Citrix SD-WAN WANOP 10.2

Machine translated content

Disclaimer

Contents

Acerca de Citrix SD-WAN WANOP

April 23, 2021

Los dispositivos de Citrix SD-WAN WANOP optimizan sus enlaces WAN, ofreciendo a los usuarios la máxima capacidad de respuesta y rendimiento a cualquier distancia. Un dispositivo Citrix SD-WAN WANOP es fácil de implementar, ya que funciona de forma transparente. Una instalación de veinte minutos acelera el tráfico WAN sin necesidad de otra configuración. No es necesario cambiar sus aplicaciones, servidores, clientes o infraestructura de red. Sin embargo, puede cambiarlos después de la instalación de Citrix SD-WAN WANOP sin que ello afecte a la aceleración del tráfico. Un dispositivo de Citrix SD-WAN WANOP solo necesita reconfiguración cuando cambian los vínculos WAN.

Los dispositivos de Citrix SD-WAN WANOP admiten una amplia gama de optimizaciones, entre las que se incluyen:

- Compresión multisesión con relaciones de compresión de hasta 10, 000:1.
- Aceleración de protocolos para sistemas de archivos de red de Windows (CIFS), aplicaciones virtuales (ICA y CGP, incluido el nuevo estándar*ICA multisesión*), Microsoft Outlook (MAPI) y SSL.
- Conformación del tráfico para garantizar que el tráfico interactivo y de alta prioridad tenga prioridad sobre el tráfico masivo o de baja prioridad.
- Aceleración avanzada del protocolo TCP, que reduce los retrasos en enlaces congestionados o de alta latencia.
- Almacenamiento en caché de vídeo.

¿ Cómo funciona Citrix SD-WAN WANOP?

Los productos de Citrix SD-WAN WANOP funcionan en pares, uno en cada extremo de un enlace, para acelerar el tráfico a través del enlace. Las transformaciones realizadas por el remitente son invertidas por el receptor.

Sin embargo, un dispositivo (o dispositivo virtual) puede manejar muchos vínculos, por lo que no es necesario dedicar un par a cada conexión.

Una empresa suele tener un dispositivo WANOP Citrix SD-WAN por sitio (dispositivos más grandes en sitios más grandes, otros más pequeños en sitios más pequeños), aunque una empresa con numerosas sucursales puede tener varios dispositivos en su centro de datos central.

Un vínculo desde un sitio con un dispositivo Citrix SD-WAN WANOP a un sitio que no tiene un dispositivo Citrix
SD-WAN WANOP funciona normalmente, pero su tráfico no se acelera.

Las características de Citrix SD-WAN WANOP incluyen compresión robusta para un rendimiento rápido en enlaces relativamente lentos y control de flujo sin pérdidas para hacer frente a la con-

gestión. Las optimizaciones TCP superan las principales limitaciones de los enlaces problemáticos, y la optimización de aplicaciones hace desaparecer las limitaciones de las aplicaciones diseñadas para redes locales de alta velocidad. Una función de detección automática hace que la implementación sea rápida y sencilla.

Características y ventajas de Citrix SD-WAN WANOP

El tiempo que los trabajadores pasan esperando a que sus equipos respondan, por pequeño que sea, es tiempo perdido, lo que resulta en una pérdida de productividad. Cuando los usuarios trabajan de forma remota o utilizan recursos externos, su productividad depende de la capacidad de respuesta de sus conexiones de red. La protección de la capacidad de respuesta de sus conexiones requiere una aceleración avanzada de la red.

La línea de productos Citrix SD-WAN WANOP protege su productividad al proporcionar un rendimiento fiable de conexión WAN e Internet a través de un conjunto de múltiples optimizaciones entrelazadas, cada una de las cuales refuerza las demás. Para ofrecer la máxima productividad en toda su empresa, existen productos Citrix SD-WAN WANOP para cada necesidad, desde el centro de datos más grande, hasta la sucursal más pequeña e incluso el portátil individual.

Citrix SD-WAN WANOP proporciona una usabilidad sólida incluso con enlaces de tamaño insuficiente o degradados.

Funciones desglosadas:

Para obtener más información, consulte la table.

Características y beneficios:

Las siguientes son algunas de las ventajas clave de nuestra línea de productos Citrix SD-WAN WANOP.

La**compresión supera las bajas velocidades de enlace**.El problema más obvio con los enlaces de red de área amplia (WAN) y los enlaces a Internet es su bajo ancho de banda en comparación con las redes de área local (LAN). Una WAN de 1 Mbps tiene solo el 1% del rendimiento de una LAN de 100 Mbps. ¿Cómo se supera el bajo ancho de banda de enlace? Con compresión. Una relación de compresión de 100:1 permite que un enlace de 1 Mbps transfiera datos tan rápido como 100 Mbps. Este factor de aceleración se logra siempre que se cumplan los siguientes criterios:

- El algoritmo de compresión debe ser capaz de ofrecer altas relaciones de compresión.
- El algoritmo de compresión debe ser muy rápido (mucho más rápido que el ancho de banda del enlace, e idealmente tan rápido como la LAN).
- Los segmentos LAN del enlace deben tener un control de flujo independiente del segmento WAN, ya que los diferentes segmentos manejan datos a diferentes velocidades.

- Se deben utilizar varios motores de compresión para manejar las diferentes necesidades de los diferentes tipos de tráfico. El tráfico interactivo requiere relativamente poco ancho de banda, pero es muy sensible al retraso, mientras que las transferencias en masa son muy sensibles al ancho de banda pero son insensibles al retraso.

La aceleración del protocolo TCP supera la congestión.Cualquier intento de enviar tráfico más rápido que la velocidad del enlace produce congestión, lo que da lugar a muchos problemas causados por altas pérdidas de paquetes y alta latencia en cola.

Control de flujo sin pérdida. El protocolo TCP/IP no tiene control de flujo para ralentizar a los remitentes directamente, y la ausencia de este mecanismo de control necesario hace que las pérdidas de paquetes y los retrasos excesivos en la cola sean normales, incluso en enlaces de misión crítica. (En todo caso, este problema está empeorando con el tiempo, como lo atestiguan los documentos sobre el fenómeno de **saturación de búferes**.)

Un dispositivo Citrix SD-WAN WANOP resuelve este problema proporcionando el control de flujo omitido en el protocolo TCP/IP. A diferencia de las soluciones de calidad de servicio (QoS) ordinarias, que simplemente reasignan la pérdida de paquetes, Citrix SD-WAN WANOP proporciona un control de flujo sin pérdidas que controla la velocidad a la que los remitentes de punto final transmiten datos, en lugar de permitir que los remitentes transmitan datos a la velocidad que quieran y descartan paquetes cuando envían Demasiado. Cada remitente transmite sólo tantos datos como Citrix SD-WAN WANOP le permite enviar, sin dejar caer un paquete, y estos datos se colocan en el enlace exactamente a la velocidad correcta para mantener el enlace lleno sin desbordarse. Al eliminar el exceso de datos, Citrix SD-WAN WANOP no se ve obligado a descartarlos. Sin Citrix SD-WAN WANOP, los paquetes descartados deben enviarse de nuevo, lo que provoca retrasos innecesarios. El control de flujo sin pérdidas también elimina los retrasos causados por el exceso de almacenamiento en búfer. El control de flujo sin pérdidas es la clave para la máxima capacidad de respuesta en un enlace ocupado, lo que permite que un enlace que una vez estuvo congestionado hasta el punto de no usabilidad en un 40% de utilización siga siendo productivo y receptivo con una utilización del 95%.

Eliminar la injusticia basada en la distancia. Los enlaces con alta latencia o pérdidas de paquetes son difíciles de usar con ancho de banda completo, especialmente con variantes TCP ordinarias como TCP Reno. Las consecuencias son retrasos excesivos y dificultad para obtener el ancho de banda que está pagando. Cuanto más larga sea la distancia del enlace, peor será el problema.

La aceleración del protocolo TCP WANOP de Citrix SD-WAN minimiza estos efectos, permitiendo que los enlaces intercontinentales e incluso por satélite funcionen a toda velocidad.

El modelado del tráfico administra el ancho de banda automáticamente.En el lado de salida, un algoritmo similar a la cola justa garantiza que cada conexión esté en cola de forma independiente y dada su parte justa del ancho de banda del enlace. Las directivas de modelado de tráfico permiten que diferentes servicios tengan una precedencia mayor o menor. Las optimizaciones de aplicaciones superan las limitaciones de diseño

Las aplicaciones y protocolos diseñados para su uso en redes de área local son notorios por el bajo rendimiento en redes de área amplia, porque los diseñadores no tuvieron en cuenta los efectos de los largos retrasos en la velocidad de la luz en sus protocolos. Por ejemplo, una operación simple de sistema de archivos de Windows (CIFS) puede tardar hasta 50 viajes de ida y vuelta a medida que los mensajes pasan por la red. En una red de área amplia con un tiempo de ida y vuelta de 100 ms, 50 viajes de ida y vuelta causan un retraso de cinco segundos.

Aunque los retrasos en la velocidad de la luz son una limitación fundamental, las optimizaciones de aplicaciones pueden realizar las mismas operaciones en un número menor de viajes de ida y vuelta, generalmente a través de operaciones especulativas. Cuando la aplicación original emitiera un comando a la vez y esperara a que se completara antes de emitir el siguiente, a menudo es perfectamente seguro emitir una serie de comandos sin esperar. Además, las transferencias de datos se pueden acelerar mediante una combinación de operaciones de recuperación previa, lectura anticipada y escritura detrás. Al empaquetar tantas operaciones como sea posible en un solo viaje de ida y vuelta, el rendimiento se puede multiplicar por diez o más.

Las optimizaciones WANOP de Citrix SD-WAN son especialmente efectivas en CIFS/SMB (el sistema de archivos Windows), MAPI (protocolo Outlook/Exchange) y HTTP.

Las múltiples optimizaciones mejoran el rendimiento de Virtual Apps/Virtual Desktops (Citrix HDX). Dado que los dispositivos Citrix SD-WAN WANOP son productos Citrix, son especialmente eficaces para acelerar los protocolos Citrix, como Citrix Virtual Apps and Desktops. Todos los aspectos de la aceleración WANOP de Citrix SD-WAN entran en juego con estos protocolos para que la experiencia del usuario remoto sea lo más productiva posible.

Los dispositivos Citrix SD-WAN WANOP negocian las opciones de sesión con los servidores Citrix Virtual Apps and Desktops. Esto permite que el dispositivo Citrix SD-WAN WANOP aplique las siguientes mejoras:

- Reemplaza la compresión nativa del servidor por compresión de Citrix SD-WAN WANOP de mayor rendimiento.
- Basa la prioridad de modelado de tráfico de la conexión en los bits de prioridad incrustados en cada conexión de Citrix Virtual Apps and Desktops. Esto permite que la prioridad de la conexión varíe según el tipo de tráfico. Por ejemplo, las tareas interactivas son tareas de alta prioridad y los trabajos de impresión son tareas de baja prioridad.
- Recopila e informa estadísticas basadas en las aplicaciones de Virtual Apps o Virtual Desktops que se utilizan.
- Mantiene el cifrado de extremo a extremo de la conexión original.

Detección automática para una configuración mínima.Dado que la solución es de doble extremo, lo que requiere que un producto Citrix SD-WAN WANOP esté presente en ambos extremos del enlace, la implementación parece imponer una carga a las oficinas remotas, especialmente a las que carecen

de personal de TI dedicado. Sin embargo, Citrix SD-WAN WANOP está diseñado para ser muy fácil de instalar y mantener. Una instalación típica tarda unos veinte minutos. Los únicos parámetros necesarios son los parámetros de red habituales (como la dirección IP y la máscara de subred), la dirección de un servidor de licencias Citrix y la velocidad de envío y recepción del vínculo.

Es posible requerir solo un nivel mínimo de configuración debido a la detección automática, a través de la cual un Citrix SD-WAN WANOP determina qué conexiones se pueden acelerar (y cuáles no), sin ninguna configuración manual. Se detecta automáticamente un WANOP de Citrix SD-WAN en el otro extremo del enlace y, a continuación, se acelera la conexión. Puede agregar dispositivos WANOP Citrix SD-WAN a su red de forma ad hoc. Ni siquiera tiene que informar a los dispositivos existentes de la llegada de uno nuevo. Lo descubren por sí mismos.

Un Citrix SD-WAN WANOP utiliza opciones de encabezado TCP para informar de su presencia y negociar parámetros de aceleración con el Citrix SD-WAN WANOP remoto porque las opciones de encabezado TCP forman parte del estándar TCP, este método funciona muy bien, excepto en los casos en que los firewalls están programados para rechazar todos excepto los más comunes opciones. Estos cortafuegos existen, pero se pueden configurar para permitir el paso de las opciones utilizadas por Citrix SD-WAN WANOP.

Las operaciones WANOP de Citrix SD-WAN son transparentes tanto para el remitente como para el receptor. Los demás dispositivos de la red no saben que Citrix SD-WAN WANOP
existe. Siguen trabajando igual que antes de la instalación de Citrix SD-WAN WANOP. Esta transparencia también elimina cualquier necesidad de instalar software especial en sus servidores o clientes para beneficiarse de la aceleración de Citrix SD-WAN WANOP. Todo funciona de forma transparente.

Capacidades de la línea de productos:

Todos los productos de la línea de productos WANOP de Citrix SD-WAN ofrecen funciones básicas de aceleración WANOP de Citrix SD-WAN. La mayoría de los modelos también tienen funciones adicionales, tales como:

- Almacenamiento en caché de vídeo
- Múltiples puentes acelerados con función de bypass Ethernet
- Supervisión y administración a través de GUI, CLI, SNMP, AppFlow y Citrix ADM.

Los diferentes productos Citrix SD-WAN WANOP tienen diferentes capacidades. Los productos que admiten anchos de banda WAN más altos también admiten más usuarios y, por lo general, disponen de más recursos: CPU más potencia, memoria, disco más grande y puentes más acelerados.

Las capacidades de los productos que se ejecutan en su propio hardware, como Citrix SD-WAN WANOP Plug-in y Citrix SD-WAN WANOP VPX, dependen de la velocidad del hardware y de la cantidad de recursos del sistema que dedique a la aceleración.

Para obtener especificaciones actualizadas, consulte Citrix Hoja de datos del producto SD-WAN.

Arquitectura de Citrix SD-WAN WANOP

Los dispositivos de Citrix SD-WAN WANOP aceleran el tráfico a través de sus enlaces WAN. Para acelerar una WAN, necesita al menos dos dispositivos Citrix SD-WAN WANOP, uno por cada sitio que desee acelerar.

El dispositivo Citrix SD-WAN WANOP del lado del remitente aplica una serie de optimizaciones y transformaciones al tráfico, como compresión y cifrado. Muchas operaciones requieren que el Citrix SD-WAN WANOP del lado del receptor realice una operación inversa, como la descompresión o el descifrado, para restaurar el tráfico a su estado original.

Por lo tanto, la mayoría de las optimizaciones requieren que el tráfico pase a través de dos dispositivos Citrix SD-WAN WANOP. Algunas optimizaciones son de extremo único y las realiza el dispositivo local actuando solo. Estas optimizaciones incluyen el modelado del tráfico y el almacenamiento en caché de vídeo.

Los dispositivos Citrix SD-WAN WANOP son en gran medida transparentes para la red. El dispositivo parece ser un puente, no un enrutador, una Gateway o un proxy. Esta invisibilidad permite que el dispositivo se instale sin configurar ningún otro hardware. Las optimizaciones del dispositivo también son transparentes y solo las detecta el dispositivo asociado en el otro extremo del vínculo.

Los dispositivos de Citrix SD-WAN WANOP se pueden agregar a la red a voluntad, ya que sus funciones de detección automática y negociación automática garantizan que otros dispositivos detecten inmediatamente un nuevo dispositivo en la red y que la aceleración comience a la vez.

Aunque el diagrama anterior muestra una red con solo dos dispositivos, un único dispositivo Citrix SD-WAN WANOP puede comunicarse con cualquier número de sitios asociados. Se admiten redes punto a punto, radial y radial y redes de malla.

Además de los dispositivos independientes, los productos de aceleración WANOP de Citrix SD-WAN incluyen máquinas virtuales (la serie Citrix SD-WAN WANOP VPX) y un servicio de aceleración instalable para sistemas Windows (el complemento Citrix SD-WAN WANOP).

Qué significa aceleración

En la terminología WANOP de Citrix SD-WAN, la «aceleración» es la reducción del tiempo de transacción, lo que reduce el tiempo que los usuarios pasan esperando. Dado que el tiempo que los usuarios pasan esperando representa una pérdida directa de productividad, el principal beneficio de la aceleración es el aumento de la productividad.

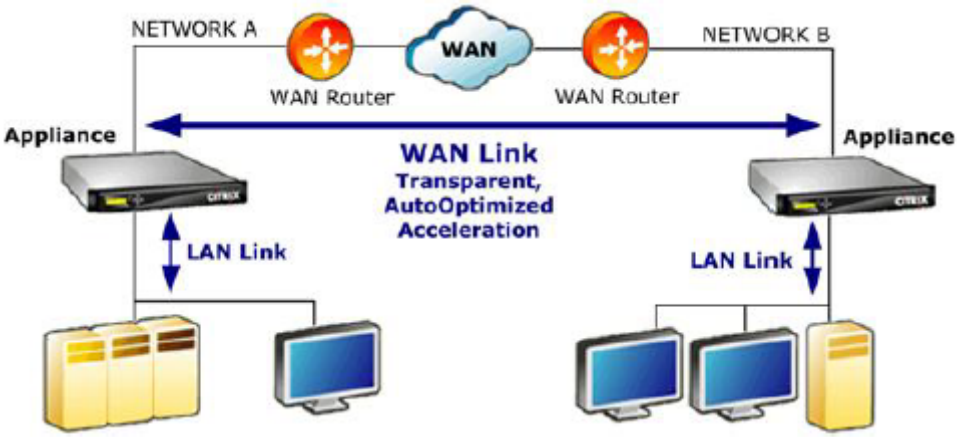
En el tráfico de red, una transacción varía desde muy pequeña (un solo byte de datos en una sesión de terminal telnet o SSH) hasta muy grande, como ocurre con las transferencias FTP, que a menudo superan un gigabyte de tamaño. Un acelerador práctico tiene que acelerar toda la gama de tamaños de transacción, desde el tráfico interactivo hasta el tráfico masivo, proporcionando el mejor rendimiento

y experiencia de usuario en todos los ámbitos.La tecnología WANOP de Citrix SD-WAN logra esto de diversas maneras.

Cómo funciona la aceleración: El proceso

Para ver cómo funciona el dispositivo Citrix SD-WAN WANOP, eche un vistazo de cerca al diagrama de la canalización de flujo de tráfico. Como puede ver, hay dos procesos:

1. El proceso de envío, que acelera la entrada de datos a la WAN desde la LAN local.
2. El proceso de recepción, que acelera la salida de los datos de la WAN y la entrada de la LAN local.



Proceso de envío

Para comprender el dispositivo, considere el proceso de envío para cada unidad.

1. Búfer de entrada. El dispositivo recibe paquetes de la LAN. Dado que el conformador de tráfico no TCP/IP solo optimiza el tráfico, los paquetes que no son TCP se desvían directamente al conformador de tráfico. El tráfico TCP/IP (llamado tráfico TCP a partir de ahora) atraviesa el resto del proceso.
2. Caché de vídeo. Si el tráfico TCP coincide con la configuración de la caché de vídeo, la solicitud se traspasa a la unidad de caché de vídeo.
3. Detección automática del lado de la LAN. Aparte del modelado del tráfico, las optimizaciones del lado del remitente requieren que haya un dispositivo remoto así como el dispositivo local. Cualquier conexión que no pase a través de un dispositivo remoto se desvía al formador de tráfico. Esta acción se realiza mediante la lógica de detección automática del lado LAN. La prueba real de un dispositivo remoto se realiza mediante la unidad de detección automática del lado WAN.

4. Control de flujo en el lado de LAN.Citrix SD-WAN WANOP actúa como un proxy TCP transparente, recibiendo y reconociendo paquetes del remitente del punto final en nombre del receptor del punto final. Esto permite que el dispositivo acepte grandes cantidades de datos del remitente local muy rápidamente, a velocidades de LAN completas, independientemente de la lentitud con que el tráfico se mueva a través de la WAN. (TCP normal utiliza un control de velocidad de extremo a extremo, que no es lo suficientemente ágil como para permitir el máximo rendimiento). Además, el control de flujo WANOP de Citrix SD-WAN no tiene pérdidas, lo que significa que el remitente local nunca ve un paquete perdido, lo que aumenta la fiabilidad y la eficiencia.
5. Motores de aplicaciones. Citrix SD-WAN WANOP realiza optimizaciones específicas para varios protocolos, entre ellos:
   - Citrix Virtual Apps and Desktops, mediante los protocolos ICA y CGP.
   - Sistema de archivos de Windows (CIFS, incluidas las versiones SMB1 y SMB2)
   - Outlook/Exchange (MAPI)

     Estas optimizaciones reducen el tiempo de transacción. Esto se hace mediante la reescritura, la combinación y el reordenamiento de comandos, mediante lectura anticipada y escritura detrás, mediante un conocimiento del protocolo para un modelado de tráfico más avanzado y sugerencias de compresión.
6. Motor de compresión. La compresión hace que las transacciones sean más pequeñas, lo que reduce el tiempo que se tarda en transferir los datos a través del enlace. El compresor de Citrix SD-WAN WANOP utiliza varios algoritmos de compresión, algunos muy eficientes para transacciones pequeñas, otros optimizados para transacciones masivas y otros para transacciones de tamaño mediano. El compresor Citrix SD-WAN WANOP logra fácilmente relaciones de compresión de 10, 000:1. El compresor es muy rápido, lo que permite mantener altas relaciones de compresión a velocidades WAN completas. Con el procesamiento WANOP de Citrix SD-WAN, un archivo que se comprime a una proporción de 100:1 se puede enviar fácilmente a través de un enlace de 1 Mbps con un rendimiento total de 100 Mbps.
7. Motor de seguridad. Algunas características de Citrix SD-WAN WANOP requieren que los dos dispositivos introduzcan una relación de pares segura entre sí y con el servidor de origen. El motor de seguridad autentica esta relación entre pares y cifra las conexiones de datos aceleradas entre ellos. Una relación de pares segura permite el uso de compresión SSL y la aceleración del tráfico cifrado de Virtual Apps/Virtual Desktops (ICA/CGP), sistema de archivos de Windows (CIFS) y Outlook/Exchange (MAPI).
8. Control de flujo en el lado WAN y detección automática. El enlace WAN es donde se producen desaceleraciones de tráfico y, si el enlace está congestionado, los paquetes se pierden y deben retransmitirse. La retransmisión de paquetes siempre provoca un retraso significativo, que a veces dura más de un segundo. La unidad de control de flujo del lado WAN utiliza elementos de

retransmisión avanzados y un protocolo TCP/IP avanzado para obtener el máximo rendimiento en enlaces limpios y problemáticos. La unidad de detección automática identifica la presencia de una unidad WANOP de Citrix SD-WAN asociada en función de conexión por conexión, lo que evita que se utilicen optimizaciones donde no se desean y permite que los dispositivos nuevos sean detectados por los existentes tan pronto como se añaden a la red. La detección automática utiliza opciones en el campo de encabezado TCP. Normalmente, esto es transparente, pero puede ser bloqueado por algunos firewalls, que necesitan ser reconfigurados.

9. Clasificador de aplicaciones. Esta unidad examina todo el tráfico que fluye a través de Citrix SD-WAN WANOP e identifica a qué aplicación o protocolo pertenece. Esta información se utiliza en la elaboración de informes y por el formador de tráfico.
10. Moldeador de tráfico. Para evitar congestión, colas excesivas y otras fuentes de retrasos evitables, el formador de tráfico inyecta tráfico en la WAN a una velocidad ligeramente inferior a la velocidad de datos de la WAN, para garantizar que la WAN nunca se invade. Se utiliza un algoritmo de cola justa ponderada para garantizar que todo el tráfico obtenga su parte justa del ancho de banda del enlace. Las directivas de modelado de tráfico permiten que los diferentes tipos de tráfico reciban diferentes pesos, de modo que algunos de ellos obtienen más ancho de banda que otros.

Proceso de recepción

El proceso en la dirección de recepción es similar a la dirección de envío, excepto que, en lugar de cifrar, descifra, y, en lugar de comprimir, descomprime. Además, tenga en cuenta que también hay un conformador de tráfico en la dirección de recepción, que aplica directivas de modelado de tráfico al tráfico WAN entrante, de modo que ambas direcciones estén reguladas.

Detección automática y transformación a nivel de paquete

El algoritmo de detección automática inserta opciones de encabezado TCP para anunciar la presencia de un dispositivo Citrix SD-WAN WANOP y facilitar la negociación. Estas opciones están en el rango de 24-31. Se utilizan las siguientes transformaciones de nivel de paquete:

- En el paquete inicial de la conexión (el paquete SYN), el dispositivo de envío adjunta opciones de encabezado identificándose como un dispositivo Citrix SD-WAN WANOP y también declara otras capacidades, como la compresión. Esto se llama un paquete SYN etiquetado.
- Al recibir un paquete SYN etiquetado, el dispositivo receptor adjunta opciones de encabezado al paquete SYN-ACK, identificándose a sí mismo a su vez y anunciando sus capacidades.
- Una vez que el dispositivo de envío recibe el paquete SYN-ACK etiquetado, la conexión se puede acelerar según las capacidades compartidas por ambos dispositivos. Por ejemplo, la conexión se comprime si ambos dispositivos declaran soporte para compresión.

- Los números de secuencia inicial (ISN) de TCP en ambas direcciones se alteran agregando 2.000.000.000 a los valores originales. Se trata de una precaución que impide que la conexión continúe si un dispositivo falla o tiene un cambio de enrutamiento que le impide ver todo el tráfico de la conexión. Una vez que una conexión se acelera, debe permanecer acelerada durante toda su vida útil.
- El valor de MSS se reduce, normalmente a 1380 bytes, para garantizar que cada paquete tenga espacio para las opciones de encabezado TCP WANOP WANOP insertadas de Citrix SD-WAN.
- Las direcciones IP y los números de puerto de la conexión permanecen sin cambios.

Acuse de recibo previo

Los paquetes SYN y SYN-ACK fluyen de extremo a extremo:

- El paquete SYN fluye desde el cliente de extremo, a través del dispositivo del lado del cliente, a través de la WAN, a través del dispositivo del lado del servidor y, finalmente, al servidor.
- El paquete SYN-ACK fluye desde el servidor, a través del dispositivo del lado del servidor, a través de la WAN, a través del dispositivo del lado del cliente y, finalmente, al cliente.

Lo mismo ocurre con los paquetes finales de la conexión, los paquetes FIN, FIN-ACK y RST.

Sin embargo, otros paquetes son confirmados previamente. Por ejemplo, cuando el dispositivo del lado del servidor recibe un paquete del servidor, lo reconoce a través de la LAN de inmediato y lo almacena en búfer para su posible transmisión a través de la WAN. Esto permite que los búferes del dispositivo del lado del servidor se llenen muy rápidamente, por lo que siempre tiene muchos datos que usar para la compresión y otras optimizaciones. (Esto es muy diferente de la operación TCP normal, donde todas las confirmaciones provienen del lado opuesto de la WAN, lo que hace que el reconocimiento sea muy lento y obliga a cada segmento de la conexión a moverse no más rápido que el segmento más lento, lo que reduce en gran medida la efectividad de la aceleración).

Mover tráfico dentro y fuera del dispositivo

Los dispositivos Citrix SD-WAN WANOP tienen una serie de «modos de reenvío». Un modo de reenvío es un método para obtener tráfico de entrada y salida del dispositivo. El más común es el modo en línea, donde Citrix SD-WAN WANOP parece ser un dispositivo puente. Los paquetes que entran en un puerto de puente parecen salir del otro. Por supuesto, Citrix SD-WAN WANOP transforma los datos de diversas maneras, por lo que en muchos casos el paquete que sale del segundo puerto no es idéntico al que entró en el primer puerto, pero así es como parece al resto de la red.

Cuando el modo en línea no es práctico, hay varios otros métodos disponibles, sobre todo el modo WCCP. Estos son modos de un brazo, mediante un solo cable de interfaz.

> **Sugerencia**
>
> Puede administrar y supervisar sus dispositivos Citrix SD-WAN WANOP mediante Citrix ADM. Para obtener más información, consulte Administración de instancias de Citrix SD-WAN mediante Citrix ADM

Introducción a Citrix SD-WAN WANOP

April 23, 2021

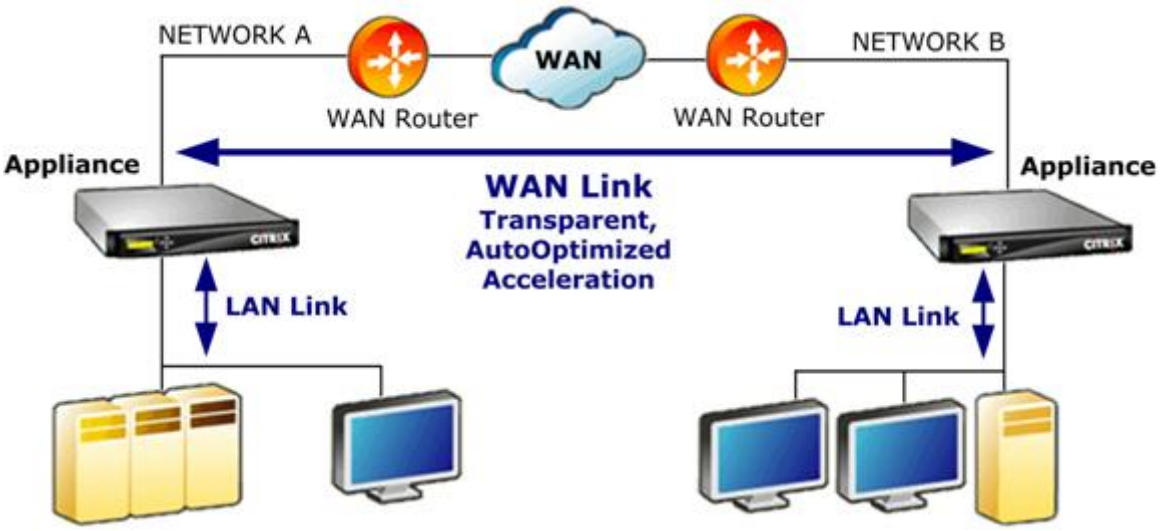
Implementar correctamente los dispositivos WANOP de Citrix SD-WAN no es difícil, pero las implementaciones incorrectas pueden causar problemas y proporcionar una aceleración inadecuada. Asegúrese de seleccionar dispositivos con capacidad suficiente para los vínculos que desea que aceleren. La selección de productos también es uno de los factores a tener en cuenta a la hora de decidir la mejor forma de encajar los dispositivos en su topología.

Los criterios de implementación más básicos son:

- Todos los paquetes de la conexión TCP deben pasar a través de una combinación compatible de dos *unidades de aceleración* (dispositivos Citrix SD-WAN WANOP o plug-ins).
- El tráfico debe atravesar las dos unidades de aceleración en ambas direcciones.

Cuando se cumplen estos criterios, la aceleración es automática.

La aceleración mejora el rendimiento cuando el tráfico pasa a través de dos dispositivos



Para los sitios con una sola red WAN, estos criterios se pueden cumplir colocando el dispositivo Citrix SD-WAN WANOP en línea con la WAN. En sitios más complejos, hay otras opciones disponibles. Algunos, como el soporte WCCP, están disponibles en todos los modelos. Otros solo están disponibles

en algunos modelos. Por lo tanto, las necesidades de un sitio más complejo podrían limitar su elección de dispositivos.

Al evaluar las opciones, tenga en cuenta la importancia de mantener varios segmentos de la red en funcionamiento en caso de que un dispositivo falle o tenga que inhabilitarse. Para implementaciones en línea, Citrix recomienda una *tarjeta de derivación Ethernet*. Esta tarjeta, que es opcional en los dispositivos Citrix SD-WAN WANOP, tiene un relé que se cierra si falla el dispositivo, lo que permite que los paquetes pasen incluso si se pierde o extrae la energía.

La redundancia es una consideración para todos los tipos de implementaciones.Los dispositivos Citrix SD-WAN WANOP ofrecen diferentes tipos de redundancia:

- Los dispositivos SD-WAN WANOP 4000/5000 tienen dos fuentes de alimentación.
- Los dispositivos SD-WAN WANOP 4000/5000 tienen unidades de disco redundantes.
- Los dispositivos se pueden utilizar en modo de alta disponibilidad (dos dispositivos redundantes con conmutación por error automática). Este modo es compatible con todos los modelos.

> **Nota**
>
> Para obtener más información sobre los dispositivos Citrix SD-WAN WANOP y los modos de implementación, consulte la Documentación de la plataforma SD-WAN WANOP

Seleccionar un dispositivo en función de la capacidad

April 23, 2021

Para un funcionamiento adecuado, el dispositivo Citrix SD-WAN WANOP debe tener los recursos adecuados para admitir el número de vínculos WAN que desea acelerar y para admitir a todos los usuarios de dichos vínculos. Al seleccionar un
dispositivo Citrix SD-WAN WANOP, son importantes tres capacidades: capacidad de enlace (ancho de banda), capacidad del usuario y capacidad de disco.

Capacidad de enlace

Al seleccionar un dispositivo Citrix SD-WAN WANOP, el factor más importante es que admita los vínculos WAN. Si el sitio tiene un único vínculo WAN, el dispositivo debe admitir la velocidad de enlace. Por ejemplo, un Citrix SD-WAN WANOP 2000-010 puede admitir enlaces de hasta 10 Mbps, lo que sería adecuado para un enlace de 8 Mbps pero no para un enlace de 12 Mbps. Si el sitio tiene varios vínculos

que se van a acelerar con un único dispositivo, el dispositivo debe admitir la velocidad total de todos estos vínculos WAN agregados.

La velocidad máxima admitida viene determinada por una combinación del hardware del dispositivo y la licencia del producto. El límite de ancho de banda con licencia es la velocidad de enlace máxima que admite la licencia.

Producto	Gama WAN BW con licencia.
Productos actuales	
Plug-in WANOP SD-WAN	N/D
SD-WAN WANOP 400	2-6 Mbps
SD-WAN WANOP 800	2-10 Mbps
SD-WAN WANOP 2000, 2000WS	10-50 Mbps
SD-WAN WANOP 3000 NEGRO	5 0-155
SD-WAN WANOP 4000	310-1.000 Mbps
SD-WAN WANOP 5000	1.500-2,000 Mbps
SD-WAN WANOP VPX	1-45 Mbps

Cuadro 1 Límites de ancho de banda con licencia por línea de productos

Capacidad de usuarios de Virtual Apps/Virtual Desktops

Cada dispositivo se clasifica para un número máximo de usuarios de XenApp o Virtual Desktops. Este valor no debe superarse cuando la implementación utiliza Virtual Apps o Virtual Desktops. Si no está utilizando Virtual Apps o Virtual Desktops, considere que este número es una guía aproximada para el número de usuarios de otras aplicaciones.

Producto	Número máximo de usuarios
Plug-in WANOP SD-WAN	1
SD-WAN WANOP 400	10-30
SD-WAN WANOP 800	20-100
SD-WAN WANOP 2000, 2000WS	100-300
SD-WAN WANOP 3000 NEGRO	300-500
SD-WAN WANOP VPX	20-350

Producto	Número máximo de usuarios
SD-WAN WANOP 4000	750-2,500
SD-WAN WANOP 5000	3,500-5,000

Tabla 2. Capacidad de usuarios de Virtual Apps/Virtual Desktops

Tamaño del disco

El espacio en disco se utiliza principalmente para el historial de compresión, y más espacio en disco da como resultado un mayor rendimiento de compresión.

La serie SD-WAN WANOP 4000/5000 ofrece entre 1,8 TB y 2,4 TB de capacidad de disco. Esto se compara con 2,1 TB para la WANOP 3000 SD-WAN, 470 GB para la WANOP 2000, 80 GB para la SD-WAN WANOP 800 y 40 GB para la SD-WAN WANOP 400. SD-WAN WANOP VPX tiene una capacidad de disco de 100-500 GB. Idealmente, un dispositivo debería tener una capacidad de disco mayor que el tiempo de ciclo de los datos del vínculo. Por ejemplo, un enlace que transporta principalmente tráfico de actualización diario debería tener 24 horas de capacidad de disco o más. Con un enlace que lleva principalmente sesiones de usuario, esta ventana puede ser más pequeña. (Un enlace de 1 Mbps puede transferir unos 10 GB por día a toda velocidad).

Tabla 3. Ejemplos de vida útil de datos para tamaños de disco

Modelo de dispositivo	Velocidad de enlace 1 Mbps	Velocidad de enlace: 10 Mbps	Velocidad de enlace: 100 Mbps	Velocidad de enlace: 1000 Mbps
Vida útil de los datos al 33% de utilización de enlaces				
SD-WAN WANOP 800	23 días	2.3 días	n/d	n/d
SD-WAN WANOP 2000, 2000WS	141 días	14 días	n/d	n/d
SD-WAN WANOP 5000	717 días	72 días	7,2 días	17 horas

Modelo de dispositivo	Velocidad de enlace 1 Mbps	Velocidad de enlace: 10 Mbps	Velocidad de enlace: 100 Mbps	Velocidad de enlace: 1000 Mbps
Vida útil de los datos al 100% de utilización de enlaces				
SD-WAN WANOP 800	8 días	19 horas	n/d	n/d
SD-WAN WANOP 2000, 2000WS	47 días	4.7 días	n/d	n/d
SD-WAN WANOP 5000	239 días	24 días	2,4 días	6 horas

Seleccionar el modo de implementación basado en la topología del centro de datos

April 23, 2021

El dispositivo se puede colocar en línea con el vínculo WAN. El dispositivo utiliza dos puertos Ethernet en puente para el modo en línea. Los paquetes entran en un puerto Ethernet y salen por el otro. Este modo coloca el dispositivo entre el router WAN y la LAN. Para el resto de la red, es como si el dispositivo no estuviera allí en absoluto. Su funcionamiento es completamente transparente.

El modo en línea tiene las siguientes ventajas sobre los otros modos de implementación:

- Máximo rendimiento.
- Configuración muy sencilla, mediante solo la página Instalación rápida.
- No hay reconfiguración de su otro equipo de red.

Otros modos (WCCP, línea virtual, redirector) son menos convenientes de configurar, generalmente requieren que reconfigure el router y tienen un rendimiento algo menor.

Una consideración básica de implementación es si su sitio tiene un único enrutador WAN o varios enrutadores WAN. También debe pensar en qué entidades se pueden usar en qué modos. Un requisito para admitir VPNs afecta a la ubicación del dispositivo en la red.

Los dispositivos Access Gateway admiten optimizaciones de Citrix SD-WAN WANOP TCP, permitiendo conexiones VPN aceleradas cuando los dispositivos Citrix SD-WAN WANOP se implementan con Access Gateway.

Descripción general de los modos de implementación

El dispositivo se puede implementar en los siguientes modos:

Modos de reenvío

- **Modo en línea**: el modo más transparente y de mayor rendimiento. Los datos entran en un puerto Ethernet acelerado y salen en el otro. No requiere ninguna reconfiguración del router de ningún tipo.
- **En línea con puentes dobles**: igual que en línea, pero con dos puentes acelerados independientes.
- **Modo WCCP**: se recomienda cuando el modo en línea no es práctico. Compatible con la mayoría de los routers. Requiere solo tres líneas de configuración del router. Para utilizar el modo WCCP en un router Cisco, el router debe estar ejecutando al menos la versión 12.0(11)S or 12.1(3)T de IOS. (WCCP significa Web Cache Communications Protocol, pero el protocolo se expandió en gran medida con la versión 2.0 para admitir una amplia variedad de dispositivos de red).
- **Modo virtual en línea**: similar al modo WCCP. Utiliza enrutamiento basado en directivas. Por lo general, requiere un puerto LAN dedicado en el router. No se recomienda en unidades sin una tarjeta de derivación Ethernet. Para utilizar el modo virtual en línea en un router Cisco, el router debe estar ejecutando IOS versión 12.3 (4) T o posterior.
- **Modo de grupo**: se utiliza con dos o más dispositivos en línea, uno por vínculo, dentro de un sitio. Se recomienda solo cuando múltiples puentes, WCCP y modos en línea virtuales no son prácticos.
- **Modo de alta disponibilidad**: combina de forma transparente dos dispositivos en línea o virtuales en un par primario y secundario. El dispositivo principal controla todo el tráfico. Si falla, el dispositivo secundario se hace cargo. No requiere configuración de enrutador. Requiere un dispositivo con una tarjeta de derivación Ethernet.
- **Modo transparente**: el modo recomendado para la comunicación con el complemento WANOP de Citrix SD-WAN. En modo transparente, el complemento inicia las conexiones esencialmente de la misma manera que el dispositivo Citrix SD-WAN WANOP, manteniendo la dirección IP y el número de puerto originales de la conexión y agregando las opciones de Citrix SD-WAN WANOP a los encabezados TCP/IP de los paquetes seleccionados. Por el contrario, en el modo de redi-

rector (no recomendado), el complemento altera la IP de destino y los números de puerto de los paquetes para que coincidan con la IP de señalización (y el puerto) del dispositivo.

- **Modo de redirector** (no recomendado): utilizado por Citrix SD-WAN WANOP Plug-in para reenviar tráfico al dispositivo. Se puede utilizar como modo autónomo o combinado con una de las otras implementaciones. No requiere configuración de enrutador.

Modos de aceleración

- **Modo Softboost**: una variante TCP de alto rendimiento que se recomienda para la mayoría de los enlaces. Aunque proporciona menos rendimiento que el modo hardboost, funciona con cualquier implementación. Actúa como TCP normal, pero más rápido.
- **Modo Hardboost**: variante TCP altamente agresiva y limitada a ancho de banda, útil para enlaces de alta velocidad, enlaces intercontinentales, enlaces satelitales y otros enlaces de velocidad fija para los que es difícil alcanzar la velocidad de enlace completa. Recomendado para enlaces punto a punto de velocidad fija en los que no es necesario dar forma al tráfico.

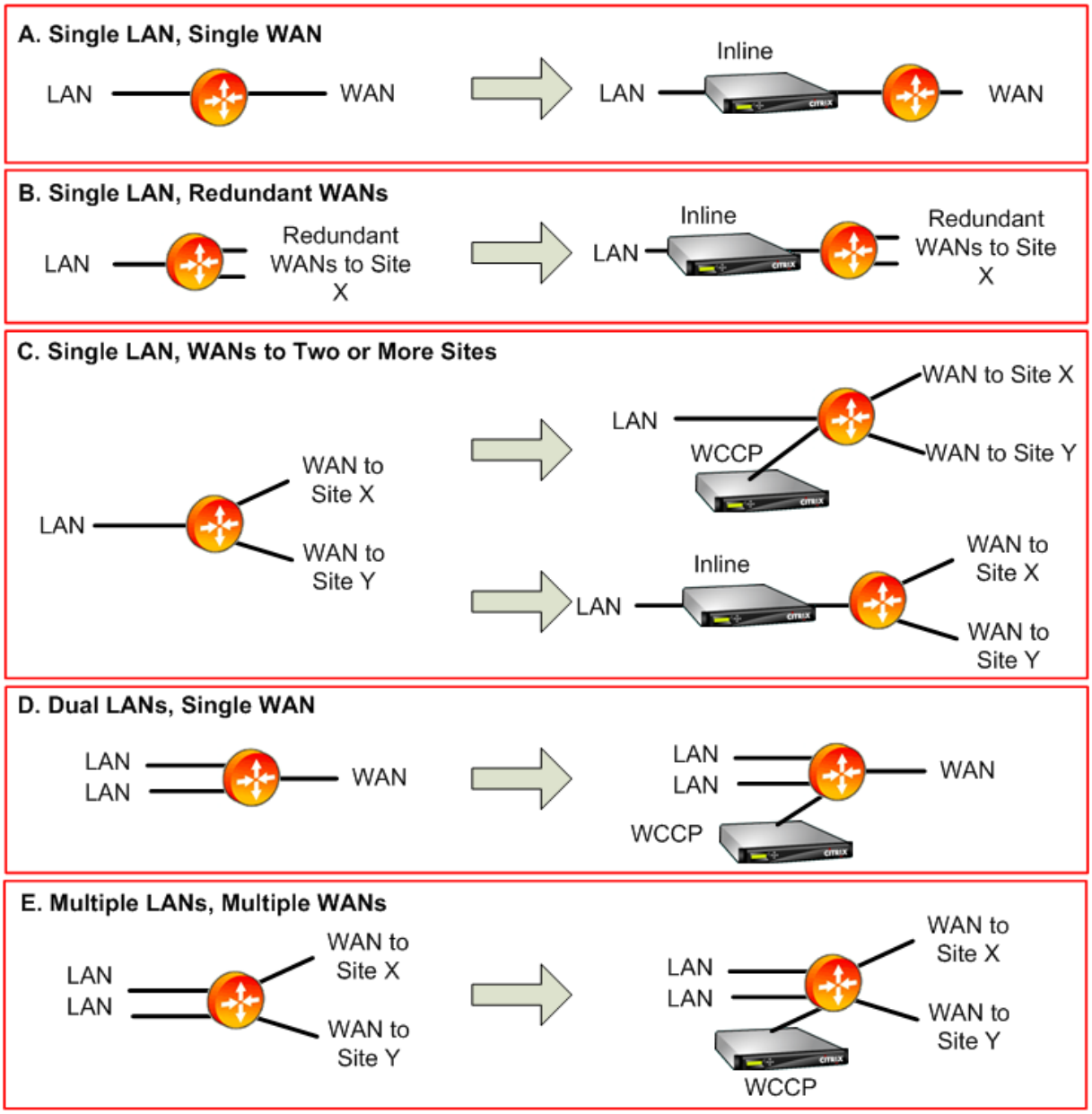
> **Nota**
>
> Para obtener más información sobre los dispositivos Citrix SD-WAN WANOP y los modos de implementación, consulte Documentación de la plataforma WANOP de Citrix SD-WAN.

Sitios con un enrutador WAN

April 23, 2021

Para un sitio con un solo enrutador WAN, el problema principal en la implementación es permitir que el dispositivo Citrix SD-WAN WANOP funcione en armonía con el enrutador. La siguiente imagen muestra los modos de implementación recomendados para un único enrutador. Compárelo con el cableado de su router para encontrar el mejor modo para su entorno.

Modos de implementación recomendados, basados en la topología de enrutador WAN



Comentarios sobre los modos de implementación recomendados:

1. **LAN única, WAN única: modo en línea.** El router tiene una única interfaz LAN activa y una única interfaz WAN activa. El modo recomendado para este caso es el modo en línea, que proporciona la instalación más simple, la mayoría de las funciones y el mayor rendimiento de cualquier modo.
2. **LAN única, WAN redundantes: modo en línea.** El modo en línea es el mejor para esta configuración también.
3. **LAN única, múltiples WAN: en línea o WCCP.** Esta topología se divide en dos categorías: hub-and-spoke o multihop. En una implementación de concentrador y radio, las conexiones se re-

alizan principalmente entre un sitio radial y el sitio del concentrador. En una implementación de multisalto, muchas conexiones se encuentran entre dos sitios radiales, con los datos que pasan a través del sitio del concentrador. Por lo tanto, una única conexión multisalto puede incluir hasta tres dispositivos, dependiendo de los detalles de dónde se coloca el dispositivo del sitio concentrador en el flujo de tráfico.

Para dar forma adecuada al tráfico en las implementaciones de multisalto, todo el tráfico WAN del enrutador WAN del sitio del concentrador también debe pasar a través del dispositivo, en lugar de pasar por el enrutador directamente entre las interfaces WAN. En este caso, WCCP es el modo preferido. Si la implementación es radial y radial, con la mayor parte del tráfico termina en el sitio del concentrador, es preferible una implementación en línea.

4. **LAN duales, WAN única: en línea (con puentes duales) o WCCP.** Este modo es compatible con puentes acelerados duales, modo WCCP o modo virtual en línea.
5. **Múltiples LAN, múltiples WAN: Inline (puentes duales) o WCCP.** Esto es similar al caso C, pero complicado por la presencia de múltiples interfaces LAN, así como múltiples WAN. El WCCP siempre se puede utilizar aquí. En el caso de dos LAN, también se puede utilizar un dispositivo con puentes duales en modo inline.

   Para obtener más información, consulte table

Sitios con varios enrutadores WAN

April 23, 2021

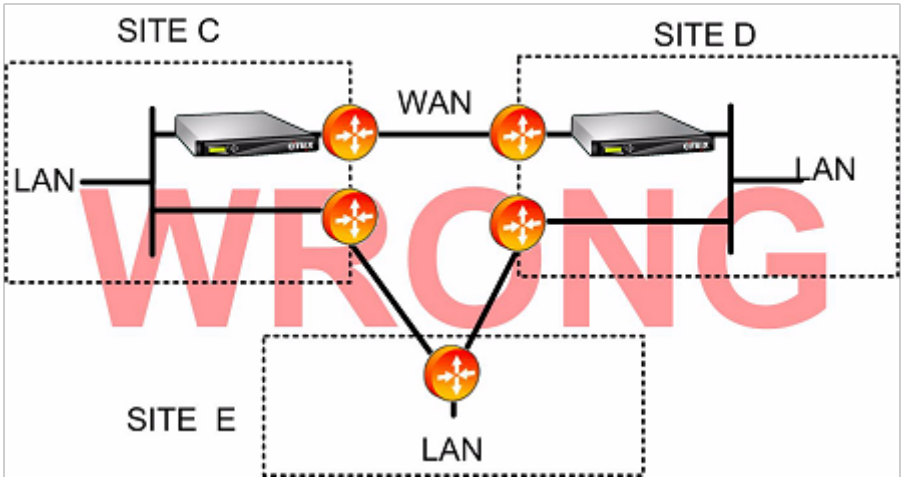
Más de un enrutador WAN en el mismo sitio plantea la posibilidad de *enrutamiento asimétrico.* Normalmente, las redes IP no se ven afectadas por la ruta que toman los paquetes, siempre que lleguen a su destino. Sin embargo, el dispositivo depende de ver todos los paquetes de la conexión. Los paquetes de "final"no son aceptables.

En un sitio con un solo enrutador WAN, el enrutamiento asimétrico no es un problema, ya que el dispositivo se puede colocar en la ruta entre el enrutador y el resto del sitio, de modo que el tráfico que entra o sale del enrutador también pasa a través del dispositivo. Pero con dos enrutadores WAN, el enrutamiento asimétrico puede convertirse en un problema.

Los problemas de enrutamiento asimétrico pueden aparecer durante la instalación o posterior, como resultado de la conmutación por error a un vínculo secundario u otras formas de enrutamiento dinámico y equilibrio de carga. La siguiente imagen muestra un ejemplo de sitios que pueden sufrir un enrutamiento asimétrico. Si los sitios C y D siempre usan la ruta directa, C-D o D-C, al enviar tráfico entre sí, todo está bien. Sin embargo, los paquetes que toman la ruta más larga, C-E-D o

D-E-C, omiten los dispositivos, lo que provoca que las nuevas conexiones no se aceleren y que las conexiones existentes se bloqueen.

Enrutamiento asimétrico

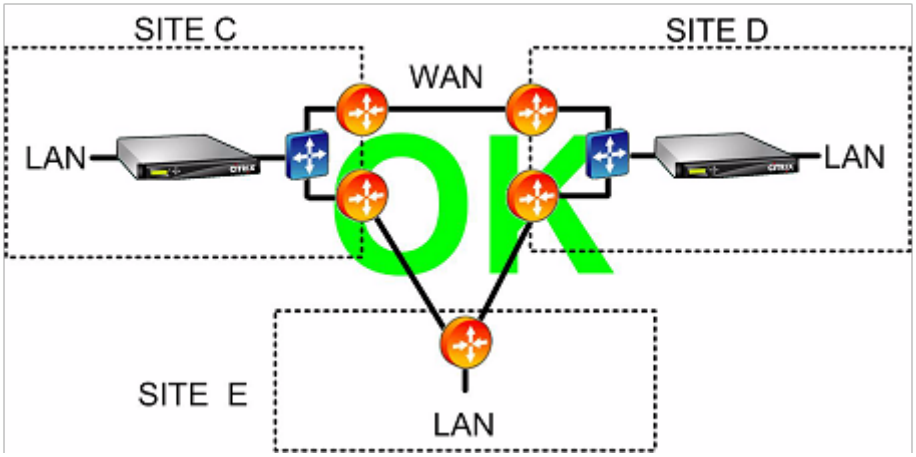


El enrutamiento asimétrico se puede abordar mediante la configuración del enrutador, la ubicación del dispositivo o la configuración del dispositivo.

Si el router está configurado para asegurarse de que todos los paquetes de una conexión dada pasan siempre por el dispositivo en ambas direcciones, no hay asimetría.

Si el dispositivo se coloca después del punto en el que se combinan todas las secuencias WAN, se evita la asimetría y se acelera todo el tráfico, como se muestra en la imagen siguiente.

Evitar el enrutamiento asimétrico mediante la colocación adecuada del dispositivo

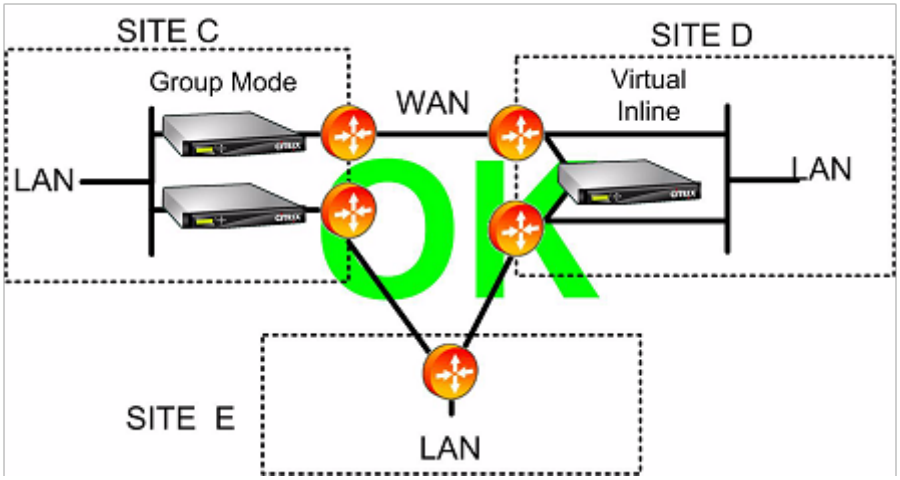


La configuración del dispositivo para utilizar uno de los siguientes modos de reenvío resistentes a la asimetría puede eliminar el problema:

- *Puentes múltiples.* Un dispositivo con dos puentes acelerados, o *pares acelerados*, (por ejemplo, apA y apB), permite acelerar dos enlaces en modo inline. Los dos vínculos pueden ser totalmente independientes, equilibrados de carga o vínculos principales/de copia de seguridad.

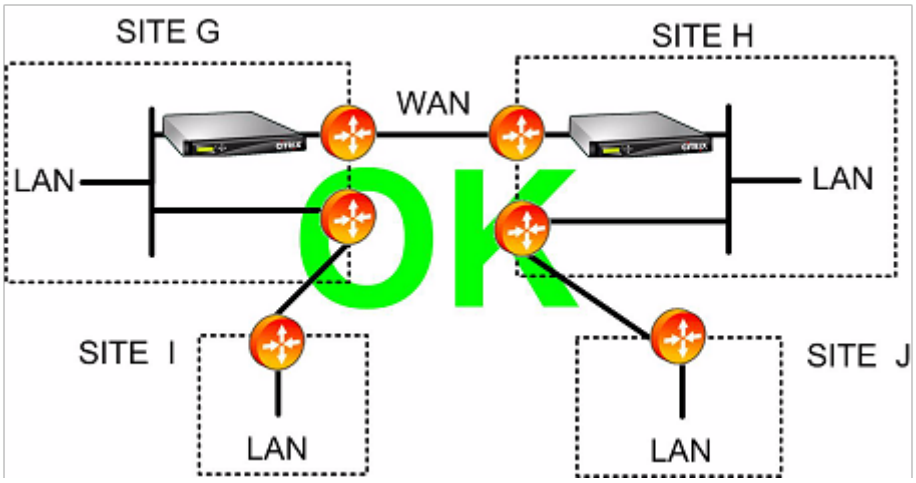
- El*modo WCCP* permite compartir un único dispositivo entre varios enrutadores WAN, lo que le permite gestionar todo el tráfico WAN independientemente del enlace al que llegue.
- El*modo virtual en línea* permite compartir un único dispositivo entre varios enrutadores WAN, lo que le permite gestionar todo el tráfico WAN independientemente del enlace al que llegue.
- *El modo de grupo* permite que dos o más dispositivos en línea compartan tráfico entre sí, lo que garantiza que el tráfico que llega al enlace incorrecto se distribuya correctamente. Debido a que el modo de grupo requiere múltiples dispositivos, es una solución costosa que se adapta mejor a instalaciones donde los enlaces acelerados tienen una amplia separación física, dificultando las otras alternativas. Por ejemplo, si los dos enlaces WAN están en diferentes oficinas de la misma ciudad (pero los campus están conectados por un enlace de velocidad LAN), el modo de grupo podría ser la única opción.

Eliminación del enrutamiento asimétrico mediante el modo de grupo o el modo virtual en línea



> **Nota**
>
> Un extremo del vínculo puede utilizar el modo virtual en línea mientras que el otro extremo utiliza el modo de grupo. Los dos extremos de un vínculo no tienen que utilizar el mismo modo de reenvío.

Los sitios con un solo enlace WAN no pueden tener problemas de enrutamiento asimétrico



Error del dispositivo controlado en varios modos de implementación

April 23, 2021

Los dispositivos de Citrix SD-WAN WANOP cuentan con protección contra la pérdida de conectividad en caso de fallas de software, hardware y energía. Estas salvaguardias dependen del modo.

En el **modo en línea**, los dispositivos mantienen la continuidad de la red en caso de que falle el hardware, el software o el suministro eléctrico. Si está presente, el relé de derivación del dispositivo se cierra si se pierde la alimentación o se produce algún otro fallo. Los dispositivos en línea sin una tarjeta de derivación generalmente bloquean el tráfico en caso de un fallo grave, pero continúan reenviando el tráfico en algunas condiciones, es decir, cuando la pila de red se está ejecutando pero el software de aceleración se ha desactivado o se ha apagado por sí mismo debido a errores persistentes.

Las conexiones aceleradas existentes suelen dejar de responder después de una falla y finalmente terminan por la aplicación o la pila de red en uno de los puntos finales. Algunas conexiones aceleradas pueden continuar como conexiones no aceleradas después del error. Las nuevas conexiones se ejecutan en modo no acelerado.

Cuando el dispositivo vuelve a conectarse, las conexiones existentes continúan como conexiones no aceleradas. Las nuevas conexiones se aceleran.

En el **modo WCCP**, el enrutador omite un dispositivo que deja de responder y vuelve a abrir la conexión cuando el dispositivo comienza a responder de nuevo. El protocolo del WCCP tiene un control integral del estado.

Si la opción verify-availability se utiliza con el **modo virtual inline**, el router se comporta como con el modo WCCP, omitiendo el dispositivo cuando no está disponible y reconectando cuando lo está. Si no se utiliza verify-availability, se descartan todos los paquetes reenviados al dispositivo si el dispositivo no está disponible.

En el **modo de grupo**, se puede configurar un dispositivo para que falle abierto (puente desactivado) o cerrado (puente o relé de derivación habilitado).

En el modo de **alta disponibilidad**, si falla un dispositivo de alta disponibilidad, el otro se hace cargo automáticamente. Las tarjetas de derivación de los dispositivos están desactivadas en modo HA, por lo que si los dispositivos HA están en modo en línea y ambos equipos fallan, se pierde la conectividad.

En el **modo de redirector**, el complemento WANOP de Citrix SD-WAN realiza la comprobación del estado de los dispositivos en modo redirector y omite los dispositivos que no responden, enviando tráfico directamente a servidores de puntos finales.

Modo y matriz de características compatibles

April 23, 2021

En general, todos los modos están activos simultáneamente. Sin embargo, algunas combinaciones no deben utilizarse juntas, como se muestra en la tabla siguiente.

| **Combinaciones admitidas, unidades con tarjetas de derivación Ethernet** |
——	——-	——-	——-	——-	——-	——-	——
Config.	**En línea**	**Modo virtual en línea**	**CMP- GRE**	**CMP- L2**	**Puentes múltiples**	**Alta disponibilidad.**	**Modo de grupo**
Complemento WANOP de CitrixSD-WAN	**S**	**S**	**S**	**S**	**S**	**S**	N
En línea	**S**	N	N	N	**S**	**S**	**S**
Modo virtual en línea		**S**	**S**	**S**	**S**	**S**	N
CMP- GRE			**S**	**S**	**S**	**S**	N
CMP- L2				**S**	**S**	**S**	N
Puentes múltiples					**S**	**S**	N
Alta disponibilidad.						**S**	**S**
Supported Combinations, Units WITHOUT Ethernet Bypass Cards							
Config.	**Inline**	**Virtual Inline**	**WCCP- GRE**	**WCCP- L2**	**Multiple Bridges**	**High Avail. **	**Modo Grupo**
Citrix SD-WAN WANOP Plug-in	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	N	N
Virtual en línea		**Y	Y**	**Y** |**Y****	N	N	N
WCCP-GRE			Y	**Y **	N	N	N	N		**WCCP- L2
**				**Y**	N	N	N	N	N	N	N
Múltiples puentes**					N	N	**Y**
Alta Vail.						N	N

Y = Sí, compatible. N = No se admite.

Configurar el complemento de Citrix SD-WAN WANOP con VPN de Access Gateway

April 23, 2021

La VPN de Access Gateway Standard Edition admite la aceleración del complemento Citrix SD-WAN WANOP Plug-in, siempre que se implemente un dispositivo Citrix SD-WAN WANOP con el dispositivo Access Gateway y el dispositivo Access Gateway esté configurado para admitirlo.

Para obtener la compatibilidad con Citrix SD-WAN WANOP Plug-in con otras VPN, consulte la documentación de su VPN o póngase en contacto con su representante de Citrix.

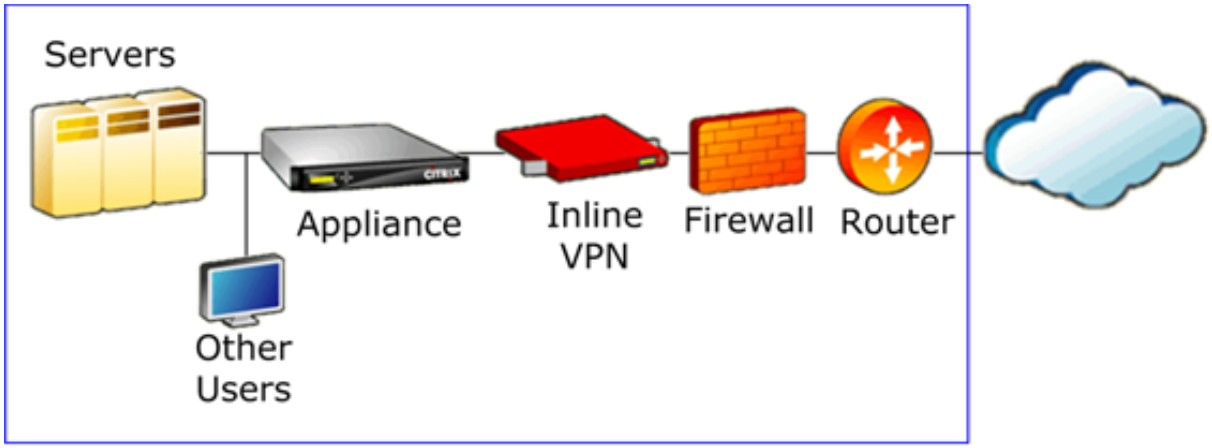
Para configurar la compatibilidad con Citrix SD-WAN WANOP, utilice la herramienta de administración de Access Gateway, de la siguiente manera:

1. En la página Directivas globales de clúster, en Opciones avanzadas, active la casilla de verificación **Habilitar la optimización TCP con el complemento WANOP de Citrix SD-WAN**.
2. Asegúrese de que las direcciones IP utilizadas por Citrix SD-WAN WANOP (IP del redirector e IP de administración) tienen acceso habilitado en la sección Recursos de red de la página Administrador de directivas de acceso.
3. Para cada una de estas direcciones, habilite todos los protocolos (TCP, UDP, ICMP) y habilite Conservar opciones TCP.
4. Asegúrese de que estas mismas direcciones se incluyen en Grupos de usuarios: Predeterminado: Directivas de red en la página Administrador de directivas de acceso.

Opciones de soporte de VPN

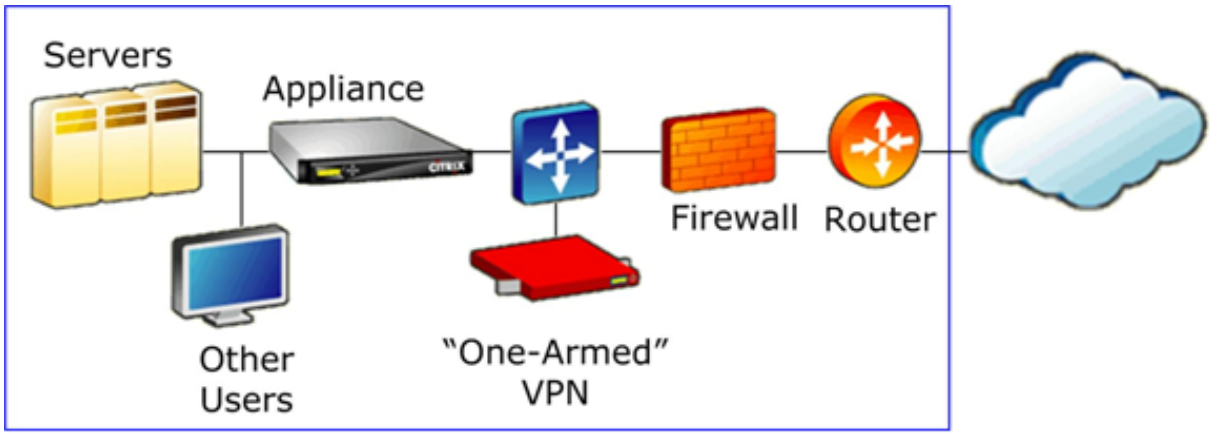
La compatibilidad con VPN es simplemente una cuestión de colocar el dispositivo en el lado LAN de la VPN, como se muestra en la siguiente imagen. Esta ubicación garantiza que el dispositivo reciba y transmita la versión desencapsulada, descifrada y de texto sin formato del tráfico de vínculos, lo que permite que la compresión y la aceleración de aplicaciones funcionen. (La aceleración y compresión de aplicaciones no tienen ningún efecto en el tráfico cifrado. Sin embargo, la aceleración del protocolo TCP funciona en tráfico cifrado).

Cableado VPN para una VPN en línea



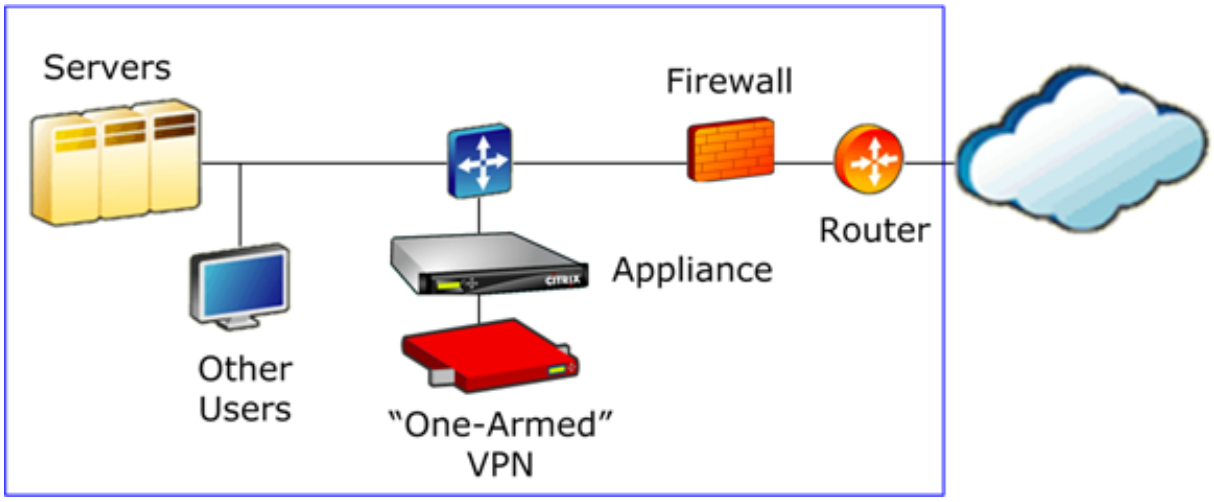
La siguiente imagen muestra una opción para acelerar VPN de un brazo. El dispositivo está en el lado del servidor de la VPN. Todo el tráfico VPN con destino local se acelera. El tráfico VPN con destino remoto no se acelera. El tráfico que no sea VPN también se puede acelerar.

Aceleración VPN de un brazo, Opción A



La siguiente imagen muestra otra opción para acelerar VPNs de un brazo. El dispositivo está en el lado del servidor de la VPN. Todo el tráfico VPN con destino local se acelera. El tráfico VPN con destino remoto no se acelera. El tráfico que no sea VPN también se puede acelerar.

Aceleración VPN de un brazo, Opción B



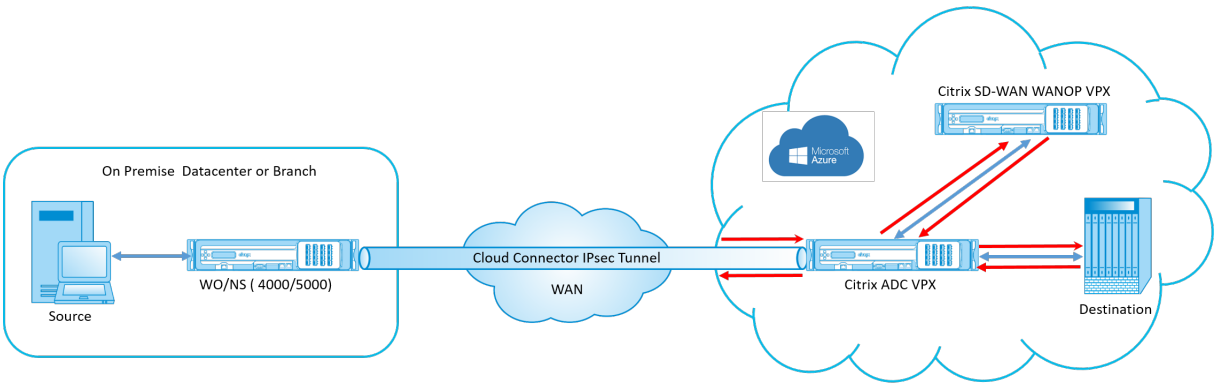
> **Importante**
>
> Para que la aceleración sea efectiva, la VPN debe conservar las opciones de encabezado TCP. La mayoría de las VPN lo hacen.

Implementar SD-WAN WANOP VPX en Microsoft Azure

April 23, 2021

Citrix SD-WAN WANOP Edition ya está disponible en Azure Marketplace, lo que permite la optimización WAN entre el centro de datos de empresa o sucursal y la nube de Azure. Dado que la compatibilidad con el modo L2 no está disponible en infraestructuras de nube, no puede implementar Citrix SD-WAN WANOP como VPX independiente en Azure Cloud. Sin embargo, puede implementar Citrix SD-WAN WANOP VPX junto con Citrix ADC VPX en la infraestructura de nube de Azure. Citrix ADC utiliza un conector en la nube para crear un túnel IPSec, mientras que Citrix SD-WAN WANOP VPX acelera las conexiones, proporcionando un rendimiento similar a LAN para las aplicaciones.

de Citrix SD-WAN WANOP en la topología de nube de Azure



El diagrama de topología muestra un Citrix SD-WAN 4000/5000 implementado en el centro de datos o en las instalaciones de la sucursal. También puede implementar el dispositivo Citrix SD-WAN WANOP y Citrix ADC en modo de dos cajas o ambos podrían ser VPX. En la VNET de nube de Azure, Citrix SD-WAN WANOP VPX se implementa en modo de un brazo (PBR) con Citrix ADC VPX.

Introducción a la implementación

Para implementar WANOP SD-WAN en Microsoft Azure:

1. Implemente una instancia de Citrix ADC VPX en la nube de Azure. Para obtener más información, consulte Implementar una instancia de Citrix ADC VPX en Microsoft Azure. Configure cuatro interfaces de red en cuatro subredes diferentes y habilite el reenvío IP en todas las interfaces de red. Las cuatro interfaces de red se utilizan como:
   - Interfaz de administración
   - Interfaz lateral WAN, para túnel IPSec
   - Interfaz del lado LAN, para conectarse al servidor
   - Interfaz de comunicación WANOP, para comunicarse con Citrix SD-WAN WANOP VPX en la nube de Azure.
2. Implementar un Citrix SD-WAN WANOP VPX en la nube de Azure. Para obtener más información, consulte el procedimiento de implementación que aparece a continuación.

   > **Nota**: Habilite el reenvío IP en la interfaz WANOP.

3. Configure un túnel IPSec entre el dispositivo local y Citrix ADC VPX en la nube de Azure, mediante la dirección IP pública de la interfaz WAN de Citrix ADC. Para obtener más información sobre la configuración de túneles IP, consulte Túneles IP.
4. Configure Citrix ADC VPX para redirigir los paquetes a Citrix SD-WAN WANOP VPX. Utilice la dirección IP privada de la interfaz de comunicación WANOP y cree un servidor virtual de equilibrio de carga. Para obtener más información, consulte Crear un servidor virtual de equilibrio de carga.

5. Configure las siguientes tablas de ruta en Azure:
   - Tabla de rutas para la interfaz orientada a WANOP en Citrix ADC VPX: las entradas de la tabla de rutas deben tener direcciones de origen y destino como subredes de cliente y servidor respectivamente. La dirección IP de la interfaz WANOP de Citrix ADC VPX es el salto siguiente.
   - Tabla de rutas para la interfaz de Citrix SD-WAN WANOP: las entradas de la tabla de rutas deben tener direcciones de origen y destino como subredes de cliente y servidor respectivamente. La dirección IP de la interfaz de Citrix SD-WAN WANOP es el salto siguiente.

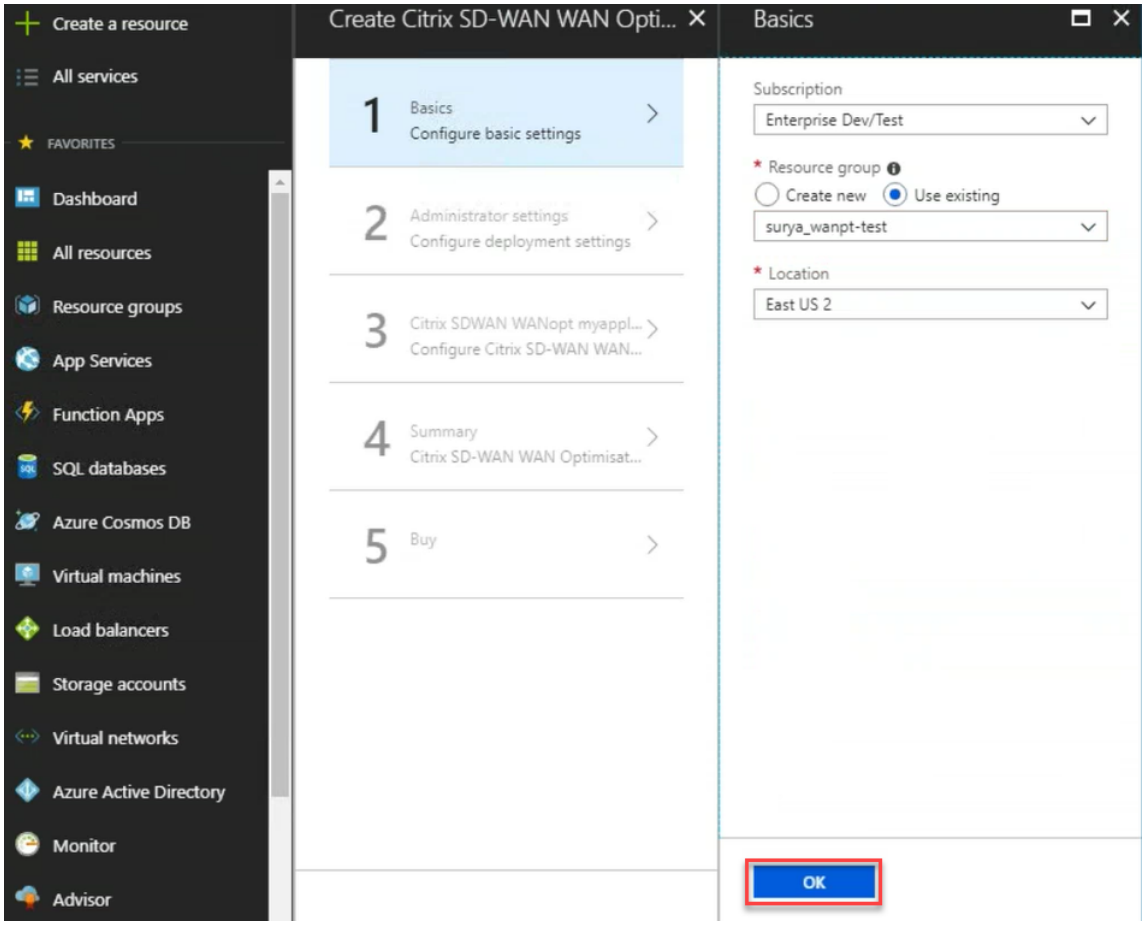
En el ejemplo anterior, cuando el origen intenta acceder a una aplicación en el destino de la nube, los paquetes fluyen a través del túnel IPSec establecido. En el extremo VNET de la nube de Azure, Citrix ADC VPX recibe los paquetes, los descifra y los reenvía a Citrix SD-WAN WANOP VPX. Citrix SD-WAN WANOP VPX procesa los paquetes, los optimiza y los envía de vuelta a Citrix ADC VPX. Citrix ADC VPX envía el paquete al destino. En la ruta de retorno, Citrix ADC VPX reenvía los paquetes a Citrix SD-WAN WANOP VPX para su optimización. Los paquetes optimizados se transmiten de nuevo al origen a través del túnel IPSec establecido.

Implementación de Citrix SD-WAN WANOP VPX en Microsoft Azure

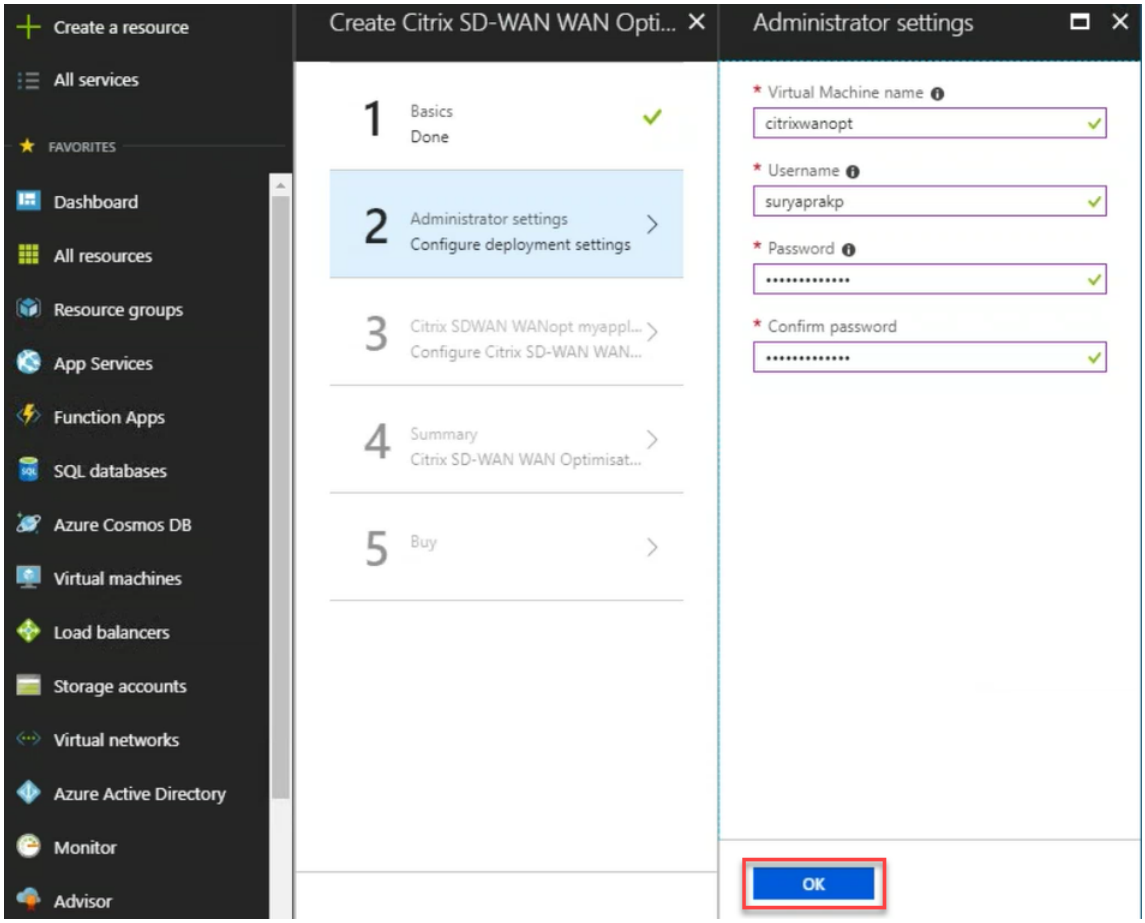
Para implementar Citrix SD-WAN WANOP VPX en Microsoft Azure:

1. En Microsoft Azure, vaya a **Inicio** > **Marketplace** > **Redes**, busque **Citrix SD-WAN WANOP** e instálelo.
2. En la página Citrix SD-WAN WANOP, en la lista desplegable seleccione **Administrador de recursos** y haga clic en **Crear**. Aparecerá la página **Crear optimización Citrix SD-WAN**.
3. En la sección **Básicos**, seleccione el tipo de suscripción, el grupo de recursos y la ubicación. Haga clic en OK.

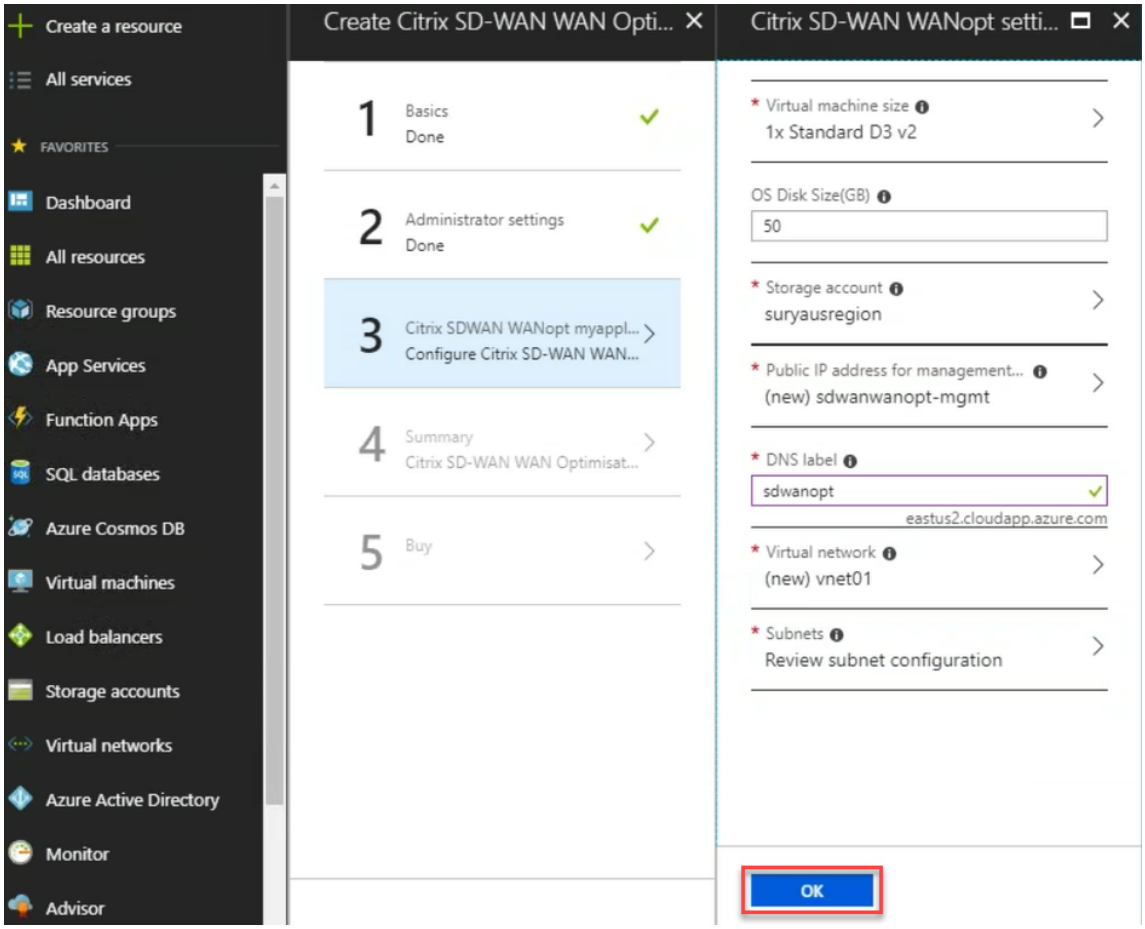
   > **Nota**: Puede elegir crear un grupo de recursos. Un grupo de recursos es un contenedor que contiene recursos relacionados para una solución de Azure. El grupo de recursos puede incluir todos los recursos de la solución o solo los recursos que quiera administrar como grupo.



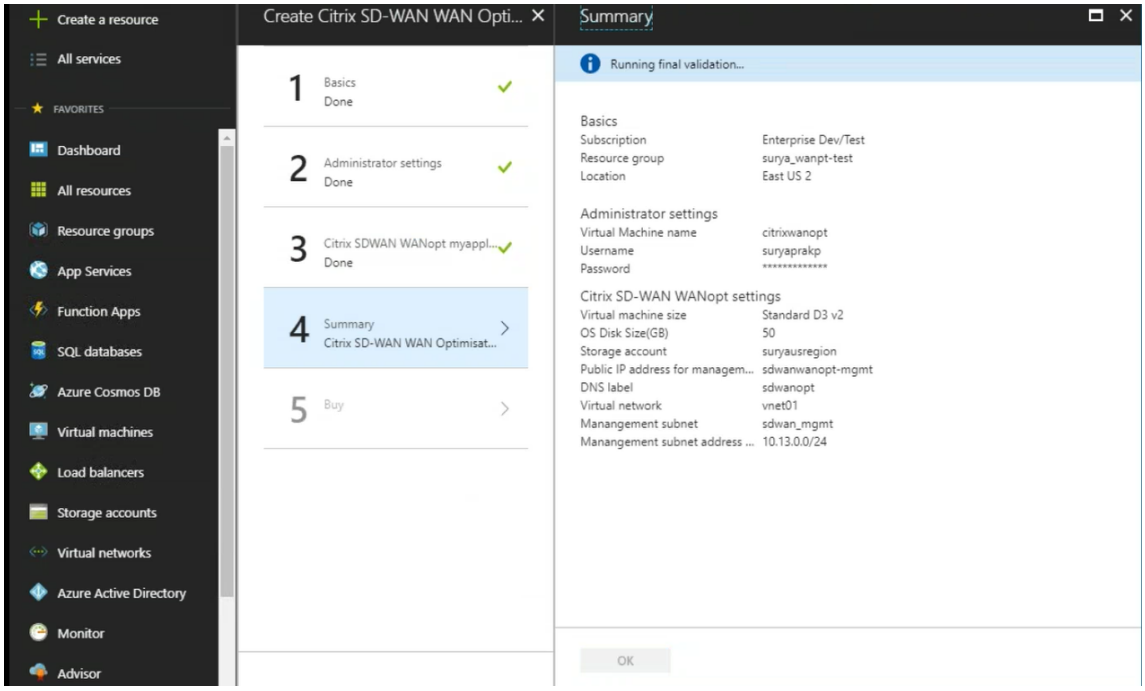
4. En la sección **Administrador**, escriba el nombre y las credenciales de la máquina virtual Citrix SD-WAN WANOP. Haga clic en **Aceptar**.



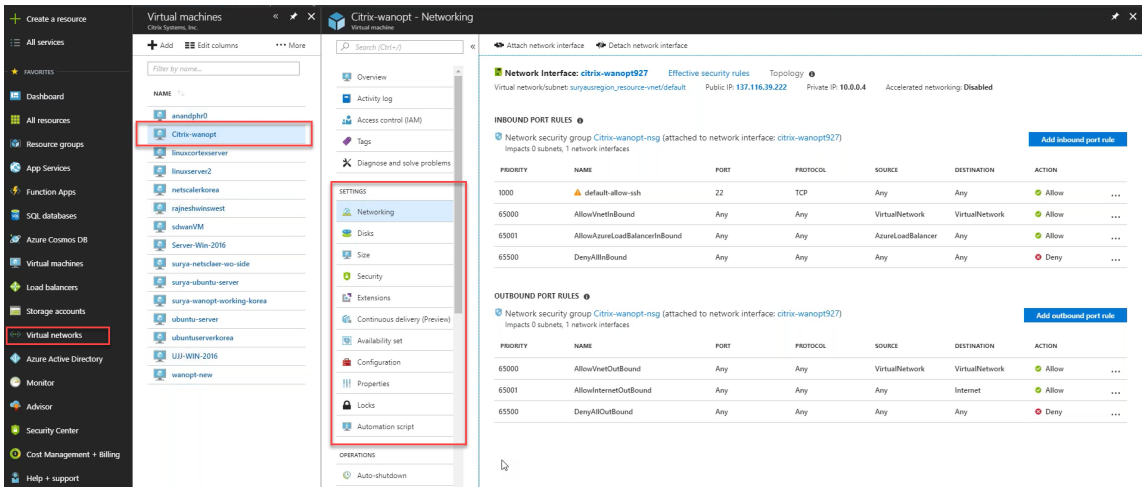
5. En la sección **Configuración de Citrix SD-WAN WANOP**, defina el parámetro de Citrix SD-WAN WANOP VPX según sus requisitos. Haga clic en **OK**.



6. La configuración proporcionada en los pasos anteriores se valida y aplica. Si ha configurado correctamente, aparecerá el mensaje de validación pasada. Haga clic en **OK**.



7. Después de la implementación correcta, vaya a **Redes virtuales** para ver Citrix SD-WAN WANOP VPX. Puede configurar los parámetros de la máquina virtual mediante la opción de configuración.



Procedimiento de actualización de WANOP SD-WAN

December 14, 2022

En esta sección se proporciona información sobre la descarga y la actualización de los paquetes de software de optimización de WAN (WANOP) de Citrix SD-WAN.

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

Descargar los paquetes de software

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

Para descargar el paquete de software Citrix SD-WAN WANOP:

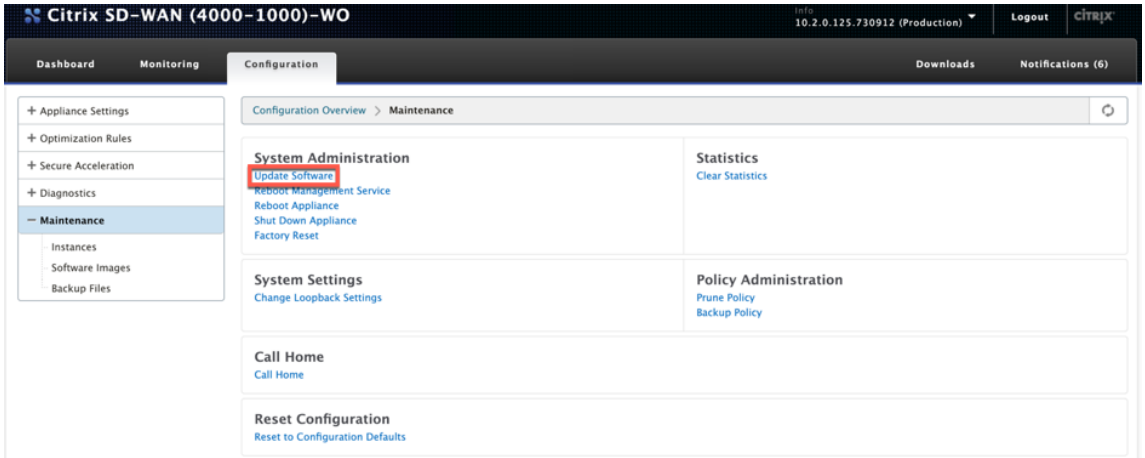
1. Inicie sesión en citrix.com con sus credenciales.
2. Vaya a la página de descargas y seleccione el producto (Citrix SD-WAN) en la lista desplegable.
3. Amplíe la **edición WANOP de Citrix SD-WAN** y seleccione la versión de software requerida.
4. Están disponibles las siguientes opciones de descarga. Descarga el software necesario.
   - Descargue el archivo de actualización.upg para los dispositivos SD-WAN WANOP 400/1000/2000/3000/4000/4100/5000/5100.
   - Descargue el archivo de actualización.bin para los dispositivos SD-WAN WANOP VPX.

Para obtener más información sobre las plataformas compatibles con SD-WAN WANOP, consulte los modelos de plataforma SD-WAN y los paquetes de software.

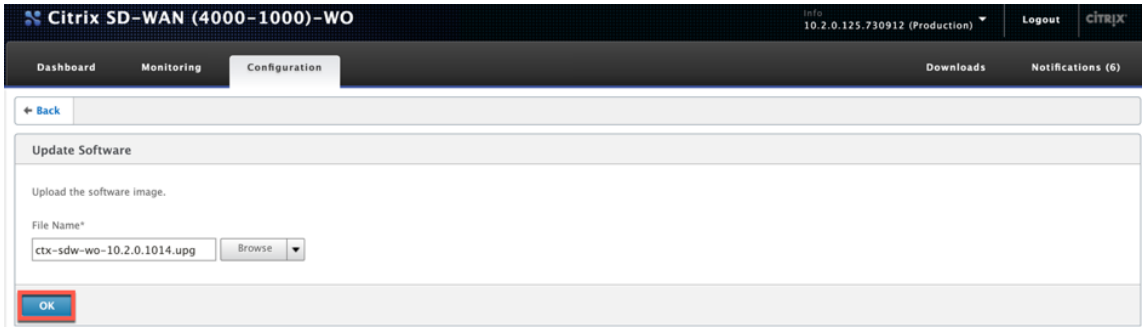
Procedimiento de actualización

Realice el siguiente procedimiento para actualizar el software:

1. Vaya a **Configuración > Mantenimiento > Administración del sistema** haga clic en **Actualizar software**.

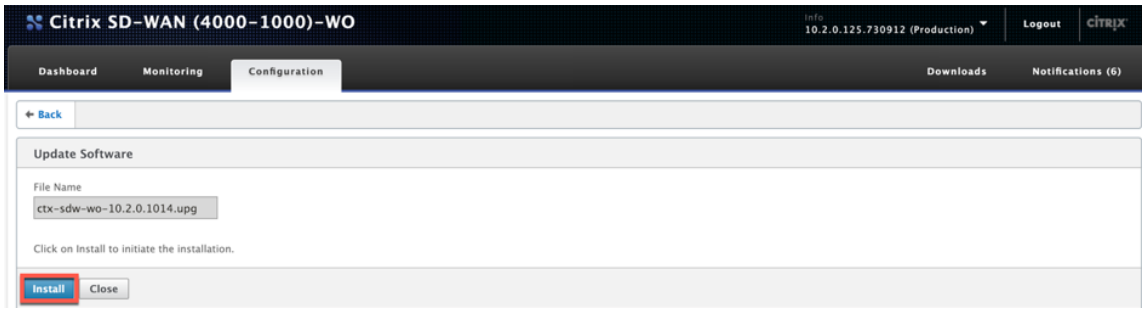


2. Haga clic en **Examinar** para proporcionar el archivo **CTX-SDW-WO-10.2.x.upg** . Haga clic en **Aceptar**.



Puedes ver la barra de estado de carga.

3. Cuando aparezca un mensaje en el que se anuncia que la carga se ha realizado correctamente, haga clic en **Instalar**.



4. El dispositivo realiza la actualización, que tarda entre 10 y 40 minutos según el modelo de plataforma. Muestra una serie de mensajes de estado, que comienzan con **Preparándose para la actualización** y terminan con La **actualización se completó correctamente**.

5. Haga clic en **Aceptar** para mostrar la interfaz de usuario actualizada.

Configuración inicial

April 23, 2021

Después de comprobar las conexiones, estará listo para implementar los dispositivos SD-WAN en la red.

El dispositivo enviado desde Citrix tiene las direcciones IP predeterminadas configuradas en él. Para implementar el dispositivo en la red, debe configurar las direcciones IP adecuadas en el dispositivo para acelerar el tráfico de red.

La configuración inicial consta de las siguientes tareas:

- Identifique los requisitos previos para la configuración inicial.
- Registre varios valores necesarios en el procedimiento de configuración inicial.
- Configure el dispositivo conectándolo al puerto Ethernet.
- Asigne la dirección IP de administración a través de la consola serie.

De forma predeterminada, la configuración inicial implementa el dispositivo en modo en línea.

Requisitos previos

April 23, 2021

Para implementar un dispositivo Citrix SD-WAN 4100 o 5100, debe completar la siguiente configuración de requisitos previos antes de configurar el dispositivo.

Versiones de software

Este documento cubre la versión del software SD-WAN. Consulte las notas de la versión para ver las versiones recomendadas del software NetScaler correspondientes a la versión deseada del software SD-WAN. Nunca utilice ninguna versión que no sea la recomendada para los dispositivos SD-WAN 4100 y 5100.

Archivo de licencias

El número de dispositivos aceleradores depende de la plataforma de hardware y del tipo de licencia que aplique al dispositivo. En la lista siguiente se muestra el número de aceleradores que se aprovisionan automáticamente por el Asistente para configuración:

- Modelo 310: Dos
- Modelo 500: Tres
- Modelos 1000 y 1500: Seis
- Modelo 2000: Eight

Antes de empezar a Provisioning el dispositivo, Citrix recomienda que tenga el archivo de licencia con usted, ya que es necesario al principio del proceso de configuración Para descargar un archivo de licencia, complete el procedimiento descrito en My Account All Licensing Tools: User Guide.

Instalación del hardware

Después de recibir el dispositivo de hardware de Citrix, debe instalarlo en la red. Para instalar el hardware del dispositivo SD-WAN 4100/5100, siga el procedimiento de instalación que se encuentra en Instalación del hardware.

Hoja de trabajo de implementación

April 23, 2021

> **Nota**
>
> Utilice esta hoja de cálculo solo al Provisioning un dispositivo de restablecimiento de fábrica con el asistente de configuración de la versión 9.3. Si simplemente actualiza un sistema configurado anteriormente a la versión 9.3, el dispositivo conserva su configuración anterior, que será diferente.

El dispositivo utiliza al menos dos puertos: El puerto de administración (normalmente 0/1) y el puerto de tráfico (como 10/1). El modo en línea utiliza puertos de tráfico en pares, como puertos 10/1 y 10/2. Los puertos deben seleccionarse con anticipación, ya que la configuración depende de su identidad.

El dispositivo utiliza directamente tres subredes: La subred de administración, la subred de tráfico externo y la subred de tráfico interno. Se utilizan varias direcciones IP en cada subred. Cada subred debe especificarse junto con la máscara de subred correcta.

