del MCN principal y el MCN en espera. Esto es 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 alternando el rol del MCN activo para que el MCN primario original pueda organizar paquetes de componentes del sistema operativo en las sucursales.

¿Es compatible con la actualización de un solo paso para la implementación sin contacto para reiniciar la correa de los dispositivos?

Sí, se puede usar.

¿Puedo usar la actualización de un solo paso para actualizar mi dispositivo WANOP independiente?

No.

¿Puedo usar la actualización de 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 caja de dos y no el dispositivo autónomo WANOP.

¿Qué paquete debo usar para actualizar a una red de varios niveles?

Utilice el archivo *ns-sdw-sw-<release-version>.zip* del paquete de actualización de un solo paso cuando la versión actual del software sea 9.3.x o superior. 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 bajo el software actual?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A partir de la versión 10.0, se introduce la 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 bajo el software actual. Se lista/visualizar/procesan otros paquetes de dispositivos al pulsar el botón **Verificar** o **Stage Appliance**.

Para dispositivos VPX/VPXL/sin sistema operativo, ¿qué paquetes se organizan para RCN?

El paquete se pone en escena en RCN porque las sucursales RCN pueden ser de cualquier modelo de plataforma. Por lo tanto, necesitan todos los paquetes.

¿Cómo obtiene mi sitio de sucursal detrás del RCN los paquetes de componentes del sistema operativo si RCN es un dispositivo VPX y sucursal es un dispositivo que necesita estos paquetes?

RCN entrega el paquete correspondiente a la sucursal que necesita los paquetes de componentes del sistema operativo después de la activación del paquete de software SD-WAN VW.

¿Puedo elegir Ignorar incompleta durante la puesta en escena y pasar a la siguiente etapa de administración de cambios? ¿Qué impacto tiene para los sitios que no han finalizado la fase intermedia cuando se selecciona este botón?

Sí, puede hacer clic en **Omitir incompleto.** Esto activa el botón **Siguiente** y se muestra la barra de progreso. Esta opción se proporciona para casos en los que el sitio no es accesible y la administración de cambios aún está esperando que se complete la etapa intermedia para esos sitios, de modo que los usuarios pueden pasar a la siguiente etapa ignorando el estado de la etapa y proceder a la activación. Después de que el sitio aparezca, MCN realiza el proceso en etapas del paquete después de la finalización de la activación.

Actualización parcial del software

¿Qué es la actualización parcial del sitio y cómo puedo usarla?

La actualización parcial del software del sitio es una nueva función introducida en la versión 10.0. Puede organizar la versión más reciente de la versión 10.x del MCN y activar la versión de software por etapas desde la página **Administración 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 está 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 habilitando una casilla de verificación en la página **Configuración** > **Configuración de Gestión 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 en el que se puede utilizar una actualización parcial del software del sitio:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Validar si un parche de software con cambios relevantes es compatible y funciona para un sitio específico (donde se realiza la 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.y
- 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 10.x o posterior de software, y se puede utilizar dentro de la misma versión principal del software. Se puede usar entre las versiones 10.0 a 10.0.x/10.x. Solo como parte de la actualización parcial del software del sitio, la configuración no se puede cambiar.

¿Puedo probar una nueva función para probar como parte de la actualización parcial del software habilitándolos desde la configuración?

No, la actualización parcial del software requiere que ahora la configuración activa y en etapas sea idéntica. Solo la versión del software puede cambiar.

¿Puedo desactivar la actualización parcial de software para RCN?

No, la actualización parcial de software solo se puede habilitar o inhabilitar desde MCN. En RCN, la función está en modo de solo lectura.

¿Puedo usar la actualización parcial de software cuando tengo activo como 9.3.x y 10.0.x como caso?

No, el dispositivo debe ejecutarse en la versión 10.0 como software activo.

¿Qué sucede cuando la opción de actualización parcial de software está inhabilitada desde MCN, mientras que algunas sucursales ya están actualizadas a través de esta función?

MCN envía una notificación a todos los dispositivos de la red de que la función Actualización parcial de 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 en etapas desde 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.

Actualización del firmware de LTE

¿Es posible actualizar el firmware LTE a través del paquete SSUP?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A partir de la versión 10.2.6 y 11.0.3, el firmware LTE se puede actualizar a través del paquete SSUP en SD-WAN SE 210 y otras plataformas compatibles con LTE.