La siguiente imagen es una hoja de cálculo para estos parámetros. Admite modos en línea y WCCP, con y sin alta disponibilidad. La tabla que aparece debajo de la imagen describe lo que significa cada entrada.

Tabla 1.Parámetros de la hoja de cálculo de implementación

	Parámetro	Ejemplo	Su valor	Descripción
Subred de administración				
M2.	Dirección IP de puerta de enlace	10.199.79.254		Puerta de Gateway predeterminada que sirve a la subred de administración.
M3.	Máscara de subred	255.255.255.128		Máscara de subred para la subred de administración.
M4.	Dirección IP del hipervisor Xen	10.199.79.225		Dirección IP de Xen Hypervisor.
M5.	Dirección IP de VM de servicio	10.199.79.226		Dirección IP de la máquina virtual del servicio de administración, que controla la configuración.
M6.	IU Acelerador	10.199.79.227		La GUI del Acelerador, también llamada interfaz de usuario del Broker, que administra las instancias como una unidad.
M7.	Dirección IP de NetScaler Management	10.199.79.245		Dirección IP de las interfaces GUI y CLI de la instancia de NetScaler.
Subred de tráfico externo				

	Parámetro	Ejemplo	Su valor	Descripción
T1.	Dirección IP del router	172.17.17.1		Dirección IP del enrutador en la subred de tráfico externo.
T2.	Máscara de subred	255.255.255.0		Máscara de subred de subred de tráfico externo.
T3.	Dirección IP de NetScaler	172.17.17.2		Dirección IP de NetScaler en la subred de tráfico externo.
T4.	Dirección IP de señalización externa	172.17.17.10		El tráfico a esta dirección IP está equilibrado de carga entre las direcciones IP de señalización de los aceleradores.
T5.	Dirección IP externa del WCCP #1	172.17.17.11		Mapas a través de NAT a WCCP VIP en el acelerador #1.
T6.	Dirección IP externa del WCCP #2	172.17.17.12		Mapas a través de NAT a WCCP VIP en el acelerador #2.
T7.	Subredes LAN locales	10.200.0.0/16		La subred local LAN que se va a acelerar. Esta es la única subred que recibe aceleración.
T8.	ID de host del router GRE	n/d		Solo WCCP-GRE. ID de host del enrutador GRE.

	Parámetro	Ejemplo	Su valor	Descripción
T9.	Puerto de tráfico	10/1		Puerto utilizado para el tráfico acelerado.
T10+.	(En línea) más puerto de tráfico			Otro puerto de tráfico en par.
T11, T12	(WCCP) Grupos de servicios: TCP, UDP	71, 72		Grupos de servicio utilizados por el acelerador #1 para WCCP. La primera es para el tráfico TCP, la segunda es para UDP.
T13, T14	(No utilizado)			
T15, T16	(En línea) Puertos utilizados por el enlace #2	10/5, 10/6		Si se utilizan varios vínculos con el modo en línea, estos puertos se utilizan para el enlace #2.
T17, T18	(En línea) Puertos utilizados por el enlace #3	10/7, 10/8		Si se utilizan varios vínculos con el modo en línea, estos puertos se utilizan para el enlace #3.
VLAN1.1, VLAN1.2, VLAN1.3, VLAN1.4	VLAN externas para Bridge #1	412		Cuando se utiliza la conexión troncal de VLAN, se etiquetan las VLAN cruzando el puente #1.

	Parámetro	Ejemplo	Su valor	Descripción
VLAN2.1, VLAN2.2, VLAN2.3, VLAN2.4				Cuando se utiliza la conexión troncal de VLAN, se etiquetan las VLAN cruzando el puente #2.
VLAN3.1, VLAN3.2, VLAN3.3, VLAN3.4	VLAN externas para Bridge #1			Cuando se utiliza la conexión troncal de VLAN, se etiquetan las VLAN cruzando el puente #3.

Configuración del dispositivo

April 23, 2021

Antes de comenzar a configurar el dispositivo, debe cambiar la dirección IP del servicio de administración por la de la red de administración, de modo que pueda acceder al dispositivo a través de la red. Puede cambiar la dirección IP de administración conectando un equipo al dispositivo a través del puerto Ethernet o de la consola serie.

Asignar una dirección IP de administración a través del puerto Ethernet

April 23, 2021

Utilice el procedimiento siguiente para la configuración inicial de todos los dispositivos SD-WAN 1000 o 2000 con Windows Server. El procedimiento realiza las siguientes tareas:

- Configure el dispositivo para su uso en el sitio.
- Instale la licencia de Citrix.
- Activar aceleración.
- Habilitar el modelado del tráfico (solo modo en línea).

Con las implementaciones en línea, esta configuración puede ser todo lo que necesita, ya que la mayoría de las funciones de aceleración están habilitadas de forma predeterminada y no requieren configuración adicional.

Si quiere configurar el dispositivo conectándolo al equipo a través de la consola serie, asigne la dirección IP del servicio de administración de la hoja de cálculo completando el procedimiento Asignación de una dirección IP de administración a través de la consola serie y, a continuación, siga los pasos del 4 al 15 del procedimiento que se indica a continuación.

> **Nota**:
>
> Debe tener acceso físico al dispositivo.

Para configurar el dispositivo conectando un equipo al puerto Ethernet 0/1 del dispositivo SD-WAN

1. Establezca la dirección del puerto Ethernet de un equipo (u otro dispositivo equipado con un puerto Ethernet), en 192.168.100.50, con una máscara de red 255.255.0.0. En un dispositivo Windows, esto se hace cambiando las propiedades del Protocolo de Internet versión 4 de la conexión LAN, como se muestra a continuación. Puede dejar en blanco los campos de Gateway y servidor DNS.

2. Con un cable Ethernet, conecte este equipo al puerto etiquetado PRI en el dispositivo SD-WAN.
3. Encender el dispositivo. Con el explorador web del equipo, acceda al dispositivo mediante la dirección IP del servicio de administración predeterminada, que es http://192.168.100.1.
4. En la página de inicio de sesión, utilice las siguientes credenciales predeterminadas para iniciar sesión en el dispositivo:

- **Nombre de usuario**: nsroot
- **Contraseña**: nsroot

1. Inicie el asistente de configuración haciendo clic en **Introducción**.
2. En la página **Configuración de plataforma**, introduzca los valores respectivos de la hoja de cálculo, como se muestra en el ejemplo siguiente:

3. Haga clic en **Done**. Aparecerá una pantalla que muestra el mensaje Instalación en curso…Este proceso tarda aproximadamente de 2 a 5 minutos, dependiendo de la velocidad de la red.
4. Aparece un mensaje Redireccionamiento a la nueva dirección IP de administración.
5. Haga clic en **OK**.
6. Desconecte el equipo del puerto Ethernet y conecte el puerto a la red de administración.
7. Restablezca la dirección IP de su equipo a su configuración anterior.

8. Desde un equipo de la red de administración, inicie sesión en el dispositivo introduciendo la nueva dirección IP del servicio de administración, como, por ejemplo, `https://<Managemnt_IP_Address>`, en un explorador web.
9. Para continuar con la configuración, acepte el certificado y continúe. La opción de continuar varía según el explorador web que esté utilizando.
10. Inicie sesión en el dispositivo con el nombre de usuario **nsroot** y la contraseña de su hoja de cálculo.
11. Para completar el proceso de configuración, consulte Aprovisionar el dispositivo.

Asignar una dirección IP de administración a través del puerto serie

April 23, 2021

Si no desea cambiar la configuración del equipo, puede configurar el dispositivo conectándolo al equipo con un cable de módem nulo serie. Debe tener acceso físico al dispositivo.

Para configurar el dispositivo a través de la consola serie

1. Conecte un cable de módem nulo serie al puerto de consola del dispositivo.
2. Conecte el otro extremo del cable al puerto COM serie de un equipo que ejecuta un emulador de terminal, como Microsoft HyperTerminal, con la configuración 9600, N,8,1, p.
3. En la salida de HyperTerminal, pulse **Entrar**. La pantalla del terminal muestra el mensaje de inicio de sesión. **Nota**: Es posible que tenga que presionar **Entrar** dos o tres veces, dependiendo del programa de terminal que esté utilizando.
4. En el símbolo del sistema de inicio de sesión, inicie sesión en el dispositivo con las siguientes credenciales predeterminadas:

- **Nombre de usuario**: nsroot
- **Contraseña**: nsroot

1. En el símbolo del sistema **$**, ejecute el siguiente comando para cambiar al símbolo del shell del dispositivo: `$ ssh 169.254.0.10`
2. Introduzca **Sí** para continuar conectando con el servicio de administración.
3. Inicie sesión en el símbolo del shell del dispositivo con las siguientes credenciales predeterminadas:
   Contraseña: Nsroot.
4. En el indicador de inicio de sesión, ejecute el siguiente comando para abrir el menú Configuración inicial de dirección de red del servicio de administración: `# networkconfig`

5. Escriba **1** y pulse **Entrar** para seleccionar la opción 1 y especifique una nueva dirección IP de administración para el servicio de administración.
6. Escriba **2** y presione **Intro** para seleccionar la opción 2 y especifique una nueva dirección IP de administración para Citrix Hypervisor.
7. Escriba **3** y pulse **Entrar** para seleccionar la opción 3 y especifique la máscara de red para las direcciones IP.
8. Escriba **4** y pulse **Entrar** para seleccionar la opción 4 y especifique la Gateway predeterminada para la dirección IP del servicio de administración.
9. Escriba **8** y pulse **Entrar** para guardar la configuración y salir.
10. Acceda al dispositivo SD-WAN introduciendo la nueva dirección IP del servicio de administración del dispositivo, como, por ejemplo, `https://<Management_Service_IP_Address>`, en un explorador web de un equipo de la red de administración.
11. Para continuar con la configuración, acepte el certificado y continúe. La opción de continuar varía según el explorador web que esté utilizando.
12. Para completar el proceso de configuración, consulte Aprovisionar el dispositivo.

Aprovisionar el dispositivo

April 23, 2021

Después de asignar una dirección IP al servicio de administración, está listo para aprovisionar las instancias de NetScaler y acelerador. Al iniciar sesión en el dispositivo, aparece el asistente de configuración.

Cuando utilice el asistente de configuración, tenga en cuenta los siguientes puntos:

- En el procedimiento siguiente se supone que ya ha rellenado la hoja de cálculo de configuración.
- Si cambia las direcciones IP de la red de administración o cambia la Gateway predeterminada a una dirección que no esté en la red de administración, perderá la conectividad con el dispositivo a menos que se encuentre en el mismo segmento Ethernet que el puerto de administración.
- Cuando utilice el asistente de configuración, compruebe cuidadosamente las entradas. El asistente no tiene botón Atrás. Si necesita modificar la pantalla anterior, utilice el botón **Atrás** de su explorador. Esto le lleva a la página de inicio de sesión y, a continuación, a la pantalla anterior.
- El asistente de configuración solo se muestra cuando inicia sesión en el dispositivo por primera vez para configurar el dispositivo. Cuando termine de configurar el dispositivo, este asistente se vuelve inaccesible y solo volverá a aparecer después de un restablecimiento de fábrica. Revisa tus entradas cuidadosamente.

Este asistente le guiará por una nueva configuración del dispositivo.

> **Nota**:
>
> Si recibe un error #SESS_CORRUPTED en cualquier momento durante estos procedimientos, haga clic en
> **Cerrar sesión**, borre la caché del explorador, cierre el explorador y vuelva a abrirlo.

Para configurar el dispositivo mediante el asistente de configuración:

1. En la página de bienvenida, haga clic en **Introducción**.

   > **Nota**:
   >
   > Todas las páginas después de la página Introducción tienen un encabezado que dice "Modo de implementación: Modo de en línea/L2", pero este asistente se utiliza para todos los modos de implementación.

2. Siga estos pasos para configurar un sistema totalmente compatible con 7.3:

   - Adquiera las siguientes distribuciones de software de la versión 7.3 de la página de descargas de la versión 7.3 de My Citrix:
     - Servicio de administración (como un archivo.tgz)
     - VM de NetScaler (como un archivo.xva)
     - Accelerator VM (como un archivo.xva)
     - Actualizar el paquete (como un archivo.upg)
   - Vaya a la página **Sistema > Configuración > Servicio de administración > Imágenes de software** y, a continuación, seleccione **Cargar** en la lista Acción.
   - Cargue una imagen del servicio de administración de la versión 7.3 (distribuida como un archivo.tgz).
   - Vaya a la página **Sistema > Configuración > NetScaler\ > Imágenes de software** y, a continuación, cargue una imagen de NetScaler XVA de la versión 7.3.
   - Vaya a la página **Sistema > Configuración > SD-WAN > Imágenes de software** y, a continuación, cargue la imagen XVA del acelerador.
   - Vaya a la página **Sistema > Configuración > Servicio de Gestión** y, a continuación, haga clic en el vínculo **Actualizar Servicio de Gestión**.
   - Seleccione la imagen del servicio de administración que ha cargado recientemente y haga clic en **Aceptar**.
   - Cuando la esquina inferior izquierda de la pantalla muestre Servicio de administración actualizado correctamente, cierre la sesión y borre la caché del explorador. Inicie sesión después de reiniciar el servicio de administración (unos minutos).
   - En la pantalla de **bienvenida**, haga clic en **Introducción**.

3. En Configuración de acceso de administración, especifique valores para los distintos campos según la configuración de red. La siguiente captura de pantalla muestra los valores de ejemplo

utilizados en esta documentación. Introduzca los valores de la siguiente manera:

- **Dirección IP de Citrix Hypervisor**: (Elemento M4 de la hoja de cálculo o H4 si se trata del segundo dispositivo de un par de alta disponibilidad). La dirección de administración del hipervisor Citrix Hypervisor integrado. Debe ser una dirección válida en la red de administración.
- **Dirección IP del servicio de administración**: (elemento M5 de la hoja de cálculo o H5 si este es el segundo dispositivo de un par de alta disponibilidad). La dirección de la máquina virtual del servicio de administración que se utiliza para realizar la mayoría de las tareas de administración del sistema. Debe ser una dirección válida en la red de administración.
- **Máscara**de red: (elemento M3 de la hoja de cálculo). La máscara de subred de la red de administración.
- **Puerta de enlace**: (Elemento M2 en la hoja de cálculo). La Gateway predeterminada para la red de administración.
- **Servidor DNS**: La dirección IP del servidor DNS. Este es un parámetro obligatorio.
- **Servidor NTP**: Dirección IP o FQDN del servidor horario. Esto será utilizado por todas las máquinas virtuales del dispositivo. > **Tenga en cuenta** que si utiliza CIFS avanzada o aceleración MAPI, la hora del sistema del dispositivo debe ser cercana a la del servidor de dominio de Windows, por lo que elija un servidor NTP que mantenga una estrecha relación con la hora de su Windows servidor de dominio.

  > **Nota**:
  >
  > A menos que el servidor NTP se especifique como una dirección IP, el acelerador no lo utiliza.

- **Zona horaria**: Seleccione su zona horaria en el menú desplegable.
- **Cambiar contraseña**: Active esta casilla de verificación y escriba una nueva contraseña nsroot dos veces para cambiar la contraseña. Esta misma contraseña se utiliza en el servicio de administración y la instancia de NetScaler para la cuenta nsroot, y en el acelerador para la cuenta de administrador. Si la contraseña no se cambia, permanece establecida en nsroot (el valor predeterminado).
  Imagen 1.Valores de ejemplo para los campos de la página Configuración de Acceso de Administración de la Configuración

4. Comprueba la configuración y haga clic en **Continuar**.
5. En la sección **Administrar licencias**, vea si ya aparece una licencia adecuada en el campo **Nombre**. Si es así, selecciónelo y vaya al paso 8.

6. Haga clic en **Cargar** en la sección **Actualizar licencias**.
7. Desplácese hasta la carpeta que contiene el archivo de licencia y abra el archivo.
8. Haga clic en **Agregar licencia** y cargue el archivo de licencia proporcionado por Citrix. La licencia se agrega al dispositivo, como se muestra en la imagen siguiente.
   Imagen 2. Licencia de ejemplo agregada al dispositivo en la página Administrar archivos de licencia del Asistente de configuración También

   puede obtener un archivo de licencia en el sitio web de Citrix.com haciendo clic en el botón **aquí** y mediante sus credenciales de My Citrix.
9. Seleccione la licencia en el campo **Nombre** y haga clic en **Continuar**. Aparecerá la página Configuración de SD-WAN. Rellene los campos de la siguiente manera:

   a) **Configuración de red**: Esta sección informa a los aceleradores de la red de administración.

      - **Dirección IP del Acelerador SD-WAN**: Introduzca el valor de M6 de la hoja de cálculo. Esta es la dirección IP del acelerador
      - **Dirección IP de NetScaler**: Introduzca el valor de M7 de la hoja de cálculo. Ésta es la dirección IP de la GUI de NetScaler.
      - **Usar máscara de red del sistema y Gateway**: Seleccione esta opción si desea utilizar la máscara de red y las direcciones IP de la puerta de enlace especificadas en la página Configuración de la plataforma.
      - **Máscara**de red: Introduzca el valor de M3 de la hoja de cálculo. Esta es la máscara de subred (máscara de red) de la red de administración (tenga en cuenta que ya lo ha introducido, en una página anterior).
      - **Puerta de enlace**: Introduzca de nuevo el valor de M2 de la hoja de cálculo.
      - **Dirección IP de señalización**: Introduzca el valor de T4 de la hoja de cálculo. Ésta es la dirección IP de señalización externa del acelerador, utilizada por los Plug-ins SD-WAN para conectarse al dispositivo.
      - **Máscara de red de señalización**: Introduzca el valor de T2 de la hoja de cálculo. Esta es la máscara de subred (máscara de red) de la red de tráfico externa.

   b) **Archivos XVA**: Esta sección le permite especificar archivos XVA cargados previamente (máquinas virtuales Xen) para las instancias de NetScaler y acelerador. Seleccione las imágenes XVA que ha subido como parte del paso 2.
      Imagen 3. Página Configuración de SD-WAN
10. Haga clic en **Continuar**. El asistente comienza a Provisioning las instancias necesarias, como se muestra en la siguiente imagen.
    Imagen 4. Indicador
    de progreso de aprovisionamiento

11. Después de aprovisionar las instancias, agregue una de las subredes LAN locales a la sección **Configuración de vínculos** de la lista T7 de la hoja de cálculo, como se muestra en la siguiente imagen. Esta subred se agrega como subred LAN local en el acelerador. Si tiene más de una subred LAN, puede agregarlas a la definición de **vínculo LAN** en la GUI del Acelerador una vez finalizado el asistente de configuración. Haga clic en **Agregar** para agregar la subred.
    Imagen 5. La configuración de vínculos está en la parte inferior de esta página

12. Cierre la sesión y vuelva a iniciarla. Si aparece el mensaje Incompatibilidad de versiones detectada, instale el paquete de actualización que descargó en el paso 2.

Se ha completado la configuración básica. A continuación, realice la configuración específica del modo de implementación (como para el modo WCCP).

> **Nota**:
>
> Una vez finalizado el asistente, el dispositivo se configura para la configuración básica. Para configurar el dispositivo para un caso de implementación específico, consulte Modos de implementación.

Modos de implementación

April 23, 2021

Un dispositivo SD-WAN actúa como Gateway virtual. No es ni un punto final TCP ni un enrutador. Como cualquier Gateway, su trabajo es almacenar en búfer los paquetes entrantes y ponerlos en el enlace saliente a la velocidad correcta. Este reenvío de paquetes se puede realizar de diferentes maneras, como el modo en línea, el modo en línea virtual y el modo WCCP. Aunque estos métodos se denominan *modos*, no es necesario inhabilitar un modo de reenvío para habilitar otro. Si la implementación admite más de un modo, el modo que utiliza el dispositivo se determina automáticamente mediante el formato Ethernet e IP de cada paquete.

Dado que el dispositivo admite diferentes modos de reenvío y diferentes tipos de conexiones no reenviadas, necesita una forma de distinguir un tipo de tráfico de otro. Para ello, examina la dirección IP de destino y la dirección Ethernet de destino (dirección MAC), como se muestra en la tabla siguiente. Por ejemplo, en el modo en línea, el dispositivo actúa como un puente. A diferencia de otros tipos de tráfico, los paquetes en puente se dirigen a un sistema más allá del dispositivo, no al propio dispositivo. Los campos de dirección no contienen ni la dirección IP del dispositivo ni la dirección MAC Ethernet del dispositivo.

Además de los modos de reenvío puros, el dispositivo tiene que tener en cuenta otros tipos de conexiones, incluidas las conexiones de administración a la GUI y la señal de latido que pasa entre los miem-

bros de un par de alta disponibilidad. Para completar, estos modos de tráfico adicionales también se enumeran en la tabla siguiente.

Cuadro 1 Cómo determinan el modo las direcciones IP y Ethernet

Dirección IP de destino	Dirección Ethernet de destino	Modo
No es un dispositivo	No es un dispositivo	Modo en línea o PassThrough
No es un dispositivo	Dispositivo	WCCP virtual en línea o L2
Dispositivo	Dispositivo	Directo (acceso a la interfaz de usuario)
Dispositivo (VIP)	Dispositivo	Alta disponibilidad. Modo proxy
Dispositivo (paquete GRE de WCCP)	Dispositivo	Modo GRE de WCCP
Dispositivo (IP de señalización)	Dispositivo	Conexión de señalización (conexión de señalización del plugin SD-WAN (plugin SD-WAN, Secure Peer) o Conexión de modo de redirector (plugin SD-WAN)

Todos los modos pueden estar activos simultáneamente. El modo utilizado para un paquete determinado está determinado por los encabezados Ethernet e IP.

Los modos de reenvío son:

- **Modo en línea**, en el que el dispositivo acelera de forma transparente el tráfico que fluye entre sus dos puertos Ethernet. En este modo, el dispositivo aparece (para el resto de la red) como un puente Ethernet. Se recomienda el modo en línea, ya que requiere la menor configuración.
- **Modo WCCP**, que utiliza el protocolo WCCP v. 2.0 para comunicarse con el enrutador. Este modo es fácil de configurar en la mayoría de los enrutadores. El WCCP tiene dos variantes: WCCP-GRE y WCCP-L2. WCCP-GRE encapsula el tráfico WCCP dentro de los túneles de encapsulación de enrutamiento genérico (GRE). WCCP-L2 utiliza transporte de capa 2 (Ethernet) de red no encapsulada.
- **Modo virtual en línea,** en el que un enrutador envía tráfico WAN al dispositivo y el dispositivo lo devuelve al enrutador. En este modo, el dispositivo parece ser un enrutador, pero no utiliza tablas de enrutamiento. Envía el tráfico de retorno al enrutador real. Se recomienda el modo virtual en línea cuando el modo en línea y el funcionamiento WCCP de alta velocidad no son prácticos.

- **Modo de grupo,** que permite que dos dispositivos funcionen juntos para acelerar un par de enlaces WAN ampliamente separados.
- **Modo de alta disponibilidad**, que permite a los dispositivos funcionar como un par de alta disponibilidad activo/en espera. Si se produce un error en el dispositivo principal, el dispositivo secundario se hace cargo.

Los tipos de tráfico adicionales se enumeran aquí para su integridad:

- El **tráfico de paso a través** hace referencia a cualquier tráfico que el dispositivo no intente acelerar. Es una categoría de tráfico, no un modo de reenvío.
- **Acceso directo**, donde el dispositivo actúa como un servidor o cliente normal. La GUI y CLI son ejemplos de acceso directo, mediante los protocolos HTTP, HTTPS, SSH o SFTP. El tráfico de acceso directo también puede incluir los protocolos NTP y SNMP.
- **Comunicación de dispositivo a dispositivo**, que puede incluir conexiones de señalización (utilizadas en peering seguro y por el complemento SD-WAN), latidos VRRP (utilizados en modo de alta disponibilidad) y túneles GRE cifrados (utilizados en modo de grupo).
- **Modos obsoletos.** El modo proxy y el modo redirector son modos de reenvío heredados que no deben utilizarse en instalaciones nuevas.

Los dispositivos SD-WAN 4100/5100 tienen dos modos de implementación recomendados: WCCP y en línea. Estos modos se utilizan comúnmente sin alta disponibilidad (alta disponibilidad), y menos comúnmente con alta disponibilidad.

Actualmente, Citrix recomienda el modo WCCP, con un único enrutador y sin alta disponibilidad, para la mayoría de las implementaciones. Utilice el modo en línea cuando WCCP no esté disponible.

Aunque actualmente no se recomiendan todos los modos siguientes, todos son compatibles:

- Modo WCCP con un único router
- Modo WCCP con un único router y alta disponibilidad
- Cascada de dos o más dispositivos en modo WCCP junto con un dispositivo NetScaler MPX
- Cascada de dos o más dispositivos en modo WCCP junto con un dispositivo NetScaler MPX en alta disponibilidad
- Modo en línea
- Modo en línea en alta disponibilidad
- Modo virtual en línea
- Modo virtual en línea en alta disponibilidad

> **Nota**
>
> Aunque se admiten modos distintos de WCCP y en línea, no están completamente documentados y no se recomiendan para instalaciones típicas. Póngase en contacto con su representante de Citrix cuando considere uno de estos modos.

Personalizar los puertos Ethernet

April 23, 2021

Un dispositivo típico tiene cuatro puertos Ethernet: Dos puertos en puente acelerados, denominados *par acelerado A* (apA.1 y apA.2), con un relé de derivación (fallo a cable) y dos puertos de placa base no acelerados, llamados Primary y Aux1. Los puertos en puente proporcionan aceleración, mientras que los puertos de la placa base a veces se utilizan para fines secundarios. La mayoría de las instalaciones utilizan solo los puertos con puentes.

Algunas unidades SD-WAN tienen solo los puertos de la placa base. En este caso, los dos puertos de la placa base están conectados en puente.

Se puede acceder a la interfaz de usuario del dispositivo mediante una red VLAN o que no sea VLAN. Puede asignar una VLAN a cualquiera de los puertos con puentes o puertos de tarjeta madre del dispositivo para fines de administración.

Ilustración 1. Puertos Ethernet

Lista de puertos

Los puertos se denominan de la siguiente manera:

Puerto Ethernet	Nombre
Puerto 1 de la placa base	Principal (o apA.1 si no hay tarjeta de derivación)
Puerto 2 de la placa base	Auxiliary1 o Aux1 (o apA.2 si no hay tarjeta de derivación)
Puente #1	Par acelerado A (apA, con puertos apA.1 y apA.2)
Puente #2	Par acelerado B (apB, con puertos apB.1 y apB.2)

Cuadro 1 Nombres de puertos Ethernet

Parámetros de puerto

April 23, 2021

Cada puente y puerto de placa madre puede ser:

- Activado o desactivado
- Se ha asignado una dirección IP y una máscara de subred
- Se ha asignado una Gateway predeterminada
- Asignado a una VLAN
- Establecer en 1000 Mbps, 100 Mbps o 10 Mbps
- Configura en dúplex completo, semidúplex o automático (en dispositivos SD-WAN WANOP 4000/5000, algunos puertos se pueden configurar en 10 Gbps)

Todos estos parámetros, excepto la configuración de velocidad/dúplex, se establecen en la página Configuración: Dirección IP. Los ajustes de velocidad/dúplex se establecen en la página Configuración: Interfaz.

> **Notas** sobre los parámetros:

- Los puertos inhabilitados no responden a ningún tráfico.
- La interfaz de usuario basada en explorador se puede habilitar o inhabilitar de forma independiente en todos los puertos.
- Para proteger la interfaz de usuario en puertos con direcciones IP, seleccione HTTPS en lugar de HTTP en la página Configuración: Interfaz de administrador: Acceso web.
- El modo en línea funciona incluso si un puente no tiene dirección IP. Todos los demás modos requieren que se asigne una dirección IP al puerto.
- El tráfico no se enruta entre interfaces. Por ejemplo, una conexión en el puente apA no cruza los puertos primario o Aux1, sino que permanece en el puente apA. Todos los problemas de enrutamiento se dejan en manos de sus routers.

Puentes acelerados (apA y apB)

January 10, 2022

Cada dispositivo tiene al menos un par de puertos Ethernet que funcionan como un puente acelerado, denominado *apA* (para el *par acelerado A*). Un puente puede actuar en modo en línea, funcionando como un puente transparente, como si se tratara de un conmutador Ethernet. Los paquetes fluyen en un puerto y salen del otro. Los puentes también pueden actuar en un modo de arma, en el que los paquetes fluyen en un puerto y retroceden en el mismo puerto.

Un dispositivo que tiene una tarjeta de derivación mantiene la continuidad de la red si un puente o dispositivo no funciona correctamente.

Algunas unidades tienen más de un par acelerado, y estos pares acelerados adicionales se denominan apB, apC, etc.

Tarjeta de derivación

Si el dispositivo pierde energía o falla de alguna otra manera, se cierra un relé interno y los dos puertos conectados en puente se conectan eléctricamente. Esta conexión mantiene la continuidad de la red, pero hace que los puertos del puente sean inaccesibles. Por lo tanto, es posible que desee utilizar uno de los puertos de la placa base para el acceso a la administración.

Precaución: No habilite el puerto primario si no está conectado a la red. De lo contrario, no podrá acceder al dispositivo, como se explica en
Omisión de Ethernet y propagación de enlaces inactivos

Las tarjetas de derivación son estándar en algunos modelos y opcionales en otros. Citrix recomienda comprar dispositivos con tarjetas de omisión para todas las implementaciones en línea.

La función de derivación está cableada como si un cable cruzado conectara los dos puertos, que es el comportamiento correcto en instalaciones correctamente cableadas.

Importante: Las instalaciones de derivación deben probarse: El cableado incorrecto puede funcionar en funcionamiento normal, pero no en modo de derivación. Los puertos Ethernet son tolerantes a un cableado inadecuado y a menudo se ajustan silenciosamente a él. El modo de derivación está cableado y no tiene tal adaptabilidad. Pruebe las instalaciones en línea con el dispositivo apagado para comprobar que el cableado es correcto para el modo de derivación.

Uso de varios puentes

Si el dispositivo está equipado con dos puentes acelerados, se pueden utilizar para acelerar dos enlaces diferentes. Estos vínculos pueden ser totalmente independientes o pueden ser enlaces redundantes que se conectan al mismo sitio. Los vínculos redundantes pueden equilibrarse la carga o utilizarse como enlace principal y enlace de conmutación por error.

Ilustración 1. Uso de puentes dobles

Cuando llega el momento de que el dispositivo envíe un paquete para una conexión determinada, el paquete se envía a través del mismo puente desde el que el dispositivo recibió el paquete de entrada más reciente para esa conexión. Por lo tanto, el dispositivo respeta las decisiones de enlace que tome el router y realiza un seguimiento automático del algoritmo de equilibrio de carga o de enlace principal/failover-link prevaleciente en tiempo real. Para los enlaces no equilibrados de carga, este último algoritmo también asegura que los paquetes siempre usen el puente correcto.

Modos en línea virtuales y WCCP

Se admiten varios puentes tanto en el modo WCCP como en el modo virtual en línea. El uso es el mismo que en el caso de puente único, excepto que WCCP tiene la limitación adicional de que todo el tráfico de un grupo de servicios WCCP determinado debe llegar al mismo puente.

Alta disponibilidad con varios puentes

Dos unidades con varios puentes se pueden utilizar en un par de alta disponibilidad. Simplemente haga coincidir los puentes para que todos los enlaces pasen a través de ambos dispositivos.

Puertos de la placa base

April 23, 2021

Aunque los puertos Ethernet de una tarjeta de derivación son inaccesibles cuando el relé de derivación está cerrado, los puertos de la placa base permanecen activos. En ocasiones, puede acceder a un dispositivo que ha fallado a través de los puertos de la tarjeta madre si los puertos conectados en puente son inaccesibles.

El puerto principal

Si el puerto principal está habilitado y tiene asignada una dirección IP, el dispositivo utiliza esa dirección IP para identificarse con otras unidades de aceleración. Esta dirección se utiliza internamente para una variedad de propósitos y es más visible para los usuarios como el campo Unidad de Socio en la página Supervisión: Optimización: Conexiones. Si no se habilita ningún puerto de la tarjeta madre, el dispositivo utiliza la dirección IP del par acelerado A.

El puerto primario se utiliza para:

- Administración a través de la interfaz de usuario basada en web
- Un canal posterior para el modo de grupo
- Un canal posterior para el modo de alta disponibilidad

El puerto Aux1

El puerto Aux1 es idéntico al puerto primario. Si el puerto Aux1 está habilitado y el puerto primario no lo está, el dispositivo toma su identidad de la dirección IP del puerto Aux1. Si ambos están habilitados, la dirección IP del puerto primario es la identidad de la unidad

Compatibilidad con VLAN

April 23, 2021

Una red de área local virtual (VLAN) utiliza parte del encabezado Ethernet para indicar a qué red virtual pertenece una trama Ethernet determinada. Los dispositivos SD-WAN admiten la conexión troncal VLAN en todos los modos de reenvío (en línea, WCCP, virtual en línea y modo de grupo). El tráfico con cualquier combinación de etiquetas VLAN se gestiona y acelera correctamente.

Por ejemplo, si una secuencia de tráfico que pasa por el puente acelerado está dirigida a 10.0.0.1, VLAN 100 y otra a 10.0.0.1, VLAN 111, el dispositivo sabe que se trata de dos destinos distintos, aunque las dos VLAN tengan la misma dirección IP.

Puede asignar una VLAN a todos, algunos o ninguno de los puertos Ethernet del dispositivo. Si se asigna una VLAN a un puerto, las interfaces de administración (GUI y CLI) solo escuchan el tráfico en esa VLAN. Si no se asigna ninguna VLAN, las interfaces de administración solo escuchan el tráfico sin VLAN. Esta selección se realiza en la ficha Configuración: Configuración del dispositivo: Adaptadores de red: Direcciones IP.

Personalizar los puertos Ethernet

April 23, 2021

Un dispositivo típico tiene cuatro puertos Ethernet: Dos puertos en puente acelerados, denominados *par acelerado A* (apA.1 y apA.2), con un relé de derivación (fallo a cable) y dos puertos de placa base no acelerados, llamados Primary y Aux1. Los puertos en puente proporcionan aceleración, mientras que los puertos de la placa base a veces se utilizan para fines secundarios. La mayoría de las instalaciones utilizan solo los puertos con puentes.

Algunas unidades SD-WAN tienen solo los puertos de la placa base. En este caso, los dos puertos de la placa base están conectados en puente.

Se puede acceder a la interfaz de usuario del dispositivo mediante una red VLAN o que no sea VLAN. Puede asignar una VLAN a cualquiera de los puertos con puentes o puertos de tarjeta madre del dispositivo para fines de administración.

Ilustración 1. Puertos Ethernet

Lista de puertos

Los puertos se denominan de la siguiente manera:

Puerto Ethernet	Nombre
Puerto 1 de la placa base	Principal (o apA.1 si no hay tarjeta de derivación)

Puerto Ethernet	Nombre
Puerto 2 de la placa base	Auxiliary1 o Aux1 (o apA.2 si no hay tarjeta de derivación)
Puente #1	Par acelerado A (apA, con puertos apA.1 y apA.2)
Puente #2	Par acelerado B (apB, con puertos apB.1 y apB.2)

Cuadro 1 Nombres de puertos Ethernet

Omisión de Ethernet y propagación de enlaces inactivos

April 23, 2021

Nota: La propagación de Link-Down se agregó a los dispositivos SD-WAN (anteriormente SD-WAN) 1000, 2000, 3000, 4000 y 5000 con la versión 7.2.1.

La mayoría de los modelos de dispositivos incluyen una función de fail-to-wire (derivación Ethernet) para el modo en línea. Si falla la alimentación, se cierra un relé y los puertos de entrada y salida se conectan eléctricamente, lo que permite que la señal Ethernet pase de un puerto a otro como si el dispositivo no estuviera allí. En el modo de conmutación por error, el dispositivo parece un cable cruzado que conecta los dos puertos.

Cualquier fallo en el hardware o software del dispositivo también cierra el relé. Cuando se reinicia el dispositivo, el relé de derivación permanece cerrado hasta que el dispositivo esté completamente inicializado, lo que mantiene la continuidad de la red en todo momento. Esta función es automática y no requiere configuración del usuario.

Cuando se cierra el relé de derivación, no se puede acceder a los puertos del puente del dispositivo.

Si el transportista se pierde en uno de los puertos del puente, el transportista se deja caer en el otro puerto del puente para asegurarse de que la condición de enlace se propaga al dispositivo del otro lado del dispositivo. Las unidades que supervisan el estado del enlace (como los enrutadores) son notificadas de las condiciones en el otro lado del puente.

La propagación de enlaces tiene dos modos de funcionamiento:

- Si el puerto primario no está habilitado, el estado de enlace en un puerto de puente se refleja brevemente en el otro puerto de puente y, a continuación, se vuelve a habilitar el puerto. Esto permite llegar al dispositivo a través del puerto todavía conectado para la administración, el latido de alta disponibilidad y otras tareas.

- Si el puerto primario está habilitado, el dispositivo asume (sin comprobar) que el puerto primario se utiliza para la administración, el latido de alta disponibilidad y otras tareas. La condición de enlace descendente en un puerto de puente se refleja persistentemente en el otro puerto, hasta que se restaure el transportista o se reinicie la unidad. Esto es cierto incluso si el puerto primario está habilitado en la GUI pero no conectado a una red, por lo que el puerto primario debe estar inhabilitado (el valor predeterminado) cuando no esté en uso.

Acelerar un sitio completo

April 23, 2021

Modo en línea, aceleración de todo el tráfico en una WAN muestra una configuración típica para el modo en línea. Para ambos sitios, los dispositivos se colocan entre la LAN y la WAN, por lo que se acelera todo el tráfico WAN que se puede acelerar. Este es el método más simple para implementar la aceleración, y debe usarse cuando sea práctico.

Debido a que todo el tráfico de enlaces fluye a través de los dispositivos, los beneficios de la cola justa y el control de flujo impiden que el enlace se invente.

En las redes IP, la Gateway de cuello de botella determina el comportamiento de la cola para todo el vínculo. Al convertirse en la Gateway de cuello de botella, el dispositivo obtiene el control del enlace y puede administrarlo de forma inteligente. Esto se hace estableciendo el límite de ancho de banda ligeramente inferior a la velocidad del enlace. Cuando esto se hace, el rendimiento del enlace es ideal, con una latencia y pérdida mínimas incluso en la utilización completa del enlace.

Acelerar sitios parciales

April 23, 2021

Para reservar el ancho de banda acelerado del dispositivo para un grupo determinado de sistemas, como los servidores de copia de seguridad remotos, puede instalar el dispositivo en una red de sucursales que incluya únicamente esos sistemas. Esto se muestra en la siguiente imagen.

Ilustración 1. Modo en línea, acelerando solo los sistemas seleccionados

El modelado del tráfico SD-WAN depende del control de todo el vínculo, por lo que el modelado del tráfico no es efectivo con esta topología, ya que el dispositivo solo ve una parte del tráfico de vínculos. El control de latencia es hasta la Gateway de cuello de botella, y la capacidad de respuesta interactiva puede verse afectada.

Modo WCCP

April 23, 2021

Web Cache Communication Protocol (WCCP) es un protocolo de enrutamiento dinámico introducido por Cisco. Originalmente diseñado solo para el almacenamiento en caché web, WCCP versión 2 se convirtió en un protocolo de uso más general, adecuado para el uso de aceleradores como los dispositivos Citrix SD-WAN.

El modo WCCP es la forma más sencilla de instalar un dispositivo SD-WAN cuando el funcionamiento en línea no es práctico. También es útil cuando se produce el enrutamiento asimétrico, es decir, cuando los paquetes de la misma conexión llegan a través de diferentes enlaces WAN. En el modo WCCP, los enrutadores utilizan el protocolo WCCP 2.0 para desviar el tráfico a través del dispositivo. Una vez recibido por el dispositivo, el motor de aceleración y el formador de tráfico tratan el tráfico como si se recibiera en modo en línea.

> **Nota**
>
> - A los efectos de esta discusión, la versión 1 del WCCP se considera obsoleta y solo se presenta la versión 2 del WCCP.
> - La documentación estándar de WCCP llama a los clientes de WCCP cachés. Para evitar confusiones con cachés reales, Citrix generalmente evita llamar a un cliente WCCP como caché. En su lugar, los clientes WCCP suelen denominarse appliances.
> - Esta discusión utiliza el término enrutador para indicar enrutadores compatibles con WCCP y conmutadores compatibles con WCCP. Aunque aquí se utiliza el término enrutador, algunos conmutadores de gama alta también admiten WCCP y se pueden usar con dispositivos SD-WAN.
>
> Los dispositivos SD-WAN admiten dos modos WCCP:
>
> - WCCP es la oferta original de SD-WAN WCCP admitida desde la versión 3.x. Es compatible con un único grupo de servicios de dispositivo (sin clústeres).
> - La agrupación en clústeres WCCP, introducida en la versión 7.2, permite al router equilibrar la carga del tráfico entre varios dispositivos.

Cómo funciona el modo WCCP

El modo físico para la implementación de WCCP de un dispositivo SD-WAN es el modo de un armado en el que el dispositivo está conectado directamente a un puerto dedicado en el enrutador WAN. El estándar WCCP incluye una negociación de protocolo en la que el dispositivo se registra con el router y

ambos negocian el uso de funciones que admiten en común. Una vez que esta negociación se realiza correctamente, el tráfico se enruta entre el enrutador y el dispositivo de acuerdo con el enrutador WCCP y las reglas de redirección definidas en el enrutador.

Un dispositivo en modo WCCP solo requiere un puerto Ethernet único. El dispositivo debe implementarse en un puerto de enrutador dedicado (o en un puerto de conmutador compatible con WCCP) o aislado de otro tráfico a través de una VLAN. No mezcle los modos en línea y WCCP.

En la siguiente imagen se muestra cómo se configura un enrutador para interceptar el tráfico en las interfaces seleccionadas y reenviarlo al dispositivo habilitado para WCCP. Siempre que el dispositivo habilitado para WCCP no esté disponible, el tráfico no se intercepta y se reenvía normalmente.

Ilustración 1. Flujo de tráfico de WCCP

Encapsulación de tráfico

WCCP permite que el tráfico se reenvíe entre el router y el dispositivo en cualquiera de los modos siguientes:

- Modo L2: Requiere que el enrutador y el dispositivo estén en el mismo segmento L2 (normalmente un segmento Ethernet). El paquete IP no está modificado y solo se altera el direccionamiento L2 para reenviar el paquete. En muchos dispositivos, el reenvío L2 se realiza en la capa de hardware, dándole el máximo rendimiento. Debido a su ventaja de rendimiento, el reenvío L2 es el modo preferido, pero no todos los dispositivos compatibles con WCCP lo admiten.
- Modo GRE: La encapsulación de redirección genérica (GRE) es un protocolo redirigido y, en teoría, el dispositivo puede colocarse en cualquier lugar, pero para el rendimiento debe colocarse cerca del enrutador, en una ruta rápida y no congestionada que atraviesa el menor número posible de conmutadores y enrutadores. GRE es el modo WCCP original. Se crea un encabezado GRE y se anexa el paquete de datos. El dispositivo receptor quita el encabezado GRE. Con la encapsulación, el dispositivo puede estar en una subred que no esté conectada directamente al enrutador. Sin embargo, tanto el proceso de encapsulación como el enrutamiento posterior agregan sobrecarga de CPU al enrutador, y la adición del encabezado GRE de 28 bytes puede conducir a la fragmentación de paquetes, lo que agrega sobrecarga adicional.

El modo WCCP admite múltiples enrutadores y GRE frente a Reenvío L2. Cada router puede tener varios enlaces WAN. Cada vínculo puede tener su propio grupo de servicios WCCP.

El modelado del tráfico no es efectivo a menos que el dispositivo administre tanto el tráfico UDP como el tráfico TCP. Se recomienda un segundo grupo de servicios, con un grupo de servicios UDP para cada vínculo WAN, si se desea dar forma al tráfico.

Actualizaciones de registro y estado

Un cliente WCCP (un dispositivo) utiliza el puerto UDP 2048 para registrarse con el enrutador y negociar qué tráfico debe enviarse a él, y también qué funciones de WCCP deben utilizarse para este tráfico. El dispositivo opera en este tráfico y reenvía el tráfico resultante al extremo original. El estado de un dispositivo se realiza un seguimiento a través del proceso de registro WCCP y un protocolo de latidos. El dispositivo se pone en contacto primero con el router a través del canal de control WCCP (puerto UDP 2048) y el dispositivo y el router intercambian información con paquetes denominados Here_I_Am e I_See_You, respectivamente. De forma predeterminada, este proceso se repite cada 10 segundos. Si el enrutador no recibe un mensaje del dispositivo durante tres de estos intervalos, considera que el dispositivo ha fallado y detiene el reenvío del tráfico hasta que se restablezca el contacto.

Servicios y grupos de servicios

Diferentes dispositivos que usan el mismo enrutador pueden proporcionar diferentes servicios. Para realizar un seguimiento de los servicios asignados a los dispositivos, el protocolo WCCP utiliza un identificador de grupo de servicios, un entero de un byte. Cuando un dispositivo se registra con un enrutador, también incluye números de grupo de servicio.

- Un único dispositivo puede admitir más de un grupo de servicios.
- Un único enrutador puede admitir más de un grupo de servicios.
- Un único dispositivo puede utilizar el mismo grupo de servicios con más de un enrutador.
- Un único enrutador puede utilizar el mismo grupo de servicios con más de un dispositivo. Para los dispositivos SD-WAN, se admiten varios dispositivos en el modo de clúster WCCP y se admite un único dispositivo en el modo WCCP.
- Cada dispositivo especifica un tipo de retorno (L2 o GRE) independientemente para cada dirección y cada grupo de servicio. Los dispositivos SD-WAN 4000/5000 siempre especifican el mismo tipo de retorno para ambas direcciones. Otros dispositivos SD-WAN permiten que el tipo de devolución sea diferente.

Imagen 2. Uso de diferentes grupos de servicios de WCCP para diferentes servicios

Se pueden utilizar **varios grupos de servicios** con WCCP en el mismo dispositivo. Por ejemplo, el dispositivo puede recibir tráfico del grupo de servicios 51 desde un vínculo WAN y el tráfico del grupo de servicios 62 desde otro vínculo WAN. El dispositivo también admite varios enrutadores. Es indiferente si todos los enrutadores usan el mismo grupo de servicio o diferentes enrutadores usan diferentes grupos de servicio.

Seguimiento de grupos de servicios. Si llega un paquete a un grupo de servicios, los paquetes de salida para la misma conexión se envían en el mismo grupo de servicios. Si llegan paquetes para la

misma conexión en varios grupos de servicios, los paquetes de salida rastrean el grupo de servicios visto más recientemente para esa conexión.

Comportamiento de alta disponibilidad

Cuando WCCP se utiliza con el modo de alta disponibilidad, el dispositivo principal envía su propia dirección IP de administración apA o apB, no la dirección virtual del par de alta disponibilidad, cuando se pone en contacto con el router. Si se produce una conmutación por error, el nuevo dispositivo principal se pone en contacto con el router automáticamente, restableciendo el canal WCCP. En la mayoría de los casos, el período de tiempo de espera de WCCP y el tiempo de conmutación por error de alta disponibilidad se superponen. Como resultado, la interrupción de la red es menor que la suma de los dos retrasos.

WCCP estándar permite solo un único dispositivo en un grupo de servicios WCCP. Si un nuevo dispositivo intenta ponerse en contacto con el router, descubre que el otro dispositivo está manejando el grupo de servicios y que el nuevo dispositivo establece una alerta. Comprueba periódicamente si el grupo de servicios sigue activo con el otro dispositivo y el nuevo dispositivo gestiona el grupo de servicios cuando el otro dispositivo se vuelve inactivo. La agrupación en clústeres WCCP permite varios dispositivos por grupo de servicios.

Topología de implementación

La siguiente imagen muestra una implementación simple de WCCP, adecuada para L2 o GRE. El puerto de tráfico (1/1) está conectado directamente a un puerto de enrutador dedicado (Gig 4/12).

Imagen 3. Implementación simple del WCCP

En este ejemplo, el SD-WAN 4000/5000 se implementa en modo de un brazo, con el puerto de tráfico (1/1) y el puerto de administración (0/1) cada uno de ellos se conecta a su propio puerto de enrutador dedicado.

En el enrutador, WCCP se configura con una redirección IP wccp idéntica en las instrucciones de los puertos WAN y LAN. Se utilizan dos grupos de servicio, 71 y 72. El grupo de servicios 71 se utiliza para el tráfico TCP y el grupo de servicios 72 se utiliza para el tráfico UDP. El dispositivo no acelera el tráfico UDP, pero puede aplicarle directivas de modelado de tráfico.

> **Nota**: La especificación WCCP no permite reenviar protocolos distintos de TCP y UDP, por lo que protocolos como ICMP y GRE siempre omiten el dispositivo.

Agrupación en clústeres de WCCP

Los dispositivos SD-WAN admiten la agrupación en clústeres WCCP, lo que permite al router equilibrar la carga del tráfico entre varios dispositivos. Para obtener más información acerca de la implementación de dispositivos SD-WAN como clúster, consulte Agrupación en clústeres de WCCP.

Especificación WCCP

Para obtener más información acerca de WCCP, consulte Web Cache Communication Protocol V2, Revisión 1, http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00.

> **Nota**
>
> Al implementar SD-WAN en WCCP para redundancia de switch, podemos conectar el switch 2 a apB. Cree un SG diferente para apB, dele una prioridad más baja que el SG para apA. Si apA mayor SG está arriba, eso se usará para la redirección. Si no está disponible, se utilizará el apB SG. Tenga en cuenta que APA y APB deben estar en una subred diferente.

Modo WCCP (no agrupado en clústeres)

January 10, 2022

El modo WCCP solo permite un único dispositivo en un grupo de servicios WCCP. Si un nuevo dispositivo intenta ponerse en contacto con el router, descubre que el otro dispositivo está manejando el grupo de servicios y que el nuevo dispositivo establece una alerta. Comprueba periódicamente si el grupo de servicios sigue activo con el otro dispositivo y el nuevo dispositivo gestiona el grupo de servicios cuando el otro dispositivo se vuelve inactivo.

> **Nota: La**agrupación en clústeres WCCP permite varios dispositivos por grupo de servicios.

Limitaciones y prácticas recomendadas

A continuación se presentan las limitaciones y las prácticas recomendadas para el modo WCCP (no agrupado en clústeres):

- En los dispositivos con más de un par acelerado, todo el tráfico de un grupo de servicios WCCP determinado debe llegar al mismo par acelerado.
- No mezcle tráfico en línea y WCCP en el mismo dispositivo. El dispositivo no aplica esta directriz, pero infringirla puede causar dificultades con la aceleración. (Los modos en línea virtuales y

WCCP se pueden mezclar, pero solo si el WCCP y el tráfico en línea virtual provienen de diferentes enrutadores).

- Para sitios con un único enrutador WAN, use WCCP siempre que el modo en línea no sea práctico.
- Solo se admite un dispositivo por grupo de servicios. Si más de un dispositivo intenta conectarse al mismo enrutador con el mismo grupo de servicios, la negociación solo tendrá éxito para el primer dispositivo.
- Para sitios con varios enrutadores WAN atendidos por el mismo dispositivo, WCCP puede utilizarse para admitir uno, algunos o todos los enrutadores WAN. Otros enrutadores pueden usar el modo virtual en línea.

Disponibilidad de router para WCCP

Configurar el enrutador para WCCP es muy simple. La compatibilidad con WCCP versión 2 está incluida en todos los routers modernos, habiéndose agregado al IOS de Cisco en la versión 12.0 (11) S y 12.1 (3) T. La mejor estrategia de configuración del router está determinada por las funciones del router y los switches. El modelado del tráfico requiere dos grupos de servicio.

Si su router admite Reverse Path Forwarding, debe inhabilitarlo en todos los puertos, ya que puede confundir el tráfico WCCP con tráfico falsificado. Esta función se encuentra en los routers Cisco más recientes, como el Cisco 7600.

Estrategias de configuración del router

Existen dos enfoques básicos para redirigir el tráfico desde el enrutador al dispositivo:

Solo en el puerto WAN, agregue una instrucción WCCP redirect in y una instrucción WCCP redirect out.
En cada puerto del enrutador, excepto en el puerto conectado al dispositivo, agregue una instrucción WCCP redirect in.

El primer método redirige solo el tráfico WAN al dispositivo, mientras que el segundo redirige todo el tráfico del enrutador al dispositivo, esté relacionado o no con WAN. En un router con varios puertos LAN y tráfico LAN a LAN sustancial, el envío de todo el tráfico al dispositivo puede sobrecargar su segmento LAN y sobrecargar al dispositivo con esta carga innecesaria. Si se utiliza GRE, el tráfico innecesario también puede cargar el router.

En algunos routers, la ruta de redireccionamiento en es más rápida y pone menos carga en la CPU del router que la ruta de redireccionamiento hacia fuera. Si es necesario, esto puede determinarse mediante un experimento directo en su router: Pruebe ambos métodos de redirección bajo carga de red completa para ver cuál ofrece las tasas de transferencia más altas.

Algunos routers y conmutadores compatibles con WCCP no admiten WCCP redirect out, por lo que se debe usar el segundo método. Para evitar sobrecargar el enrutador, se recomienda evitar redirigir

grandes cantidades de puertos del enrutador a través del dispositivo, tal vez mediante el uso de dos enrutadores, uno para el enrutamiento WAN y otro para el enrutamiento LAN a LAN.

En general, el método 1 es más simple, mientras que el método 2 puede proporcionar un mayor rendimiento.

Modelado de tráfico y WCCP

Un grupo de servicios puede ser TCP o UDP, pero no ambos. Para que el formador de tráfico sea eficaz, ambos tipos de tráfico WAN deben pasar por el dispositivo. Por lo tanto:

La aceleración requiere un grupo de servicios, para el tráfico TCP.
El modelado del tráfico requiere dos grupos de servicios, uno para el tráfico TCP y otro para el tráfico UDP. La diferencia entre los dos está configurada en el dispositivo y el enrutador acepta esta configuración.

Configurar el router

El dispositivo negocia WCCP-GRE o WCCP-L2 automáticamente. La opción principal es entre la *operación de unidifusión* (en la que el dispositivo está configurado con la dirección IP de cada enrutador) o la *operación de multidifusión* (en la que tanto el dispositivo como los enrutadores están configurados con la dirección de multidifusión).

Operación normal (unidifusión): Para el funcionamiento normal, el procedimiento consiste en declarar WCCP versión 2 y el Id. de grupo WCCP para el router en su conjunto y, a continuación, habilitar la redirección en cada interfaz WAN. A continuación se muestra un ejemplo de Cisco IOS:

```
1  config term
2  ip wccp version 2
3  ! We will configure the appliance to use group 51 for TCP and 52 for
      UDP.
4  ip wccp 51
5  ip wccp 52
6
7  ! Repeat the following three lines for each WAN interface
8  ! you wish to accelerate:
9  interface your_wan_interface
10 ! If Reverse Path Forwarding is enabled (with an ip verify unicast
11 ! source reachable ” statement), delete or comment out the statement:
12 ! ip verify unicast source reachable-via any
13 ! Repeat on all ports.
14
15 ip wccp 51 redirect out
16 ip wccp 51 redirect in
17 ip wccp 52 redirect out
18 ip wccp 52 redirect in
19
```



```
! If the appliance is inline with one of the router interfaces
! (NOT SUPPORTED), add the following line for that interface
! to prevent loops:
ip wccp redirect exclude in
^Z
<!--NeedCopy-->
```

Si varios enrutadores van a utilizar el mismo dispositivo, cada uno se configura como se muestra anteriormente, mediante los mismos grupos de servicio o diferentes.

Operación de multidifusión: Cuando se proporciona al dispositivo y a cada enrutador una dirección de multidifusión, la configuración es ligeramente diferente a la de la operación normal. A continuación se muestra un ejemplo de Cisco IOS:

```
config term
ip wccp version 2
ip wccp 51 group-address 225.0.0.1

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable ” statement), delete or comment out the statement:
! ip verify unicast source reachable-via any

ip wccp 51 redirect out
ip wccp 51 redirect in
!
! The following line is needed only on the interface facing the other
    router,
! if there is another router participating in this service group.
ip wccp 51 group-listen

!If the appliance is inline with one of the router interfaces,
!(which is supported but not recommended), add
!the following line for that interface to prevent loops:
ip wccp redirect exclude in
^Z
<!--NeedCopy-->
```

Procedimiento de configuración básico para el modo WCCP en el dispositivo SD-WAN

Para la mayoría de los sitios, puede utilizar el procedimiento siguiente para configurar el modo WCCP en el dispositivo. El procedimiento tiene que establecer varios parámetros en valores predeterminados sensibles. Es posible que las implementaciones avanzadas requieran que establezca estos parámetros en otros valores. Por ejemplo, si el router ya utiliza el grupo de servicios 51 de WCCP, deberá utilizar un valor diferente para el dispositivo.

Para configurar el modo WCCP en el dispositivo:

1. En la página Configuración: Configuración del equipo: WCCP.
2. Si no se han definido grupos de servicios, aparece la página Seleccionar Modo. Las opciones son Single SD-WAN y Cluster (Múltiples SD-WAN). Seleccione SD-WAN único. Se le lleva a la página del WCCP.
   Nota: Las etiquetas de modo son engañosas. El modo SD-WAN único también se utiliza para pares de alta disponibilidad SD-WAN.
3. Si el modo WCCP no está habilitado, haga clic en **Habilitar**.
4. Haga clic en **Agregar grupo de servicios**.
5. Los valores predeterminados de interfaz (apA), Protocolo (TCP), Prioridad WCCP (0), Comunicación del router (Unicast), (Contraseña en blanco) y Tiempo de vida (1) normalmente no tienen que cambiarse para el primer grupo de servicios que cree, pero si lo hacen, escriba nuevos valores en los campos proporcionados.
6. En el campo **Dirección del enrutador** (si está utilizando unidifusión) o en el campo **Dirección de multidifusión** (si está utilizando multidifusión), escriba la dirección IP del enrutador. Utilice la IP para el puerto del router utilizado para la comunicación WCCP con el dispositivo.
7. Si más de un enrutador utiliza WCCP para comunicarse con este dispositivo, agregue más enrutadores ahora.
8. Si los enrutadores tienen requisitos especiales, configure los campos Reenvío del enrutador (Auto/GRE/Level-2), Retorno del paquete del enrutador (Auto/GRE/Level-2) y Asignación del enrutador (Máscara/Hash) en consecuencia. Los valores predeterminados producen resultados óptimos con la mayoría de los enrutadores.
9. Haga clic en **Agregar**.
10. Repita los pasos anteriores para crear otro grupo de servicios, para el tráfico UDP (por ejemplo, Id. de grupo de servicios 52 y UDP de protocolo).
11. Vaya a la página Supervisión: Rendimiento del equipo: WCCP. El campo **Estado** debe cambiar a Conectado en 60 segundos.
12. Envíe tráfico a través del vínculo y, en la página Conexiones, compruebe que las conexiones están llegando y se están acelerando.

Detalles de configuración del grupo de servicios WCCP

En un grupo de servicios, un enrutador WCCP y un dispositivo SD-WAN (“WCCP Cache”en terminología WCCP) negocian atributos de comunicación (capacidades). El enrutador anuncia sus capacidades en el mensaje Le veo. Los atributos de comunicación son:

- Método de reenvío: GRE o Level-2
- Método de devolución de paquetes (solo multidifusión): GRE o Level-2
- Método de asignación: Hash o máscara
- Contraseña (el valor predeterminado es none)

El dispositivo activa una alerta si detecta una incompatibilidad entre sus atributos y los del enrutador. El dispositivo puede ser incompatible debido a un atributo específico de un grupo de servicios (como GRE o Level-2). Más raramente, en un grupo de servicios de multidifusión, se puede activar una alerta cuando la selección Auto elige un atributo particular con un enrutador determinado conectado, pero el atributo es incompatible con un enrutador posterior.

Las siguientes son las reglas básicas para los atributos de comunicación dentro de un dispositivo SD-WAN.

Para el reenvío del router:

- Cuando se selecciona Automático, la preferencia es para el nivel 2, ya que es más eficiente tanto para el enrutador como para el dispositivo. El nivel 2 se negocia si el enrutador lo admite y el enrutador se encuentra en la misma subred que el dispositivo.
- Los enrutadores de un grupo de servicios de unidifusión pueden negociar diferentes métodos si se selecciona Auto.
- Los enrutadores de un grupo de servicios de multidifusión deben utilizar el mismo método, ya sea forzado con GRE o Nivel-2 o, con Automático, según determine el primer enrutador del grupo de servicios que se conecte.
- Para una incompatibilidad, una alerta anuncia que el enrutador tiene reenvío de enrutador incompatible.

Para la asignación de enrutadores:

- El valor predeterminado es Hash.
- Cuando se selecciona Auto, el modo se negocia con el enrutador.
- Todos los enrutadores de un grupo de servicios deben admitir el mismo método de asignación (Hash o Mask).
- Para cualquier grupo de servicios, si este atributo está configurado como Automático, el dispositivo selecciona Hash o Máscara cuando se conecta el primer enrutador. Hash se elige si el enrutador lo admite. De lo contrario, se selecciona Máscara. El problema de que los enrutadores subsiguientes sean incompatibles con el método seleccionado automáticamente se puede minimizar seleccionando manualmente un método común a todos los enrutadores del grupo de servicios.
- Para una incompatibilidad, una alerta anuncia que el enrutador tiene un método de asignación de enrutador incompatible.
- Con cualquiera de los dos métodos, el dispositivo único del grupo de servicios indica a todos los enrutadores del grupo de servicios que dirijan todos los paquetes TCP o UDP al dispositivo. Los enrutadores pueden modificar este comportamiento con listas de acceso o seleccionando qué interfaces redirigir al grupo de servicios.

Para el método Mask, el dispositivo negocia la máscara dirección IP de origen. El dispositivo no proporciona ningún mecanismo para seleccionar dirección IP de destino o los puertos para el origen o el destino. La máscara dirección IP de origen no identifica específicamente ninguna dirección IP o rango específicos. El protocolo no proporciona un medio para especificar una dirección IP específica. De forma predeterminada, dado que solo hay un único dispositivo en el grupo de servicios, se utiliza una máscara de un bit para conservar los recursos del enrutador. (La versión 6.0 utiliza una máscara más grande).

Para contraseña:

- Si el router requiere una contraseña, la contraseña definida en el dispositivo debe coincidir. Si el enrutador no requiere una contraseña, el campo de contraseña del dispositivo debe estar en blanco.

Pruebas y solución de problemas de WCCP

Cuando se trabaja con WCCP, el dispositivo proporciona diferentes formas de supervisar el estado de la interfaz WCCP, y el router también debe proporcionar información.

Página**Supervisión: Rendimiento del Equipo: Página WCCP**: La página WCCP informa del estado actual del vínculo WCCP e informa de la mayoría de los problemas.

Entradas de Registro: La página Supervisión: Rendimiento del Equipo: Registro muestra una nueva entrada cada vez que se establece o pierde el modo WCCP.

Ilustración 1. Entradas de registro de WCCP (el formato varía un poco con la versión)

Estado del router: En el router, el comando show ip wccp muestra el estado del enlace WCCP:

```
Router>enable
Password:
Router#show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  172.16.2.4
        Protocol Version:                   2.0

    Service Identifier: 51
        Number of Cache Engines:            0
        Number of routers:                  0
        Total Packets Redirected:           19951
        Redirect access-list:               -none-
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
<!--NeedCopy-->
```


Verificar el modo WCCP

Puede supervisar la configuración de WCCP desde la GUI de SD-WAN.

Para supervisar la configuración de WCCP

1. Acceda a la página **Supervisión > Rendimiento del dispositivo > WCCP**.
2. Seleccione una caché y haga clic en **Obtener información**. Una página Estado de caché muestra la configuración de WCCP, como se muestra en la siguiente imagen.
3. Inicie el tráfico que debe reenviarse a través del dispositivo SD-WAN y supervise la conexión en la página **Supervisión > Optimización > Conexiones**.
   - Si las conexiones se muestran en la ficha **Conexiones aceleradas**, es un indicador de que todo está funcionando.
   - Si las conexiones se encuentran en la ficha **Conexiones no aceleradas**, consulte la columna **Detalles**. Un mensaje de asimetría de enrutamiento detectado implica que falta una de las líneas de redireccionamiento ip wccp en el router o tiene un error, o que el tráfico cliente-servidor y servidor-cliente toman diferentes rutas.
   - Si no se muestra ninguna conexión, pero el dispositivo informa de que está conectado al enrutador y la página de supervisión de WCCP no muestra ningún error, probablemente el problema esté relacionado con la configuración del enrutador.

Agrupación en clústeres de WCCP

December 14, 2022

La función de agrupación en clústeres WCCP le permite multiplicar la capacidad de aceleración asignando más de un dispositivo SD-WAN a los mismos vínculos. Puede agrupar hasta 32 dispositivos idénticos, hasta 32 veces la capacidad. Debido a que utiliza el estándar WCCP 2.0, la agrupación en clústeres WCCP funciona en la mayoría de los enrutadores y algunos conmutadores inteligentes, lo más probable es que incluya aquellos que ya está utilizando.

Debido a que utiliza un protocolo descentralizado, la agrupación en clústeres WCCP permite agregar o quitar dispositivos SD-WAN a voluntad. Si un dispositivo falla, su tráfico se redirecciona a los dispositivos restantes.

A diferencia de la alta disponibilidad SD-WAN, un par activo/pasivo que utiliza dos dispositivos para proporcionar el rendimiento de un solo dispositivo, los mismos dispositivos implementados como un clúster WCCP tienen el doble de rendimiento que un único dispositivo, lo que ofrece redundancia y rendimiento mejorado.

Además de agregar más dispositivos a medida que aumentan las necesidades de su sitio, puede usar la función Pagar a medida que crece de Citrix para aumentar las capacidades de sus dispositivos mediante actualizaciones de licencias.

Se recomienda Citrix Command Center para administrar clústeres WCCP. La siguiente imagen muestra una red básica de un clúster de dispositivos SD-WAN en modo WCCP, administrada mediante Citrix Command Center.

Ilustración 1. Clúster SD-WAN administrado mediante Citrix Command Center

Clústeres WCCP con equilibrio de carga

El protocolo WCCP admite hasta 32 dispositivos en una matriz tolerante a errores y equilibrada de carga llamada clúster. En el ejemplo siguiente, tres dispositivos idénticos (el mismo modelo, la misma versión de software) se cablean de forma idéntica y se configuran de forma idéntica, excepto para sus direcciones IP. Los dispositivos que utilizan los mismos grupos de servicio con el mismo enrutador pueden convertirse en un clúster WCCP con equilibrio de carga. Cuando un nuevo dispositivo se registra en el router, puede unirse al grupo de dispositivos existente y recibir su parte de tráfico. Si un dispositivo sale de la red (como indica la ausencia de señales de latido), el clúster se reequilibra para que solo se utilicen los dispositivos restantes.

Imagen 2. Un clúster WCCP con equilibrio de carga con tres dispositivos

Se selecciona un dispositivo del clúster como caché designada y controla el comportamiento de equilibrio de carga de los dispositivos del clúster. La caché designada es el dispositivo con la dirección IP más baja. Dado que los dispositivos tienen configuraciones idénticas, no importa cuál es la caché designada. Si la caché designada actual se desconecta, un dispositivo diferente se convierte en la caché designada.

La caché designada determina cómo se asigna el tráfico equilibrado de carga e informa al router de estas decisiones. El enrutador comparte información con todos los miembros del clúster, por lo que el clúster puede funcionar incluso si la caché designada se desconecta.

> **Nota**: Como se configura normalmente, un dispositivo SD-WAN 4000/5000 aparece como dos cachés WCCP en el router.

Algoritmo de equilibrio de carga

El equilibrio de carga en WCCP es estático, excepto cuando un dispositivo entra o sale del clúster, lo que hace que el clúster se vuelva a equilibrar entre sus miembros actuales.

El estándar WCCP admite el equilibrio de carga basado en una máscara o un hash. Por ejemplo, la agrupación en clústeres WCCP de SD-WAN utiliza únicamente el método de máscara, mediante una

máscara de 1-6 bits de la dirección IP de 32 bits. Estos bits de dirección pueden ser no consecutivos. Todas las direcciones que dan el mismo resultado cuando se enmascaran se envían al mismo dispositivo. La eficacia del equilibrio de carga depende de la elección de un valor de máscara adecuado: Una elección de máscara deficiente puede resultar en un equilibrio de carga deficiente o incluso en ninguno, con todo el tráfico enviado a un único dispositivo.

Topología de implementación

Dependiendo de la topología de red, puede implementar el clúster WCCP con un único enrutador o con varios enrutadores. Tanto si está conectado a un único enrutador como a varios enrutadores, cada dispositivo del clúster debe estar conectado de manera idéntica a todos los enrutadores en uso.

Implementación de un solo enrutador

En el siguiente diagrama, tres dispositivos SD-WAN aceleran la WAN de 200 Mbps del centro de datos. El sitio admite 750 usuarios de Virtual Apps.

Como se muestra en la Hoja de datos de SD-WAN, un SD-WAN 3000-100 admite usuarios de 100 Mbps y 400, por lo que un par de estos dispositivos admite usuarios de 200 Mbps y 800, lo que satisface los requisitos del centro de datos de un enlace de 200 Mbps y 750 usuarios.

Sin embargo, para la tolerancia a fallos, el clúster WCCP debe seguir funcionando sin sobrecargarse si falla un dispositivo. Esto se puede lograr mediante el uso de tres dispositivos cuando los cálculos requieren dos. Esto se denomina regla N+1.

El fracaso es un evento inusual, por lo que generalmente los tres dispositivos están en funcionamiento. En este caso, cada dispositivo admite solo 67 Mbps y 250 usuarios, lo que deja mucho margen de ampliación y hace buen uso del hecho de que el clúster tiene tres veces la potencia de CPU y tres veces el historial de compresión de un único dispositivo.

Sin clústeres WCCP, tanta capacidad y tolerancia a fallos requerirían un par de dispositivos SD-WAN 4000-500 en modo de alta disponibilidad. Solo uno de estos dispositivos está activo a la vez.

Implementaciones de varios enrutadores

El uso de varios enrutadores WAN es similar al uso de un único enrutador WAN. Si se cambia el ejemplo anterior para incluir dos enlaces de 100 Mbps en lugar de un vínculo de 200 Mbps, la topología cambia, pero los cálculos no.

Limitaciones

La configuración de dispositivos en un clúster WCCP tiene las siguientes limitaciones:

- Todos los dispositivos de un clúster deben ser del mismo modelo y utilizar la misma versión de software.
- La sincronización de parámetros entre dispositivos dentro del clúster no es automática. Utilice el Command Center para administrar los dispositivos como un grupo.
- El modelado del tráfico SD-WAN no es efectivo, ya que depende de controlar todo el enlace como una unidad, y ninguno de los dispositivos está en condiciones de hacerlo. Se puede utilizar QoS del router en su lugar.
- Los algoritmos de equilibrio de carga basados en WCCP no varían dinámicamente con la carga, por lo que lograr un buen equilibrio de carga puede requerir algún ajuste.
- No se admite el método hash de asignación de caché. La asignación de máscara es el método admitido.
- Mientras que el estándar WCCP permite longitudes de máscara de 1 a 7 bits, el dispositivo admite máscaras de 1 a 6 bits.
- No se admiten grupos de servicios de multidifusión. Solo se admiten grupos de servicios de unidifusión.
- Todos los enrutadores que utilicen el mismo par de grupos de servicios deben admitir el mismo método de reenvío (GRE o L2).
- El método de reenvío y devolución negociado con el router debe coincidir: Ambos deben ser GRE o ambos deben ser L2. Algunos routers no admiten L2 en ambas direcciones, lo que da como resultado un error de Desajuste de la capacidad de reenvío o devolución del router o asignación. En este caso, el grupo de servicios debe configurarse como GRE.
- SD-WAN VPX no admite la agrupación en clústeres WCCP.
- El dispositivo admite (y negocia) solo asignaciones de caché no ponderadas (iguales). No se admiten asignaciones ponderadas.
- Algunos dispositivos antiguos, como el SD-WAN 700, no admiten la agrupación en clústeres WCCP.
- (Solo SD-WAN 4000/5000) Se requieren dos instancias de acelerador por interfaz en modo L2. Se admiten tres interfaces por dispositivo (y, a continuación, solo en dispositivos con seis o más instancias de acelerador).
- (solo SD-WAN 4000/5000) Los paquetes de control WCCP del enrutador deben coincidir con una de las direcciones IP del enrutador configuradas en el dispositivo para el grupo de servicios. En la práctica, se debe usar la dirección IP del enrutador para la interfaz que lo conecta al dispositivo. No se puede utilizar la IP de loopback del router.

Limitaciones de la hoja de trabajo de implementación y del clúster

En la siguiente hoja de cálculo, puede calcular el número de dispositivos necesarios para la instalación y el tamaño de campo de máscara recomendado. El tamaño de máscara recomendado es de 1 a 2 bits más grande que el tamaño mínimo de máscara para su instalación.

Parámetro	Valor	Notas
Modelo de dispositivo utilizado		—
Usuarios de Citrix Virtual Apps and Desktops compatibles por dispositivo	Uspec =	De la hoja de datos
Usuarios de Citrix Virtual Apps and Desktops en WAN Link	Uwan =	—
Factor de sobrecarga de usuario	Uoverload = Uwan/Uspec =	—
BW admitido por dispositivo	BWspec =	De la hoja de datos
Enlace WAN BW	BWwan =	—
Factor de sobrecarga BW	BWoverload = BWwan/BWspec =	—
Número de dispositivos necesarios	N = max(Uoverload, BWoverload) +1 =	Incluye uno de más
		—
Número mínimo de cubos	Bmin = N, redondeado una potencia de 2 =	—
Si SD-WAN 4000 o 5000,	Bmin = 2N, redondeado a una potencia de 2 =	—
Valor recomendado	B = 4 Bmin si Bmin <= 16, de lo contrario 2 Bmin =	—
Número de bits uno en la máscara de direcciones	M = log2 (B)	Si B=16, M=4.

Valor de máscara: El valor de máscara es una máscara de dirección de 32 bits con varios bits uno iguales a M en la hoja de cálculo proporcionada anteriormente. A menudo, estos bits pueden ser los bits menos significativos en la máscara de subred WAN utilizada por los sitios remotos. Si las máscaras de los sitios remotos varían, utilice la máscara mediana. (Ejemplo: Con /24 subredes, los bits menos significativos de la subred son 0x00 00 nn 00. El número de bits a establecer en uno es log2 (tamaño de máscara): Si el tamaño de máscara es 16, establezca 4 bits en uno. Por lo tanto, con un tamaño de máscara de 16 y una subred /24, establezca el valor de máscara en 0x00 00 0f 00.)

Las directrices anteriores solo funcionan si el campo de subred seleccionado se distribuye uniformemente en el tráfico, es decir, que cada bit de dirección seleccionado por la máscara es uno para la mitad de los hosts remotos y un cero para la otra mitad. De lo contrario, el equilibrio de carga se ve

afectado. Esta distribución uniforme podría ser cierta para solo unos pocos bits en el campo de red (solo 2 bits). Si es así con su red, en lugar de enmascarar bits en el área ofensiva del campo de subred, desplace esos bits a una parte del campo de dirección de host que tenga la propiedad 50/50. Por ejemplo, si solo tres bits de subred en una subred /24 tienen la propiedad 50/50 y utiliza cuatro bits de máscara, una máscara de 0x00 00 07 10 evita el bit ofensivo en 0x00 00 0800 y lo desplaza a 0x00 00 00 10, una parte del campo de dirección que es probable que tenga la propiedad 50/50 si sus subredes remotas generalmente usan al menos 32 direcciones IP cada una.

Parámetro	Valor	Notas
Valor final de máscara		—
Puente acelerado		Por lo general apA
Grupo de servicios WAN		Un grupo de servicios que aún no esté en uso en el router (51-255)
Grupo de servicios LAN		Otro grupo de servicios no utilizado
Dirección IP del router		Dirección IP de la interfaz del router en el puerto frente al dispositivo
Protocolo WCCP (generalmente Auto)		—
Algoritmo DC		Utilice Deterministic si solo tiene dos dispositivos o está utilizando equilibrio de carga dinámico como HSRP o GSLB. De lo contrario, utilice Menos disruptivo.

La configuración de dispositivos en un clúster WCCP tiene las siguientes limitaciones:

- Todos los dispositivos de un clúster deben ser del mismo modelo y utilizar la misma versión de software.
- La sincronización de parámetros entre dispositivos dentro del clúster no es automática. Utilice el Command Center para administrar los dispositivos como un grupo.
- El modelado del tráfico SD-WAN no es efectivo, ya que depende de controlar todo el enlace como una unidad, y ninguno de los dispositivos está en condiciones de hacerlo. Se puede utilizar QoS del router en su lugar.

- Los algoritmos de equilibrio de carga basados en WCCP no varían dinámicamente con la carga, por lo que lograr un buen equilibrio de carga puede requerir algún ajuste.
- No se admite el método hash de asignación de caché. La asignación de máscara es el método admitido.
- Mientras que el estándar WCCP permite longitudes de máscara de 1 a 7 bits, el dispositivo admite máscaras de 1 a 6 bits.
- No se admiten grupos de servicios de multidifusión; solo se admiten grupos de servicios de unidifusión.
- Todos los enrutadores que utilicen el mismo par de grupos de servicios deben admitir el mismo método de reenvío (GRE o L2).
- El método de reenvío y devolución negociado con el router debe coincidir: Ambos deben ser GRE o ambos deben ser L2. Algunos routers no admiten L2 en ambas direcciones, lo que da como resultado un error de Desajuste de la capacidad de reenvío o devolución del router o asignación. En este caso, el grupo de servicios debe configurarse como GRE.
- SD-WAN VPX no admite la agrupación en clústeres WCCP.
- El dispositivo admite (y negocia) solo asignaciones de caché no ponderadas (iguales). No se admiten asignaciones ponderadas.
- Algunos dispositivos antiguos, como el SD-WAN 700, no admiten la agrupación en clústeres WCCP.
- (SD-WAN WANOP 4000/5000 solamente) Se requieren dos instancias de acelerador por interfaz en modo L2. No se admiten más de tres interfaces por dispositivo (y, a continuación, en dispositivos con seis o más instancias de acelerador).
- (solo SD-WAN 4000/5000) Los paquetes de control WCCP del enrutador deben coincidir con una de las direcciones IP del enrutador configuradas en el dispositivo para el grupo de servicios. En la práctica, se debe usar la dirección IP del enrutador para la interfaz que lo conecta al dispositivo. No se puede utilizar la IP de loopback del router.

Pruebas y solución de problemas

La página **Supervisión** > **Dispositivo** > **Rendimiento de la aplicación** > **WCCP** muestra el estado actual no solo del dispositivo local sino de todos los demás dispositivos que se han unido al clúster. Seleccione una caché de WCCP y haga clic en **Obtener información**.

La ficha Estado de caché muestra el estado del dispositivo local. Cuando todo está bien, el estado es 25: Tiene asignación. Debe actualizar la página manualmente para supervisar los cambios en el estado. Si el dispositivo no alcanza el estado 25: Tiene asignación dentro de un período de tiempo de espera, se mostrarán otros mensajes de estado informativos.

Se muestra información adicional al hacer clic en las fichas **Grupo de servicios o Routers**.

La ficha Resumen del clúster muestra información sobre el clúster WCCP en su conjunto. Como

efecto secundario del protocolo WCCP, cada miembro del clúster tiene información sobre todos los demás, por lo que esta información se puede supervisar desde cualquier dispositivo del clúster.

Su router también puede proporcionar información de estado. Consulte la documentación de su router.

Configurar clústeres de WCCP

Después de finalizar la topología de implementación, considerar todas las limitaciones y completar la hoja de trabajo de implementación, estará listo para implementar los dispositivos en un clúster WCCP. Para configurar el clúster WCCP, debe realizar las siguientes tareas:

- Configuración de las instancias de NetScaler
- Configuración del router
- Configuración del dispositivo

Modo virtual en línea

April 23, 2021

> **Nota**: Utilice el modo virtual en línea solo cuando el modo en línea y el modo WCCP no sean prácticos. No mezcle los modos en línea y virtual en línea dentro del mismo dispositivo. Sin embargo, puede mezclar los modos virtual en línea y WCCP dentro del mismo dispositivo. Citrix no recomienda el modo virtual en línea con enrutadores que no admitan la supervisión del estado.

En el modo virtual en línea, el enrutador utiliza reglas de enrutamiento basado en directivas (PBR) para redirigir el tráfico WAN entrante y saliente al dispositivo para acelerar, y el dispositivo reenvía los paquetes procesados al enrutador. Casi todas las tareas de configuración se realizan en el enrutador. Lo único que se debe configurar en el dispositivo es el método de reenvío y se recomienda el método predeterminado.

Al igual que WCCP, la implementación virtual en línea no requiere recableado ni tiempo de inactividad, y proporciona una solución para los problemas de enrutamiento asimétrico que se enfrentan en una implementación con dos o más enlaces WAN. A diferencia de WCCP, no contiene supervisión de estado ni comprobación de estado incorporada, lo que dificulta la solución de problemas. WCCP es, por tanto, el modo recomendado, y virtual en línea solo se recomienda cuando los modos en línea y WCCP no son prácticos.

Ejemplo

La siguiente imagen muestra una red sencilla en la que todo el tráfico destinado al sitio remoto o recibido desde él se redirige al dispositivo. En este ejemplo, tanto el sitio local como el sitio remoto utilizan el modo virtual en línea.

Ilustración 1. Ejemplo virtual en línea

A continuación se presentan algunos detalles de configuración para la red en este ejemplo:

- Los sistemas de punto final tienen sus puertas de enlace establecidas en el enrutador local (que no es exclusivo del modo virtual en línea).
- Cada router está configurado para redirigir el tráfico WAN entrante y saliente al dispositivo local.
- Cada dispositivo procesa el tráfico recibido de su router local y lo reenvía al router.
- Las reglas PBR configuradas en el enrutador evitan los bucles de enrutamiento al permitir que los paquetes realicen un solo viaje hacia y desde el dispositivo. Los paquetes que el dispositivo reenvía al enrutador se envían a su destino original (local o remoto).
- Cada dispositivo tiene su Gateway predeterminada establecida en la dirección del enrutador local, como de costumbre (en la página **Configuración: Adaptadores de red**). Las opciones para reenviar paquetes al router son Return to Ethernet Sender y Send to Gateway.

Configurar el reenvío de paquetes en el dispositivo

April 23, 2021

El modo virtual en línea ofrece dos opciones de reenvío de paquetes:

Volver al remitente Ethernet (predeterminado): Este modo permite que varios enrutadores compartan un dispositivo. El dispositivo reenvía los paquetes de salida virtual en línea al lugar de origen, como indica la dirección Ethernet del paquete entrante. Si dos enrutadores comparten un único dispositivo, cada uno obtiene su propio tráfico, pero no el tráfico del otro enrutador. Este modo también funciona con un único enrutador.

Enviar a Gateway (no recomendado): En este modo, los paquetes de salida en línea virtuales se reenvían a la puerta de enlace predeterminada para su entrega, incluso si están destinados a hosts de la subred local. Esta opción suele ser menos deseable que la opción Return to Ethernet Sender, ya que agrega un elemento de complejidad fácilmente olvidado a la estructura de enrutamiento.

Para especificar la opción de reenvío de paquetes: En la página Configuración: Reglas de Optimización: Ajuste, junto a Virtual en línea, seleccione Volver al remitente Ethernet o Enviar a Gateway.

Configurar el router

April 23, 2021

El router tiene tres tareas cuando admite el modo virtual en línea:

1. Debe reenviar el tráfico WAN entrante y saliente al dispositivo SD-WAN.
2. Debe reenviar el tráfico SD-WAN a su destino (WAN o LAN).
3. Debe supervisar el estado del dispositivo para que se pueda omitir el dispositivo si falla.

Reglas basadas en directivas

En el modo virtual en línea, los métodos de reenvío de paquetes pueden crear bucles de enrutamiento si las reglas de enrutamiento no distinguen entre un paquete que ha sido reenviado por el dispositivo y otro que no lo ha hecho. Puede usar cualquier método que haga esa distinción.

Un método típico consiste en dedicar uno de los puertos Ethernet del router al dispositivo y crear reglas de enrutamiento basadas en el puerto Ethernet al que llegan los paquetes. Los paquetes que llegan a la interfaz dedicada al dispositivo nunca se reenvían al dispositivo, pero pueden serlo los paquetes que llegan a cualquier otra interfaz.

El algoritmo básico de enrutamiento es:

- No reenvíe paquetes desde el dispositivo al dispositivo.
- Si el paquete llega de la WAN, reenviarlo al dispositivo.
- Si el paquete está destinado a la WAN, reenvíe al dispositivo.
- No reenvíe el tráfico de LAN a LAN al dispositivo.
- El modelado del tráfico no es efectivo a menos que todo el tráfico WAN pase a través del dispositivo.

> **Nota**: Al considerar las opciones de enrutamiento, tenga en cuenta que los datos devueltos, no solo los datos salientes, deben fluir a través del dispositivo. Por ejemplo, colocar el dispositivo en la subred local y designarlo como el enrutador predeterminado para los sistemas locales no funciona en una implementación virtual en línea. Los datos salientes fluirían a través del dispositivo, pero los datos entrantes lo omitirían. Para forzar los datos a través del dispositivo sin reconfigurar el router, utilice el modo en línea.

Supervisión de estado

Si el dispositivo falla, los datos no se deben enrutar a él. De forma predeterminada, el enrutamiento basado en directivas de Cisco no realiza ninguna supervisión del estado. Para habilitar la supervisión

del estado, defina una regla para supervisar la disponibilidad del dispositivo y especifique la opción verify-availability para el comando set ip next-hop. Con esta configuración, si el dispositivo no está disponible, no se aplica la ruta y se omite el dispositivo.

Importante: Citrix recomienda el modo virtual en línea solo cuando se utiliza con supervisión de estado. Muchos enrutadores que admiten enrutamiento basado en directivas no admiten la comprobación de estado. La función de supervisión de la salud es relativamente nueva. Se puso disponible en la versión 12.3(4)T del IOS de Cisco.

A continuación se muestra un ejemplo de una regla para supervisar la disponibilidad del dispositivo:

“‘ pre codeblock
!- Use a ping (ICMP echo) to see if appliance is connected track 123 rtr 1 reachabilit y ! rtr 1 type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now

```
Esta regla hace ping al dispositivo en 192.168.1.200 periódicamente. Puede probar con 123 para ver si la unidad está arriba.

## Ejemplos de enrutamiento

Los siguientes ejemplos ilustran la configuración de enrutadores Cisco para los sitios locales y remotos que se muestran en [Ejemplo virtual en línea](/es-es/citrix-sd-wan-wanop/11/cb-deployment-modes-con/br-adv-virt-inline-mode-con.html). Para ilustrar la supervisión del estado, la configuración del sitio local incluye la supervisión del estado, pero la configuración del sitio remoto no lo hace.

Nota: La configuración del sitio local supone que ya se ha configurado un monitor ping.

Los ejemplos se ajustan a la CLI del IOS de Cisco. Es posible que no sean aplicables a enrutadores de otros proveedores.

Sitio local, Comprobación de estado habilitada:

``` pre codeblock
!
! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
```


```

```
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
!- Now set the appliance as the next hop, if it's up.
set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
<!--NeedCopy-->
```

Sitio remoto (sin comprobación de estado):

“‘ pre codeblock

! This example does not use health-checking.

! Remember, health-checking is always recommended,

! so this is a configuration of last resort.

!

!

ip cef

!

interface FastEthernet0/0

ip address 20.20.20.5 255.255.255.0

ip policy route-map client_side_map

!

interface FastEthernet0/1

ip address 171.68.2.5 255.255.255.0

ip policy route-map wan_side_map

!

interface FastEthernet1/0

ip address 192.168.2.5 255.255.255.0

!

ip classless

ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!_

```
Cada uno de los ejemplos anteriores aplica una lista de acceso a un
    mapa de ruta y adjunta el mapa de ruta a una interfaz. Las listas de
     acceso identifican todo el tráfico que se origina en un sitio
    acelerado y termina en el otro (IP de origen 10.10.10.0/24 y destino
     20.20.20.0/24 o viceversa). Consulte la documentación de su router
    para obtener los detalles de las listas de acceso y los mapas de
    rutas.

Esta configuración redirige todo el tráfico IP correspondiente a los
    dispositivos. Si desea redirigir solo el tráfico TCP, puede cambiar
    la configuración de la lista de acceso de la siguiente manera (solo
    se muestra la configuración del lado remoto):

``` pre codeblock
!
 ip access-list extended client_side
 permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
 ip access-list extended wan_side
 permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
<!--NeedCopy-->
```

Tenga en cuenta que, para las listas de acceso, no se usan máscaras ordinarias. En su lugar, se utilizan máscaras comodín. Tenga en cuenta que al leer una máscara comodín en binario, “1”se considera un bit de no importa.


```

## Modo virtual en línea para entornos de múltiples WAN

April 23, 2021

Las empresas con varios vínculos WAN suelen tener directivas de enrutamiento asimétricas, lo que parece requerir que un dispositivo en línea esté en dos lugares a la vez. El modo virtual en línea resuelve el problema de enrutamiento asimétrico mediante la configuración del enrutador para enviar todo el tráfico WAN a través del dispositivo, independientemente del vínculo WAN utilizado. La siguiente imagen muestra un ejemplo simple de implementación de vínculos de varias WAN.

Los dos enrutadores de lado local redirigen el tráfico al dispositivo local. Los puertos FE 0/0 para ambos enrutadores están en el mismo dominio de difusión que el dispositivo. El dispositivo local debe utilizar la configuración virtual en línea predeterminada (Return to Ethernet Sender).

Ilustración 1. Modo en línea virtual con dos enrutadores WAN

## Modo virtual en línea y alta disponibilidad

April 23, 2021

El modo virtual en línea se puede utilizar en una configuración de alta disponibilidad (alta disponibilidad). La siguiente imagen muestra una implementación simple de alta disponibilidad. En el modo virtual en línea, un par de dispositivos actúa como un dispositivo virtual. La configuración del enrutador es la misma para un par de alta disponibilidad que para un solo dispositivo, excepto que la dirección IP virtual del par de alta disponibilidad, no la dirección IP de un dispositivo individual, se utiliza en las tablas de configuración del enrutador. En este ejemplo, los dispositivos locales deben utilizar la configuración virtual en línea predeterminada (Return to Ethernet Sender).

Ilustración 1. Ejemplo de alta disponibilidad

## Supervisión y solución de problemas

April 23, 2021

En el modo virtual en línea, a diferencia del modo WCCP, el dispositivo no proporciona supervisión virtual específica en línea. Para solucionar problemas de una implementación virtual en línea, inicie sesión en el dispositivo y utilice la página Panel para comprobar que el tráfico entra y sale del dispositivo. Los errores de reenvío de tráfico suelen deberse a errores en la configuración del router.

Si las páginas Supervisión: Uso o Supervisión: Conexiones muestran que se está reenviando tráfico pero no se está produciendo aceleración (suponiendo que un dispositivo ya esté instalado en el otro extremo del vínculo WAN), compruebe que tanto el tráfico WAN entrante como el tráfico WAN saliente se reenvían a el dispositivo. Si solo se reenvía una dirección, no se puede acelerar.

Para probar la comprobación de estado, apague el dispositivo. El router debe dejar de reenviar el tráfico después de que el algoritmo de comprobación de estado se agote.

## Modo de grupo

April 23, 2021

En el modo de grupo, dos o más dispositivos se convierten en un único dispositivo virtual. Este modo es una solución al problema del enrutamiento asimétrico, que se define como cualquier caso en el que algunos paquetes de una conexión dada pasan a través de un dispositivo determinado, pero otros no. Una limitación de la arquitectura del dispositivo es que la aceleración no puede tener lugar a menos que todos los paquetes de una conexión dada pasen a través de los mismos dos dispositivos. El modo de grupo supera esta limitación.

El modo de grupo se puede utilizar con enlaces múltiples o redundantes sin reconfigurar los enrutadores.

> **Nota**
>
> El modo de grupo no es compatible con los dispositivos SD-WAN 4000 o 5000.

El modo de grupo solo se aplica a los dispositivos situados en un lado del vínculo WAN; los dispositivos locales no saben ni les importan si los dispositivos remotos utilizan el modo de grupo.

El modo de grupo utiliza un mecanismo de latido para comprobar que otros miembros del grupo están activos. Los paquetes se reenvían solo a los miembros activos del grupo.

Evitar el enrutamiento asimétrico es la razón principal para utilizar el modo de grupo, pero el modo de grupo no es el único método disponible para ese propósito. Si decide que es el mejor método para su entorno, puede habilitarlo estableciendo algunos parámetros. Si el mecanismo predeterminado para determinar qué dispositivo es responsable de una conexión determinada no proporciona una aceleración óptima, puede cambiar las reglas de reenvío.

Ilustración 1. Modo de grupo con vínculos redundantes

Imagen 2. Modo de grupo con vínculos no redundantes con posible enrutamiento asimétrico

Imagen 3. Modo de grupo en campus cercanos

## Cuándo utilizar el modo de grupo

April 23, 2021

Utilice el modo de grupo en el siguiente conjunto de circunstancias:

- Tiene varios vínculos WAN.
- Existe la posibilidad de enrutamiento asimétrico (un paquete en una conexión dada podría viajar a través de cualquiera de los enlaces).
- El modo de grupo parece más sencillo y práctico que las alternativas que utilizan un solo dispositivo.

Las alternativas son:

- Modo WCCP, en el que los enrutadores WAN envían el tráfico de dos o más vínculos al mismo dispositivo mediante el protocolo WCCP.
- Modo virtual en línea, en el que los enrutadores envían tráfico desde dos o más vínculos a través del mismo dispositivo (o par de alta disponibilidad).
- Varios puentes, donde cada vínculo pasa a través de un puente acelerado diferente en el mismo dispositivo.
- Agregación a nivel de LAN, que coloca un dispositivo (o un par de alta disponibilidad) más cerca de la LAN, antes del punto donde el tráfico WAN se divide en dos o más paths.

## Cómo funciona el modo de grupo

April 23, 2021

En el modo de grupo, los dispositivos que forman parte del grupo toman posesión de una parte de las conexiones del grupo. Si un dispositivo determinado es el propietario de una conexión, toma todas las decisiones de aceleración sobre esa conexión y es responsable de la compresión, el control de flujo, la retransmisión de paquetes, etc.

Si un dispositivo recibe un paquete para una conexión para la que no es el propietario, reenvía el paquete al dispositivo que es el propietario. El propietario examina el paquete, toma las decisiones de aceleración adecuadas y reenvía los paquetes de salida al dispositivo que no es propietario. Este proceso conserva la selección de enlaces realizada por el router, al tiempo que permite que el dispositivo propietario administre todos los paquetes de la conexión. Para los enrutadores, la introducción de los dispositivos no tiene consecuencias. Los enrutadores no necesitan reconfigurarse de ninguna manera, y los dispositivos no necesitan comprender el mecanismo de enrutamiento. Simplemente aceptan las decisiones de reenvío de los enrutadores.

Ilustración 1. Tráfico del lado del envío en modo de grupo

Imagen 2. Flujo de tráfico en el lado de recepción en modo de grupo

El modo de grupo tiene dos modos de error seleccionables por el usuario, que controlan la forma en que los miembros del grupo interactúan entre sí si uno de ellos falla. El modo de error también determina si la tarjeta de omisión del dispositivo fallido se abre (bloqueando el tráfico a través del dispositivo) o permanece cerrada (permitiendo que el tráfico pase). Los modos de fallo son:

**Continuar acelerando:** si un miembro del grupo falla, se abre su tarjeta de omisión y no pasa tráfico a través del dispositivo con error. El resultado es presumiblemente una conmutación por error si se utilizan enlaces redundantes. De lo contrario, el enlace es simplemente inaccesible. Los otros dispositivos del grupo continúan acelerándose. El algoritmo hash habitual maneja las condiciones cambiadas. (Es decir, se utiliza el antiguo algoritmo de hash, y si la unidad fallida se indica como propietario, se aplica un algoritmo de hash basado en el nuevo grupo más pequeño. Esto conserva tantas conexiones más antiguas como sea posible).

**No acelerar-** Si un miembro del grupo falla, su tarjeta de derivación se cierra, lo que permite que el tráfico pase sin aceleración. Dado que una ruta no acelerada introduce enrutamiento asimétrico, los demás miembros del grupo también entran en modo de paso a través cuando detectan el error.

## Activar el modo de grupo

April 23, 2021

Para habilitar el modo de grupo, cree un grupo de dos o más dispositivos. Un dispositivo puede ser miembro de un solo grupo. Los miembros del grupo se identifican mediante la dirección IP y el nombre común SSL en la licencia del dispositivo.

Todos los parámetros del modo de grupo se encuentran en la página Configuración: Modo de grupo, en la tabla Configuración: Modo de grupo.

Ilustración 1. Página Modo de grupo

### Para habilitar el modo de grupo

1. Seleccione la dirección que desea utilizar para la comunicación de grupo. En la parte superior de la tabla Configuración del modo de grupo de la ficha Configuración: Implementaciones avanzadas: Modo de grupo, la celda de la tabla bajo VIP miembro contiene la dirección de administración del puerto utilizado para comunicarse con otros miembros del grupo. Utilice el menú desplegable (sin etiqueta) para seleccionar la dirección correcta (por ejemplo, para utilizar el

puerto Aux1, seleccione la dirección IP asignada al puerto Aux1). A continuación, haga clic en Cambiar VIP.

2. Agregue al menos un miembro del grupo más a la lista. (Se admiten grupos de tres o más, pero rara vez se usan). En la siguiente celda de la columna VIP miembro, escriba la dirección IP del puerto utilizado por el otro dispositivo para la comunicación en modo de grupo.
3. Escriba el nombre común SSL del otro miembro del grupo en la columna Nombre común SSL. El nombre común SSL aparece en la ficha Configurar: Implementaciones avanzadas: Alta disponibilidad del otro dispositivo. Si el otro miembro del grupo es un par de alta disponibilidad, el nombre que aparece es el nombre común SSL del dispositivo principal.

   > **Nota**: Si el dispositivo local no forma parte de un par de alta disponibilidad, la primera celda del nombre común SSL secundario de alta disponibilidad está en blanco.Si el otro miembro del grupo es un par de alta disponibilidad, especifique el nombre común SSL del dispositivo secundario de alta disponibilidad en la opción de alta disponibilidad Columna de nombre común SSL secundario.

4. Haga clic en Agregar.
5. Repita los pasos 2 a 4 para cualquier dispositivo adicional o par de alta disponibilidad del grupo.
6. Los tres botones debajo de la lista de miembros del grupo son alternados, por lo que cada uno se etiqueta como el opuesto a su configuración actual:

   a) El botón superior dice: **No acelerar cuando se detecta un fallo de miembro** o **Continuar para acelerar cuando se detecta un fallo de miembro**. La configuración No acelerar… siempre funciona y no bloquea el tráfico, pero si algún miembro falla, los demás miembros del grupo pasan al modo de derivación, lo que provoca una pérdida completa de aceleración. Con la opción Continuar acelerando, el puente del dispositivo que falla se convierte en un circuito abierto y el enlace falla. Esta opción es apropiada si el enrutador WAN responde causando una conmutación por error. Se aceleran las nuevas conexiones y las conexiones abiertas pertenecientes a los dispositivos que sobreviven.
   b) El botón inferior ahora debe etiquetarse Desactivar modo de grupo. Si no es así, habilite el modo de grupo haciendo clic en el botón.

7. Actualice la pantalla. La parte superior de la página debe mostrar los asociados del modo de grupo, pero mostrar advertencias sobre su estado, porque aún no se han configurado para el modo de grupo. Por ejemplo, podría indicar que no se puede encontrar el asociado o que está ejecutando una versión de software diferente.
8. Repita este procedimiento con los demás miembros del grupo. Dentro de los 20 segundos siguientes a habilitar el último miembro del grupo, la línea Estado del modo de grupo debe mostrar NORMAL y los demás miembros del modo de grupo deben aparecer con Estado: On-Line y Configuración: OK.

# Reglas de reenvío

April 23, 2021

De forma predeterminada, el *propietario* de una conexión en modo de grupo se establece mediante un hash de las direcciones IP de origen y destino. Cada dispositivo del grupo utiliza el mismo algoritmo para determinar qué miembro del grupo posee una conexión determinada. Este método no requiere configuración. Opcionalmente, el propietario se puede especificar mediante reglas configurables por el usuario.

Dado que el hash en modo de grupo no es idéntico al utilizado por los equilibradores de carga, aproximadamente la mitad del tráfico tiende a reenviarse al dispositivo propietario en un grupo de dos dispositivos. En el peor de los casos, el reenvío hace que se duplique la carga en la interfaz LAN, lo que reduce a la mitad la velocidad máxima de reenvío del dispositivo para el tráfico WAN real.

Esta penalización de velocidad se puede reducir si se utilizan los puertos Ethernet Primary o Aux1 para el tráfico entre miembros del grupo. Por ejemplo, si tiene un grupo de dos dispositivos, puede utilizar un cable Ethernet para conectar los puertos primarios de las dos unidades y, a continuación, especificar el puerto primario en la página Modo de grupo de cada unidad. Sin embargo, se logra el máximo rendimiento si se minimiza la cantidad de tráfico reenviado entre los miembros del modo de grupo.

Opcionalmente, el propietario se puede establecer de acuerdo con reglas específicas basadas en IP/puerto. Estas reglas deben ser idénticas en todos los dispositivos del grupo. Cada miembro del grupo verifica que su configuración de modo de grupo sea idéntica a los demás. Si no todas las configuraciones son idénticas, ninguno de los dispositivos miembros entra en modo de grupo.

Si el tráfico llega primero al dispositivo que posee la conexión, se acelera y se reenvía normalmente. Si llega primero a un dispositivo diferente del grupo, se reenvía a su propietario a través de un túnel GRE, que lo acelera y lo devuelve al dispositivo original para reenviarlo. Por lo tanto, el modo de grupo deja sin cambios la selección de enlaces del enrutador.

El uso de reglas de reenvío basadas en IP explícitas puede reducir la cantidad de reenvío en modo de grupo. Esto es especialmente útil en casos de enlace principal/enlace de copia de seguridad, donde cada enlace maneja un rango determinado de direcciones IP, pero puede actuar como una copia de seguridad cuando el otro enlace está inactivo.

Ilustración 1. Selección de propietario basada en IP

Las reglas de reenvío pueden garantizar que los miembros del grupo solo manejen su tráfico natural. En muchas instalaciones, donde el tráfico suele enrutarse a través de su enlace normal y rara vez cruza el otro, estas reglas pueden reducir sustancialmente la sobrecarga.

Las reglas se evalúan en orden, de arriba a abajo, y se utiliza la primera regla coincidente. Las reglas

se comparan con un par opcional de direcciones IP/máscara (que se compara con las direcciones de origen y destino) y con un intervalo de puertos opcional.

Independientemente del orden de las reglas, si el dispositivo asociado no está disponible, el tráfico no se reenvía a él, independientemente de si una regla coincide o no.

Por ejemplo, en la imagen siguiente, el miembro 172.16.1.102 es el propietario de todo el tráfico hacia o desde su propia subred (172.16.1.0/24), mientras que el miembro 172.16.0.184 es el propietario del resto del tráfico.

Si un paquete llega a la unidad 172.16.1.102 y no se dirige a/desde net 172.16.1.0/24, se reenvía a 172.16.0.184.

Sin embargo, si la unidad 172.16.0.184 falla, la unidad 172.16.1.102 ya no reenvía paquetes. Intenta manejar el tráfico en sí mismo. Este comportamiento se puede inhibir haciendo clic en **No acelerar cuando se detecta un fallo de miembro** en la ficha Modo de grupo.

En una instalación con un vínculo WAN principal y un vínculo WAN de copia de seguridad, escriba las reglas de reenvío para enviar todo el tráfico al dispositivo en el vínculo principal. Si se produce un error en el vínculo WAN principal, pero el dispositivo principal no, el enrutador WAN realiza una conmutación por error y envía tráfico a través del vínculo secundario. El dispositivo del vínculo secundario reenvía el tráfico al dispositivo de vínculo primario y la aceleración continúa sin interrupciones. Esta configuración mantiene conexiones aceleradas después de la conmutación por error del vínculo.

Imagen 2. Reglas de reenvío

## Modo de grupo de supervisión y solución de problemas

April 23, 2021

Se deben verificar dos cosas en una instalación en modo de grupo:

- Que los dos dispositivos han entrado en modo de grupo, que se puede determinar en la página Configuración: Implementaciones avanzadas: Modo de grupo de cualquiera de los dispositivos.
- Que el comportamiento del par de modo de grupo es el deseado cuando el otro miembro falla y cuando uno de los vínculos falla, tal como se determina desactivando el otro dispositivo y desconectando temporalmente uno de los vínculos, respectivamente.

## Personalizar los puertos Ethernet

April 23, 2021

Un dispositivo típico tiene cuatro puertos Ethernet: Dos puertos en puente acelerados, denominados *par acelerado A* (apA.1 y apA.2), con un relé de derivación (fallo a cable) y dos puertos de placa base no acelerados, llamados Primary y Aux1. Los puertos en puente proporcionan aceleración, mientras que los puertos de la placa base a veces se utilizan para fines secundarios. La mayoría de las instalaciones utilizan solo los puertos con puentes.

Algunas unidades SD-WAN tienen solo los puertos de la placa base. En este caso, los dos puertos de la placa base están conectados en puente.

Se puede acceder a la interfaz de usuario del dispositivo mediante una red VLAN o que no sea VLAN. Puede asignar una VLAN a cualquiera de los puertos con puentes o puertos de tarjeta madre del dispositivo para fines de administración.

Ilustración 1. Puertos Ethernet

### Lista de puertos

Los puertos se denominan de la siguiente manera:

| Puerto Ethernet | Nombre |
|---|---|
| Puerto 1 de la placa base | Principal (o apA.1 si no hay tarjeta de derivación) |
| Puerto 2 de la placa base | Auxiliary1 o Aux1 (o apA.2 si no hay tarjeta de derivación) |
| Puente #1 | Par acelerado A (apA, con puertos apA.1 y apA.2) |
| Puente #2 | Par acelerado B (apB, con puertos apB.1 y apB.2) |

Cuadro 1 Nombres de puertos Ethernet

## Cómo funciona el modo de alta disponibilidad

April 23, 2021

En un par de alta disponibilidad (alta disponibilidad), un dispositivo es primario y el otro es secundario. El primario supervisa su propio estado y el secundario. Si detecta un problema, el procesamiento del tráfico pasa por error al dispositivo secundario. Las conexiones TCP existentes finalizan. Para garantizar la conmutación por error correcta, los dos dispositivos mantienen sus configuraciones sincronizadas. En una configuración de alta disponibilidad en modo WCCP, el dispositivo que procesa el tráfico mantiene la comunicación con el enrutador ascendente.

**Supervisión de estado**: Cuando se habilita la alta disponibilidad, el dispositivo principal utiliza el protocolo VRRP para enviar una señal de latido al dispositivo secundario una vez por segundo. Además, el dispositivo principal supervisa el estado de la portadora de sus puertos Ethernet. La pérdida de transportista en un puerto previamente activo implica una pérdida de conectividad.

**Failover** Si se produce un error en la señal de latido del dispositivo principal o si el dispositivo principal pierde la portadora durante cinco segundos en cualquier puerto Ethernet previamente activo, el dispositivo secundario se hace cargo y se convierte en el principal. Cuando se reinicia el dispositivo con errores, se convierte en el secundario. La nueva primaria se anuncia en la red con una transmisión ARP. No se utiliza la suplantación de MAC. El puente Ethernet está inhabilitado en el dispositivo secundario, dejando el dispositivo principal como la única ruta para el tráfico en línea. La falla de cableado está inhibida en ambos dispositivos para evitar bucles.

> **Advertencia**
>
> La función de derivación Ethernet está desactivada en modo de alta disponibilidad. Si ambos dispositivos en un par de alta disponibilidad en línea pierden energía, se pierde la conectividad. Si se necesita conectividad WAN durante cortes de energía, al menos un dispositivo debe estar conectado a una fuente de alimentación de respaldo.
>
> **Nota**
>
> El dispositivo secundario del par de alta disponibilidad tiene uno de sus puertos de puente, el puerto apA.1, inhabilitado para evitar bucles de reenvío. Si el dispositivo tiene puentes dobles, apB.1 también está inhabilitado. En una instalación con un brazo, utilice el puerto apA.2. De lo contrario, el dispositivo secundario se vuelve inaccesible cuando se habilita la alta disponibilidad.

**Asignación primaria/secundaria**: Si se reinician ambos dispositivos, el primero en inicializarse completamente se convierte en el principal. Es decir, los dispositivos no tienen roles asignados y el primero en estar disponibles toma el relevo como principal. El dispositivo con la dirección IP más alta en la interfaz utilizada para el latido del VRRP se utiliza como desempate si ambos están disponibles al mismo tiempo.

**Terminación de conexión durante la conmutación por error**: Tanto las conexiones TCP aceleradas como las no aceleradas se terminan como un efecto secundario de la conmutación por error. Las sesiones no TCP no se ven afectadas, excepto por el retraso causado por el breve período (varios segundos) entre el error del dispositivo principal y la conmutación por error del dispositivo secundario.

Los usuarios experimentan el cierre de conexiones abiertas, pero pueden abrir nuevas conexiones.

**Sincronización de configuración**: Dos dispositivos sincronizan su configuración para asegurarse de que el secundario está listo para asumir el control del primario. Si la configuración del par se cambia a través de la interfaz basada en el explorador, el dispositivo principal actualiza el dispositivo secundario inmediatamente.

La alta disponibilidad no se puede habilitar a menos que ambos dispositivos ejecuten la misma versión de software.

**Alta disponibilidad en modo WCCP**: Cuando se utiliza WCCP con un par de alta disponibilidad, el dispositivo principal establece la comunicación con el router. El dispositivo utiliza su dirección IP de administración en apA o apB, no su dirección IP virtual, para comunicarse con el router. Tras la conmutación por error, el nuevo dispositivo principal establece la comunicación WCCP con el router.

## Requisitos de cableado

April 23, 2021

Los dos equipos del par de alta disponibilidad se instalan en la misma subred en una disposición paralela o en una disposición de un brazo, ambos se muestran en la imagen siguiente. En una disposición de un brazo, utilice el puerto apA.2 (y, opcionalmente, el puerto apB.2), no el puerto apA.1. Algunos modelos requieren una LAN de administración independiente, ya sea implementada en modo en línea o con un solo brazo. Esto se representa solo en el diagrama central.

Ilustración 1. Cableado para pares de alta disponibilidad

No rompa la topología anterior con conmutadores adicionales. No se admiten arreglos de conmutadores aleatorios. Cada uno de los conmutadores debe ser un único conmutador monolítico, un único conmutador lógico o parte del mismo chasis.

Si el protocolo de árbol de expansión (STP) está habilitado en los puertos del router o del switch conectados a los dispositivos, la conmutación por error funcionará, pero el tiempo de conmutación por error puede aumentar a aproximadamente treinta segundos. Sin STP, el tiempo de conmutación por error es de aproximadamente cinco segundos. Por lo tanto, para lograr el intervalo de conmutación por error más breve posible, inhabilite STP en los puertos que se conectan a los dispositivos.

## Otros requisitos

April 23, 2021

Ambos dispositivos en un par de alta disponibilidad deben cumplir los siguientes criterios:

- Tener hardware idéntico, como se muestra en la entrada Hardware del sistema en la página Panel.
- Ejecute exactamente la misma versión de software.
- Estar equipado con tarjetas de derivación Ethernet. Para determinar qué está instalado en los dispositivos, consulte la página Panel de control.

Los dispositivos que no admiten alta disponibilidad muestran una advertencia en la página Configuración: Alta disponibilidad.

## Acceso de administración al par de alta disponibilidad

April 23, 2021

Al configurar un par de alta disponibilidad (alta disponibilidad), asigne al par una dirección IP virtual (VIP), que le permite administrar los dos dispositivos como si fueran una sola unidad. Después de habilitar el modo de alta disponibilidad, la administración del dispositivo secundario a través de su dirección IP se inhabilita principalmente, con la mayoría de los parámetros atenuados. Un mensaje de advertencia muestra el motivo en cada página. Utilice el VIP de alta disponibilidad para todas las tareas de administración. Sin embargo, puede inhabilitar el estado de alta disponibilidad del dispositivo secundario desde su interfaz de administración.

## Configurar el par de alta disponibilidad

April 23, 2021

Puede configurar dos dispositivos recién instalados como un par de alta disponibilidad o puede crear un par de alta disponibilidad agregando un segundo dispositivo a una instalación existente.

Prerrequisitos: Instalación física y procedimientos básicos de configuración

Para configurar la alta disponibilidad

1. Asegúrese de que no hay más de un dispositivo conectado a las redes de tráfico (en los puentes acelerados). Si ambos están conectados, desconecte un cable de puente de los puentes activos del segundo dispositivo. Esto evitará el reenvío de bucles.
2. En la página Funciones del primer dispositivo, inhabilite Procesamiento de tráfico. Esto inhabilita la aceleración hasta que se configure el par de alta disponibilidad.
3. Repita el procedimiento para el segundo dispositivo.

4. En el primer dispositivo, vaya a la ficha Configuración: Implementaciones avanzadas: Alta disponibilidad, mostrada a continuación.
5. Marque la casilla Activado.
6. Haga clic en el enlace Configurar dirección IP virtual de alta disponibilidad y asigne una dirección IP virtual a la interfaz apA. Esta dirección se usará más adelante para controlar ambos dispositivos como una unidad.
7. Vuelva a la página Alta disponibilidad y, en el campo VRRP VRID, asigne un ID VRRP al par. Aunque el valor predeterminado es cero, el rango válido de números de ID VRRP es del 1 al 255. Dentro de este rango, puede especificar cualquier valor que no pertenezca a otro dispositivo VRRP de la red.
8. En el campo Nombre común SSL del socio, escriba el nombre común SSL del otro dispositivo, que se muestra en la ficha Configuración: Implementaciones avanzadas: Alta disponibilidad del dispositivo, en el campo Nombre común SSL del socio. Las credenciales SSL utilizadas aquí están instaladas de fábrica.
9. Haga clic en Update.
10. Repita los pasos 3 a 8 en el segundo dispositivo. Si administra el dispositivo a través de un puente acelerado (como apA), es posible que tenga que volver a conectar el cable Ethernet que eliminó en el paso 1 para conectarse al segundo dispositivo. Si es así, conecte este cable y desconecte el cable correspondiente del primer dispositivo.
11. Con su explorador, navegue hasta la dirección IP virtual del par de alta disponibilidad. Habilite el procesamiento de tráfico en la página Funciones. Cualquier configuración adicional se realizará desde esta dirección virtual.
12. Conecte el cable que quedó desconectado.
13. En cada dispositivo, la página Configuración: Implementaciones Avanzadas: Alta disponibilidad debería mostrar ahora que la alta disponibilidad está activa y que un dispositivo es el principal y el otro es el secundario. Si este no es el caso, aparece un banner de advertencia en la parte superior de la pantalla, indicando la naturaleza del problema.

Ilustración 1. Página de configuración de alta disponibilidad

## Actualizar software en un par de alta disponibilidad

April 23, 2021

La actualización del software SD-WAN en un par de alta disponibilidad provoca una conmutación por error en un momento durante la actualización.

Nota: Al hacer clic en el botón Actualizar se terminan todas las conexiones TCP abiertas.

### Para actualizar el software en un par de alta disponibilidad

1. Inicie sesión en ambos dispositivos.
2. En el dispositivo secundario, actualice el software y reinicie. Después del reinicio, el dispositivo sigue siendo el secundario. Compruebe que la instalación se realizó correctamente. El dispositivo principal debe mostrar que el dispositivo secundario existe pero que la sincronización automática de parámetros no funciona, debido a una discrepancia de versión.
3. En el dispositivo principal, actualice el software y, a continuación, reinicie. El reinicio provoca una conmutación por error y el dispositivo secundario se convierte en el principal. Cuando se complete el reinicio, la alta disponibilidad debe establecerse por completo, ya que ambos dispositivos ejecutan el mismo software.

## Guardar/Restaurar parámetros de un par de alta disponibilidad

April 23, 2021

La función Mantenimiento del sistema: Copia de seguridad/restauración se puede utilizar para guardar y restaurar parámetros de un par de alta disponibilidad de la siguiente manera:

### Para realizar una copia de seguridad de los parámetros

Utilice la función de copia de seguridad como de costumbre. Es decir, inicie sesión en la GUI a través de la dirección VIP de alta disponibilidad (como es normal al administrar el par de alta disponibilidad) y, en la página Administración del sistema: Copia de seguridad/restauración, haga clic en Configuración de descarga.

### Para restaurar los parámetros

1. Inhabilite la alta disponibilidad en ambos dispositivos desactivando la casilla de verificación Habilitado en la ficha Configuración: Implementaciones avanzadas: Alta disponibilidad (alta disponibilidad).
2. Desconecte un cable de red del puente de un dispositivo. (Llámalo Dispositivo A)
3. Desconecte el cable de alimentación del dispositivo A.
4. Restaure los parámetros del otro dispositivo (Appliance B) cargando un conjunto de parámetros previamente guardado en la página Mantenimiento del sistema: Copia de seguridad/restauración y haciendo clic en Restaurar configuración. (Para completar esta operación se requiere un reinicio, lo que vuelve a habilitar la alta disponibilidad).
5. Espere a que se reinicie el dispositivo B. Se convierte en el primario.

6. Reinicie el dispositivo A.
7. Inicie sesión en la interfaz gráfica de usuario del dispositivo A y vuelva a habilitar la alta disponibilidad en la ficha Configuración: Implementaciones avanzadas: Alta disponibilidad (alta disponibilidad). El dispositivo obtiene sus parámetros del primario.
8. Enchufe el cable de red extraído en el paso 2.

Ambos dispositivos ahora se restauran y sincronizan.

## Solución de problemas de pares de alta disponibilidad

April 23, 2021

Si los dispositivos informan de algún error al entrar en el modo de alta disponibilidad, el mensaje de error también anotará la causa. Algunos problemas que pueden interferir con el modo de alta disponibilidad son:

- El otro dispositivo no se está ejecutando.
- Los parámetros de alta disponibilidad de los dos dispositivos no son idénticos.
- Los dos dispositivos no ejecutan la misma versión de software.
- Los dos dispositivos no tienen el mismo número de modelo.
- El cableado incorrecto o incompleto entre los dispositivos no permite que el latido de alta disponibilidad pase entre ellos.
- Los certificados SSL de alta disponibilidad/modo de grupo en uno o ambos dispositivos están dañados o faltan.

## Modo de dos cajas

April 23, 2021

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 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.
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 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**. 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**.

### 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 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 la conexión, los detalles del socio seguro, etc., en el nodo de optimización WAN en la interfaz de usuario de SDWAN-SE.

### 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 de dos cajas.

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.

   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.

### 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 SD-WAN WANOP se borre 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.

### 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 que vea el dispositivo SD-WAN WANOP dos páginas en modo de caja en la GUI web de SD-WAN SE. Para borrar estas páginas, ejecute el comando: *clear_wo_sync*.

## Preguntas frecuentes

April 23, 2021



## Aceleración

April 23, 2021

**¿La aceleración usa un túnel**?

No, la aceleración es transparente, mediante las mismas direcciones IP y números de puerto que la conexión original. Esto permite que los métodos de supervisión actuales sigan funcionando normalmente.

**¿Cómo cambia la aceleración el flujo de paquetes**?

Con conexiones no comprimidas, la aceleración agrega opciones al encabezado TCP del paquete, pero deja intacta la carga útil del paquete. Estas opciones permiten que los dispositivos WANOP de Citrix SD-WAN en cada extremo de la conexión se comuniquen entre sí. Además, el número de secuencia TCP se ajusta para evitar que los problemas de enrutamiento o la falla del dispositivo mezclen paquetes acelerados y paquetes no acelerados en la misma conexión.

Con conexiones comprimidas, la carga útil se comprime, por supuesto, y la salida del compresor se acumula en paquetes de tamaño completo. El resultado es que, por ejemplo, la compresión 3:1 da como resultado un tercio más de paquetes que se transmiten, en lugar del mismo número de paquetes, cada uno reducido a un tercio de tamaño. La compresión también utiliza opciones de encabezado TCP WANOP de Citrix SD-WAN y el ajuste del número de secuencia.

**¿Cuáles son los requisitos básicos de la aceleración**?

La aceleración requiere un dispositivo Citrix SD-WAN WANOP en ambos extremos de la conexión, la conexión debe usar el protocolo TCP y todos los paquetes de la conexión deben pasar a través de ambos dispositivos WANOP de Citrix SD-WAN.

## CIFS y MAPI

April 23, 2021

**¿ Qué requisitos previos se requieren antes de configurar MAPI y SMB firmado en un dispositivo Citrix SD-WAN WANOP**?

Debe cumplir las siguientes condiciones antes de configurar MAPI y SMB firmado en un dispositivo Citrix SD-WAN WANOP:

- La opción Secure Peer debe establecerse en True tanto en el cliente como en el dispositivo del lado del servidor.
- Se debe agregar un usuario delegado al dispositivo lateral del centro de datos y su estado debe marcarse como Correcto.
- El dispositivo lateral del centro de datos debe unirse correctamente al dominio.
- La dirección IP DNS configurada en el dispositivo del lado del servidor debe ser accesible.

  Para obtener más información, consulte Configurar un dispositivo Citrix SD-WAN WANOP para optimizar el tráfico seguro de Windows.

**¿Qué necesito configurar en el Controller de dominio para un usuario delegado**?

Debe crear un usuario en el controlador de dominio antes de configurar la delegación para el usuario en un dispositivo Citrix SD-WAN WANOP.

**¿Necesito configurar algo en el servidor DNS**?

Sí. En el servidor DNS, debe configurar búsquedas hacia adelante e inversas para todas las direcciones IP de los controladores de dominio.

**¿ Qué debo verificar antes de que el dispositivo Citrix SD-WAN WANOP se una al dominio**?

Antes de que el dispositivo se una al dominio, compruebe lo siguiente:

- Las direcciones IP configuradas para servidores DNS primarios o secundarios deben ser accesibles.
- El dominio debe ser accesible.
- Las direcciones IP de dominio resueltas deben ser accesibles.
- Opcionalmente, debe pasar el estado de la utilidad Comprobación de unión previa al dominio.

**¿ Cómo puedo verificar si el dispositivo Citrix SD-WAN WANOP está listo para agregar un usuario como usuario delegado**?

Puede verificar el usuario mediante la utilidad Comprobar usuario delegado en la página de dominio de Windows. Si el estado de todos los parámetros no contiene mensajes de error, el dispositivo está listo para agregar al usuario como usuario delegado.

Si la utilidad muestra errores, debe solucionarlos antes de agregar un usuario como usuario delegado. Puede consultar el registro para comprender los resultados de la prueba.

**¿ Hay algún requisito para el nombre de host y la longitud del nombre de host del dispositivo Citrix SD-WAN WANOP del lado del servidor**?

En el dispositivo Citrix SD-WAN WANOP del lado del servidor, asegúrese de que el nombre de host es único dentro de la red. Además, la longitud del nombre de host no debe ser superior a 15 caracteres.

**¿Puedo configurar la confianza unidireccional en el dominio**?

No. El cliente y el servidor deben ser los miembros de un dominio que tenga confianza bidireccional con el dominio del dispositivo Citrix SD-WAN WANOP del lado del servidor. El dispositivo no admite la confianza unidireccional.

**¿ Puedo utilizar el cliente Macintosh Outlook y obtener beneficios de aceleración del dispositivo Citrix SD-WAN WANOP**?

No. Macintosh Outlook no utiliza MAPI como protocolo de comunicación. Por lo tanto, no puede utilizar Macintosh Outlook en esta instalación.

**¿ Es necesario que el dispositivo Citrix SD-WAN WANOP del lado de la sucursal se una al dominio para acelerar MAPI cifrado**?

No. No es necesario hacer que el dispositivo Citrix SD-WAN WANOP del lado de la sucursal se una al dominio para acelerar MAPI cifrado.

**¿ Puedo configurar un dispositivo Citrix SD-WAN WANOP 2000 con Windows-Server en un lado del centro de datos para MAPI cifrado**?

Sí. Puede configurar un dispositivo Citrix SD-WAN WANOP 2000 con Windows-Server en un lado del centro de datos para MAPI cifrado.

**Cuando hago un dispositivo Citrix SD-WAN WANOP para unirse a un dominio y existe un servidor NTP configurado con una zona horaria diferente en la red, ¿sincroniza el dispositivo la hora con el controlador de dominio o el servidor NTP**?

Cuando hace que el dispositivo Citrix SD-WAN WANOP se una a un dominio, el dispositivo siempre sincronizó su hora con el controlador de dominio y no con el servidor NTP.

**En el dispositivo Citrix SD-WAN WANOP, ¿cuál es la duración predeterminada para borrar la conexión de la lista negra**?

De forma predeterminada, las conexiones de la lista de bloqueados se borran en 900 segundos.

**¿ Qué mecanismos de autenticación de Outlook se admiten en un dispositivo Citrix SD-WAN WANOP**?

A partir de la versión 6.2.4, el dispositivo admite la autenticación Negotiate (predeterminada) y Outlook NTLM v2, pero no se admite la autenticación Kerberos. Sin embargo, la versión 6.2.3 y versiones anteriores solo admiten la autenticación Negotiate Outlook.

**¿ Citrix SD-WAN WANOP admite Outlook Anywhere, RPC a través de HTTPS**?

Sí, a partir de la versión 7.3.

## Compresión

April 23, 2021

**¿ Cuál es el beneficio de la compresión WANOP de Citrix SD-WAN**?

Mientras que el mecanismo básico de compresión es reducir los flujos de datos, el beneficio de esto es hacer las cosas más rápidas. Un archivo más pequeño (o una transacción más pequeña) tarda menos tiempo en transferirse. El tamaño no importa: el punto de compresión es la velocidad.

**¿Cómo se mide el beneficio de compresión**?

Existen dos formas de medir el beneficio de la compresión: tiempo y relación de compresión. Los dos están relacionados cuando el enlace WAN es el cuello de botella dominante. Dado que el compresor WANOP de Citrix SD-WAN es muy rápido, al comprimir datos en tiempo real, un archivo que comprime 5:1 transfiere en una quinta parte del tiempo. Esto es cierto hasta que se encuentra un cuello de botella secundario. Por ejemplo, si el cliente es demasiado lento para manejar una transferencia a toda velocidad, una relación de compresión 5:1 ofrece menos de una aceleración de 5:1.

**¿Cómo funciona la compresión**?

El motor de compresión conserva los datos previamente transferidos a través del enlace, con los datos más recientes retenidos en la memoria y una cantidad mucho mayor en el disco. Cuando una cadena que se transfirió antes se encuentra de nuevo, se reemplaza con una referencia a la copia anterior. Esta referencia se envía a través de la WAN en lugar de la cadena real, y el dispositivo en el otro extremo busca la referencia y la copia en la secuencia de salida.

**¿Cuál es la relación de compresión máxima alcanzable**?

La relación de compresión máxima alcanzable en un dispositivo Citrix SD-WAN WANOP es de aproximadamente 10, 000:1.

**¿Cuál es la relación de compresión esperada**?

La relación de compresión general es el promedio de todos los intentos de comprimir las secuencias de datos en el vínculo. Algunas compresas mejor que otras, y algunas nunca se comprimen en absoluto. El dispositivo utiliza clases de servicio para evitar el envío de flujos obviamente no compresibles al compresor. El efecto de la compresión en diferentes tipos de datos varía de la siguiente manera:

Los datos comprimidos o cifrados de una sola vez (flujos que nunca se volverán a ver y que ya han sido comprimidos o cifrados, como túneles SSH cifrados y monitorización de cámaras de vídeo en tiempo real) no se comprimen, ya que sus flujos de datos nunca son los mismos dos veces.

Los datos binarios comprimidos o los datos cifrados que se ven más de una vez se comprime extremadamente bien en la segunda transferencia y posteriores, con relaciones de compresión en el rango de cientos a miles a uno en estas transferencias posteriores. En la primera transferencia, no se comprimen. La relación media de compresión de dichos datos depende de la frecuencia con la que se ven los datos más de una vez. Mientras que las transferencias individuales a veces muestran relaciones de compresión superiores a 1000:1, los promedios para los datos binarios comprimidos en el enlace promedian entre 1,5:1 y 5:1 en la mayoría de los enlaces, con promedios superiores a 10:1 en algunos enlaces, dependiendo de la naturaleza del tráfico.

Los flujos de texto y los datos binarios descomprimidos/no cifrados se comprimen incluso en la primera pasada. Las secuencias de texto se comprimen bien porque incluso los textos no relacionados tienen muchas subcadenas en común. Esto es cierto para los documentos, el código fuente, las páginas HTML, etc. La compresión de primer paso en el orden de 1,5:1 a 4:1 es común. En la segunda pasada y posteriores, comprimen casi tan bien como los datos binarios comprimidos (100:1 o más).

Los datos binarios sin comprimir son variables, pero a menudo se comprime mejor que el texto. Ejemplos de datos binarios sin comprimir incluyen imágenes de CD, archivos ejecutables y formatos de imagen, audio y vídeo sin comprimir. En la segunda pasada y posteriores, comprimen los datos binarios así como los comprimidos.

Los datos de Citrix Virtual Apps and Desktops se comprimen especialmente bien con las transferencias de archivos, la salida de la impresora y el vídeo, siempre que las mismas secuencias de datos hayan atravesado el enlace antes. Debido a la sobrecarga del protocolo, la compresión de pico es de aproximadamente 40:1, y es probable que la compresión promedio esté en la vecindad de 3:1. Los flujos de datos interactivos, como las actualizaciones de pantalla), dan resultados de compresión en el orden de 2:1.

¿**Cuál es la diferencia entre el almacenamiento en caché y la compresión**?

El almacenamiento en caché guarda objetos enteros con nombre en el dispositivo del cliente. El nombre puede ser una ruta y un nombre de archivo en el caso del almacenamiento en caché del sistema de archivos, o una URL en el caso del almacenamiento en caché web. Si transfiere un objeto idéntico con un nombre diferente, la caché no proporciona ningún beneficio. Si transfiere un objeto con el mismo nombre que un objeto almacenado en caché, pero con ligeras diferencias de contenido, la caché no proporciona ningún beneficio. Si el objeto se puede servir desde la caché, no se obtiene del servidor.

La compresión, por otro lado, no tiene concepto de nombres de objeto, y proporciona beneficios siempre que una cadena en la transferencia coincida con una que ya está en el historial de compresión. Esto significa que si descargas un archivo, cambias el 1% de su contenido y subes el nuevo archivo, es posible que consigas una compresión de 99:1 en la carga. Si descarga un archivo y lo carga a un directorio diferente en el sitio remoto, también puede lograr una alta relación de compresión. La compresión no requiere bloqueo de archivos y no sufre de estancamiento. El objeto siempre se obtiene del servidor y, por lo tanto, siempre es correcto byte por byte.

## RPC sobre HTTPS

April 23, 2021

### ¿Es obligatorio crear una clase de servicio para acelerar RPC a través de conexiones HTTPS?

Crear una nueva clase de servicio es una tarea opcional. Puede utilizar una clase de servicio HTTPS existente. Sin embargo, para crear informes específicamente para RPC a través de conexiones HTTPS, debe crear una nueva clase de servicio y enlazar el perfil SSL a ella. Si no desea crear una clase de

servicio para RPC a través de conexiones HTTPS, puede enlazar el perfil SSL que ha creado a la clase de servicio web (Private-Secure).

### No he creado ninguna clase de servicio para la RPC sobre aplicaciones HTTPS. ¿Cómo afectará esto a los informes del RPC a través de conexiones HTTPS?

Al actualizar el dispositivo a la versión 7.3, las aplicaciones RPC sobre HTTPS que se crean no pertenecen a ninguna clase de servicio. Como resultado, todas las conexiones RPC a través de HTTPS se enumeran como las conexiones TCP Otras en los informes. Si desea clasificar estas conexiones como RPC sobre conexiones HTTPS, debe crear una clase de servicio para estas aplicaciones.

### ¿Hay una clase de servicio predeterminada para RPC a través de HTTPS en el dispositivo?

No. El dispositivo solo tiene aplicaciones predeterminadas y no clases de servicio predeterminadas. Debe crear la clase de servicio para una aplicación.

### ¿Ofrece el dispositivo ventajas de compresión SSL a la RPC a través de conexiones HTTPS?

No. El dispositivo no proporciona beneficios de compresión SSL para RPC a través de conexiones HTTP. Los beneficios de compresión solo están disponibles para el cifrado y descifrado del tráfico HTTPS.

### Al igual que MAPI, ¿optimiza el dispositivo la latencia para RPC a través de conexiones HTTPS?

No. El dispositivo no optimiza la latencia para RPC a través de HTTPS.

### ¿Es MAPI sobre HTTP diferente de RPC sobre HTTPS?

Sí. MAPI sobre HTTP es un nuevo protocolo compatible con Microsoft Exchange Server 2013 SP1 o posterior.

### ¿Cuál es la diferencia entre la configuración de RPC sobre HTTPS en los dispositivos Citrix SD-WAN WANOP del lado del cliente y del lado del servidor?

Excepto por crear una clase de servicio y agregar aplicaciones RPC a través de HTTPS, no necesita ninguna configuración adicional en un dispositivo Citrix SD-WAN WANOP del lado del cliente.

### ¿Qué sucede si configuro el perfil SSL en modo proxy transparente?

Algunos servidores de Exchange requieren compatibilidad con tickets de sesión TLS. Para acelerar las conexiones a estos servidores, debe crear un perfil SSL con proxy dividido, ya que el modo proxy transparente no admite tickets de sesión TLS.

### Si se utiliza una configuración de equilibrio de carga para Microsoft Exchange Server, ¿qué dirección IP de destino debo agregar a la regla de filtro al crear una clase de servicio RPC a través de HTTPS?

Si utiliza un dispositivo de equilibrio de carga, agregue su dirección IP virtual (VIP) a la regla de filtro al crear una clase de servicio RPC sobre HTTP.

### ¿Cómo puedo diferenciar entre el tráfico MAP y RPC sobre HTTPS en la página de Outlook (MAPI)?

Puede diferenciar el tráfico en función de las aplicaciones que se muestran en la página de Outlook (MAPI). Por ejemplo, MAPI y RPC a través de HTTPS se utilizan para las siguientes aplicaciones:

- **MAPI**: MAPI y eMAPI
- **RPC por HTTPS**: HTTP MAPI, HTTP eMAPI, HTTPS MAPI y HTTPS eMAPI

## SCPS

April 23, 2021

**¿Qué es el protocolo SCPS**?

El protocolo estándar de protocolo de comunicaciones espaciales (SCPS) es una variante del protocolo TCP.

**¿Cuál es el uso del protocolo SCPS**?

El protocolo SCPS se utiliza en comunicaciones por satélite y aplicaciones similares.

**¿ Se admite el protocolo SCPS en un dispositivo Citrix SD-WAN WANOP**?

Sí. El dispositivo Citrix SD-WAN WANOP admite el protocolo SCPS y acelera los datos transferidos mediante este protocolo.

**¿Puedo usar un dispositivo habilitado para SCPS con otro que no esté habilitado para SCPS**?

Sí. Si debe mezclar dispositivos habilitados para SCPS con dispositivos no habilitados para SCPS, implemente de tal manera que no se produzcan discrepancias. Puede utilizar reglas de clase de servicio basadas en IP u organizar la implementación para que cada ruta tenga dispositivos coincidentes.

**¿Qué sucede si utilizo un dispositivo habilitado para SCPS en un extremo que no esté habilitado para SCPS en el otro extremo del vínculo**?

Si el dispositivo de un extremo de la conexión tiene SCPS habilitado y uno no lo hace, el rendimiento de la retransmisión se verá afectado. Esta condición también provoca una alerta de Discordancia del modo SCPS.

**¿Cuál es la diferencia entre el comportamiento de un dispositivo habilitado para SCPS y el dispositivo predeterminado**?

La principal diferencia entre un comportamiento de dispositivo habilitado para SCPS y el predeterminado es que se utilizan reconocimientos negativos selectivos (Snacks) de estilo SCPS en lugar de reconocimientos selectivos estándar (SACK).

## Emparejamiento seguro

April 23, 2021

**¿ Qué características de Citrix SD-WAN WANOP requieren un peering seguro**?

Debe establecer un peering seguro entre los dispositivos Citrix SD-WAN WANOP en dos extremos del vínculo cuando desee utilizar cualquiera de las siguientes características:

- Compresión SSL
- Soporte de CIFS firmado
- Compatibilidad con MAPI cifrada

**¿Debo considerar algo antes de configurar un túnel seguro**?

Sí. Debe solicitar y recibir una licencia de cifrado antes de configurar un túnel seguro entre los dispositivos Citrix SD-WAN WANOP hasta los extremos del enlace.

**¿Qué sucede cuando habilita el peering seguro en un dispositivo en un extremo del vínculo**?

Cuando habilita el peering seguro en un dispositivo Citrix SD-WAN WANOP en un extremo del vínculo, el otro dispositivo lo detecta e intenta abrir un túnel de señalización SSL. Si los dos dispositivos se autentican correctamente entre sí a través de este túnel, los dispositivos tienen una relación de peering segura. Todas las conexiones aceleradas entre los dos dispositivos están cifradas y la compresión está habilitada.

**¿Qué ocurre cuando no activo el peering seguro en el dispositivo asociado**?

Cuando un dispositivo tiene habilitado el emparejamiento seguro, las conexiones con un asociado para el que no tiene una relación de pares seguros no se cifran ni comprimen, aunque la aceleración del control de flujo TCP sigue estando disponible. La compresión está inhabilitada para garantizar que los datos almacenados en el historial de compresión de socios seguros no se puedan compartir con socios no seguros.

**¿Por qué necesito una contraseña de almacén de claves**?

Necesita una contraseña de almacén de claves para acceder a los parámetros de seguridad. Esta contraseña es diferente de la contraseña del administrador y permite separar la administración de seguridad de otras tareas. Si se restablece la contraseña del almacén de claves, se pierden todos los datos cifrados y las claves privadas existentes.

Para proteger los datos incluso en caso de robo del dispositivo, se debe volver a introducir la contraseña del almacén de claves cada vez que se reinicie el dispositivo. Hasta que esto se haga, el peering seguro y la compresión están inhabilitados.

**¿ El dispositivo Citrix SD-WAN WANOP que recibí de Citrix contiene claves y certificado para configurar un túnel seguro**?

No. Los productos Citrix SD-WAN WANOP se envían sin las claves y certificados necesarios para el túnel de señalización SSL. Debes generarlos tú mismo.

## Aceleración SSL

April 23, 2021

**¿La aceleración usa un túnel**?

No, la aceleración es transparente, mediante las mismas direcciones IP y números de puerto que la conexión original. Esto permite que los métodos de supervisión actuales sigan funcionando normalmente.

**¿Cómo cambia la aceleración el flujo de paquetes**?

Con conexiones no comprimidas, la aceleración agrega opciones al encabezado TCP del paquete, pero deja intacta la carga útil del paquete. Estas opciones permiten que los dispositivos WANOP de Citrix SD-WAN en cada extremo de la conexión se comuniquen entre sí. Además, el número de secuencia TCP se ajusta para evitar que los problemas de enrutamiento o la falla del dispositivo mezclen paquetes acelerados y paquetes no acelerados en la misma conexión.

Con conexiones comprimidas, la carga útil se comprime, por supuesto, y la salida del compresor se acumula en paquetes de tamaño completo. El resultado es que, por ejemplo, la compresión 3:1 da

como resultado un tercio más de paquetes que se transmiten, en lugar del mismo número de paquetes, cada uno reducido a un tercio de tamaño. La compresión también utiliza opciones de encabezado TCP WANOP de Citrix SD-WAN y el ajuste del número de secuencia.

**¿Cuáles son los requisitos básicos de la aceleración**?

La aceleración requiere un dispositivo WANOP de Citrix SD-WAN en ambos extremos de la conexión, la conexión debe utilizar el protocolo TCP y todos los paquetes de la conexión deben pasar a través de ambos dispositivos Citrix SD-WAN WANOP.

## Plug-in de Citrix SD-WAN WANOP

April 23, 2021

**¿ Qué métodos puedo usar para instalar el complemento Citrix SD-WAN WANOP en mi equipo**?

Puede utilizar cualquiera de los métodos siguientes para instalar el complemento Citrix SD-WAN WANOP en su equipo:

- Instalación independiente: ejecute el archivo de Microsoft Installer (msi).
- Instalación silenciosa: ejecute el siguiente comando:

  *> msiexec.exe /i ruta\ CitrixSD-wanwanOpPluginReleasex64- <Release_Nunmer> /qn*
- Instalación remota: instale el complemento Citrix SD-WAN WANOP de forma remota desde Citrix Receiver. Esta instalación se realiza mediante el servidor de merchandising.

**¿ Puedo personalizar el instalador del plug-in WANOP de Citrix SD-WAN**?

Sí. Puede personalizar la dirección IP de señalización y el tamaño de compresión basada en disco (DBC) con el archivo msi del complemento WANOP de Citrix SD-WAN.

**¿ Cuáles son los requisitos mínimos de hardware para instalar el complemento Citrix SD-WAN WANOP**?

Para el complemento WANOP de Citrix SD-WAN, el equipo debe cumplir los siguientes requisitos:

- CPU Pentium 4 clase
- Mínimo 4 GB de RAM
- Mínimo 2 GB para espacio libre en el disco duro

¿**En qué sistemas operativos puedo instalar el complemento Citrix SD-WAN WANOP**?

Puede instalar el complemento WANOP de Citrix SD-WAN en los siguientes sistemas operativos:

| Sistema operativo | Edición | Versión |
|---|---|---|
| Windows XP | Hogar, Profesional | 32-bits |
| Windows Vista | Home Basic, Home Premium, Business, Enterprise, Ultimate | 32-bits |
| Windows 7 | Home Basic, Home Premium, Business, Enterprise, Ultimate | 32 bits, 64 bits |
| Windows 8 | Profesional, Empresa | 32 bits, 64 bits |
| Windows 10 | Profesional, Empresa | 32 bits, 64 bits |

**¿ Qué precauciones debo tomar antes de instalar el complemento Citrix SD-WAN WANOP**?

Antes de instalar el complemento WANOP de Citrix SD-WAN en el equipo, tome las siguientes precauciones:

- Dependiendo de la versión del sistema operativo, descargue la versión del instalador de Citrix SD-WAN WANOP de 32 bits o 64 bits.
- No puede instalar el complemento WANOP de Citrix SD-WAN en una unidad o carpeta comprimidas.
- Asegúrese de que el equipo tenga suficiente espacio libre en disco.
- No puede degradar la versión del complemento WANOP de Citrix SD-WAN. Si desea utilizar una versión anterior de Citrix SD-WAN WANOP, debe desinstalar la versión actual e instalar una versión anterior.

**¿ Qué dispositivos Citrix SD-WAN WANOP admiten el complemento Citrix SD-WAN WANOP**?

Los siguientes dispositivos Citrix SD-WAN WANOP admiten el complemento Citrix SD-WAN WANOP:

- SD-WAN WANOP 2000
- Dispositivo WANOP 2000 SD-WAN con Windows Server
- SD-WAN WANOP 3000 NEGRO
- SD-WAN WANOP 4000
- SD-WAN WANOP 5000

¿**Qué dispositivos Citrix SD-WAN WANOP no admiten el complemento WANOP de Citrix SD-WAN**?

Los siguientes dispositivos Citrix SD-WAN WANOP no admiten el complemento Citrix SD-WAN WANOP:

- SD-WAN WANOP 400
- SD-WAN WANOP 700
- SD-WAN WANOP 800
- WANOP 1000 SD-WAN con Windows Server

**¿ Es necesario instalar una licencia simultánea (CCU) en los dispositivos Citrix SD-WAN WANOP 2000, 3000 y VPX para utilizar el complemento Citrix SD-WAN WANOP**?

Sí. Debe instalar una licencia CCU en los dispositivos Citrix SD-WAN WANOP 2000, 3000 y VPX para utilizar el complemento Citrix SD-WAN WANOP.

**¿ Necesito instalar una licencia CCU en los dispositivos Citrix SD-WAN WANOP 4000 y 5000 para utilizar el complemento Citrix SD-WAN WANOP**?

No. No es necesario instalar una licencia CCU en los dispositivos Citrix SD-WAN WANOP 4000 y 5000 para utilizar el complemento Citrix SD-WAN WANOP. La licencia base del dispositivo es suficiente para que el complemento WANOP de Citrix SD-WAN se conecte a estos dispositivos.

**¿Cuáles son las recomendaciones de Citrix para acelerar las subredes**?

Citrix recomienda lo siguiente para acelerar las subredes:

- Nunca use ALL/ALL para la configuración de aceleración. Especifique las subredes en función de los requisitos.
- No configure la aceleración para la dirección VIP de Citrix Gateway.

**¿ El complemento WANOP de Citrix SD-WAN es compatible con los clientes ligeros de Windows**?

No. El complemento WANOP de Citrix SD-WAN no es compatible con los clientes ligeros de Windows.

**¿ Qué versiones de Citrix Receiver y Citrix Gateway se admiten con el complemento WANOP de Citrix SD-WAN**?

El complemento WANOP de Citrix SD-WAN admite las versiones de Citrix Receiver 4.1 y Citrix Gateway 10.5.

**¿ Qué características de Citrix SD-WAN WANOP no son compatibles con el complemento Citrix SD-WAN WANOP**?

El complemento WANOP de Citrix SD-WAN no admite las siguientes características de Citrix SD-WAN WANOP:

- Almacenamiento en caché de vídeo
- Modelado del tráfico

- IPv6

**¿ Es necesario configurar reglas de aceleración en un dispositivo Citrix SD-WAN WANOP 4000 o 5000 para que el complemento WANOP de Citrix SD-WAN funcione con él**?

Sí. Debe configurar reglas de aceleración en un dispositivo Citrix SD-WAN WANOP 4000 o 5000 para que el complemento WANOP de Citrix SD-WAN funcione con él.

**¿Cuál es la importancia del filtrado de fuentes de canal de señal**?

Mediante el filtrado de origen del canal de señal, puede permitir o denegar a una subred o dirección IP específica la capacidad de conectarse al dispositivo y obtener reglas de aceleración. La subred de origen denegada no puede establecer conexiones de señalización y acelerar el tráfico.

**¿Cuál es la importancia de la detección de LAN**?

Cuando habilita la detección de LAN, evita la aceleración del tráfico cuando el complemento y el dispositivo de Citrix SD-WAN WANOP están en la misma LAN. La aceleración local no es deseable, ya que aplicar el límite de ancho de banda del dispositivo a la conexión local podría reducir la velocidad del tráfico local.

**Para acelerar el tráfico, ¿cuál es el valor mínimo de RTT recomendado entre el complemento y el dispositivo de Citrix SD-WAN WANOP**?

Citrix recomienda configurar un valor RTT mayor que cualquier RTT (tiempo de ping) en la LAN local, pero menor que el RTT para cualquier usuario remoto. El valor predeterminado de 20 milisegundos es adecuado para la mayoría de las redes.

**¿ Qué condiciones debo tener en cuenta al definir reglas de aceleración para el complemento WANOP de Citrix SD-WAN**?

Tenga en cuenta las siguientes condiciones al definir reglas de aceleración para el complemento WANOP de Citrix SD-WAN:

- Defina reglas de aceleración para todas las subredes que son locales en el dispositivo. Estas subredes son las subredes LAN del sitio donde está instalado el dispositivo.
- Si hay direcciones IP de destino que no formen parte de la LAN, agregue reglas de exclusión para estas direcciones IP. Asegúrese de que las reglas para excluir direcciones IP preceden a las reglas para acelerar el tráfico de subredes. Esto incluye subredes en sitios remotos con direcciones IP que parecen locales.
- Si ha instalado el dispositivo en modo en línea con una VPN y funciona en modo transparente, puede configurar el dispositivo para acelerar todo el tráfico empresarial, no solo el tráfico originado por el sitio local o destinado a él. En este caso, las únicas conexiones aceleradas son entre el complemento Citrix SD-WAN WANOP y la VPN. La aceleración del tráfico entre el complemento WANOP de Citrix SD-WAN y la VPN es óptima.

**¿Dónde están los archivos de seguimiento y bloqueo del complemento de Citrix SD-WAN WANOP almacenados en el equipo**?

Los archivos de bloqueo y seguimiento del complemento WANOP de Citrix SD-WAN se almacenan en las carpetas siguientes:

- Archivos de bloqueo: C: /ProgramFiles/Citrix/Citrix SD-WAN WANOP
- Archivos de seguimiento: C: /Users/admin/AppData/Local/Temp

**¿ Cómo se conecta el complemento WANOP de Citrix SD-WAN a un par de alta disponibilidad**?

El complemento WANOP de Citrix SD-WAN siempre se conecta a la misma dirección IP de señalización. La dirección IP de señalización está enlazada únicamente al dispositivo principal del par de alta disponibilidad, no al dispositivo secundario. Por lo tanto, el complemento WANOP de Citrix SD-WAN siempre se conecta al dispositivo principal del par de alta disponibilidad.

¿**Qué modos de implementación admite el complemento de Citrix SD-WAN WANOP**?

El complemento Citrix SD-WAN WANOP admite los siguientes modos de implementación:

- En línea.
- WCCP.
- Alta disponibilidad.
- Plug-in WANOP de Citrix SD-WAN con implementación de NAT.
- Complemento WANOP de Citrix SD-WAN con el dispositivo Citrix SD-WAN WANOP en modo WCCP mediante proxy ICA.
- Complemento WANOP de Citrix SD-WAN con el dispositivo Citrix SD-WAN WANOP 4000 o 5000. En esta implementación, el puerto de administración (0/1) está conectado a la red de administración y la dirección IP de señalización está en una red diferente.

**¿Cómo fluyen los paquetes en los modos transparente y redirector**?

En modo transparente, el dispositivo Citrix SD-WAN WANOP no cambia la dirección IP de origen del paquete. En modo de redirector, el dispositivo Citrix SD-WAN WANOP proxies servidores y cambia la dirección IP de los paquetes.

> **Nota**
>
> Citrix recomienda el modo transparente para la implementación de producción.

**¿Cómo puedo establecer un túnel seguro entre el plug-in WANOP y el dispositivo de Citrix SD-WAN**?

Para establecer un túnel seguro entre el plug-in WANOP y el dispositivo de Citrix SD-WAN, siga el procedimiento siguiente:

1. En la interfaz de usuario del complemento WANOP de Citrix SD-WAN, abra la ficha **Certificados**.
2. Seleccione la opción **Certificado de CA**.
3. Haga clic en **Importar** y cargue el certificado de CA correspondiente.
4. Seleccione un Almacén de certificados donde desee almacenar el certificado.
5. Seleccione la opción **Certificado de cliente**.
6. Haga clic en **Importar**.
7. Seleccione los formatos de certificado adecuados y cargue los certificados pertinentes.
8. Almacene los certificados en un Almacén de certificados.
9. Si la clave privada está protegida por contraseña, introduzca la contraseña para descifrar la clave privada.
10. Debe cargar el mismo certificado de CA y par de claves en el dispositivo para establecer un túnel seguro.

**¿Cómo puedo verificar que se ha establecido un túnel seguro**?

Para verificar que se ha establecido un túnel seguro, siga el procedimiento siguiente:

1. El equipo en el que ha instalado el complemento Citrix SD-WAN WANOP, ejecute el siguiente comando:

   > *telnet localhost 1362*

2. En la consola, ejecute el siguiente comando:

   > *túneles de exhibición*

   Lo que sigue es un ejemplo de salida del comando. Si la salida incluye el texto seguro en la sección Connected Available, se ha establecido un túnel seguro. Si no se establece un túnel seguro, el texto lee *texto claro*.

   ```
   ```
   Mostrar túneles
   Túneles de mensajes:
     Conectado disponible:
       172.16.9.100 automático, seguro, cliente, iniciador,
          configurado
       CN: mike.199.130


   Conectado disponible: 1
   Clientes: 1 pares: 0
   <!--NeedCopy--> ```
   ```

   Para obtener más información sobre el complemento WANOP de Citrix SD-WAN, consulte [Citrix SD-WAN WANOP Plug-in] (/en-us/citrix-sd-wan-wanop/10-2/wanopt-plug-in.html).


   ```

# Modelado del tráfico

April 23, 2021

**¿ Qué es Citrix SD-WAN WANOP Traffic Shaping**?

El modelado de tráfico WANOP de Citrix SD-WAN utiliza un grupo de políticas para establecer la prioridad del tráfico de enlace diferente y enviar tráfico al enlace a una velocidad cercana, pero no mayor que, a la velocidad del enlace. A diferencia de la aceleración, que solo se aplica al tráfico TCP/IP, el formador de tráfico controla todo el tráfico del vínculo.

**¿Cuál es el beneficio del modelado del tráfico**?

El modelado del tráfico utiliza recursos de enlace escasos según las directivas establecidas, de modo que el tráfico que se sabe que es importante recibirá más ancho de banda que el tráfico que se sabe que no es importante.

**¿Cómo interactúa el modelador de tráfico con el tráfico de Citrix Virtual Apps and Desktops**?

El dispositivo Citrix SD-WAN WANOP analiza el flujo de datos de aplicaciones virtuales y escritorios virtuales y conoce los diferentes tipos de tráfico y sus prioridades, favoreciendo el tráfico de alta prioridad. Es el único producto que puede priorizar flujos ICA cifrados y proporcionar soporte nativo para MultiStream ICA, que divide la sesión de un usuario en hasta cuatro conexiones con diferentes prioridades.

**¿Qué es la cola justa ponderada**?

Un dispositivo WANOP de Citrix SD-WAN utiliza colas equitativas ponderadas, que proporciona una cola independiente para cada conexión. Con una cola justa, una conexión demasiado rápida puede desbordar solo su propia cola. No tiene ningún efecto en otras conexiones.

**¿Cuál es la diferencia entre la cola justa ponderada y no ponderada**?

La cola justa ponderada incluye la opción de dar a algunos tráfico una prioridad (peso) más alta que a otros. El tráfico con un peso de dos recibe el doble del ancho de banda del tráfico con un peso de uno. En una configuración WANOP de Citrix SD-WAN, los pesos se asignan en las políticas de modelado de tráfico.

**¿Qué es una definición de enlace**?

Una definición de vínculo especifica qué tráfico está asociado al vínculo definido, el ancho de banda máximo para permitir el tráfico recibido en el vínculo y el ancho de banda máximo para el tráfico enviado a través del vínculo. La definición también identifica el tráfico como entrante o saliente y como tráfico de lado WAN o LAN.

**¿Cuáles son las ventajas de la definición de enlaces**?

Las definiciones de vínculos permiten que el dispositivo evite la congestión y la pérdida en los vínculos WAN y realice el modelado del tráfico. La definición también identifica el tráfico como entrante o saliente y como tráfico de lado WAN o LAN. Todo el tráfico que fluye a través del dispositivo se compara con la lista de definiciones de vínculo y la primera definición coincidente identifica el vínculo al que pertenece el tráfico.

**No he configurado ninguna clase de servicio con Directiva predeterminada. Sin embargo, los informes de modelado de tráfico muestran una gran cantidad de tráfico representado por la directiva predeterminada. ¿He configurado algo incorrectamente**?

No. No hay ningún problema con su configuración. El modelado del tráfico solo es aplicable al vínculo WAN. El tráfico en la LAN o en cualquier otro vínculo está representado por la directiva predeterminada.

Por ejemplo, considere una configuración en la que cree una clase de servicio, como Management_Service_Class, que tenga la subred de administración como dirección IP de destino y que vincule una directiva de modelado de tráfico personalizada a esta clase de servicio. En este caso, cuando no hay tráfico en WAN, puede observar que el tráfico de administración se clasifica como Management_Service_Class en el informe de clase de servicio. Sin embargo, en el informe de la directiva de modelado de tráfico, todavía existen entradas para la directiva predeterminada que puede esperar que existan como directiva de modelado de tráfico personalizada.

En el informe Directiva de modelado de tráfico, el dispositivo no utiliza la directiva de modelado de tráfico personalizada para la directiva Management_Service_Class y aplica la directiva predeterminada. Para evitar esta confusión, puede desactivar la opción Todos los demás o definir el vínculo de tipo LAN para la interfaz de administración.

## Proceso de actualización (SO)

April 23, 2021

### ¿La nueva actualización del kernel del sistema operativo WANOP es compatible desde qué versión SD-WAN?

Citrix SD-WAN versión 10.1 y posterior.

### ¿Se admite el nuevo sistema operativo en todas las plataformas SD-WAN?

Sí. La actualización del sistema operativo es compatible con todos los dispositivos SD-WAN WANOP (VPX, Physical, Cloud) y Premium/Enterprise Edition.

### ¿Cuáles son los perfiles WANOP VPX (RAM/Disco/vCPU) compatibles con la versión 10.1?

- 6 GB de RAM, 100 GB de disco y 2 vCPU
- 6 GB de RAM, 250 GB de disco y 2 vCPU
- 8 GB de RAM, disco de 500 GB y 4 vCPU
- 16 GB de RAM, disco de 500 GB y 4 vCPU

### ¿Cuáles son las diferencias de características clave entre WANOP que se ejecuta con la versión 10.0 o inferior frente a la 10.1?

| Función | 10.0 o anterior | 10.1 o posterior | Comentarios |
|---|---|---|---|
| Soporte de almacenamiento en caché de vídeo en WANOP | compatibles | No se admite | Ninguno |
| Requisito mínimo de RAM para WANOP VPX | 4 GB DE RAM | 6 GB DE RAM | Ninguno |
| Asistente de implementación WANOP VPX | compatibles | No se admite | Ninguno |
| Dirección IP de administración del adaptador principal/aPA para WANOP VPX | DHCP está inhabilitado de forma predeterminada | DHCP está habilitado de forma predeterminada | Ninguno |
| Compatibilidad con la actualización de WANOP VPX independiente existente en Citrix Hypervisor | compatibles | se admiten. Se debe importar una nueva imagen SD-WAN 10.1 XVA | Ninguno |

| Función | 10.0 o anterior | 10.1 o posterior | Comentarios |
| --- | --- | --- | --- |
| Compatibilidad con la actualización en la plataforma WANOP física que tenga la versión de Citrix Hypervisor 6.0 Hypervisor 6.0 (las plataformas que se suministran con la versión 7.2.2 o anterior de la imagen base de fábrica tendrían la versión de Citrix Hypervisor 6.0), versión 10.1 | compatibles | Tiene que actualizar Citrix Hypervisor a la versión 6.5 (con el paquete de actualización WANOP Citrix Hypervisor 6.5) y, a continuación, realizar la actualización WANOP 10.1. | Al hacer clic en “Configuración”GUI, se mostrará la versión del hipervisor de Citrix Hypervisor |

### La actualización de WANOP VPX que se ejecuta en Citrix Hypervisor independiente (con compilación WO 10.0 o anterior) a la versión 10.1 es compatible. Si no, ¿por qué?

Esta actualización no es compatible debido a la conversión de PV a HVM. Tiene que aprovisionar una nueva versión SD-WAN en Citrix Hypervisor WANOP VPX 10.1 mediante la imagen XVA.

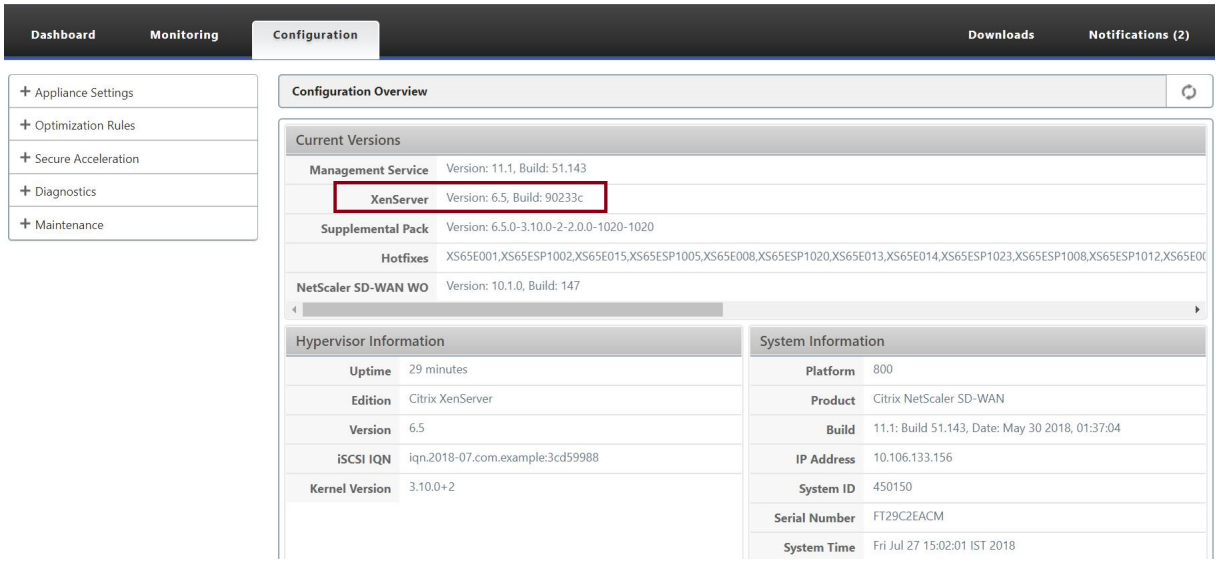
### La actualización de WANOP VPX que se ejecuta en ESXi /Hyper-V independiente (con WO build 10.0 o anterior) a la versión 10.1 es compatible, si no, ¿por qué?

Esta actualización es compatible. Antes de la actualización, tenga en cuenta los nuevos cambios en los requisitos de recursos de RAM.

### La actualización de WANOP en el dispositivo físico (con WANOP build 10.0 o anterior) a la versión 10.1 es compatible, si no, ¿por qué?

Esta actualización es compatible. El requisito previo para esta actualización es que el Hypervisor Hypervisor de Citrix Hypervisor (en un dispositivo SD-WAN físico) tenga Citrix Hypervisor versión 6.2/6.5 o superior. Esto se puede verificar en la ficha **Configuración**.

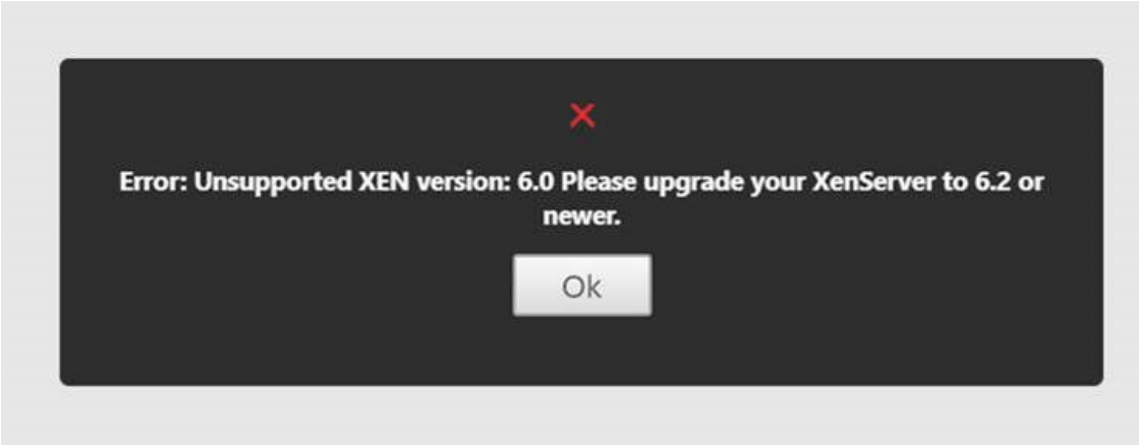
 




## Si el dispositivo físico WANOP no se ejecuta con Citrix Hypervisor 6.2/6.5 o superior, ¿qué debe hacer el usuario?

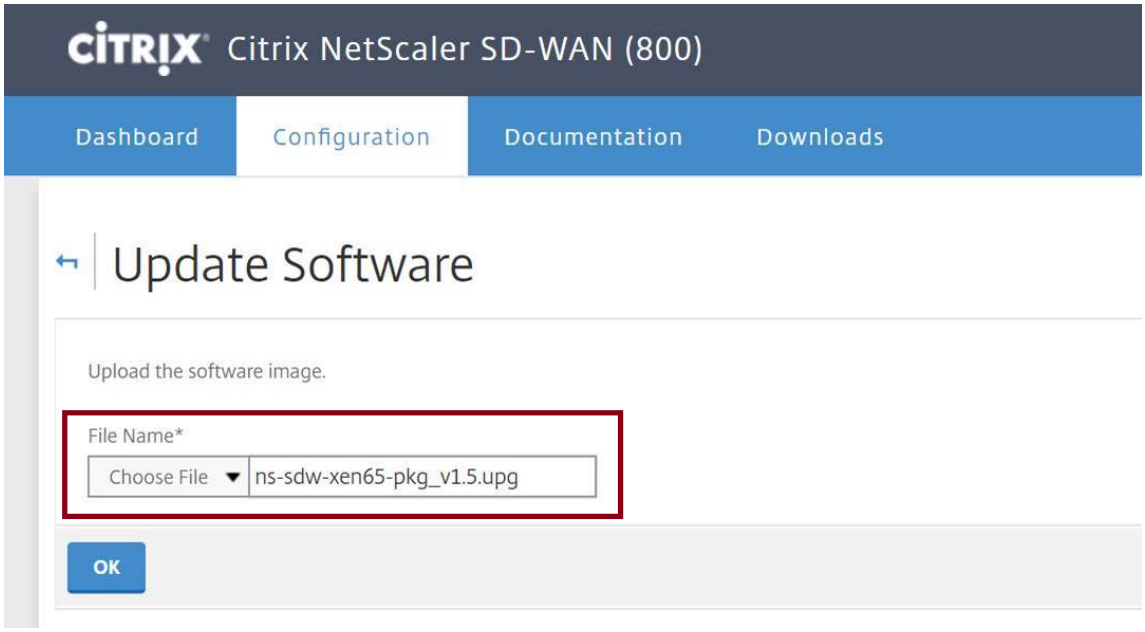
Tiene que actualizar Citrix Hypervisor antes de actualizar la versión WO de SD-WAN. Por ejemplo, en este caso de uso que aparece a continuación, consideremos la posibilidad de actualizar la plataforma SD-WAN 800 WANOP que se ejecute con 7.2.2 (que tenga la versión 6.0 de Citrix Hypervisor).

1. Al actualizar este dispositivo a la versión SD-WAN 10.1, se produciría el siguiente mensaje de error.

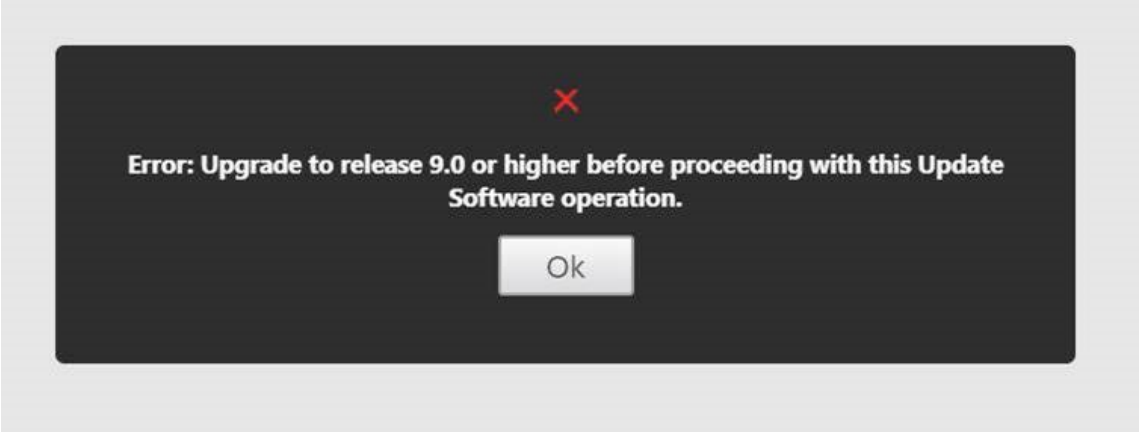



2. Actualice Citrix Hypervisor a 6.5, mediante “ns-sdw-xen65-pkg_v1.5.upg”(puede descargarse desde el sitio web de descarga de Citrix.

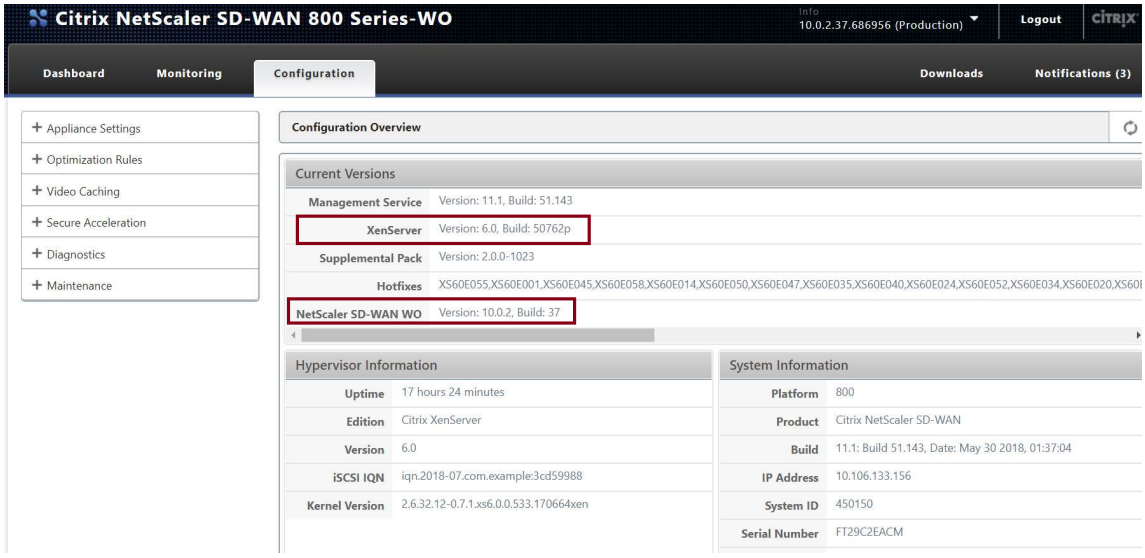



3. Si SD-WAN WO no tiene versión 9.0 o posterior, no se actualizará a Citrix Hypervisor 6.5. Aparecerá el siguiente mensaje de error.

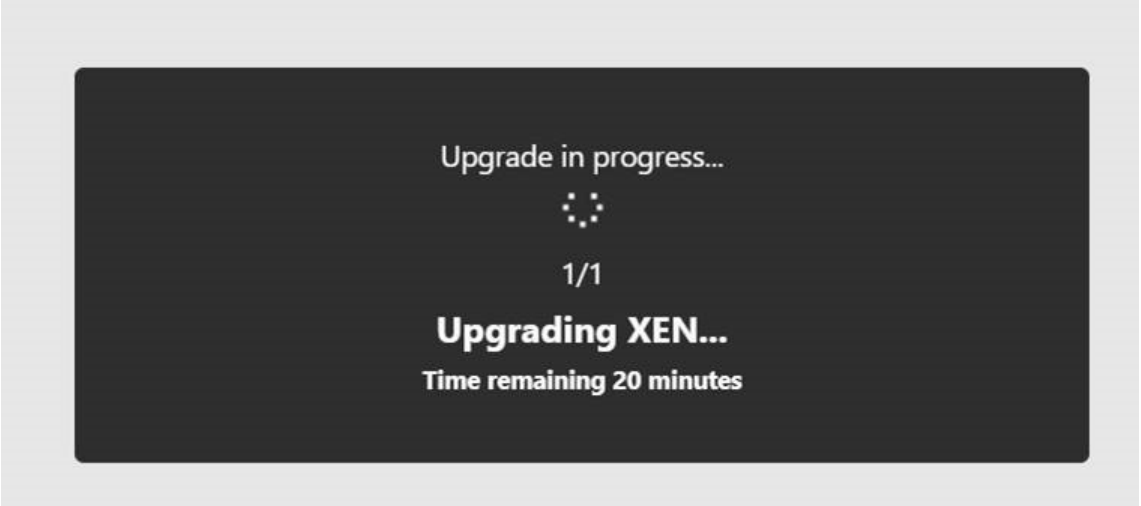



4. Supongamos que el usuario ha actualizado la versión WO a 10.0.2 ahora.

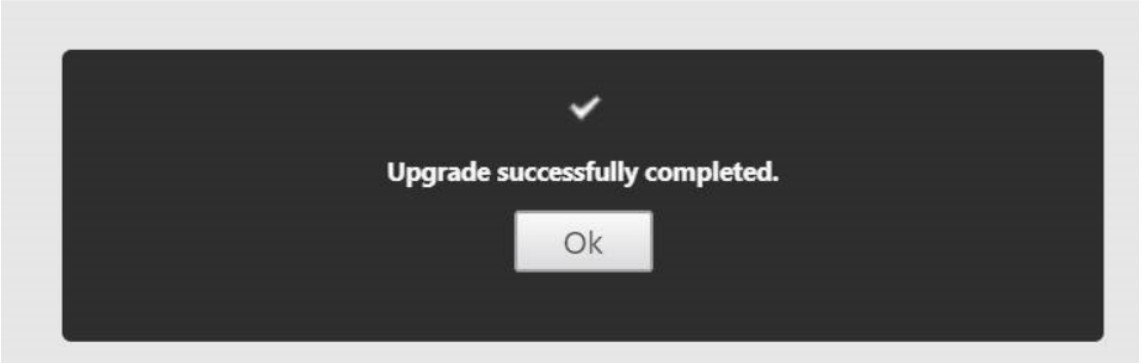
 

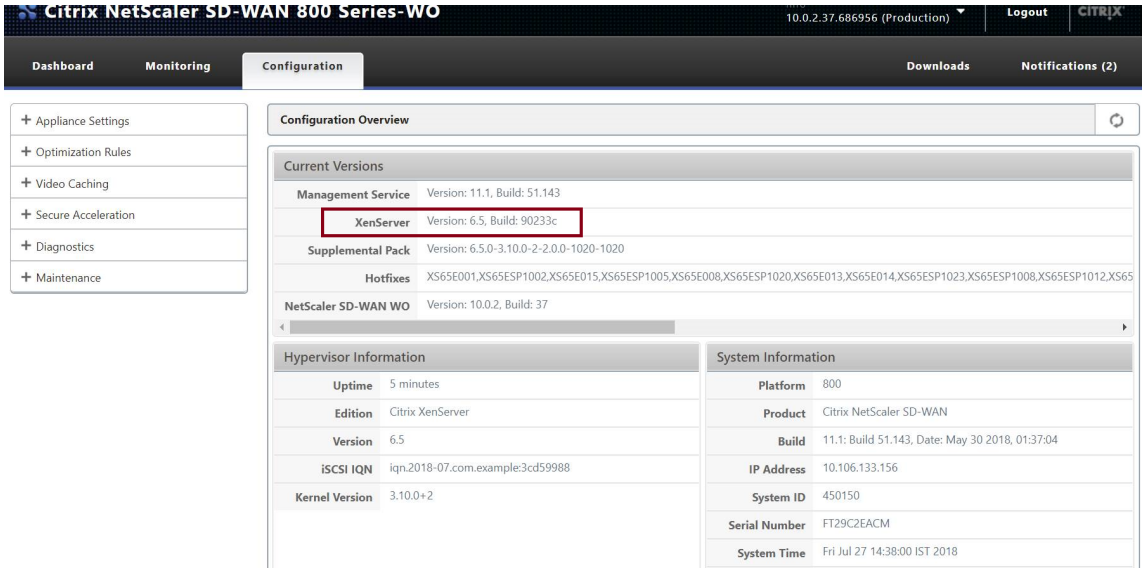



5. Ahora, actualice Citrix Hypervisor a 6.5, mediante “ns-sdw-xen65-pkg_v1.5.upg”.

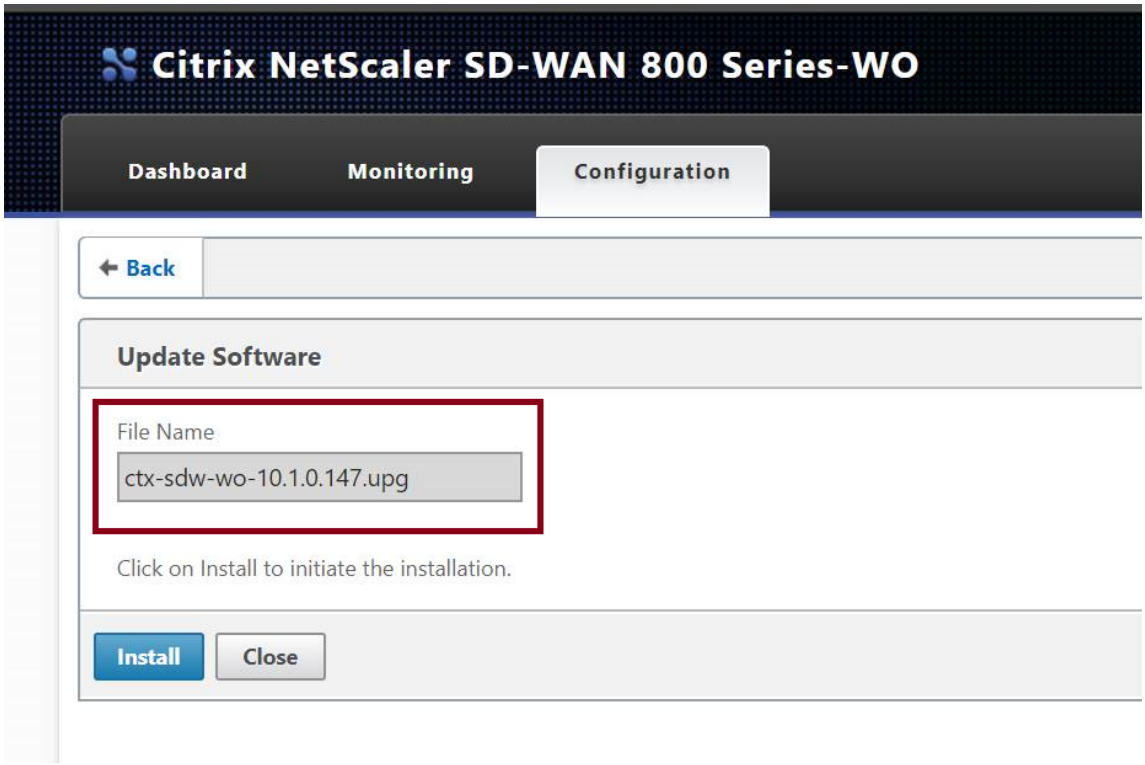

 

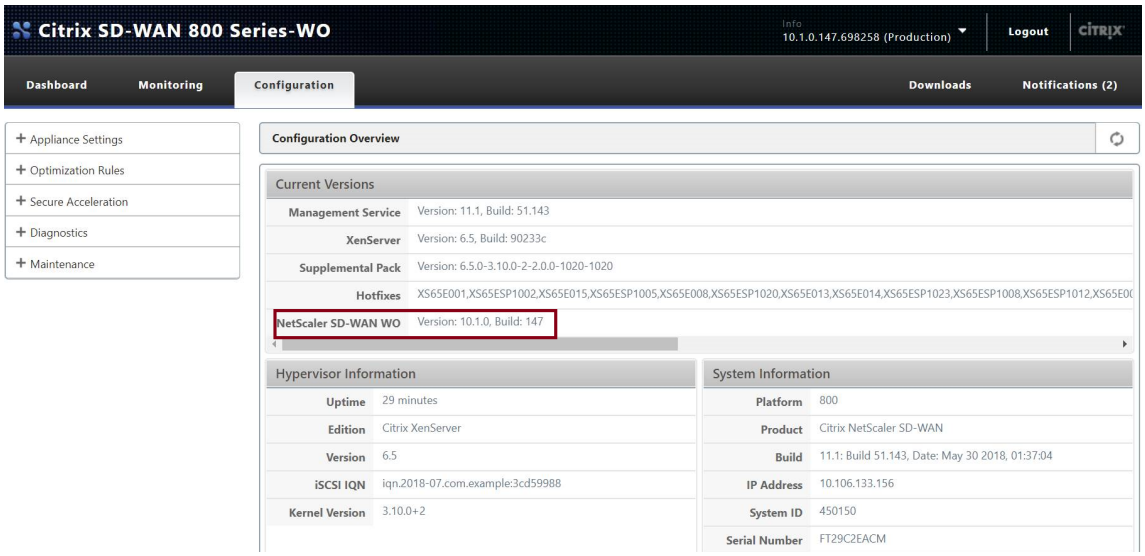



6. Ahora, actualice SD-WAN a la versión 10.1.




## El ping ICMP de cliente a servidor funciona bien, pero el tráfico TCP no pasa por el dispositivo WANOP VPX (inhabilitar el procesamiento de tráfico WANOP funciona bien)?

Compruebe la configuración del firewall en el Cliente, el Servidor y el Router.
Cuando WANOP VPX o Client/Servidor se hospedan como VM, asegúrese de que la suma de comprobación está inhabilitada en la VM de hosts finales.

```
Comandos de Linux de ejemplo:
    ethtool -K eth0 tx off
    ethtool -K eth0 rx off
    ethtool --offload eth0 tx off
    ethtool --offload eth0 rx off
```

Habilite el parámetro Checksum.SendForceSW en ambos VPX WO. Debe estar activado.

```
Ejemplo:
    Checksum.SendForceSW activo
```

¿Hay algún cambio en el proceso de actualización de SDWAN SE/EE/WO Appliance debido al nuevo núcleo WO OS?

No.

Almacenamiento en caché de vídeo

January 10, 2022

¿En qué se diferencia el almacenamiento en caché de vídeo de la compresión basada en disco?

Con el almacenamiento en caché, el dispositivo local sirve una copia local del objeto almacenado en caché, sin descargarlo de nuevo desde el servidor remoto. El almacenamiento en caché no requiere un dispositivo en ambos extremos del vínculo, solo en el extremo local. Con la compresión, el servidor remoto sirve una copia remota del objeto. El dispositivo remoto (del lado del servidor) lo comprime, reduciendo su tamaño y, por lo tanto, aumentando su velocidad de transmisión, y el dispositivo local (del lado del cliente) lo descomprime.

La compresión funciona tanto en objetos modificados como no modificados. Si un archivo cambia un 1% en el servidor, la siguiente transferencia logra una compresión de hasta 99:1.

El almacenamiento en caché solo funciona en objetos no modificados. Si un archivo cambia un 1% en el servidor, la nueva versión debe descargarse en su totalidad. El almacenamiento en caché y la compresión son tecnologías complementarias, porque todo lo que no se almacena en caché, se comprime, logrando los beneficios de ambos.

¿ Puedo dividir la memoria total del dispositivo entre la caché de vídeo y otras características de Citrix SD-WAN WANOP?

No. La partición de caché y la memoria requerida no son configurables.

¿Cuáles son los formatos de contenedor de vídeo compatibles?

El almacenamiento en caché de vídeo es independiente del formato de códec y admite todos los formatos principales de contenedor.

¿Puedo activar el almacenamiento en caché de vídeos empresariales internos y externos en mis propios sitios?

Sí. Si el acceso a estos vídeos es a través de HTTP, puede configurar estos sitios para el almacenamiento en caché.

¿Puedo configurar el tamaño máximo para un objeto almacenado en caché?

Sí. Un objeto mayor que el límite que configura no se almacena en caché. Para establecer este límite, vaya a **Configuración** > **Reglas de optimización** > Almacenamiento en **caché de vídeo** y seleccione el valor entre los límites disponibles.

¿Cómo mejora el almacenamiento en caché de vídeo la experiencia del usuario?

El almacenamiento en caché mejora la experiencia del usuario para los vídeos que se ven más de una vez, especialmente en enlaces más lentos. El primer visor de una secuencia de vídeo determinada no se beneficia de la función de almacenamiento en caché de vídeo, pero las vistas posteriores se entregan a velocidad LAN desde el dispositivo Citrix SD-WAN WANOP, con la ventaja adicional de reducir el uso de WAN.

Además, si un segundo usuario solicita el mismo vídeo mientras se está reproduciendo para el primer usuario, el segundo usuario recibirá la copia almacenada en caché.

A diferencia del funcionamiento normal de Citrix SD-WAN WANOP TCP, donde el dispositivo conserva las direcciones IP de origen y destino originales, el dispositivo reemplaza la dirección de origen del cliente por la dirección IP asignada al puente acelerado, de modo que todo el tráfico HTTP que pasa a través del dispositivo parece originarse del dispositivo en sí.

¿ Qué dispositivos Citrix SD-WAN WANOP admiten el almacenamiento en caché de vídeo?

Los siguientes dispositivos admiten la función de almacenamiento en caché de vídeo:

- Dispositivo SD-WAN WANOP 800 con todos los modelos de licencia de ancho de banda.
- Dispositivo WANOP 1000 SD-WAN con Windows Server, con todos los modelos de licencia de ancho de banda.
- Dispositivo SD-WAN WANOP 2000 con todos los modelos de licencia de ancho de banda.
- Dispositivo WANOP 2000 SD-WAN con Windows Server, con todos los modelos de licencia de ancho de banda.
- Dispositivo SD-WAN WANOP 3000 con todos los modelos de licencia de ancho de banda.

Para el almacenamiento en caché de vídeo, ¿qué modos de implementación son compatibles con un dispositivo Citrix SD-WAN WANOP?

- Implementación admitida: Inline Virtual Inline, VLAN y WCCP
- Funciones no admitidas: alta disponibilidad de Citrix SD-WAN WANOP, modos de grupo y encadenamiento en margarita

¿Qué extensiones de archivo son compatibles con el almacenamiento en caché de vídeo?

El nombre del archivo de vídeo debe tener una de las siguientes extensiones: .3gp, .avi, .dat, .divx, .dv-avi, .flv, .fmv, .h264, .hdmov, .m15, .m1v, .m21, .m2a, .m2v, .m4e .m4v, .m75, .moov, .mov, .movie, .mp21, mp2v, .mp4, .mp4v, .mpe, .mpeg, mpeg4, mpg, mpg2, .mpv, .mts, .ogg, .ogv, .qt, .qtm, .ra, .rm, .ram, .rmd,. rms, rmvb, .rp, rv, .swf, .ts, .vfw, .vob, .webm, .wm, .wma, .wmv y .wtv.

¿ Puedo habilitar la función de almacenamiento en caché de vídeo en una plataforma Citrix SD-WAN WANOP no compatible?

No. La función Almacenamiento en caché de vídeo no se puede utilizar en plataformas no compatibles.

¿Cuáles son la configuración mínima y otros requisitos previos para habilitar la función de almacenamiento en caché de vídeo?

Para habilitar la función de almacenamiento en caché de vídeo, debe:

- Asigne una dirección IP y una puerta de enlace válidas a la interfaz apA y, si está presente, a la interfaz apB.
- En el dispositivo, configure un servidor DNS válido que se pueda resolver en www.citrix.com.
- Tener al menos una aplicación en la lista Aplicaciones de almacenamiento en caché de vídeo seleccionadas.
- Compruebe las alertas GUI WANOP de Citrix SD-WAN o la notificación de alertas de configuración existentes.

¿ Puede el complemento WANOP de Citrix SD-WAN utilizar la función de almacenamiento en caché de vídeo?

No. No puede utilizar la función de almacenamiento en caché de vídeo con el complemento Citrix SD-WAN WANOP.

¿**Cuáles son los exploradores y dispositivos compatibles**?

El almacenamiento en caché de vídeo es compatible con los exploradores Internet Explorer, Firefox y Chrome. Los vídeos se pueden ver en Windows 7 u 8, iPad de Apple y dispositivos Android iOS.

¿ El dispositivo Citrix SD-WAN WANOP admite el almacenamiento en caché de vídeo para todos los sitios web de vídeo?

No. El sitio web de vídeo está disponible y agregado desde la lista Aplicación admitida en la página de configuración de Almacenamiento en caché de vídeo. Por defecto, las aplicaciones compatibles

incluyen YouTube, Vimeo, Youku, Dailymotion y Metacafe. Puede agregar otros sitios web especificando sus direcciones IP, si no utilizan mecanismos de evitación de almacenamiento en caché, como agregar caracteres aleatorios a las direcciones URL.

¿Se admite la supervisión SNMP para el almacenamiento en caché de vídeo?

Sí. Puede utilizar MIB SNMP para supervisar tareas específicas de almacenamiento en caché de vídeo.

¿Se admite el almacenamiento en caché de vídeo para el tráfico que no sea HTTP?

No. El almacenamiento en caché de vídeo no es compatible con el tráfico que no es HTTP, como HTTPs, RTSP y RTMP.

¿Puedo usar el almacenamiento en caché de vídeo con tráfico HTTP enviado a un puerto distinto del puerto 80?

Sí. Para el almacenamiento en caché de vídeo, puede agregar puertos personalizados al dispositivo. Para agregar puertos personalizados para el almacenamiento en caché de vídeo, vaya a la página **Configuración** > **Reglas de optimización** > Almacenamiento en **caché de vídeo** y haga clic en el vínculo **Configuración global** de la ficha **Configuración**.

¿ Se puede usar la compresión WANOP de Citrix SD-WAN (mediante una directiva de clase de servicio HTTP) con el almacenamiento en caché de vídeo?

Sí. Cuando los objetos almacenados en caché están presentes tanto en el historial de compresión WANOP de Citrix SD-WAN como en la caché de vídeo, el contenido se sirve desde la caché en una visita de caché y se obtiene del servidor (y comprimido) en un fallo de caché.

¿Una aplicación HTTP existente que requiere configuración de dirección IP cuando hay un proxy transparente, requiere algún cambio?

Sí.Citrix SD-WAN WANOP realiza proxy transparente HTTP, en el que reemplaza la dirección IP de origen del paquete. Por lo tanto, si la aplicación HTTP existente tiene ciertas directivas (como bloquear determinadas direcciones IP o mecanismos de proxy), esas directivas tienen que cambiarse.

¿Cuáles son los límites de memoria del sistema y conexión para la conexión proxy HTTP?

Para determinar los límites, compruebe los gráficos y las estadísticas en la página Depuración de caché de vídeo (support.html). Además, compruebe que el comando Videocaching.cmd stats info muestra la siguiente información.

	SD-WAN WANOP 800	SD-WAN 1000 con Windows Server	SD-WAN 2000 con Windows Server	SD-WAN 2000	SD-WAN 3000
——	——-	——	——	——	——
Disco	25 GB	25 GB	50 GB	50 GB	99 GB
RAM	375 MB	375 MB	700 MB	700 MB	1024 MB
Límite total de conexiones HTTP	1000	1000	1500	1500	3000

| Límite máximo de escritura HTTP | 200 | 200 | 300 |
300 | 600 |

Después de alcanzar los límites de conexión HTTP anteriores, se pasan por alto las nuevas conexiones.

> **Nota**
>
> Asegúrese de no cambiar la configuración anterior.

¿La página Supervisión para el almacenamiento en caché de vídeo incluye solo el tráfico de vídeo?

Sí. El tráfico HTTP que no sea de vídeo (aunque sea interceptado por el proxy), no se incluye en las estadísticas de la GUI de almacenamiento en caché de vídeo.

¿ Es necesario configurar las interfaces APB y APB con una dirección IP válida en un dispositivo Citrix SD-WAN WANOP?

No. No es necesario asignar una dirección IP válida a ambas interfaces. Los paquetes HTTP recibidos desde la interfaz apA se envían por proxy con la dirección IP de apA, y los paquetes HTTP recibidos desde la interfaz apB se envían por proxy con la dirección IP de apB.

Si no configura una dirección IP para una interfaz, los paquetes HTTP recibidos en esa interfaz no obtienen el beneficio del almacenamiento en caché.

¿Cuál es el límite mínimo y máximo para el tamaño de un archivo de vídeo que se puede almacenar en caché?

- Mínimo: 100 KB
- Máximo: 300 MB
- Valor predeterminado: 100 MB

¿Cómo se borra el disco de almacenamiento en caché de vídeo?

Los objetos almacenados en caché se borran según lo especificado por el algoritmo de uso menos reciente.

¿Qué ocurre cuando actualizo el dispositivo Citrix SD-WAN WANOP de la versión 6.x a la 7.y, y el almacenamiento en caché de vídeo está habilitado?

El historial existente de Citrix SD-WAN WANOP DBC se pierde y se crea una partición independiente para el almacenamiento en caché de vídeo.

¿ Qué ocurre cuando desnivel el dispositivo Citrix SD-WAN WANOP de la versión 7.y a la 6.x y se habilita el almacenamiento en caché de vídeo?

Se conserva el historial de almacenamiento en caché de vídeo y DBC de Citrix SD-WAN WANOP. Sin embargo, la función de almacenamiento en caché de vídeo no está disponible con la versión 6.x.

¿ Qué ocurre cuando actualizo el dispositivo Citrix SD-WAN WANOP de la versión 7.x a 7.y y se habilita el almacenamiento en caché de vídeo?

Se conserva el historial de almacenamiento en caché de vídeo y DBC de Citrix SD-WAN WANOP.

Tengo una sola red en la sucursal que comparte una gestión, así como tráfico de datos. ¿Cómo debo configurar el almacenamiento en caché de vídeo en esta red?

Si tiene una sola red para la administración y el tráfico de datos, Citrix recomienda agregar la dirección IP principal al lado LAN del puerto de puente acelerado.

¿Cuál es el número máximo de tareas de prerrellenado que puedo ejecutar al mismo tiempo?

Uno. Si intenta iniciar varias tareas de prerrellenado al mismo tiempo, el dispositivo crea una cola de tareas por orden de salida.

¿Cuál es el número máximo de fuentes de vídeos que puedo configurar en el dispositivo?

100

¿Cuál es el número máximo de entradas de prerrellenado que puedo agregar al dispositivo?

50

¿Cuál es el número máximo de archivos de vídeo que se descargan y se almacenan en caché desde una carpeta de la lista de directorios?

300

¿**La descarga de vídeo y el almacenamiento en caché iniciados por la función de prerrellenado obtienen los beneficios de compresión basada en disco (DBC)**?

Sí. Dado que el archivo de vídeo está almacenado en caché, el intento de acceder al vídeo se sirve desde la caché.

Aceleración de Office 365

April 23, 2021

1. ¿Por qué analizamos el SAN?

   Es tedioso crear múltiples perfiles para nombres FQDN para cada uno de los dominios, para superar esto analizamos el SAN a partir de los certificados.

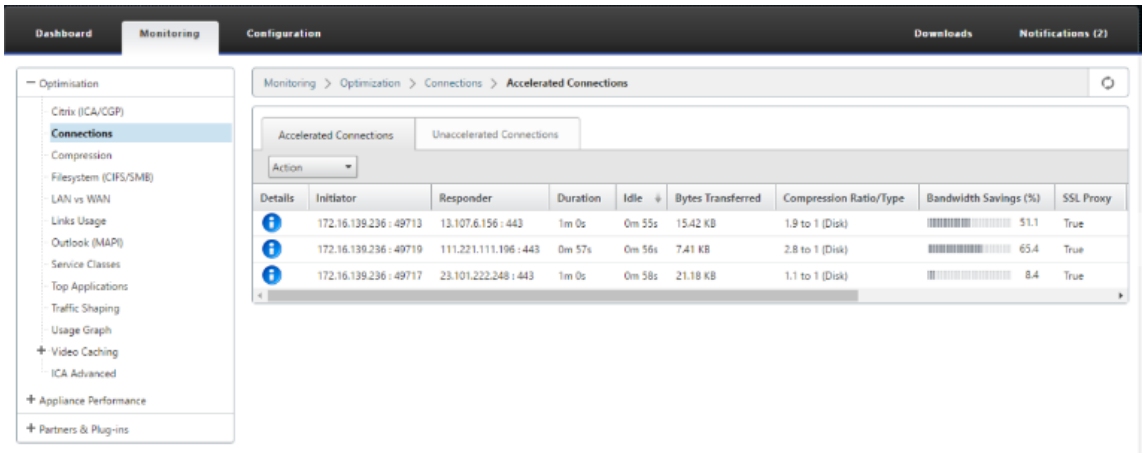
2. ¿Qué es una lista de exclusión?

   Se muestra un mensaje de error o advertencia Si el navegador o la aplicación no contienen el certificado de CA, en tales casos la dirección IP del cliente se agregará a una lista de exclusión

después de algunos intentos de conexión desde el navegador/aplicación (2-3 veces). En el siguiente intento, la conexión no es proxy SSL y la página se carga sin ningún error o advertencia. La dirección IP del cliente permanecerá en la lista de exclusión durante 48 horas. La lista de exclusión se mantiene solo para el proxy dividido.

3. ¿Dónde verificar la información de conexión de aceleración de Office 365?

   Vaya a**Supervisión** > **Conexiones > Conexionesaceleradas**, compruebe el estado del proxy SSL. Para obtener detalles de la conexión, haga clic en el icono de detalles.



4. ¿Qué sucede si la opción de excluir lista no está habilitada de forma predeterminada como parte de la configuración del perfil SSL?

   Si el explorador web o la aplicación no contienen el certificado de CA, muestra un error o advertencia y las conexiones de ese cliente o aplicación se bloquearán. Para evitar estos problemas, seleccione la opción **Excluir lista** como parte de la configuración del perfil SSL.

5. ¿Qué sucede si las SAN requeridas no forman parte del certificado proxy configurado o creado?

   Las conexiones no serán proxy SSL y no habrá beneficios de aceleración para conexiones SSL no proxy.

6. ¿Qué sucede cuando el cliente no forma parte del dominio o si el cliente no tiene el certificado raíz del dominio?

   Las conexiones se bloquean si la lista de exclusión no está habilitada.

7. ¿Qué sucede si el lado del centro de datos Citrix SD-WAN WANOP no tiene CA raíz o intermedia?

   Las conexiones están bloqueadas o las páginas de aplicación de Office 365 que requieren las CA raíz o intermedias que faltan están parcialmente cargadas. Para desbloquear las conexiones o tener estas páginas completamente cargadas, agregue los certificados de CA apropiados o inhabilite el perfil SSL de la aceleración.

8. ¿Cómo saber qué clientes están excluidos de la aceleración?

La información de cliente excluida se puede conocer de los registros o mediante el comando CLI *show ssl-exclude -list*.

9. ¿Qué hacer cuando se excluye a los clientes?

   De forma predeterminada, la información de la lista de exclusión del dispositivo se borrará después de 48 horas. El usuario puede borrar por la fuerza la información de la lista de exclusión mediante comandos CLI *clear ssl-exclude-list -/*<all> <Client_IP>.

10. ¿Cómo saber qué conexiones SSL (SNI) no son proxy?

    Desde los registros o usando el comando CLI*show ssl-non-proxied-sni*, puede conocer la lista de los SNI no proxy.

11. ¿Cómo borrar SNI no proxy?

    Utilizando el comando CLI*clear ssl-non-proxied-sni - <all>/<server name identifier>.*

12. ¿Cuál es el tiempo predeterminado para el cliente en estado de exclusión?

    El cliente permanece en estado de exclusión durante 48 horas.

13. ¿Podemos tener varios perfiles aplicados para una clase de servicio en particular?

    Sí, podemos aplicar clases de servicio con múltiples perfiles SSL.