Retirada de la administración de cambios

¿Qué es la función de revertir en el proceso de administración de cambios?

A partir de la versión 9.3, la función de reversión de administración de cambios permite volver a la configuración de trabajo cuando eventos inesperados como el bloqueo de la aplicación t2-o el estado de la ruta virtual se vuelven inactivos después de una actualización de configuración - Sí. La red y los dispositivos se supervisan durante 10 minutos después de la actualización de configuración y durante ese intervalo si se cumplen las siguientes condiciones (siempre que el usuario haya habilitado la función), se activará la configuración en etapas. El software activo se vuelve a poner en escena.

¿Cuáles son los criterios para reiniciar la reversión de configuración?

La reversión se produce, si se encuentran los siguientes casos:

1. MCN - Después del cambio de config/software, si el servicio t2_app se inhabilita debido a un bloqueo dentro de un intervalo de 30 min.
2. MCN: Después del cambio de config/software, si el servicio de ruta virtual está inactivo durante 30 minutos o más después de la activación. La función Rollback se inicia en los sitios.
3. Sitio: Después del cambio de config/software, si el Sitio pierde su comunicación con MCN, se inicia la función de reversión.
4. Sitio: Después del cambio de config/software, el servicio t2_app se inhabilita debido a un bloqueo dentro de un intervalo de 30 minutos.

¿Qué sucede después de la reversión?

Después de la reversión de la configuración, la config/software defectuoso se presenta como software en etapas.

¿Cómo se notifica a los usuarios que se produjo la revuelta?

Se muestra un banner amarillo en la parte superior de la GUI que dice que Config se deshace debido a los errores respectivos. Además, puede ver que es la tabla de estado de administración de cambios. Muestra **Error de configuración o error** de **software** correspondiente al sitio para el que se produjo la reversión.

¿Se revierten 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 rollback entonces Software también se deshace.

¿Qué sucede si hay un problema en MCN y se bloquea o pierde la conectividad con todos los sitios?

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Toda la red se deshace excepto MCN. Se muestra la notificación y todos los sitios muestran el estado de retroceso en la sección de administración de cambios. Puede resolver el problema en MCN manualmente.

¿Podemos desactivar esta función?

Sí, podemos desactivar esta función justo antes de la activación. Sin embargo, esta función está habilitada de forma predeterminada.

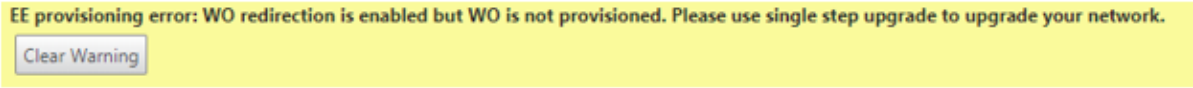
¿Cómo interactúa revertir con la actualización parcial de software cuando tengo una red de varios niveles?

- 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 reversión se propaga hasta el MCN. Como resultado, el MCN y el resto de la red para revertir. Tanto el RCN de la región que se ha revertido como el MCN muestran el banner de rollback que el MCN no puede descartar automáticamente el banner de rollback en el RCN.
- Si la actualización parcial de software está habilitada y si un sitio de una región (o el RCN) retrocede, solo esa región se deshace. El evento rollback no se propaga de nuevo al MCN. Como resultado, el MCN abandona la región. El MCN no muestra el banner de rollback y no retrocede ni a sí mismo ni a la red.

En ambos casos, el RCN muestra el banner de rollback hasta que se descarta. Porque MCN no puede descartarse automáticamente.

Edición 2100 Premium (Enterprise)

¿Qué indica el siguiente mensaje cuando se actualiza un dispositivo 2100 EE a la versión 10.0?



El dispositivo tiene licencia EE o la redirección WANOP está habilitada desde MCN. Puede programar la instalación de componentes de WANOP para iniciar el Provisioning de funciones de WANOP en esta plataforma.

Información relacionada

- Implementación sin contacto a través de LTE
- Configurar el MCN secundario en HA

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Material de referencia

May 7, 2021

Biblioteca de firmas de aplicaciones

Una lista de aplicaciones que los dispositivos Citrix SD-WAN pueden identificar mediante la inspección profunda de paquetes.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).