    Para ello, en el dispositivo WAN virtual, vaya a **Configuración** > **Clase de servicio** > **Web (Internet Secure)** > **Modificar** > **Modificar** (Aplicación) y agregue los perfiles disponibles.

14. ¿Cómo se verifica el motivo de las conexiones no proxy?

    Compruebe la página de conexión TCP, para obtener más información, consulte los registros. Para depurar los problemas de conexión no proxy, haga lo siguiente.

    a) Si el registro no muestra ninguna configuración válida -
       Establezca la configuración válida. Para obtener más información sobre cómo configurar la función Office 365, consulte Aceleración de Office 365.

    b) Si el registro muestra que no se pudo verificar la certificación, agregue certificados de CA válidos al dispositivo Citrix SD-WAN WANOP del lado del centro de datos.

    c) <Client\ _IP\ >si el registro muestra cliente excluido: la información sobre los clientes excluidos se puede borrar del dispositivo mediante el comando CLI *clear ssl-exclude-list -\/ <all\ > *.

Notas adicionales

- El registro en el cliente de OneDrive a veces muestra un mensaje de advertencia «advertencia falsa», Este es un problema conocido de Microsoft (https://support.microsoft.com/en-us/kb/3097938) y no específico del dispositivo Citrix SD-WAN WANOP.

- Para que las páginas redirigidas de Office 365 sean proxy, se recomienda crear un certificado proxy independiente que contenga la lista SAN correspondiente al certificado de las páginas redirigidas. Cree otro perfil con este certificado proxy y aplíquelo a la clase de servicio. También agregue la CA relevante en el dispositivo Citrix SD-WAN WANOP.
- A veces el explorador web no muestra los certificados de CA correctos, en tales casos usa Wireshark o OpenSSL para obtener los nombres de CA raíz e intermedia y obtener los certificados de origen 'auténtico'(por ejemplo, almacén SSL de Windows).
- Se puede observar una diferencia en el comportamiento del explorador al acceder a las aplicaciones de Office 365 desde diferentes exploradores que no tienen certificados requeridos y con la opción Excluir lista deshabilitada.
- Cuando las conexiones de Office 365 son proxy SSL (es decir, proxy SSL establecido en True) y en el explorador se muestra el certificado de Office 365 en lugar del certificado proxy, se recomienda abrir el explorador web en modo incógnito y comprobar el comportamiento o borrar la caché y, a continuación, comprobar el comportamiento de nuevo.
- Microsoft Office 365 incluye muchos componentes y aplicaciones como OneDrive, Outlook, SharePoint, Word, PPT, Excel y OneNote. Todas estas aplicaciones han sido probadas y se sabe que funcionan sin ningún problema. Se espera que otras aplicaciones funcionen también sin problemas; sin embargo, este estado puede cambiar con el tiempo y es posible que se produzcan problemas desconocidos.

Compresión

April 23, 2021

La compresión de Citrix SD-WAN WANOP utiliza tecnología innovadora para proporcionar una compresión transparente de varios niveles. Es la compresión verdadera que actúa sobre flujos de bytes arbitrarios. No es consciente de la aplicación, es indiferente a los límites de conexión y puede comprimir una cadena de forma óptima la segunda vez que aparece en los datos.La compresión WANOP de Citrix SD-WAN funciona a cualquier velocidad de enlace.

El motor de compresión es muy rápido, lo que permite que el factor de aceleración de la compresión se aproxime a la relación de compresión. Por ejemplo, una transferencia masiva monopolizando un enlace T1 de 1,5 Mbps y logrando una relación de compresión de 100:1 puede ofrecer una relación de aceleración de casi 100x, o 150 Mbps, siempre que el ancho de banda WAN sea el único cuello de botella en la transferencia.

A diferencia de la mayoría de los métodos de compresión, el historial de compresión WANOP de Citrix SD-WAN se comparte entre todas las conexiones que pasan entre los mismos dos dispositivos. Los

datos enviados horas, días o incluso semanas antes por la conexión A pueden ser referidos más adelante por la conexión B, y reciben el beneficio de aceleración total de la compresión. El rendimiento resultante es mucho mayor de lo que se puede lograr con métodos convencionales.

La compresión puede utilizar el disco del dispositivo, así como la memoria, lo que proporciona hasta terabytes de historial de compresión.

Cómo funciona la compresión

Todos los algoritmos de compresión exploran los datos que se van a comprimir, buscando cadenas de datos que coincidan con cadenas que se han enviado antes. Si no se encuentran tales coincidencias, se envían los datos literales. Si se encuentra una coincidencia, los datos coincidentes se reemplazan con un puntero a la ocurrencia anterior. En una cadena coincidente muy grande, los megabytes o incluso gigabytes de datos pueden representarse mediante un puntero que contenga solo unos pocos bytes, y solo esos pocos bytes deben enviarse a través del enlace.

Los motores de compresión están limitados por el tamaño de su historial de compresión. Los algoritmos de compresión tradicionales, como LZS y ZLIB, utilizan historiales de compresión de 64 KB o menos.Los dispositivos WANOP de Citrix SD-WAN mantienen al menos 100 GB de historial de compresión. Con más de un millón de veces el historial de compresión de los algoritmos tradicionales, el algoritmo WANOP de Citrix SD-WAN encuentra más coincidencias y coincidencias más largas, lo que da como resultado una relación de compresión superior.

El algoritmo de compresión WANOP de Citrix SD-WAN es muy rápido, de modo que incluso los dispositivos de nivel básico pueden saturar una LAN de 100 Mbps con la salida del compresor. Los modelos de mayor rendimiento pueden ofrecer más de 1 Gbps de rendimiento.

Solo se comprimen los datos de carga útil. Sin embargo, los encabezados se comprimen indirectamente. Por ejemplo, si una conexión alcanza la compresión 4:1, solo se envía un paquete de salida de tamaño completo por cada cuatro paquetes de entrada de tamaño completo. Por lo tanto, la cantidad de datos de encabezado también se reduce en 4:1.

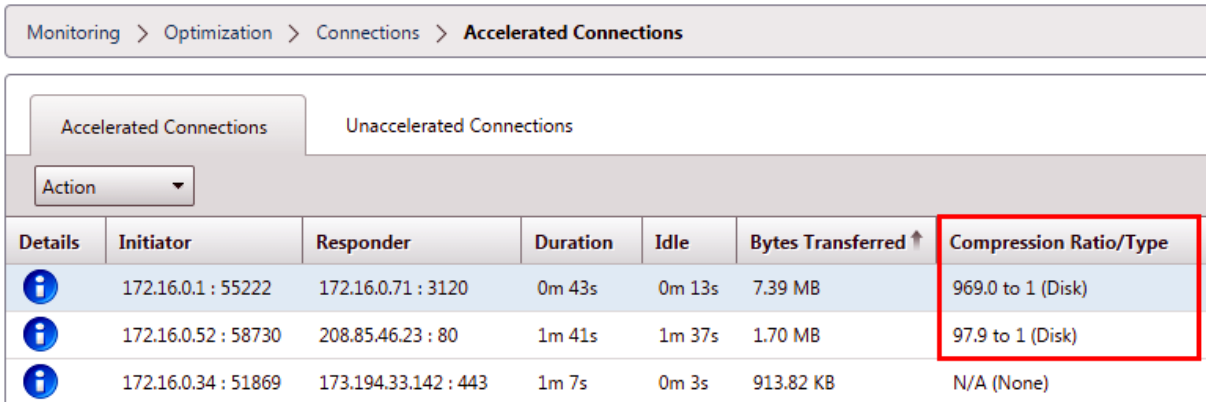
Compresión como optimización de propósito general:

La compresión WANOP de Citrix SD-WAN es independiente de la aplicación: puede comprimir datos de cualquier conexión TCP no cifrada.

A diferencia del almacenamiento en caché, el rendimiento de compresión es sólido frente a los datos cambiantes. Con el almacenamiento en caché, cambiar un solo byte de un archivo invalida toda la copia en la caché. Con la compresión, cambiar un solo byte en el medio de un archivo simplemente crea dos coincidencias grandes separadas por un solo byte de datos que no coinciden, y el tiempo de transferencia resultante es solo ligeramente mayor que antes. Por lo tanto, la relación de compresión se degrada con gracia con la cantidad de cambio. Si descarga un archivo, cambia el 1% y vuelve a subirlo, espera una relación de compresión de 99:1 en la carga.

Otra ventaja de un gran historial de compresión es que los datos precomprimidos se comprime fácilmente con la tecnología Citrix SD-WAN WANOP. Una imagen JPEG o un vídeo de YouTube, por ejemplo, está precomprimido, dejando pocas posibilidades de compresión adicional la primera vez que se envía a través del enlace. Pero cada vez que se envía de nuevo, la transferencia completa se reduce a solo un puñado de bytes, incluso si es enviada por diferentes usuarios o con diferentes protocolos, como por ejemplo por FTP la primera vez y HTTP el siguiente.

En la práctica, el rendimiento de compresión depende de la cantidad de datos que atraviesan el vínculo es la misma que los datos que han atravesado previamente el vínculo. La cantidad varía de una aplicación a otra, de un día a otro, e incluso de un momento a otro. Cuando vea una lista de conexiones aceleradas activas, espere ver relaciones entre 1:1 y 10 000:1.

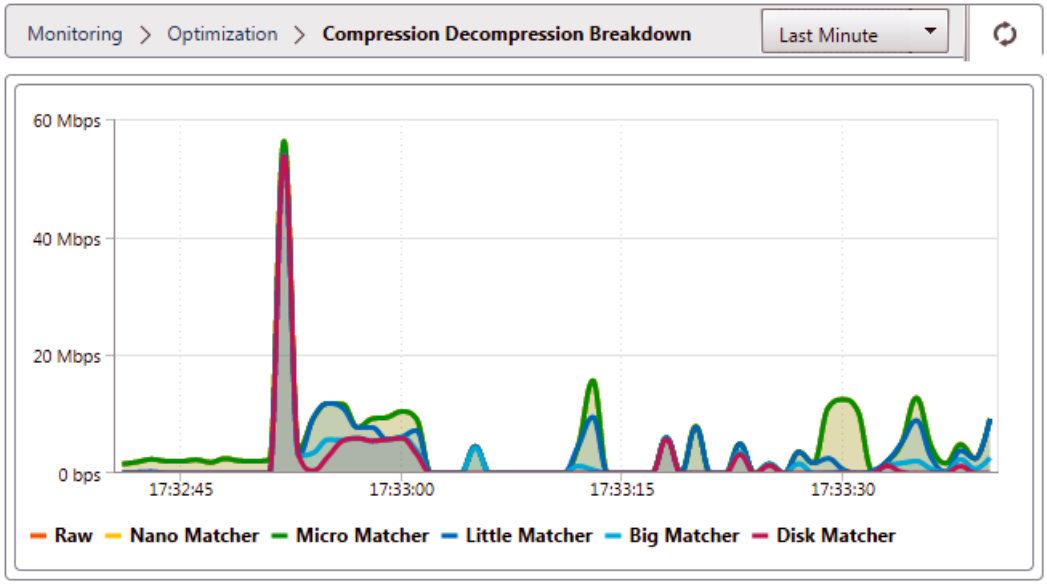


Comprimir protocolos cifrados:

Muchas conexiones que muestran un rendimiento de compresión deficiente lo hacen porque están cifradas. El tráfico cifrado normalmente no se puede comprimir, pero los dispositivos Citrix SD-WAN WANOP pueden comprimir conexiones cifradas cuando los dispositivos se unen a la infraestructura de seguridad.Los dispositivos WANOP de Citrix SD-WAN se unen automáticamente a la infraestructura de seguridad con Citrix Citrix Virtual Apps and Desktops, y pueden unirse a la infraestructura de seguridad de servidores SSL, sistema de archivos Windows (CIFS/SMB) y Outlook/Exchange (MAPI) con configuración manual.

Operación adaptativa de configuración cero:

Para satisfacer las diferentes necesidades de diferentes tipos de tráfico, los dispositivos Citrix SD-WAN WANOP utilizan no uno, sino cinco motores de compresión, por lo que las necesidades de todo, desde la transferencia masiva más masiva hasta el tráfico interactivo más sensible a la latencia, se pueden satisfacer con facilidad. El motor de compresión se adapta dinámicamente a las necesidades cambiantes de las conexiones individuales, de modo que la compresión se optimiza automáticamente. Una ventaja adicional es que el motor de compresión no requiere configuración.



Compresión basada en memoria

La mayoría de los motores de compresión usan RAM para almacenar su historial de compresión. Esto se denomina compresión basada en memoria. Algunos dispositivos dedican gigabytes de memoria a estos motores de compresión. La compresión basada en memoria tiene una latencia baja y a menudo se elige automáticamente para tareas interactivas como el tráfico de Virtual Apps/Virtual Desktops.

Compresión basada en disco

El motor de compresión basado en disco utiliza entre decenas de gigabytes y terabytes de memoria para almacenar el historial de compresión, lo que permite más y mejores coincidencias de compresión. El motor de compresión basado en disco es muy rápido, pero a veces tiene una latencia más alta que los motores basados en memoria, y a menudo se elige automáticamente para transferencias masivas.

Habilitar o inhabilitar la compresión

La compresión está activada, por clase de servicio, en la página
Configuración: Clases de Servicio. Esta página tiene un menú desplegable para cada clase de servicio, con las siguientes opciones:

- **Disco**, lo que significa que la compresión basada en disco y la compresión basada en memoria están habilitadas. Esta opción debe seleccionarse a menos que tenga un motivo específico para desactivarla.

- **Memoria**, lo que significa que la compresión basada en memoria está habilitada pero la compresión basada en disco no lo está. Esta configuración rara vez se utiliza, ya que el dispositivo selecciona automáticamente la memoria o el disco si ambos tipos de compresión están habilitados.
- **Solo control de flujo**, que inhabilita la compresión pero habilita la aceleración de control de flujo. Seleccione esta opción para los servicios que siempre están cifrados y para el canal de control FTP.
- **Ninguno**, lo que significa que la compresión y el control de flujo están inhabilitados.

Para obtener más información, consulte Clases de Servicio.

Medir el rendimiento de compresión basado en disco

La ficha Estado de compresión de la página
Informes: Compresión informa del rendimiento de compresión del sistema desde que se inició el sistema o desde que se utilizó el botón Borrar para restablecer las estadísticas. La compresión para conexiones individuales se informa en los mensajes de cierre de conexión en el registro del sistema.

El rendimiento de compresión varía según una serie de factores, incluida la cantidad de redundancia en el flujo de datos y, en menor medida, la estructura del protocolo de datos.

Algunas aplicaciones, como FTP, envían flujos de datos puros; la carga útil de la conexión TCP siempre es idéntica byte por byte al archivo de datos original. Otros, como CIFS o NFS, no envían flujos de datos puros, sino que mezclan comandos, metadatos y datos en la misma secuencia. El motor de compresión distingue los datos del archivo mediante el análisis de la carga útil de la conexión en tiempo real. Tales flujos de datos pueden producir fácilmente relaciones de compresión entre 100:1 y 10 000:1 en la segunda pasada.

Las proporciones medias de compresión para el enlace dependen de la prevalencia relativa de las coincidencias largas, las coincidencias cortas y las no coincidencias. Esta relación depende del tráfico y es difícil de predecir en la práctica.

Los resultados de las pruebas muestran el efecto de la compresión multinivel en su conjunto, con la compresión basada en memoria y en disco haciendo su contribución.

El rendimiento máximo de compresión no se logra hasta que se llena el espacio de almacenamiento disponible para la compresión basada en disco, lo que proporciona una cantidad máxima de datos anteriores para que coincidan con los datos nuevos. En un mundo perfecto, las pruebas no concluirían hasta que los discos del dispositivo no solo se hubieran llenado, sino que se hubieran llenado y sobrescrito al menos una vez, para garantizar que se hubiera alcanzado el funcionamiento en estado estacionario. Sin embargo, pocos administradores tienen esa cantidad de datos representativos a su disposición.

Otra dificultad en las pruebas de rendimiento es que la aceleración a menudo expone enlaces débiles en la red, normalmente en el rendimiento del cliente, el servidor o la LAN, y a veces se diagnostica erróneamente como rendimiento de aceleración decepcionante.

Puede usar Iperf o FTP para pruebas preliminares e iniciales. Iperf es útil para pruebas preliminares. Es extremadamente compresible (incluso en la primera pasada) y utiliza relativamente poca CPU y ningún recurso de disco en los dos sistemas de punto final. El rendimiento comprimido con Iperf debe enviar más de 200 Mbps a través de un enlace T1 si las LAN de ambos lados utilizan Gigabit Ethernet, o ligeramente menos de 100 Mbps si hay algún equipo Fast Ethernet en las rutas LAN entre los extremos y los dispositivos.

Iperf está preinstalado en los dispositivos (en el menú Diagnóstico) y está disponible desdehttp://iperf.sourceforge.net/. Idealmente, debería instalarse y ejecutarse desde los sistemas de punto final, de modo que la red se pruebe de extremo a extremo, no solo de dispositivo a dispositivo.

FTP es útil para pruebas más realistas de lo que es posible con Iperf. FTP es simple y familiar, y sus resultados son fáciles de interpretar. El rendimiento de segundo paso debe ser más o menos el mismo que con Iperf. De lo contrario, el factor limitante es probablemente el subsistema de disco en uno de los sistemas de punto final.

Para probar el sistema de compresión basado en disco:

1. Transferir una secuencia de datos de varios gigabytes entre dos dispositivos con compresión basada en disco habilitada. Tenga en cuenta la compresión lograda durante esta transferencia. Dependiendo de la naturaleza de los datos, se puede observar una compresión considerable en la primera pasada.
2. Transfiera la misma secuencia de datos por segunda vez y observe el efecto sobre la compresión.

Informes de compresión en edición premium

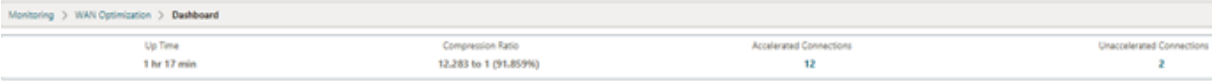
Citrix SD-WAN Premium (Enterprise) Edition no tiene una vista para mostrar informes de compresión por protocolo o aplicación a través de clases de servicio WANOP, que tienen la asociación de protocolo o aplicación. Si utiliza un dispositivo de edición Premium (Enterprise), el único informe disponible para la compresión es un informe de compresión de nivel de conexión que no da visibilidad a la medida en que se ha optimizado o comprimido un protocolo. Los informes de compresión están disponibles en la GUI de optimización de WAN, que muestra una ruptura de todos los protocolos únicos y cómo los informes se han optimizado durante un período de tiempo.

En la GUI del dispositivo Citrix SD-WAN Premium (Enterprise) Edition, para la optimización de WAN, se han agregado los siguientes widgets en el panel de optimización de WAN.

- Relación de compresión consolidada: todo el tráfico que pasa a través del dispositivo WANOP y número total de conexiones aceleradas y no aceleradas. Esto le permite supervisar el tráfico total transmitido de LAN a WAN.
- Relación de compresión: las 10 mejores clases de servicio.
- Rendimiento de enlace agregado: LAN y WAN.

Relación de compresión consolidada:

Este informe muestra la relación de compresión consolidada para todo el tráfico transmitido a WANOP y el número total de conexiones aceleradas y no aceleradas. También muestra el tiempo de actividad del servicio WANOP en el dispositivo.



Rendimiento agregado de enlaces:

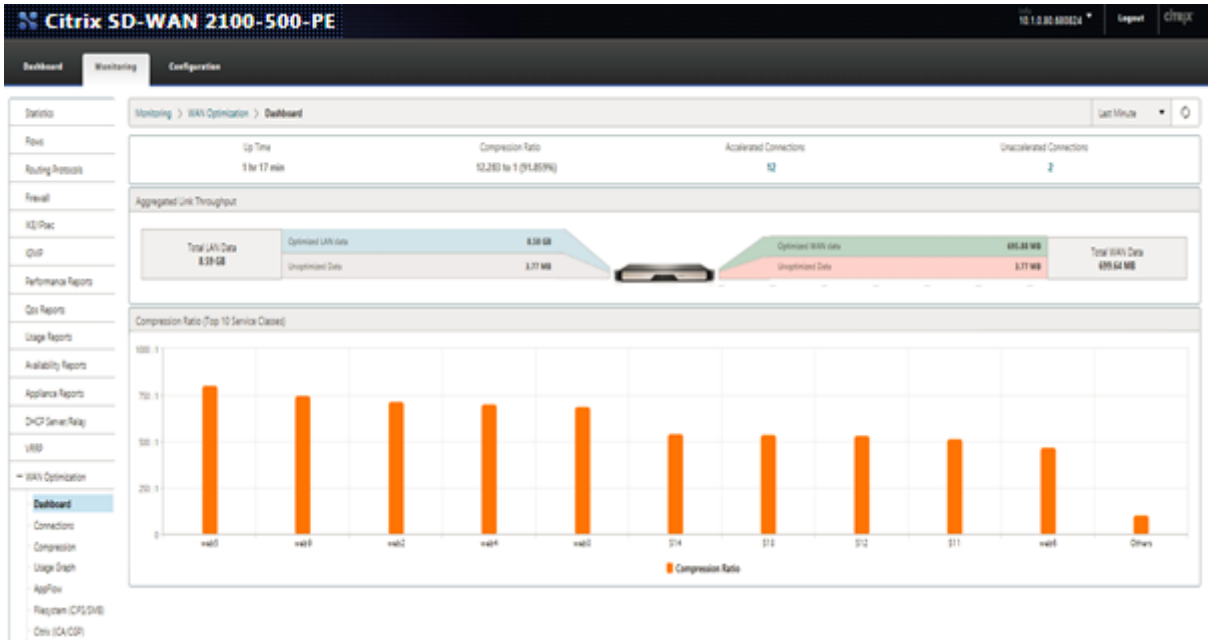
Este informe muestra el tráfico total que se transmite a WANOP y el tráfico total que transmite con rupturas en categorías de datos optimizados y no optimizados en ambos extremos.

Relación de compresión (las 10 clases de servicio principales):

En la GUI del dispositivo Citrix SD-WAN, puede comprobar los detalles de la conexión y la relación de compresión (por panel de clase de servicio) navegando a **Monitoring** > **WAN Optimization**. Esta opción selecciona automáticamente el nodo Panel y proporciona una visión general en forma de panel.

El gráfico muestra los 10 valores principales de la relación de compresión para el tráfico clasificado por clases de servicio.

Se muestra una barra adicional otros, que muestra la relación de compresión de todas las demás conexiones aceleradas que forman parte del sistema, además de los informes de relación de compresión de las 10 clases de servicio principales.



Aceleración HTTP

April 23, 2021

El acelerador WANOP de Citrix SD-WAN utiliza una variedad de optimizaciones de configuración cero para acelerar el tráfico HTTP. Esto, a su vez, acelera las páginas web y cualquier otra aplicación que utilice el protocolo HTTP (descargas de archivos, transmisión de vídeo, actualizaciones automáticas, etc.).

Las optimizaciones que aceleran HTTP incluyen compresión, modelado del tráfico, control de flujo y almacenamiento en caché.

Compresión

HTTP es una aplicación ideal para la compresión multinivel WANOP de Citrix SD-WAN.

El contenido estático, incluidas páginas HTML estándar, imágenes, vídeo y archivos binarios, recibe cantidades variables de compresión de primer paso, normalmente 1:1 en contenido binario precomprimido, y 2:1 o más en contenido basado en texto. A partir de la segunda vez que se ve el objeto, los dos motores de compresión más grandes (compresión basada en memoria y compresión con base en disco) ofrecen relaciones de compresión extremadamente altas, con objetos más grandes que reciben relaciones de compresión de 1000:1 o más. Con tan altas proporciones de compresión, el enlace WAN deja de ser el factor limitante y el servidor, el cliente o la LAN se convierte en el cuello de botella.

El dispositivo cambia entre compresores dinámicamente para ofrecer el máximo rendimiento. Por ejemplo, el dispositivo utiliza un compresor más pequeño en el encabezado HTTP y uno más grande en el cuerpo HTTP.

El contenido dinámico, incluidos los encabezados HTTP y las páginas generadas dinámicamente, páginas que nunca son iguales dos veces pero tienen similitudes entre sí, se comprimen por los tres motores de compresión que tratan con coincidencias más pequeñas. La primera vez que se ve una página, la compresión es buena. Cuando se ve una variante en una página anterior, la compresión es mejor.

Modelado del tráfico

HTTP consiste en una mezcla de tráfico interactivo y masivo. El tráfico de cada usuario es una mezcla de ambos, y a veces la misma conexión contiene una mezcla de ambos. El formador de tráfico garantiza de forma fluida y dinámica que cada conexión HTTP obtenga su parte justa del ancho de banda del enlace, evitando que las transferencias masivas monopolicen el enlace a expensas de los usuarios interactivos, al tiempo que garantiza que las transferencias masivas obtengan cualquier ancho de banda que las conexiones interactivas no utilicen.

Control de flujo

Los algoritmos avanzados de retransmisión y otras optimizaciones a nivel de TCP conservan la capacidad de respuesta y mantienen las tasas de transferencia frente a la latencia y la pérdida.

Almacenamiento en caché de vídeo

El almacenamiento en caché HTTP para archivos de vídeo se introdujo en la versión 7.0 El almacenamiento en caché implica guardar objetos HTTP en el almacenamiento local y servirlos a clientes locales sin volver a cargarlos desde el servidor.

¿Cuál es la diferencia entre el almacenamiento en caché y la compresión? Mientras que el almacenamiento en caché proporciona una aceleración similar a la compresión, los dos métodos son diferentes, haciéndolos complementarios.

- La compresión acelera las transferencias desde el servidor remoto, y esta velocidad de datos más alta puede colocar una carga más alta en el servidor si la compresión no estaba presente. El almacenamiento en caché impide las transferencias desde el servidor y reduce la carga en el servidor.
- La compresión funciona en cualquier flujo de datos, esto es similar a una transferencia anterior: si cambia el nombre de un archivo en el servidor remoto y lo transfiere de nuevo, la compresión

funcionará perfectamente. El almacenamiento en caché solo funciona cuando se sabe que el objeto solicitado por el cliente y el objeto en el disco son idénticos. Si cambia el nombre de un archivo en el servidor remoto y lo transfiere de nuevo, no se utiliza la copia almacenada en caché.

- Los datos comprimidos no se pueden entregar más rápido que el servidor puede enviarlos. Los datos almacenados en caché dependen únicamente de la velocidad del dispositivo del cliente.
- La compresión requiere mucha CPU; el almacenamiento en caché no lo es.

Cómo funciona HTML5

April 23, 2021

HTML5 utiliza HTTP, que es un protocolo de solicitud/respuesta para la comunicación entre clientes y servidores. Un cliente inicia una conexión TCP y la utiliza para enviar solicitudes HTTP al servidor. El servidor responde a estas solicitudes otorgando derechos de acceso a los recursos disponibles. Después de que el cliente y el servidor establecen una conexión, los mensajes intercambiados entre ellos contienen solo encabezados WebSocket, no encabezados HTTP.

La infraestructura de HTML5 consiste en WebSockets, que utilizan aún más la infraestructura HTTP existente para proporcionar un mecanismo ligero para la comunicación entre un cliente y un servidor web. Normalmente se implementa el protocolo WebSocket en un explorador y servidores web. Sin embargo, puede utilizar este protocolo con cualquier aplicación cliente o servidor.

Cuando un cliente intenta realizar una conexión mediante WebSockets, los servidores web tratan el protocolo WebSocket como una solicitud de actualización y el servidor cambia al protocolo WebSocket. El protocolo WebSocket permite la interacción frecuente entre el explorador y los servidores web. Por lo tanto, puede utilizar este protocolo para actualizaciones en vivo, como índices de acciones y tarjetas de puntuación, e incluso juegos en vivo. Esto es posible debido a una forma estandarizada para que el servidor envíe respuestas no solicitadas al cliente mientras mantiene una conexión abierta para la comunicación continua bidireccional entre el explorador del cliente y el servidor.

> **Nota**
>
> También puede lograr este efecto, de formas no estandarizadas, mediante el uso de varias otras tecnologías, como Comet. Para obtener más información acerca de Comet, consultehttp://en.wikipedia.org/wiki/Comet_(programming).

El protocolo WebSocket se comunica a través de los puertos TCP 80 y 443. Esto facilita la comunicación en entornos que utilizan firewalls para bloquear conexiones a Internet no web. Además, WebSocket tiene su propio mecanismo de fragmentación. Un mensaje WebSocket se puede enviar como múltiples fotogramas de WebSocket.

> **Nota**
>
> No puede utilizar WebSocket si las aplicaciones web de los servidores no lo admiten.

Cómo HTML5 establece una sesión WebSocket

Un explorador web compatible con HTML5 utiliza API de JavaScript para realizar las siguientes tareas:

- Abra una conexión WebSocket.
- Comunicarse a través de la conexión WebSocket.
- Cierre las conexiones WebSocket.

Para abrir una conexión WebSocket, el explorador web envía un mensaje de actualización HTTP al servidor para cambiar al protocolo WebSocket. El servidor acepta o rechaza esta solicitud. Los siguientes son fragmentos de una solicitud de cliente de ejemplo y respuesta del servidor:

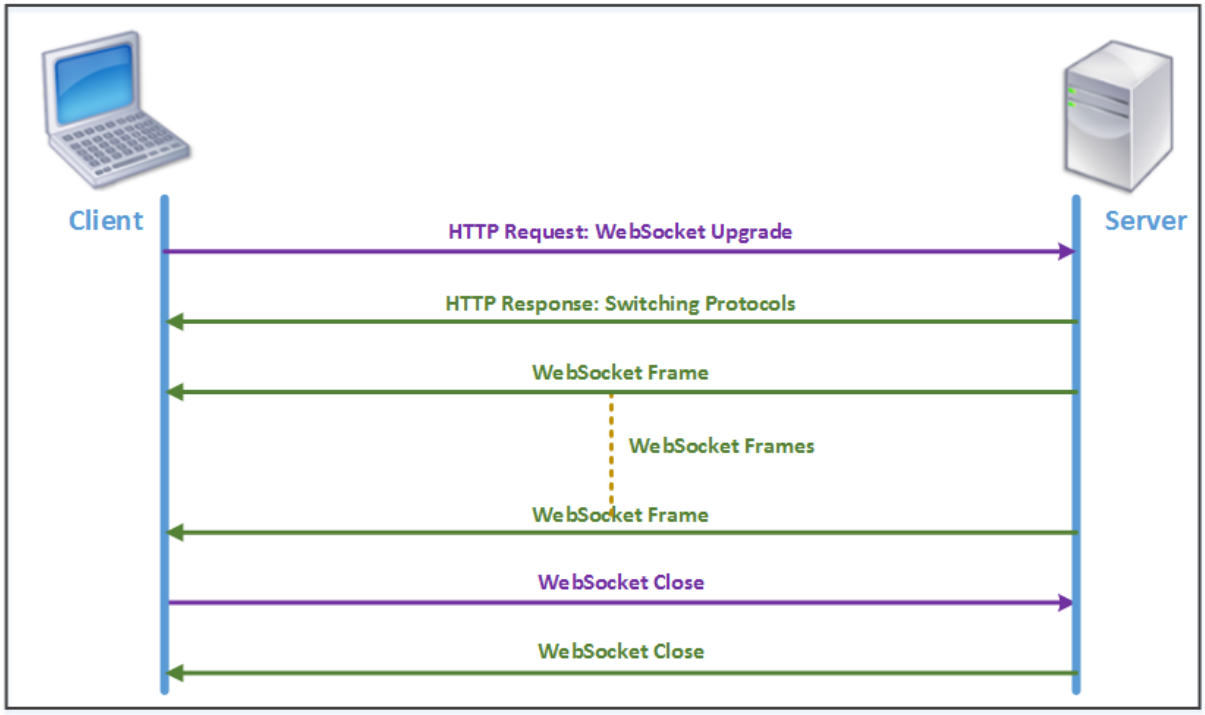
- Solicitud de cliente de ejemplo

  ```
  pre codeblock GET /HTTP/1.1 Upgrade: websocket Sec-websocket-
  protocol: <List of protocols that the client supports over this
   websocket session, such as an application level protocol, for
   example ICA.> Sec-websocket-extensions: <List of extensions
  client wants applied to this session, such as compression.> Sec-
  Websocket-version: <Version of websocket protocol that the client
   intends to use.> <!--NeedCopy-->
  ```

- Respuesta del servidor de ejemplo

  ```
  pre codeblock HTTP/1.1 101 Switching Protocols Upgrade: websocket
   Connection: Upgrade Sec-Websocket-Protocol: <One from the list
  of protocols in the client request.> Sec-Websocket-extensions:
  <List of extensions server accepts for session.> Sec-Websocket-
  version: <Version of websocket protocol that the server supports
  .> <!--NeedCopy-->
  ```

La siguiente imagen muestra la secuencia de mensajes intercambiados entre un cliente y un servidor:



Durante una conexión HTML5, se intercambian los siguientes mensajes entre el cliente y el servidor:

- El cliente envía una solicitud HTTP para actualizar WebSocket.
- El servidor responde a la solicitud del cliente y cambia al protocolo WebSocket.
- El servidor envía fotogramas de WebSocket al cliente.
- El cliente envía una solicitud para cerrar el WebSocket.
- El servidor cierra el WebSocket.

Aceleración del Protocolo de Internet versión 6 (IPv6)

April 23, 2021

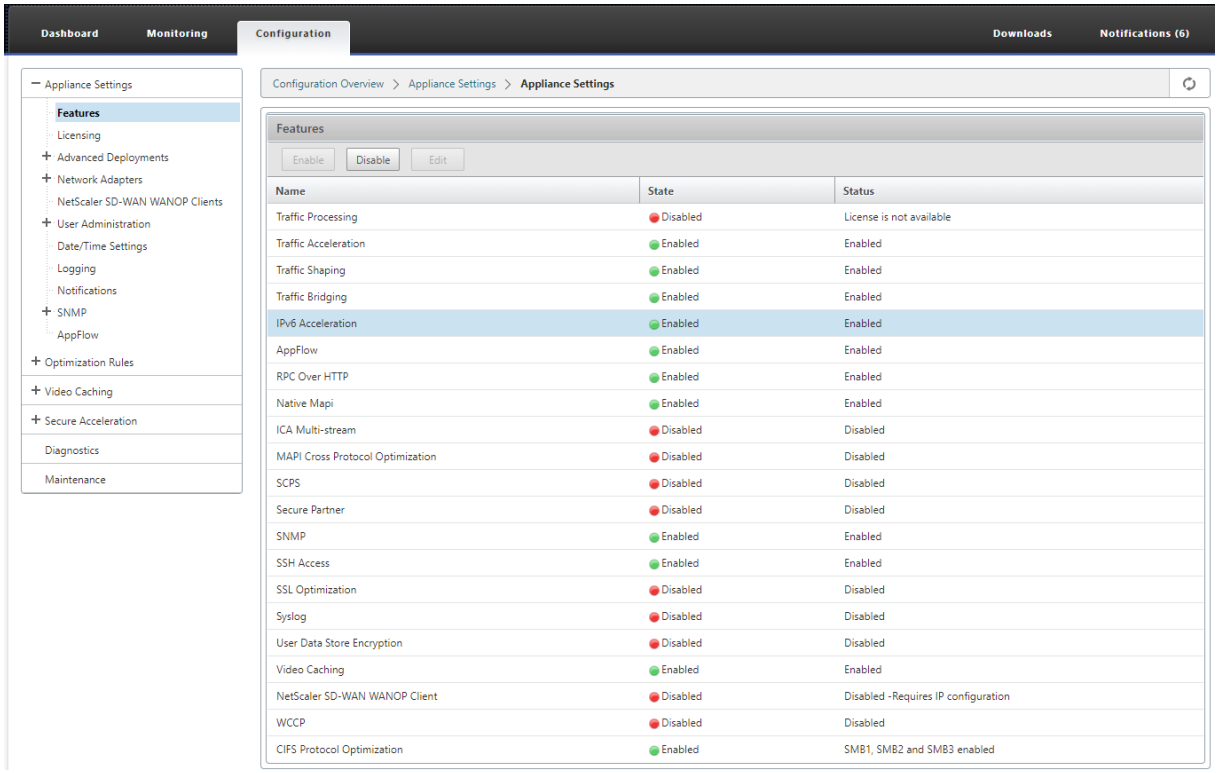
Cuando se conecta a Internet a través de un dispositivo, al dispositivo se le asigna una dirección IP. La dirección IP identifica el dispositivo e indica su ubicación. La cantidad de dispositivos que se conectan a Internet está aumentando rápidamente. Como resultado, es difícil administrar la solicitud de las direcciones IP con la versión existente de Protocolo de Internet (IP), IPv4, que utiliza direcciones de 32 bits. Mediante el uso de IPv4, se pueden asignar aproximadamente 4300 millones de direcciones a los dispositivos que se conectan a Internet.

IPv6 soluciona este problema mediante el uso de direcciones de 128 bits y una etiqueta hexadecimal para identificar las interfaces de red de los dispositivos en una red IPv6. Debido a que IPv6 admite

muchas más direcciones IP que IPv4, las organizaciones y las aplicaciones están introduciendo gradualmente compatibilidad con el protocolo IPv6.

Los protocolos IPv4 e IPv6 no son interoperables, lo que dificulta la transición. Para acelerar el aumento del tráfico IPv6 de varias aplicaciones compatibles con el dispositivo Citrix SD-WAN WANOP, puede habilitar la función de aceleración IPv6.

De forma predeterminada, IPv6 está inhabilitado en el dispositivo. Para habilitar la aceleración IPv6 en un dispositivo Citrix SD-WAN WANOP, vaya a **Configuration** > **Appliance Settings** > **Feature** page y active la función **Aceleración IPv6**.



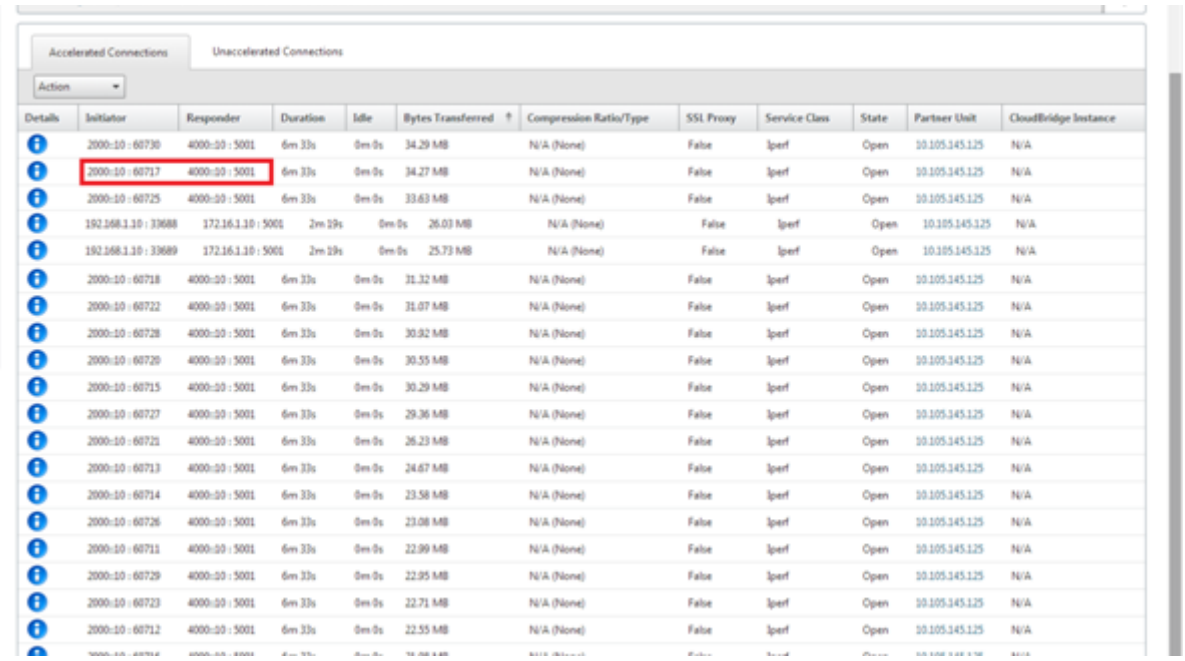
Verificar conexiones IPv6

Después de habilitar la aceleración IPv6 en el dispositivo, el dispositivo comienza a acelerar el tráfico de las aplicaciones que utilizan el protocolo IPv6. Para asegurarse de que el dispositivo está acelerando el tráfico IPv6, puede supervisar dichas conexiones en el dispositivo.

Para supervisar las conexiones IPv6, vaya a la ficha Supervisión. La página**Conexiones**de la ficha**Supervisión**muestra estadísticas relacionadas con el tráfico de protocolos IPv6:

Conexiones: la página Conexiones muestra detalles de todas las conexiones establecidas con el dispositivo. Esta página consta de dos fichas, Conexiones aceleradas y Conexiones no aceleradas. La ficha Conexiones aceleradas muestra todas las conexiones que el dispositivo está acelerando. Puede identificar el tráfico IPv6 en esta ficha haciendo referencia a la columna Iniciador y Respondedor de

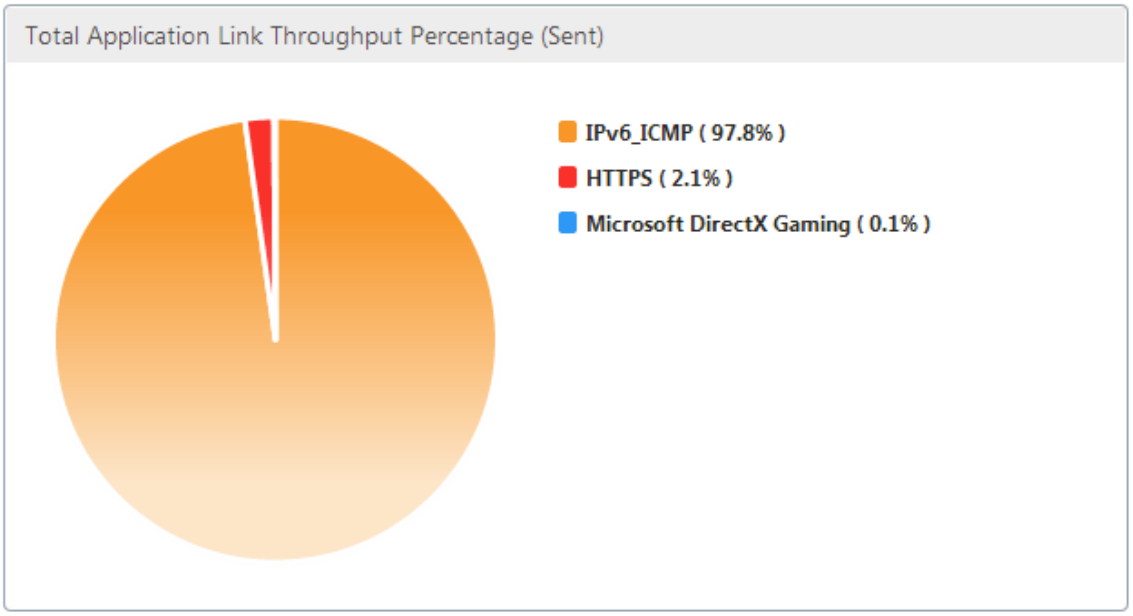
cada entrada. Si estas columnas contienen valores de dirección IP hexadecimales, la entrada representa una conexión IPv6, como se muestra en la siguiente captura de pantalla.



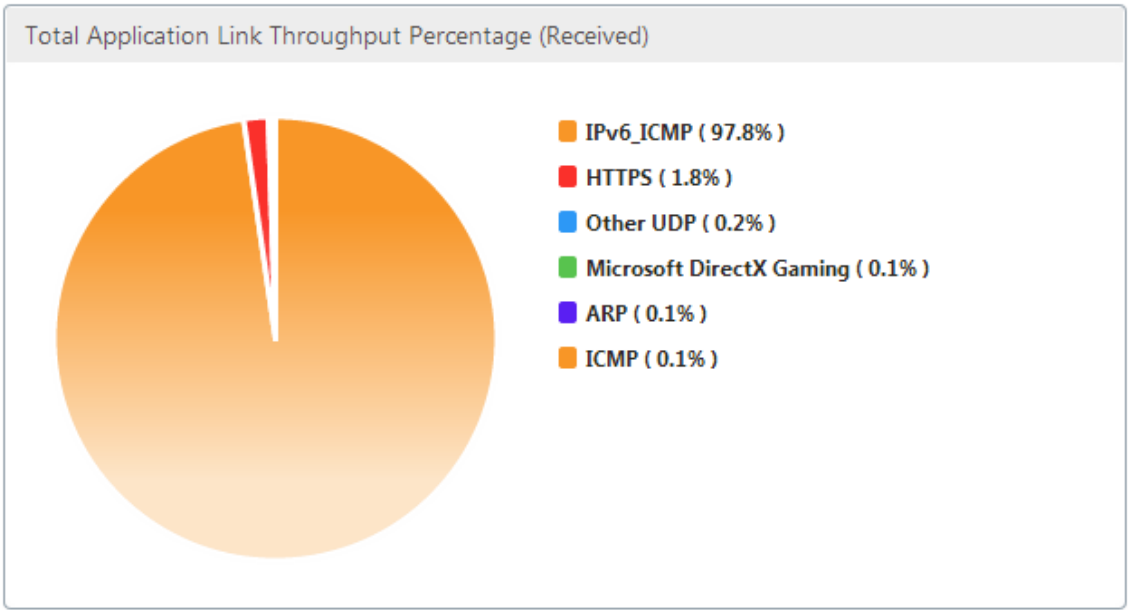
Las conexiones IPv6 que no están aceleradas se muestran en la ficha Conexiones no aceleradas. Si desea acelerar estas conexiones, es posible que deba solucionar problemas y ajustar los parámetros de la aplicación en el dispositivo. Al igual que en la ficha**Conexiones aceleradas**, puede identificar las conexiones IPv6 de esta ficha haciendo referencia a las columnas**Iniciador**y**Respondedor**de cada entrada.

Aplicaciones Principales: La página Aplicaciones Principales proporciona granularidad en el período de tiempo que puede utilizar para representar gráficamente el rendimiento de tráfico de varias aplicaciones servidas por el dispositivo Citrix SD-WAN. De forma predeterminada, el rendimiento del tráfico se muestra en el último minuto. Sin embargo, puede cambiar el período de tiempo seleccionando Último minuto, Última hora, Último día, Última semana o Último mes en la lista disponible en la barra de título de la página. Esta página tiene tres fichas: **Gráficos de aplicaciones principales**, **Desde el último reinicio** y **Aplicaciones activas (desde el último reinicio)**. La ficha Gráficos de aplicaciones principales contiene las siguientes estadísticas:

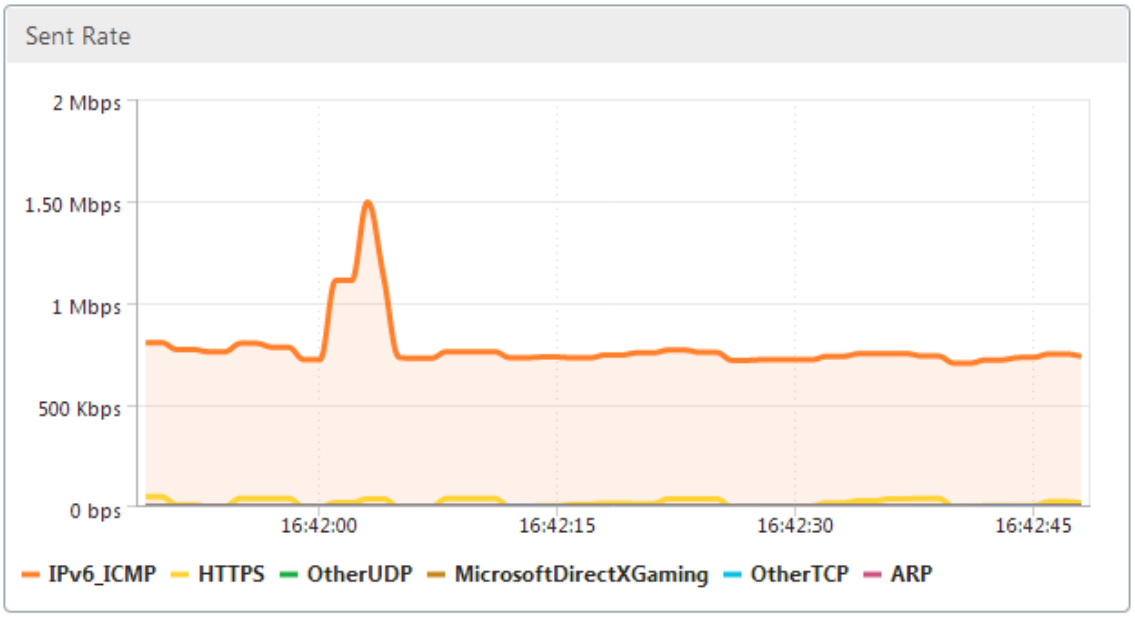
- **Porcentaje de rendimiento total de vínculos de aplicación (enviado)**: es un gráfico circular que muestra el porcentaje de tráfico que el dispositivo ha enviado a cada aplicación. Si el dispositivo ha enviado un porcentaje significativo de tráfico para una aplicación que utiliza el protocolo IPv6, la aplicación tiene su porcentaje de tráfico representado en este gráfico.



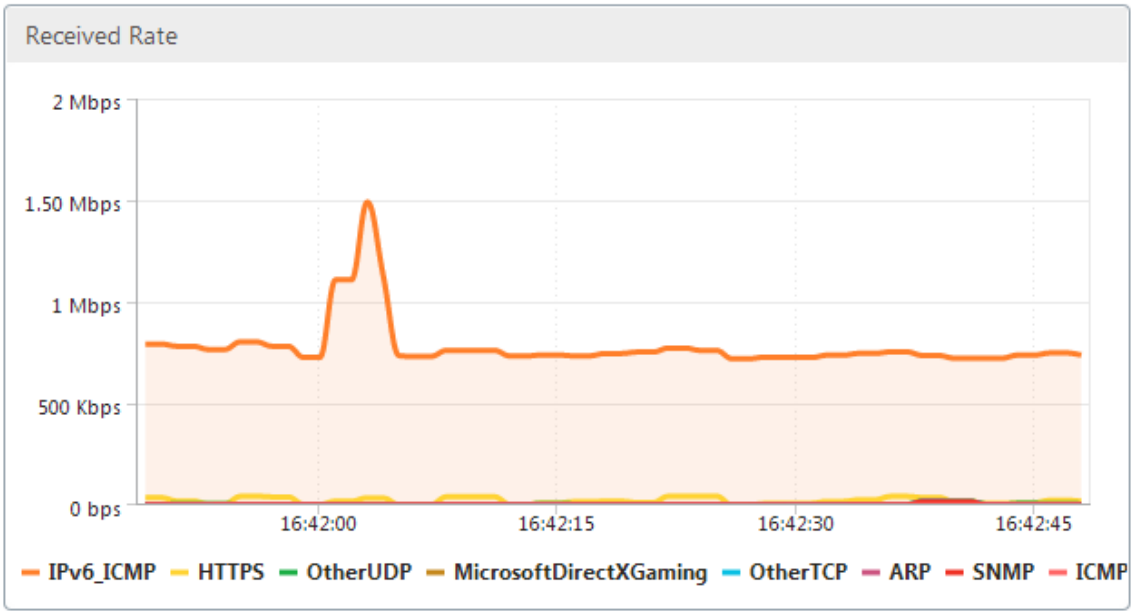
- **Porcentaje de rendimiento total de vínculos de aplicación (recibido)**: es un gráfico circular que muestra el porcentaje de tráfico que el dispositivo ha recibido de cada aplicación. Si el dispositivo ha recibido un porcentaje significativo de tráfico de una aplicación que utiliza el protocolo IPv6, el gráfico muestra el porcentaje de tráfico generado por la aplicación.



- **Tasa de envío**: se trata de un gráfico apilado de series de datos que representa la velocidad, en bits por segundo, a la que el dispositivo ha enviado tráfico a cada aplicación. Si el dispositivo ha enviado datos a una aplicación mediante el protocolo IPv6, también se traza en este gráfico una serie que muestra cada aplicación que utiliza el protocolo IPv6.



- **Tasa de recepción**: es un gráfico apilado de series de datos que representa la velocidad, en bits por segundo, a la que el dispositivo ha recibido tráfico de cada aplicación. Si el dispositivo ha recibido datos de una aplicación que utiliza el protocolo IPv6, también se traza en este gráfico una serie que muestra cada aplicación que utiliza el protocolo IPv6.



- **Tabla de aplicaciones principales**: Esta es una tabla de estadísticas para cada aplicación. La tabla muestra todas las aplicaciones para las que el dispositivo ha servido tráfico, junto con las tasas de envío y recepción en bits por segundo, el total de bytes enviados y recibidos, el porcentaje del tráfico de la aplicación y la velocidad a la que el dispositivo ha servido tráfico para la aplicación. Si el dispositivo ha servido tráfico para una aplicación que utiliza el protocolo

IPv6, la aplicación aparece en esta tabla junto con sus estadísticas.

Top Applications

Application	Sent Rate (bps)	Received Rate (bps)	Total Bytes Sent	Total Bytes Received	Total %	Order
IPv6_ICMP	719.56 K	719.56 K	5.4 M	5.4 M	98.3	1
HTTPS	10.57 K	9.64 K	79.3 K	72.35 K	1.38	2
Microsoft DirectX Gaming	416	416	3.14 K	3.14 K	0.06	4
Other TCP	312	312	2.35 K	2.35 K	0.04	5
Other UDP	128	1.7 K	984	12.73 K	0.12	3
ARP	24	488	232	3.66 K	0.04	6
SNMP	0	496	0	3.76 K	0.03	7
ICMP	0	376	0	2.84 K	0.03	8

- **Grupos de aplicaciones**: Esta es una tabla de estadísticas para cada aplicación, junto con su grupo de aplicaciones y la aplicación principal, en su caso. La tabla muestra los bytes enviados y recibidos para la aplicación. Cada aplicación, su grupo de aplicaciones y la aplicación principal se muestran como hipervínculos. Si hace clic en el hipervínculo, se muestran detalles granulares de las estadísticas para el vínculo en el que ha hecho clic. Si el dispositivo ha servido tráfico para una aplicación que utiliza el protocolo IPv6, la aplicación aparece en esta tabla junto con sus estadísticas.

Application Groups

Application	Application Group	Parent Application	Bytes Sent	Bytes Received
IPv6_ICMP	IP Protocols	IPv4	5.4 M	5.4 M
HTTPS	Web, Security Protocols	TCP	79.3 K	72.35 K
Microsoft DirectX Gaming	Games	TCP	3.14 K	3.14 K
Other TCP	N/A	N/A	2.35 K	2.35 K
Other UDP	N/A	N/A	984	12.73 K
ARP	Legacy Or Non-IP	N/A	232	3.66 K
SNMP	Network Management, Infrastructure	UDP	0	3.76 K
ICMP	Infrastructure, IP Protocols	IPv4	0	2.84 K

La ficha **Desde el último reinicio** contiene estadísticas sobre el tráfico de la aplicación desde el momento en que reinició el dispositivo. La ficha contiene los gráficos Porcentaje de rendimiento total de vínculos de aplicación (enviado) y Porcentaje de rendimiento total de vínculos de aplicación (recibido) y las tablas Aplicaciones principales y Grupos de aplicaciones, que muestran estadísticas similares a la ficha Gráficos de aplicaciones principales pero con datos desde que se reinició el dispositivo. La ficha **Aplicaciones activas (desde el último reinicio)** contiene una tabla con todas las aplicaciones activas desde que se reinició el dispositivo. Esta tabla contiene detalles sobre la velocidad de envío y recepción, el total de bytes enviados y recibidos y el total de paquetes enviados y recibidos para las aplicaciones.

Definiciones de enlaces

April 23, 2021

Las definiciones de vínculos permiten que el dispositivo evite la congestión y la pérdida en los vínculos WAN y realice el modelado del tráfico. Una definición de vínculo especifica qué tráfico está asociado al vínculo definido, el ancho de banda máximo para permitir el tráfico recibido en el vínculo y el ancho de banda máximo para el tráfico enviado a través del vínculo. La definición también identifica el tráfico como entrante o saliente y como tráfico de lado WAN o LAN. Todo el tráfico que fluye a través del dispositivo se compara con la lista de definiciones de vínculo y la primera definición coincidente identifica el vínculo al que pertenece el tráfico.

Al realizar el procedimiento de instalación rápida, puede personalizar las definiciones de vínculos predeterminadas del dispositivo. A continuación, ha definido el vínculo del dispositivo a la WAN y su vínculo a la LAN. Para una implementación sencilla en línea, no es necesaria ninguna configuración adicional de definiciones de enlaces. Otros tipos de implementaciones requieren una configuración adicional de definiciones de vínculos.

Cada enlace tiene dos límites de ancho de banda, que representan la velocidad de envío y la velocidad de recepción. Solo cuando se conoce la velocidad del enlace, el dispositivo puede inyectar tráfico en el enlace exactamente a la velocidad correcta, eliminando así la congestión y la pérdida de paquetes resultantes de intentar enviar demasiado, o la pérdida de rendimiento resultante de enviar demasiado poco. Cuando se coloca entre una LAN rápida y una WAN más lenta y actúa como puerta de *enlace virtual,* el dispositivo tiene la capacidad de recibir tráfico más rápido de lo que la WAN puede aceptarlo, creando un retraso de tráfico. La existencia de esta acumulación permite al dispositivo elegir qué paquete enviar a continuación, y esta opción a su vez hace posible el modelado del tráfico. A menos que haya paquetes de varias secuencias para elegir, no hay capacidad para favorecer una secuencia sobre la otra. Por lo tanto, el modelado del tráfico depende de la existencia de la Gateway virtual y establece correctamente los límites de ancho de banda.

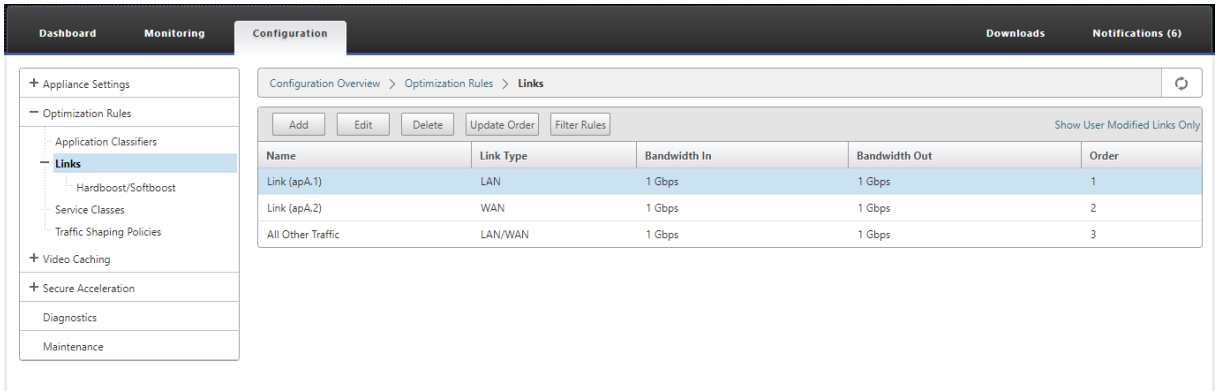
> **Nota**
>
> Las definiciones de enlace normalmente se aplican a las conexiones al par acelerado de puertos de puente. Los dos puertos de la placa base, Primary y Aux1, también se pueden definir como enlaces, pero hacerlo rara vez sirve para ningún propósito, ya que se utilizan para la administración y como canal posterior para los modos de alta disponibilidad y grupo, no para el tráfico WAN.
>
> **Importante**
>
> Importante: Para fines de definición de vínculo, un*enlace*es un enlace físico, con su propia capacidad de ancho de banda. Normalmente es un cable que sale del edificio. Recuerde los siguientes puntos:
>
> - Una VLAN no es un enlace.
> - Un vínculo virtual no es un vínculo.
> - Un túnel no es un enlace.

Definiciones de vínculos predeterminadas

Vaya a **Configuración** > **Reglas de optimización** > **Vínculos** para ver los vínculos definidos actualmente. Los siguientes vínculos se definen de forma predeterminada.

1. **apA.1**, uno de los dos puertos en el puente acelerado.
2. **apA.2**, el otro puerto en el puente acelerado.
3. Si el sistema tiene puentes acelerados dobles, también existen apB.1 y apB.2.
4. Todo otro tráfico, que no es un enlace verdadero, pero es un elemento general para el tráfico que no coincide con ninguna definición de enlace real.

El orden en que se muestran los enlaces en esta página es significativo. Al decidir a qué enlace pertenece un paquete, el dispositivo prueba los vínculos en orden y se selecciona el primer vínculo coincidente. Esto significa que se permiten definiciones superpuestas, y que la última definición del vínculo puede coincidir con todo el tráfico, sirviendo como enlace predeterminado. Para cambiar el pedido, haga clic en **Actualizar pedido**.



Administrar definiciones de enlaces en el modelado del tráfico

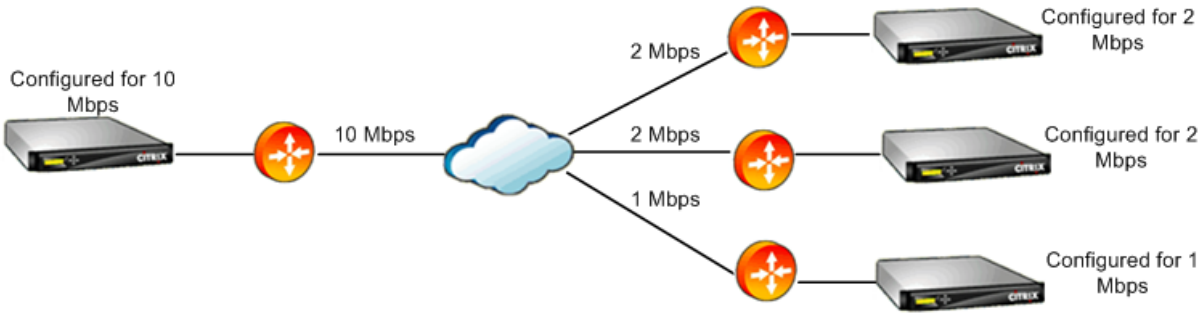
April 23, 2021

Para administrar un vínculo, el formador de tráfico necesita la siguiente información:

- La velocidad del enlace tanto en las direcciones de envío como de recepción.
- Si el vínculo es un vínculo WAN o una red LAN.
- Una forma de distinguir el tráfico de enlaces de otro tráfico.
- La dirección en la que fluye el tráfico sobre el enlace.

Velocidad del enlace: La *velocidad del enlace* siempre se refiere a la velocidad del enlace físico. En el caso de un enlace WAN, es la velocidad del segmento WAN la que termina en el edificio con el dispositivo Citrix SD-WAN WANOP. No se considera la velocidad del otro extremo del enlace. Por ejemplo, la siguiente imagen muestra una red de cuatro dispositivos. Cada dispositivo tiene sus anchos de banda entrantes y salientes establecidos en el 95% de la velocidad de su propio segmento WAN local, independientemente de la velocidad de los extremos remotos.

Ilustración 1. Los límites de ancho de banda local rastrean las velocidades de enlace locales



La razón para establecer los límites de ancho de banda en el 95% de la velocidad del enlace en lugar del 100% es permitir la sobrecarga del enlace (pocos enlaces pueden transportar datos al 100% de sus velocidades publicadas) y garantizar que el dispositivo sea ligeramente más lento que el enlace, de modo que se convierta en un ligero cuello de botella. El modelado del tráfico no es efectivo a menos que el formador del tráfico sea el cuello de botella en la conexión.

Distinguir diferentes tipos de tráfico: en cada definición de vínculo, debe declarar si la definición se aplica a un vínculo WAN o a una red LAN.

El formador de tráfico necesita saber si un paquete está viajando en la WAN y, en caso afirmativo, en qué dirección. Para proporcionar esta información:

- Para implementaciones simples en línea, declara que un puerto del puente acelerado pertenece al vínculo WAN y que el otro puerto pertenece a la LAN.
- En otros modos de implementación, el dispositivo examina direcciones IP, direcciones MAC, VLAN o grupos de servicios WCCP. (Tenga en cuenta que aún no se admiten pruebas para grupos de servicios WCCP).
- Si un sitio tiene varias WAN, las definiciones de vínculo local deben incluir reglas que permitan al dispositivo distinguir el tráfico de diferentes WAN.

Configurar definiciones de enlaces

April 23, 2021

Las definiciones de enlaces se organizan en una lista ordenada, una entrada por enlace, que se prueba de arriba a abajo para cada paquete que entra o sale del dispositivo. La primera definición coincidente determina a qué enlace pertenece el paquete. Dentro de cada definición de enlace hay una lista ordenada de reglas, que también se prueba de arriba a abajo. Cada paquete se compara con estas reglas, y si coincide con una de ellas, se considera que el paquete está viajando a través de ese enlace.

Dentro de una sola regla, los campos están todos juntos, por lo que todos los valores especificados deben coincidir. El valor predeterminado de todos los campos es Cualquiera, una entrada comodín que siempre coincide. Cuando un campo consta de una lista, como una lista de subredes IP, las entradas de la lista se ORE juntas. Es decir, si algún elemento coincide, la lista como un todo se considera una coincidencia.

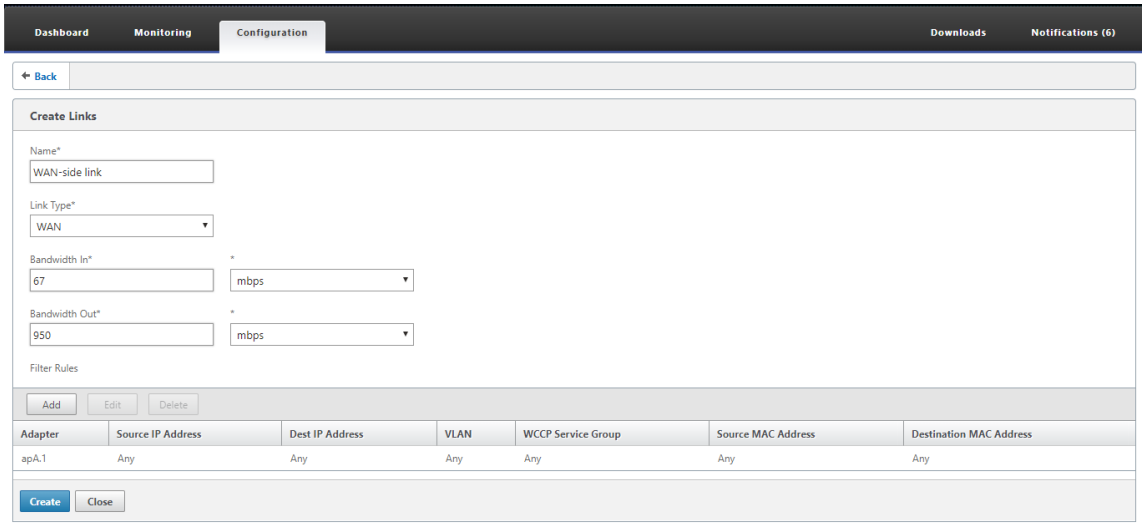
Los vínculos pueden basarse en el adaptador Ethernet asociado al tráfico, las direcciones IP de origen y destino, la etiqueta VLAN, el grupo de servicios WCCP (solo para WCCP-GRE) y la dirección MAC Ethernet de origen y destino. Una implementación en línea simple podría identificar solo los puertos de puente acelerado de lado LAN y lado WAN (apA.1 y apA.2), mientras que una implementación de centro de datos compleja podría necesitar usar la mayoría de las opciones proporcionadas para desambiguar el tráfico.

La definición de un enlace en términos de sus direcciones IP es posible excepto cuando se utilizan enlaces redundantes. Dado que un paquete determinado puede pasar por un enlace en una implementación de doble enlace activo-en espera o activo-activo, se debe usar otro método para determinar qué enlace está utilizando el paquete. Si se utilizan puentes dobles, entonces el tráfico de un enlace puede pasar sobre apA y el otro sobre apB, y los enlaces se pueden definir en términos de adaptadores. Si los dos enlaces son servidos por enrutadores diferentes, las direcciones MAC de los enrutadores se pueden usar para diferenciar el tráfico. Cuando todo lo demás falla, se puede utilizar WCCP-GRE y el router puede utilizar un grupo de servicios diferente para cada enlace WAN, lo que permite a la unidad WANOP de Citrix SD-WAN distinguir el tráfico de enlace por grupo de servicio.

Citrix recomienda definiciones de vínculos basados en puertos para implementaciones simples en línea, y definiciones de vínculos basadas en IP para todas las demás implementaciones.

Para configurar definiciones de vínculos:

1. Vaya a **Configuración** > **Reglas de optimización** > **Vínculos** y haga clic en **Agregar.**



2. Introduzca valores para los siguientes parámetros:

   - **Nombre: nombre**descriptivo del vínculo, que también puede describir si se trata de un vínculo de lado LAN o de un vínculo de lado WAN.
   - **Tipo de vínculo**: El tipo de vínculo, ya sea LAN o WAN.
   - **Ancho de banda en**: límite de ancho de banda entrante.
   - **Ancho de banda saliente**: límite de ancho de banda saliente.

3. En la sección **Reglas de filtro**, haga clic en **Agregar** e introduzca valores para los siguientes parámetros:

   - **Adaptador:** especifica una lista de adaptadores (puertos Ethernet). Cuando los enlaces se pueden identificar mediante el adaptador ethernet, esto simplifica la configuración.
   - **Dirección IP de origen:** se tienen en cuenta las reglas IP de origen para los paquetes que entran en la unidad (se ignoran los paquetes que salen de la unidad). En estos paquetes, las reglas del campo IP Src se comparan con el campo Dirección de origen del encabezado IP. La regla especifica una lista de direcciones IP o subredes. También se admiten coincidencias negativas, como Excluir 10.0.0.1.
   - **Dirección IP de destino:** se tienen en cuenta las reglas IP de destino para los paquetes que salen de la unidad (se ignoran los paquetes que entran en la unidad). En estos paquetes, las reglas del campo IP Dst se comparan con el campo Dirección de destino del encabezado IP. La regla especifica una lista de direcciones IP o subredes. También se admiten coincidencias negativas, como Excluir 10.0.0.1.
   - **VLAN:** Las reglas de VLAN se aplican a los encabezados de VLAN de los paquetes que entran o salen de la unidad.

- Grupo de**servicios WCCP: Las reglas del grupo** de servicios WCCP se aplican a los paquetes WCCP encapsulados en GRE-encapsulados que entran o salen de la unidad. (Esto no funciona con L2 WCCP).
- **Dirección MAC de origen:** La dirección MAC de origen usa d como criterio de filtro.
- **Dirección MAC de**destino: La dirección MAC de destino utilizada como criterio de dilatador.

4. Haga clic en **Crear**.

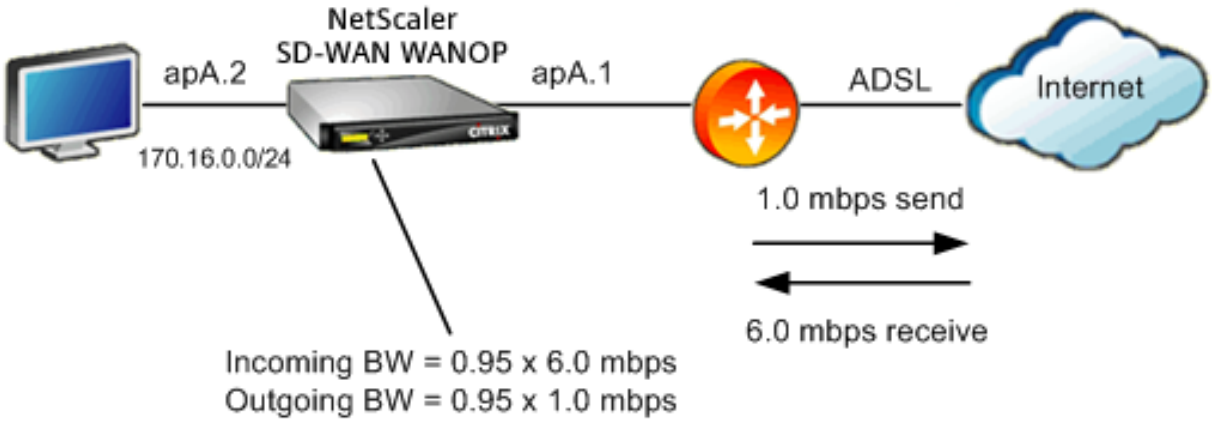
   El clasificador de tráfico utiliza los campos IP de Src y Dest de una manera especializada (lo mismo se aplica a Src MAC y Dst MAC):

   - El campo Src solo se examina en los paquetes que entran en el dispositivo.
   - El Dst solo se examina en los paquetes que salen del dispositivo.

Enlaces en línea

La mayoría de los dispositivos de Citrix SD-WAN WANOP utilizan una implementación en línea simple, donde cada puente acelerado sirve solo un enlace WAN. Este es el modo más simple de configurar.

Enlace en línea simple



En la imagen anterior, se supone que todo el tráfico que pasa a través del puente acelerado es tráfico WAN. El enlace es un enlace ADSL con diferentes velocidades de envío y recepción (6,0 mbps down, 1,0 mbps up). La WAN está conectada al puerto de puente acelerado apA.1 y la LAN está conectada al puerto de puente acelerado apA.2.

Las tareas para definir el enlace del lado WAN (apA.1) son:

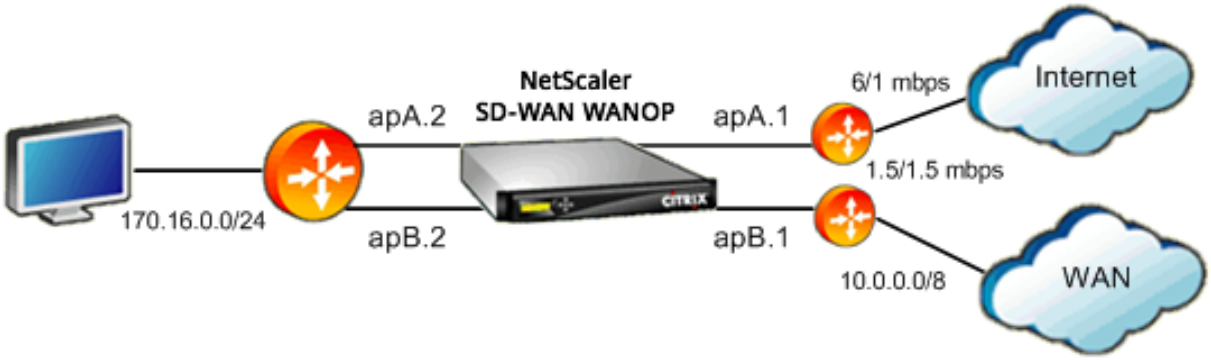
1. Asigne a la WAN un nombre descriptivo, como “WAN to HQ (apA.1)”.

2. Establezca el tipo en WAN.
3. Establezca los límites de ancho de banda entrante y saliente en el 95% de la velocidad nominal del enlace.
4. Compruebe que se haya definido una regla que especifique el adaptador Ethernet WAN, que en este ejemplo es apA.
5. Haga clic en Crear.

Las tareas para el enlace LAN (apA.2) son similares:

1. Asigne un nombre descriptivo, como "Local LAN (apA.2)".
2. Establezca el tipo en LAN.
3. Establezca los límites de ancho de banda entrante y saliente en el 95% de la velocidad nominal de Ethernet (95 mbps o 950 mbps).
4. Compruebe que existe una regla que especifique el adaptador LAN Ethernet, que en este ejemplo es apA.2.
5. Haga clic en Crear.

Implementación en línea con puentes dobles



La configuración es similar a la simple configuración de enlaces en línea, pero el sitio tiene un segundo enlace, un enlace T1 a la WAN corporativa, además del enlace de Internet ADSL. El dispositivo Citrix SD-WAN WANOP tiene dos puentes acelerados, uno para cada vínculo WAN.

La configuración es casi tan simple como la caja de un solo puente, con los siguientes pasos adicionales:

1. Modifique un segundo enlace WAN en apB, que en este caso es apB.1. Establezca el tipo en WAN. Establezca el ancho de banda del enlace en el 95% de la velocidad T1 de 1,5 mbps y asígnele un nuevo nombre al enlace, como WAN to HQ.

2. Agregue una regla que especifique apB.2 a la definición de LAN y elimine la definición de vínculo predeterminada para apB.2. (Alternativamente, puede modificar la definición de enlace predeterminada para apB.2 para especificarla como enlace LAN, como se hizo con apA.2.)

Enlaces no alineados

Para implementaciones en línea distintas de simples (que solo sirven una WAN por puente acelerado), utilice subredes IP en lugar de puertos de puente para distinguir el tráfico LAN del tráfico WAN. Este enfoque es esencial para implementaciones con un solo brazo, que utilizan un solo puerto de puente. Las subredes IP también son útiles para implementaciones en línea, especialmente cuando el dispositivo sirve más de una WAN. Sin embargo, para implementaciones simples en línea, los vínculos basados en puertos son más fáciles de definir.

El clasificador de tráfico aplica una convención especializada al examinar la IP Src y la IP Dst:

- El campo IP Src examina solo en paquetes que entran en el dispositivo.
- El campo Dst IP solo se examina en los paquetes que salen del dispositivo.

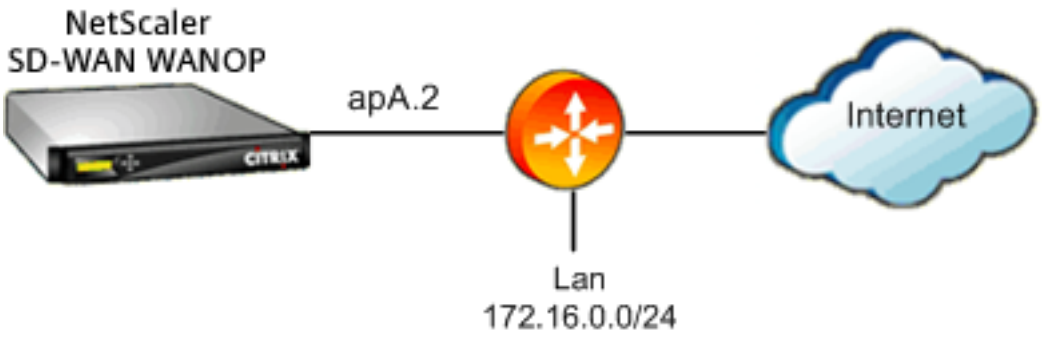
Esta convención a veces puede ser confusa, pero permite que la dirección del viaje de paquetes se considere implícitamente como parte de la definición.

Usar la dirección IP en las definiciones de enlace

Para configurar una definición simple de LAN en línea mediante reglas basadas en IP, puede definir los vínculos LAN y WAN sin especificar los puertos Ethernet en absoluto, mediante la subred LAN en su lugar:

- Cree una regla para la definición de vínculo LAN y especifique la subred LAN en el campo IP Src.
- Cree una regla para la definición de vínculo WAN y especifique la subred LAN (no la subred WAN) en el campo Dst IP.

Modos en línea virtuales y WCCP



Configuración WCCP o implementación virtual en línea mediante reglas basadas en IP es lo mismo que usar la dirección IP en la definición de vínculo, porque las subredes IP LAN y WAN son idénticas.

Cuando se utiliza WCCP-GRE, se ignoran los encabezados GRE y se utilizan los encabezados IP dentro de los paquetes de datos encapsulados. Por lo tanto, esta misma definición de enlace funciona para los modos en línea WCCP-L2, WCCP-GRE, en línea y virtual.

(WCCP y los modos en línea virtuales requieren la configuración de su router. WCCP también requiere configuración en la página Configuración: Implementaciones Avanzadas.)

Administrar y supervisar mediante Citrix Application Delivery Management

December 14, 2022

La compatibilidad con Citrix SD-WAN WANOP AppFlow permite una supervisión flexible y personalizada de sus dispositivos Citrix SD-WAN WANOP.

La interfaz AppFlow funciona con Citrix Application Delivery Management (ADM).Citrix ADM recibe información detallada del dispositivo mediante el estándar abierto AppFlow (http://www.appflow.org) .Citrix ADM le permite supervisar, administrar y ver análisis de los dispositivos Citrix SD-WAN de la red.

Citrix ADM admite una amplia gama de dispositivos y puede presentar una vista más completa de su red. El dispositivo Citrix SD-WAN WANOP tiene una amplia vista del tráfico WAN, incluidas estadísticas detalladas sobre el tráfico de aplicaciones virtuales y escritorios virtuales, y proporciona información clave sobre la experiencia del usuario de la WAN.

Para obtener más información, consulte Administración de instancias de Citrix SD-WAN mediante Citrix Application Delivery Management.

Ejemplo de Virtual Apps/Virtual Desktops

En un entorno de Citrix Virtual Apps and Desktops, si un usuario de sucursal encuentra bajo rendimiento, es posible que el administrador tenga que supervisar la red, los usuarios y las aplicaciones alojadas en Virtual Apps o Virtual Desktops. Es posible que los administradores tengan que hacer las siguientes preguntas:

- ¿Qué parte de la red está causando una mala experiencia de usuario?
- ¿Cuál es una manera fácil de identificar la lentitud en las aplicaciones publicadas?
- ¿Qué canales virtuales consumen la mayor cantidad de ancho de banda en un período de tiempo determinado?
- ¿Qué usuarios de Virtual Desktops o Virtual Apps consumen la mayor cantidad de ancho de banda durante un período de tiempo determinado?
- Para un usuario de Virtual Desktops determinado, ¿cuál es la latencia media del lado del cliente y del servidor, y la fluctuación promedio?
- ¿Cuáles son las aplicaciones principales de todos los usuarios de Virtual Apps, por tiempo de actividad y número total de lanzamientos durante un período de tiempo determinado?
- ¿Qué es la latencia del centro de datos?

La compatibilidad con Citrix SD-WAN WANOP AppFlow proporciona respuestas a todas las preguntas anteriores, lo que permite, por ejemplo, distinguir un enlace WAN congestionado de un servidor lento o un cliente lento.

Citrix Cloud Connector

April 23, 2021

La función Citrix Cloud Connector del dispositivo Citrix SD-WAN WANOP conecta centros de datos empresariales a nubes externas y entornos de hospedaje, lo que convierte a la nube en una extensión segura de su red empresarial. Las aplicaciones alojadas en la nube aparecen como si se estuvieran ejecutando en una red empresarial contigua. Con Citrix Cloud Connector, puede aumentar sus centros de datos con la capacidad y eficiencia disponibles en los proveedores de la nube.

Citrix Cloud Connector le permite mover sus aplicaciones a la nube para reducir costes y aumentar la fiabilidad.

La función de optimización WAN del dispositivo Citrix SD-WAN WANOP acelera el tráfico y proporciona un rendimiento similar a LAN para aplicaciones que se ejecutan en centros de datos y nubes empresariales.

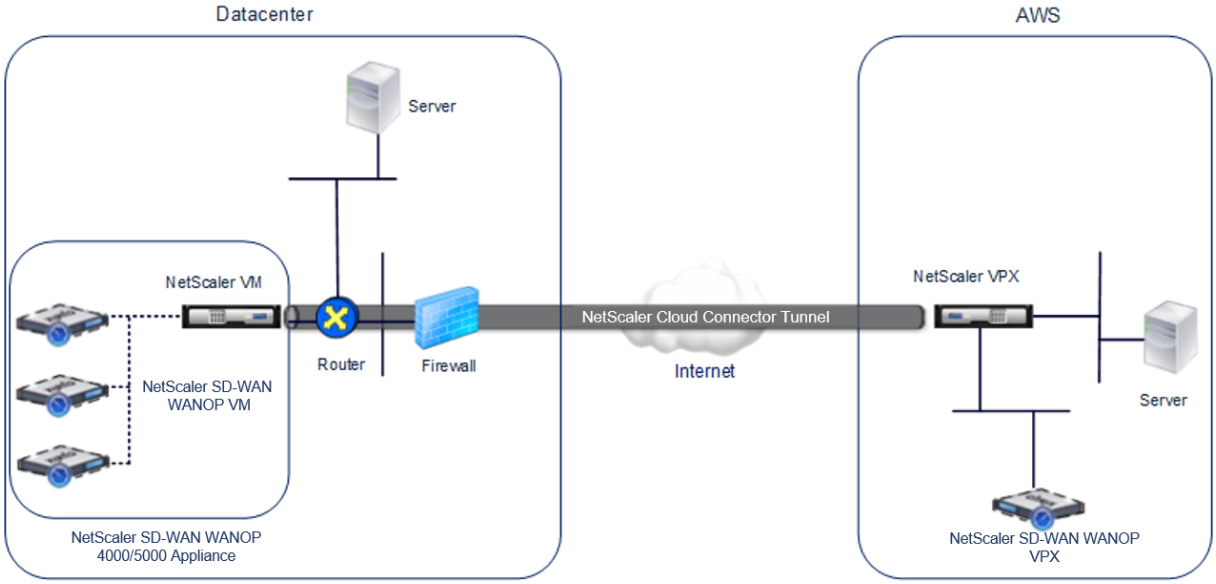
Además de usar Citrix Cloud Connector entre un centro de datos y una nube, puede usarlo para conectar dos centros de datos para crear un vínculo seguro y acelerado de alta capacidad.

Para implementar la solución Citrix Cloud Connector, conecte un centro de datos a otro centro de datos o a una nube externa configurando un túnel denominado túnel Citrix Cloud Connector.

Para conectar un centro de datos a otro centro de datos, configure un
túnel de Citrix Cloud Connector entre dos dispositivos, uno en cada centro de datos.

Para conectar un centro de datos a una nube externa (por ejemplo, la nube de Amazon AWS), debe configurar un túnel de Citrix Cloud Connector entre un dispositivo Citrix SD-WAN WANOP del centro de datos y un dispositivo virtual (VPX) que reside en la nube. El punto final remoto puede ser Citrix Cloud Connector o Citrix VPX con licencia platino.

La siguiente ilustración muestra un túnel de Citrix Cloud Connector configurado entre un centro de datos y una nube externa.



Los dispositivos entre los que se configura un túnel de Citrix Cloud Connector se denominan *puntos finales* o *pares* del túnel de Citrix Cloud Connector.

Un túnel de Citrix Cloud Connector utiliza los siguientes protocolos:

- Protocolo de encapsulación de enrutamiento genérico (GRE)
- Conjunto de protocolos IPSec estándar abierto, en modo de transporte

El protocolo GRE proporciona un mecanismo para encapsular paquetes, de una amplia variedad de protocolos de red, para ser reenviados a través de otro protocolo. GRE se utiliza para:

- Conecte redes que ejecutan protocolos no IP y no enrutables.
- Puente a través de una red de área amplia (WAN).

- Cree un túnel de transporte para cualquier tipo de tráfico que deba enviarse sin cambios a través de una red diferente.

El protocolo GRE encapsula los paquetes agregando un encabezado GRE y un encabezado IP GRE a los paquetes.

El conjunto de protocolos de seguridad de protocolo Internet (IPSec) protege la comunicación entre pares en el túnel Citrix Cloud Connector.

En un túnel de Citrix Cloud Connector, IPSec garantiza:

- Integridad de los datos
- Autenticación de origen de datos
- Confidencialidad de los datos (cifrado)
- Protección contra ataques de repetición

IPSec utiliza el modo de transporte en el que se cifra el paquete encapsulado GRE. El cifrado se realiza mediante el protocolo Encapsulating Security Payload (ESP). El protocolo ESP garantiza la integridad del paquete mediante el uso de una función hash HMAC y garantiza la confidencialidad mediante el uso de un algoritmo de cifrado. Después de que el paquete se cifra y se calcula el HMAC, se genera un encabezado ESP. El encabezado ESP se inserta después del encabezado IP GRE y se inserta un remolque ESP al final de la carga útil cifrada.

Los pares del túnel Citrix Cloud Connector utilizan el protocolo de la versión de intercambio de claves de Internet (IKE) (parte del conjunto de protocolos IPSec) para negociar la comunicación segura, como se indica a continuación:

- Los dos pares se autentican mutuamente mediante uno de los siguientes métodos de autenticación:
  - **Autenticación de clave previamente compartida**. Una cadena de texto denominada clave previamente compartida se configura manualmente en cada par. Las claves previamente compartidas de los pares se comparan entre sí para la autenticación. Por lo tanto, para que la autenticación sea correcta, debe configurar la misma clave previamente compartida en cada uno de los pares.
  - **Autenticación de certificados digitales**. El par iniciador (remitente) firma los datos de intercambio de mensajes mediante su clave privada y el otro par receptor utiliza la clave pública del remitente para verificar la firma. Normalmente, la clave pública se intercambia en mensajes que contienen un certificado X.509v3. Este certificado proporciona un nivel de seguridad de que la identidad de un par tal y como se representa en el certificado está asociada a una clave pública determinada.
- A continuación, los pares negocian para llegar a un acuerdo sobre:

- Un algoritmo de cifrado.
- Claves criptográficas para cifrar datos en un par y descifrar los datos en el otro.

Este acuerdo sobre el protocolo de seguridad, el algoritmo de cifrado y las claves criptográficas se denomina Asociación de Seguridad (SA). Las SA son unidireccionales (simplex). Por ejemplo, cuando dos pares, CB1 y CB2, se comunican a través de un túnel Connector, CB1 tiene dos asociaciones de seguridad. Una SA se utiliza para procesar paquetes de salida y la otra SA se utiliza para procesar paquetes de entrada.

Las SA caducan después de un período de tiempo especificado, que se denomina *duración*. Los dos pares utilizan el protocolo de intercambio de claves de Internet (IKE) (parte del conjunto de protocolos IPSec) para negociar nuevas claves criptográficas y establecer nuevas SA. El propósito de la duración limitada es evitar que los atacantes rompan una clave.

Además, las instancias WANOP de Citrix SD-WAN en los puntos finales del
túnel de Citrix Cloud Connector proporcionan optimización de WAN sobre el túnel.

Requisitos previos para configurar el túnel de Citrix Cloud Connector

Antes de configurar un túnel de Citrix Cloud Connector entre AWS Cloud y un dispositivo Citrix SD-WAN WANOP configurado para el modo de un brazo en el centro de datos, compruebe que se han completado las siguientes tareas:

1. Asegúrese de que el dispositivo Citrix SD-WAN WANOP del centro de datos está configurado correctamente. Para obtener más información sobre la implementación de un dispositivo Citrix SD-WAN en modo de un brazo que utiliza el protocolo WCCP/Virtual Inline, consulte Sitios con un enrutador WAN.
2. Instale, configure e inicie un dispositivo virtual Citrix (instancia VPX) en la nube de AWS. Para obtener más información, consulte Instalación de NetScaler VPX en AWS.
3. Instale, configure e inicie una instancia de Citrix SD-WAN WANOP virtual Appliance (VPX) en la nube de AWS. Para obtener más información, consulte Instalación de SD-WAN VPX S AMI en Amazon AWS.
4. En AWS, vincule la instancia de Citrix SD-WAN WANOP VPX en AWS a un servidor virtual de equilibrio de carga en la instancia de Citrix VPX en AWS. Este enlace es necesario para enviar tráfico a través de las instancias de Citrix SD-WAN WANOP VPX, a fin de lograr la optimización de la WAN a través del túnel de Citrix Cloud Connector.

Para crear un servidor virtual de equilibrio de carga mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

- **enable ns mode** l2
- **add lb vserver** <cbvpxonaws_vs_name> CUALQUIER * -**L2conn** ON -**m** MAC

Para agregar la instancia de Citrix SD-WAN WANOP VPX en AWS como servicio y enlazarla al servidor virtual de equilibrio de carga mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

- **add service** < cbvpxonaws_service_name> <cbvpxonaws_IP> ANY * -**cltTimeou**t 14400 -**svrTimeout** 14400
- **bind lb vserver** <cbvpxonaws_vs_name> <cbvpxonaws_service_name>

Configurar túnel de conector de nube

April 23, 2021

Para configurar el túnel de Citrix Cloud Connector, utilice la utilidad de configuración de ambos dispositivos Citrix VPX para realizar las siguientes tareas:

- **Crear un perfil IPSec**: una entidad de perfil IPSec especifica los parámetros del protocolo IPSec, como la versión IKE, el algoritmo de cifrado, el algoritmo hash y PSK, que utilizará el protocolo IPSec en el túnel de Citrix Cloud Connector.
- **Cree un túnel IP y asocie el perfil IPSec con él**: un túnel IP especifica la dirección IP local, la dirección IP remota, el protocolo utilizado para configurar el túnel de Citrix Cloud Connector y una entidad de perfil IPSec. La entidad de túnel IP creada también se denomina entidad de túnel de Citrix Cloud Connector.
- **Cree una regla PBR y asocie el túnel IP con ella**: una entidad PBR especifica un conjunto de condiciones y una entidad de túnel IP (túnel de Citrix Cloud Connector). El intervalo de direcciones IP de origen y el intervalo IP de destino son las condiciones para la entidad PBR. Debe establecer el intervalo de direcciones IP de origen y el rango de direcciones IP de destino para especificar la subred cuyo tráfico va a atravesar el túnel de Citrix Cloud Connector. Por ejemplo, considere un paquete de solicitud que se origina en un cliente de la subred del centro de datos y está destinado a un servidor de la subred en la nube de AWS. Si este paquete coincide con el rango IP de origen y destino de la entidad PBR en el dispositivo virtual Citrix en el dispositivo Citrix SD-WAN WANOP del centro de datos, se considera para el procesamiento WANOP de Citrix SD-WAN, que envía el paquete a través del túnel de Citrix Cloud Connector asociado a la entidad PBR.

Para crear un perfil IPSEC mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

- **añadir perfil ipsec** <ipsec_profile_name> -**EnCalgo** AES -**HaShalgo** HMAC_SHA1 -**Lifetime** 500 -**psk** <password>

Para crear un túnel IP y enlazar el perfil IPSEC mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

- **add iptunnel** <tunnel_name> <Remote CBC Public IP> <remote_cbs_Netmask> <lan_subnet_IP> -**protocolo** GRE -**IPsecProfileName** <ipsec_profile>

Para crear una regla PBR y enlazar el túnel IPSEC mediante la interfaz de línea de comandos:

En el símbolo del sistema, escriba:

- **add ns pbr ALLOW** <pbr_name> -**srCip** = <local_lan_subnet> -**DeSip** = <remote_lan_subnet> -**IPTunnel** <tunnel_name>
- **apply ns pbrs**

Para crear un perfil IPSEC mediante la utilidad de configuración:

1. Vaya a **Sistema** >**Citrix Cloud Connector** > **Perfil IPSec**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar perfil IPSec, defina los siguientes parámetros:
    - Nombre
    - Algoritmo de cifrado
    - Algoritmo hash
    - Versión del protocolo IKE (seleccione V2)
4. Utilice uno de los siguientes métodos de autenticación IPSec que los dos pares utilizarán para autenticarse mutuamente.
    - Para el método de autenticación de clave previamente compartida, establezca el parámetro Existes de clave previamente compartida.
    - Para el método de autenticación de certificados digitales, establezca los siguientes parámetros:
        - Clave pública
        - Clave privada
        - Clave pública del mismo nivel
5. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear un túnel IP y enlazar el perfil IPSEC mediante la utilidad de configuración:

1. Vaya a **Sistema** >**Citrix Cloud Connector** > **Túneles IP**.
2. En la ficha Túneles IPv4, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar túnel IP, establezca los siguientes parámetros:
   - Nombre
   - IP remota
   - Máscara remota
   - Tipo de IP local (en la lista desplegable Tipo de IP local, seleccione IP de subred).
   - IP local (todas las direcciones IP configuradas del tipo IP seleccionado se rellenarán en la lista desplegable de IP local. Seleccione la IP deseada de la lista.)
   - Protocolo
   - Perfil IPSec
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Para crear una regla PBR y enlazar el túnel IPSEC con ella mediante la utilidad de configuración:

1. Vaya a **Sistema** > **Red** > **PBR**.
2. En la ficha PBR, haga clic en **Agregar**.
3. En el cuadro de diálogo crear PBR, defina los siguientes parámetros:
   - Nombre
   - Acción
   - Tipo de salto siguiente (Seleccionar túnel IP)
   - Nombre del túnel IP
   - IP de origen bajo
   - IP de origen alto
   - IP de destino bajo
   - IP de destino alto
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

   La nueva configuración del túnel de Citrix Cloud Connector en el dispositivo Citrix SD-WAN WANOP del centro de datos aparece en la ficha Inicio de la interfaz de usuario del Servicio de administración.

La nueva configuración del túnel de Citrix Cloud Connector correspondiente en el dispositivo Citrix VPX en la nube de AWS aparece en la utilidad de configuración.

El estado actual del túnel de Citrix Cloud Connector se indica en el panel Configurado de Citrix SD-WAN WANOP. Un punto verde indica que el túnel está arriba. Un punto rojo indica que el túnel está caído.

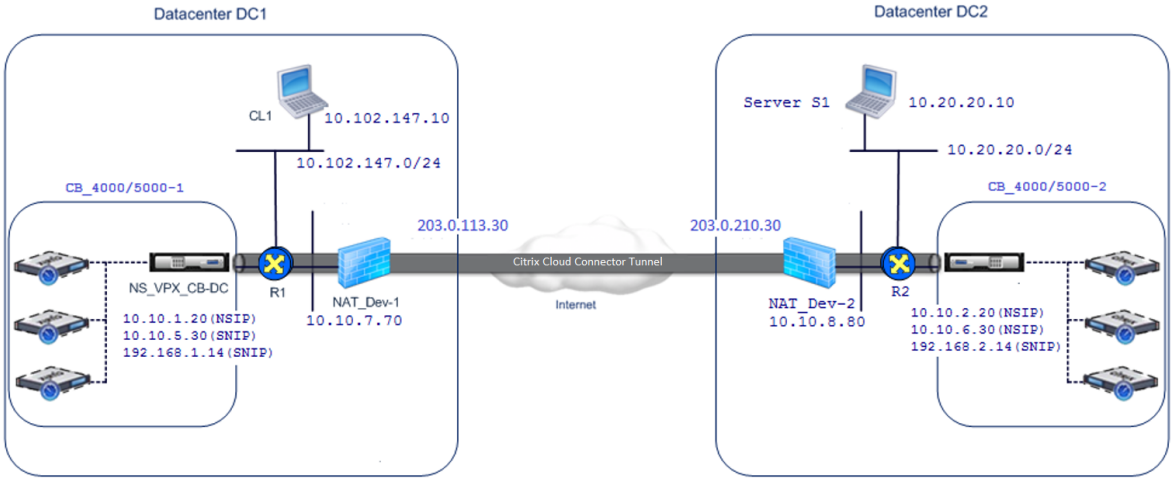
Configurar el túnel del conector de nube entre dos centros de datos

April 23, 2021

Puede configurar un túnel de Citrix Cloud Connector entre dos centros de datos diferentes para ampliar la red sin volver a configurarla y aprovechar las capacidades de los dos centros de datos. Un túnel de Citrix Cloud Connector entre los dos centros de datos separados geográficamente le permite implementar redundancia y proteger su configuración de errores. El túnel de Citrix Cloud Connector ayuda a lograr una utilización óptima de la infraestructura y los recursos en dos centros de datos. Las aplicaciones disponibles en los dos centros de datos aparecen como locales para el usuario.

Para conectar un centro de datos a otro centro de datos, debe configurar un túnel de Citrix Cloud Connector entre un dispositivo SD-WAN WANOP 4000/5000 que reside en un centro de datos y otro dispositivo SD-WAN WANOP 4000/5000 que reside en el otro centro de datos.

Para comprender cómo se configura un túnel de Citrix Cloud Connector entre dos centros de datos diferentes, considere un ejemplo en el que se configura un túnel de Cloud Connector entre el dispositivo Citrix CB_4000/5000-1 en el centro de datos DC1 y el dispositivo Citrix CB_4000/5000-2 en el centro de datos DC2.



Tanto CB_4000/5000-1 como CB_4000/5000-2 funcionan en modo de un brazo (WCCP/PBR). Permiten la comunicación entre redes privadas en centros de datos DC1 y DC2. Por ejemplo, CB_4000/5000-1 y

CB_4000/5000-2 permiten la comunicación entre el cliente CL1 en el centro de datos DC1 y el servidor S1 del centro de datos DC2 a través del túnel de Citrix Cloud Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

Para una comunicación adecuada entre CL1 y S1, el modo L3 está habilitado en NS_VPX_CB_4000/5000-1 y NS_VPX_CB_ 4000/5000-2, y las rutas se configuran de la siguiente manera:

- El router R1 tiene una ruta para llegar a S1 a través de NS_VPX_CB_ 4000/5000-1.
- NS_VPX_CB_4000/5000_1 tiene una ruta para llegar a NS_VPX-CB_4000/5000-2 a través de R1.
- S1 debe tener una ruta que llegue a CL1 a través de NS_VPX-CB_4000/5000-2.
- NS_VPX-CB_ 4000/5000-2 tiene una ruta para llegar a NS_VPX_CB_4000/5000-1 a R2.

La siguiente tabla muestra la configuración de CB_4000/5000-1 en el centro de datos DC1.

Entidad	Nombre	Detalles
Dirección IP del cliente CL1		10.102.147.10
Parámetros en el dispositivo NAT-Dev-1		
Dirección IP NAT en el lado público		203.0.113.30*
Dirección IP NAT en el lado privado		10.10.7.70
Configuración en CB_4000/5000-1		
Dirección IP del servicio de gestión de CB_4000/5000-1		10.10.1.10
Configuración en NS_VPX_CB_4000/5000-1 que se ejecuta en CB_4000/5000-1		
La dirección NSIP		10.10.1.20
Dirección SNIP		10.10.5.30
Túnel Cloud Connector	Cloud_Connector_DC1-DC2	Dirección IP de punto final local del túnel de Citrix Cloud Connector = 10.10.5.30, Dirección IP de punto final remoto del túnel de Citrix Cloud Connector = 203.0.210.30*

Entidad	Nombre	Detalles
		Detalles del túnel GRE Nombre = Cloud_Connector_DC1-DC2 **Detalles del perfil IPSec** Nombre = Cloud_Connector_DC1-DC2, Algoritmo de cifrado = AES, Algoritmo hash = HMAC SHA1
Ruta basada en políticas	CBC_DC1_DC2_PBR	Rango IP de origen = Subred en datacenter1 = 10.102.147.0-10.102.147.255, Intervalo IP de destino = Subred en datacenter2 = 10.20.20.0-10.20.20.255, Tipo de salto siguiente = túnel IP, Nombre del túnel IP = CBC_DC1_DC2

*Deben ser direcciones IP públicas.

En la siguiente tabla se enumeran los parámetros de CB-4000/5000-2 en el centro de datos DC2.

Entidad	Nombre	Detalles
Dirección IP del servidor S1		10.20.20.10
Parámetros en el dispositivo NAT-Dev-2		
Dirección IP NAT en el lado público		203.0.210.30*
Dirección IP NAT en el lado privado		10.10.8.80
Configuración en CB_4000/5000-2		
Dirección IP del servicio de administración de CB_SDX-1		10.10.2.10

Entidad	Nombre	Detalles
Configuración en NS_VPX_CB_4000/5000-2 que se ejecuta en CB_4000/5000-2		
La dirección NSIP		10.10.2.20
Dirección SNIP		10.10.6.30
Túnel de Citrix Cloud Connector	Cloud_Connector_DC1-DC2	Dirección IP de punto final local del túnel de Citrix Cloud Connector = 10.10.6.30, Dirección IP del extremo remoto del túnel de Citrix Cloud Connector = 203.0.113.30* **Detalles del túnel GRE** Nombre = Cloud_Connector_DC1-DC2 **Detalles del perfil IPSec** Nombre = Cloud_Connector_DC1-DC2, Algoritmo de cifrado = AES, Algoritmo hash = HMAC SHA1
Ruta basada en políticas	CBC_DC1_DC2_PBR	Rango IP de origen = Subred en datacenter2 = 10.20.20.0-10.20.20.255, Intervalo IP de destino = Subred en datacenter1 = 10.102.147.0-10.102.147.255, Tipo de salto siguiente = túnel IP, Nombre del túnel IP = CBC_DC1_DC2

*Deben ser direcciones IP públicas.

A continuación se muestra el flujo de tráfico en el túnel de Citrix Cloud Connector:

1. El cliente CL1 envía una solicitud al servidor S1.
2. La solicitud llega al dispositivo virtual Citrix NS_VPX_CB_4000/5000-1 que se ejecuta en el dispositivo Citrix SD-WAN WANOP CB_4000/5000-1.

3. NS_VPX_CB_4000/5000-1 reenvía el paquete a una de las instancias WANOP de SD-WAN que se ejecutan en el dispositivo Citrix SD-WAN WANOP CB_4000/5000-1 para la optimización de WAN. Después de procesar el paquete, la instancia WANOP de SD-WAN devuelve el paquete a NS_VPX_CB_4000/5000-1.
4. El paquete de solicitud coincide con la condición especificada en la entidad PBR CBC_DC1_DC2_PBR (configurada en NS_VPX_CB_4000/5000-1), porque la dirección IP de origen y la dirección IP de destino del paquete de solicitud pertenecen al intervalo IP de origen y al intervalo IP de destino, respectivamente, establecidos en CBC_DC1_DC2_PBR.
5. Dado que el túnel CBC_DC1_DC2_PBR está enlazado a CBC_DC1_DC2_PBR, el dispositivo prepara el paquete para que se envíe a través del túnel Cloud_Connector_DC1-DC2.
6. NS_VPX_CB_4000/5000-1 utiliza el protocolo GRE para encapsular cada uno de los paquetes de solicitud mediante la adición de un encabezado GRE y un encabezado IP GRE al paquete. En el encabezado IP GRE, la dirección IP de destino es la dirección del punto final del túnel del conector de nube (Cloud_Connector_DC1-DC2) en el centro de datos DC2.
7. Para el túnel de Cloud Connector Cloud_Connector_DC1-DC2, NS_VPX_CB_4000/5000-1 comprueba los parámetros de asociación de seguridad (SA) StoredIPSec para procesar paquetes salientes, según lo acordado entre NS_VPX_CB_4000/5000-1 y NS_VPX_CB_4000/5000-2. El protocolo IPSec Encapsulating Security Payload (ESP) en NS_VPX_CB_4000/5000-1 utiliza estos parámetros de SA para los paquetes salientes, para cifrar la carga útil del paquete encapsulado GRE.
8. El protocolo ESP garantiza la integridad y confidencialidad del paquete mediante la función hash HMAC y el algoritmo de cifrado especificado para el túnel de Citrix Cloud Connector Cloud_Connector_DC1-DC2. El protocolo ESP, después de cifrar la carga útil GRE y calcular el HMAC, genera un encabezado ESP y un remolque ESP y los inserta antes y al final de la carga útil GRE cifrada, respectivamente.
9. NS_VPX_CB_4000/5000-1 envía el paquete resultante NS_VPX_CB_4000/5000-2.
10. NS_VPX_CB_4000/5000-2 comprueba los parámetros de asociación de seguridad (SA) IPSec almacenados para procesar paquetes entrantes, según lo acordado entre CB_DC-1 y NS_VPX-AWS para el túnel de Cloud Connector Cloud_Connector_DC1-DC2. El protocolo ESP IPSec en NS_VPX_CB_4000/5000-2 utiliza estos parámetros de SA para los paquetes entrantes y el encabezado ESP del paquete de solicitud para descifrar el paquete.
11. NS_VPX_CB_4000/5000-2 luego descapsulará el paquete mediante la eliminación del encabezado GRE.
12. NS_VPX_CB_4000/5000-2 reenvía el paquete resultante a CB_VPX_CB_4000/5000-2, que aplica el procesamiento relacionado con la optimización WAN al paquete. CB_VPX_CB_4000/5000-2 devuelve el paquete resultante a NS_VPX_CB_4000/5000-2.

13. El paquete resultante es el mismo que recibió CB_VPX_CB_4000/5000-2 en el paso 2. Este paquete tiene la dirección IP de destino establecida en la dirección IP del servidor S1. NS_VPX_CB_4000/5000-2 reenvía este paquete al servidor S1.
14. S1 procesa el paquete de solicitud y envía un paquete de respuesta. La dirección IP de destino del paquete de respuesta es la dirección IP del cliente CL1 y la dirección IP de origen es la dirección IP del servidor S1.

Configurar el túnel de conector de nube entre un centro de datos y AWS/Azure

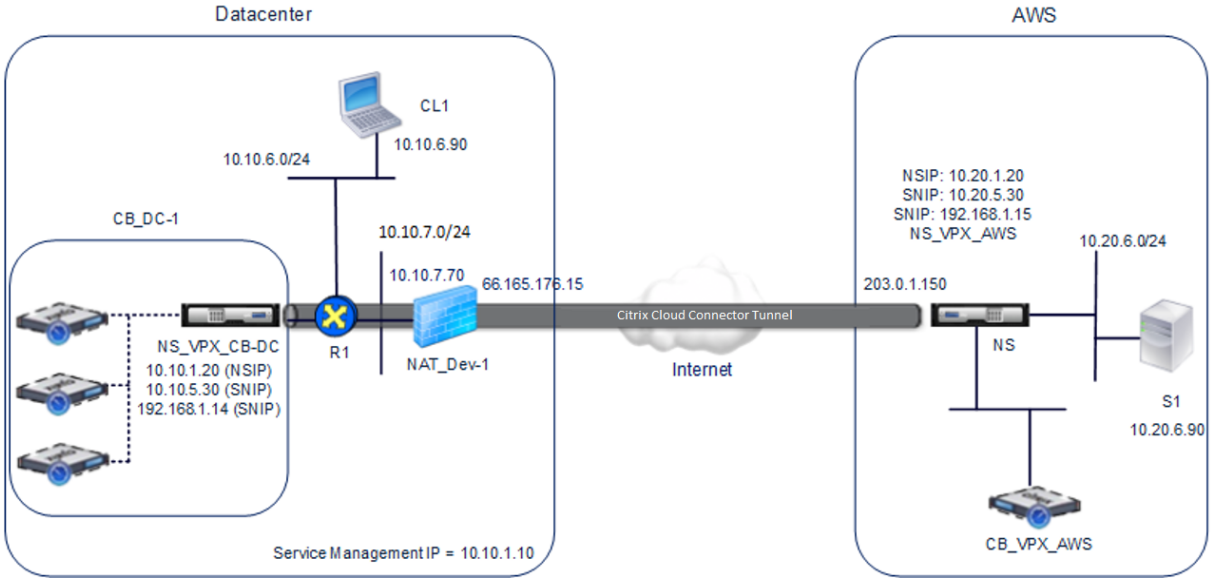
April 23, 2021

Puede configurar un túnel de conector de nube entre un centro de datos y AWS, o la nube de Azure.

Considere un ejemplo en el que se configura un túnel de Citrix Cloud Connector entre el dispositivo Citrix SD-WAN WANOP CB_DC-1, que se implementa en modo WCCP/PBR de un brazo en un centro de datos, y la nube de AWS. CB_DC-1 está conectado al router R1. Un dispositivo NAT también está conectado a R1 para conexiones entre el centro de datos e Internet.

Nota: La configuración del ejemplo también funcionaría para cualquier tipo de implementación WANOP de Citrix SD-WAN. Esta configuración de este ejemplo incluye rutas basadas en directivas en lugar de netbridge para permitir que el tráfico de la subred deseada pase a través del túnel de Citrix Cloud Connector.

Como se muestra en la siguiente figura, el túnel del conector de Citrix Cloud se establece entre el dispositivo virtual Citrix NS_VPX_CB-DC, que se ejecuta en el dispositivo Citrix SD-WAN WANOP CB_DC-1 y el dispositivo virtual Citrix NS_VPX-AWS que se ejecuta en la nube de AWS. Para optimizar la WAN el flujo de tráfico a través del túnel de Citrix Cloud Connector, NS_VPX_CB-DC está emparejado con las instancias WANOP de Citrix SD-WAN que se ejecutan en CB_DC-1 y, en el lado de AWS, el dispositivo virtual Citrix SD-WAN WANOP CB_VPX-AWS está emparejado con NS_VPX-AWS.



En la tabla siguiente se enumeran los parámetros del centro de datos de este ejemplo.

Entidad	Nombre	Detalles
Dirección IP del cliente CL1		10.10.6.90
Parámetros en el dispositivo NAT-Dev-1		
Dirección IP NAT en el lado público		66.165.176.15 *
Dirección IP NAT en el lado privado		10.10.7.70
Configuración en CB_DC-1		
Dirección IP del servicio de administración de CB_DC-1		10.10.1.10
Configuración en NS_VPX_CB-DC que se ejecuta en CB_DC-1		
La dirección NSIP		10.10.1.20
Dirección SNIP		10.10.5.30
Perfil IPSec	CBC_DC_AWS_IPSec_Profile	Versión IKE = v2, Algoritmo de cifrado = AES, Algoritmo hash = HMAC SHA1

Entidad	Nombre	Detalles
Túnel Cloud Connector	CBC_DC_AWS	Dirección IP de extremo local del túnel Cloud Connector = 10.10.5.30, dirección IP de extremo remoto del Cloud Connector = dirección EIP pública asignada a la dirección de extremo de Cloud Connector (SNIP) en NS_VPX-AWS en AWS = 203.0.1.150*, protocolo de túnel = GRE e IPSEC, nombre de perfil IPSec = CBC_DC_AWS_IPSEC_PROFILE
Ruta basada en políticas	CBC_DC_AWS_PBR	Rango IP de origen = Subred en el centro de datos = 10.10.6.0-10.10.6.255, Intervalo IP de destino = Subred en AWS = 10.20.6.0-10.20.6.255, Tipo de salto siguiente = túnel IP, Nombre del túnel IP = CBC_DC_AWS

*Deben ser direcciones IP públicas.

En la siguiente tabla se enumeran las opciones de configuración en la nube de AWS en este ejemplo.

Entidad	Nombre	Detalles
——	—-	——-
Dirección IP del servidor S1		10.20.6.90
Configuración en NS_VPX-AWS
Dirección NSIP		10.20.1.20
Dirección EIP pública asignada a la dirección NSIP		203.0.1.120*
Dirección SNIP		10.20.5.30
Dirección EIP pública asignada a la dirección SNIP		203.0.1.150*
IPSec profile	CBC_DC_AWS_IPSec_Profile
IKE version = v2, Encryption algorithm = AES, Hash algorithm = HMAC SHA1
Cloud Connector tunnel	CBC_DC_AWS	Local endpoint IP address of the Cloud Connector tunnel =10.20.5.30, Remote endpoint IP address of the Cloud Connector tunnel = Public NAT IP address of NAT device NAT-Dev-1 in the datacenter = 66.165.176.15*, Tunnel protocol = GRE and IPSEC, IPSec profile name = CBC_DC_AWS_IPSec_Profile

| Policy based route | CBC_DC_AWS_PBR | Source IP range = Subnet in the AWS = 10.20.6.0-10.20.6.255, Destination IP range = Subnet in datacenter = 10.10.6.0-10.10.6.255, Next hop type = IP Tunnel, IP tunnel name = CBC_DC_AWS |

*Deben ser direcciones IP públicas.

Tanto NS_VPX_CB-DC, en CB_DC-1, como NS_VPX-AWS funcionan en modo L3. Permiten la comunicación entre redes privadas en el centro de datos y la nube de AWS. NS_VPX_CB-DC y NS_VPX-AWS permiten la comunicación entre el cliente CL1 en el centro de datos y el servidor S1 en la nube de AWS a través del túnel Cloud Connector. El cliente CL1 y el servidor S1 están en diferentes redes privadas.

Nota: AWS no admite el modo L2. Por lo tanto, es necesario tener solo el modo L3 habilitado en ambos extremos.

Para una comunicación adecuada entre CL1 y S1, el modo L3 está habilitado en NS_VPX_CB-DC y NS_VPX-AWS, y las rutas se configuran de la siguiente manera:

- R1 tiene una ruta para llegar a S1 a través de NS_VPX_CB-DC.
- NS_VPX_CB-DC tiene una ruta para llegar a NS_VPX-AWS a través de R1.
- S1 debería tener una ruta que llegue a CL1 a través de NS_VPX-AWS.
- NS_VPX-AWS tiene una ruta para llegar a NS_VPX_CB-DC a través de un router ascendente.

Las siguientes son las rutas configuradas en varios dispositivos de red en el centro de datos para que el túnel Cloud Connector funcione correctamente:

Rutas	Red	Puerta de enlace
Rutas en el router R1		
Ruta para llegar al servidor S1	10.20.6.X/24	Dirección SNIP del extremo del túnel de NS_VPX_CB-DC = 10.10.5.30
Ruta para llegar al punto final remoto del túnel Cloud Connector	Dirección EIP asignada a la dirección SNIP del conector de nube de NS_VPX-AWS = 203.0.1.50	Dirección IP privada del dispositivo NAT = 10.10.7.70
Rutas en NS_VPX_CB-DC		
Ruta para llegar a NS_VPX-AWS	Dirección EIP asignada a la dirección SNIP del conector de nube de NS_VPX-AWS = 203.0.1.50	Dirección IP de R1 = 10.10.5.1

Las siguientes son las rutas configuradas en varios dispositivos de red en la nube de AWS para que el túnel Cloud Connector funcione correctamente:

Rutas	Red	Puerta de enlace
Rutas en el servidor S1		
Ruta para llegar al cliente CL1	10.10.6.X/24	Dirección SNIP del extremo del túnel de NS_VPX-AWS = 10.10.6.1
Rutas en el dispositivo virtual de Citrix NS_VPX-AWS		
Ruta para llegar a NS_VPX_CB-DC	Dirección IP pública de NAT_dev-1 en el centro de datos = 66.165.176.15*	Dirección IP del router ascendente en AWS

A continuación se presenta el flujo de tráfico de un paquete de solicitud de cliente CL1 en el túnel Cloud Connector:

1. El cliente CL1 envía una solicitud al servidor S1.
2. La solicitud llega al dispositivo virtual Citrix NS_VPX_CB-DC que se ejecuta en el dispositivo Citrix SD-WAN WANOP CB_DC-1.
3. NS_VPX_CB-DC reenvía el paquete a una de las instancias WANOP de Citrix SD-WAN que se ejecuta en el dispositivo Citrix SD-WAN WANOP CB_DC-1 para la optimización de WAN. Después de procesar el paquete, la instancia WANOP de Citrix SD-WAN devuelve el paquete a NS_VPX_CB-DC.
4. El paquete de solicitud coincide con la condición especificada en la entidad PBR CBC_DC_AWS_PBR (configurada en NS_VPX_CB-DC), porque la dirección IP de origen y la dirección IP de destino del paquete de solicitud pertenecen al intervalo IP de origen y al intervalo IP de destino, respectivamente, establecidos en CBC_DC_AWS_PBR.
5. Dado que el túnel del conector de nube CBC_DC_AWS está enlazado a CBC_DC_AWS_PBR, el dispositivo prepara el paquete para enviarlo a través del túnel CBC_DC_AWS.
6. NS_VPX_CB-DC utiliza el protocolo GRE para encapsular cada uno de los paquetes de solicitud mediante la adición de un encabezado GRE y un encabezado IP GRE al paquete. El encabezado IP GRE tiene la dirección IP de destino establecida en la dirección IP del punto final del túnel del conector de la nube (CBC_DC-AWS) en el lado de AWS.
7. Para el túnel de Cloud Connector CBC_DC-AWS, NS_VPX_CB-DC comprueba los parámetros de asociación de seguridad (SA) IPSec almacenados para procesar paquetes salientes, según lo

acordado entre NS_VPX_CB-DC y NS_VPX-AWS. El protocolo IPSec Encapsulating Security Payload (ESP) en NS_VPX_CB-DC utiliza estos parámetros de SA para los paquetes salientes, para cifrar la carga útil del paquete encapsulado GRE.

8. El protocolo ESP garantiza la integridad y confidencialidad del paquete mediante la función hash HMAC y el algoritmo de cifrado especificado para el túnel de Cloud Connector CBC_DC-AWS. El protocolo ESP, después de cifrar la carga útil GRE y calcular el HMAC, genera un encabezado ESP y un remolque ESP y los inserta antes y al final de la carga útil GRE cifrada, respectivamente.
9. NS_VPX_CB-DC envía el paquete resultante a NS_VPX-AWS.
10. NS_VPX-AWS comprueba los parámetros de asociación de seguridad (SA) IPSec almacenados para procesar paquetes entrantes, según lo acordado entre CB_DC-1 y NS_VPX-AWS para el túnel de Cloud Connector CBC_DC-AWS. El protocolo ESP IPSec en NS_VPX-AWS utiliza estos parámetros de SA para los paquetes entrantes y el encabezado ESP del paquete de solicitud para descifrar el paquete.
11. A continuación, NS_VPX-AWS descapsulará el paquete mediante la eliminación del encabezado GRE.
12. NS_VPX-AWS reenvía el paquete resultante a CB_VPX-AWS, que aplica el procesamiento relacionado con la optimización WAN al paquete. CB_VPX-AWS devuelve el paquete resultante a NS_VPX-AWS.
13. El paquete resultante es el mismo paquete que el recibido por CB_DC-1 en el paso 2. Este paquete tiene la dirección IP de destino establecida en la dirección IP del servidor S1. NS_VPX-AWS reenvía este paquete al servidor S1.
14. S1 procesa el paquete de solicitud y envía un paquete de respuesta. La dirección IP de destino del paquete de respuesta es la dirección IP del cliente CL1 y la dirección IP de origen es la dirección IP del servidor S1.

Aceleración de Office 365

April 23, 2021

Citrix SD-WAN WANOP optimiza la WAN para proporcionar una experiencia de usuario coherente para las aplicaciones empresariales en sucursales y sitios remotos.

Microsoft Office 365 es una aplicación de software como servicio (SaaS), que proporciona el conjunto de aplicaciones de productividad de nivel empresarial de Office de Microsoft. Esta aplicación está alojada en la nube y se entrega bajo demanda a los usuarios.

La función de aceleración de Office 365 permite a las sucursales obtener los beneficios de optimización que Citrix SD-WAN WANOP proporciona para la aplicación Microsoft Office 365.

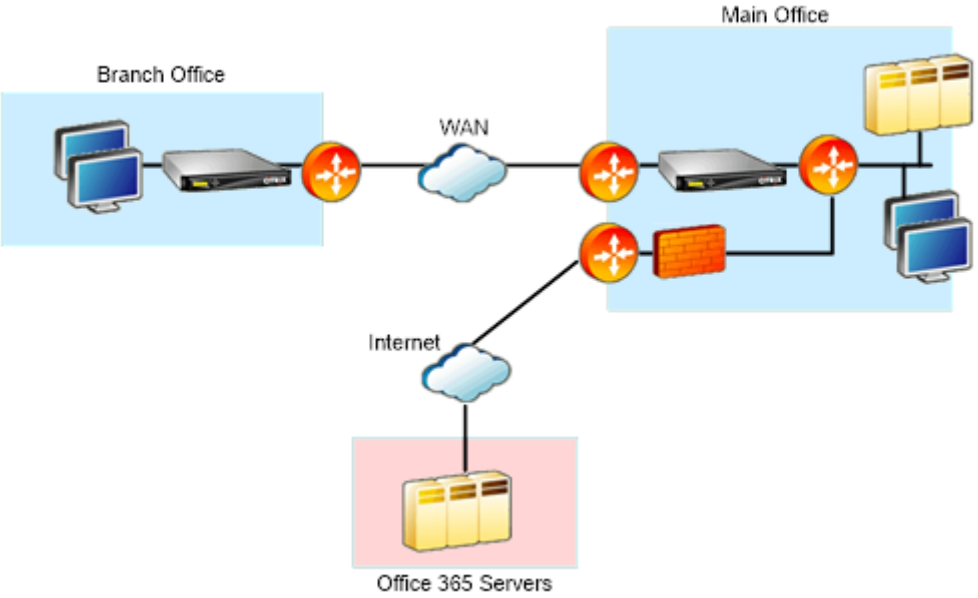
Caso de uso

Cuando el segmento WAN es considerablemente más lento que el segmento de Internet, y los servidores de Microsoft Office 365 están más cerca de la oficina más grande que la sucursal.

Topología

El tráfico de Office 365 de sucursales se envía a través de la WAN a la oficina principal y, a continuación, se reenvía a los servidores de Office 365 a través de Internet. El segmento entre la sucursal y la oficina principal se acelera.

> **Nota**
>
> El segmento entre la oficina principal y los servidores de Microsoft Office 365 no se acelera. Se recomienda que la oficina principal se conecte al servidor de Office 365 más cercano.



¿Cómo funciona?

La aceleración SSL WANOP de Citrix SD-WAN puede descifrar y acelerar el tráfico de Office 365, proporcionando compresión. En resumen, la aceleración de sucursales de Office 365 se puede considerar como un caso especial de aceleración RPC-sobre HTTPS.

Procedimiento

1. Cree un peering seguro entre la sucursal y la oficina principal de Citrix SD-WAN WANOP.
2. Generar certificados proxy/clave privada en la entidad emisora de certificados de dominio (CA).
3. Agregue todas las CA necesarias en Citrix SD-WAN WANOP.
   a) CA, CA intermedias, CA raíz de los certificados de Microsoft.
   b) Certificados de proxy y claves privadas generadas para URL de Office 365.

   > **Nota**
   >
   > Para evitar alertas de seguridad en los exploradores, los certificados proxy deben estar firmados por el servidor de CA de su dominio de Windows, lo que lo hace aceptable para cualquier usuario de dominio.

4. Crear perfil proxy dividido SSL y enlazar el proxy dividido a la clase de servicio (web (seguro de Internet)).
5. Inicie la conexión de Office 365 y compruebe las conexiones aceleradas.

   > **Advertencia**
   >
   > Los dispositivos de sucursales que no forman parte del dominio mostrarán advertencias de seguridad a menos que instale los certificados manualmente. Los usuarios de Firefox también tienen que instalar los certificados manualmente, ya que Firefox no respeta el almacén de certificados del dispositivo.

Configurar la aceleración de Office 365

Para configurar la aceleración de Office 365:

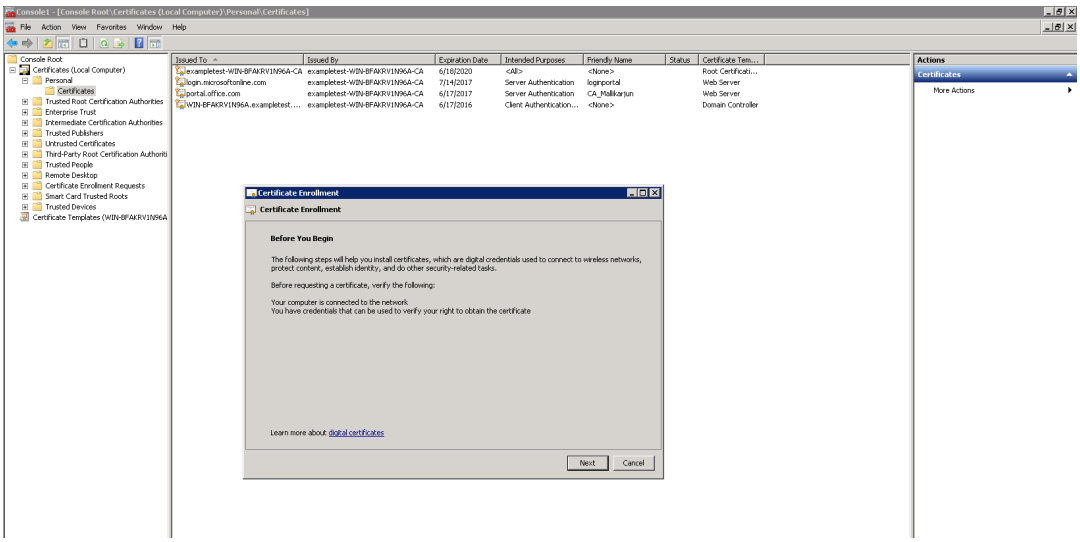
1. Configurar una relación de peering segura entre los dos dispositivos Citrix SD-WAN WANOP, como se describe en *Secure Peering*
2. Cree un nuevo certificado.

   > **Nota**
   >
   > El dispositivo Citrix SD-WAN WANOP del lado del servidor sirve como intermediario entre Office 365 y los clientes, por lo que estos certificados serán firmados por el controlador de dominio del lado del servidor, pero hace referencia a los dominios de Office 356.

   a) Inicie sesión en el **servidor de la entidad de certificación** del dominio de Windows.
   b) Si es necesario, agregue los complementos para **Entidad de certificación**, **Plantilla de certificado** y **Certificados**.

c) Vaya a **Plantillas de certificado** > **Propiedades del servidor web** > **Seguridad** y seleccione todas las opciones.

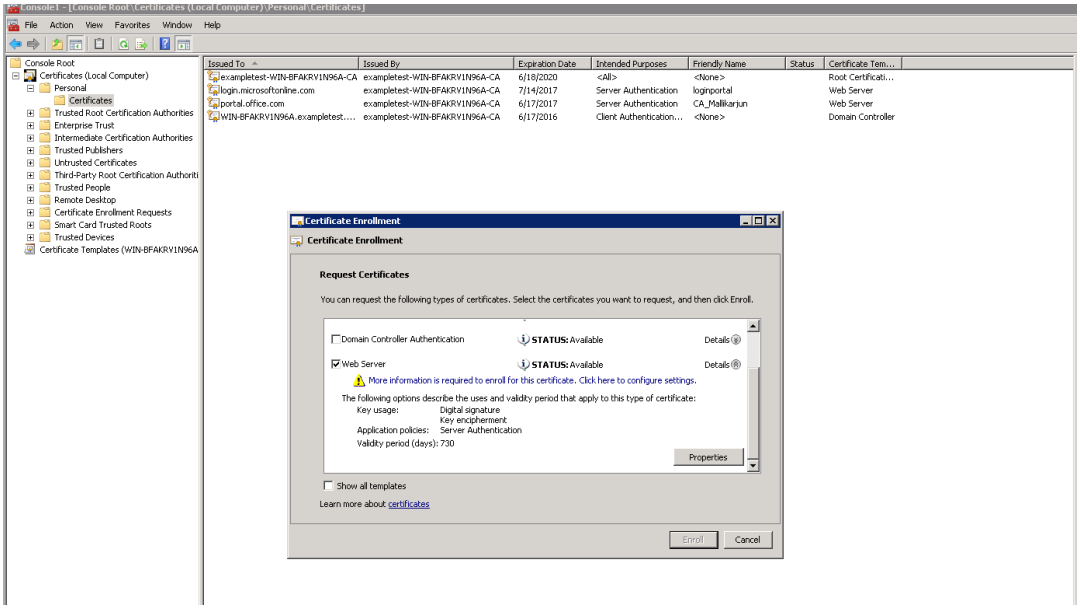
d) Desplácese a **Certificados** > **Personal** > **Certificados (Equipo)** > **Todas las tareas** > **Solicitar nuevo certificado**.



e) En la **ventana Registro de certificados**, haga clic en **Siguiente**.

f) En la ventana **Seleccionar directiva de inscripción de certificados**, seleccione **Directiva de inscripción de Active Directory**.

g) En la ventana **Directiva de inscripción de Active Directory**, seleccione **Servidor web** > **Detalles** > **Propiedades**.



3. Copie la información de los certificados de Office365 en los certificados nuevos. Terminará con un solo certificado de tres certificados de Office365. Lleve a cabo lo siguiente:

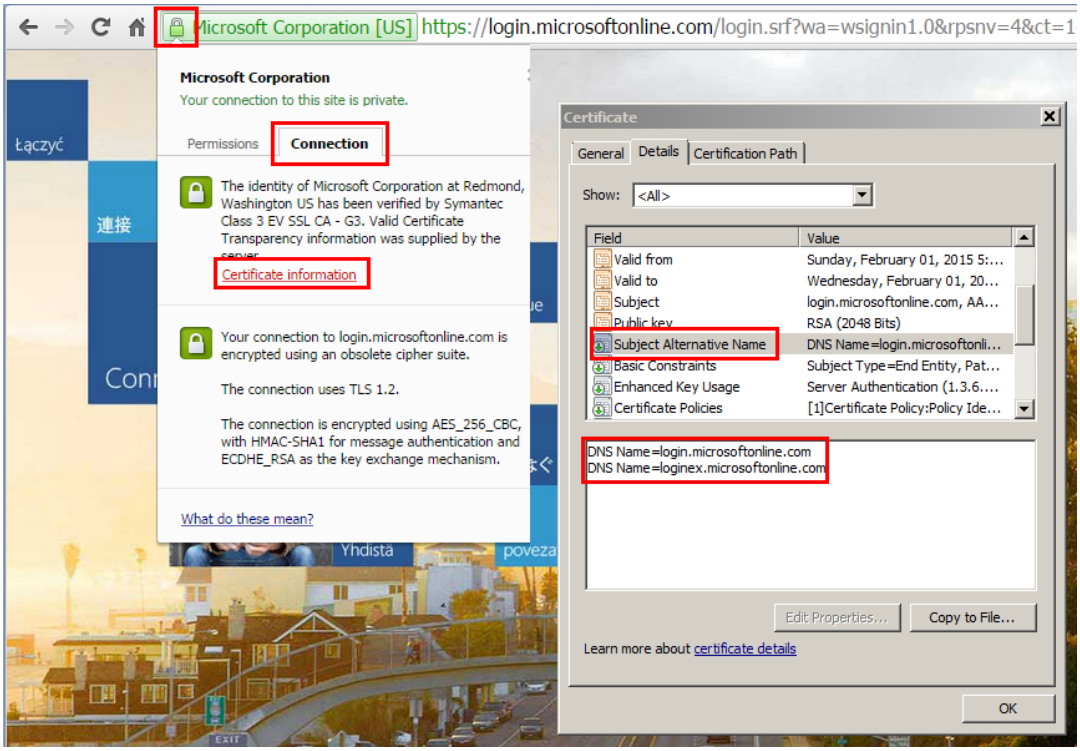
a) En un navegador, como Chrome, introduzca la url -https://login.microsoftonline.com.

> **Nota**
>
> No iniciar sesión.

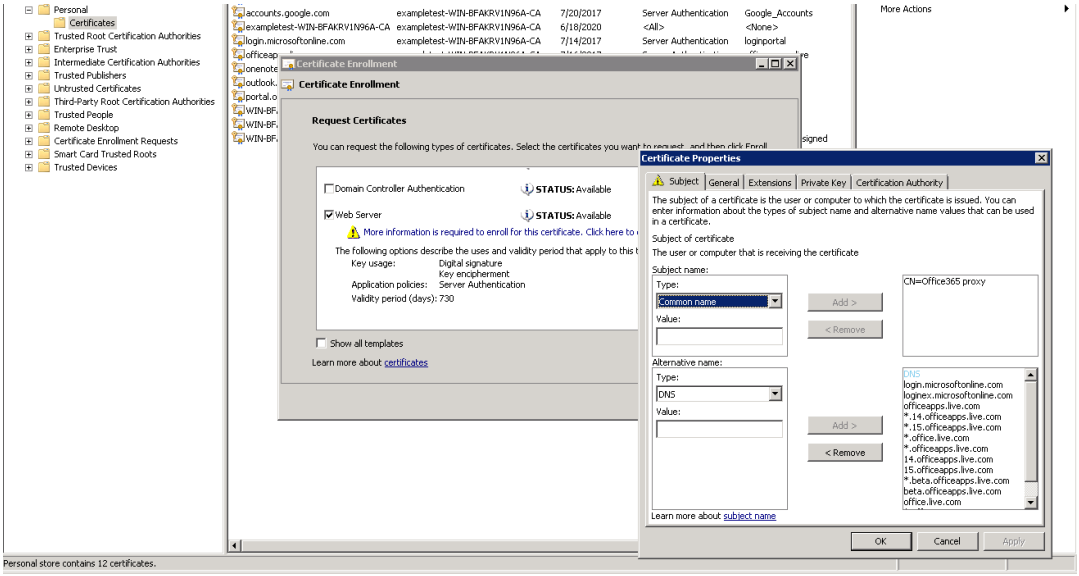
b) Haga clic en el icono de candado de la barra de direcciones URL y seleccione **Conexión** > **Información del certificado** > **Detalles**.

> **Nota**
>
> Estas instrucciones son para el explorador Chrome; el procedimiento es el mismo para otros exploradores web también.

c) Haga clic en **Nombre alternativo del asunto**, esto mostrará una lista de nombres DNS como login.microsoftonline.com. Copie la información en el cuadro de texto debajo.

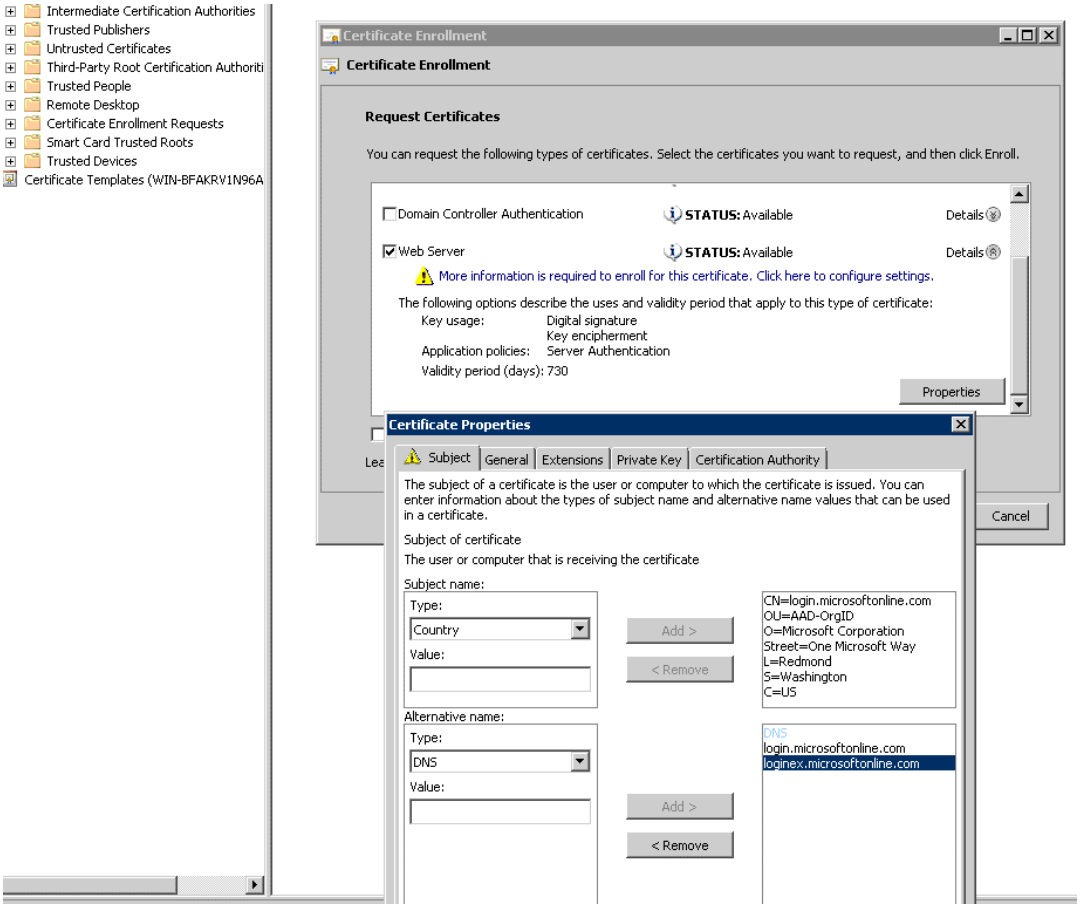


d) Vuelva a la ventana **Propiedades de certificados** del nuevo certificado. Agregue los nombres alternativos en el campo **Valor** con **Tipo** como **DNS** para que coincidan con cada nombre alternativo en el certificado de Microsoft.



e) Repita el proceso de descubrir nombres alternativos del sujeto y agregarlos a su certificado para https://outlook.office365.com, https://portal.office.com, https://office.live.com y https://sharepoint.com (la URL de SharePoint es específica del cliente).

f) Cree un nombre común para el nuevo certificado. El ejemplo anterior muestra un nombre común como Proxy de Office365.

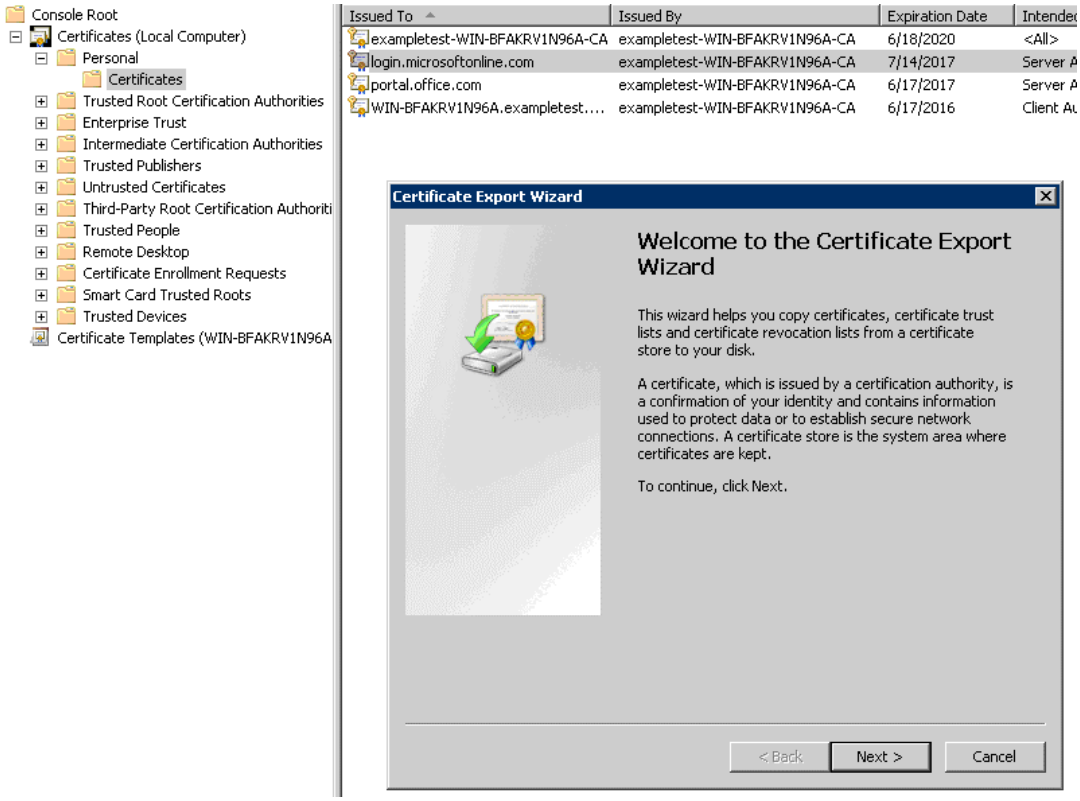


g) En la ficha **Clave privada**, seleccione **Hacer que la clave privada sea exportable**.

h) Haga clic en **Aceptar**, **Inscribir** y **Finalizar**.

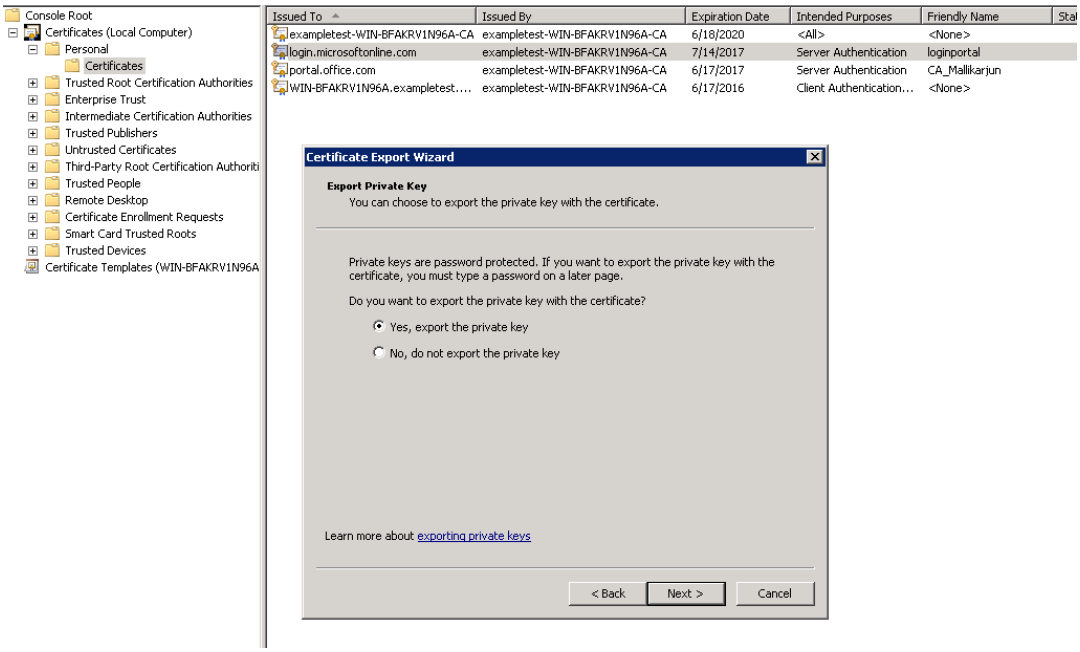
4. Exporte el certificado.

a) En **Certificados** > **Personal** > **Certificados**, seleccione el certificado proxy creado anteriormente y, a continuación, seleccione **Todas las tareas** > **Exportar**.



b) Aparecerá el **Asistente para exportación de certificados**. Haga clic en **Siguiente**.

c) En **Exportar clave privada**, seleccione la opción **Sí, exporte la clave privada** y haga clic en **Siguiente**.

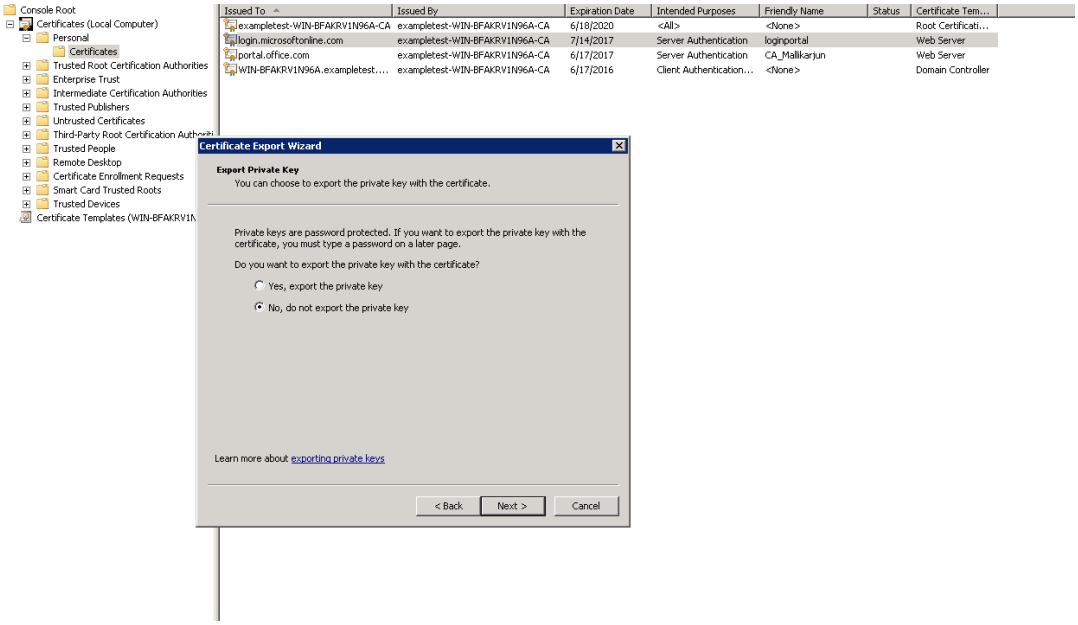


d) Conservar los valores predeterminados para el formato de archivo de exportación.

e) Escriba y confirme la contraseña, exporte la clave privada y guarde el certificado como *loginportal.pfx*.

5. Exporte sus certificados.

a) En el **Asistente para exportación de certificados**, haga clic en **Siguiente**. En **Exportar clave privada**, seleccione la opción **No, no exporte la clave privada**. Haga clic en **Siguiente**.



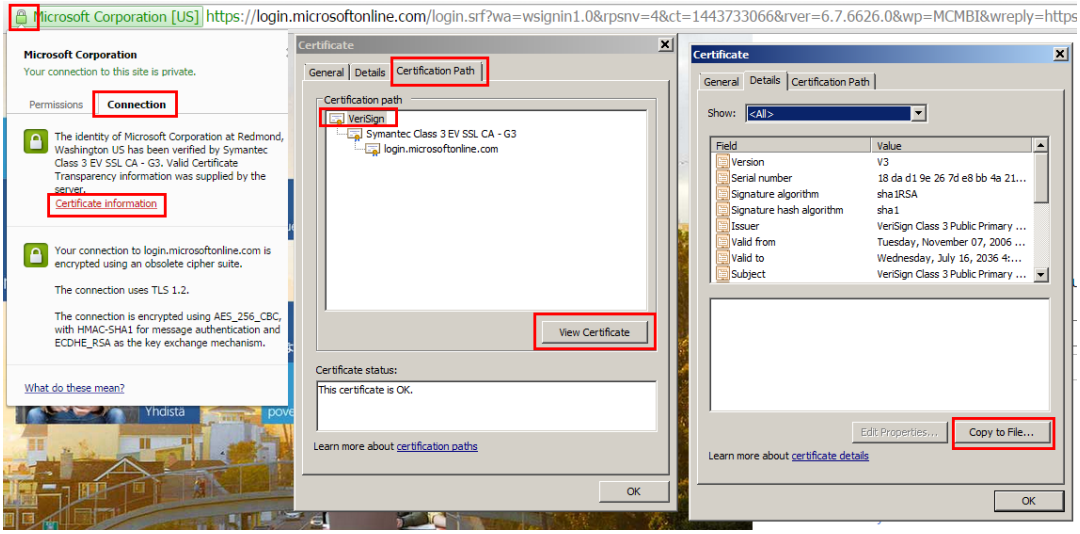
b) Conservar los valores predeterminados para el formato de archivo de exportación.

c) Escriba y confirme la contraseña y exporte la clave privada y el certificado, guardando el archivo en un archivo en un nombre de archivo como office365_keys.pfx.

6. Descargue las claves públicas de la CA raíz y las CA intermedias de los certificados de Microsoft.

a) Desde el explorador web, vaya a https://login.microsoftonline.com. Haga clic en el icono de candado en el explorador web. Desplácese a **Conexión** > **Información del certificado** > **Ruta de certificación**.

b) Seleccione el certificado raíz (el que se encuentra en la parte superior de la lista) y, a continuación, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo**. Aparecerá el **Asistente para exportación de certificados**. Haga clic en **Siguiente**.



c) Introduzca el nombre del archivo y guarde el archivo.

> **Nota**
>
> Alternativamente, puede usar Wireshark o OpenSSL para obtener los nombres de CA raíz e intermedia y obtener los certificados de origen 'AUTHENTIC'(por ejemplo, almacén SSL de Windows).

d) Repita el paso 6 para guardar las CA raíz e intermedias de los siguientes dominios:

   i. login.microsoftonline.com

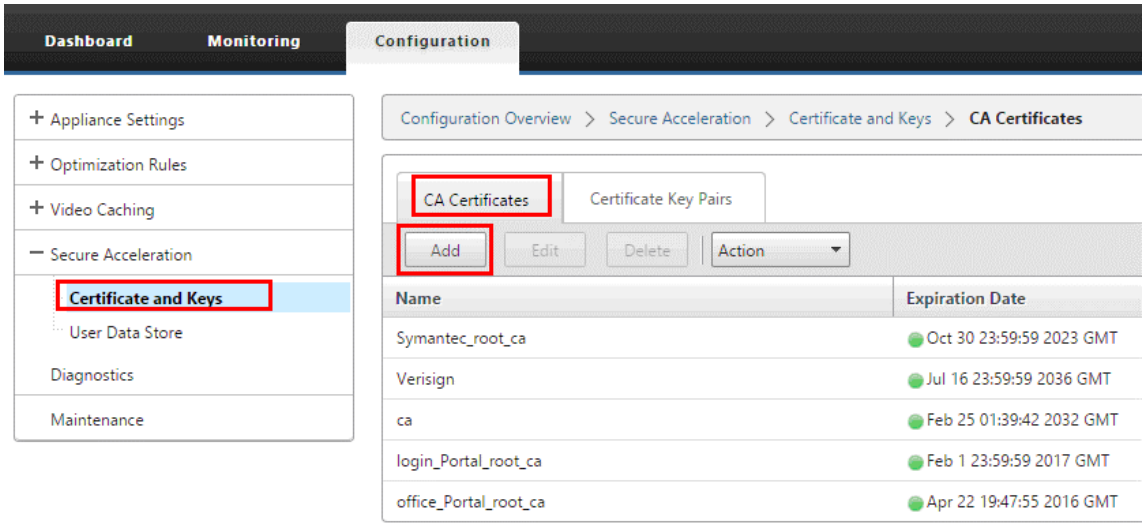
   ii. portal.office.com

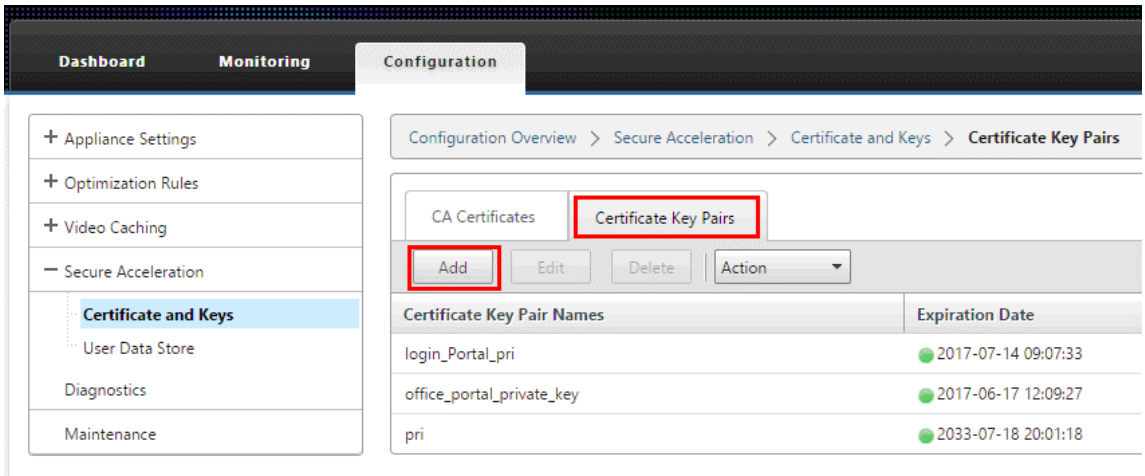
   iii. outlook.office356.com

   iv. *.sharepoint.com

   v. office.live.com

7. Agregue todas las CA del servidor de Office 365, los pares de certificados y claves de proxy y las claves privadas al dispositivo Citrix SD-WAN WANOP del servidor. Las CA se agregan mediante la ficha **Certificados de CA** de la página **Certificados y claves**. Los certificados y los pares de certificados y claves se agregan en la ficha **Pares de certificados y claves**.





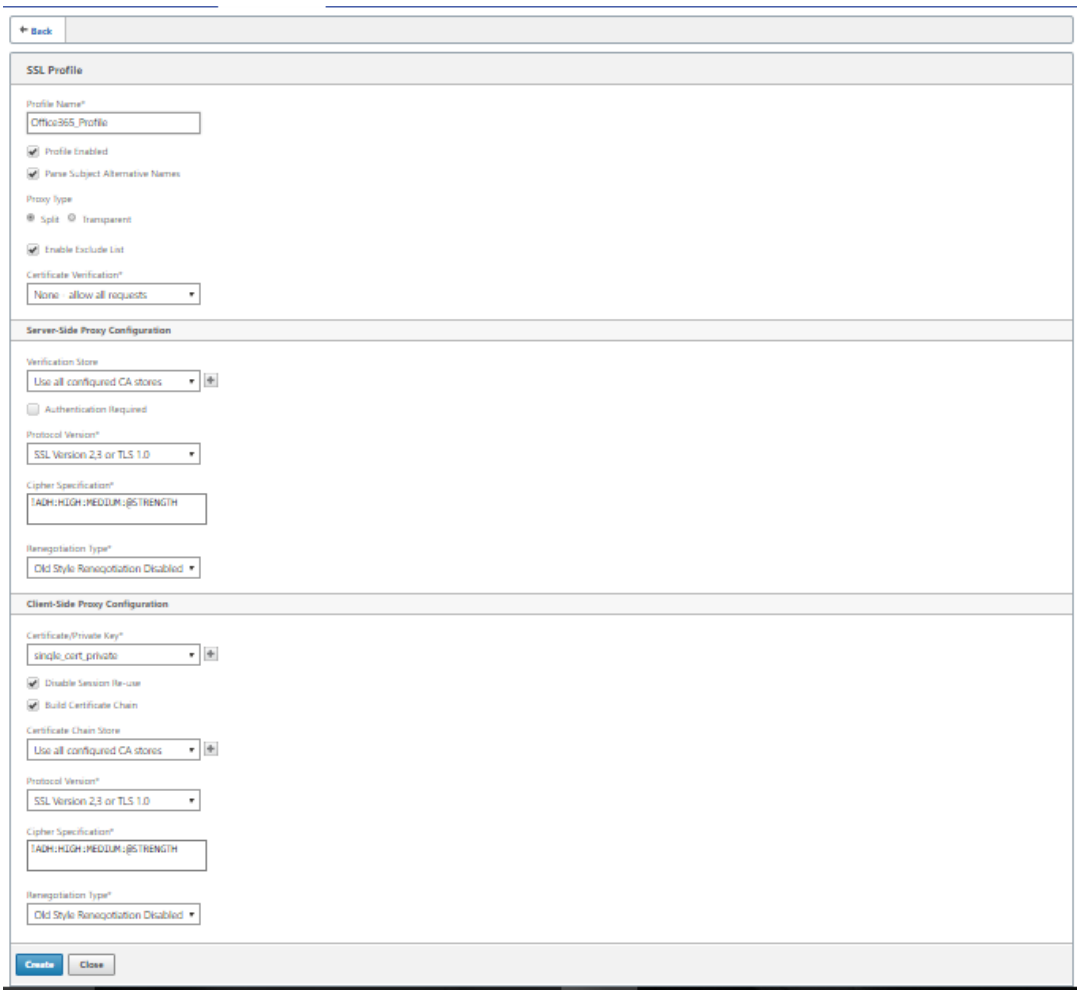
8. Cree un perfil de proxy dividido SSL y vincule el proxy dividido a la clase de servicio web (Internet Secure).

   a) Vaya a **Configuración** > **Aceleración segura** > **Perfil SSL** > **Agregar perfil**.

   b) Introduzca el nombre de perfil de su elección. Seleccione **Perfil habilitado**, **Analizar nombres alternativos de sujeto** y **Dividir proxy**.

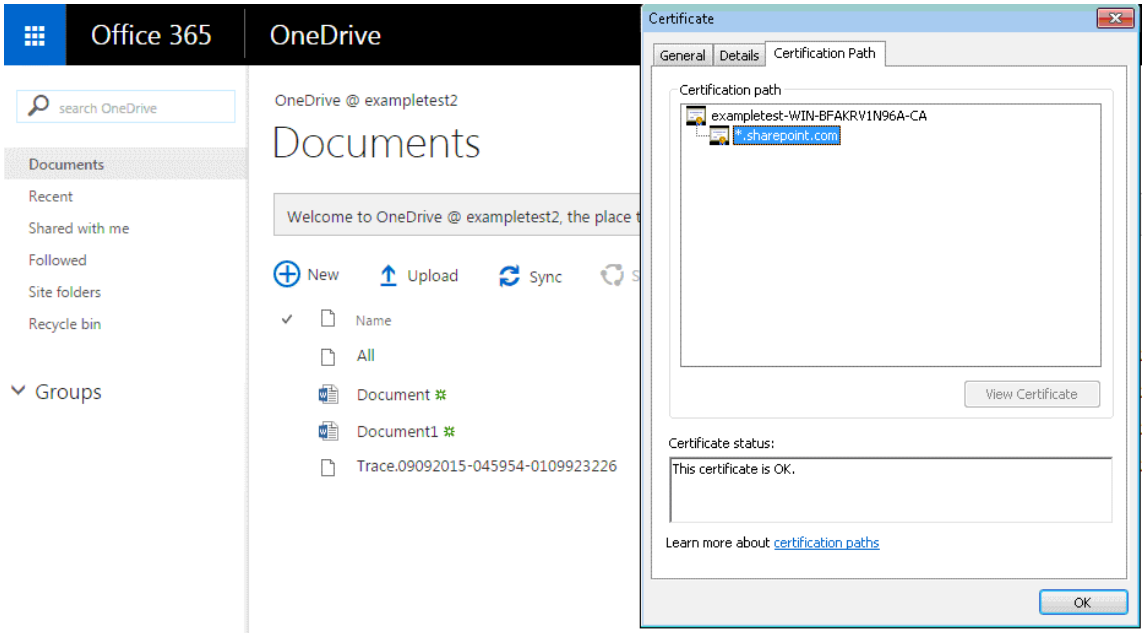
   c) En **Configuración de proxy del lado del servidor** > **Almacén de verificación**, seleccione **Usar todos los almacenes de CA configurados**.

   d) En **Configuración de proxy del lado del cliente** > **Clave certificada/privada**, seleccione el par de claves cert/privada que ha creado y exportado previamente (el que se muestra en el ejemplo como loginportal.pfx). Seleccione **Crear cadena de certificados**. Seleccione la entidad emisora de certificados asociada al par de certificados y claves en **Almacén de cadena de certificados**.

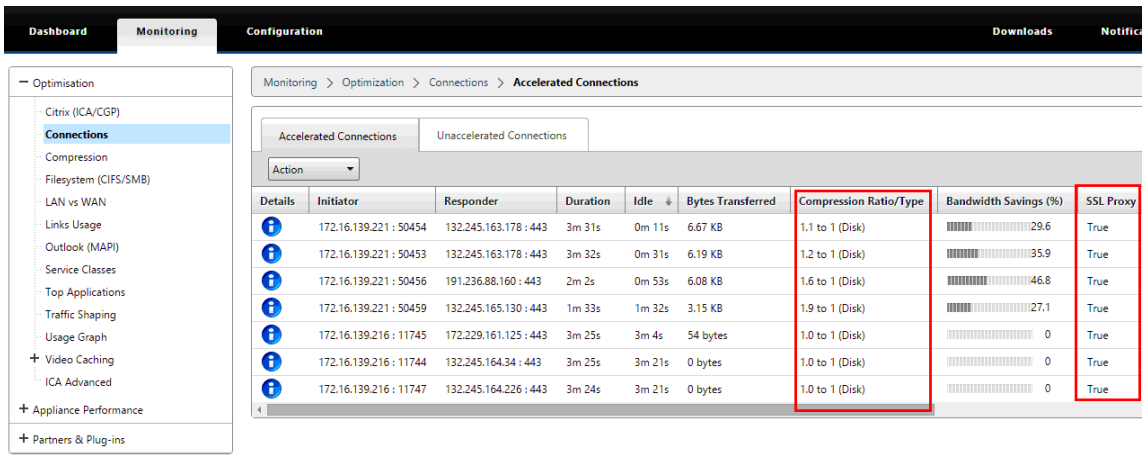


9. Enlace el perfil SSL creado a la clase de servicio Internet (Web-Secure). Desplácese hasta **Configurar** > **Reglas de optimización** > **Clases de servicio** y agregue el perfil SSL a la lista de perfiles SSL.
10. Habilite la aceleración y la compresión basada en disco para la clase de servicio **Internet (Web-Secure)**.
11. Inicie una sesión de Office 365 desde el explorador.

    La conexión se acelera. En el explorador, el certificado debe mostrar la CA raíz, no el certificado real de Office 365, como certificado de CA del dispositivo del servidor.



12. En la página **Supervisión** del dispositivo > **Conexiones**, compruebe que las conexiones de Office 365 estén comprimidas y estén recibiendo aceleración SSL.

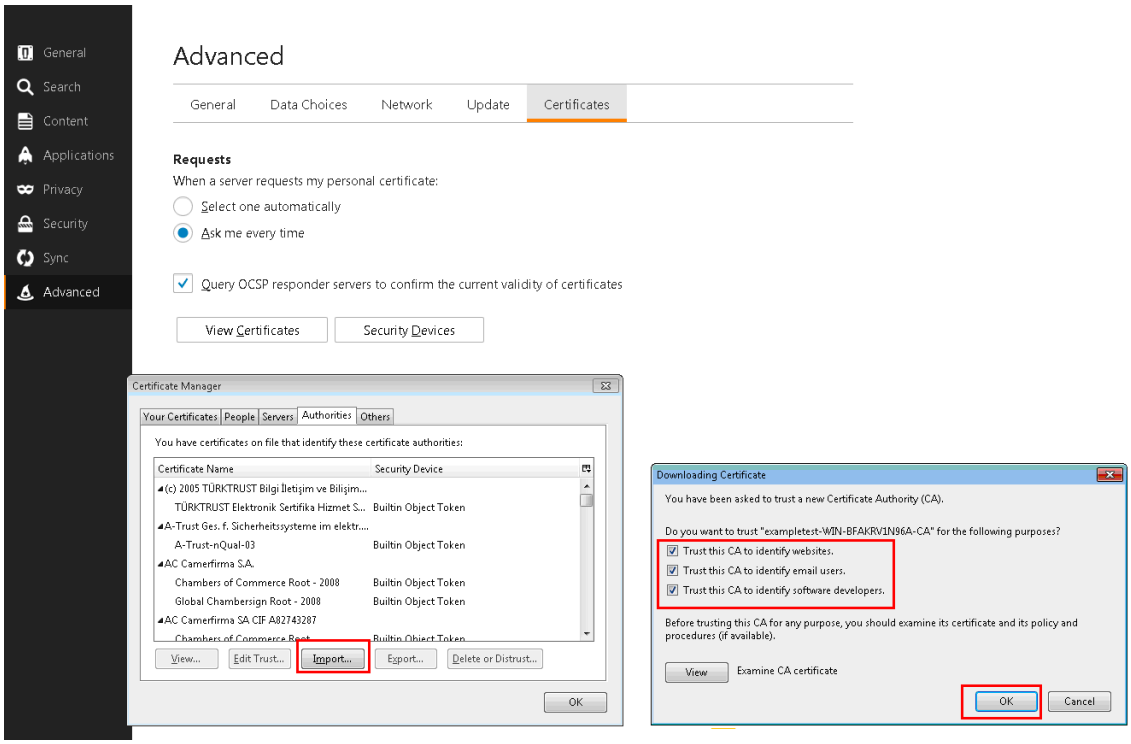


> **Nota**
>
> Firefox no acepta los certificados del dispositivo de forma predeterminada, pero tiene su propio almacén de certificados. Por lo tanto, las credenciales aceptadas en el comportamiento normal del dominio de Windows por otros exploradores web, y por el dispositivo en su conjunto, deben instalarse manualmente en Firefox.Para instalar certificados en Firefox, siga el procedimiento de la sección Instalación de certificados en Firefox.

Instalar los certificados en Firefox

Para instalar el certificado proxy del dispositivo del servidor en el almacén de certificados de Firefox:

1. En el navegador Firefox navegando a **Opciones**> **Avanzadas** > **Certificado** > **Ver certificados** > **Autoridades** > **Importar**.
2. Cargue el certificado proxy de CA local, seleccione todas las opciones en el Asistente de **descarga de certificados** y haga clic en **Aceptar**.



Soporte de SCPS

April 23, 2021

Citrix SD-WAN WANOP admite la variante TCP SCPS (Space Communications Protocol Standard). SCPS es ampliamente utilizado para la comunicación por satélite.

Consulte http://www.scps.org para obtener información general sobre SCPS.

SCPS es una variante TCP utilizada en comunicaciones por satélite y aplicaciones similares. El dispositivo puede acelerar las conexiones SCPS si se selecciona la opción **SCPS** en la página Configuración: Ajuste.

La principal diferencia práctica entre SCPS y el comportamiento predeterminado del dispositivo es que se utilizan reconocimientos negativos selectivos (Snacks) de estilo SCPS en lugar de reconocimientos selectivos estándar (SACK). Estos dos métodos de mejora de las retransmisiones de datos son mutuamente excluyentes, por lo que si el dispositivo en un extremo de la conexión tiene

SCPS habilitado y uno no lo hace, el rendimiento de la retransmisión se ve afectado. Esta condición también provoca una alerta de Discordancia del modo SCPS.

Si debe mezclar dispositivos habilitados para SCPS con dispositivos no habilitados para SCPS, implemente de tal manera que no se produzcan discrepancias. Puede utilizar reglas de clase de servicio basadas en IP u organizar la implementación para que cada ruta tenga dispositivos coincidentes.

Aceleración segura del tráfico

April 23, 2021

La aceleración segura del tráfico se logra mediante un peering seguro. Varias funciones avanzadas requieren que los dispositivos Citrix SD-WAN WANOP en los dos extremos del enlace establezcan una *relación de pares segura* entre sí, configurando un túnel de señalización SSL (también denominado *conexión de señalización*). Estas funciones son compresión SSL, soporte CIFS firmado y compatibilidad con MAPI cifrada.

Cuando se habilita el peering seguro, la compresión se deshabilita automáticamente para todos los dispositivos asociados (y los equipos que ejecutan Citrix SD-WAN WANOP Plug-in) que no han establecido una relación de pares segura con el dispositivo local.

Para establecer una relación de pares segura, debe generar claves de seguridad y certificados y configurar un túnel de señalización de seguridad entre los dispositivos. Antes de configurar el túnel, solicite una licencia criptográfica a Citrix.

Emparejamiento seguro

April 23, 2021

Cuando un dispositivo tiene habilitado el emparejamiento seguro, las conexiones con un asociado para el que no tiene una relación de pares seguros no se cifran ni comprimen, aunque la aceleración del control de flujo TCP sigue estando disponible. La compresión está inhabilitada para garantizar que los datos almacenados en el historial de compresión de socios seguros no se puedan compartir con socios no seguros.

Cuando el dispositivo en un extremo de una conexión detecta que el otro dispositivo tiene habilitado el peering seguro, intenta abrir un túnel de señalización SSL. Si los dos dispositivos se autentican correctamente a través de este túnel, tienen una relación de peering segura. Todas las conexiones aceleradas entre los dos dispositivos están cifradas y la compresión está habilitada.

> **Nota**
>
> Un dispositivo con emparejamiento seguro habilitado no comprime las conexiones a socios no seguros, por lo que resulta difícil utilizar correctamente el mismo dispositivo con una combinación de asociados seguros y no protegidos. Tenga en cuenta este punto al diseñar su red acelerada.

Se requiere una contraseña de almacén de claves para acceder a los parámetros de seguridad. Esta contraseña de almacén de claves es diferente de la contraseña del administrador, para permitir que la administración de seguridad se separe de otras tareas. Si se restablece la contraseña del almacén de claves, se pierden todos los datos cifrados y las claves privadas existentes.

Para proteger los datos incluso en caso de robo del dispositivo, se debe volver a introducir la contraseña del almacén de claves cada vez que se reinicie el dispositivo. Hasta que esto se haga, el peering seguro y la compresión están inhabilitados.

Generar claves de seguridad y certificados

Los productos de Citrix SD-WAN WANOP se envían sin las claves y certificados necesarios para el túnel de señalización SSL. Debes generarlos tú mismo. Puede generar claves y certificados a través de su proceso normal para generar credenciales, o con el paquete openssl de http://www.openssl.org.

Para fines de prueba, puede generar y usar un certificado X509 autofirmado basado en una clave privada (que también genera). En producción, utilice certificados que hagan referencia a una autoridad certificadora de confianza. El siguiente ejemplo llama a openssl desde la línea de comandos en un PC para generar una clave privada (
my.key) y un certificado autofirmado (
my.crt):

```
pre codeblock
# Generate a 2048-bit private key
openssl genrsa -out my.key 2048
# Now create a Certificate Signing Request
openssl req -new -key my.key -out my.csr
# Finally, create a self-signed certificate with a 365-day expiration
openssl x509 -req -days 365 -in my.csr -signkey my.key -out my.crt
<!--NeedCopy-->
```

Para el uso de producción, consulte las directrices de seguridad de su organización.

Configurar emparejamiento seguro

Existen dos formas de establecer un peering seguro:

1. Con las credenciales generadas por los dispositivos.
2. Con las credenciales que usted mismo proporcione.

   Dado que un dispositivo con peering seguro habilitado solo comprimirá las conexiones con dispositivos asociados con los que tenga una relación de peering segura, este procedimiento debe aplicarse al mismo tiempo a todos los dispositivos.

Para preparar los dispositivos para un peering seguro:

Realice el siguiente procedimiento en cada dispositivo de la red.

1. Instale una licencia criptográfica en el dispositivo. Sin una licencia criptográfica, la aceleración segura no está disponible.

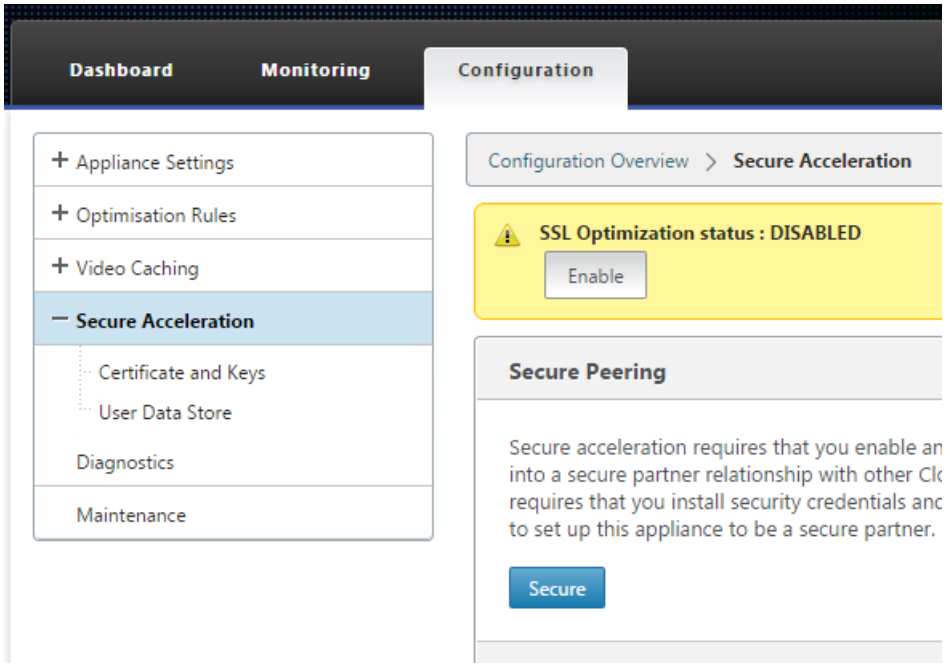
   a) Si aún no lo ha hecho, adquiera licencias criptográficas de Citrix.

   b) Si utiliza un servidor de licencias de red, vaya a **Configuración > Configuración** del **dispositivo** > **Licencias.** En la sección**Agregar licencia**, haga clic en **editar**, seleccione el servidor de licencias remoto y configure Crypto License Activado.

   c) Si utiliza licencias locales, vaya a **Configuración > Configuracióndel dispositivo**>**Licencias.**En la página**Agregar licencia**, haga clic en la opción Servidor de licencias local y haga clic en**Agregar** para cargar una licencia criptográfica local.

   d) Compruebe la instalación correcta de la licencia en la página **Configuración** > **Configuración del equipo** > Licencias. En Información de licencia, una licencia criptográfica debe mostrarse como activa y con una fecha de caducidad en el futuro.

2. Vaya a la página **Configuración** > **Aceleración segura**. Si la página tiene un botón denominado Seguro, haga clic en él.



3. Si se le lleva a una pantalla de configuración de almacén de claves automáticamente, haga lo siguiente:

   a) Introduzca una contraseña de almacén de claves dos veces y haga clic en Guardar.

   b) Cuando la pantalla se actualice para mostrar la sección Secure Peering Certificates and Keys, haga clic en Habilitar Secure Peering and CA Certificate y, a continuación, haga clic en Guardar.

   c) Vaya al paso 6.

4. Si no se le ha llevado a la pantalla Configuración del almacén de claves automáticamente, haga clic en el icono del lápiz debajo de Configuración del almacén de claves **y, a**continuación, haga clic en el icono del lápiz debajo de **Configuración del almacén de claves.** Abra en el menú desplegable Estado del almacén de claves e introduzca dos veces una contraseña del almacén de claves. Haga clic en **Guardar**.

5. Habilite el peering seguro yendo a la página **Configuración** > **Aceleración segura** y haciendo clic en el botón **Habilitar**. Ignore cualquier advertencia en esta etapa. Esta configuración permite establecer un peering seguro cuando se completa la configuración adicional requerida.

6. Habilite el cifrado del historial de compresión yendo a **Configuración** > **Almacén de datos de usuario** de **aceleración segura** y haciendo clic en el icono del lápiz. Haga clic en **Habilitar cifrado de disco**y, a continuación, en **Guardar**. El cifrado del almacén de datos del usuario impide la lectura no autorizada del historial de compresión basado en el disco, en caso de que el dispositivo sea robado o devuelto a fábrica. La seguridad del cifrado de datos de disco se basa en la contraseña del almacén de claves. Esta función utiliza el cifrado AES-256. (El cifrado de datos de disco no cifra todo el disco, solo el historial de compresión.)

7. Si utiliza credenciales generadas por dispositivos, vaya al paso siguiente. Si utiliza sus propias credenciales, haga lo siguiente:

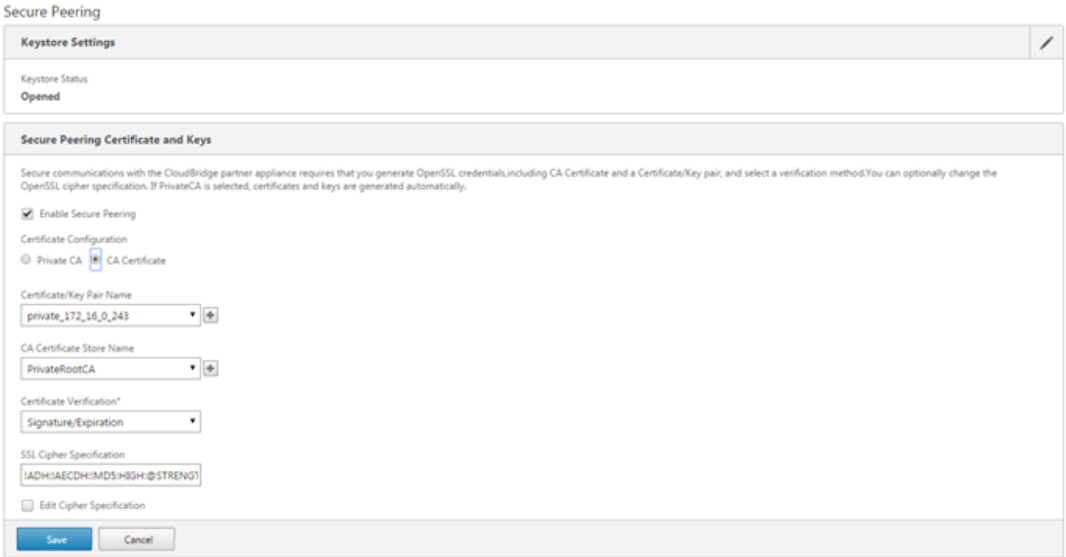
   a) Vaya a **Configuración** > **Aceleración segura** y haga clic en el icono del lápiz en Secure Peering y, a continuación, haga clic en el icono del lápiz en **Certificados y claves de Secure Peering**. Haga clic en **Habilitar configuración de pares seguros y certificados** > **Certificado de CA**. Aparecen los campos de especificación de credenciales.

   b) En **Nombre del par de certificados y claves**, haga clic en el icono **+** y cargue o pegue el par de certificados y claves para este dispositivo. Si las credenciales lo requieren, introduzca también la contraseña clave o la contraseña del archivo. Haga clic en **Crear**.

   c) En **Nombre del almacén de certificados de CA**, haga clic en el icono **+** y cargue o pegue el certificado de CA para este dispositivo.

   d) Mantenga los valores predeterminados para los campos Verificación de certificado y Especificación de cifrado SSL, a menos que su organización requiera lo contrario.

   e) Haga clic en **Guardar**.



8. Repita para el resto de sus dispositivos.
9. Si está utilizando las credenciales que ha proporcionado usted mismo, se ha completado la configuración de pares seguros.
10. Si utiliza credenciales generadas por el dispositivo, realice el procedimiento siguiente.

Para utilizar el peering seguro con credenciales generadas pordispositivos:

1. Utilice el procedimiento Preparar los dispositivos para asegurar el peering, arriba, para preparar sus dispositivos para este procedimiento.

2. En un dispositivo de centro de datos, vaya a **Configuración** > **Aceleración segura** y haga clic en el botón **Habilitar**, si está presente, para habilitar el peering seguro.
3. Haga clic en el icono del lápiz en Secure Peering. El almacén de claves debe estar abierto. Si no lo es, ábrela ahora.
4. Haga clic en el icono del lápiz en **Secure Peering Certificate and Keys**. Haga clic en las opciones **Habilitar pares seguros y CA privada y**, a continuación, haga clic en **Guardar**. Esto generará un certificado de CA autofirmado local y un par de certificados y claves locales.
5. Haga clic en **+** en **Peers conectados**. Introduzca la dirección IP, el nombre de usuario del administrador y la contraseña del administrador de uno de sus dispositivos remotos y haga clic en **Conectar**. Esto emite un certificado de CA y un par de claves de certificado para el dispositivo remoto y lo copia en el dispositivo remoto.

   > **Nota**
   >
   > Para los dispositivos WANOP SD-WAN, la dirección IP podría ser la dirección IP de cualquiera de la interfaz en la que está habilitado el acceso web. Para los dispositivos SD-WAN PE, la dirección IP es la dirección IP de administración.

6. Repita este proceso para los demás dispositivos remotos.
7. En el dispositivo del centro de datos, compruebe la conectividad en **Supervisión** > **Socios y complementos** > **Socios seguros**. Para cada dispositivo remoto, el contenido del campo Secure debe ser True y el Estado de conexión debe ser Connected Available.

CIFS, SMB2 y MAPI

April 23, 2021

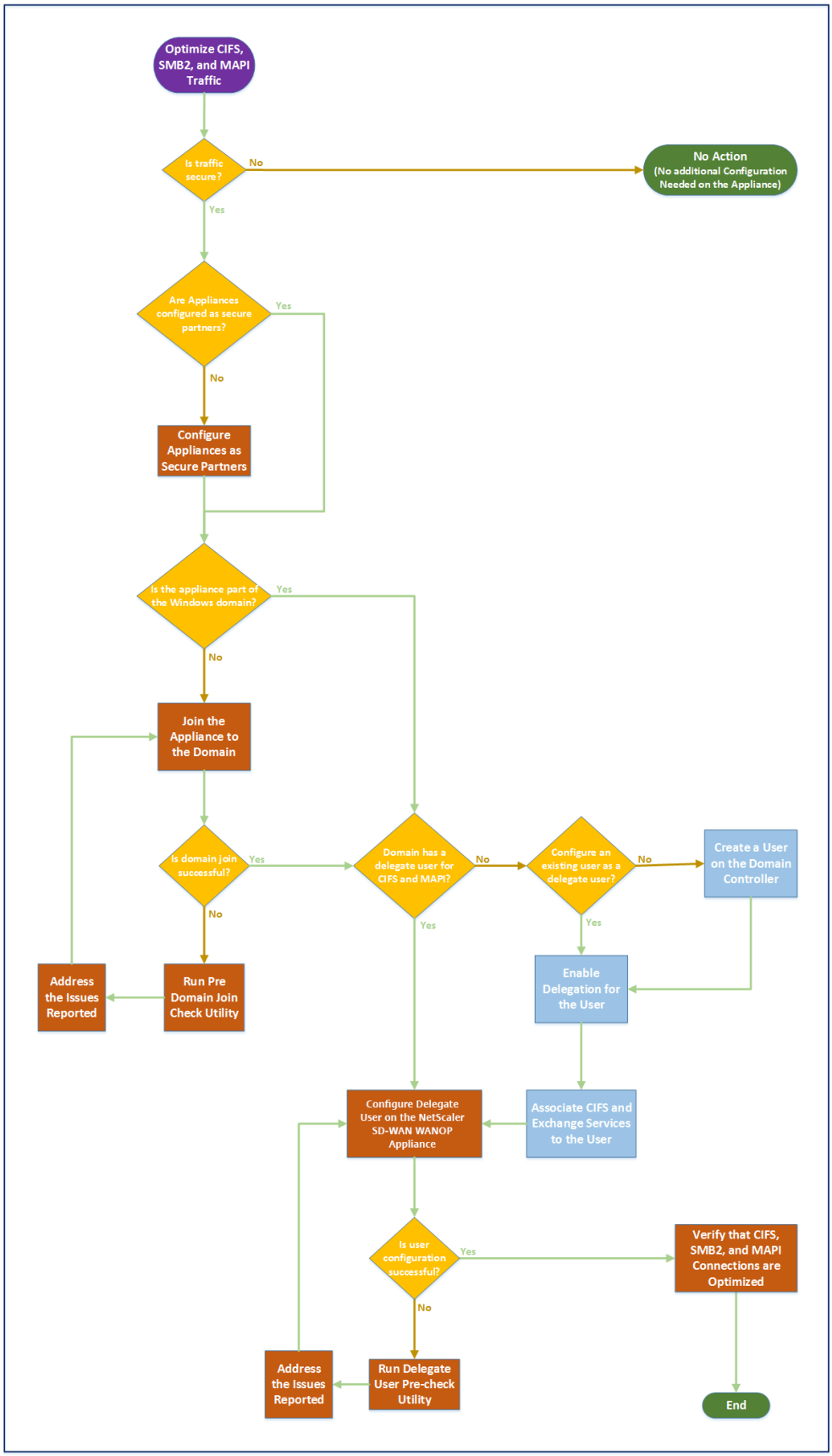
Windows es uno de los sistemas operativos comunes implementados en la red. El sistema operativo Windows admite recursos distribuidos compartidos entre ubicaciones. Por ejemplo, puede hacer que los recursos del centro de datos sean accesibles desde varias sucursales. Para obtener acceso a través de la red, Windows utiliza el protocolo CIFS (Common Internet File System) para acceder a archivos compartidos, y los protocolos MAPI (Messaging Application Programming Interface) para acceder al correo electrónico a través de Microsoft Outlook. Es decir, Windows utiliza el protocolo CIFS para la transferencia de archivos basada en CIFS (Windows y Samba) y la exploración de directorios, y Microsoft Outlook utiliza el protocolo MAPI para acceder a los datos de Outlook.

Puede utilizar un dispositivo Citrix SD-WAN WANOP para optimizar las conexiones CIFS, el bloque de mensajes de servidor versión 2 (SMB2) y MAPI a través de la red.

Además de admitir el sistema operativo Windows, los dispositivos Citrix SD-WAN WANOP admiten CIFS y SMB2 en sistemas de almacenamiento de NetApp e Hitachi.

El siguiente diagrama de flujo muestra el procedimiento completo para configurar un dispositivo Citrix SD-WAN WANOP para optimizar el tráfico CIFS, SMB2 y MAPI.

Configuración de un dispositivo Citrix SD-WAN WANOP para optimizar el tráfico CIFS, SMB2 y MAPI



Configurar el dispositivo Citrix SD-WAN WANOP para optimizar el tráfico seguro de Windows

April 23, 2021

Debe agregar el dispositivo Citrix SD-WAN WANOP a la infraestructura de seguridad de Windows antes de poder optimizar el sistema de archivos firmado de Windows y el tráfico de MAPI Outlook/Exchange cifrado.

Como resultado de las mejoras introducidas en el sistema de seguridad de Windows en las últimas versiones de Windows, los clientes y servidores protegen el tráfico mediante la autenticación y el cifrado de datos. Esto requiere que el dispositivo Citrix SD-WAN WANOP sea un miembro de confianza de la infraestructura de seguridad de Windows antes de poder optimizar el sistema de archivos firmado de Windows y el tráfico de MAPI Outlook/Exchange cifrado.

Después de agregar el dispositivo a la infraestructura de seguridad de Windows, el dispositivo tiene las siguientes capacidades:

- Aceleración del tráfico de servidores de archivos para servidores Microsoft Windows, servidores NetApp y Hitachi HNAS mediante el protocolo SMB firmado y SMB2 firmado.
- Aceleración del tráfico del servidor de Microsoft Exchange cuando los clientes de Outlook acceden a él mediante MAPI o RPC cifrado a través de HTTPS.

Cómo funciona el dispositivo Citrix SD-WAN WANOP en un sistema de seguridad de Windows

Unir el dispositivo a un dominio de Windows requiere credenciales de administrador. Cuando se une al dominio de Windows, el dispositivo se convierte en un miembro de confianza del dominio. Esto permite que el dispositivo se declare miembro de la infraestructura de seguridad del dominio.

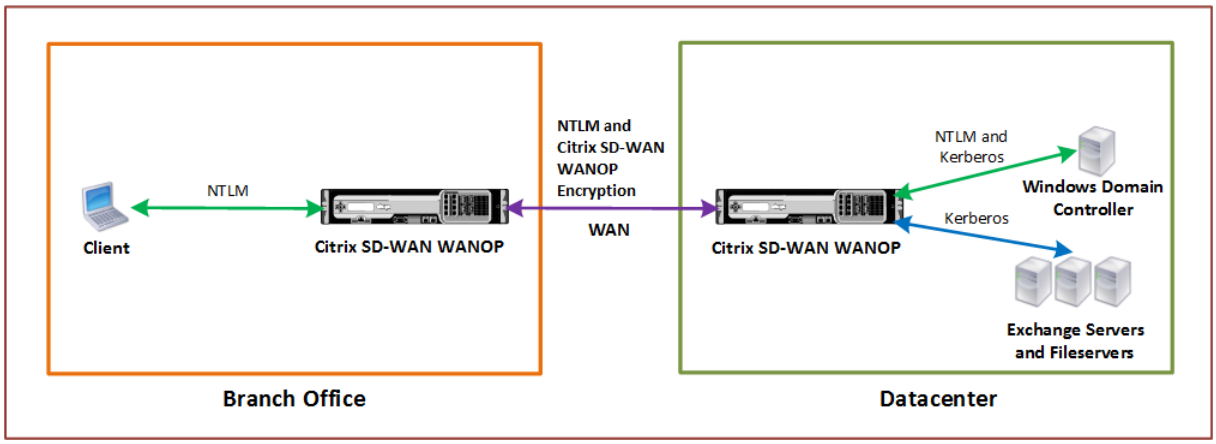
Una vez que el dispositivo se ha convertido en parte de la infraestructura de seguridad de Windows, los usuarios deben autenticarse para poder acceder a los recursos. Para evitar la dificultad de configurar un gran número de usuarios en el dominio, puede delegar la responsabilidad de autenticación en un usuario delegado.

Crear un usuario delegado en el directorio activo. Este usuario es similar a un usuario normal, pero con privilegios especiales. Después de crear el usuario delegado, debe configurarlo en el dispositivo Citrix SD-WAN WANOP. El dispositivo utiliza el usuario delegado para autenticarse en nombre de los usuarios cuando tienen acceso a secuencias de datos autenticadas y cifradas mediante protocolos de Windows, como CIFS y MAPI.

Para acelerar el tráfico CIFS y MAPI, el mecanismo de delegación estándar de Windows permite limitar la delegación de seguridad a los servicios pertinentes. Esta delegación restringida ha estado disponible desde el lanzamiento de Windows Server 2003.

Después de convertirse en parte del dominio, el dispositivo acelera el tráfico seguro de Windows. Un dispositivo de centro de datos que se une a un dominio de Windows debe tener una relación de pares segura con el dispositivo remoto o el complemento WANOP de Citrix SD-WAN, pero sólo el dispositivo del centro de datos se une al dominio de Windows. A efectos de la aceleración CIFS o MAPI, el dispositivo remoto actúa como esclavo del dispositivo del centro de datos, controlándose a través del túnel SSL seguro entre ambos. Por lo tanto, las credenciales de usuario delegado no salen del centro de datos.

La siguiente imagen muestra un diagrama de topología de ejemplo para esta configuración.



En la imagen anterior, un cliente de sucursal accede a los recursos del centro de datos. El cliente de la sucursal, al estar en otro dominio, utiliza la autenticación NTLM como parte del sistema de seguridad de Windows. Al igual que con todas las conexiones aceleradas entre dos dispositivos Citrix SD-WAN WANOP en una relación de pares segura, las conexiones CIFS o MAPI y las autenticaciones NTLM a través de la WAN están cifradas. Según la versión del controlador de dominio de Windows, la solicitud del usuario desde el dispositivo Citrix SD-WAN WANOP del centro de datos se autentica mediante el protocolo de autenticación NTLM o Kerberos. Después de que el dominio autentica al usuario, las solicitudes de acceso posteriores al servidor de Exchange y los servidores de archivos utilizan el protocolo de autenticación Kerberos. El dispositivo Citrix SD-WAN WANOP optimiza las conexiones establecidas entre el cliente y el servidor.

Si los dispositivos no tienen una relación de pares segura o si el dispositivo del centro de datos no se ha unido correctamente al dominio, las conexiones utilizan la aceleración de control de flujo TCP, que no realiza operaciones de seguridad, compresión ni transformaciones de datos. Las conexiones entre el cliente y el servidor se establecen como si los dispositivos Citrix SD-WAN WANOP no estuvieran allí.

Puede configurar diferentes modos de autenticación de cliente en sistemas operativos Windows. Los

tipos de conexiones que optimiza el dispositivo Citrix SD-WAN WANOP dependen del modo de autenticación de cliente que configure.

En la tabla siguiente se enumeran los modos de autenticación de cliente de Windows en Windows y las optimizaciones WANOP de Citrix SD-WAN correspondientes.

Autenticación y optimización compatibles con el sistema operativo Windows

Sistema operativo cliente	Modo de autenticación de cliente	Optimización	Comentarios
Windows XP/Windows Vista/Windows 7/Windows 8	Autenticación de negociación (SPNEGO)	Aceleración de control de flujo TCP, compresión, aceleración del protocolo CIFS	Configuración predeterminada utilizada para todas las versiones de Windows.
Windows XP/Windows Vista/Windows7/Windows 8	Solo NTLM o solo Kerberos	Aceleración de control de flujo TCP solamente	Modos de autenticación no predeterminados

Nota: Si utiliza los modos de autenticación de cliente sólo NTLM o sólo Kerberos, el tráfico no se acelera si está cifrado.

Requisitos para agregar un dispositivo Citrix SD-WAN WANOP al sistema de seguridad de Windows

Para optimizar el tráfico para SMB firmado por Windows y tráfico MAPI cifrado, la implementación de Citrix SD-WAN WANOP debe cumplir los siguientes requisitos antes de agregar el dispositivo a la infraestructura de seguridad de Windows:

- Tanto los dispositivos de aceleración del lado del cliente como del lado del servidor deben haber establecido una relación de pares segura.
- Los dispositivos deben utilizar un servidor NTP que esté estrechamente sincronizado con la hora en el servidor de dominio de Windows. Idealmente, los dispositivos y el servidor de dominio de Windows son todos clientes del mismo servidor NTP.
- Outlook **no debe** configurarse para la opción solo **Kerberos** (no predeterminada) o **solo NTLM**. La opción predeterminada (negociada) es necesaria para la aceleración.
- El cliente y el servidor pueden ser miembros de cualquier dominio que tenga confianza bidireccional con el dominio del dispositivo del servidor. No se admite la confianza unidireccional.

- Se debe configurar un usuario delegado de Kerberos en el Controller de dominio, para que lo utilice el dispositivo que participa en la infraestructura de seguridad del dominio.
- Las direcciones IP del servidor DNS para el dominio deben configurarse y alcanzarse en el dispositivo del servidor.
- Los servidores de dominio deben ser totalmente accesibles, con búsquedas tanto hacia adelante como hacia atrás para todas las direcciones IP de los controladores de dominio configurados en los servidores DNS.
- El nombre de host del dispositivo Citrix SD-WAN WANOP del lado del servidor debe ser único. Es probable que el uso del nombre de host predeterminado de hostname cause problemas.

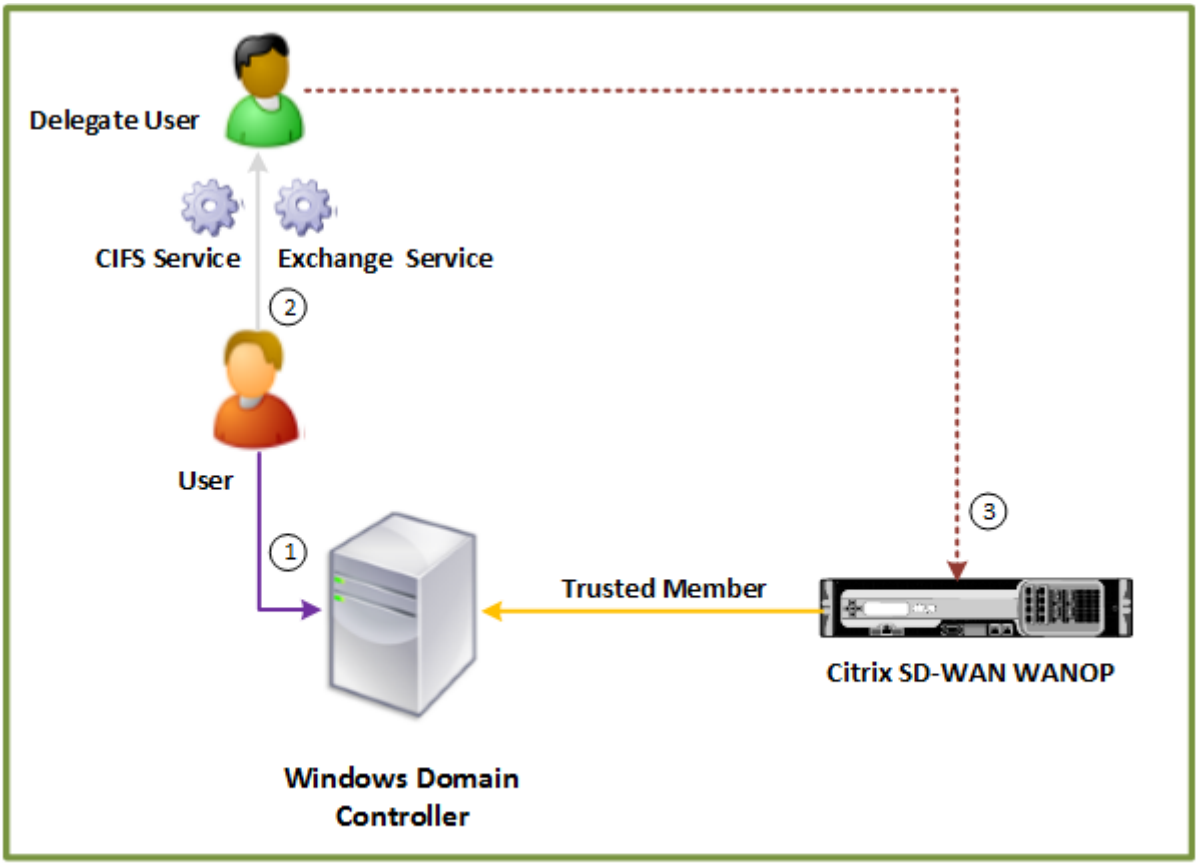
> **Nota**
>
> El cliente Macintosh Outlook no utiliza el estándar MAPI (Outlook/Exchange) y esta función no acelera.

Agregar un dispositivo Citrix SD-WAN WANOP a la infraestructura de seguridad de Windows

Para optimizar el tráfico seguro de Windows, el dispositivo Citrix SD-WAN WANOP debe formar parte del sistema de seguridad de Windows y debe autenticarse con el sistema de seguridad o dominio. Como se muestra en la imagen siguiente, para que el dispositivo forme parte del sistema de seguridad de Windows, debe hacer que el dispositivo se una a un dominio (mediante credenciales administrativas). Además, debe configurar un usuario nuevo o existente como usuario delegado asociando los servicios CIFS y Exchange con ese usuario. A continuación, debe configurar este usuario delegado en el dispositivo Citrix SD-WAN WANOP.

Puede utilizar la utilidad **Comprobación previa del dominio** para averiguar si hay algún problema al unir el dispositivo a un dominio.

> **Nota**
>
> El sistema de seguridad de Windows utiliza el servicio de Exchange para administrar las conexiones MAPI. Configuración de la instalación para optimizar el tráfico seguro de Windows



Únete a un dispositivo Citrix SD-WAN WANOP al dominio Windows:

Cuando el dispositivo se une al dominio, intercambia un secreto compartido con el Controller de dominio, lo que permite que el dispositivo permanezca parte del dominio indefinidamente. Al unir un dispositivo a un dominio, asegúrese de que dispone de credenciales de administrador para el Controller de dominio.

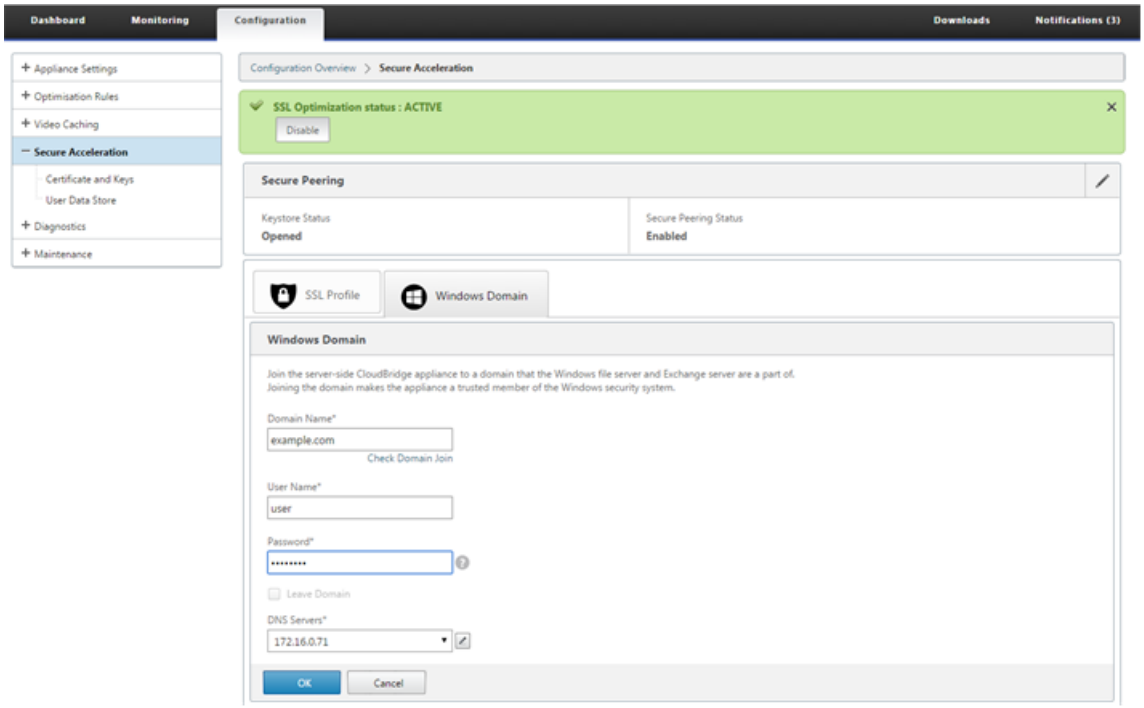
Para asegurarse de que el dispositivo Citrix SD-WAN WANOP optimiza el tráfico CIFS y MAPI (incluido el tráfico encapsulado como RPC a través de HTTPS), debe hacer que el dispositivo forme parte del dominio del que forman parte el servidor de archivos de Windows y el servidor Exchange. Debe unir el dispositivo del lado del servidor al dominio.

Nota: Las credenciales de administración del dominio no se guardan en el dispositivo.

Para unir un dispositivo Citrix SD-WAN WANOP a un dominio de Windows:

1. Vaya a la ficha **Configuración** > **Aceleración segura** > **Dominio de Windows**.
2. Haga clic en **Unirse al dominio de Windows**.
3. Escriba el nombre de dominio de Windows en el campo Nombre de dominio.

4. En el campo Nombre de usuario, escriba el nombre de usuario del administrador del Controller de dominio.
5. En el campo Contraseña, especifique la contraseña del administrador del Controller de dominio.
6. Si es necesario, modifique los servidores DNS para obtener coherencia con el dominio de Windows.
7. Haga clic en **OK**.
8. En la sección Delegar usuarios, agregue un usuario delegado, como se describe en los procedimientos siguientes.



Configurar un usuario delegado:

Después de unir el dispositivo a un dominio de Windows, debe crear un usuario que el dispositivo pueda utilizar para autenticar usuarios con el dominio. Este usuario se conoce como *usuario delegado*.

Nota: Para crear una cuenta de usuario delegado, necesita acceso de administrador al Controller de dominio de Windows y al dispositivo. Si no tiene acceso de administrador al Controller de dominio de Windows, asegúrese de que un administrador autorizado realiza las tareas necesarias en el Controller de dominio.

La configuración de la autenticación de usuarios mediante la delegación de Kerberos implica dos tareas: configurar un usuario delegado en el controlador de dominio y, a continuación, agregar este usuario al dispositivo Citrix SD-WAN WANOP.

Configurar un usuario delegado en un Controller de dominio:

Antes de configurar un usuario delegado en un dispositivo Citrix SD-WAN WANOP, debe configurar un usuario delegado con las propiedades necesarias en el controlador de dominio. Puede crear una cuenta de usuario delegado o utilizar una cuenta de usuario existente como cuenta de usuario delegado.

Después de crear una cuenta o seleccionar una cuenta existente, habilite la delegación para este usuario. A continuación, asociará el usuario delegado con los servicios CIFS y Exchange, de modo que el tráfico de estos servicios se pueda acelerar. Después de agregar este usuario al dispositivo Citrix SD-WAN WANOP, el dispositivo presenta credenciales delegadas para los servicios asociados a esta cuenta.

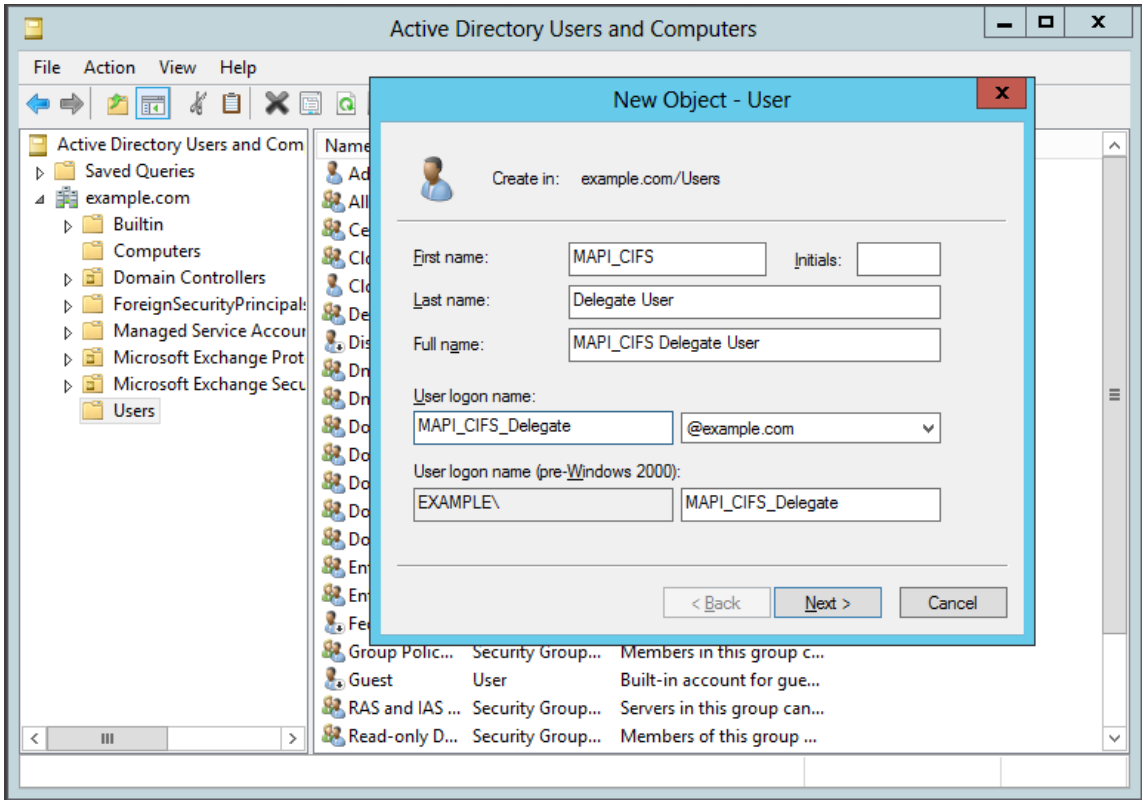
Crear una cuenta de usuario delegado:

Cree una cuenta de usuario delegado en el controlador de dominio de Windows para que el dispositivo Citrix SD-WAN WANOP pueda utilizar esta cuenta en nombre de los usuarios para autenticarlos con el controlador de dominio.

Nota: Si desea configurar un usuario existente como usuario delegado, omita este procedimiento.

Para crear una cuenta de usuario delegado:

1. Inicie sesión en el Controller de dominio de Windows como administrador. Asegúrese de que el servidor de archivos o el servidor de Exchange es miembro de este dominio.
2. En el menú **Inicio**, abra la ventana **Usuarios y equipos de Active Directory**.
3. Cree un usuario delegado, como se muestra en la siguiente captura de pantalla:

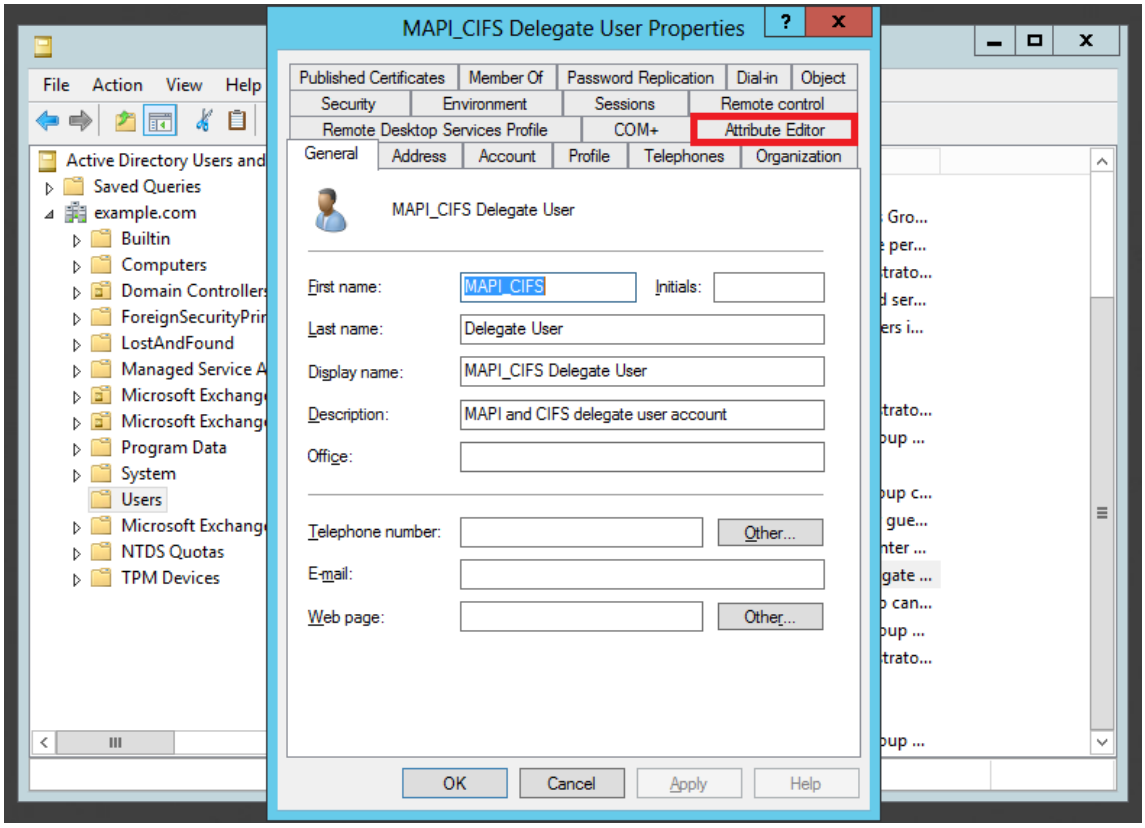


Habilitar delegación para un usuario:

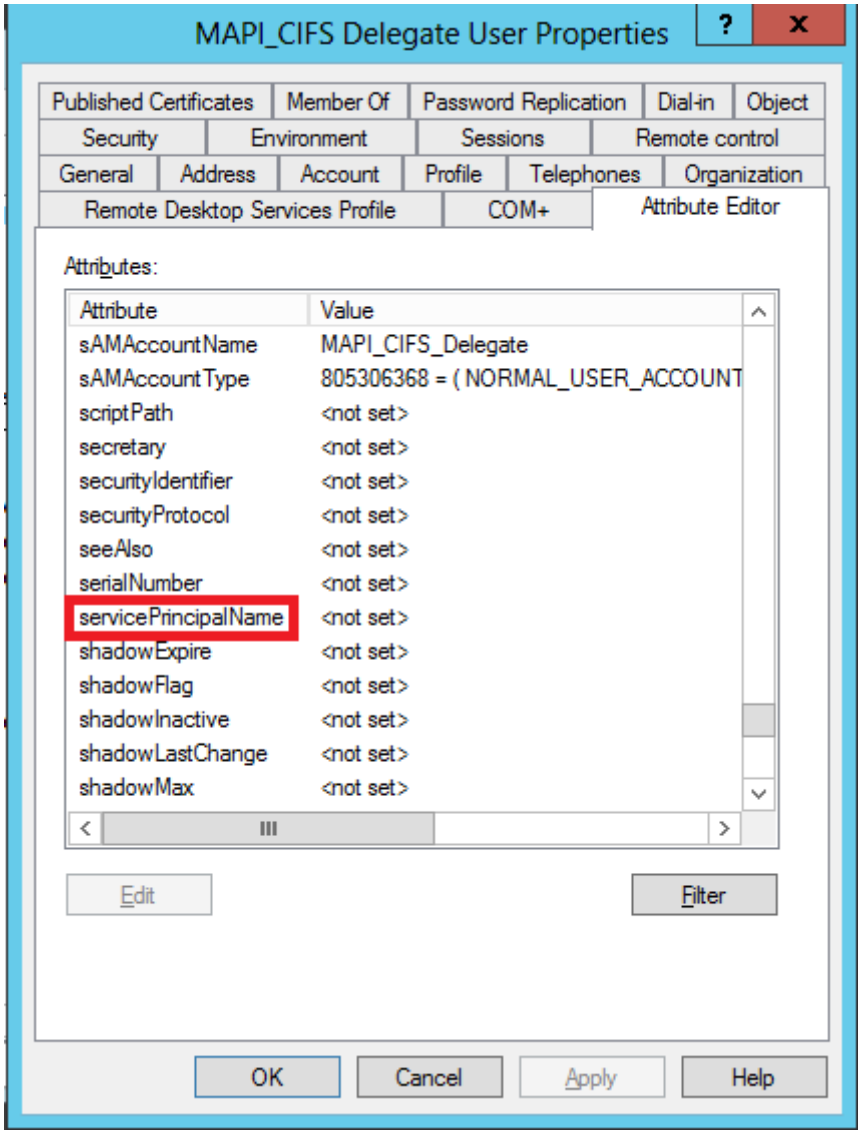
Hasta ahora, el usuario que ha creado es similar a cualquier usuario que cree en el servidor de Active Directory. Para habilitar la delegación para el usuario, debe establecer el atributo Nombre principal de servicio del usuario para *delegar* y asociar el usuario delegado con los servicios necesarios. Esto hace que el usuario tenga privilegios especiales asociados y lo convierta en un usuario delegado.

Para habilitar la delegación para el usuario:

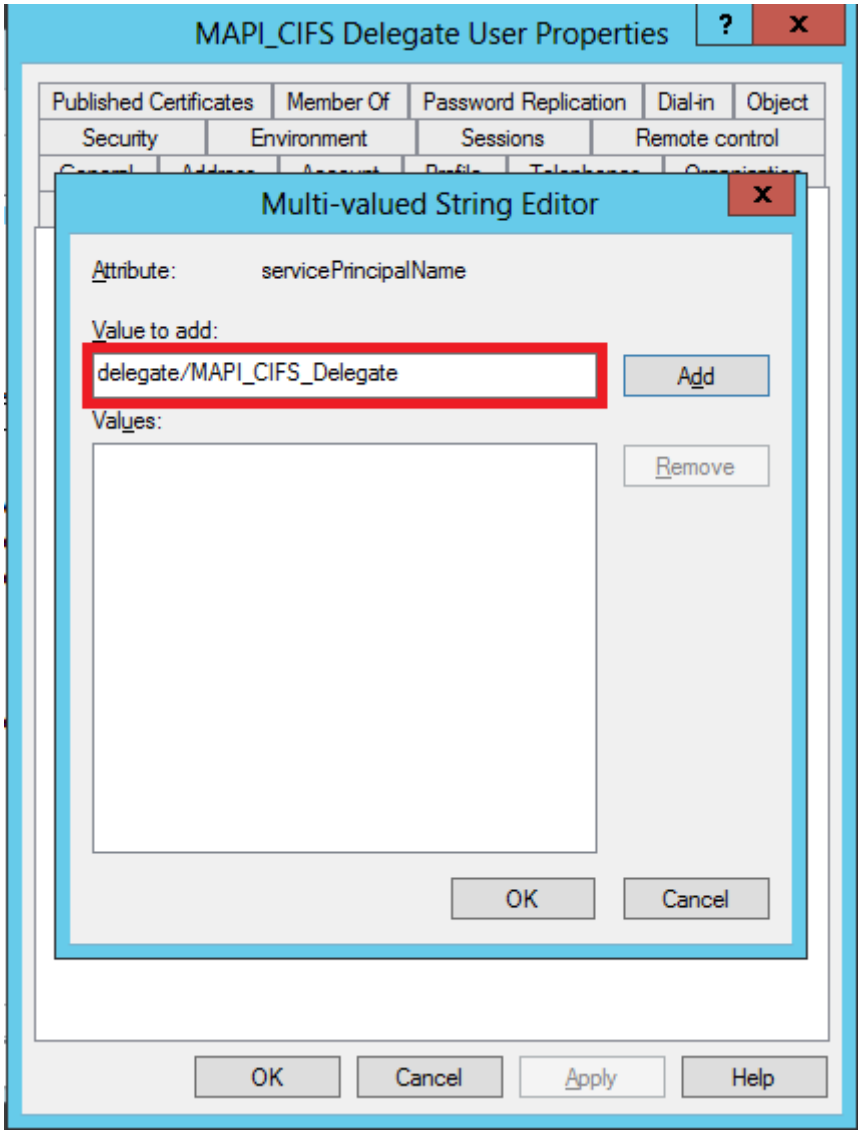
1. En el menú **Inicio**, abra la ventana **Usuarios y equipos de Active Directory**.
2. En el menú Ver, seleccione **Funciones avanzadas**.
3. Seleccione el nodo **Usuario**.
4. Haga clic con el botón secundario del mouse (ratón) en el usuario que desea convertir en usuario delegado.
5. En el menú contextual, seleccione **Propiedades** y vaya a la ficha **Editor de atributos**, como se muestra en la siguiente captura de pantalla:



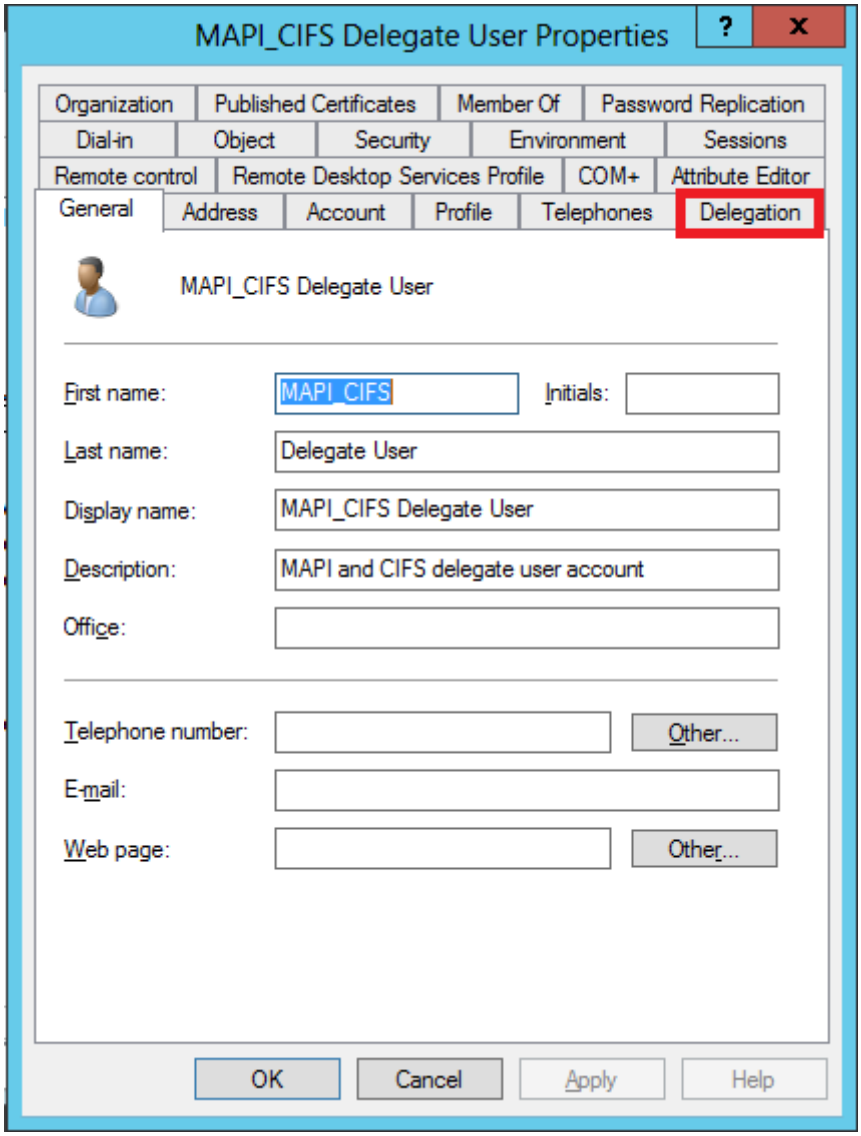
6. En la lista **Atributos**, seleccione **ServicePrincipalName**, como se muestra en la siguiente captura de pantalla:



7. Haga clic en **Edit**.
8. En el cuadro de diálogo **Editor de cadenas de valores múltiples**, en el campo **Valor a agregar**, especifique **delegate/*<User_Name>***, como se muestra en la siguiente captura de pantalla:



9. Haga clic en **Agregar**.
10. Haga clic en **OK**.
11. Haga clic en **Aplicar**.
12. Haga clic en **OK**.
13. Abra el cuadro de diálogo **Propiedades de usuario delegado MAPI-CIFS** del usuario y compruebe que se ha agregado la ficha **Delegación** al cuadro de diálogo, como se muestra en la siguiente captura de pantalla:



Asocie el usuario delegado a CIFS y Servicios de Exchange:

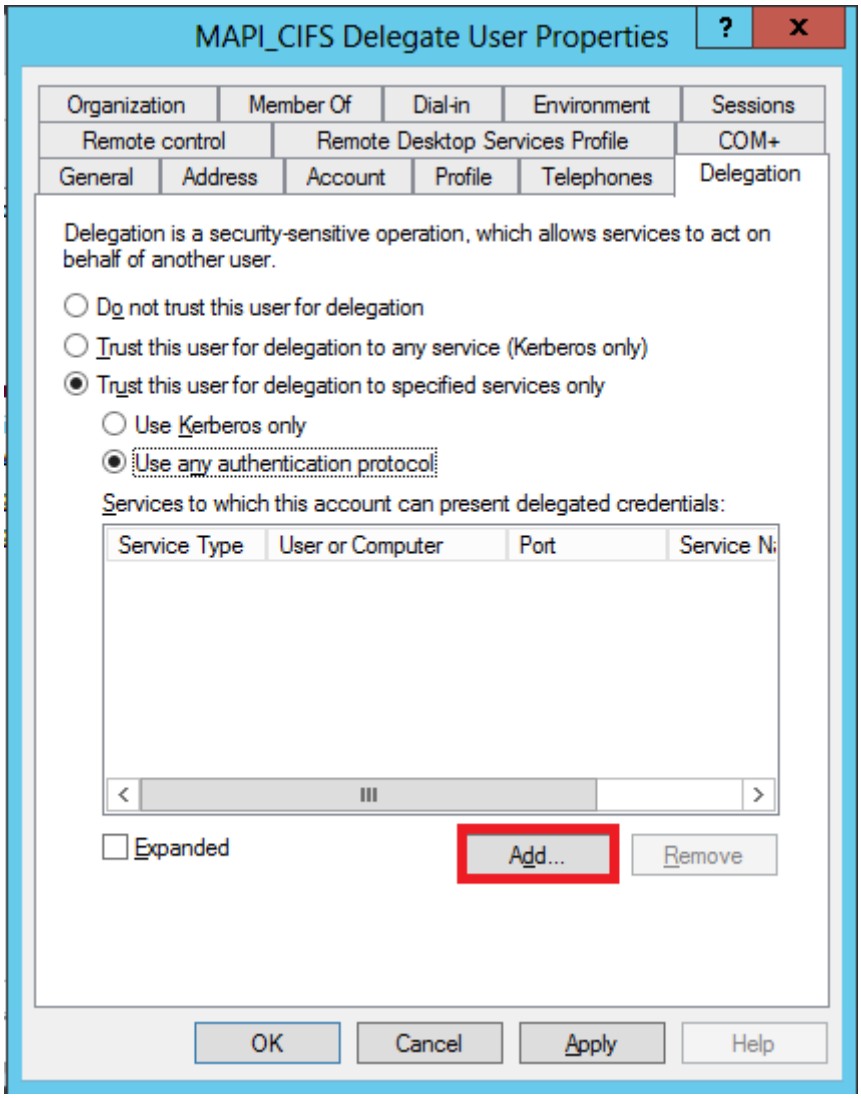
Después de habilitar la ficha Delegación para el usuario, puede asociar el usuario con servicios para los que el usuario puede presentar credenciales delegadas. Cuando agrega este usuario al dispositivo Citrix SD-WAN WANOP, el dispositivo presenta credenciales delegadas para los servicios asociados a esta cuenta.

Nota: La infraestructura de seguridad de Windows utiliza el servicio Exchange para administrar el tráfico MAPI.

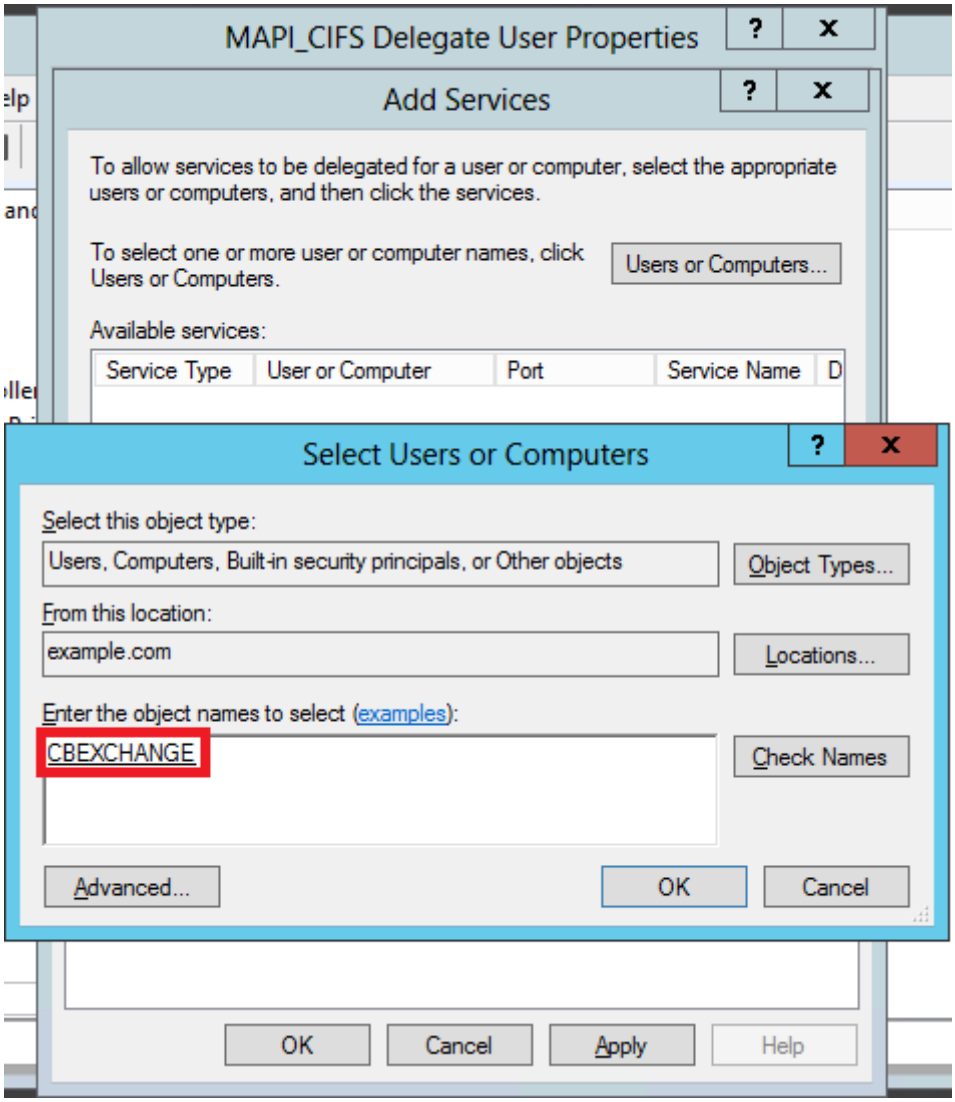
Para asociar el usuario delegado a los servicios CIFS y Exchange:

1. En la ficha Delegación, seleccione la opción **Confiar en este usuario solo para la delegación a servicios específicos**.
2. Seleccione la opción **Usar cualquier protocolo de autenticación**.

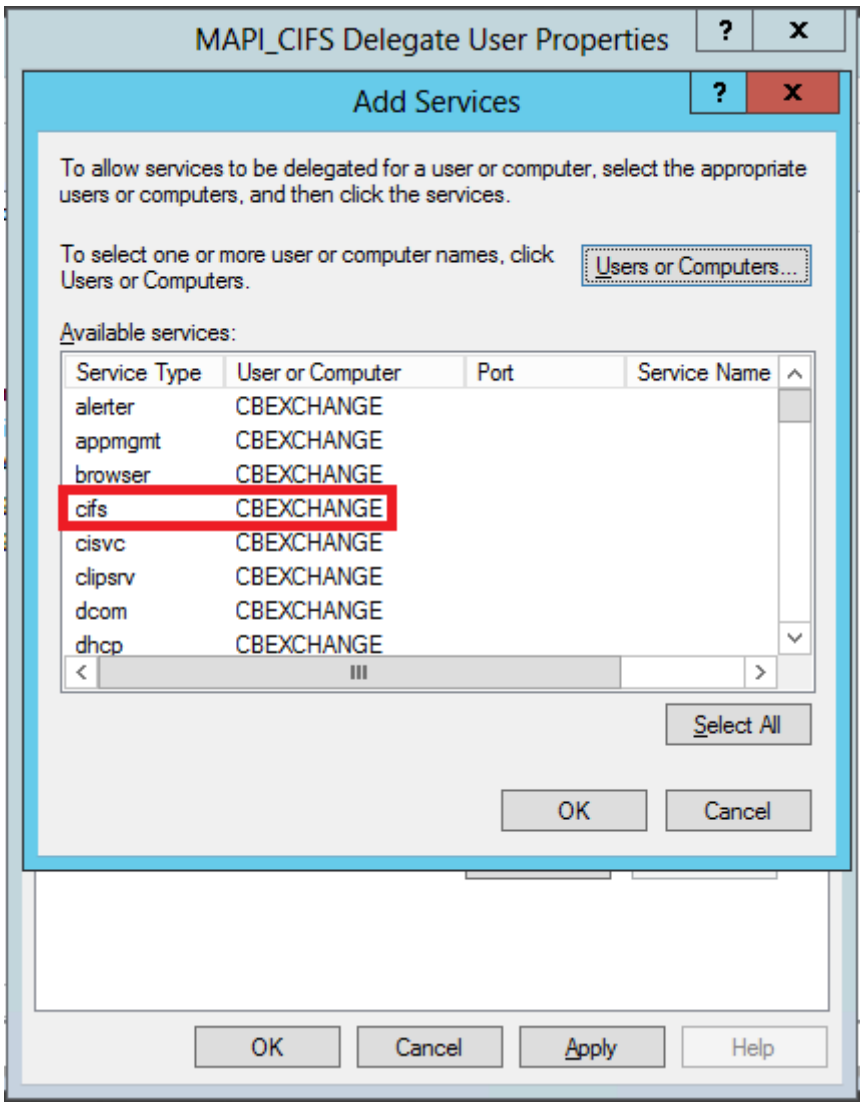
3. Haga clic en **Agregar**, como se muestra en la siguiente captura de pantalla:



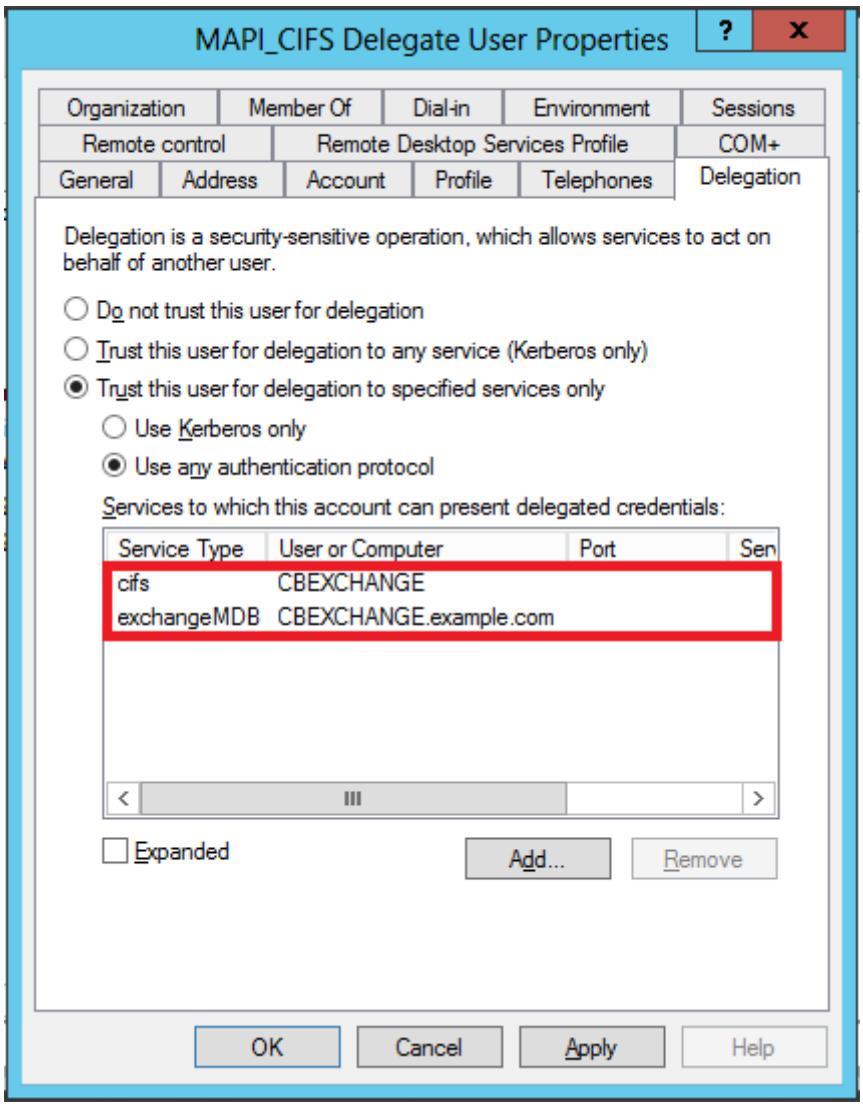
4. En el cuadro de diálogo **Agregar servicio**, haga clic en **Usuarios y equipos**.
5. En el cuadro de diálogo **Seleccionar usuarios o equipos**, agregue el equipo local que se va a seleccionar, como se muestra en la siguiente captura de pantalla:



6. Haga clic en **OK**.
7. En el cuadro de diálogo Agregar servicios, en la lista **Servicios disponibles**, seleccione **cifs**, como se muestra en la siguiente captura de pantalla:



8. Si tiene que configurar la aceleración MAPI en el dispositivo Citrix SD-WAN WANOP, mantenga presionada la **tecla Ctrl** y seleccione el servicio **ExchangeDB**.
9. Haga clic en **OK**. Los servicios que ha seleccionado se agregan a la lista **Servicios en los que esta cuenta puede presentar credenciales delegadas**, como se muestra en la siguiente captura de pantalla:



10. Haga clic en **Aceptar**.
11. Cierre la ventana **Usuarios y equipos de Active Directory**.

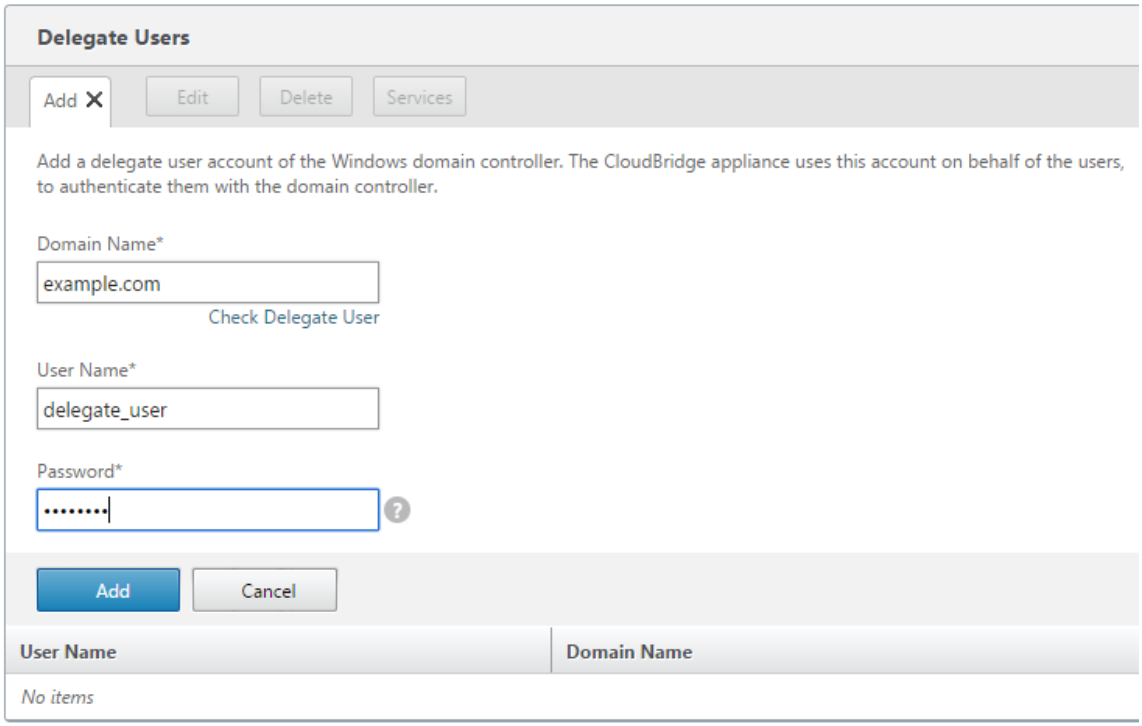
Configure un usuario delegado en un dispositivo Citrix SD-WAN WANOP:

Después de configurar el usuario delegado en el servidor de Active Directory, debe configurarlo en el dispositivo Citrix SD-WAN WANOP, de modo que el dispositivo pueda presentar las credenciales delegadas de este usuario en el dominio. Esto permite al dispositivo optimizar activamente el tráfico de red para las funciones avanzadas de aceleración CIFS y MAPI.

Para agregar el usuario delegado al dispositivo del servidor:

1. Vaya a la ficha **Configuración**> **Aceleración segura**> **Dominio de Windows** .
2. Haga clic en el botón **Unirse al dominio de Windows**, si está presente.
3. En **Delegar usuarios**, haga clic en **Agregar**.

4. En el campo **Nombre de dominio**, especifique el nombre de dominio. Normalmente es el dominio que especificó en la sección **Dominio de Windows**.
5. En el campo **Nombre de usuario**, escriba el nombre de usuario del usuario delegado.
6. En el campo **Contraseña**, especifique la contraseña del usuario delegado.
7. Haga clic en **Agregar**.



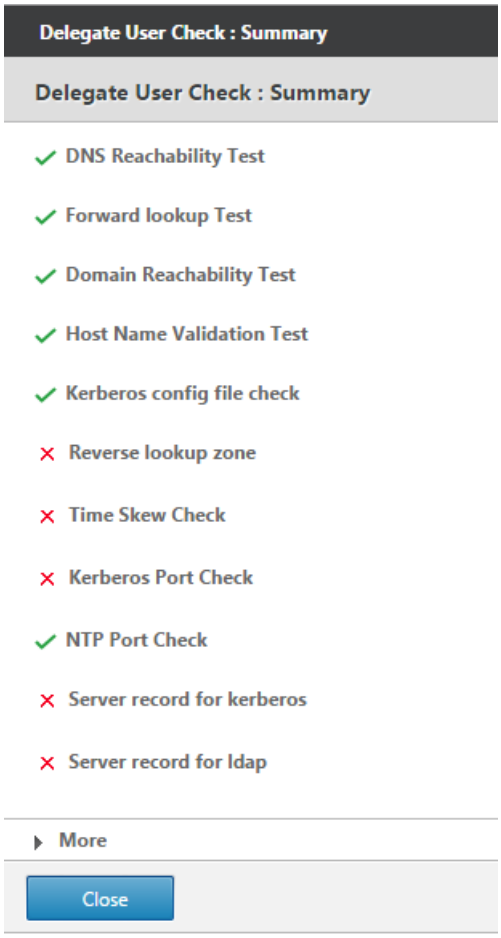
Compruebe que el dispositivo se ha unido al dominio

Si, después de agregar el dispositivo al dominio, observa que el dispositivo no está optimizando el tráfico seguro de Windows, es posible que algún error haya impedido que el dispositivo se una al dominio. Puede utilizar la utilidad **Comprobación previa del dominio** para averiguar si hay algún problema con el dispositivo que se une al dominio. Incluso puede ejecutar esta utilidad para identificar posibles problemas antes de intentar unir el dispositivo a un dominio.

Para comprobar el usuario delegado:

1. Inicie sesión en el dispositivo Citrix SD-WAN WANOP del lado del servidor.
2. Vaya a **Configuración** > **Aceleración segura** > ficha **Windows**.
3. Haga clic en el botón **Unirse al dominio de Windows**, si está presente.
4. Seleccione un usuario delegado y haga clic en **Modificar**.
5. Haga clic en **Comprobar usuario delegado**.

6. Espere a que finalice la comprobación de dominio de usuario delegado y examine los resultados.



Configurar CIFS y aceleración SMB2/SMB3

April 23, 2021

La función de aceleración CIFS proporciona un conjunto de mejoras de rendimiento específicas del protocolo para la transferencia de archivos basada en CIFS (Windows y Samba) y la exploración de directorios, incluidas mejoras en el transporte CIFS y protocolos relacionados como DCERPC.

La aceleración CIFS consta de tres partes:

- Aceleración de control de flujo TCP: esto se realiza en todas las conexiones CIFS aceleradas, independientemente de la versión del protocolo (SMB1, SMB2 o SMB3) o del grado de autenticación y cifrado.

- Aceleración del protocolo CIFS: estas optimizaciones aumentan el rendimiento de CIFS al reducir el número de viajes de ida y vuelta necesarios para ejecutar un comando CIFS. Estas optimizaciones se realizan automáticamente en conexiones CIFS SMB1 y SMB2 que no utilizan autenticación de paquetes CIFS (firma) o donde se utiliza la firma y los dispositivos se han unido al dominio de Windows en una función de delegado de seguridad.
- Compresión CIFS: las conexiones CIFS se comprimen automáticamente siempre que cumplen los requisitos para la aceleración del protocolo CIFS. Además, las conexiones SMB3 se comprimen cuando no se firman y no se sellan.

En las redes en las que la firma CIFS está habilitada, la aceleración y compresión del protocolo CIFS requieren que deshabilite la autenticación de paquetes CIFS (firma) o que los dispositivos del centro de datos se unan al dominio de Windows y cree una relación de pares segura entre los dispositivos del centro de datos y los dispositivos remotos y los complementos WANOP de Citrix SD-WAN.

Cuadro 1 Funciones de aceleración CIFS, según la versión del protocolo SMB y si el dispositivo se ha unido al dominio de Windows.

Versión SMB	Control de flujo TCP	Compresión	Aceleración de protocolos
		Firma inhabilitada	
SMB 1.0	S	S	S
SMB 2.0	S	S	S
SMB 2.1	S	S	N
SMB 3.0	S	S	N
		*Firma habilitada, Citrix SD-WAN WANOP se ha unido al dominio **	
SMB 1.0	S	S	S
SMB 2.0	S	S	S
SMB 2.1	S	S	S
SMB 3.0	S	S	Y *
		Firma habilitada, Citrix SD-WAN WANOP no se ha unido al dominio	
SMB 1.0	S	N	N
SMB 2.0	S	N	N

Versión SMB	Control de flujo TCP	Compresión	Aceleración de protocolos
SMB 2.1	S	N	N
SMB 3.0	S	N	N

* SMB 3.0 Support fue agregado en la versión 7.4.2.

** Citrix SD-WAN WANOP no admite la autenticación NTLMv2 (predeterminada para Windows 7) con SMB 1/ SMB 2/SMB 3 y con el servidor NetApp. Habilitar la autenticación Kerberos permite la aceleración.

Tabla 2. La versión del protocolo SMB, por cliente y sistema operativo.

Sistema operativo cliente/servidor	Windows 8, Windows 10 o Windows Server 2012	Windows 7 o Windows Server 2008 R2	Windows Vista o Windows Server 2008	Versiones anteriores de Windows
Windows 8, Windows 10 o Windows Server 2012	SMB 3,0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 o Windows Server 2008 R2	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista o Windows Server 2008	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
Versiones anteriores de Windows	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

Versiones compatibles de CIFS:

No todas las implementaciones de CIFS utilizan patrones de solicitud reconocidos por el dispositivo. Estas versiones no admitidas no logran aceleración en toda la gama de casos, como se muestra en la siguiente tabla.

Tabla 3.Soporte WANOP de Citrix SD-WAN para servidores y clientes CIFS.

Producto	Servidor	Cliente
Windows Server 2003-2012	Sí*	Sí*
Windows XP, Vista, 7, 8, 2000	Sí*	Sí*
NetApp	Sí**	N/D
Hitachi	Sí**	N/D
Windows NT	Sí	No
Windows ME y versiones anteriores	No	No
Otros	Ver Nota	Ver Nota

* El soporte para SMB 3.0 se introdujo en la versión 7.4.2.

** El funcionamiento con SMB 3.0 no se ha probado a partir de la versión 7.4.2.

> **Nota**: La mayoría de las implementaciones CIFS de terceros emulan uno de los servidores o clientes enumerados anteriormente. En la medida en que la emulación tenga éxito, el tráfico se acelera, o no, como se muestra en la tabla anterior. Si la emulación se comporta de manera diferente de lo que espera el acelerador CIFS, la aceleración CIFS finaliza para esa conexión.

El comportamiento de la aceleración CIFS con una implementación CIFS determinada no se puede conocer con certeza hasta que se haya probado.

Los modos de aceleración CIFS son:

- Lecturas y escrituras de archivos grandes
- Lectura y escritura de archivos pequeños
- Exploración de directorios.

Lecturas y escrituras de archivos grandes: estas optimizaciones SMB1 son para transferencias de archivos de al menos 640 KB. Las técnicas seguras de lectura anticipada y escritura detrás se utilizan para transmitir los datos sin pausas para cada transferencia (una transferencia es de 64 KB o menos).

Estas optimizaciones solo se activan si la transferencia tiene un bloqueo BATCH o EXCLUSIVO y es simple. Las copias de archivos siempre son simples. Los archivos abiertos a través de aplicaciones pueden o no serlo, dependiendo de cómo se manejen dentro de la aplicación.

Las relaciones de velocidad de 10x se pueden obtener fácilmente con la aceleración CIFS, siempre que el enlace y los discos sean lo suficientemente rápidos como para acomodar diez veces las velocidades de transferencia actuales. Se puede obtener velocidad de 50x si es necesario, pero normalmente no

está habilitado, debido al consumo de memoria. Póngase en contacto con su representante de Citrix si 10x no es suficiente.

Lecturas y escrituras de archivos pequeños: las mejoras de archivos pequeños se centran más en las optimizaciones de metadatos (directorio) que en la transmisión de datos. CIFS nativo no combina solicitudes de metadatos de una manera eficiente. La aceleración CIFS sí. Al igual que con la aceleración de archivos grandes, estas optimizaciones no se realizan a menos que sean seguras (por ejemplo, no se realizan si al cliente CIFS no se le concedió un bloqueo exclusivo en el directorio). Cuando se utiliza el protocolo SMB2, los metadatos de los archivos se almacenan en caché localmente para mejorar aún más.

Exploración de directorios: los clientes CIFS estándar realizan la exploración de directorios de una manera extremadamente ineficiente, lo que requiere un gran número de viajes de ida y vuelta para abrir una carpeta remota. La aceleración CIFS reduce el número de viajes de ida y vuelta a 2 o 3. Cuando se utiliza el protocolo SMB2, los datos del directorio se almacenan en caché localmente para mejorar aún más.

Aceleración del protocolo CIFS

La aceleración CIFS es compatible con todos los modelos. CIFS es un protocolo basado en TCP y se beneficia del control de flujo. Sin embargo, el CIFS se implementa de una manera altamente ineficiente en las redes de larga distancia, lo que requiere un número excesivo de viajes de ida y vuelta para completar una operación. Dado que el protocolo es muy sensible a la latencia de enlace, la aceleración completa debe ser compatible con el protocolo.

La aceleración CIFS reduce el número de viajes de ida y vuelta a través de una variedad de técnicas. Se analiza el patrón de solicitudes del cliente y se pronostica su siguiente acción. En muchos casos, es seguro actuar sobre la predicción incluso si es incorrecta, y estas operaciones seguras son la base de muchas optimizaciones.

Por ejemplo, los clientes SMB1 emiten lecturas secuenciales de archivos de manera no solapada, esperando que se complete cada lectura de 64 KB antes de emitir la siguiente. Mediante la implementación de lectura anticipada, el dispositivo puede ofrecer una aceleración de hasta 10 veces de forma segura mediante la obtención de los datos anticipados por adelantado.

Las técnicas adicionales aceleran la exploración de directorios y las operaciones de archivos pequeños. La aceleración se aplica no solo a las operaciones CIFS, sino también a las operaciones RPC relacionadas.

Requisitos previos

La aceleración CIFS es compatible con todos los modelos. CIFS es un protocolo basado en TCP y se beneficia del control de flujo. Sin embargo, el CIFS se implementa de una manera altamente inefi-

ciente en las redes de larga distancia, lo que requiere un número excesivo de viajes de ida y vuelta para completar una operación. Dado que el protocolo es muy sensible a la latencia de enlace, la aceleración completa debe ser compatible con el protocolo.

La aceleración CIFS reduce el número de viajes de ida y vuelta a través de una variedad de técnicas. Se analiza el patrón de solicitudes del cliente y se pronostica su siguiente acción. En muchos casos, es seguro actuar sobre la predicción incluso si es incorrecta, y estas operaciones seguras son la base de muchas optimizaciones.

Por ejemplo, los clientes SMB1 emiten lecturas secuenciales de archivos de manera no solapada, esperando que se complete cada lectura de 64 KB antes de emitir la siguiente. Mediante la implementación de lectura anticipada, el dispositivo puede ofrecer una aceleración de hasta 10 veces de forma segura mediante la obtención de los datos anticipados por adelantado.

Las técnicas adicionales aceleran la exploración de directorios y las operaciones de archivos pequeños. La aceleración se aplica no solo a las operaciones CIFS, sino también a las operaciones RPC relacionadas.

Si la red utiliza la firma CIFS, el dispositivo debe ser un miembro de confianza del dominio. Para convertir el dispositivo en un miembro de confianza del dominio, consulte Agregar un dispositivo Citrix SD-WAN WANOP a la infraestructura de seguridad de Windows.

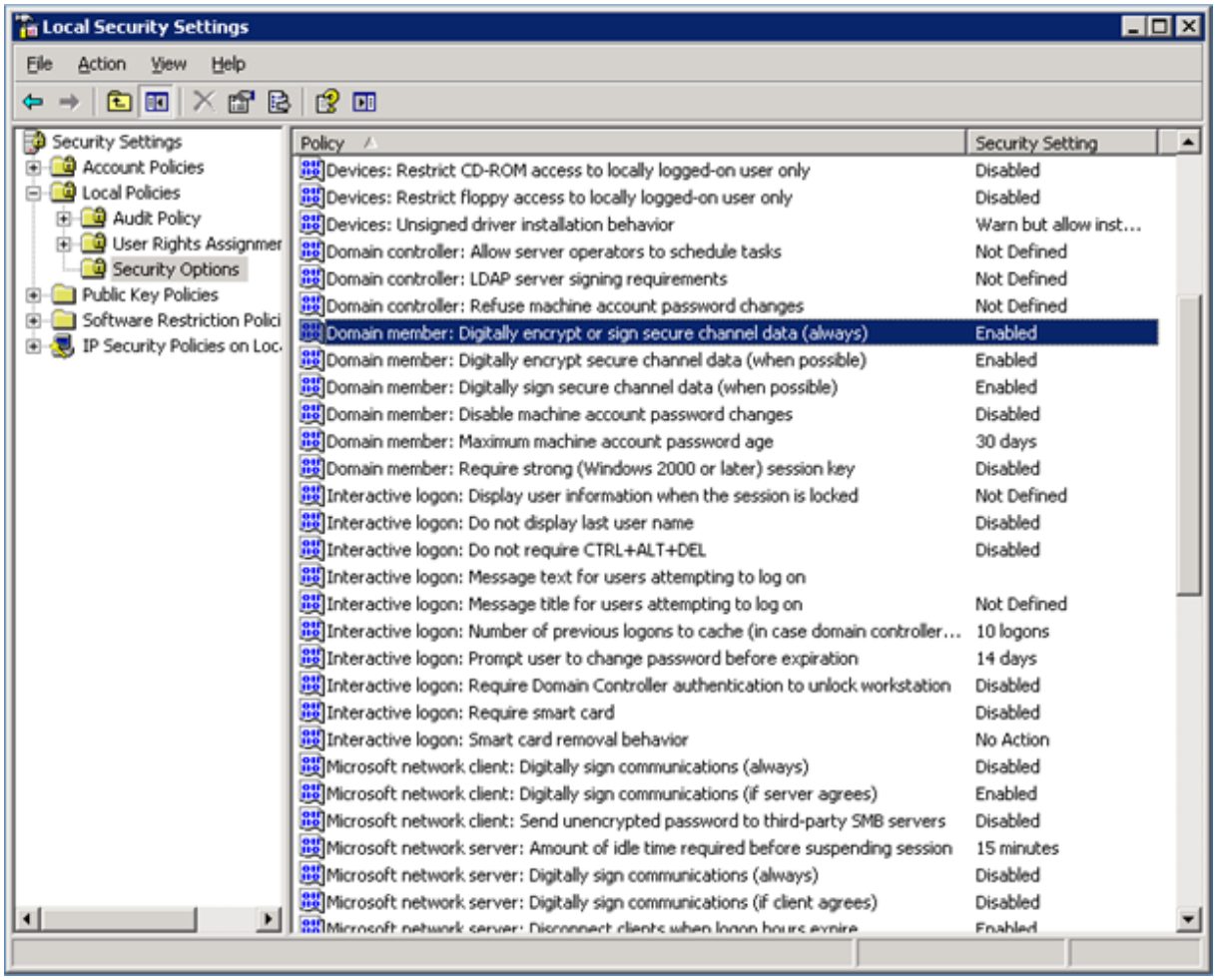
Configurar la aceleración del protocolo CIFS

La aceleración CIFS está habilitada de forma predeterminada para las conexiones que no utilizan la firma CIFS. Si la red utiliza la firma, se puede inhabilitar o los dispositivos del lado del servidor se unan al dominio de Windows.

Inhabilitar firma CIFS

Dependiendo de su configuración de seguridad, es posible que los servidores Windows o los servidores de dominio tengan que ajustar su configuración de seguridad.

Ilustración 1. Opciones de seguridad de Windows Server, Windows Server 2003 y Windows Server 2008.



Los servidores de archivos de Windows tienen dos modos de seguridad: sellado y firma.

El sellado cifra el flujo de datos y evita la aceleración del protocolo CIFS por completo.

La firma agrega datos de autenticación a cada paquete de datos, sin cifrar el flujo de datos. Esto evita la aceleración a menos que haya implementado los procedimientos descritos en Agregar un dispositivo Citrix SD-WAN WANOP a la infraestructura de seguridad de Windows. Cuando se cumple este requisito, la firma se acelera automáticamente. De lo contrario, la firma debe estar inhabilitada (si aún no está inhabilitada) para que se lleve a cabo la aceleración del protocolo.

De forma predeterminada, los servidores de archivos de Windows ofrecen firma pero no la requieren, excepto para los servidores de dominio, que la requieren de forma predeterminada.

Para lograr la aceleración CIFS con sistemas que actualmente requieren firma, debe cambiar la configuración de seguridad del sistema para inhabilitar este requisito. Puede hacerlo en la configuración de seguridad local del servidor de archivos o en directivas de grupo. En los ejemplos siguientes, para Windows Server 2003 y Windows Server 2008, se muestra la configuración local. Los cambios en la directiva de grupo son, por supuesto, casi idénticos.

Citrix SD-WAN WANOP

Para cambiar la configuración del servidor para permitir la aceleración CIFS

1. Acceda a la página Configuración de seguridad local del sistema.
2. Establecer miembro del dominio: cifrar digitalmente o firmar datos de canal seguro (siempre) como Inhabilitado.
3. Establezca el cliente de red de Microsoft: firmar digitalmente las comunicaciones (siempre) en Inhabilitado.
4. Establecer el servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre) en Inhabilitado.

Interpretar estadísticas CIFS

La página Supervisión: Sistema de Archivos (CIFS/SMB) muestra una lista de conexiones CIFS aceleradas. Estas conexiones se dividen en conexiones optimizadas y no optimizadas. Debido a que todas estas conexiones son aceleradas (con control de flujo y compresión), las conexiones optimizadas tienen optimizaciones CIFS además de control de flujo y compresión, mientras que las conexiones no optimizadas solo tienen control de flujo y compresión.

Resumen de gestión de CIFS

- La aceleración CIFS proporciona una mejora significativa incluso a distancias de enlace relativamente cortas.
- La aceleración CIFS comienza cuando el cliente accede por primera vez a un sistema de archivos. Si la aceleración está habilitada con el servidor de archivos y el cliente ya activos y en ejecución, no se produce ninguna aceleración durante muchos minutos, hasta que las conexiones CIFS preexistentes se cierran por completo. Las conexiones CIFS son muy persistentes y duran mucho tiempo antes de cerrarse, incluso cuando están inactivas. Este comportamiento es molesto durante la prueba, pero tiene poca importancia en la implementación normal.
- Desmontar y volver a montar un sistema de archivos en Windows no cierra las conexiones CIFS, porque Windows realmente no desmonta completamente el sistema de archivos. El reinicio del cliente o servidor funciona. Para una medida menos invasiva, utilice el comando NET USE devicename /DELETE de la línea de comandos de Windows para desmontar completamente el volumen. En Linux, smbmount y umount desmontan completamente el volumen.
- Inhabilitar y volver a habilitar las optimizaciones de lectura y escritura CIFS en el dispositivo plantea problemas similares. Las conexiones existentes no se aceleran cuando CIFS está habilitado y el número de errores de protocolo detectados en la página Monitoring: Filesystem (CIFS/SMB) aumenta brevemente.

- Las estadísticas CIFS pueden ser confusas, porque solo el dispositivo más alejado del servidor de archivos informa de la aceleración CIFS con estadísticas completas. El otro dispositivo lo ve como una aceleración ordinaria.
- La aceleración CIFS no se admite en modo proxy.
- Si la aceleración CIFS no se produce con un servidor Windows, compruebe la configuración de seguridad del servidor.

Configurar la aceleración MAPI

April 23, 2021

La aceleración de Microsoft Outlook proporciona un rendimiento mejorado para el tráfico entre los clientes de Microsoft Outlook y los servidores de Microsoft Exchange, lo que aumenta el rendimiento con una variedad de optimizaciones, incluida la captura previa de datos y la compresión.

Esta función también se denomina aceleración MAPI, en nombre del protocolo MAPI utilizado entre Outlook y Exchange Server.

En las redes donde la secuencia de datos de Outlook no está cifrada (el valor predeterminado anterior a Outlook 2007), esta función no requiere configuración.

En redes donde los datos de Outlook están cifrados (el valor predeterminado con Outlook 2007 y versiones posteriores), la aceleración se puede obtener de dos maneras: inhabilitando el cifrado en los clientes de Outlook o haciendo que los dispositivos se unan al dominio de Windows.

Versiones y modos de intercambio de Outlook compatibles

Los dispositivos WANOP de Citrix SD-WAN proporcionan aceleración MAPI para Microsoft Outlook 2003-2016 y Exchange Server 2003-2010, en las siguientes circunstancias:

- Se admite cualquier combinación de clientes y servidores compatibles (mediante el protocolo MAPI).
- Si el dispositivo del lado del servidor se ha unido a un dominio de Windows, las conexiones con cifrado MAPI se aceleran. De lo contrario, no lo están, y el cifrado debe inhabilitarse en los clientes de Outlook.

> **Nota**
>
> En Exchange Server 2013, el protocolo MAPI cambió a RPC sobre protocolo HTTP, este protocolo es compatible. Con Exchange Server SP1, el protocolo RPC sobre HTTP cambió a

> MAPI sobre protocolo HTTP, este protocolo no se admite actualmente.

Requisitos previos

Si la red utiliza datos cifrados de Outlook, que es la configuración predeterminada en Outlook 2007 y versiones posteriores, debe implementar uno de los siguientes requisitos previos para asegurarse de que las conexiones MAPI se aceleran:

- Inhabilitar el cifrado en los clientes de Outlook.
- Realice las tareas descritas enAgregar un dispositivo Citrix SD-WAN WANOP a la infraestructura de seguridad de Windows.

Configuración

La aceleración de Outlook es una función de configuración cero que está habilitada de forma predeterminada. (Si no se desea, se puede inhabilitar inhabilitando la aceleración en la clase de servicio MAPI en la página
Configuración: Directiva de clase de servicio.) La aceleración de Outlook se produce automáticamente si se cumplen las siguientes condiciones:

- Hay un dispositivo en el extremo de Exchange Server de la WAN.
- O bien hay un dispositivo en el extremo de Outlook de la WAN o el sistema que ejecuta Outlook también está ejecutando el complemento WANOP de Citrix SD-WAN.
- Todo el tráfico de Outlook/Exchange pasa a través de los dispositivos (o dispositivo y plug-in).
- Se reinicia Exchange Server o Outlook (la aceleración no comienza hasta que se cierran las conexiones MAPI existentes).
- El cifrado está deshabilitado en Outlook o el dispositivo del lado del servidor pertenece al dominio de Windows y tiene una relación de pares segura con el dispositivo del lado del cliente (o el complemento WANOP de Citrix SD-WAN). En el caso en que el dispositivo se haya unido al dominio de Windows, la autenticación en el dominio debe mantenerse en la configuración predeterminada (negociar) para que la aceleración funcione.

Inhabilitar el cifrado en Outlook 2007 o Outlook 2010

A menos que el dispositivo del lado del servidor se haya unido al dominio de Windows y tenga una relación de pares segura con el dispositivo del lado del cliente (o el complemento WANOP de Citrix SD-WAN), el cifrado entre Outlook y Exchange Server debe deshabilitarse para que se lleve a cabo la aceleración.

El cifrado se inhabilitó de forma predeterminada antes de Outlook 2007. A partir de Outlook 2007, el cifrado está habilitado de forma predeterminada.

Nota sobre la ejecución

MAPI utiliza un formato de datos diferente de otros protocolos. Esta diferencia impide una compresión efectiva entre protocolos. Es decir, un archivo que primero se transfirió a través de FTP y luego como archivo adjunto de correo electrónico no recibe una ventaja de compresión en la segunda transferencia. Si los mismos datos se envían dos veces en formato MAPI, la segunda transferencia recibe compresión completa.

Compresión SSL

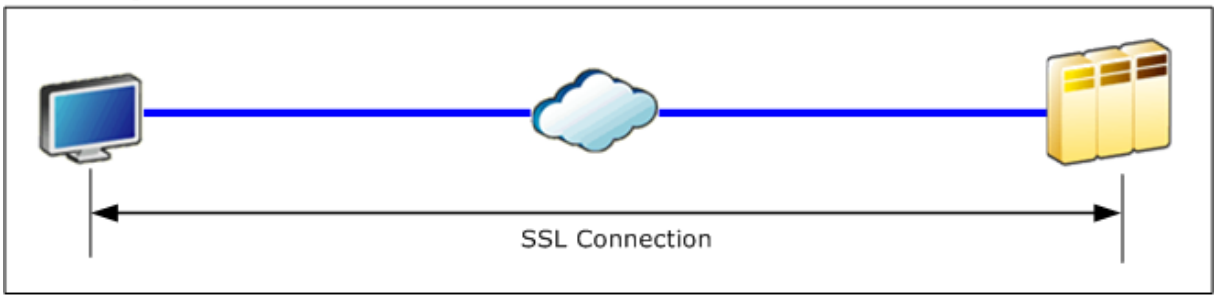
April 23, 2021

La compresión SSL WANOP de Citrix SD-WAN aplica compresión multisesión a conexiones SSL (por ejemplo, tráfico HTTPS), proporcionando relaciones de compresión de hasta 10, 000:1.

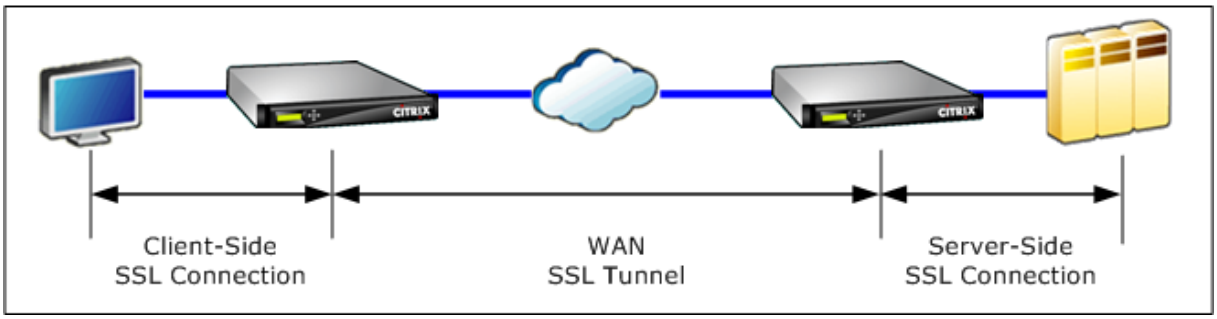
> **Nota**
>
> La compresión SSL requiere una conexión de peering (señalización) segura entre los dos dispositivos en los extremos del vínculo acelerado.

El cifrado se mantiene de extremo a extremo dividiendo la conexión en tres segmentos cifrados: de cliente a dispositivo de cliente, de dispositivo de cliente a dispositivo de servidor y de dispositivo de servidor a servidor.

Ordinary SSL Connection



Accelerated SSL Connection



Precaución: La compresión SSL descifra el flujo de datos cifrado y, a menos que se utilice la opción Cifrado de datos de usuario, los historiales de compresión de ambas unidades de aceleración conservan los registros de texto claro de los datos descifrados. Compruebe que la implementación y la configuración sean coherentes con las directivas de seguridad de la organización. Citrix recomienda habilitar el cifrado del historial de compresión en cada unidad al configurar la conexión de señalización de pares segura necesaria para la aceleración SSL.

> **Nota**
>
> - Cuando habilita la compresión SSL, el dispositivo deja de intentar la compresión con otros dispositivos con los que no tiene una relación de pares segura (ya sea Citrix SD-WAN WANOP o Citrix SD-WAN WANOP Plug-in). Por lo tanto, esta función es la más adecuada para redes donde todos los dispositivos están configurados para la compresión SSL.
> - Con la compresión SSL habilitada, debe escribir manualmente la contraseña del almacén de claves cada vez que se reinicie el dispositivo.

Cómo funciona la compresión SSL

April 23, 2021

La compresión SSL tiene acceso a los datos de texto claro de la conexión, ya que el dispositivo del lado del servidor actúa como *delegado de seguridad* de los servidores de extremo. Este comportamiento

es posible porque el dispositivo del lado del servidor está configurado con copias de las credenciales de seguridad de los servidores (claves privadas y certificados), lo que le permite actuar en nombre de los servidores. Para el cliente, este comportamiento es equivalente a comunicarse directamente con el servidor de extremo.

Dado que el dispositivo funciona como delegado de seguridad del servidor, la mayor parte de la configuración se realiza en el dispositivo del servidor. El dispositivo del cliente (o complemento) actúa como satélite del dispositivo del servidor y no requiere configuración por servidor.

Los dispositivos del lado del servidor y del lado del cliente comparten el estado de la sesión a través de una *conexión de señalización SSL.* Todas las conexiones aceleradas entre los dos dispositivos se envían a través de *conexiones de datos SSL,* independientemente de que las conexiones originales estuvieran cifradas o no.

Nota: La compresión SSL no encripta necesariamente todo el tráfico de enlaces. El tráfico que se cifró originalmente permanece cifrado, pero el tráfico no cifrado no siempre está cifrado. Los dispositivos no intentan cifrar el tráfico no acelerado. Debido a que no hay ninguna garantía absoluta de que una conexión determinada se acelerará (varios eventos evitan la aceleración), no hay garantía de que los dispositivos cifrarán una conexión no cifrada determinada.

La compresión SSL funciona en uno de los dos modos: proxy transparente o proxy dividido. Estos dos modos admiten funciones SSL ligeramente diferentes. Seleccione el modo que proporciona las funciones que requiere una aplicación determinada.

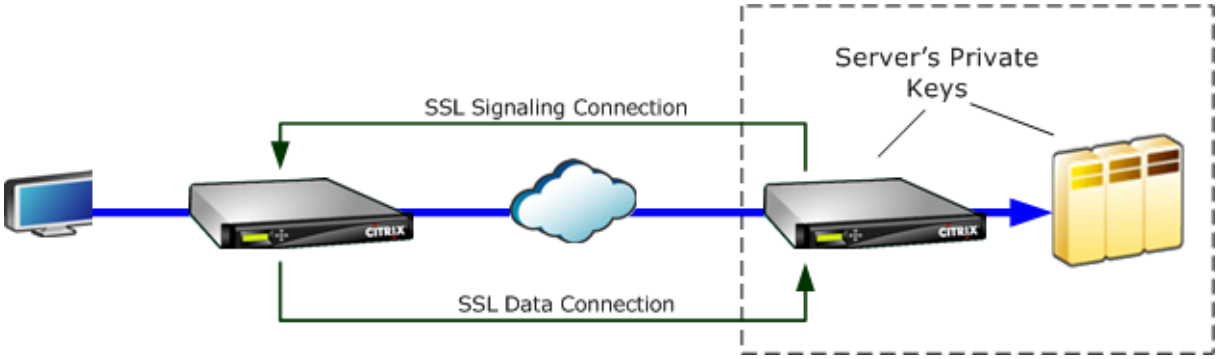
Modo proxy SSL utilizar: Utilice el modo proxy transparente SSL *solo* si necesita autenticación de cliente real (es decir, autenticación que identifique correctamente al cliente de extremo individual) *y* no necesita entradas de sesión Diffie-Hellman, Temp RSA, TLS, SSL versión 2, o renegociación de sesión. Utilice el proxy dividido SSL para todas las demás implementaciones.

Proxy transparente SSL

En el *modo proxy transparente SSL* (no debe confundirse con el modo transparente en el complemento Citrix SD-WAN WANOP), el dispositivo del lado del servidor se disfraza como servidor. Las credenciales del servidor (par de certificados y claves) se instalan en el dispositivo del lado del servidor para que pueda actuar en nombre del servidor. A continuación, el dispositivo del lado del servidor configura el dispositivo del lado del cliente para controlar el extremo del cliente de la conexión. Las credenciales del servidor no están instaladas en el dispositivo del cliente.

En este modo se admite la autenticación de cliente verdadera, pero Temp RSA y Diffie-Hellman no lo son. El modo proxy transparente SSL es adecuado para aplicaciones que requieren autenticación de cliente, pero solo si no se requiere ninguna de las siguientes funciones: Diffie-Hellman, Temp RSA, tickets de sesión TLS, SSL versión 2. Además, no se debe intentar la renegociación de la sesión o la conexión termina.

No se requiere ninguna configuración en el dispositivo del cliente (aparte de configurar una relación de peering segura con el dispositivo del lado del servidor) y no se requiere ninguna configuración en el cliente, lo que trata la conexión exactamente como si se estuviera comunicando directamente con el servidor.



Proxy de división SSL

El*modo proxy dividido SSL* es preferido en la mayoría de las instancias, ya que soporta Temp RSA y Diffie-Hellman, que requieren muchas aplicaciones. En el modo proxy dividido SSL, el dispositivo del lado del servidor se hace pasar por un servidor para el cliente y como cliente para el servidor. Instalar credenciales de servidor (un par de claves de certificado) en el dispositivo del lado del servidor para que pueda actuar en nombre del servidor.

El modo de proxy dividido también admite la autenticación de cliente proxy si instala credenciales de cliente opcionales, que se presentan a la aplicación de servidor de extremo si solicita autenticación de cliente. Estas credenciales de cliente se presentarán en lugar de las credenciales reales del cliente de punto final. (Utilice proxy transparente si la aplicación requiere las credenciales del cliente de extremo).

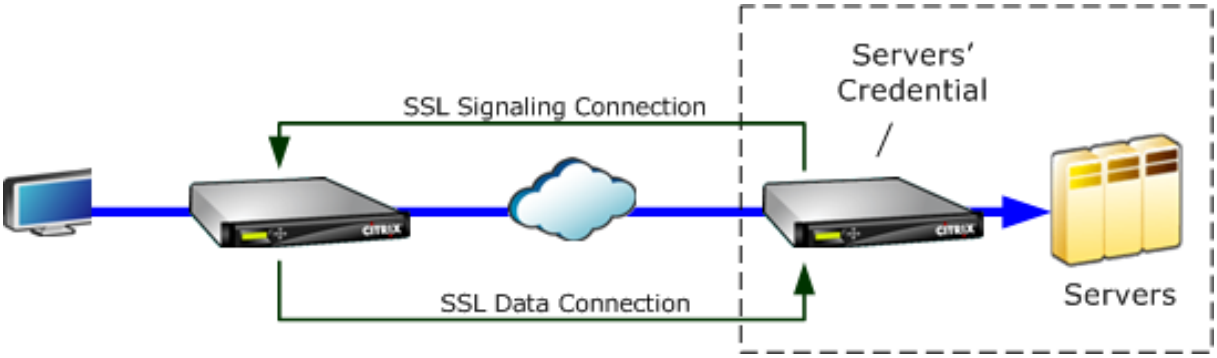
Dado que la autenticación de cliente verdadero no se admite en este modo, el servidor no puede autenticar el cliente de extremo real. Si el dispositivo del lado del servidor no está configurado con credenciales de cliente, se producirá un error en todos los intentos de la aplicación del lado del servidor en la autenticación del cliente. Si el dispositivo del lado del servidor está configurado con credenciales de cliente, todas las solicitudes de autenticación del cliente se responderán con estas credenciales, independientemente de la identidad del cliente real.

No se requiere ninguna configuración en el dispositivo del cliente (aparte de configurar una relación de peering segura con el dispositivo del lado del servidor) y no se requiere ninguna configuración en el cliente, lo que trata la conexión como si se estuviera comunicando directamente con el servidor. Las credenciales del servidor en el dispositivo del servidor no están instaladas en el dispositivo del cliente.

Para admitir varios servidores, se pueden instalar varios pares privados de clave de certificado en

el dispositivo, uno por perfil SSL. Las reglas SSL especiales en las definiciones de clase de servicio coinciden con los servidores con los perfiles SSL y, por lo tanto, los perfiles SSL con las credenciales.

En el modo proxy dividido SSL, los certificados de CA y los pares de clave de certificado y certificados de CA no tienen que coincidir con los de los servidores, aunque pueden hacerlo. Debido a la naturaleza de un proxy dividido, el dispositivo del lado del servidor puede utilizar credenciales aceptables para la aplicación cliente (credenciales válidas emitidas por una autoridad de confianza). Tenga en cuenta que, en el caso de conexiones HTTPS, los exploradores web emiten una advertencia si el nombre común no coincide con el nombre de dominio en la URL. En general, el uso de copias de las credenciales del servidor es la opción más libre de problemas.



Configurar compresión SSL

April 23, 2021

La característica de compresión SSL WO WO de Citrix SD-WAN permite la compresión multisesión de conexiones SSL (por ejemplo, tráfico HTTPS), lo que proporciona una relación de compresión de hasta 10, 000:1. Para obtener más información, consulte Compresión SSL.

Para que la compresión SSL funcione, el dispositivo Citrix SD-WAN WANOP necesita certificados del servidor o del cliente. Para admitir varios servidores, se pueden instalar varias claves privadas en el dispositivo, una por cada perfil SSL. Las reglas SSL especiales en las definiciones de clase de servicio coinciden con los servidores con los perfiles SSL y, por lo tanto, los perfiles SSL con las claves privadas.

La compresión SSL funciona en modo proxy dividido o proxy transparente, puede elegir el modo según sus requisitos. Para obtener más información, consulte Cómo funciona la compresión SSL.

> **Nota**
>
> Actualmente no se admite el modo proxy transparente.

Para habilitar el acceso seguro con el túnel SSL, el último protocolo SSL TLS 1.2 se utiliza en proxy SSL. Puede elegir utilizar el protocolo TLS1.2 o los protocolos TLS1.0, TLS1.1 y TLS1.2.

> **Nota**
>
> Los protocolos SSL v3 y SSL v2 ya no son compatibles.

Para configurar la compresión SSL:

1. Adquiera copias del certificado de CA del servidor y del par de claves de certificado privado e instálelas en el dispositivo del servidor. Es probable que estas credenciales sean específicas de la aplicación. Es decir, un servidor puede tener credenciales diferentes para un servidor web Apache que para un Exchange Server que ejecuta RPC a través de HTTPS.
2. Puede elegir crear un perfil SSL de proxy dividido o un perfil SSL de proxy transparente.

   Para obtener información sobre la configuración del perfil SSL de proxy dividido, consulte la sección **Configuración de un perfil SSL de proxy dividido** a continuación.

   Para obtener información sobre la configuración del perfil SSL de proxy transparente, consulte la sección **Configuración del perfil SSL de proxy transparente** a continuación.

   > **Nota**
   >
   > Actualmente no se admite el perfil SSL de proxy transparente.

3. Adjunte el perfil SSL a una clase de servicio en el dispositivo del lado del servidor. Esto se puede hacer creando una nueva clase de servicio basada en la IP del servidor o modificando una clase de servicio existente.

   Para obtener más información, consulte la sección **Creación o Modificación de la Clase de Servicio** a continuación.
4. Establezca clases de servicio en el dispositivo del cliente. El tráfico SSL no se comprime a menos que caiga en una clase de servicio, en el dispositivo del cliente, que habilite la aceleración y la compresión. Puede ser una regla de clase de servicio ordinaria, no una regla SSL (solo el dispositivo del lado del servidor necesita reglas SSL), pero debe habilitar la aceleración y la compresión. El tráfico entra en una clase de servicio existente, como HTTPS u Otro tráfico TCP. Si la directiva de esta clase habilita la aceleración y la compresión, no se necesita ninguna configuración adicional.
5. Verifique el funcionamiento de la regla. Enviar tráfico que debería recibir aceleración SSL a través de los dispositivos. En el dispositivo del lado del servidor, en la ficha Supervisión: Optimización: Conexiones: Conexiones aceleradas, la columna Clase de servicio debe coincidir con la clase de servicio configurada para una aceleración segura, y la columna Proxy SSL debe mostrar True para las conexiones adecuadas.

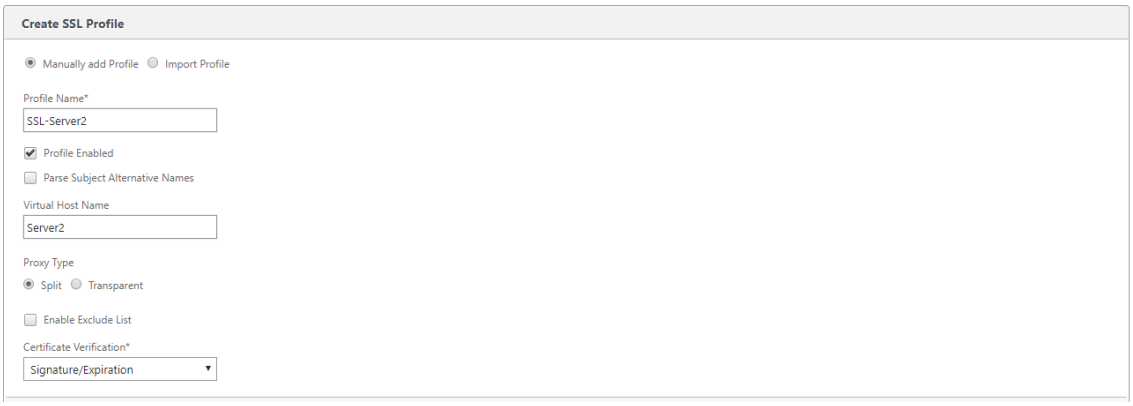
Configurar un perfil SSL de proxy dividido

Para configurar un perfil SSL de proxy dividido:

1. En el dispositivo Citrix SD-WAN WO del lado del servidor, vaya a **Configuración** > **Aceleración segura** > **Perfil SSL** y haga clic en **Agregar perfil**.

   > **Nota**
   >
   > Puede agregar manualmente un perfil SSL o importar uno almacenado en el equipo local.

2. En el campo **Nombre de perfil**, introduzca un nombre para el perfil SSL y seleccione **Perfil habilitado**.
3. Si el servidor SSL utiliza más de un nombre de host virtual, en el campo **Nombre de host virtual**, escriba el nombre de host virtual de destino. Éste es el nombre de host que aparece en las credenciales del servidor.



   > **Nota**
   >
   > Para admitir varios hosts virtuales, cree un perfil SSL independiente para cada nombre de host.

4. Elija **Dividir** tipo de proxy.
5. En el campo **Verificación de certificados**, conserve el valor predeterminado (Firma/Expiración) a menos que las directivas dicten lo contrario.
6. Realice la configuración de proxy del lado del servidor:

   En el campo **Almacén de verificación**, seleccione una entidad emisora de certificados (CA) de servidor existente o haga clic en **+** para cargar una entidad emisora de certificados de servidor.

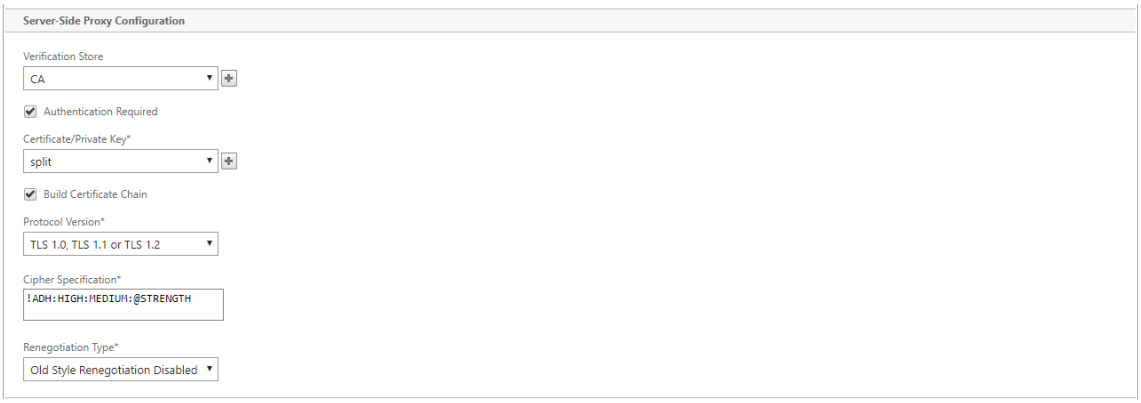
   Elija **Autenticación requerida** y en el campo **Certificado/Clave privada** seleccione un par de claves de certificado o haga clic en **+** para cargar un par de claves de certificado.

   En el campo **Versión del protocolo**, seleccione los protocolos que acepta el servidor.

> **Nota**
>
> Citrix SD-WAN WO admite una combinación de **TLS1.0, TLS1.1 o TLS1.2**o **TLS1.2** solamente**.** Los protocolos SSL SSLv3 y SSLv2 no son compatibles.

Si es necesario, modifique la cadena de **especificación de cifrado** mediante la sintaxis OpenSSL.

Si es necesario, seleccione el tipo de renegociación en la lista implementable **Tipo de renegociación** para permitir la renegociación de sesiones SSL del lado del cliente.



7. Realice la configuración del proxy del lado del cliente:

   En el campo **Certificado/Clave privada**, conserve el valor predeterminado.

   Elija **Crear cadena de certificados** para permitir que el dispositivo del lado del servidor cree la cadena de certificados SSL.

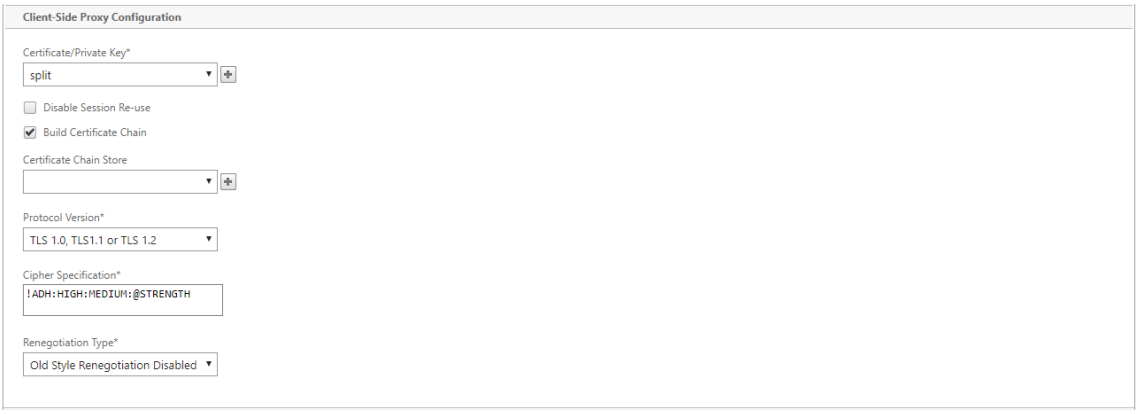
   Si es necesario, seleccione o cargue un almacén de CA para utilizarlo como Almacén de cadena de certificados.

   En el campo **Versión del protocolo**, seleccione las versiones de protocolo que quiere admitir en el lado del cliente.

   > **Nota**
   >
   > Citrix SD-WAN WO admite una combinación de **TLS1.0, TLS1.1 o TLS1.2**, o **TLS1.2** solamente**.** Los protocolos SSL SSLv3 y SSLv2 no son compatibles.

   Si es necesario, modifique la especificación de cifrado del lado cliente.

   Si es necesario, seleccione el tipo de renegociación en la lista implementable **Tipo de renegociación** para permitir la renegociación de sesiones SSL del lado del cliente.



8. Haga clic en **Crear**.

Configurar perfil SSL de proxy transparente

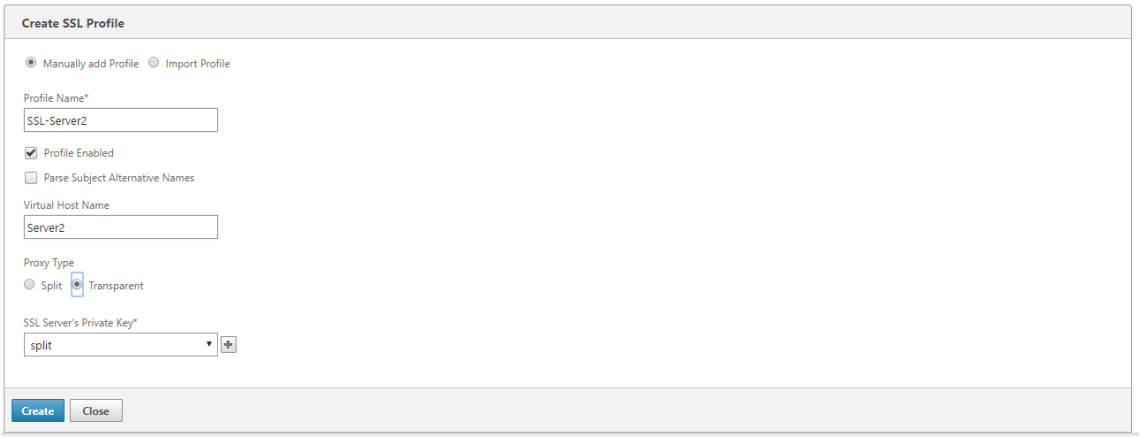
Para configurar un perfil SSL de proxy transparente:

1. En el dispositivo Citrix SD-WAN WO del lado del servidor, vaya a **Configuración** > **Aceleración segura** > **Perfil SSL** y haga clic en **Agregar perfil**.

   > **Nota**
   >
   > Puede agregar manualmente un perfil SSL o importar uno almacenado en el equipo local.

2. En el campo **Nombre de perfil**, introduzca un nombre para el perfil SSL y seleccione **Perfil habilitado**.
3. Si el servidor SSL utiliza más de un nombre de host virtual, en el campo **Nombre de host virtual**, escriba el nombre de host virtual de destino. Éste es el nombre de host que aparece en las credenciales del servidor.

   > **Nota**
   >
   > Para admitir varios hosts virtuales, cree un perfil SSL independiente para cada nombre de host.



4. Elija Tipo de proxy **transparente**.
5. En el campo **Clave privada del servidor SSL**, seleccione la clave privada del servidor en el menú implementable o haga clic en **+** para cargar una nueva clave privada.
6. Haga clic en **Crear**.

Crear o modificar la clase de servicio

Para crear o modificar la clase de servicio y adjuntar el perfil SSL:

1. En la interfaz web del dispositivo Citrix SD-WAN WO, vaya a **Configuración > Reglas de optimización > Clases de servicio** y haga clic en **Agregar**. Para modificar una clase de servicio existente, seleccione la clase de servicio adecuada y haga clic en **Modificar**.
2. En el campo Nombre, escriba un nombre para la nueva clase de servicio (por ejemplo, HTTPS acelerado).
3. Habilite la compresión estableciendo la directiva de aceleración en **Disco**, **Memoria** o **Control de flujo**.
4. En la sección **Reglas de filtro**, haga clic en **Agregar**.
5. En el **campo Dirección IP de destino**, escriba la dirección IP del servidor (por ejemplo, 172.16.0.1 o, equivalente, 172.16.0.1/32.
6. En el campo **Dirección**, establezca la regla en Unidireccional. Los perfiles SSL están inhabilitados si se especifica Bidireccional.
7. En la sección **Perfiles SSL**, seleccione el perfil SSL que creó y muévalo a la sección **Configurado**.
8. Haga clic en **Crear** para crear la regla.
9. Haga clic en **Crear** para crear la clase de servicio.

Comando CLI actualizado

Citrix SD-WAN WO 9.3 admite el protocolo SSL TLS1.2 más reciente. Puede elegir utilizar el protocolo TLS1.2 o cualquier versión de los protocolos TLS. Los protocolos SSL v3 y SSL v2, y los perfiles SSL proxy transparente no son compatibles. Los comandos **add ssl-profile** y **set ssl-profile** CLI se actualizan para reflejar estos cambios.

add ssl-profile:

```
*-name " profile-name " *

*\[-state {
 enable, disable }
 \]*

*-proxy-type split*

*\[-virtual-hostname " hostname " \]*

*-cert-key " cert-key-pair-name " *

*\[-build-cert-chain {
 enable, disable }
 \]*

*\[-cert-chain-store {
 use-all-configured-CA-stores, " store-name " }
 \]*

*\[-cert-verification {
 none, Signature/Expiration, Signature/Expiration/*

*Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
 \]*

*\[-verification-store {
 use-all-configured-CA-stores, " store-name " }
 \]*

*\[-server-side-protocol {
  TLS-1.2, TLS-version-any }
 \]*

*\[-server-side-ciphers " ciphers " \]*

*\[-server-side-authentication {
 enable, disable }
 \]*

*\[-server-side-cert-key " cert-key-pair-name " \]*

*\[-server-side-build-cert-chain {
```



```
 enable, disable }
 \]*

*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*

*\[-client-side-protocol-version {
  TLS-1.2, TLS-version-any }
 \]*

*\[-client-side-ciphers “ ciphers ” \]*

*\[-client-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*
```

set ssl-profile:

```
*-name “ profile-name ” \[-state {
 enable, disable }
 \]*

*\[-proxy-type split\]*

*\[-virtual-hostname “ hostname ” \]*

*\[-cert-key “ cert-key-pair-name ” \]*

*\[-build-cert-chain {
 enable, disable }
 \]*

*\[-cert-chain-store {
 use-all-configured-CA-stores, “ store-name ” }
 \]*

*\[-cert-verification {
 none, Signature/Expiration, Signature/Expiration/*

*Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
 \]*

*\[-verification-store {
 use-all-configured-CA-stores, “ store-name ” }
 \]*

*\[-server-side-protocol {
 TLS-1.2, TLS-version-any }
```



```
 \]*

*\[-server-side-ciphers  “ ciphers ” \]*

*\[-server-side-authentication {
 enable, disable }
 \]*

*\[-server-side-cert-key  “ cert-key-pair-name ” \]*

*\[-server-side-build-cert-chain {
 enable, disable }
 \]*

*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*

*\[-client-side-protocol-version {
 TLS-1.2, TLS-version-any }
 \]*

*\[-client-side-ciphers  “ ciphers ” \]*

*\[-client-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*
```

Compresión SSL con el plug-in de Citrix SD-WAN WANOP

April 23, 2021

El complemento WANOP de Citrix SD-WAN se utiliza siempre como unidad del lado del cliente y, por lo tanto, no requiere ninguna configuración SSL adicional que la instalación de credenciales para la conexión de señalización SSL (peering seguro). La principal diferencia entre la compresión SSL en el complemento y el dispositivo es que el complemento no puede cifrar los datos de usuario en el historial de compresión basado en disco.

Precaución: Dado que el historial de compresión basado en disco en el Plug-in no está cifrado, conserva un registro de texto claro de comunicaciones cifradas potencialmente sensibles y efímeras . Esta falta de cifrado es potencialmente peligrosa en equipos para los que no se controla el acceso físico. Por lo tanto, Citrix recomienda las siguientes prácticas recomendadas:

- No utilice **Validación de certificados: Ninguno** en sus dispositivos. (Tenga en cuenta que, en este caso, el dispositivo se niega a permitir la compresión con complementos que no tienen certificados adecuados).
- Instale certificados solo en sistemas que puedan verificarse para que cumplan los requisitos de seguridad física o de datos de su organización (por ejemplo, portátiles que utilizan cifrado de disco completo).

El complemento WANOP de Citrix SD-WAN admite tanto el proxy dividido SSL como el proxy transparente SSL. El complemento se envía sin pares de clave de certificado para la conexión de señalización SSL. Si lo desea, todos los plug-ins pueden utilizar las mismas credenciales, o cada plug-in puede tener sus propias credenciales.

El complemento no intenta la compresión SSL a menos que se hayan instalado credenciales.

El complemento hereda su licencia criptográfica del dispositivo.

RPC sobre HTTP

April 23, 2021

Microsoft Exchange Server es uno de los servidores de correo electrónico comunes utilizados en todas las organizaciones. Como resultado de las mejoras recientes en Microsoft Exchange Server, puede conectarse de forma segura a él a través de Internet. Dependiendo del ancho de banda disponible, es posible que experimente latencia en el correo electrónico entregado al cliente de Outlook. Además del protocolo MAPI, el dispositivo Citrix SD-WAN WANOP admite la llamada a procedimiento remoto a través de HTTPS (RPC sobre HTTPS) para optimizar el tráfico de Microsoft Exchange. Esta función también se conoce como Outlook Anywhere.

RPC sobre HTTPS no es un protocolo nuevo, pero a partir de Microsoft Exchange 2013, reemplaza MAPI como protocolo predeterminado. La principal ventaja de RPC sobre HTTPS es que permite a los clientes conectarse de forma segura al servidor de correo a través de Internet.

Cuando se utiliza RPC a través de HTTPS, el servidor de Microsoft Exchange debe utilizar un certificado digital y una clave privada para autenticarse en el cliente de Outlook. La comunicación entre el cliente y el servidor utiliza HTTPS como protocolo de transporte.

En el dispositivo Citrix SD-WAN WANOP, RPC a través de HTTPS es compatible con las siguientes versiones de Microsoft Outlook y Exchange Server:

- Microsoft Outlook
  - Microsoft Outlook versión 2007

  - Microsoft Outlook versión 2010
  - Microsoft Outlook versión 2013
- Microsoft Exchange Server
  - Microsoft Exchange Server versión 2007
  - Microsoft Exchange Server versión 2010
  - Microsoft Exchange Server versión 2013

De estos, todas las versiones excepto Microsoft Exchange Server 2013 admiten MAPI (a través de TCP), así como RPC a través de HTTPS. Sin embargo, Microsoft Exchange Server 2013 obliga a las conexiones a utilizar RPC a través de HTTPS, independientemente de la versión de Microsoft Outlook que utilice, para conectarse al servidor de Exchange.

Configurar RPC a través de HTTPS

De forma predeterminada, la función RPC sobre HTTPS está habilitada en el dispositivo. Sin embargo, para configurar el dispositivo para acelerar RPC a través de HTTPS, debe realizar las siguientes tareas adicionales:

- Configure MAPI cifrada.
- Configure un perfil SSL con un certificado de servidor.
- Cree una clase de servicio RPC sobre HTTPS y vincule el perfil SSL a ella.

Configurar MAPI cifrada

> **Nota**
>
> Omita esta sección si ya ha configurado la aceleración MAPI cifrada en el dispositivo.

Microsoft Outlook utiliza conexiones MAPI (Interfaz de programación de aplicaciones de mensajería) entre los clientes de Outlook y el servidor de Microsoft Exchange. Las conexiones MAPI utilizan RPC, que están encapsuladas por una conexión HTTP. Por lo tanto, antes de configurar RPC a través de HTTPS en un dispositivo Citrix SD-WAN WANOP, debe configurar MAPI cifrado en el dispositivo.

Requisitos previos:

Antes de configurar MAPI cifrada, asegúrese de que se cumplen los siguientes requisitos previos:

- La opción Secure Peer debe establecerse en True tanto en el cliente como en el dispositivo del lado del servidor. Para configurar un asociado seguro, consulte Peering seguro.
- La dirección IP DNS configurada en el dispositivo del servidor debe ser accesible.

- El dispositivo del centro de datos debe unirse correctamente al dominio.
- Se debe agregar un usuario delegado al dispositivo del centro de datos y su estado debe marcarse como Correcto.

Para obtener más información, consulte Configurar un dispositivo Citrix SD-WAN WANOP para optimizar el tráfico seguro de Windows.

Configurar un perfil SSL con un certificado de servidor

La conexión HTTPS que encapsula la conexión MAPI está protegida por SSL. Como resultado, RPC sobre HTTPS requiere conectividad a través del puerto TCP 443. Este puerto se asigna a HTTPS, que los administradores del servidor web suelen mantener abiertos en la aplicación de firewall. El uso de la comunicación protegida por SSL ayuda a RPC a través de HTTPS a mantener la seguridad de todas las comunicaciones.

Para habilitar la aceleración RPC a través de HTTPS, debe instalar un certificado de servidor en el dispositivo. Con este certificado de servidor, puede configurar un perfil SSL que RPC a través de HTTPS utiliza para una comunicación segura. Para configurar un perfil SSL con un certificado de servidor Exchange, consulte Instalación de certificados de servidor y cliente.

> **Nota**
>
> Solo debe configurar un perfil SSL en el dispositivo del centro de datos.

Crear una clase de servicio RPC a través de HTTPS y enlazar el perfil SSL a ella

Para optimizar las conexiones RPC a través de HTTP, debe crear una clase de servicio que muestre HTTPS y todas las aplicaciones MAPI. Debe proporcionar la dirección IP del servidor de Microsoft Exchange como dirección IP de destino para esta clase de servicio y, a continuación, vincular el perfil SSL creado a esta clase de servicio. La vinculación del perfil a la clase de servicio garantiza que la comunicación entre el cliente de Outlook y el servidor de Microsoft Exchange está protegida mediante este perfil.

> **Nota**
>
> Debe configurar y enlazar un perfil SSL a la clase de servicio solo en el dispositivo del centro de datos.

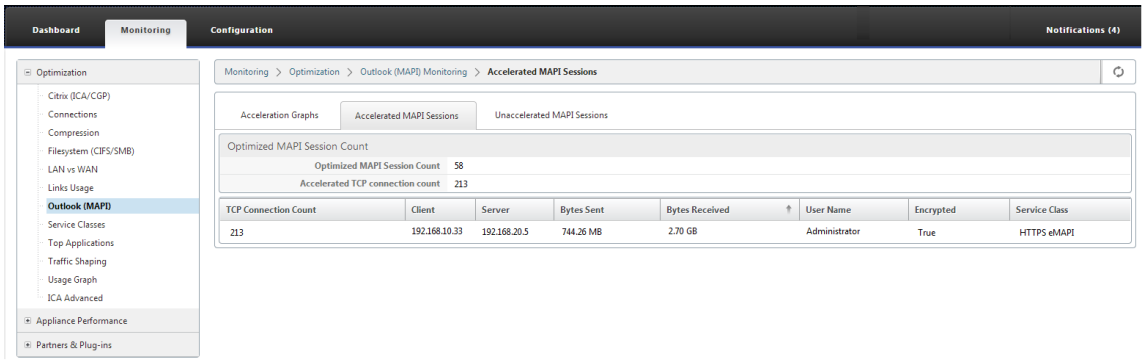
Verificar RPC acelerado a través de conexiones HTTPS

Después de configurar RPC a través de HTTPS en el dispositivo, puede comprobar que el dispositivo está acelerando la conexión RPC a través de HTTPS en la página Supervisión de MAPI. Las conexiones RPC aceleradas a través de HTTPS se enumeran en la ficha Sesiones MAPI aceleradas.

> **Nota**
>
> Debe configurar RPC a través de HTTPS en los dispositivos del lado del cliente, así como en los dispositivos Citrix SD-WAN WANOP del lado del servidor para acelerar las conexiones RPC a través de HTTPS.

Para comprobar que las conexiones RPC a través de HTTPS se están acelerando

1. Vaya a **Supervisión** > **Optimización** > **Outlook (MAPI)**.
2. En la ficha **Sesiones MAPI aceleradas**, compruebe que se aceleran las conexiones RPC a través de HTTPS.



> **Nota**
>
> La aplicación tiene posibles valores de: HTTPS EMAPI, HTTP EMAPI, HTTPS MAPI y HTTP MAPI.

Aceleración de control de flujo TCP

January 10, 2022

Las WAN ordinarias tienen una capacidad de respuesta muy deficiente en una utilización de enlaces elevada y a largas distancias. Una regla general ampliamente utilizada para los enlaces WAN ordinarios y no acelerados es: una vez que la utilización del enlace alcanza el 40%, es hora de agregar más ancho de banda, porque el rendimiento y la fiabilidad se han degradado hasta el punto en que el enlace es en gran medida inutilizable. El rendimiento interactivo sufre, lo que dificulta que las personas hagan el trabajo y que las conexiones se agoten con frecuencia. Los enlaces acelerados no tienen este problema. Un enlace con un 95% de utilización sigue siendo perfectamente utilizable.

Los dispositivos WANOP de Citrix SD-WAN se convierten en puertas de enlace virtuales que controlan el tráfico TCP en el vínculo WAN. TCP ordinario es controlado por conexión por los dispositivos de punto final. El control óptimo del tráfico de enlaces es difícil, ya que ni los dispositivos de punto final ni las conexiones individuales tienen conocimiento alguno de la velocidad del enlace ni de la

cantidad de tráfico de la competencia. Por otro lado, una Gateway está en una posición ideal para supervisar y controlar el tráfico de enlaces. Las puertas de enlace ordinarias desperdician esta oportunidad porque no pueden suministrar el control de flujo que le falta a TCP.La tecnología WANOP de Citrix SD-WAN añade la inteligencia que falta tanto en el equipo de red como en las conexiones TCP. El resultado es un rendimiento WAN muy mejorado, incluso en condiciones adversas como grandes pérdidas o distancias extremas.

El control de flujo WANOP de Citrix SD-WAN es transparente y sin pérdidas, e implementa un amplio espectro de optimizaciones de velocidad. No se requiere ninguna configuración, debido a la detección automática y la configuración automática. Sin embargo, es posible que tenga que ajustar los firewalls si bloquean las opciones TCP utilizadas por los algoritmos de aceleración.

Control de flujo transparente y sin pérdidas

April 23, 2021

La aceleración funciona en cualquier conexión TCP que pasa a través de dos dispositivos (uno en el sitio de envío y otro en el sitio receptor), o en un dispositivo Citrix SD-WAN WANOP y un complemento WANOP de Citrix SD-WAN. Aunque la imagen anterior muestra una red de dos dispositivos, cualquier dispositivo puede acelerar las conexiones entre cualquier número de sitios equipados con dispositivos simultáneamente. Esto permite utilizar un único dispositivo por sitio, en lugar de dos por vínculo.

Al igual que cualquier puerta de enlace, el dispositivo Citrix SD-WAN WANOP coloca los paquetes en el enlace. Sin embargo, a diferencia de las puertas de enlace ordinarias, impone un control de flujo transparente y sin pérdidas en cada segmento de enlace, incluyendo:

- Segmento LAN entre el remitente y el dispositivo de envío
- El segmento WAN entre los dispositivos de envío y recepción
- Segmento LAN entre el dispositivo receptor y el receptor

El control de flujo se puede administrar de forma independiente para cada uno de estos tres segmentos. Los segmentos están parcialmente desacoplados, por lo que cada uno puede tener su velocidad controlada de forma independiente. Esto es importante cuando la velocidad de una conexión debe aumentarse o bajarse rápidamente a su justa cuota de ancho de banda, y también es importante como medio de soportar algoritmos WAN mejorados y compresión.

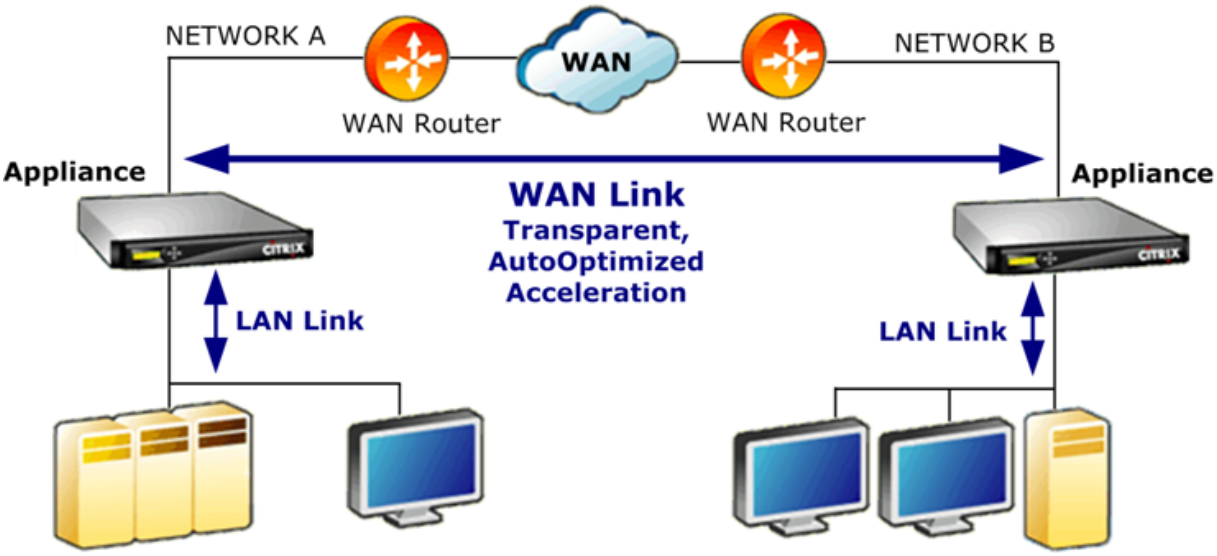
El protocolo TCP está diseñado para hacer que cada conexión TCP intente aumentar su uso de ancho de banda continuamente. Sin embargo, el ancho de banda del enlace es limitado. El resultado es que los enlaces se vuelven desbordados.El control de flujo WANOP de Citrix SD-WAN mantiene las

conexiones TCP fluyendo a la velocidad correcta. El enlace se llena pero nunca se inventa, por lo que la latencia de la cola y las pérdidas de paquetes se minimizan, mientras que el rendimiento se maximiza.

Con TCP ordinario, las conexiones de larga duración (que han tenido tiempo de aprovechar todo el ancho de banda) tienden a exprimir las conexiones de corta duración. Este problema, que arruina la capacidad de respuesta interactiva, no ocurre con el control de flujo.

El control de flujo es una característica estándar en todos los dispositivos de la familia Citrix SD-WAN WANOP.

Ilustración 1. La aceleración mejora el rendimiento de forma transparente



Optimización de velocidad

April 23, 2021

La mayoría de las implementaciones TCP no funcionan bien sobre los enlaces WAN. Por nombrar solo dos problemas, los algoritmos estándar de retransmisión TCP (Reconocimientos selectivos y Recuperación rápida TCP) son inadecuados para enlaces con altas tasas de pérdida, y no tienen en cuenta las necesidades de conexiones transaccionales de corta duración.

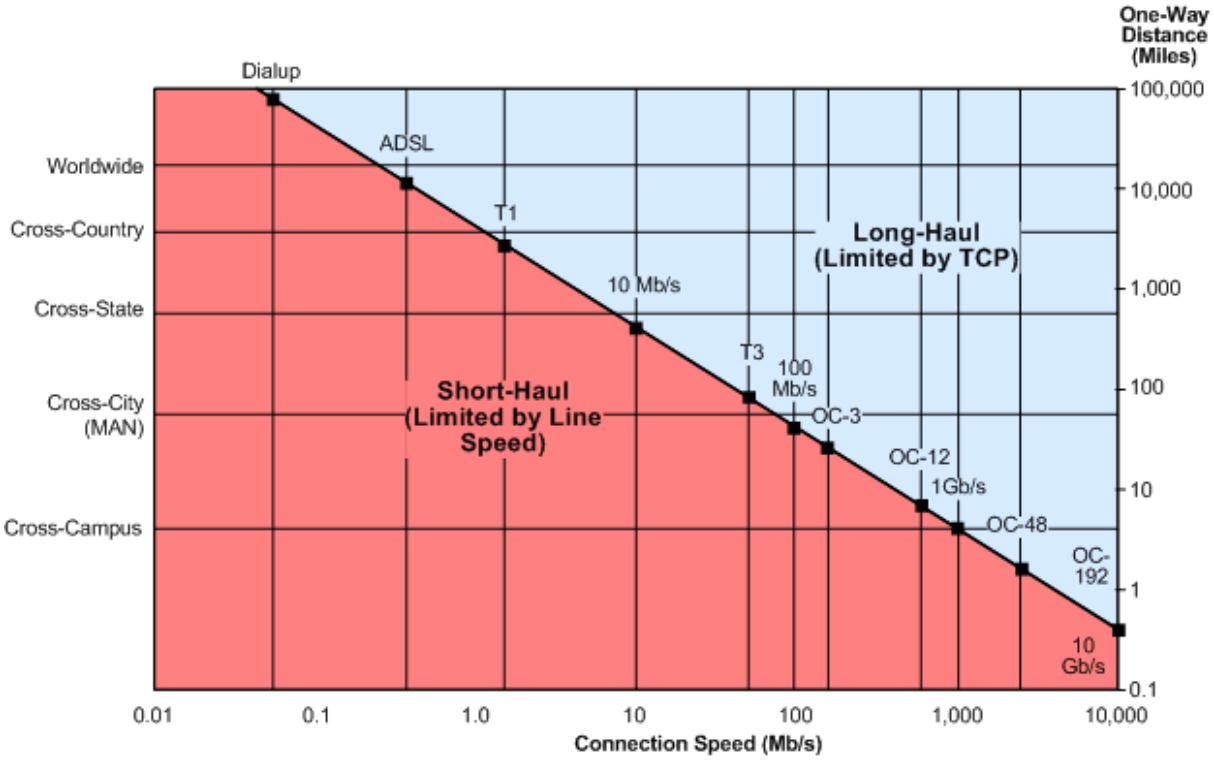
Citrix SD-WAN WANOP implementa un amplio espectro de optimizaciones de WAN para mantener los datos fluyendo en todo tipo de condiciones adversas. Estas optimizaciones funcionan de manera transparente para garantizar que los datos lleguen a su destino lo antes posible.

La optimización WAN funciona de forma transparente y no requiere configuración.

La optimización de WAN es una característica estándar en todos los dispositivos Citrix SD-WAN WANOP.

La siguiente imagen muestra las velocidades de transferencia posibles a varias distancias, sin aceleración, cuando los puntos finales utilizan TCP estándar (TCP Reno). Por ejemplo, las salidas gigabit son posibles sin aceleración dentro de un radio de unas pocas millas, 100 Mbps es alcanzable a menos de 100 millas, y el rendimiento en una conexión mundial está limitado a menos de 1 Mbps, independientemente de la velocidad real del enlace. Con la aceleración, sin embargo, las velocidades por encima de la línea diagonal están disponibles para las aplicaciones. La distancia ya no es un factor limitante.

Ilustración 1. El rendimiento TCP no acelerado se desplome con la distancia



> **Nota**
>
> Sin la aceleración de Citrix, el rendimiento TCP es inversamente proporcional a la distancia, lo que hace imposible extraer el ancho de banda completo de enlaces de larga distancia y alta velocidad. Con la aceleración, el factor de distancia desaparece y la velocidad completa de un enlace se puede usar a cualquier distancia. (Gráfico basado en el modelo de Mathis, *et al,* Pittsburgh Supercomputer Center.)

El rendimiento de transferencia acelerado es aproximadamente igual al ancho de banda del enlace. La velocidad de transferencia no solo es mayor que con TCP no acelerado, sino que también es mucho más constante ante las condiciones cambiantes de la red. El efecto es hacer que las conexiones

distantes se comporten como si fueran locales. La capacidad de respuesta percibida por el usuario permanece constante independientemente de la utilización del enlace. A diferencia de TCP normal, con el que una WAN que opera con un 90% de utilización es inútil para tareas interactivas, un enlace acelerado tiene la misma capacidad de respuesta en un 90% de utilización de enlaces que en un 10%.

Con conexiones de corto alcance (las que caen por debajo de la línea diagonal en la imagen anterior), poca o ninguna aceleración se produce en buenas condiciones de red, pero si la red se degrada, el rendimiento disminuye mucho más lentamente que con TCP ordinario.

El tráfico no TCP, como UDP, no se acelera. Sin embargo, sigue siendo administrado por el formador de tráfico.

Ejemplo

Un ejemplo de optimizaciones TCP avanzadas es una optimización de retransmisión llamada *modo transaccional*. Una peculiaridad de TCP es que, si se elimina el último paquete de una transacción, el remitente no notará su pérdida hasta que haya transcurrido un período de tiempo de espera del receptor (RTO). Este retraso, que siempre es de al menos un segundo de largo, y a menudo más largo, es la causa de los retrasos de varios segundos que se observan en los enlaces con pérdidas, que hacen que las sesiones interactivas sean desagradables o imposibles.

El modo transaccional resuelve este problema retransmitiendo automáticamente el paquete final de una transacción después de un breve retraso. Por lo tanto, un RTO no ocurre a menos que se eliminen ambas copias, lo cual es poco probable.

Una transferencia masiva es básicamente una sola transacción enorme, por lo que el ancho de banda adicional utilizado por el modo transaccional para una transferencia masiva puede ser tan pequeño como un paquete por archivo. Sin embargo, el tráfico interactivo, como pulsaciones de teclas o movimientos del ratón, tiene pequeñas transacciones. Una transacción puede consistir en un solo paquete de tamaño inferior. El envío de estos paquetes dos veces tiene un modesto requisito de ancho de banda. En efecto, el modo transaccional proporciona corrección de errores de reenvío (FEC) en el tráfico interactivo y proporciona protección de RTO al final de la transacción a otro tráfico.

Detección automática y configuración automática

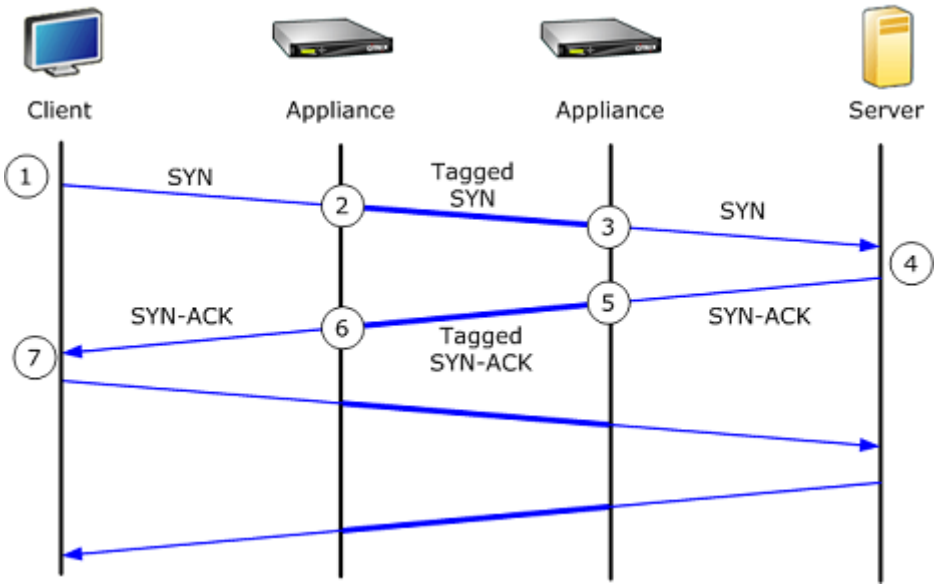
April 23, 2021

En el proceso denominado autodescubrimiento, las unidades WANOP de Citrix SD-WAN detectan automáticamente la presencia del otro. Los dispositivos adjuntan opciones de encabezado TCP a los

primeros paquetes de cada conexión: el paquete SYN (enviado por el cliente al servidor para abrir la conexión) y el paquete SYN-ACK (enviado por el servidor al cliente para indicar que la conexión ha sido aceptada). Al etiquetar los paquetes SYN y escuchar los paquetes SYN y SYN-ACK etiquetados, los dispositivos pueden detectar la presencia de los demás en tiempo real, conexión por conexión.

La principal ventaja de la detección automática es que no es necesario volver a configurar todos los dispositivos cada vez que agregue uno nuevo a la red. Se encuentran automáticamente. Además, el mismo proceso permite la configuración automática. Los dos dispositivos utilizan las opciones de encabezado TCP para intercambiar parámetros operativos, incluidos los límites de ancho de banda (tanto en las direcciones de envío como de recepción), el modo de aceleración básica (hardboost o softboost) y los modos de compresión aceptables (disco, memoria o ninguno). Toda la información que necesita cada dispositivo sobre su socio se intercambia con cada conexión, lo que permite variaciones por conexión (por ejemplo, variaciones por clase de servicio en los tipos de compresión permitidos).

Ilustración 1. Cómo funciona la detección automática



El proceso de autodescubrimiento funciona de la siguiente manera:

1. El cliente abre una conexión TCP al servidor, como de costumbre, enviándole un paquete TCP SYN.
2. El primer dispositivo pasa el paquete SYN después de adjuntar un conjunto de opciones de encabezado TCP específicas del dispositivo y ajustar su tamaño de ventana.
3. El segundo dispositivo lee las opciones TCP, las elimina del paquete y las reenvía al servidor.
4. El servidor acepta la conexión respondiendo como de costumbre con un paquete TCP SYN-ACK.
5. El segundo dispositivo recuerda que esta conexión es candidata a la aceleración y adjunta sus propias opciones de aceleración al encabezado SYN-ACK.

6. El primer dispositivo lee las opciones agregadas por el segundo dispositivo, las elimina del encabezado del paquete y reenvía el paquete al cliente. La conexión ahora se acelera. Los dos dispositivos han intercambiado los parámetros necesarios a través de los valores de opción, y los almacenan en la memoria durante la duración de la conexión.

La conexión se acelera y la aceleración es transparente para el cliente, el servidor, los enrutadores y los firewalls.

Modos de control de flujo TCP

April 23, 2021

El control de flujo TCP tiene dos modos: softboost y hardboost.

Softboost utiliza un remitente basado en velocidad que envía tráfico acelerado a velocidades hasta el límite de ancho de banda del enlace. Si el límite de ancho de banda se establece ligeramente inferior a la velocidad del enlace, la pérdida de paquetes y la latencia se minimizan, mientras que la utilización del enlace se maximiza. Las aplicaciones interactivas ven tiempos de respuesta rápidos, mientras que las aplicaciones de transferencia masiva ven un ancho de banda elevado. Softboost comparte la red con otras aplicaciones en cualquier topología e interactúa con sistemas QoS de terceros.

Hardboost es más agresivo que softboost. Al ignorar las pérdidas de paquetes y otras llamadas señales de congestión, funciona muy bien en enlaces plagados de pérdidas pesadas, no relacionadas con la congestión, como enlaces satelitales. También es excelente en enlaces de larga distancia de baja calidad con una alta pérdida de paquetes en segundo plano, como muchos enlaces en el extranjero. Hardboost se recomienda solo para enlaces punto a punto que no logran un rendimiento adecuado con softboost.

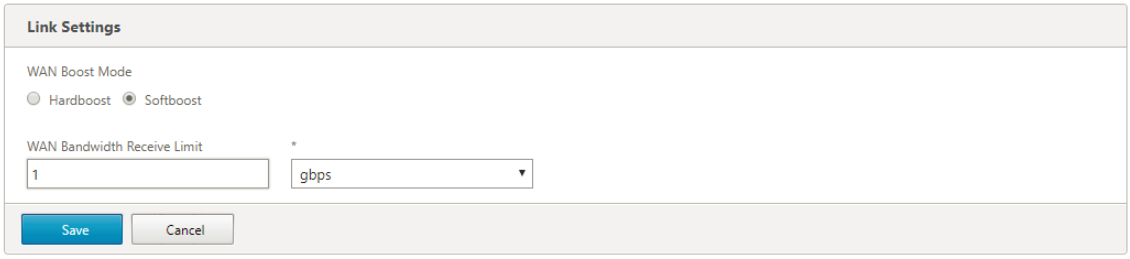
Softboost es el modo predeterminado y se recomienda en la mayoría de los casos.

> **Nota**
>
> - Hardboost solo debe utilizarse en enlaces punto a punto de velocidad fija o implementaciones de hub y radio donde el ancho de banda del hub sea al menos igual a la suma de los anchos de banda de radio acelerados.
> - Softboost y hardboost son mutuamente excluyentes, lo que significa que todos los dispositivos que deben comunicarse entre sí deben establecerse de la misma manera. Si una unidad está configurada en hardboost y la otra en softboost, no se produce ninguna aceleración.

Para seleccionar el modo softboost:

Softboost es el modo predeterminado y se recomienda en la mayoría de los casos.

1. Vaya a **Configuración** > **Enlaces** > **Hardboost/Softboost** y haga clic en Editar.
2. Seleccione**Softboost**como**Modo Boost WAN**.



3. Haga clic en **Guardar**

Para seleccionar el modo hardboost:

Seleccione el modo hardboost solo en enlaces punto a punto de velocidad fija o enlaces hub and spoke donde el ancho de banda del hub sea mayor o igual que el de los enlaces radial acelerados.

1. Vaya a **Configuración** > **Enlaces** > **Hardboost/Softboost** y haga clic en Editar.
2. Seleccione **Hardboost**como**Modo Boost WAN**.
3. Establezca el**límite de recepción de ancho de banda WAN**en 95% de la velocidad del enlace
4. Haga clic en **Guardar**.

Consideraciones sobre el firewall

April 23, 2021

El uso de opciones TCP por parte del dispositivo Citrix SD-WAN WANOP pone en riesgo el tráfico acelerado de cortafuegos que tienen reglas agresivas para denegar el servicio a conexiones mediante opciones TCP menos comunes.

Algunos firewalls quitan las opciones desconocidas y luego reenvían el paquete. Esta acción evita la aceleración pero no afecta la conectividad.

Otros firewalls niegan el servicio a conexiones con opciones desconocidas. Es decir, el firewall elimina los paquetes SYN con las opciones WANOP de Citrix SD-WAN. Cuando el dispositivo detecta errores repetidos en los intentos de conexión, vuelve a intentarlo sin las opciones. Esto restaura la conectividad después de un retraso de longitud variable, generalmente en el rango de 20-60 segundos, pero sin aceleración.

Cualquier firewall que no pase las opciones de Citrix SD-WAN WANOP a través de no modificar debe reconfigurarse para aceptar opciones TCP en el intervalo de 24 a 31 (decimal).

La mayoría de los firewalls no bloquean estas opciones. Sin embargo, los firewalls de Cisco ASA y PIX (y tal vez otros) con firmware de la versión 7.x podrían hacerlo de forma predeterminada.

Se deben examinar los firewalls en ambos extremos del vínculo, ya que cualquiera de ellos podría permitir opciones en las conexiones salientes pero bloquearlas en las conexiones entrantes.

El siguiente ejemplo debería funcionar con firewalls ASA 55x0 de Cisco con firmware 7.x. Debido a que globalmente permite opciones en el rango de 24-31, no hay configuración personalizada por interfaz o por unidad:

```
 ====================================================================
 CONFIGURATION FOR CISCO ASA 55X0 WITH 7.X CODE TO ALLOW TCP OPTIONS
 ====================================================================
 hostname(config)# tcp-map WSOptions
 hostname(config-tcp-map)# tcp-options range 24 31 allow
 hostname(config-tcp-map)# class-map WSOptions-class
 hostname(config-cmap)# match any
 hostname(config-cmap)# policy-map WSOptions
 hostname(config-pmap)# class WSOptions-Class
 hostname(config-pmap-c)# set connection advanced-options WSOptions
 hostname(config-pmap-c)# service-policy WSOptions global
<!--NeedCopy-->
```

La configuración de un firewall PIX es similar:

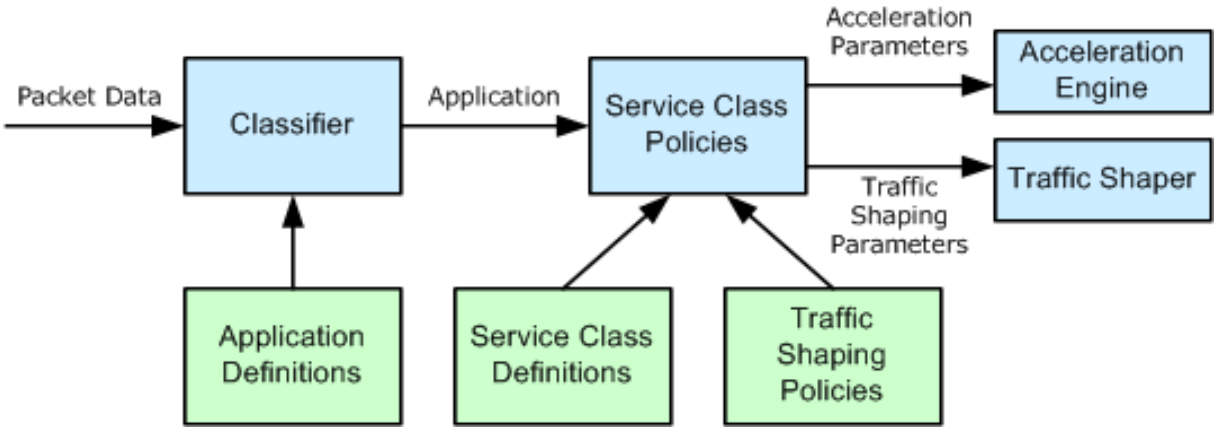
```
 ====================================================
 POLICY MAP TO ALLOW APPLIANCE TCP OPTIONS TO PASS (PIX 7.x)
 ====================================================
 pixfirewall(config)#access-list tcpmap extended permit tcp any any
 pixfirewall(config)# tcp-map tcpmap
 pixfirewall(config-tcp-map)# tcp-opt range 24 31 allow
 pixfirewall(config-tcp-map)# exit
 pixfirewall(config)# class-map tcpmap
 pixfirewall(config-cmap)# match access-list tcpmap
 pixfirewall(config-cmap)# exit
 pixfirewall(config)# policy-map global_policy
 pixfirewall(config-pmap)# class tcpmap
 pixfirewall(config-pmap-c)# set connection advanced-options tcpmap
<!--NeedCopy-->
```

Clasificación del tráfico

April 23, 2021

Las dos funciones principales de un dispositivo Citrix SD-WAN WANOP son el modelado del tráfico, que maximiza el uso de enlaces para todos los tipos de tráfico, y la aceleración, que aplica compresión y varias optimizaciones para acelerar el tráfico TCP. Dos componentes básicos del modelado y la

aceleración del tráfico son el mecanismo del clasificador de aplicaciones y el mecanismo de clase de servicio. El primero identifica el tipo de tráfico, de modo que el segundo puede asignar el tráfico a una clase de servicio. Cada clase de servicio tiene una directiva de modelado de tráfico y una directiva de aceleración.



Clasificador de aplicaciones

April 23, 2021

El clasificador de aplicaciones utiliza definiciones de aplicación para categorizar el tráfico por protocolo y aplicación. Esta información se utiliza para crear informes, y por el mecanismo de clase de servicio. Muchas aplicaciones ya están definidas, y puede definir más según sea necesario.

Especificaciones de protocolo y puerto en las definiciones de aplicaciones

El clasificador de aplicaciones utiliza el protocolo oficial y las especificaciones de puerto de Internet Assigned Numbers Authority (IANA) http://www.iana.org. A veces, aplicaciones distintas de las oficiales utilizan un puerto. Por lo general, el clasificador no puede detectar dicho uso. Si la red utiliza dichas aplicaciones, normalmente puede resolver este problema cambiando el nombre de la aplicación, en el clasificador de aplicaciones, para indicar la aplicación real que utiliza este puerto en la red. Por ejemplo, si utiliza el puerto 3128 no para su uso estándar para una caché web de Squid, sino para un proxy SOCKS, podría cambiar el nombre de la aplicación Squid (TCP) a SOCKS (puerto 3128) para mayor claridad.

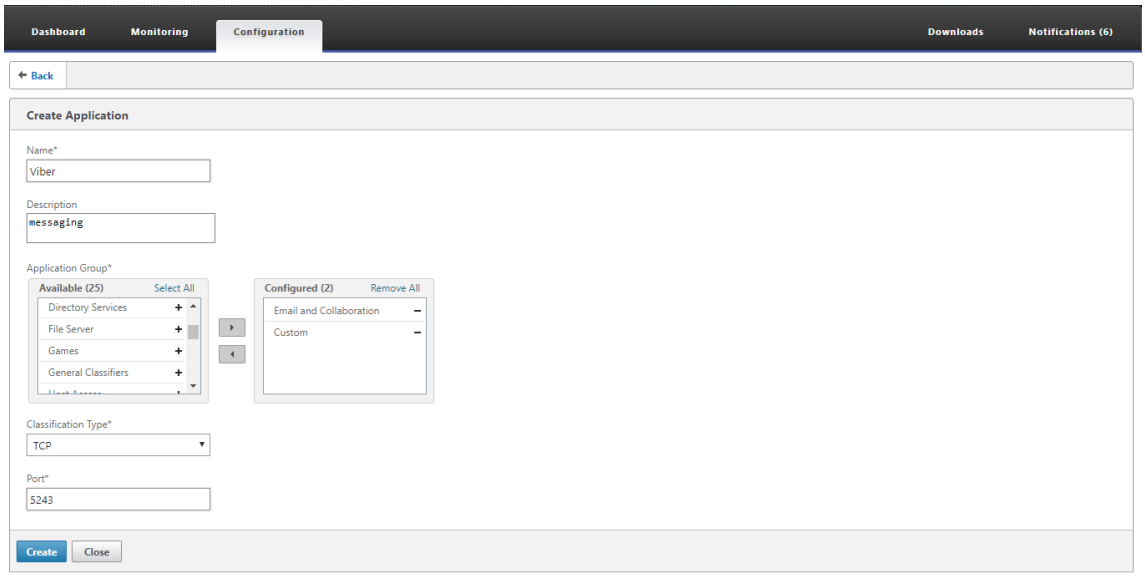
Las aplicaciones no deben tener definiciones superpuestas. Por ejemplo, si una aplicación de la red utiliza los puertos TCP 3120 y 3128 y otra aplicación utiliza el puerto 3120, solo una definición de aplicación Citrix SD-WAN WANOP puede incluir el puerto 3120.

Configurar definiciones de aplicaciones

- TCP dinámico, para aplicaciones que utilizan asignaciones de puertos dinámicos
- Tipo de éter, para tipos de paquetes Ethernet
- Aplicación publicada ICA, para aplicaciones de Virtual Apps/Virtual Desktops
- IP, para protocolos IP como ICMP o GRE
- TCP, para aplicaciones TCP
- UDP, para aplicaciones UDP
- Dirección web, para sitios web o dominios específicos.

Para configurar la defensa de aplicaciones:

1. Vaya a**Configuración**>**Reglas de optimización**>**Clasificadores de aplicaciones** y haga clic en **Agregar**.



2. En la página **Crear Aplicación**, defina los siguientes parámetros:

   - **Nombre**: Nombre del clasificador de aplicaciones. Debe comenzar con un carácter alfanumérico o de subrayado (_) ASCII y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), dos puntos (:), en (@), igual (=) y guión (-). Longitud máxima: 31 caracteres.
   - **Descripción** - Descripción del clasificador de aplicaciones.
   - **Grupo de aplicaciones**: El clasificador de aplicaciones pertenece a este grupo de aplicaciones. Los grupos de aplicaciones son un conjunto de grupos predefinidos de aplicaciones que se clasifican en función de su funcionalidad.

- **Tipo de clasificación**: Clasificación de alto nivel que desea utilizar para este clasificador de aplicaciones. La clasificación de alto nivel se realiza principalmente sobre la base del puerto que usa una aplicación.
- **Puerto**: El número de puerto que se va a utilizar. Puede introducir un rango, una lista o un número entre 0 y 65535.

3. Haga clic en **Crear**.

   La página **Clasificadores de aplicaciones** muestra todas las aplicaciones reconocidas por el clasificador SD-WAN WANOP.

La página**Clasificadores de aplicaciones** muestra todas las aplicaciones reconocidas por el clasificador SD-WAN WANOP.

> **Sugerencia**
>
> Haga clic en **Detección automática** para permitir que todas las aplicaciones publicadas de Citrix que se vean en la secuencia de datos se agreguen automáticamente a la lista de aplicaciones. Una vez descubiertos, aparecerán en los informes y se pueden utilizar para las directivas de configuración del tráfico.

Clases de servicio

April 23, 2021

A las clases de servicio se les asignan directivas de modelado de tráfico y directivas de aceleración que se utilizarán para todas las conexiones que coincidan con la definición de clase de servicio. Las clases de servicio pueden basarse en los siguientes parámetros:

- Aplicaciones
- Direcciones IP o VLAN
- bits DSCP
- Perfiles SSL

Las definiciones de clase de servicio predeterminadas se recomiendan como punto de partida. Modifíquelos si resultan inadecuados para sus enlaces.

Las clases de servicio se definen en una lista ordenada. La primera definición que coincide con el tráfico que se está procesando se convierte en la clase de servicio para el tráfico.

Diferencias entre las decisiones de aceleración y las directivas de configuración del tráfico

Para tomar una decisión de aceleración, el dispositivo Citrix SD-WAN WANOP examina el paquete SYN inicial de cada conexión TCP para determinar si la conexión es un candidato para la aceleración. El paquete SYN no contiene carga útil, solo encabezados, por lo que la decisión de aceleración debe basarse en el contenido de los encabezados del paquete SYN, como el puerto de destino o la dirección IP de destino de la conexión. La aceleración, una vez aplicada, dura la duración de la conexión.

A diferencia de las decisiones de aceleración, las directivas de modelado del tráfico se pueden basar en el contenido de la secuencia de datos de la conexión. Dependiendo del tiempo que tarda el clasificador de aplicaciones en recibir suficientes datos para una clasificación final, una conexión puede ser reclasificada durante su vida útil.

Por ejemplo, el primer paquete de una conexión HTTP a `http://www.example.com` es un paquete SYN que contiene un encabezado pero sin carga útil. El encabezado tiene un puerto de destino IP 80, que coincide con la definición de clase de servicio HTTP: Internet, por lo que el motor de aceleración basa su decisión de aceleración, en este caso, ninguna (sin aceleración) en esa clase de servicio.

El modelador de tráfico utiliza la directiva de modelado de tráfico de la clase de servicio HTTP: Internet, pero esta decisión es temporal. El primer paquete de carga útil contiene la cadena GET `http://www.example.com`, que coincide con la definición de aplicación de ejemplo en el clasificador de aplicaciones. La clase de servicio que incluye la aplicación de ejemplo es seleccionada por el shaper de tráfico, en lugar de la clase de servicio que incluye HTTP: Internet, y el shaper de tráfico utiliza la directiva de clase de servicio nombrada en esa definición de clase de servicio.

> **Nota**
>
> Independientemente de la directiva de clase de servicio, la característica de informes realiza un seguimiento del uso de la aplicación de ejemplo.
>
> **Importante**
>
> Todo el tráfico está asociado a una aplicación y una clase de servicio, y todas las clases de servicio tienen una directiva de modelado de tráfico, pero sólo las conexiones TCP tienen una directiva de aceleración distinta de ninguna.

Configurar definiciones de clases de servicio

Dado que las definiciones de clase de servicio son una lista ordenada, una definición que es una excepción a un caso general debe preceder a la definición más general en la página de clase de servicio. La primera definición cuya regla coincide con el tráfico es la que se aplica. Por ejemplo:

- Las clases de servicio basadas en direcciones URL deben preceder a las clases de servicio HTTP en la lista de clases de servicio, ya que cualquier regla basada en URL también coincide con la clase de servicio HTTP. Por lo tanto, poner primero la clase de servicio HTTP impediría que las reglas basadas en URL o las reglas basadas en aplicaciones publicadas se usaran nunca.
- Del mismo modo, las clases de servicio basadas en las aplicaciones publicadas ICA (VirtualApps y Virtual Desktops) deben preceder a la clase de servicio Citrix.

Dado que todas las reglas basadas en URL coinciden con la clase de servicio HTTP, poner la clase de servicio HTTP por encima de ellas daría como resultado que nunca se usaran las reglas basadas en URL o las reglas basadas en aplicaciones publicadas.

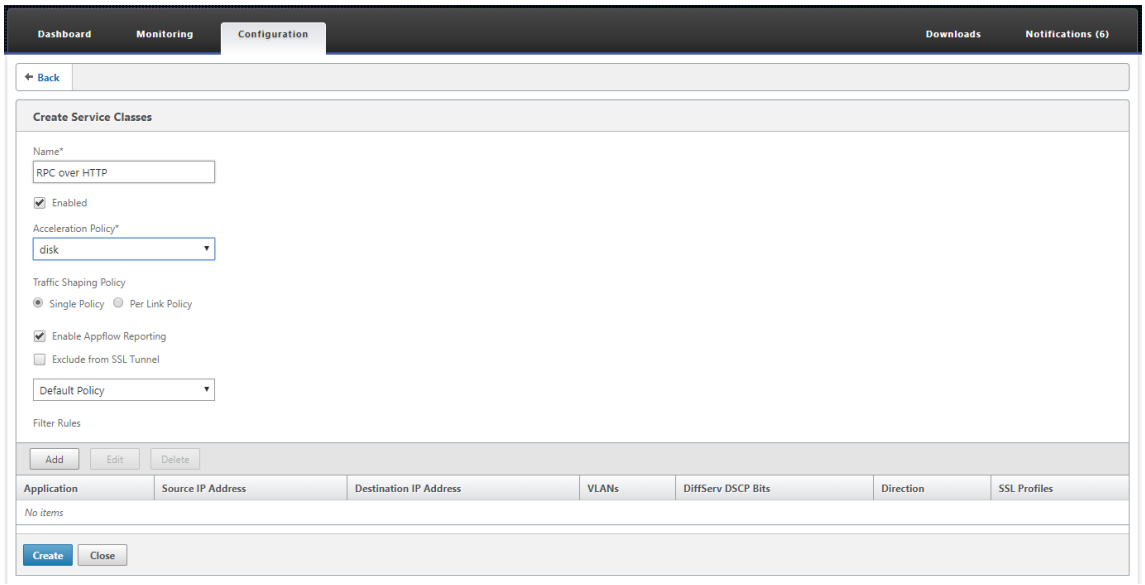
Configuration Overview > Optimization Rules > **Service Classes**

Add | Edit | Delete | Update Order | Filter Rules | Show User Modified Service Classes Only

Order	Name	Status	Acceleration Policy	Traffic Shaping Policy	Appflow Reporting Status
1	ICA	Enabled	disk	ICA Priorities	Enabled
2	Web (Private)	Enabled	disk	Default Policy	Enabled
3	Web (Private-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
4	Web (Internet)	Enabled	disk	Default Policy	Enabled
5	Web (Internet-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
6	CIFS	Enabled	disk	Default Policy	Enabled
7	NFS	Enabled	disk	Default Policy	Enabled
8	Microsoft Exchange (MAPI)	Enabled	disk	Default Policy	Enabled
9	Mail (Other)	Enabled	disk	Default Policy	Enabled
10	VOIP and Multimedia	Enabled	None	VOIP Traffic	Enabled
11	VOIP Webcam	Enabled	None	High Priority Traffic	Enabled
12	FTP Data	Enabled	disk	Low Priority Traffic	Enabled
13	FTP Control	Enabled	Flow Control Only	Default Policy	Enabled
14	Instant Messaging	Enabled	disk	Default Policy	Enabled
15	Session Applications	Enabled	Flow Control Only	Default Policy	Enabled
16	Directory and Security	Enabled	Flow Control Only	Default Policy	Enabled
17	Database Applications	Enabled	Flow Control Only	Default Policy	Enabled
18	Secure Applications	Enabled	Flow Control Only	Default Policy	Enabled
19	Iperf	Enabled	Flow Control Only	Low Priority Traffic	Enabled
20	NetApp SnapMirror	Enabled	memory	Default Policy	Enabled
21	Other TCP Traffic	Enabled	None	Default Policy	Enabled
22	Unclassified Traffic	Enabled	None	Default Policy	Enabled

Para crear una clase de servicio RPC sobre HTTP y enlazar el perfil SSL a ella:

1. Vaya a **Configuración**>**Reglas de optimización**>**Clases de servicio**y haga clic en **Agregar**.

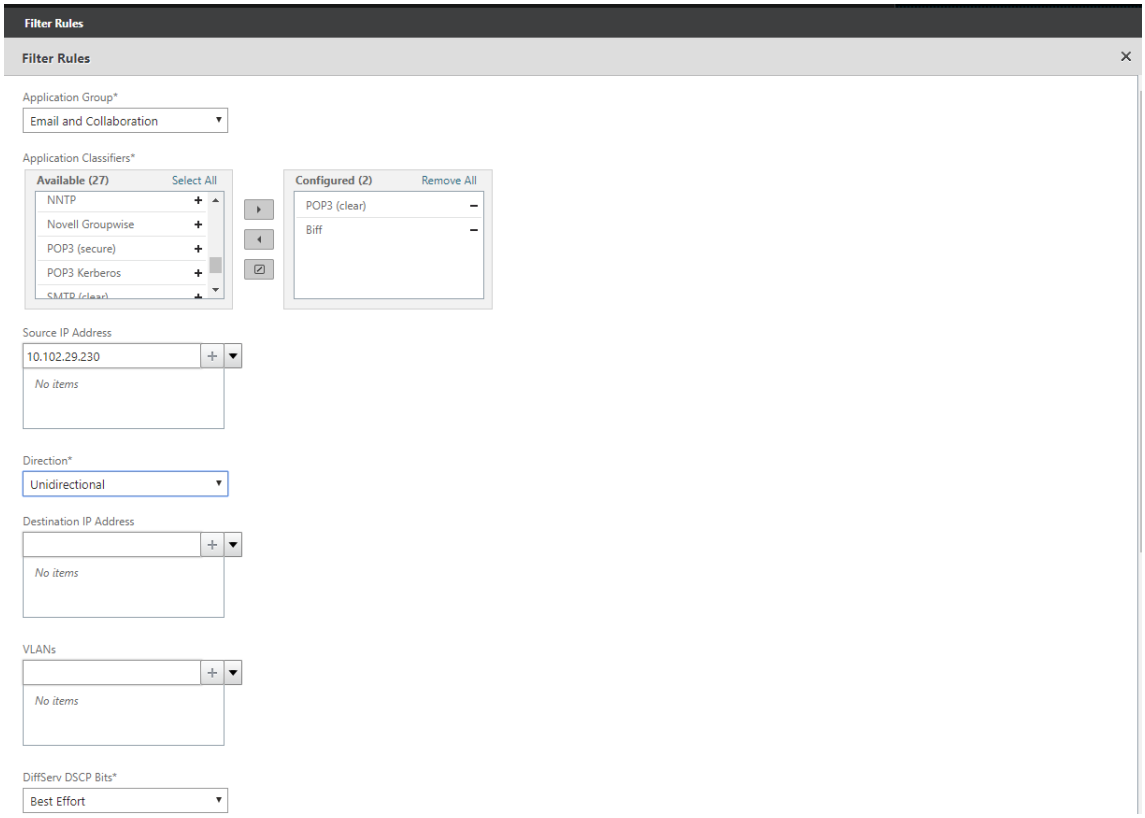


2. En el campo **Nombre**, introduzca un nombre para la clase de servicio.
3. Asegúrese de que la opción**Habilitado**está seleccionada.
4. En la lista **Directiva de aceleración**, seleccione una directiva de aceleración.**Memoria**y**disco**especifican dónde almacenar el historial de tráfico utilizado para la compresión.El**disco**suele ser la mejor opción, ya que el dispositivo selecciona automáticamente el disco o la memoria, dependiendo de cuál sea más apropiado para el tráfico.**La memoria**especifica sólo memoria. Seleccione**Sólo control de flujo** para desactivar 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.**Ninguno**se utiliza sólo para tráfico cifrado no comprimible y vídeo en tiempo real.
5. Seleccione**Habilitar informes de AppFlow**para habilitar los informes de AppFlow para esta clase de servicio. La información de esta clase de servicio se incluye en cualquier informe de AppFlow. 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 AppFlow.
6. Seleccione **Excluir del túnel SSL**para excluir el tráfico asociado a la clase de servicio del túnel SSL.
7. En la lista de directivas de modelado de tráfico, asegúrese de que está seleccionada la opción**Directiva predeterminada**. Las directivas de modelado de tráfico tienen una prioridad ponderada y otros atributos que determinan cómo se tratará el tráfico coincidente, en relación con el otro tráfico. La mayoría de las clases de servicio se establecen en Directiva predeterminada, pero al tráfico de mayor prioridad se le puede asignar una directiva de modelado de

tráfico de mayor prioridad y al tráfico de menor prioridad se le puede asignar una directiva de menor prioridad.

8. En la sección Reglas de filtro, haga clic en**Agregar**para crear una regla de filtro que tenga Cualquiera como valor predeterminado para todos los parámetros. Si una regla se evalúa como TRUE para una conexión dada, la conexión se asigna a esa clase de servicio. Las reglas de filtro para la mayoría de las clases de servicio consisten únicamente en una lista de aplicaciones, pero las reglas también pueden incluir direcciones IP, etiquetas VLAN, valores DSCP y nombres de perfil SSL. Todos los campos de una regla por defecto son Cualquiera (un comodín). Los campos dentro de una regla se unen.

9. Haga clic en **Agregar** para agregar reglas de filtro.



10. En la lista **Grupo de aplicaciones**, seleccione **Correo electrónico y colaboración**.

11. En la lista**Disponible**, seleccione las aplicaciones necesarias.

12. Mueva las aplicaciones seleccionadas a la lista**Configurado**.

13. En el campo **Direcciones IP de origen**, agregue las direcciones IP del cliente.

14. En la lista **Dirección**, seleccione la dirección del tráfico.

15. En la lista **Perfiles SSL**, seleccione el perfil SSL que ha creado.

16. Haga clic en **Crear**.

> **Nota**
>
> - Debe configurar y enlazar un perfil SSL a la clase de servicio solo en el dispositivo del centro de datos.
> - Solo las clases de servicio que tienen su dirección de reglas de filtro establecida en unidireccional se pueden asociar con perfiles SSL.

Modelado del tráfico

April 23, 2021

18 abr. 2018

El modelado del tráfico le permite regular el flujo de tráfico de red para asegurar un cierto nivel de calidad de servicio (QoS). Puede regular el flujo de paquetes a una red (limitación de ancho de banda) o fuera de una red (limitación de velocidad).

Mediante directivas de modelado de tráfico, puede establecer la prioridad del tráfico de vínculos diferente y enviar tráfico al enlace a una velocidad cercana, pero no mayor que, a la velocidad del enlace. A diferencia de la aceleración, que solo se aplica al tráfico TCP/IP, el formador de tráfico controla todo el tráfico del vínculo.

Puede establecer un ancho de banda alto para los flujos de tráfico que se consideran más importantes que el resto de los flujos de tráfico, lo que le permite utilizar de manera óptima los escasos recursos de enlace.

El modelado del tráfico se basa en la cola justa ponderada, lo que da a cada clase de servicio su parte justa del ancho de banda del enlace. Si el enlace está inactivo, cualquier conexión (en cualquier clase de servicio) puede usar el enlace completo. Cuando varias conexiones compiten por el ancho de banda de enlace, el formador de tráfico aplica directivas de modelado de tráfico para determinar la combinación correcta de tráfico.

Para obtener información sobre la cola de valores ponderados, consulte Cola justa ponderada.

Para configurar el modelado del tráfico:

1. Configure la definición de vínculo.

   El conformador de tráfico utiliza la definición de enlace para determinar la velocidad de envío y recepción del enlace y otra información relacionada con el enlace. Para obtener más información sobre cómo el modelador de tráfico utiliza la definición de vínculos y cómo configurar definiciones de vínculos, consulte Definiciones de vínculos.

2. Configure la definición de la aplicación.

   El clasificador de aplicaciones examina el tráfico que fluye a través del vínculo para determinar a qué aplicación pertenece y, a continuación, la aplicación se busca en la lista de clases de servicio para determinar a qué clase de servicio pertenece. Para obtener más información sobre la clasificación de aplicaciones y cómo configurar la definición de aplicaciones, consulte Clasificación del tráfico.

3. Cree una directiva de modelado de tráfico.

   Puede utilizar las directivas de modelado de tráfico predeterminadas o crear una nueva directiva para establecer la prioridad ponderada y otros parámetros según sus requisitos de red. Para obtener información sobre la creación de directivas de modelado de tráfico, consulte Directivas de modelado de tráfico.

4. Configure una definición de clase de servicio y asocie la directiva de modelado de tráfico a la clase de servicio.

   Para obtener información sobre la configuración de la definición de clase de servicio, consulte Clases de Servicio.

Algunos aspectos destacados del conformador de tráfico:

- Todo el tráfico WAN está sujeto a la configuración del tráfico: conexiones aceleradas, conexiones no aceleradas y tráfico no TCP, como flujos UDP y flujos GRE.
- El algoritmo es una cola justa ponderada, en la que el administrador asigna una prioridad a cada clase de servicio. Cada clase de servicio representa un grupo de ancho de banda, con derecho a una fracción mínima de la velocidad del enlace, igual a (my_priority/sum_of_all_priorities). Una clase de servicio con una prioridad ponderada de 100 obtiene el doble de ancho de banda que una clase de servicio con una prioridad ponderada de 50. Puede asignar pesos de 1 a 256.
- Cada conexión dentro de una clase de servicio obtiene una parte igual del ancho de banda asignado a esa clase de servicio.
- Cada conexión obtiene su parte justa del ancho de banda del enlace, ya que las prioridades se aplican a los datos WAN reales transferidos, después de la compresión. Por ejemplo, si tiene dos flujos de datos con la misma prioridad, uno con compresión 10:1 y el otro con compresión 2:1, los usuarios verán una diferencia 5:1 en rendimiento, aunque el uso del vínculo WAN de las dos conexiones sea idéntico. En la práctica, esta disparidad es deseable, porque el ancho de banda WAN, no el ancho de banda de aplicaciones, es el escaso recurso que se necesita administrar.
- Las directivas de configuración del tráfico se aplican por igual al tráfico acelerado y no acelerado. Por ejemplo, una conexión acelerada de Virtual Apps y una conexión de Virtual Apps no acelerada reciben modelado de tráfico, por lo que ambos pueden tener una prioridad elevada en comparación con el tráfico masivo. Como otro ejemplo, puede acelerarse el tráfico no TCP sensible al tiempo, como VoIP (que utiliza el protocolo UDP).

- El modelado del tráfico se aplica al enlace WAN tanto en las direcciones de envío como de recepción, tanto en el tráfico acelerado como en el no acelerado. Esta función evita la congestión y el aumento de la latencia incluso cuando el otro lado del vínculo no está equipado con un dispositivo Citrix SD-WAN WANOP. Por ejemplo, las descargas de Internet pueden priorizarse y administrarse.
- La directiva de modelado de tráfico para una clase de servicio se puede especificar por vínculo si se desea.
- Además de dar forma al tráfico directamente, el formador de tráfico puede afectarlo indirectamente estableciendo el campo Punto de código de servicios diferenciados (DSCP) para informar a los enrutadores descendentes sobre el tipo de tráfico que requiere cada paquete.

Cola justa ponderada

April 23, 2021

En cualquier vínculo, la Gateway de cuello de botella determina la disciplina de la cola, ya que los datos de las puertas de enlace sin cuello de botella no hacen copia de seguridad. Sin datos pendientes en las colas, el protocolo de cola es irrelevante.

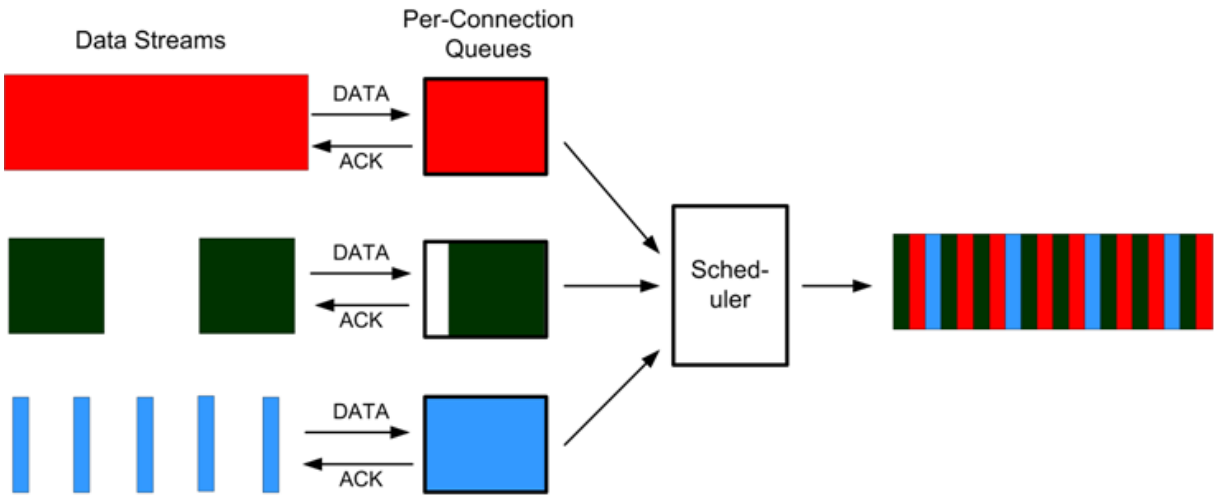
La mayoría de las redes IP utilizan colas FIFO profundas. Si el tráfico llega más rápido que la velocidad del cuello de botella, las colas se llenan y todos los paquetes sufren mayores tiempos de espera. A veces, el tráfico se divide en algunas clases diferentes con FIFO separados, pero el problema persiste. Una sola conexión que envía demasiados datos puede causar grandes retrasos, pérdidas de paquetes o ambas para todas las demás conexiones de su clase.

Un dispositivo WANOP de Citrix SD-WAN utiliza *colas equitativas ponderadas,* que proporciona una cola independiente para cada conexión. Con una cola justa, una conexión demasiado rápida puede desbordar solo su propia cola. No tiene ningún efecto en otras conexiones. Pero debido al control de flujo sin pérdidas, no existe una conexión demasiado rápida, y las colas no se desbordan.

El resultado es que cada conexión tiene su tráfico medido en el enlace de una manera justa, y el enlace en su conjunto tiene un ancho de banda óptimo y un perfil de latencia.

La siguiente imagen muestra el efecto de las colas justas. Una conexión que requiere menos de su parte justa de ancho de banda (la conexión inferior) obtiene tanto ancho de banda como intenta usar. Además, tiene muy poca latencia en cola. Las conexiones que intentan usar más de su cuota justa obtienen su cuota justa, además de cualquier ancho de banda sobrante de conexiones que usan menos de su cuota justa.

Ilustración 1. Colas justas en acción



El perfil de latencia óptimo proporciona a los usuarios de aplicaciones interactivas y transaccionales un rendimiento ideal, incluso cuando comparten el enlace con múltiples transferencias masivas. La combinación de control de flujo transparente y sin pérdidas y la cola justa le permite combinar todo tipo de tráfico en el mismo enlace de forma segura y transparente.

La diferencia entre la cola justa ponderada y la cola justa no ponderada es que la cola justa ponderada incluye la opción de dar a algún tráfico una prioridad (peso) más alta que a otros. El tráfico con un peso de dos recibe el doble del ancho de banda del tráfico con un peso de uno. En una configuración WANOP de Citrix SD-WAN, los pesos se asignan en las políticas de modelado de tráfico.

Directivas de modelado de tráfico

January 10, 2022

Cada definición de clase de servicio está asociada a una directiva de modelado de tráfico, que establece parámetros para el tráfico de la clase de servicio asociada. Puede crear y configurar directivas de modelado de tráfico para sitios con necesidades especiales, pero la configuración predeterminada de directivas funciona correctamente para la mayoría de las instalaciones, proporcionando las siguientes ventajas:

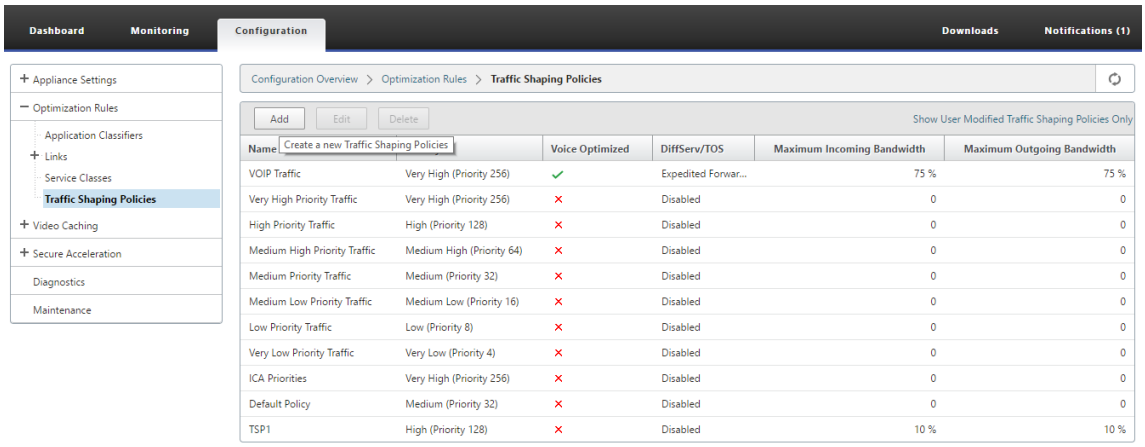
- Mayor capacidad de respuesta para el tráfico interactivo, como Citrix Virtual Apps and Desktops.
- Protección del tráfico VoIP sensible a la latencia y a la fluctuación.
- No hay fatiga durante los períodos de máxima actividad. Obtienes un rendimiento utilizable incluso bajo una carga extrema.
- Mejor utilización del ancho de banda al permitir que las transferencias masivas llenen el enlace con cualquier ancho de banda que quede de las tareas interactivas.

- Ampliación de los beneficios de la cola justa a todo el tráfico

Un dispositivo Citrix SD-WAN WANOP se suministra con políticas de modelado de tráfico predeterminadas de fábrica que abarcan una amplia gama de prioridades. Estas directivas se enumeran en la página **Directivas de modelado de tráfico**. Aparte de la **directiva predeterminada**, las demás directivas predeterminadas de fábrica no se pueden modificar ni eliminar. La razón es garantizar que tengan el mismo significado en todos los dispositivos. Para realizar cambios, cree una directiva de modelado de tráfico con los nuevos parámetros y cambie las definiciones de clase de servicio adecuadas para hacer referencia a la nueva directiva de modelado de tráfico.

Para crear una directiva de modelado de tráfico:

1. En la interfaz de usuario de administración WANOP de SD-WAN, vaya a **Configuración** > **Reglas de optimización** > **Directivas de modelado de tráfico** y haga clic en **Agregar**.

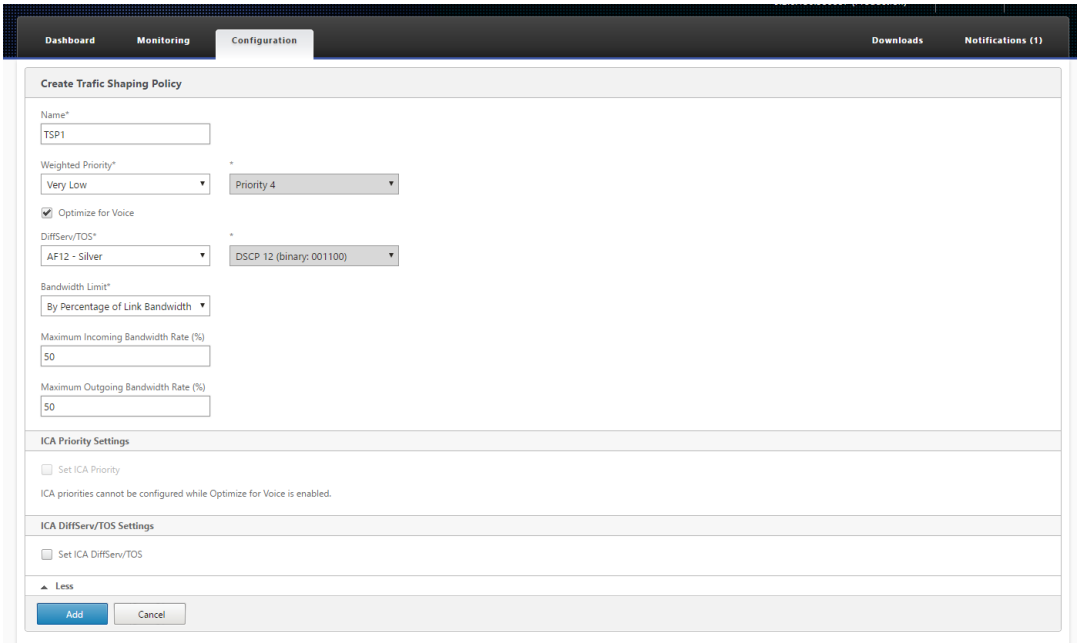


2. En la página **Crear directiva de modelado de tráfico**, introduzca valores para los siguientes parámetros:

   - **Nombre**: Nombre de la nueva directiva. Debe ser único.
   - **Prioridad ponderada**: Puede seleccionar un valor de prioridad existente o un valor personalizado entre 1 y 256. Una conexión con una prioridad de 256 obtendrá 256 veces el recurso compartido de ancho de banda como una conexión con una prioridad de 1.
   - **Optimizar para voz**: Si se selecciona, esta directiva tendrá una prioridad infinita. Esto es altamente indeseable para la mayoría del tráfico, ya que evitará un modelado significativo del tráfico y causará la falta de datos para otro tráfico si hay suficiente tráfico optimizado para voz para llenar el enlace. Utilizar solo para VoIP y utilizar siempre junto con un límite de ancho de banda en la directiva (por ejemplo, 50% de la velocidad del enlace)

     > **Nota**

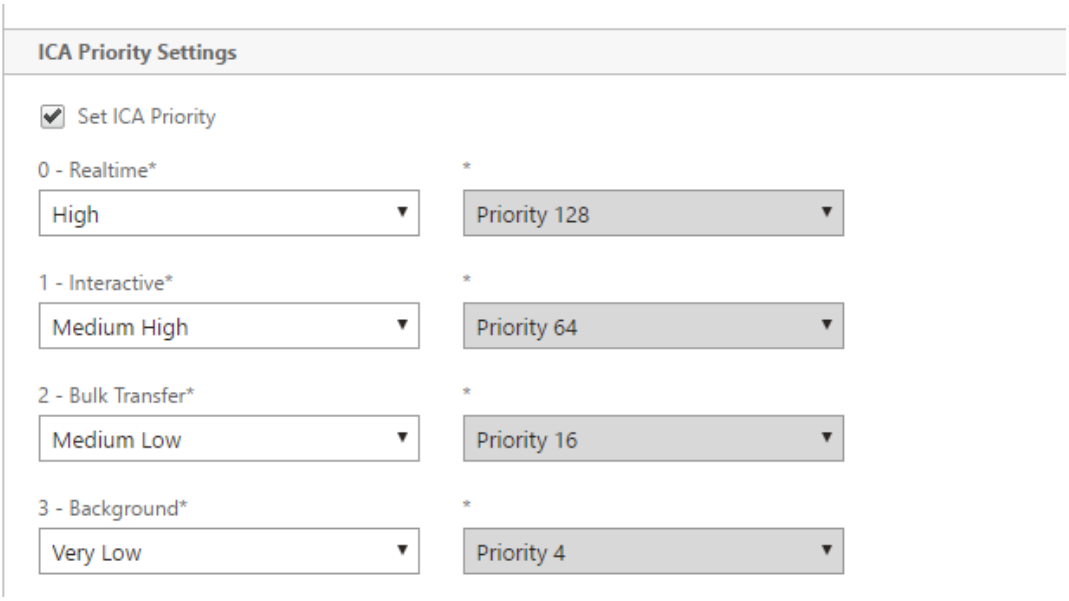
> La optimización de voz no se puede configurar mientras se establecen las prioridades ICA.



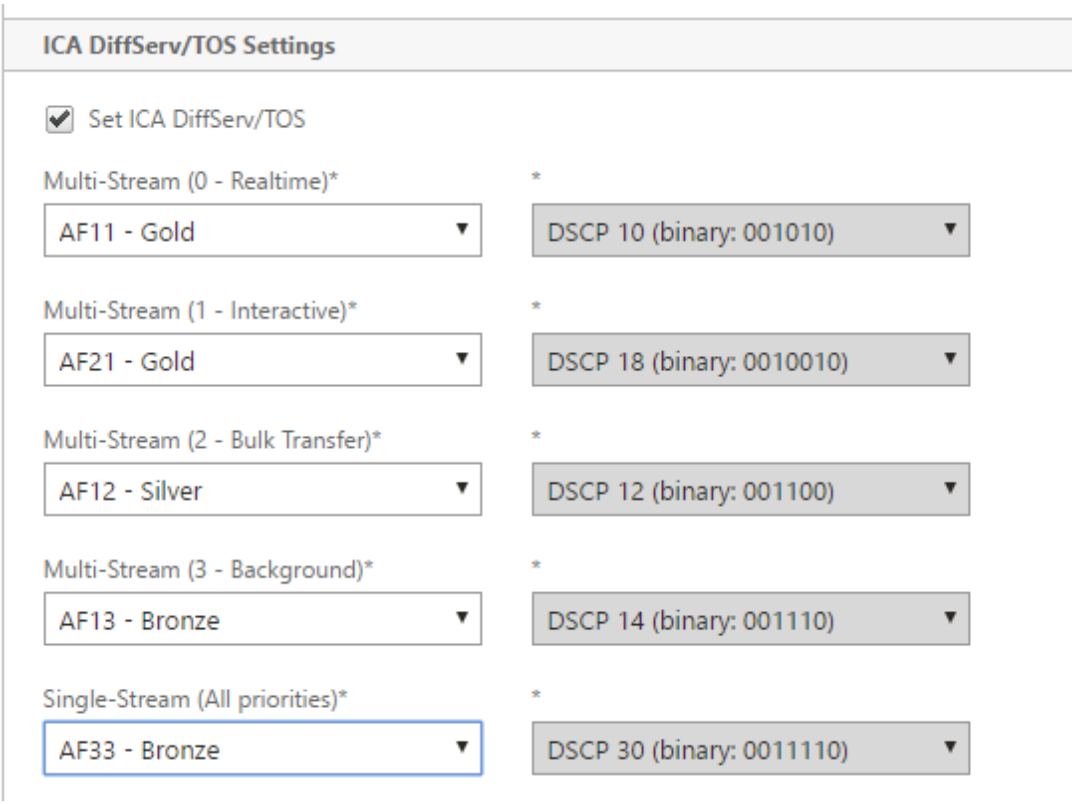
- **Diffserv/TOS**—Establece los bits DSCP en los paquetes de salida en el valor seleccionado. Se utiliza para controlar los enrutadores descendentes.
- **Límite de ancho de banda**: Evita que el tráfico que utiliza esta directiva supere el ancho de banda especificado, indicado como porcentaje de velocidad de enlace o como valor absoluto. Citrix recomienda especificar un porcentaje para que la misma definición pueda aplicarse a vínculos de diferentes velocidades. Esta función puede dejar ancho de banda sin usar. Por ejemplo, una directiva establecida en el 50% de la velocidad del vínculo no permite que el tráfico afectado utilice más del 50% del vínculo, incluso si el vínculo está inactivo. La limitación del tráfico de esta manera no es coherente con el rendimiento máximo, por lo que esta función rara vez se utiliza, excepto con el tráfico VoIP con la configuración Optimizar para voz.

  > **Nota**
  >
  > La configuración del **límite de ancho de banda** sólo se aplica a la edición WANOP de Citrix SD-WAN. Para Citrix SD-WAN PE Edition, el parámetro **Límite de ancho de banda** está inhabilitado de forma predeterminada.

- **Establecer prioridades ICA**: Si esta directiva se utiliza para el tráfico de Citrix Virtual Apps/Virtual Desktops, la prioridad interna del tráfico para el tráfico en tiempo real, interactivo, de transferencia masiva y en segundo plano se sobrescribe por la prioridad establecida aquí.



- **Establecer ICA DiffServ/TOS**: Para el tráfico ICA (Virtual Apps/Virtual Desktops), cada uno de los cuatro valores de prioridad ICA se puede etiquetar con un valor DSCP diferente. Esta prestación es particularmente útil con la nueva función ICA Multistream, en la que el cliente Virtual Apps o Virtual Desktops utiliza diferentes conexiones para diferentes niveles de prioridad.



3. Haga clic en **Agregar**. La directiva de modelado de tráfico recién creada aparece en la lista Di-

rectivas de modelado de tráfico.

Ahora puede asociar la directiva de modelado de tráfico a una clase de servicio; para obtener más información, consulte Clases de Servicio.

Almacenamiento en caché de vídeo

April 23, 2021

Muchas organizaciones utilizan vídeos para comunicaciones que no son sensibles al tiempo (por ejemplo, sesiones de formación y mensajes pregrabados a los empleados). Comunicar mensajes a través de vídeos no solo es rentable, sino también conveniente cuando la audiencia se extiende a través de zonas horarias. Sin embargo, los vídeos consumen mucho ancho de banda cuando se reproducen a través de Internet. El ancho de banda insuficiente provoca latencia, lo que afecta a la experiencia del usuario y degrada el impacto de la comunicación de vídeo.

El almacenamiento en caché de vídeo mejora la experiencia de visualización de secuencias de vídeo HTTP, especialmente en enlaces más lentos. La caché de vídeo se mantiene en el dispositivo local Citrix SD-WAN WANOP. Cuando un usuario local ve un vídeo que ya se ha almacenado en caché, el dispositivo puede entregar la copia almacenada en caché a toda velocidad de LAN.

Después de configurar el dispositivo para almacenar en caché los vídeos, éste almacena en caché los vídeos vistos por los usuarios. También puede utilizar la opción de prerrellenado para obtener vídeos seleccionados del servidor de vídeo local en previsión de su uso posterior.

La función de almacenamiento en caché de vídeo utiliza una caché proxy de interceptación para examinar todas las solicitudes HTTP. Las solicitudes que cumplen los requisitos enumerados a continuación se almacenan en caché. Los vídeos no se sirven desde la caché a menos que el motor de caché los evalúe como nuevos. De lo contrario, se recuperan de nuevo para el visor y se sobrescribe la versión previamente almacenada en caché.

Contenido más reciente garantizado. Cada vez que se visualiza un vídeo, la caché comprueba el servidor de origen y, si el vídeo ha cambiado, se descarta el contenido almacenado en caché y se descarga el nuevo contenido.

> **Nota**
>
> Ahora el almacenamiento en caché es transparente. Es decir, la dirección IP tanto del cliente como del servidor se mantienen de extremo a extremo. En versiones anteriores, la dirección IP del dispositivo Citrix SD-WAN WANOP se mostraba como la dirección de origen.

Un vídeo se almacena en caché cuando se cumplen todos los criterios siguientes:

- El protocolo utilizado para transmitir el vídeo es HTTP. De forma predeterminada, el puerto 80 está configurado para el almacenamiento en caché de vídeo. Sin embargo, si ha configurado otro puerto, como 8080 para un servidor web, debe especificar este puerto para almacenar vídeos en caché.
- Ha agregado fuentes de vídeo desde las que desea almacenar en caché los vídeos. De forma predeterminada, las fuentes de vídeo de YouTube, Vimeo, Youku, Dailymotion y Metacafe se agregan al dispositivo, pero solo YouTube y Vimeo están habilitados. Si desea almacenar en caché vídeos de cualquiera de las otras fuentes predeterminadas, debe habilitarlos. Al agregar nuevas fuentes de vídeo, puede habilitarlas a medida que las agregue.
- Además de YouTube, Vimeo, Metacafe, Dailymotion y Youku, puede especificar sitios web adicionales, direcciones IP o subredes como fuentes de vídeo. Tenga en cuenta que estos sitios web no deben tener ningún mecanismo de evitación, como agregar caracteres aleatorios a una URL.
- El vídeo debe estar en uno de los formatos de vídeo reconocidos y tener una de las siguientes extensiones de archivo: 3gp, .avi, .dat, .divx, .dvx, .dv-avi, .flv, .fmv, .h264, .hdmov, .m15, .m1v, .m21, .m2a, .m2v, .m4e .m4v, .m75, .moov, .mov, .movie, .mp21, mp2v, .mp4, .mp4v, .mpe, .mpeg, mpeg4, mpg, mpg2, .mpv, .mts, .ogg, .ogv, .qt, .qtm, .ra, .rm, .ram, .rmd, .rms, rmvb, .rp, rv, .swf, .ts, .vfw, .vob, .webm, .wm, .wma, .wmv y .wtv.

Plataformas admitidas

La función de almacenamiento en caché de vídeo es compatible con los siguientes dispositivos:

- Dispositivo SD-WAN WANOP 600 con modelos de licencia de ancho de banda de 1 Mbps y 2 Mbps.
- Dispositivo SD-WAN WANOP 800 con todos los modelos de licencia de ancho de banda.
- Dispositivo WANOP 1000 SD-WAN con Windows Server, con todos los modelos de licencia de ancho de banda.
- Dispositivo SD-WAN WANOP 2000 con todos los modelos de licencia de ancho de banda.
- Dispositivo WANOP 2000 SD-WAN con Windows Server, con todos los modelos de licencia de ancho de banda.
- Dispositivo SD-WAN WANOP 3000 con todos los modelos de licencia de ancho de banda.
- SD-WAN WANOP VPX y SD-WAN WANOP VPX para Amazon

Servidor de vídeo compatible

La función de almacenamiento en caché de vídeo es compatible con Adobe Flash Media Server 4.5 o posterior. Además, cualquier servidor de vídeo que sirva vídeos a través de HTTP como enlaces

estáticos se admite para el almacenamiento en caché de vídeo.

Modos de implementación admitidos

El almacenamiento en caché de vídeo se admite en línea, en línea dentro de los puertos troncal de VLAN, en línea virtual y en los modos de implementación WCCP.

Consideraciones para utilizar la función de almacenamiento en caché de vídeo

A continuación se presentan algunos puntos a tener en cuenta cuando se utiliza la función de almacenamiento en caché de vídeo.

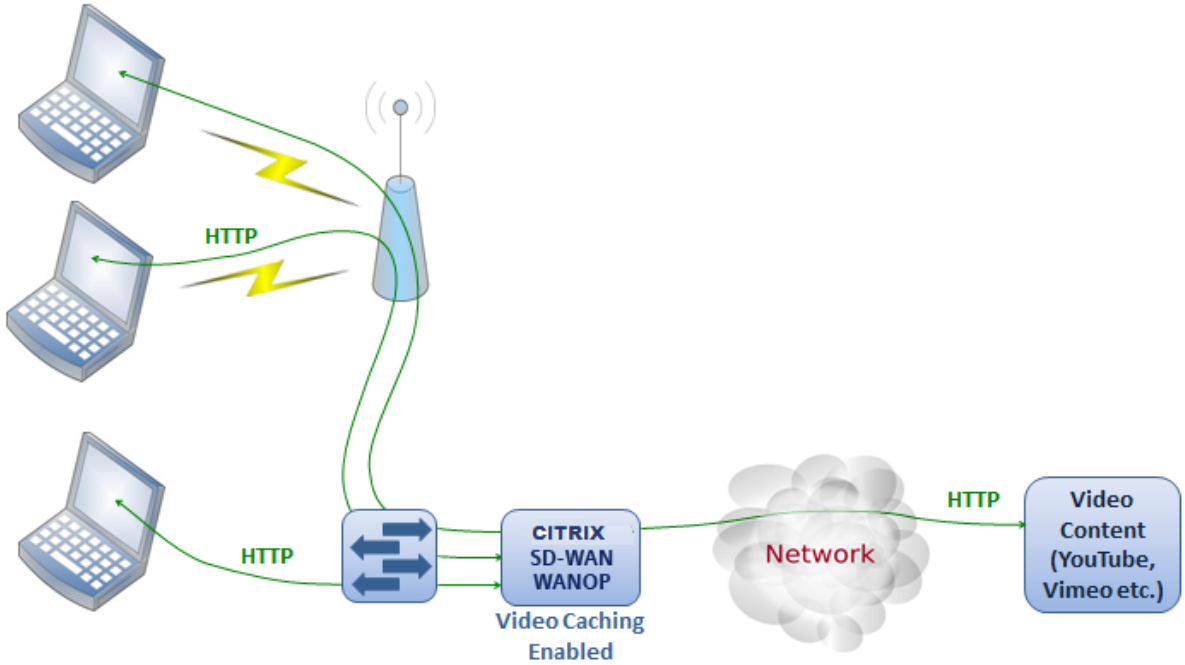
- Si alguno de los sitios web compatibles cambia la forma en que presenta el contenido, es posible que el beneficio de almacenamiento en caché de vídeo para esos sitios no se alcance hasta que se actualice el archivo de directiva de almacenamiento en caché de vídeo. Para estos cambios ocasionales, Citrix proporciona un archivo de directiva de almacenamiento en caché de vídeo actualizado. Para usarlo, consulte Actualización del archivo de directiva de almacenamiento en caché de vídeo.
- Algunos sitios web de vídeo pueden utilizar diferentes formatos de archivo para el mismo vídeo, dependiendo del sistema operativo o del explorador web utilizado para acceder al vídeo. Esto podría dar lugar a una pérdida de caché.
- Algunos sitios web de vídeo, como YouTube, se adaptan a las condiciones de la red. Por lo tanto, la calidad de un vídeo puede depender de las condiciones de la red en el momento en que se almacena en caché.

Escenarios de almacenamiento en caché de vídeo

April 23, 2021

Puede implementar el almacenamiento en caché de vídeo en el dispositivo Citrix SD-WAN WANOP en los siguientes escenarios:

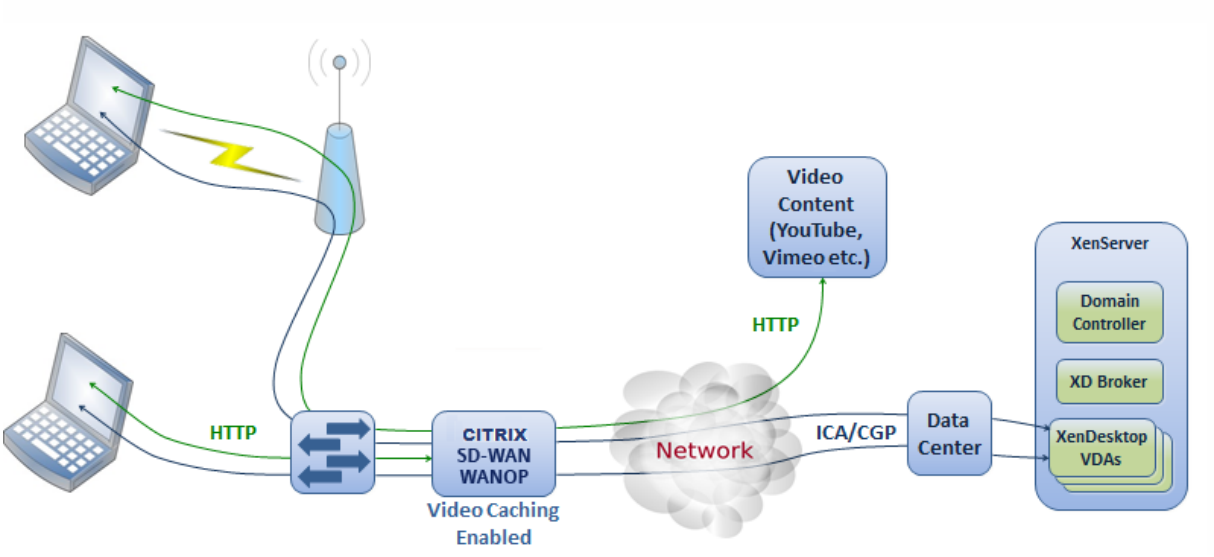
Acceso a la sucursal



En este caso, los usuarios acceden a Internet a través de los exploradores web de sus equipos. Las solicitudes que involucran contenido de vídeo de un sitio habilitado, como Vimeo, se almacenan en caché en el dispositivo local Citrix SD-WAN WANOP. Cualquier acceso posterior al mismo vídeo da lugar a visitas de caché en el dispositivo local, lo que permite que el vídeo se entregue a velocidad LAN y sin esperar al servidor remoto.

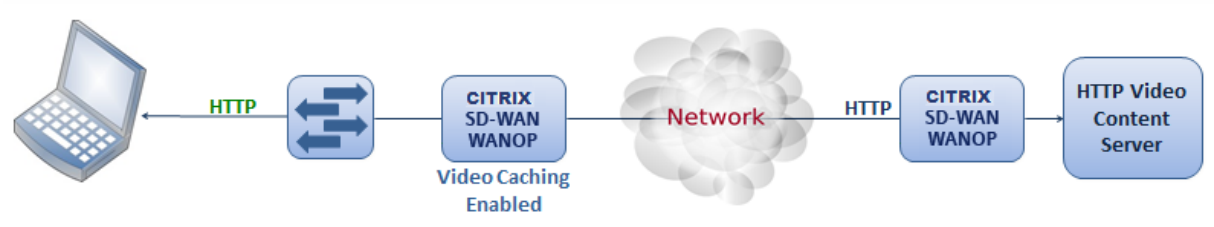
A diferencia de otras características de Citrix SD-WAN WANOP, que aceleran el tráfico entre dispositivos emparejados, esta función es una operación de un solo extremo que requiere solo el dispositivo local, con acceso al sitio web de vídeo.

Sucursal con usuarios de Citrix Virtual Apps and Desktops que utilizan la redirección flash HDX MediaStream



La redirección flash HDX es una función de Citrix Virtual Apps and Desktops. En lugar de renderizar el vídeo en la pantalla de Virtual Desktops remoto mediante Internet del servidor o del centro de datos, los vídeos flash se tunelizan hacia el sistema local mediante esta función. El vídeo se transmite a la máquina cliente real y se representa en el cliente real, mediante Internet de la sucursal. Habilitar la función de almacenamiento en caché de vídeo en el dispositivo Citrix SD-WAN WANOP del lado de sucursal puede ofrecer a los usuarios una experiencia de visualización significativamente mejorada. Además, al habilitar la función se reduce el requisito de ancho de banda para la transmisión de vídeos.

Servidor web de vídeo HTTP empresarial



En este caso, los usuarios acceden a los servidores web de vídeo desde el centro de datos. Cuando habilita la función de almacenamiento en caché de vídeo en el dispositivo Citrix SD-WAN WANOP del lado de sucursal, la solicitud del usuario se envía desde la caché del dispositivo Citrix SD-WAN WANOP del lado de sucursal. Esto ayuda a reducir el tráfico de red hacia el dispositivo Citrix SD-WAN WANOP del centro de datos. Como resultado, el ancho de banda del dispositivo Citrix SD-WAN WANOP del centro de datos se puede utilizar para servir el tráfico de otras sucursales.

Configurar el almacenamiento en caché de vídeo

April 23, 2021

Puede configurar la función de almacenamiento en caché de vídeo a través de la interfaz gráfica de usuario de Citrix SD-WAN WANOP o la interfaz de línea de comandos. De forma predeterminada, el dispositivo está configurado para almacenar en caché vídeos de YouTube y Vimeo. Youku, Metacafe y Dailymotion también están configurados en el dispositivo de forma predeterminada. Todo lo que tienes que hacer es habilitarlas. Puede agregar sitios web de vídeo, como un sitio web interno que sirva tutoriales en vídeo u otra información.

> **Nota**
>
> El almacenamiento en caché de vídeo es una función opcional que no está habilitada de forma predeterminada. No es necesario habilitarlo a menos que tenga una cantidad sustancial de tráfico de vídeo HTTP.

Requisitos previos

Para configurar el almacenamiento en caché de vídeo en el dispositivo, asegúrese de que se cumplen los siguientes requisitos previos:

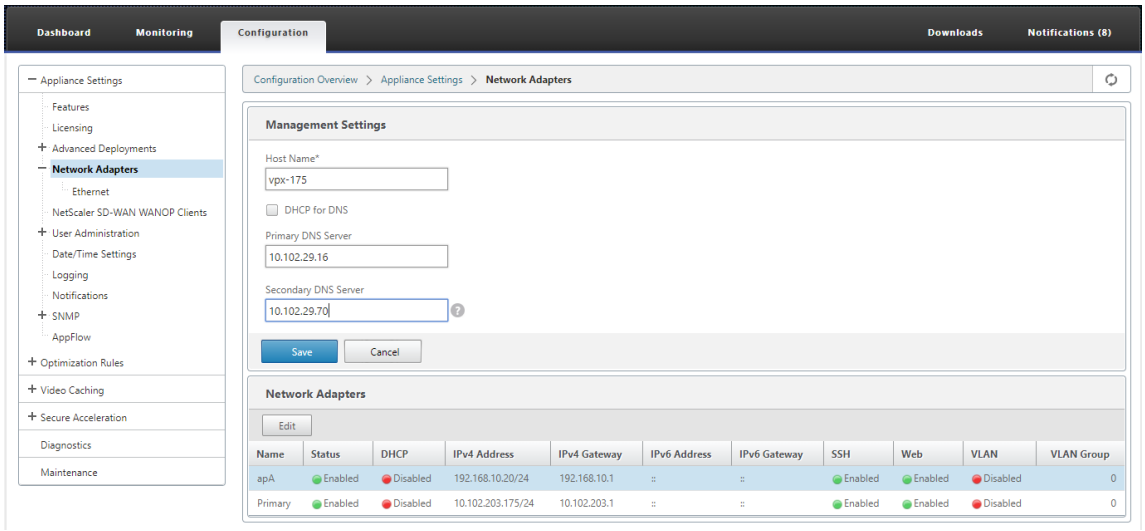
- Ha configurado la dirección IP adecuada para el puerto de puente acelerado que está planeando utilizar para el almacenamiento en caché de vídeo.
- Puede hacer ping a la puerta de enlace apA o apB desde el dispositivo.
- Los detalles del servidor DNS son precisos.
- El dispositivo puede resolver el nombre DNS www.Citrix.com.
- La dirección IP APX WANOP de Citrix SD-WAN tiene un acceso HTTP en la red corporativa.
- Si el dispositivo se implementa entre los puertos troncal de dos dispositivos de red, debe especificar el ID de VLAN con la dirección IP que utilizará el dispositivo para enviar solicitudes HTTP en la página Configuración de red.
- Para las **clases de servicio**Web (Internet)**y Web (privado)**, la configuración de**directiva de aceleración**no debe establecerse en**Ninguno**.

Habilitar la función de almacenamiento en caché de vídeo

Antes de poder comenzar a usar la función de almacenamiento en caché de vídeo, debe habilitarla.

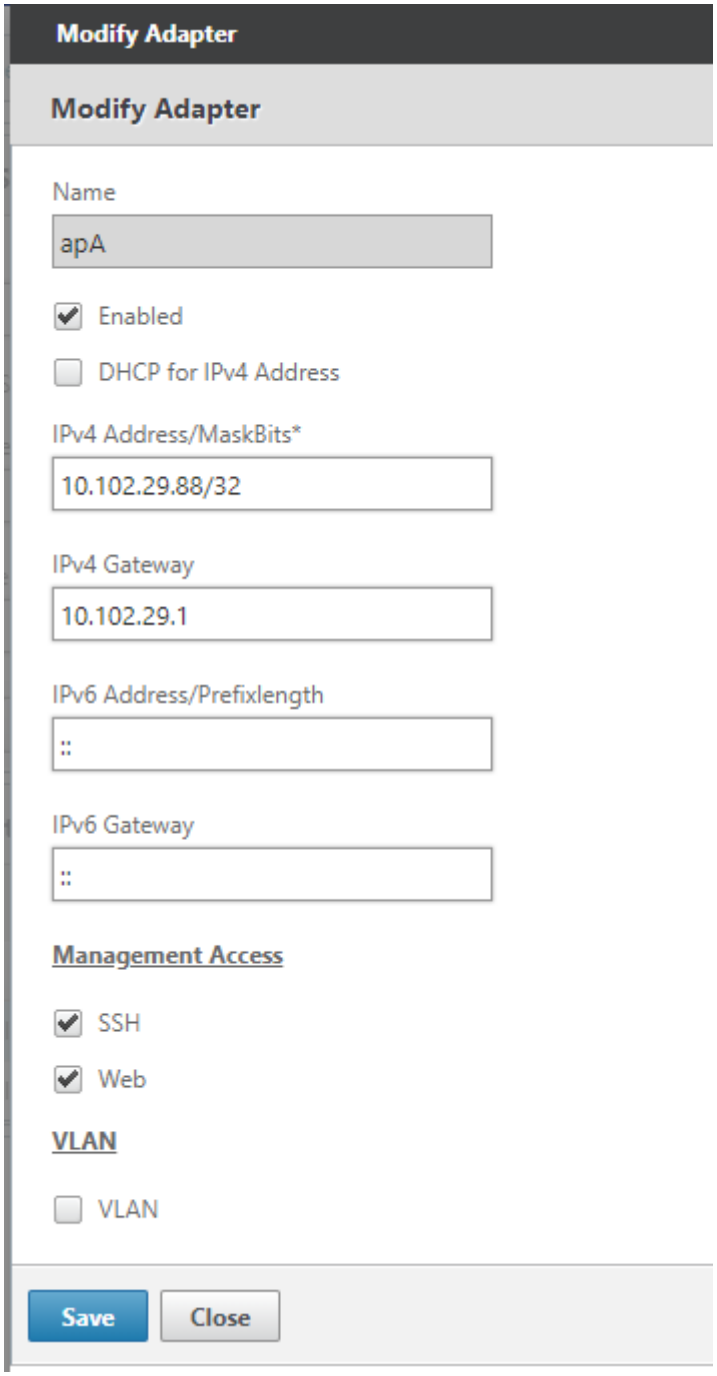
Para habilitar el almacenamiento en caché de vídeo:

1. Vaya a **Configuración > Configuración**
   Configuración del dispositivo > **Adaptadores de red**, en la sección **Configuración de administración**, compruebe y compruebe que los detalles del servidor DNS principal son precisos y que el dispositivo puede resolver el nombre DNS www.Citrix.com. Haga clic en el icono de edición para cambiar la configuración.



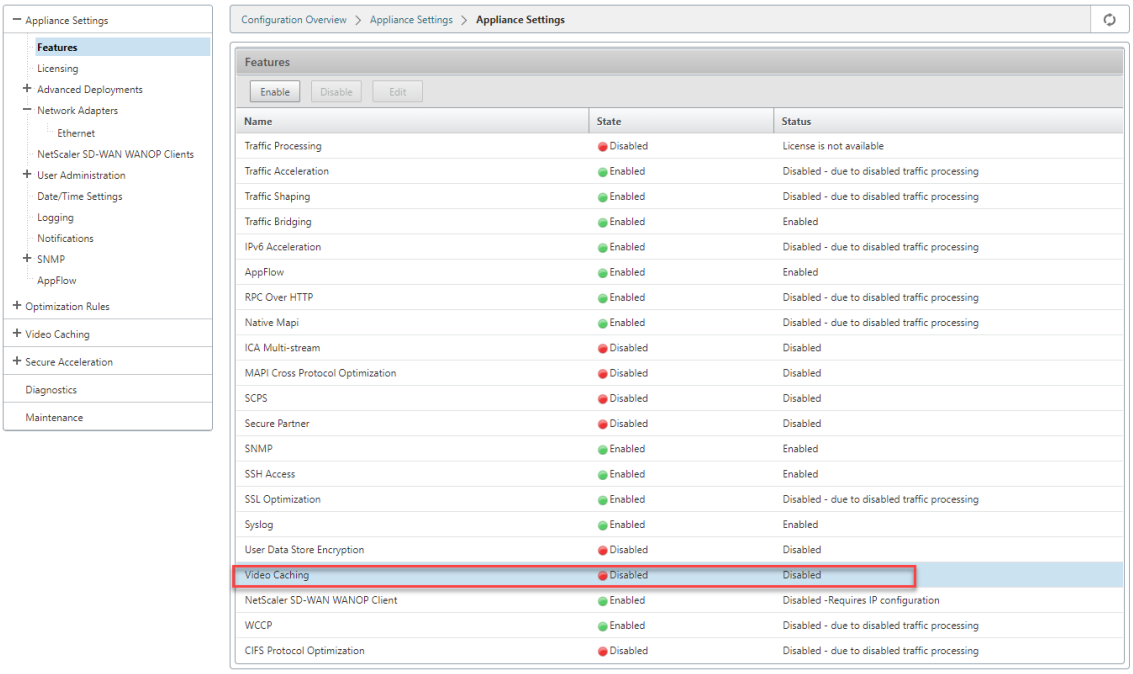
2. Vaya a **Configuración > Configuración** del **equipo** > **Adaptadores de red**. En la sección**Adaptadores de red**, seleccione un par de aceleración (por ejemplo, AP) y **Editar**clik.

   Asegúrese de que las direcciones IP, la máscara de red y las direcciones IP de Gateway predeterminadas especificadas para el par acelerado sean precisas.



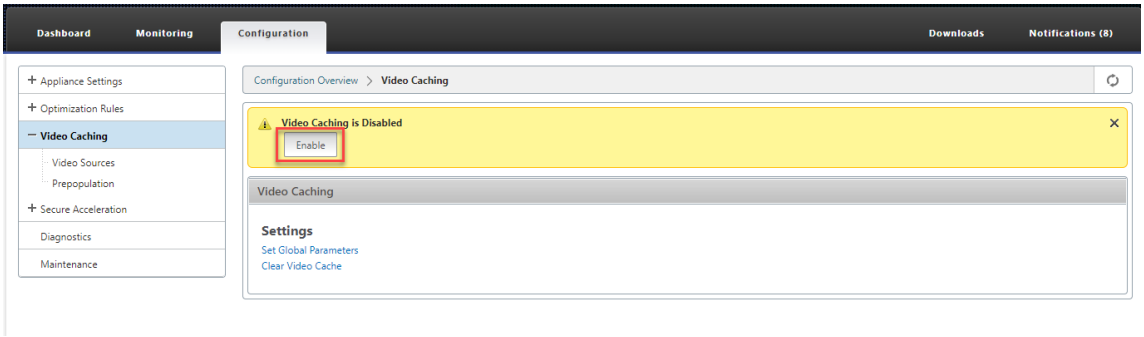
3. Acceda a la página **Configuración** > **Configuración del equipo** > **Funciones** y habilite la función **Almacenamiento en caché de vídeo**.

   Aparecerá un cuadro de diálogo de confirmación, haga clic en **Sí.**



> **Nota**
>
> El servicio se reinicia y se crea una nueva partición de almacenamiento en caché. Si habilita la función por primera vez en el dispositivo, se crea una nueva partición, con lo que se reduce el espacio en disco asignado a otra compresión basada en disco. Se restablece el historial de compresión basado en disco y se terminan las conexiones existentes.

4. También puede desplazarse a **Configuración** > **Reglas de optimización** > Almacenamiento en **caché de vídeo** y hacer clic en **Habilitar**.



Agregar sitios web de vídeo

El dispositivo está configurado para almacenar en caché vídeos de YouTube y Vimeo, y está parcialmente configurado para almacenar en caché vídeos de Youku, Metacafe y Dailymotion. Para almacenar en caché vídeos de cualquiera de los tres últimos sitios, debe habilitar el sitio. Un vídeo de un sitio web habilitado se almacena en caché tan pronto como un usuario accede a él. Puede configurar sitios

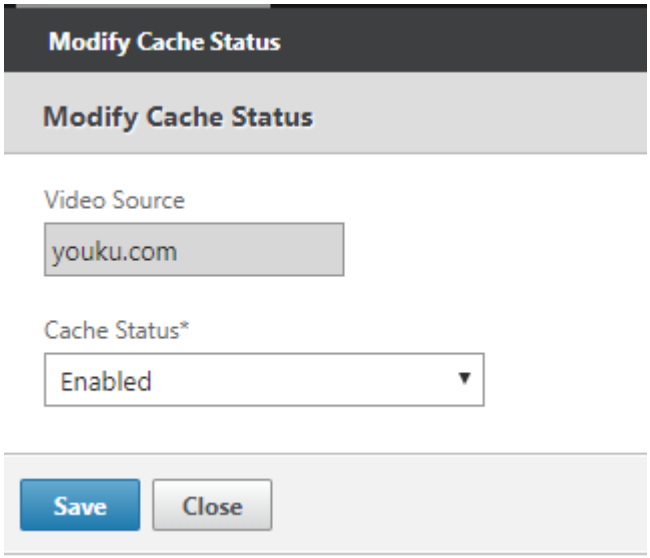
web de vídeo adicionales que no requieran la reescritura de URL agregando sus nombres de host o direcciones IP a la lista Origen de vídeo del dispositivo. También puede incluir sitios personalizados que no tienen ningún mecanismo de evitación de caché.

Debe habilitar estas fuentes de vídeo para que el dispositivo pueda almacenar en caché los vídeos de ellas.

La función de almacenamiento en caché de vídeo utiliza fuentes de vídeo para el flujo de trabajo de configuración. Si configura cualquiera de los orígenes de vídeo con un nombre de host o un sitio web/nombre de host, el dispositivo realiza el proxy de todo el tráfico HTTP que fluye a través del dispositivo. Sin embargo, si configura todos los orígenes de vídeo únicamente con direcciones IP, el dispositivo solo almacena en caché las direcciones IP y los proxies. Independientemente de si utiliza nombres de host o direcciones IP, si su organización no permite el acceso a los sitios web de YouTube, Vimeo, Dailymotion, Metacafe y Youku, asegúrese de desactivar estas fuentes de vídeo.

Para habilitar una fuente de vídeo:

1. Vaya a **Configuración** > **Reglas de optimización** > **Almacenamiento en caché de vídeo** > **Fuentes de vídeo.**
2. Seleccione una fuente de vídeo de la lista, haga clic en **Modificar.**

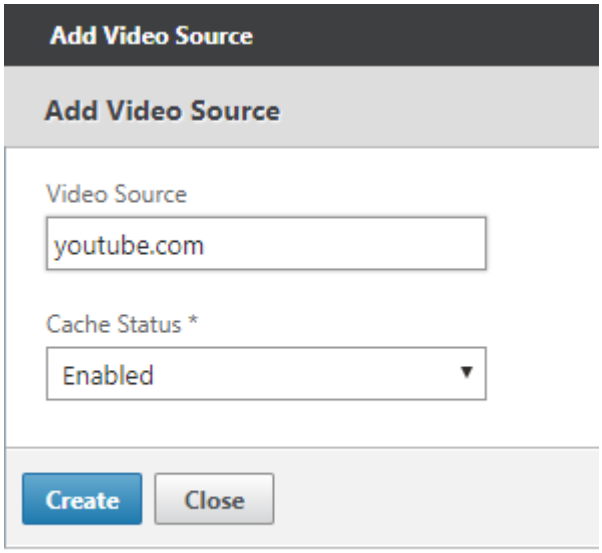


3. En el cuadro desplegable **Estado de caché**, seleccione **Habilitar** y haga clic en **Guardar**.

Para agregar una fuente de vídeo:

1. Vaya a**Configuración****> Reglas de optimización****Almacenamiento en caché de vídeo-Fuentes de vídeo**y haga clic en **Agregar.**
2. En el campo **Origen de vídeo**, escriba el nombre del sitio web o la dirección IP del servidor web que desea agregar a la lista de fuentes de vídeo.

3. En la lista **Estado de la caché**, asegúrese de que está seleccionado **Habilitado**. Puede seleccionar **Inhabilitado** en esta lista si desea habilitar el almacenamiento en caché de vídeo para este sitio más adelante.



4. Haga clic en **Crear**.

   Para eliminar una fuente de vídeo, selecciónela en la lista **Fuentes de vídeo**y haga clic en **Eliminar**.

Prerrellenado de vídeo

April 23, 2021

Un dispositivo Citrix SD-WAN WANOP puede descargar y almacenar en caché vídeos desde su servidor de vídeo interno antes de que alguien los vea. Esta función es útil cuando quiere asegurarse de que todos los usuarios obtienen los mismos beneficios (por ejemplo, al reproducir un vídeo autodidáctico cuya reproducción está programada para darse en un momento determinado). Puede programar direcciones URL estáticas desde las que obtener vídeos.

Los vídeos recuperados se almacenan en la caché de vídeo. Tan pronto como un usuario envía una solicitud para la URL, el vídeo se sirve desde la caché, incluso para el primer acceso del vídeo.

Para obtener vídeos por adelantado, puede realizar las siguientes tareas:

- Especifique una URL desde la que desea almacenar en caché los vídeos con antelación.
- Programe la fecha y hora en la que almacenar en caché los vídeos.

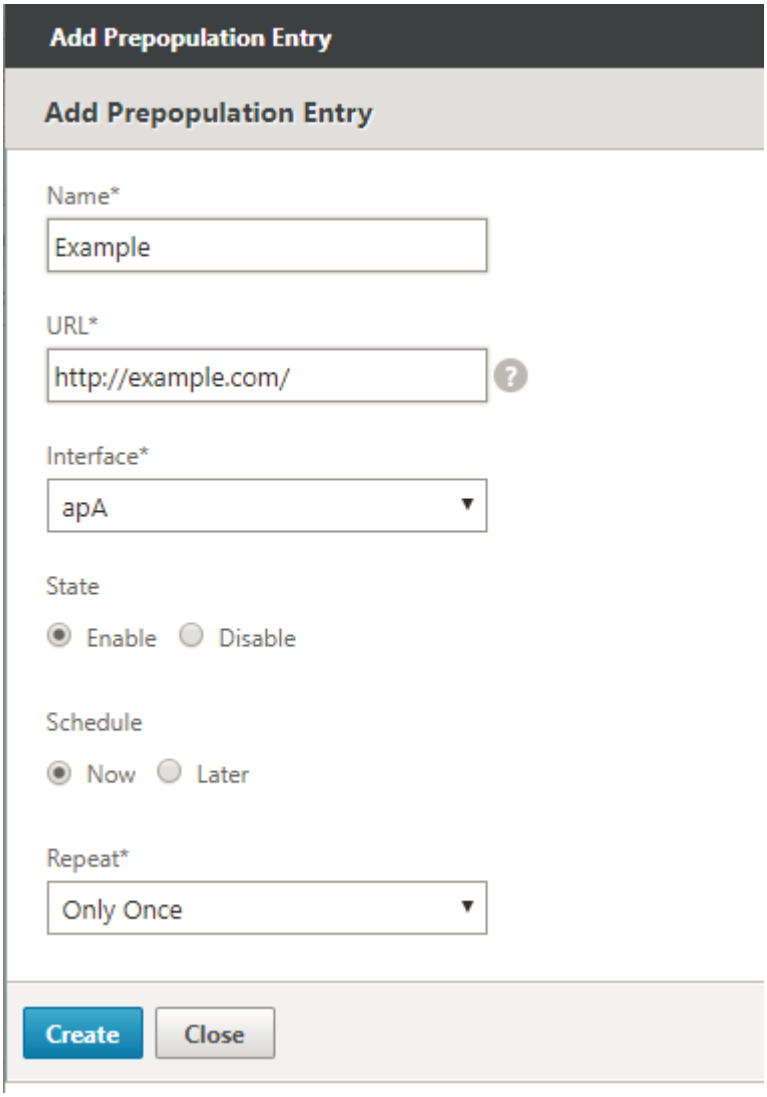
- Programe un intervalo en el que desea almacenar en caché los vídeos.
- Administre las entradas que ha agregado a la lista.

Para descargar y almacenar en caché un vídeo por adelantado, debe especificar la ruta absoluta para la URL de un vídeo específico o una carpeta de vídeo en la que está habilitada la indexación de directorios.

> **Nota**
>
> Si simplemente agrega una entrada a las tareas de prerrellenado de vídeo, el vídeo relacionado se descarga y se almacena en caché. Sin embargo, cuando un cliente accede al vídeo, se sirve desde el servidor de vídeo y no obtiene beneficios de almacenamiento en caché. Para asegurarse de que el cliente obtiene beneficios de almacenamiento en caché, debe agregar el servidor de vídeo o la dirección IP utilizada en la tarea de prerrellenado a la lista de fuentes de vídeo.

Para agregar una URL a los vídeos en caché de antemano:

1. Vaya a **Configuración** > Almacenamiento en **caché de vídeo** > **Prerrellenado** y haga clic en **Agregar**.



2. En el campo **Nombre**, especifique un nombre que pueda utilizar para identificar la entrada de prerrellenado.
3. En el campo **URL**, especifique la URL desde la que desea almacenar en caché uno o varios vídeos. La URL puede ser para un vídeo específico o un servidor de vídeo. Asegúrese de especificar una URL completa o una carpeta de vídeo.
4. En el campo **Interfaz**, seleccione el puerto de puente acelerado para descargar vídeos de la URL.
5. Establezca **Estado** en **Habilitar** para recibir información de estado. Los diversos estados y su descripción se indican en la tabla siguiente.
6. Puede iniciar la descarga y el almacenamiento en caché de vídeos desde la dirección URL al dispositivo de forma inmediata, o descargarlos a una hora programada.
7. Haga clic en **Crear**.

En la tabla siguiente se describen los mensajes de estado:

Estado	Descripción
Configurado	Recuperar vídeo para el almacenamiento en caché antes de que se configure la primera vista para la URL y se agregue una nueva tarea.
Error de tiempo de espera de conexión	Se ha agotado el tiempo de espera de la conexión al servidor y no hay respuesta del servidor.
Error 301 - Se ha movido permanentemente	El vídeo que se va a descargar y almacenar en caché se ha movido permanentemente a otra ubicación.
Error 403 - Prohibido	Se deniega el acceso al vídeo que se va a descargar y almacenar en caché.
Error 404 - No encontrado	El vídeo que se va a descargar y almacenar en caché no está disponible en el enlace proporcionado.
Error 504: servidor inaccesible	No se puede acceder a la URL especificada.
Archivos x descargados correctamente	La descarga se realiza correctamente para la URL y el número x de archivos multimedia se descarga en la caché.
Error al descargar x de los archivos y	Error de descarga para algunos de los archivos multimedia de la URL.
Error al descargar x archivos	Error al descargar ningún archivo multimedia de la URL.
Descarga completada	Se ha completado el procesamiento de todas las URL de esta entrada.
Descarga en curso	La descarga está en curso.
Empieza	El dispositivo ha comenzado a descargar archivos multimedia desde la dirección URL.
Eliminar esta entrada	La entrada se está eliminando de la lista de direcciones URL.
Error al obtener el listado del directorio	Error al obtener el listado del directorio remoto especificado.
Entrada eliminada por operación de borrado de caché	La entrada ha sido purgada por la operación de borrar caché.
Actualización del estado	El dispositivo está actualizando el estado de la entrada.

Estado	Descripción
Tiempo de programación transcurrido	La hora programada a la que descargar el objeto remoto ha pasado.
Archivos “x”/”y”en caché	Al actualizar el estado de una entrada, el dispositivo ha encontrado que el número x de archivos fuera del número y de archivos existe en la caché.
Interfaz ap”X”inhabilitada para el almacenamiento en caché de vídeo	La interfaz de puente ap”X”no está habilitada para el almacenamiento en caché de vídeo.
Estado de actualización	El estado de la entrada se está actualizando.
Error 0	Se ha producido un error desconocido al descargar los vídeos. Póngase en contacto con el equipo de soporte técnico de Citrix para resolver el problema.

Administrar prerrellenado de almacenamiento en caché de vídeo

Puede administrar la prerrellenado de almacenamiento en caché de vídeo para controlar cómo desea descargar y almacenar en caché los vídeos de las URL. Puede realizar las siguientes tareas para administrar la prerrellenado de almacenamiento en caché de vídeo:

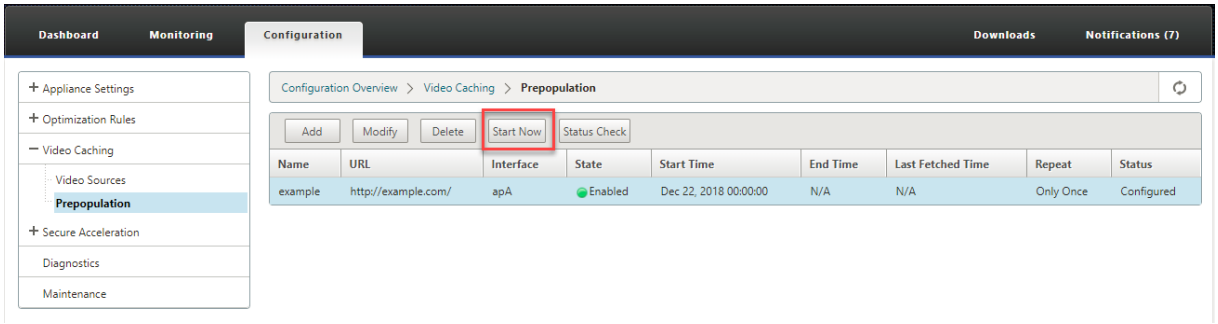
- Comienza a descargar vídeos antes o después de la fecha y hora programadas.
- Actualizar la URL de una entrada.
- Inhabilitar el almacenamiento en caché de vídeos desde una entrada de URL.
- Programar el almacenamiento en caché de vídeos desde una entrada de URL.
- Actualizar una interfaz para una entrada de URL.
- Actualizar el estado de una entrada de URL.
- Eliminar una entrada de URL.

El siguiente diagrama de flujo muestra el control de flujo de los procesos seguidos al gestionar diversas actividades de la función de prerrellenado de vídeo.

Descargar vídeos

Si problemas técnicos con un sitio web o la URL que ha agregado interfieren con la descarga programada y el almacenamiento en caché, puede comenzar a descargar y almacenar en caché vídeos cuando sea necesario en cualquier momento.

Para descargar y almacenar en caché un vídeo inmediatamente, vaya a **Configuración** > **Almacenamiento en caché de vídeo** > **Prepoblado**, seleccione la entrada del vídeo que desea almacenar en caché y, a continuación, haga clic en **Iniciar ahora**. La actualización del estado del vídeo dura aproximadamente un minuto.



Después de hacer clic en Iniciar ahora, la columna Estado muestra el estado de las descargas de vídeo desde la URL.

Actualizar la URL de una entrada de prerrellenado

Después de agregar una URL desde la que descargar y almacenar el vídeo en caché por adelantado, puede ajustar la URL para obtener resultados óptimos, como reconfigurar la URL cuando cambie la ubicación de los vídeos o cambie el nombre del archivo multimedia en el origen.

Para actualizar una URL:

1. Acceda a la página **Configuración** > **Almacenamiento en caché de vídeo** > **Prerrellenado**.
2. Seleccione la entrada que desea actualizar y haga clic en **Modificar**.
3. En el campo URL, especifique la nueva URL.
4. Haga clic en **Aceptar**.

Inhabilitar el almacenamiento en caché de vídeos de una URL en una entrada de prerrellenado

Si desea rellenar periódicamente la caché con vídeos de una URL determinada, no necesita eliminar la entrada. Puede inhabilitarlo y, a continuación, habilitarlo cuando sea necesario.

Para inhabilitar una entrada:

1. Vaya a la página **Configuración** > **Almacenamiento en caché de vídeo** > **Prerrellenado**.
2. Seleccione la entrada que desea actualizar y haga clic en **Modificar**.
3. En Estado, seleccione la opción **Inhabilitar**.
4. Haga clic en **Aceptar**.

Programar el almacenamiento en caché de vídeos de una URL en una entrada de prerrellenado

Puede programar la fecha y la hora en la que iniciar la descarga y el almacenamiento en caché de vídeos desde la dirección URL al dispositivo. Por ejemplo, es posible que desee buscar vídeos justo antes de esperar que los usuarios empiecen a acceder a ellos. Eso no solo ahorra espacio en disco, sino que también coloca las últimas versiones de los vídeos en la caché.

Para programar el almacenamiento en caché desde una URL:

1. Vaya a la página **Configuración** > **Almacenamiento en caché de vídeo** > **Prerrellenado**.
2. Seleccione la entrada que desea actualizar y haga clic en **Modificar**.
3. En **Programación**, seleccione la opción **Más tarde**.
4. En el campo **Inicio**, especifique la fecha y hora en la que desea descargar vídeos de la URL. El formato de la fecha y hora es AAAA-MM-DD HH:MM:SS.
5. En la lista **Repetir**, seleccione la frecuencia de descarga y almacenamiento en caché de los vídeos. Las opciones disponibles son:
   - **Solo una vez**: Descarga vídeos desde la URL una sola vez, a la fecha y hora programadas.
   - **Diario**: Descarga vídeos de la URL todos los días, empezando por la fecha y hora programadas. La descarga comienza todos los días a la hora de inicio que especifique.
   - **Semanal**: Descarga vídeos de la URL una vez a la semana, empezando por la fecha y hora programadas. La descarga comienza cada semana en el día y la hora que especifique.
   - **Mensual**: Descarga vídeos de la URL una vez al mes, empezando por la fecha y hora programadas. La descarga comienza cada mes en el día y la hora que especifique.
6. Haga clic en **Aceptar**.

Actualizar una interfaz en una entrada de URL

Si ha configurado varios vínculos en la red, es posible que desee utilizar un vínculo concreto para descargar vídeos, debido a una mejor conectividad de red. Para configurar varios vínculos, utilice los puertos de puente disponibles, como los puertos de puente apA y apB. Puede utilizar estos puertos para descargar vídeos para una entrada de URL.

Para actualizar una interfaz para una entrada de URL:

1. Vaya a **Configuración** > Almacenamiento en **caché de vídeo > Prepoblado**.
2. Seleccione la entrada que desea actualizar. y haga clic en **Modificar**.

3. En la lista **Interfaz**, seleccione la interfaz que desea utilizar para la entrada de URL. La lista muestra las interfaces disponibles y configuradas en el dispositivo.
4. Haga clic en **Aceptar**.

Actualizar el estado de una entrada de URL

Con el tiempo, el estado de los vídeos almacenados en caché puede cambiar. Comprobar el estado de la entrada periódicamente asegura que los usuarios no obtengan resultados inesperados al acceder a los vídeos.

Para comprobar el estado más reciente de los vídeos almacenados en caché desde una URL:

1. Vaya a **Configuración** > Almacenamiento en **caché de vídeo > Prepoblado**.
2. Seleccione la entrada para la que desea actualizar el estado de los vídeos almacenados en caché.
3. Haga clic en **Comprobación de estado**.

Eliminar una entrada de URL

Si no necesita una entrada de URL, puede eliminar si de la lista. Para eliminar una entrada de URL, selecciónela y haga clic en **Eliminar**.

> **Nota**
>
> Cuando elimina una tarea de prerrellenado de vídeo de la lista, también elimina los objetos de vídeo relacionados de la caché.

Verificar el almacenamiento en caché de vídeo

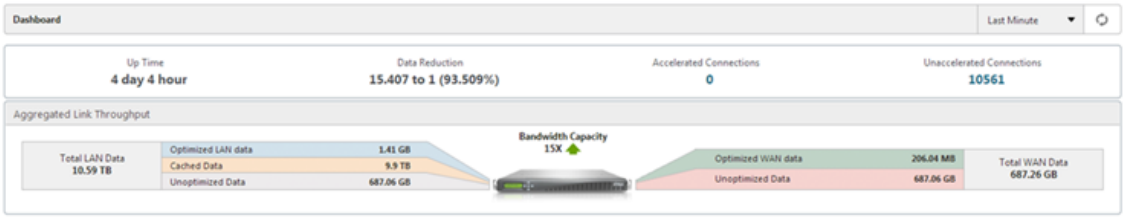
April 23, 2021

Los gráficos y los datos de la página Supervisión, la página Panel y la página Uso le ayudan a evaluar los beneficios proporcionados por la configuración de almacenamiento en caché de vídeo. La relación de reducción de datos resultante del almacenamiento en caché de vídeo (similar a la relación de compresión general) se muestra en el Panel de control, en la página de supervisión del almacenamiento en caché de vídeo y en la página Gráfico de uso. Además, al pasar el cursor sobre la relación de reducción de datos en la página Panel de control, se muestra el porcentaje de beneficio de almacenamiento en caché junto con el porcentaje de beneficio de compresión en las plataformas compatibles.

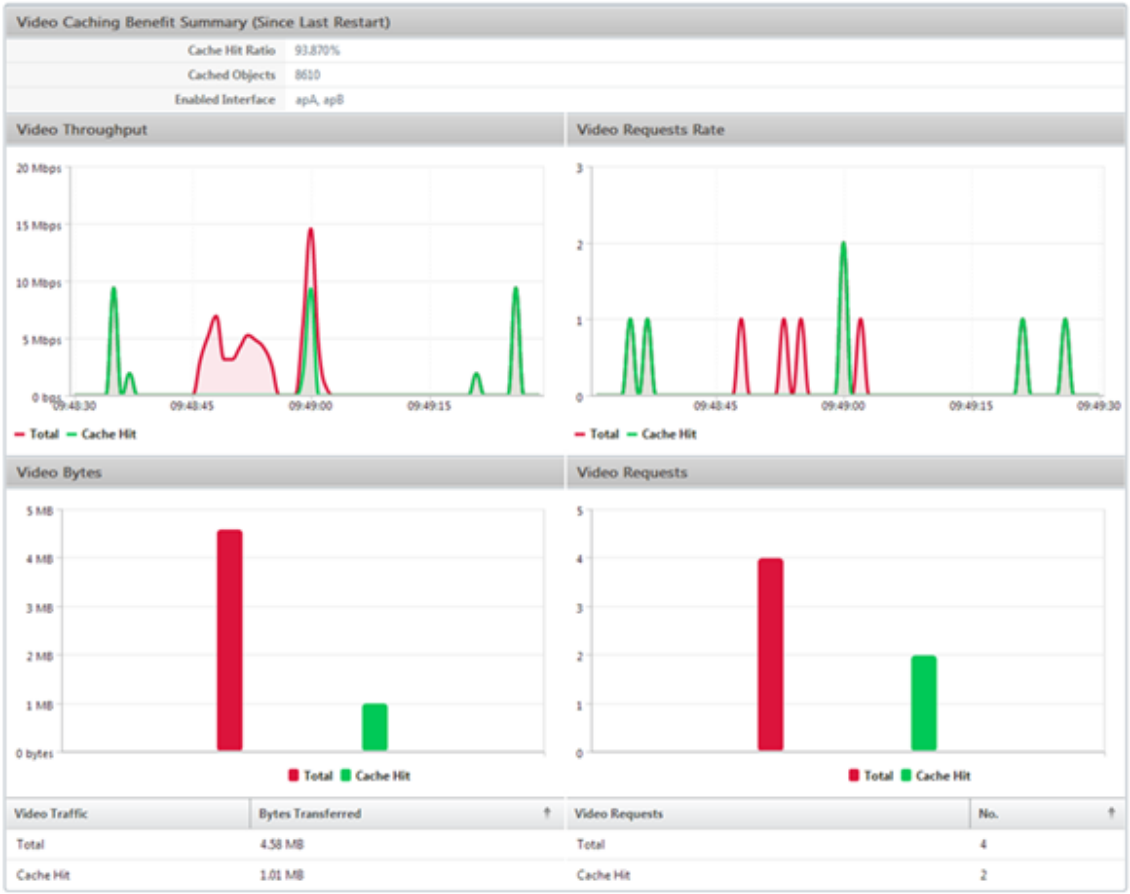
El propósito del almacenamiento en caché no es solo para ahorrar ancho de banda, sino también para aumentar el rendimiento, disminuir la carga en los servidores de vídeo y disminuir el impacto de la congestión de la red.

El ahorro estimado de ancho de banda WAN resultante del almacenamiento en caché de vídeo se muestra de la siguiente manera:

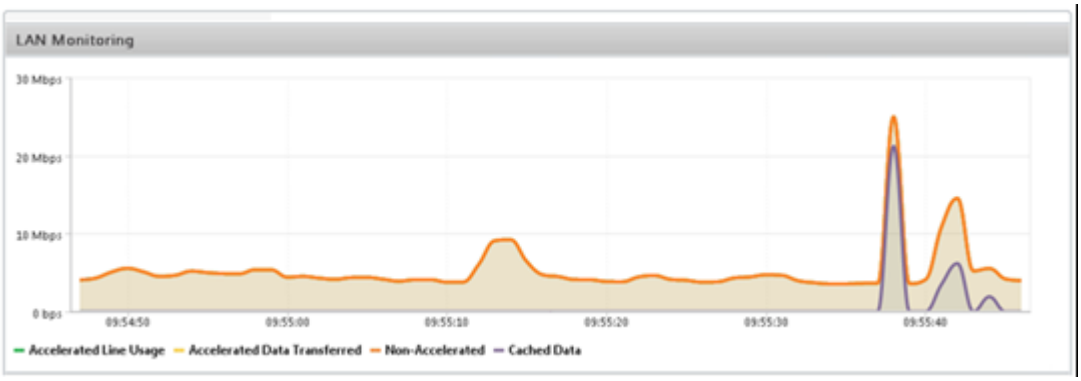
- En la página Panel, puede ver el beneficio del almacenamiento en caché, como porcentaje, si pasa el cursor sobre el campo Reducción de datos del Panel. También puede ver los bytes servidos desde la caché (Datos almacenados en caché) en Rendimiento de enlace agregado.



- En la página **Supervisión**> Almacenamiento en **caché de vídeo**, puede ver el número de objetos almacenados en caché y la proporción de aciertos de caché (como porcentaje). La barra y los gráficos de tiempo muestran el número de solicitudes y bytes servidos desde la memoria caché durante 1 minuto, 1 hora, 1 día, 1 semana y 1 mes. Estos datos también se muestran en un formato tabular debajo del gráfico.

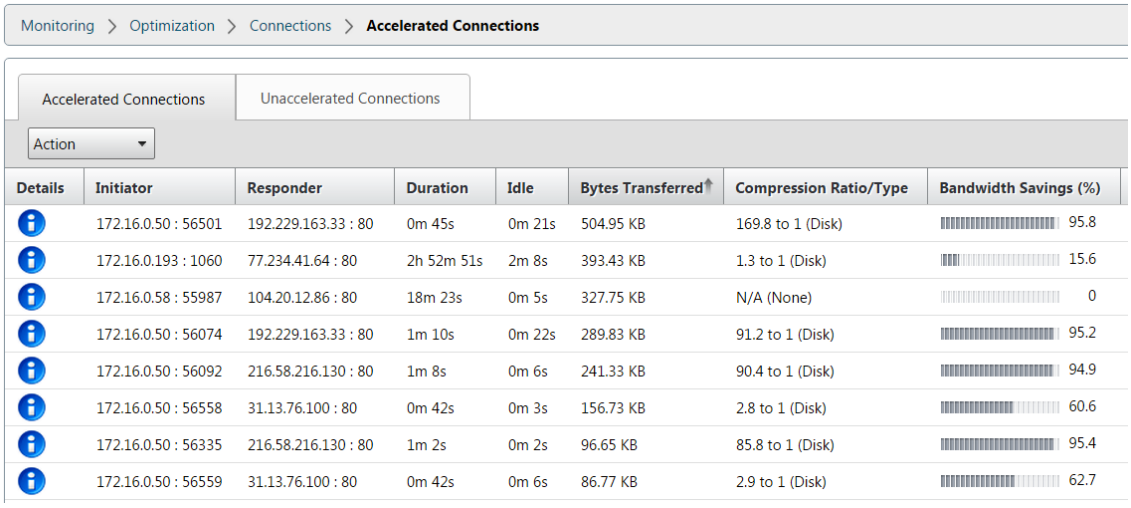


- En la página **Supervisión** > **Optimización** > **Gráfico de uso**, puede ver los datos almacenados en caché en el gráfico Supervisión de LAN.



- En la página **Supervisión** > Almacenamiento en **caché de vídeo** > **Lista deestado HTTP**, puede supervisar el comportamiento mejorado de la caché. Esta página informa del estado de las conexiones HTTP con respecto al almacenamiento en caché de vídeo.
- En la página**Supervisión**>**Optimización > Conexiones**, puede ver las conexiones almacenadas en caché en la ficha Conexiones aceleradas.Aquí se muestran tanto las visitas de caché como las faltas de caché. Las conexiones de caché se muestran aquí incluso si no están aceleradas.

Es decir, las conexiones almacenadas en caché se muestran aquí incluso si un dispositivo Citrix SD-WAN WANOP asociado no está involucrado en la conexión.La columna**Ahorro de ancho de banda** (%) muestra un gráfico de barras de cuánto ancho de banda WAN guardó la transacción, ya sea mediante almacenamiento en caché o compresión. Si bien el objetivo del almacenamiento en caché y la compresión es aumentar la velocidad y la usabilidad y no reducir el uso del ancho de banda, los aumentos de velocidad y usabilidad suelen estar relacionados con la reducción del ancho de banda. Es decir, un 90% de ahorro de ancho de banda implica un aumento de 10 veces en la velocidad.



Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)
	172.16.0.50 : 56501	192.229.163.33 : 80	0m 45s	0m 21s	504.95 KB	169.8 to 1 (Disk)	95.8
	172.16.0.193 : 1060	77.234.41.64 : 80	2h 52m 51s	2m 8s	393.43 KB	1.3 to 1 (Disk)	15.6
	172.16.0.58 : 55987	104.20.12.86 : 80	18m 23s	0m 5s	327.75 KB	N/A (None)	0
	172.16.0.50 : 56074	192.229.163.33 : 80	1m 10s	0m 22s	289.83 KB	91.2 to 1 (Disk)	95.2
	172.16.0.50 : 56092	216.58.216.130 : 80	1m 8s	0m 6s	241.33 KB	90.4 to 1 (Disk)	94.9
	172.16.0.50 : 56558	31.13.76.100 : 80	0m 42s	0m 3s	156.73 KB	2.8 to 1 (Disk)	60.6
	172.16.0.50 : 56335	216.58.216.130 : 80	1m 2s	0m 2s	96.65 KB	85.8 to 1 (Disk)	95.4
	172.16.0.50 : 56559	31.13.76.100 : 80	0m 42s	0m 6s	86.77 KB	2.9 to 1 (Disk)	62.7

Administrar orígenes de almacenamiento en caché de vídeo

April 23, 2021

Puede administrar las fuentes de vídeo de forma global, configurando la configuración global o individualmente cambiando el estado de una fuente de vídeo.

Configurar la configuración global

La configuración global permite configurar la función a nivel del dispositivo. Independientemente de las fuentes de vídeo que haya agregado, esta configuración se aplica a toda la función de almacenamiento en caché de vídeo del dispositivo. Puede hacer lo siguiente:

- Configurar el tamaño máximo de los objetos almacenados en caché
- Configurar un sufijo DNS
- Configurar puertos de almacenamiento en caché

- Actualizar el archivo de directiva de almacenamiento en caché de vídeo

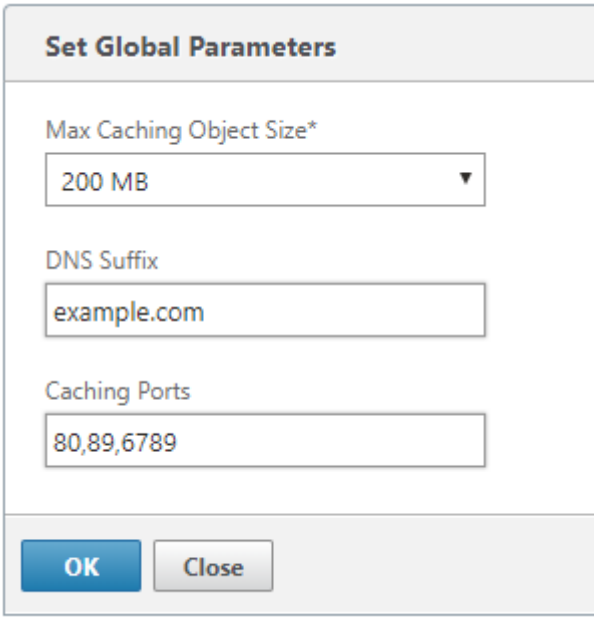
Puede configurar un tamaño máximo para los objetos almacenados en caché. Un objeto mayor que este límite no se almacena en caché. De forma predeterminada, el tamaño máximo del objeto de almacenamiento en caché es de 100 MB.

Para las direcciones URL que no contienen nombres de dominio completos y requieren sufijos de nombre de dominio para agregarse al nombre de host del servidor de vídeo, es necesario agregar un nombre de dominio predeterminado para obtener una respuesta del servidor. Por ejemplo, al acceder al vídeo `http://training/CitrixSD-WANWANOP\\_VideoCaching.mp4`, es posible que el dispositivo traduzca la dirección URL a `http://training.example.com/CitrixSD-WANWANOP\\_VideoCaching.mp4`. En este caso, debe especificar example.com como sufijo de nombre de dominio.

La función de almacenamiento en caché de vídeo requiere un número de puerto para el servidor de vídeo HTTP. El valor predeterminado es el puerto 80. Si el servidor de vídeo HTTP utiliza un puerto distinto de este puerto HTTP conocido, debe agregar el número de puerto a la lista de puertos de almacenamiento en caché.

Para configurar la configuración global para el almacenamiento en caché de vídeo:

1. Vaya a **Configuración** > **Almacenamiento en caché de vídeo** > **Establecer parámetros globales.**



2. En el campo **Tamaño de objeto MaxCaching**, establezca el tamaño máximo de los objetos almacenados en caché.

   Seleccione un valor entre los límites disponibles.Un objeto mayor que este límite no se almacena en caché.

3. En el campo **Sufijo DNS**, escriba un nombre de dominio para anexar a las direcciones URL que no contengan nombres de dominio completos y requieran que se añadan sufijos de nombre de dominio al nombre de host del servidor de vídeo.
4. En el campo **Puertos de almacenamiento en caché**, escriba el puerto del servidor de vídeo HTTP para agregarlo a la lista de puertos de almacenamiento en caché. Opcionalmente, agregue varios números de puerto separados por comas.
5. Haga clic en **Aceptar**.

El dispositivo utiliza el 10% del espacio de disco asignado para fines de administración. Cuando el uso del disco alcanza el 90% del espacio asignado en disco, es una indicación de que el disco está lleno. Para almacenar en caché más objetos de vídeo, el dispositivo elimina los objetos menos utilizados de la caché de vídeo. No es necesario borrar la caché a menos que la caché sirva objetos de vídeo obsoletos.

Para borrar la caché de vídeo, vaya a **Configuración** > **Almacenamiento en caché de vídeo** y haga clic en **Borrar caché de vídeo**.

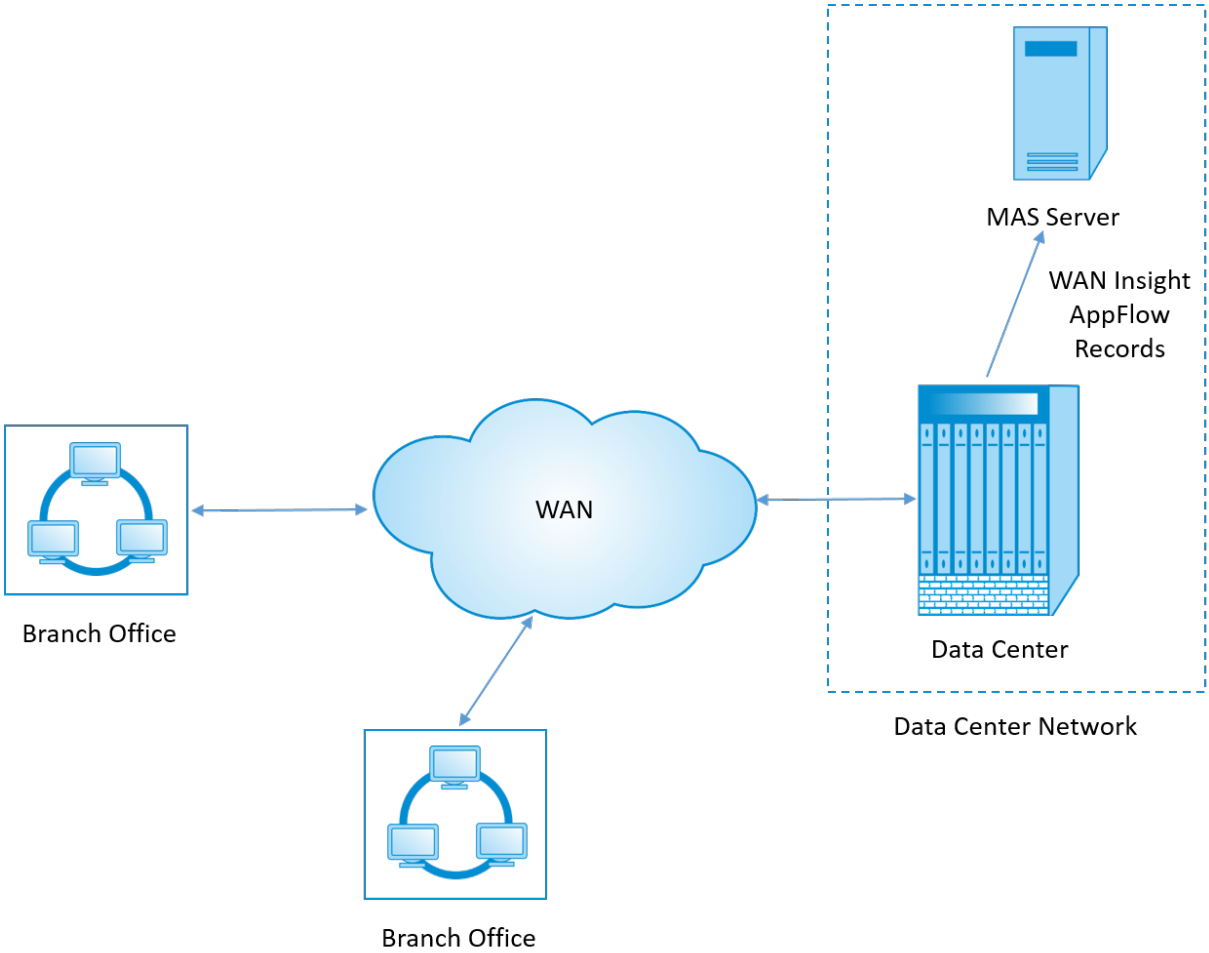
Información WAN

December 14, 2022

Los dispositivos Citrix SD-WAN WANOP optimizan la entrega de un gran número de aplicaciones a través de la WAN, al mejorar la eficiencia del flujo de datos a través de la red entre el centro de datos y los sitios de sucursales. El análisis de WAN Insight permite a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre los dispositivos de optimización WAN del centro de datos y las sucursales. WAN Insight proporciona visibilidad a los clientes, aplicaciones y sucursales de la red, para ayudar a solucionar problemas de red de manera eficaz. Los informes históricos y activos le permiten abordar problemas de forma proactiva, si los hay.

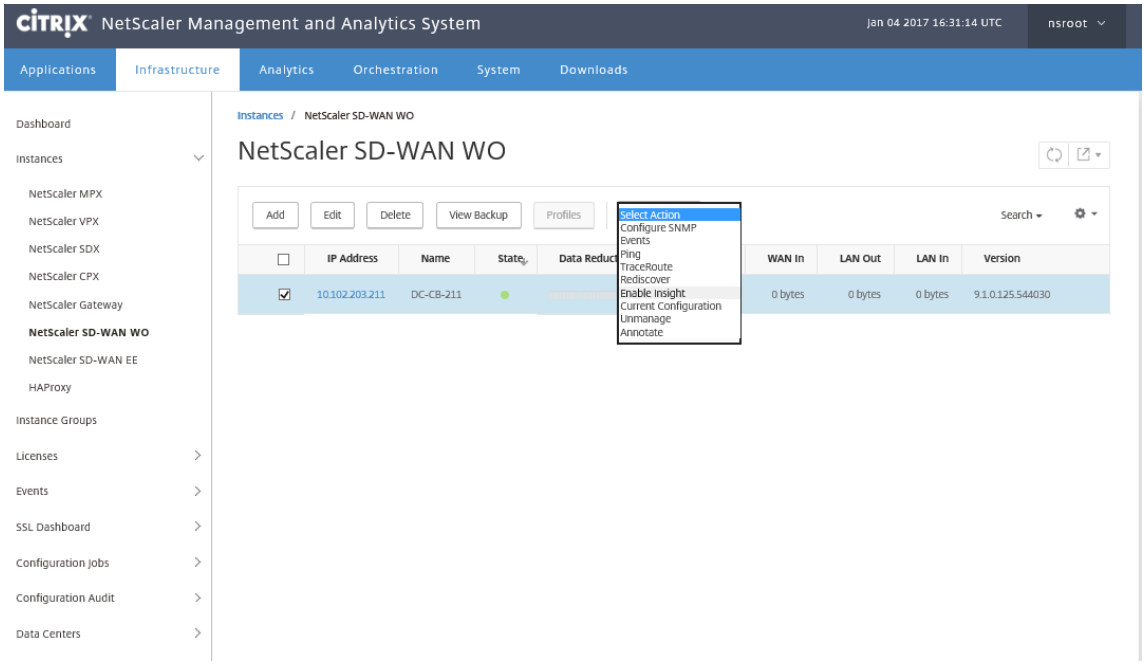
Al habilitar el análisis en el dispositivo de optimización WAN del centro de datos, Citrix Application Delivery Management (ADM) puede recopilar datos y proporcionar informes y estadísticas para el centro de datos y los dispositivos de optimización WAN de sucursal.

> **Nota**
>
> Para obtener información sobre cómo agregar una instancia, consulte Agregar instancias a Citrix ADM.

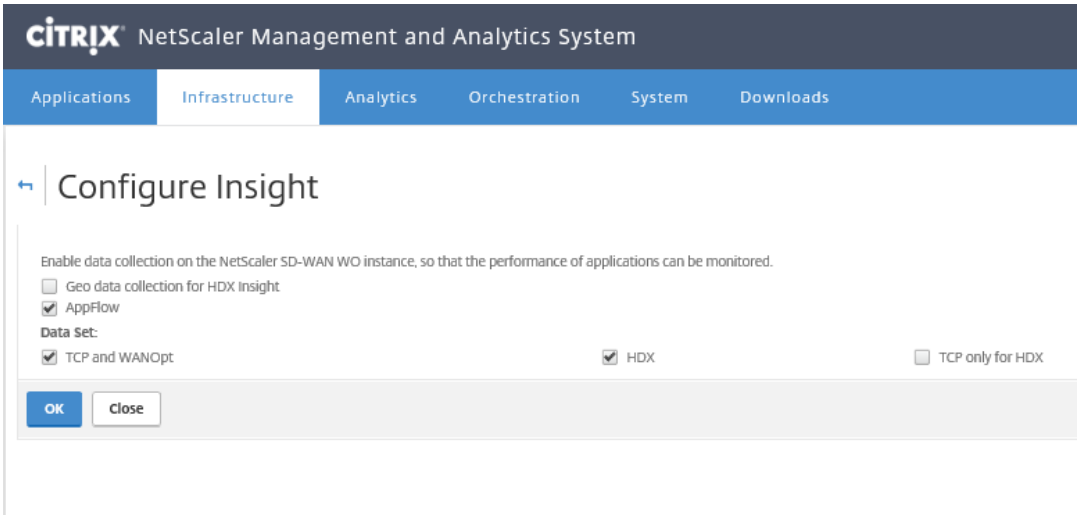


Para habilitar el análisis en el dispositivo de optimización de WAN:

1. En un explorador web, escriba la dirección IP de Citrix ADM (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario**y**Contraseña**, introduzca las credenciales de administrador.
3. Vaya a**Infraestructura** > **Instancias** > **Citrix SD-WAN WO**y seleccione el dispositivo de optimización de WAN del centro de datos.



4. En el menú desplegable **Acción**, seleccione **Habilitar información**.
5. Seleccione los siguientes parámetros según sea necesario:
   - **Recopilación de datos geográficos para HDX Insight**: Comparte la dirección IP del cliente con la API de Google Geo.
   - **AppFlow**: comienza a recopilar datos de instancias de optimización WAN.
   - **TCP y Wanopt**: Proporciona informes TCP y Wanopt Insight.
   - **HDX**: Proporciona informes HDX Insight.
   - **TCP solo para HDX**: Proporciona TCP solo para los informes HDX Insight.



6. Haga clic en **Aceptar**.

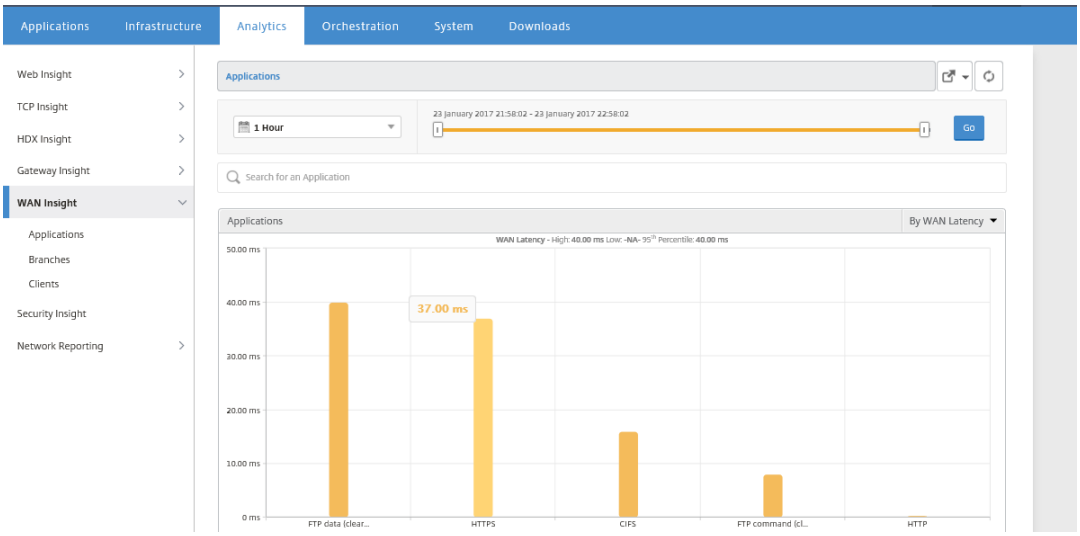
Para ver informes de WAN Insight:

1. En un explorador web, escriba la dirección IP de Citrix ADM (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario**y**Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Analytics** > **WAN Insight**.

> **Nota**
>
> La opción WAN Insight solo está visible después de agregar una instancia WO de SD-WAN a Citrix ADM.

Puede ver los siguientes informes:

- **Aplicaciones**: Muestra las estadísticas de uso y rendimiento de todas las aplicaciones durante la duración seleccionada.
- **Sucursales:** muestra las estadísticas de uso y rendimiento de todos los dispositivos de sucursales de optimización de WAN.
- **Clientes:** muestra las estadísticas de uso y rendimiento de todos los clientes que acceden a los dispositivos de optimización de WAN, en cada sucursal.



Se muestran las siguientes métricas:
Métrica	**Descripción**
———-	————
Conexiones aceleradas activas	Número de conexiones WAN activas que se aceleran.
Conexiones activas no aceleradas	Número de conexiones WAN activas que no están aceleradas.
Latencia de WAN	Retraso, en milisegundos, que el usuario experimenta mientras interactúa con una aplicación.

Índice de compresión	Relación de compresión de datos entre la sucursal y los dispositivos del centro de datos durante la duración seleccionada.
Paquetes enviados	Número de paquetes que el dispositivo de optimización WAN ha enviado a través de la red durante la duración seleccionada.
Paquetes recibidos	Número de paquetes que el dispositivo de optimización WAN ha recibido de la red durante la duración seleccionada.
Bytes enviados a través de WAN	Número de bytes que el dispositivo de optimización de WAN de Citrix ha enviado a través de la WAN durante la duración seleccionada.
Bytes recibidos a través de WAN	Número de bytes que el dispositivo de optimización WAN recibió de la WAN durante la duración seleccionada.
RTO LAN	Número de veces que el dispositivo de optimización WAN ha agotado el tiempo de espera de la retransmisión a la LAN durante la duración seleccionada.
RTO WAN	Número de veces que el dispositivo de optimización de WAN ha agotado el tiempo de espera de la retransmisión a la WAN durante la duración seleccionada.
Paquetes de retransmisión (LAN)	Número de paquetes que el dispositivo de optimización WAN ha retransmitido a la red LAN durante la duración seleccionada.
Paquetes de retransmisión (WAN)	Número de paquetes que el dispositivo de optimización WAN ha retransmitido a la red WAN durante la duración seleccionada.

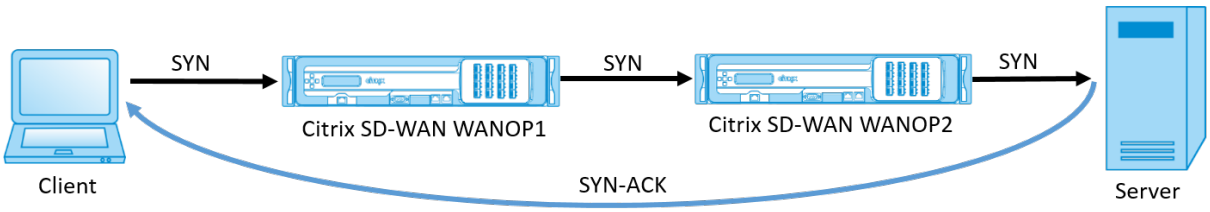
Enrutamiento asimétrico

April 23, 2021

En la red de Citrix SD-WAN WANOP, el enrutamiento asimétrico se produce cuando los paquetes que fluyen de cliente a servidor o de servidor a cliente para la misma conexión TCP no pasan a través de uno o ambos dispositivos WANOP del lado del cliente y del lado del servidor. Se observan los siguientes casos de asimetría.

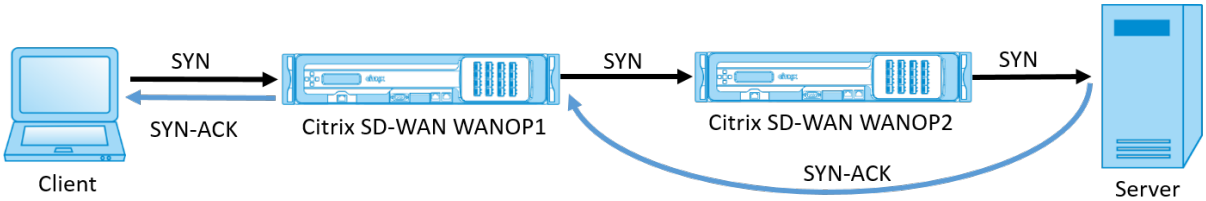
Asimetría completa:

La asimetría completa se produce cuando los paquetes fluyen desde un cliente al servidor a través de los dispositivos Citrix SD-WAN WANOP del lado del cliente y del lado del servidor. Sin embargo, en la ruta de retorno del servidor al cliente, los paquetes toman una ruta diferente sin pasar por los dispositivos de Citrix SD-WAN WANOP.



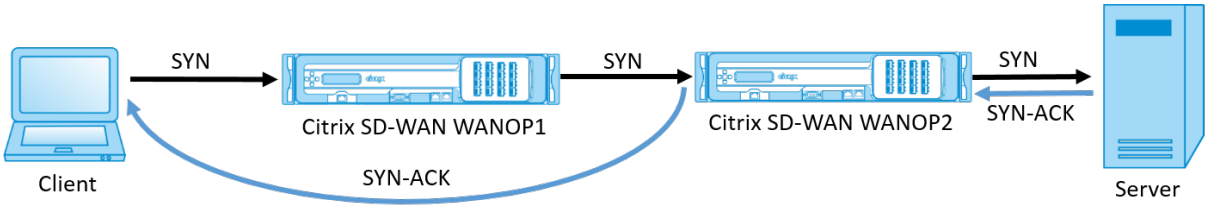
Asimetría del lado del servidor:

La asimetría del lado del servidor se produce cuando los paquetes fluyen desde un cliente al servidor a través de los dispositivos de Citrix SD-WAN WANOP del lado del cliente y del lado del servidor. Sin embargo, en la ruta de retorno, los paquetes omiten el dispositivo Citrix SD-WAN WANOP del lado del servidor, pero atraviesan el dispositivo Citrix SD-WAN WANOP del lado del cliente.



Asimetría del lado del cliente:

La asimetría del lado del cliente se produce cuando los paquetes fluyen desde un cliente al servidor a través de los dispositivos de Citrix SD-WAN WANOP del lado del cliente y del lado del servidor. Sin embargo, en la ruta de retorno, los paquetes atraviesan el dispositivo Citrix SD-WAN WANOP del lado del servidor, pero omiten el dispositivo Citrix SD-WAN WANOP del lado del cliente.



Controle la asimetría en la red de Citrix SD-WAN WANOP

En la red de Citrix SD-WAN WANOP, cuando se produce una asimetría completa, se restablece la conexión TCP. Para evitar la interrupción de la conexión TCP y continuar enviando tráfico no acelerado, se introduce una lista de conexiones asimétricas en SD-WAN WANOP 10.1. Esta función está inhabilitada de forma predeterminada; puede habilitarla en los dispositivos SD-WAN WANOP del lado del cliente y del lado del servidor.

Al detectar una conexión asimétrica por primera vez, se restablece la conexión TCP entre el cliente y el servidor y se realiza una entrada de la tupla en la lista de conexiones asimétricas. La tupla consiste en la dirección IP del cliente y la dirección IP del servidor. Las conexiones posteriores de la tupla pasan sin aceleración. La tupla de conexión permanece en la lista de conexiones asimétricas durante un período de tiempo de espera predeterminado de cuatro horas o hasta que se detecte simetría. La transferencia no acelerada es efectiva hasta que se produzca el tiempo de espera o hasta que el dispositivo detecte dinámicamente que la asimetría ya no está presente.

Cuando se detecta asimetría del lado del cliente o asimetría del lado del servidor, se retiene la conexión TCP y los paquetes pasan a través del dispositivo de Citrix SD-WAN WANOP sin acelerar, de forma

predeterminada.

Para habilitar la lista de conexiones asimétricas en dispositivos de Citrix SD-WAN WANOP:

1. Acceda al símbolo del sistema CLI de WANOP (WANOP Accelerator/Broker IP).
2. Inicie sesión con las siguientes credenciales:

   Inicie sesión como: *cli***

   Inicio de sesión: ** ***admin***

   Contraseña: ** ***nsroot***

   > **Nota**
   >
   > La contraseña predeterminada para admin es *nsroot*. Si ha cambiado la contraseña, use la correcta.

3. Escriba el siguiente comando y presione Intro.

   Establezca el parámetro AsSymetricConnectionList.Enable en

   > **Nota**
   >
   > Puede configurar el período de tiempo de espera según el requisito de red mediante el comando *AssymetricConnectionList.AutoFlushDuration*.

   Hay varios parámetros disponibles con lista de asimetría que se pueden ajustar con precisión, según demanda, en función del entorno de red. Para obtener más información, póngase en contacto con el servicio de atención al cliente de Citrix

Complemento de cliente de Citrix SD-WAN WANOP

April 23, 2021

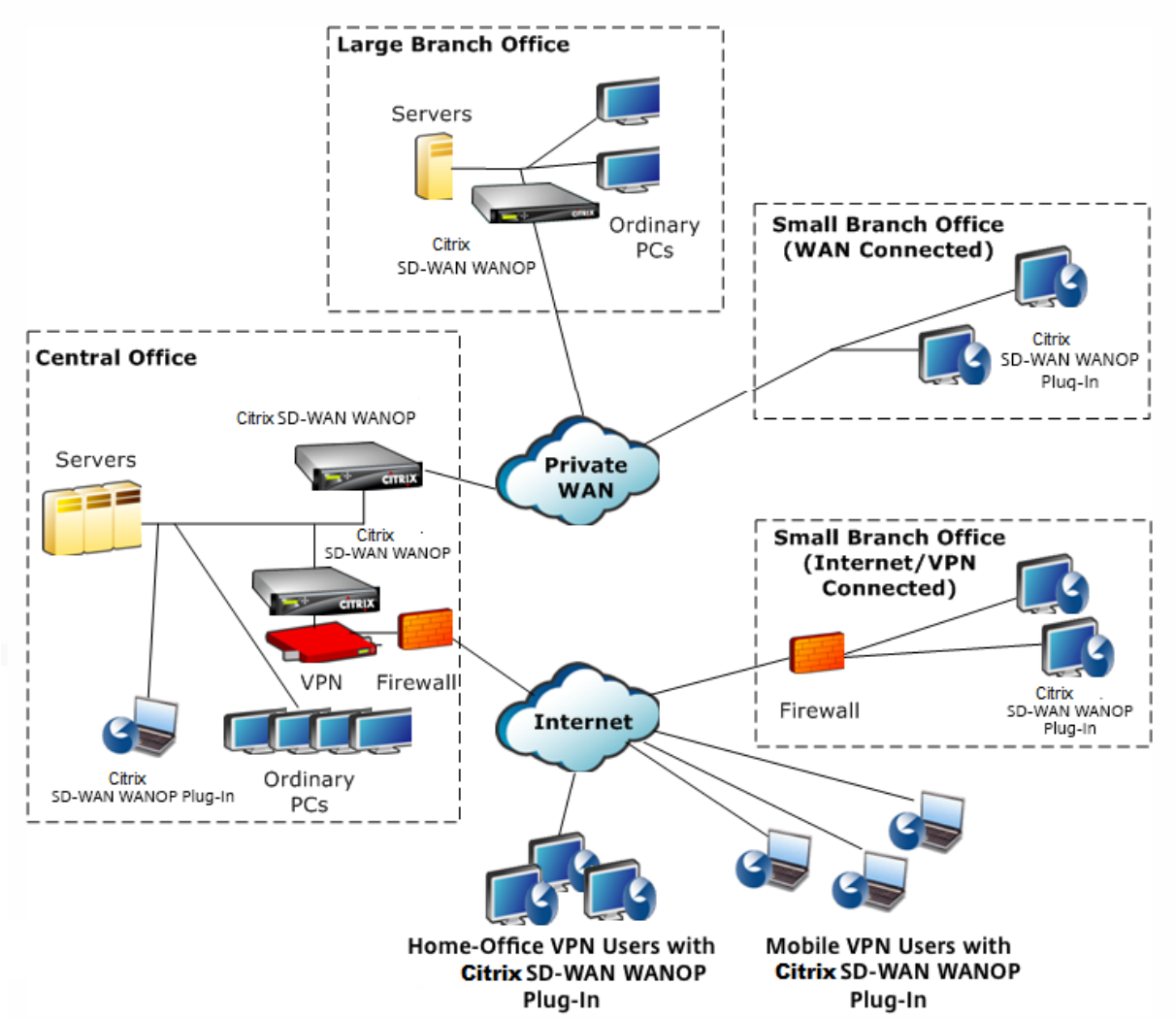
Citrix WANOP Client Plug-in es un acelerador de red basado en software que se ejecuta en portátiles y estaciones de trabajo Windows, lo que proporciona aceleración en cualquier lugar, no solo en oficinas con dispositivos WANOP Client Plug-in. Se conecta a un dispositivo Citrix WANOP en el otro extremo 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 en los otros extremos de los vínculos. Si personaliza el archivo MSI con las direcciones DNS o IP de los dispositivos WANOP 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



> **Nota**
>
> Citrix Receiver 1.2 o posterior admite el complemento, y Citrix Receiver puede distribuirlo y administrarlo.

Requisitos de hardware y software

April 23, 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
- 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 bits y 64 bits de Enterprise Edition)
- Windows 10 (versiones de 32 bits y 64 bits de Enterprise Edition)

En el lado del servidor, los siguientes dispositivos admiten actualmente implementaciones de WANOP Client Plug-in:

- 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 plug-in WANOP

April 23, 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 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 el plug-in y el dispositivo gestionan las conexiones: 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).

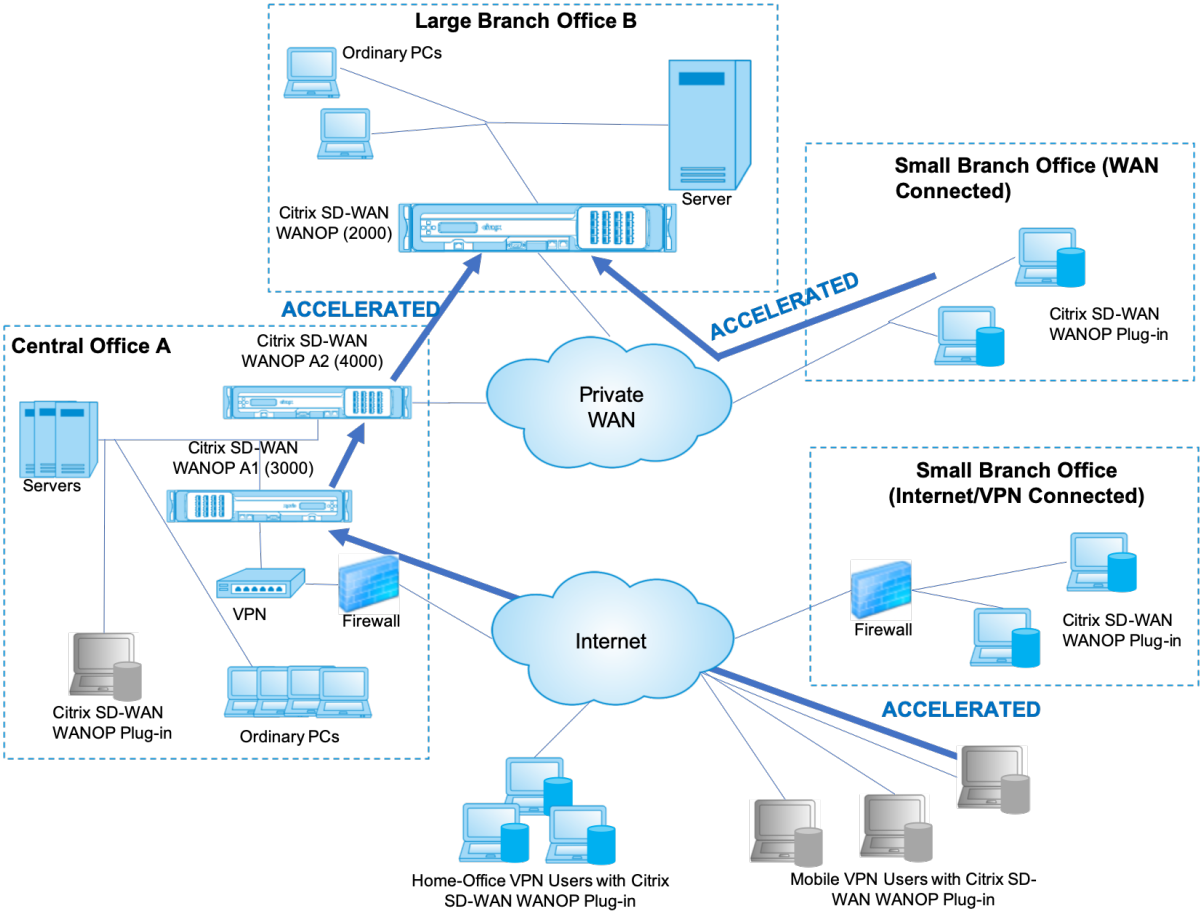
  Práctica recomendada: Utilice el modo transparente cuando pueda y el modo de redirección cuando sea necesario.

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



Nota

- Flujo de tráfico: el modo transparente acelera las conexiones entre un complemento de cliente de Citrix WANOP y un dispositivo habilitado para complementos.
- Licencias: Los dispositivos necesitan una licencia para admitir el número deseado de complementos. En el diagrama, Citrix SD-WAN WANOP A2 no necesita licencia para la aceleración de complementos, ya que Citrix SD-WAN WANOP 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, Citrix SD-WAN WANOP B. acelera el tráfico de usuarios de VPN móviles y de oficina doméstica que está destinado a la gran sucursal B con Citrix SD-WAN WANOP A1 y A2. Para que esto funcione, Citrix SD-WAN WANOP 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 dispositivo 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.

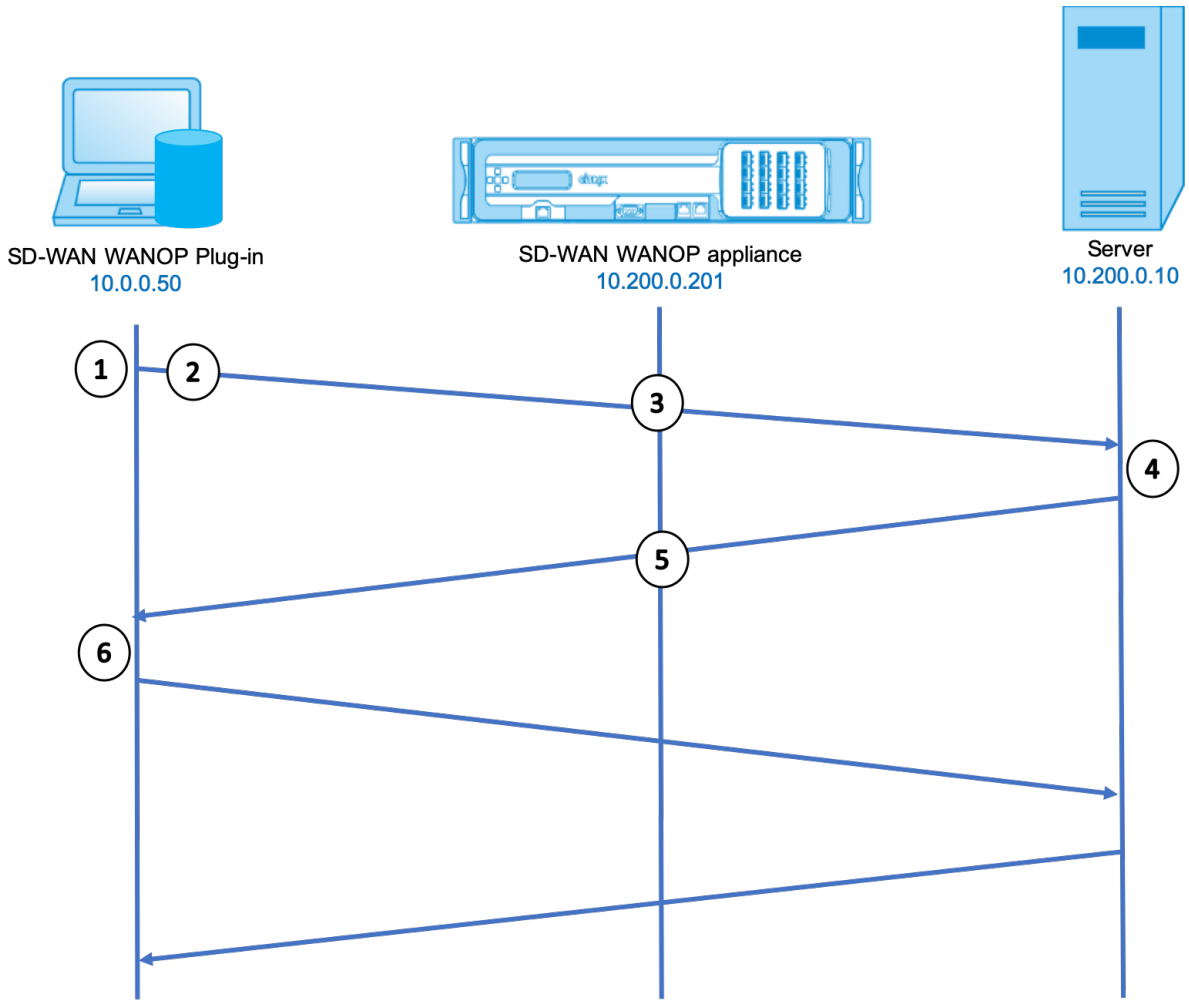
El modo transparente se asemeja a la aceleración de dispositivo a dispositivo, pero no es idéntico al mismo. Las diferencias son:

- 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



1. La aplicación del usuario abre una conexión TCP al servidor, enviando un paquete TCP SYN.

   Src: 10.0.0.50, Dst: 10.200.0.10

2. El plug-in WANOP busca la dirección de destino y comprueba que coincide con una subred acelerada por el dispositivo. Se adjunta opciones WANOP al encabezado TCP del paquete SYN. No se cambian las direcciones.

   Src: 10.0.0.50, Dst: 10.200.0.10

3. El dispositivo toma nota de las opciones SYN y reconoce que se trata de una conexión que se puede acelerar. Elimina las opciones del paquete y le permite pasar al servidor. No se cambian las direcciones.

   Src: 10.0.0.50, Dst: 10.200.0.10

4. El servidor acepta la conexión y responde con un paquete TCP SYN-ACK.

   Src: 10.200.0.10, Dst: 10.0.0.50

5. El dispositivo etiqueta el paquete SYN-ACK con una opción de encabezado TCP que muestra que se producirá la aceleración.

   Src: 10.200.0.10, Dst: 10.0.0.50

6. El plug-in WANOP recibe el paquete SYN-ACK. Las opciones en los encabezados de paquetes indican que la conexión está acelerada. El Plug-in elimina las opciones y pasa el paquete SYN-ACK a la aplicación. La conexión está ahora completamente abierta y acelerada.

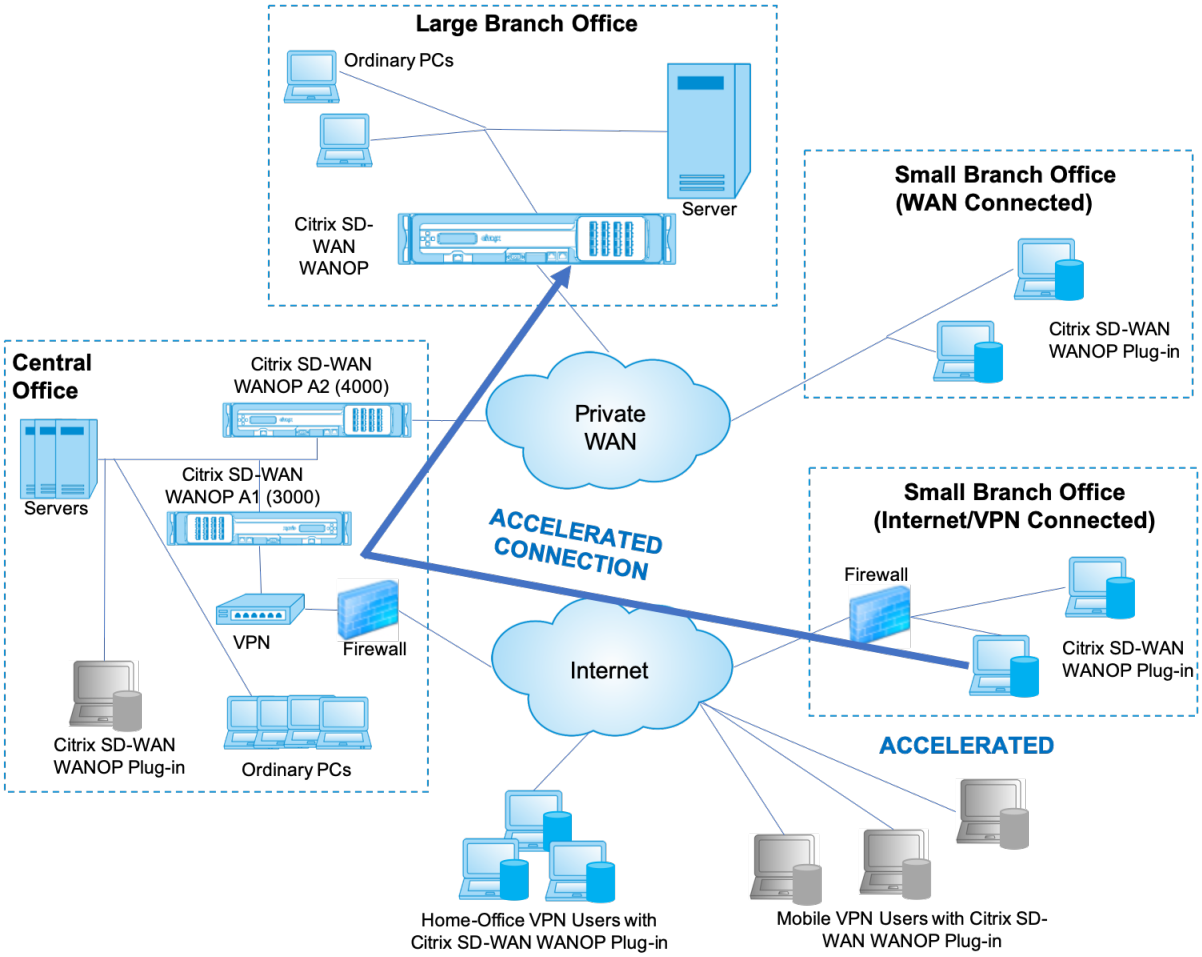
Modo Redirector

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.

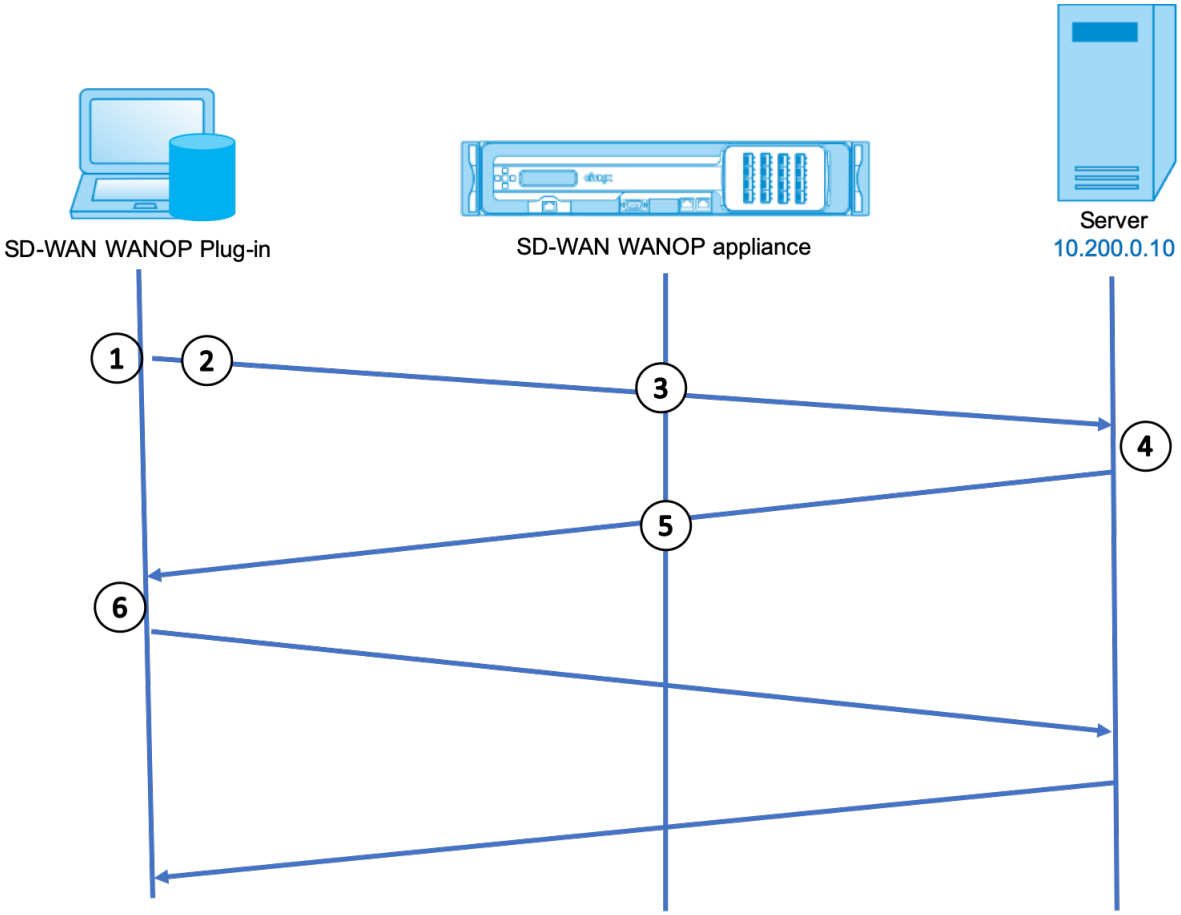
La siguiente imagen muestra cómo funciona el modo Redirector.

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



1. La aplicación del usuario abre una conexión TCP al servidor, enviando un paquete TCP SYN.

   Src: 10.0.0.50, Dst: 10.200.0.10

2. Citrix SD-WAN WANOP Plug-in busca la dirección de destino y decide redirigir la conexión al dispositivo en 10.200.0.201.

   Src: 10.0.0.50, Dst: 10.200.0.201

   (10.200.0.10 se conserva en un campo de opción TCP. Las opciones 24-31 se utilizan para varios parámetros.)

3. El dispositivo acepta la conexión y reenvía el paquete al servidor (mediante la dirección de destino del campo de opciones TCP) y se da a sí mismo como origen.

   Src: 10.200.0.201, Dst: 10.200.0.10

4. El servidor acepta la conexión y responde con un paquete TCP SYN-ACK.

   Src: 10.200.0.10, Dst: 10.200.0.201

5. El dispositivo vuelve a escribir las direcciones y reenvía el paquete al Plug-in (Colocación de la dirección del servidor en un campo de opción).

   Src: 10.200.0.201, Dst: 10.0.0.50

6. La conexión ahora está completamente abierta. El cliente y el servidor envían paquetes de ida y vuelta a través del dispositivo.

   Mientras que las direcciones se analizan en modo Redirector, los números de puerto de destino son nit (aunque el número de puerto efímero puede ser). Los datos no están encapsulados. El modo Redirector es un proxy, no un túnel.

   No hay relación 1:1 entre paquetes (aunque al final, los datos recibidos siempre son idénticos a los datos enviados). La compresión puede reducir muchos paquetes de entrada en un solo paquete. La aceleración de CIFS llevará a cabo operaciones especulativas de lectura anticipada y de retraso negativo. Además, si los paquetes se caen entre el dispositivo y el complemento Reperter, la retransmisión es manejada por el dispositivo, no el servidor, mediante algoritmos de recuperación avanzados.

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.

Implementar dispositivos para usarlos con complementos

April 23, 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.

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 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.

Definición de reglas: defina reglas de aceleración en el dispositivo, en la ficha **Configuración: WANOP Client Plug-in: Reglas de aceleración**.

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.

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.

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

April 23, 2021

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 debe ver Repeater.myCompany.com resolver 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 indeseables y confusos, especialmente si el servidor DNS gira el orden de las direcciones IP para cada solicitud.

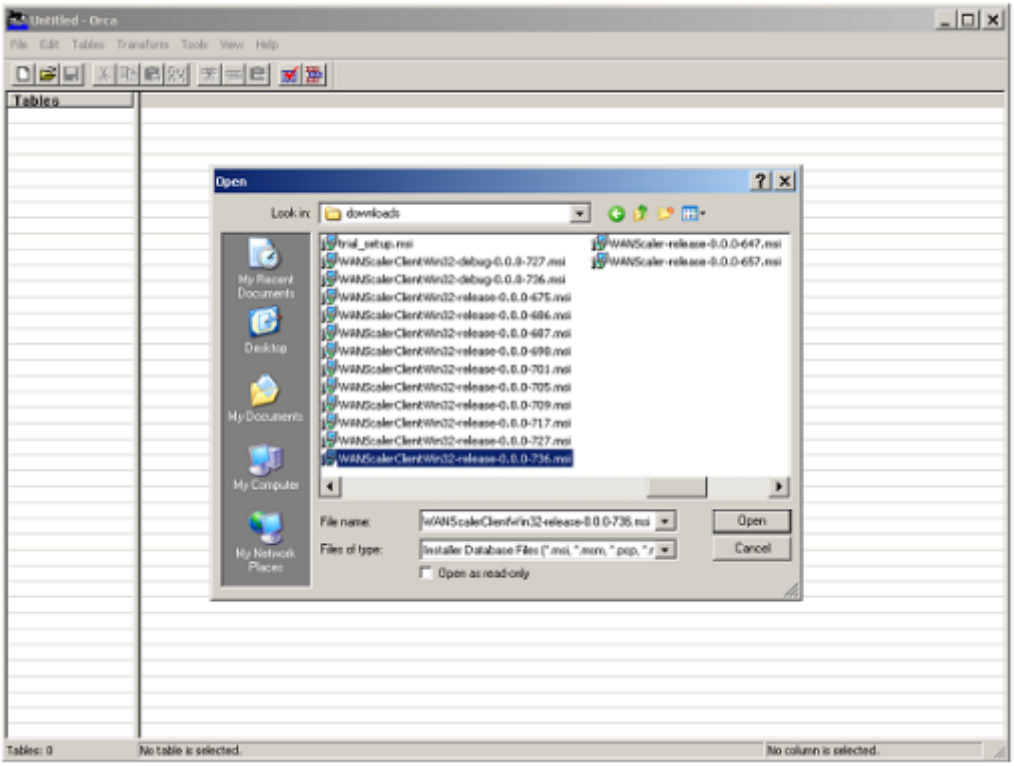
Instale el editor MSI de Orca:

Hay muchos editores MSI, incluyendo Orca, que es parte del SDK gratuito de plataforma de Microsoft y se puede descargar desde Microsoft.

Para instalar el editor MSI de Orca:

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.
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



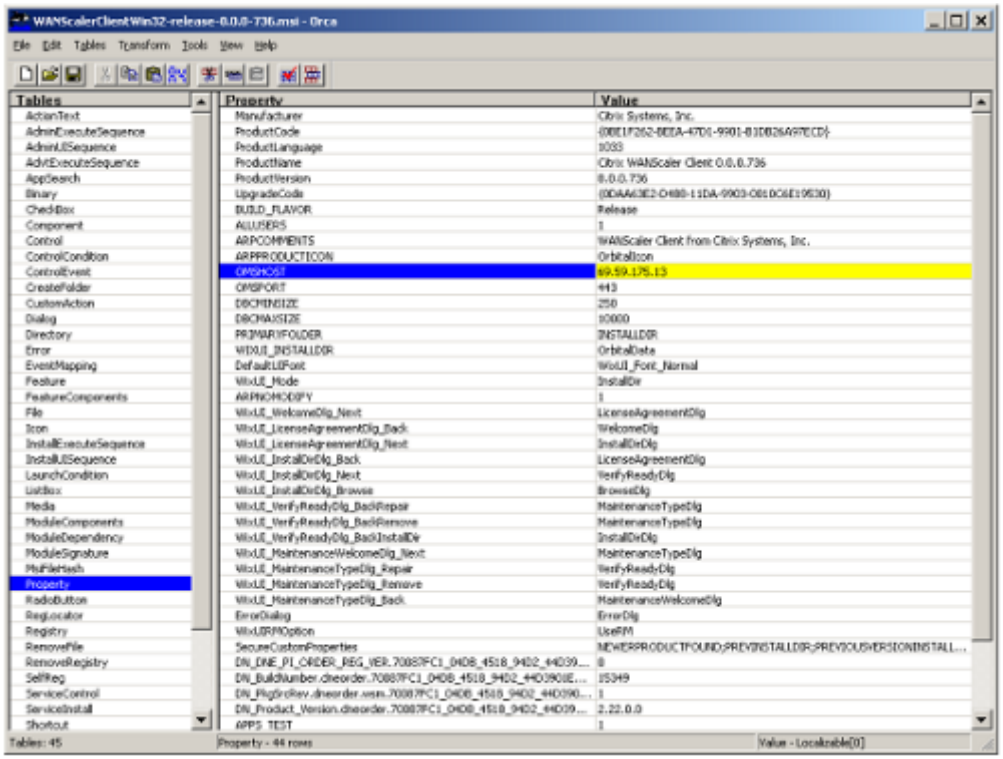
5. En el menú**Tablas**, haga clic en**Propiedad**. Aparecerá una lista de todas las propiedades modificables del archivo MSI. Modifique los parámetros que se muestran en la tabla siguiente. Para modificar un parámetro, haga doble clic en su valor, escriba el nuevo valor y pulse **Intro**.

   Para obtener más información, consulte la tabla.

   a) 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 editar un parámetro, haga doble clic en su valor, escriba el nuevo valor y pulse**Intro**.

      Para obtener más información, consulte la tabla.

      Figura 2: Modificar parámetros en Orca:



6. Cuando haya terminado, utilice el comando**Archivo: Guardar como**para guardar el archivo editado 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 Windows

April 23, 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.

> **Nota**
>
> La interfaz de usuario de WANOP Client Plug-in se refiere a sí misma como Citrix Acceleration Plug-in Manager.

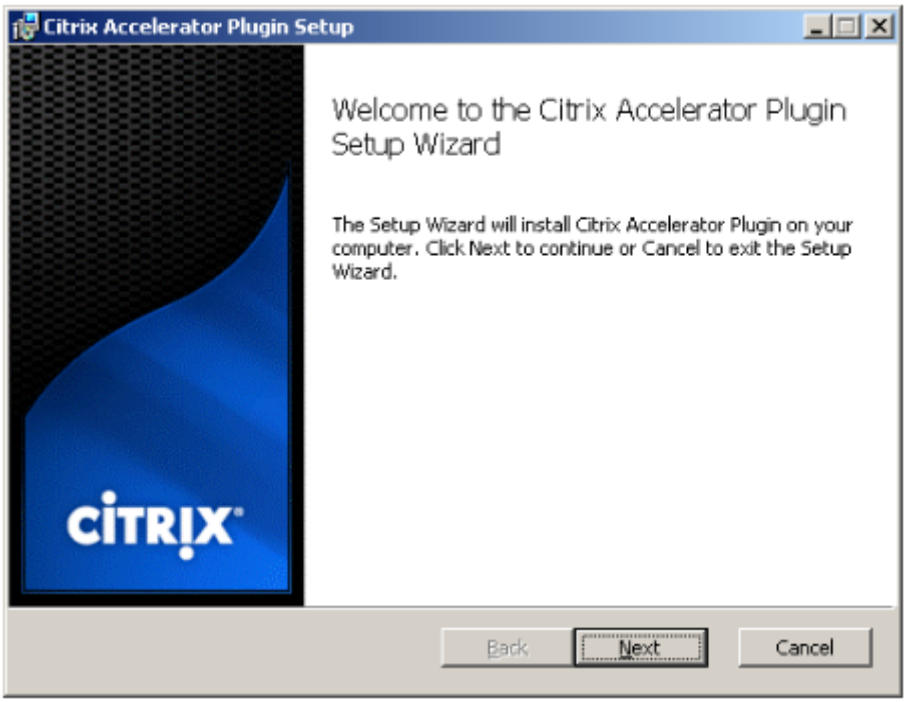
La única configuración de usuario que necesita el complemento es la lista de direcciones del dispositivo. Esta lista puede consistir en una lista separada por comas de direcciones IP o DNS. Las dos formas se pueden mezclar. Puede personalizar el archivo de distribución para que la lista señale al dispositivo 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

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:

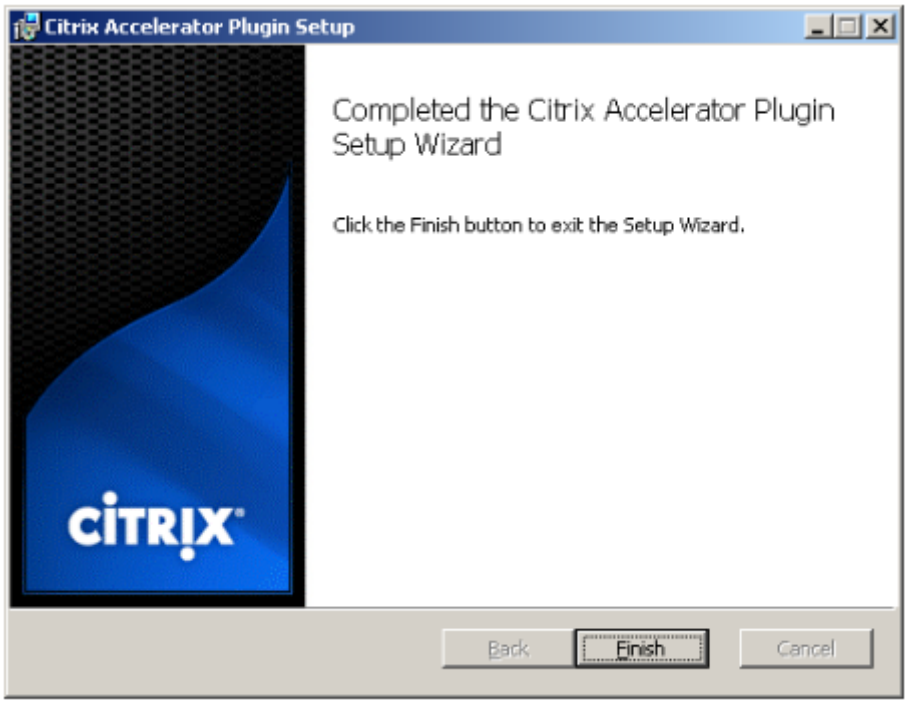
   

   Los pasos que se indican a continuación son para una instalación interactiva. Se puede realizar una instalación silenciosa con el comando:

   msiexec /i client_msi_file /qn

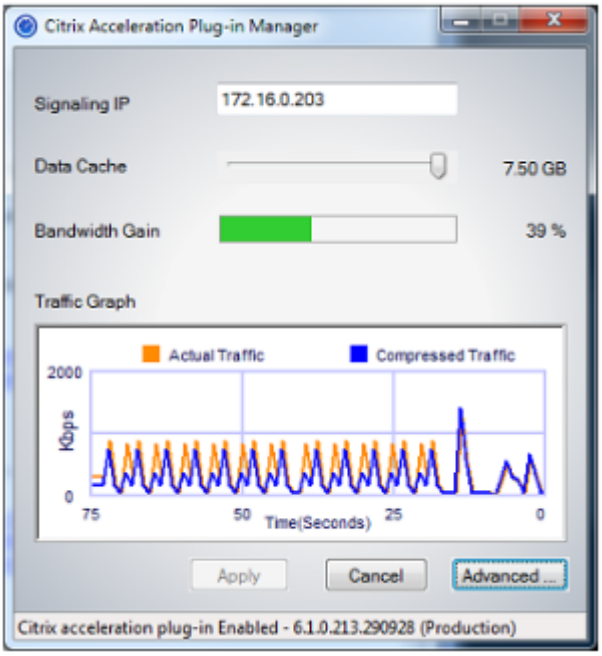
2. El programa de instalación solicita la ubicación en la que quiere instalar el software. El directorio que especifique se utiliza tanto para el software cliente como para el historial de compresión basado en disco. Juntos, requieren un mínimo de 500 MB de espacio en disco.
3. Cuando finalice el instalador, es posible que le pida que reinicie el sistema. Después de reiniciar, el complemento cliente WANOP se inicia automáticamente.

   Ilustración 2. Pantalla de 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, pantalla inicial (básica):



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:

- 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.

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.

GUI de plug-in de Citrix SD-WAN WANOP

April 23, 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.

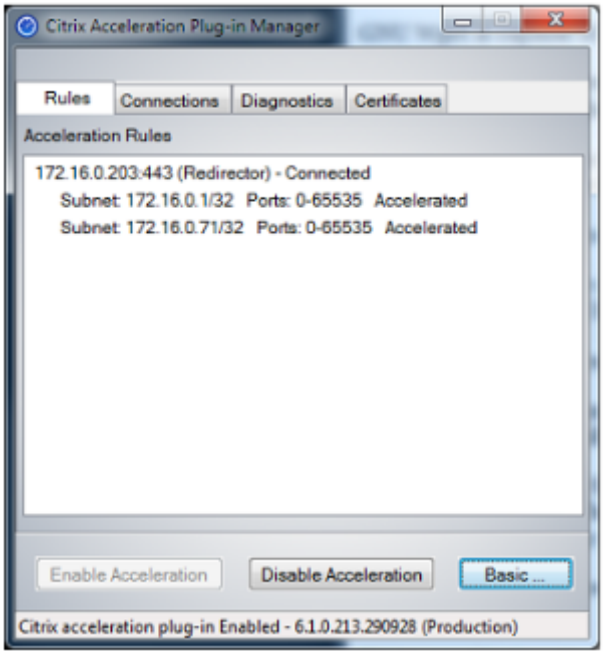
  Ejemplos: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- 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

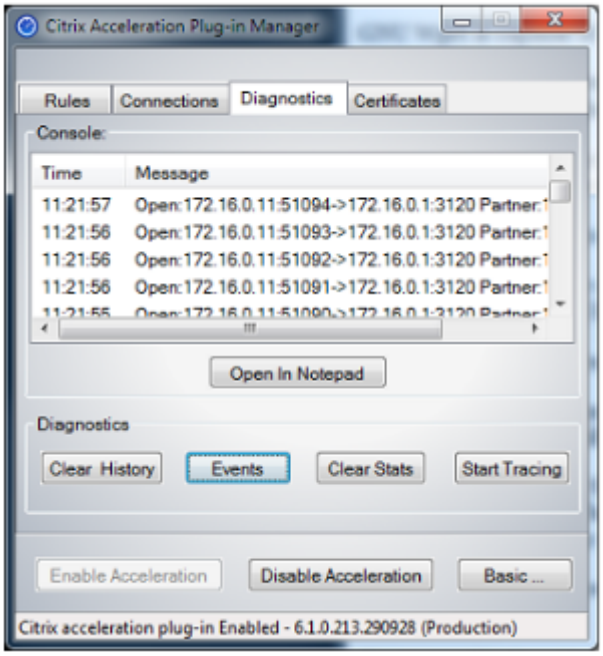
incluye conexiones CIFS aceleradas. Al hacer clic en Más, se abre una ventana con un breve resumen de cada conexión. (Todos los botones Más le permiten copiar la información de la ventana en el portapapeles, si quiere compartirla con Soporte).

- **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 Citrix Virtual Apps and Desktops 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

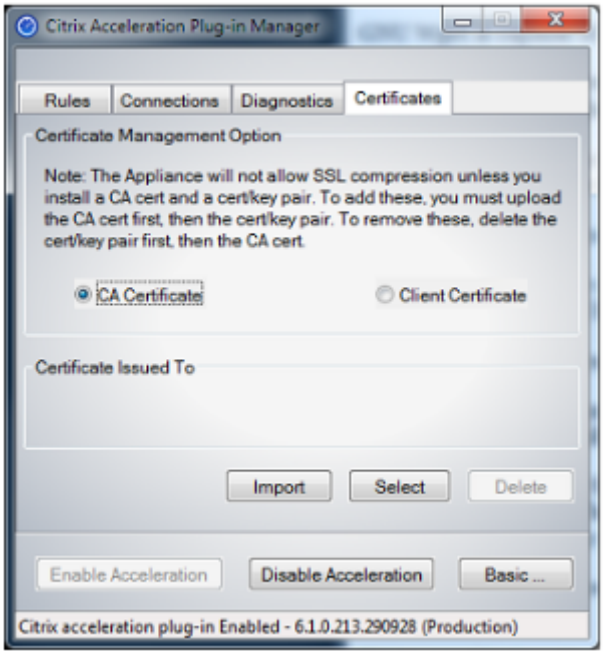
La página Diagnósticos indica el número de conexiones en diferentes categorías y otra información útil.

- **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.



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:

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 de Citrix SD-WAN WANOP

April 23, 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 cliente WANOP, 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**.

Reinicie el sistema para terminar de desinstalar el cliente.

Aceleración de Citrix Virtual Apps and Desktops

April 23, 2021

> **Nota**
>
> En esta discusión,*Virtual Apps*hace referencia a las secuencias del protocolo ICA y CGP. Por lo tanto, lo que se dice acerca de Virtual Apps se aplica también a Virtual Desktops.

La aceleración de Virtual Apps/Virtual Desktops (ICA/CGP) tiene tres componentes:

- **Compresión**: El dispositivo coopera con los clientes y servidores de Virtual Apps para comprimir los flujos de datos de Virtual Apps para datos interactivos (teclado/ratón/pantalla/audio) y datos por lotes (impresión y transferencias de archivos). Esta interacción tiene lugar de forma transparente y no requiere configuración del dispositivo. Se requiere una pequeña cantidad de configuración, que se describe a continuación, en los servidores Virtual Apps antiguos (versión 4.x).
- **ICA Multistream**: además de la compresión, los dispositivos WANOP de Citrix SD-WAN admiten el nuevo protocolo ICA Multistream, en el que se utilizan hasta cuatro conexiones para las diferentes prioridades ICA, en lugar de multiplexar todas las prioridades sobre la misma conexión. Este enfoque proporciona a las tareas interactivas una mayor capacidad de respuesta, especialmente cuando se combinan con el modelado del tráfico del dispositivo.
- Forma de**tráfico: el modelador**de tráfico WANOP de Citrix SD-WAN utiliza los bits de prioridad de los protocolos de datos de Virtual Apps para modular la prioridad de la conexión en tiempo real, haciendo coincidir el ancho de banda compartido de cada conexión con lo que la conexión está transmitiendo en este momento.

  > **Nota**
  >
  > El ICA multistream está inhabilitado de forma predeterminada. Se puede habilitar en la página Funciones. Multi-Stream ICA y AutoQoS requieren que se habilite la confiabilidad de la sesión.

Para optimizar las conexiones ICA para Citrix Virtual Apps and Desktops versión 7.0 y posterior, el dispositivo Citrix SD-WAN WANOP es compatible con Citrix Receiver para Chrome versión 1.4 y posterior, y Citrix Receiver para HTML5 versión 1.4 y posterior.

Protocolo de transporte HDX de UDP/EDT a TCP: En determinadas condiciones de red, UDP/EDT no se puede utilizar como protocolo optimizado para entregar tráfico HDX. Puede cambiar el protocolo a TCP para que WANOP pueda proporcionar:

- Ventajas de compresión/DDup
- Visibilidad (informes locales y HDX Insight)

WANOP puede bloquear el tráfico de EDT y forzar la sesión a TCP. Durante el inicio de la sesión, Citrix Receiver inicia la sesión tanto en TCP como en EDT. Si la sesión EDT no está establecida, entonces se utiliza la sesión TCP. WANOP GUI proporciona una opción para forzar la sesión en el protocolo TCP en la página de funciones.

Configurar la aceleración de Virtual Apps

April 23, 2021

La aceleración de Virtual Apps se aplica a los protocolos ICA y CGP dentro de Virtual Apps. Los dispositivos WANOP de Citrix SD-WAN, los servidores de aplicaciones virtuales y los clientes de aplicaciones virtuales proporcionan una aceleración cooperativa de las conexiones de aplicaciones virtuales, lo que proporciona una aceleración sustancial en comparación con las aplicaciones virtuales por sí solas. Esta cooperación requiere versiones actualizadas de los tres componentes.

La compresión de Virtual Apps cambia dinámicamente entre la compresión basada en memoria para canales interactivos (como el ratón, el teclado y los datos de pantalla) y la compresión basada en disco para tareas masivas (como transferencias de archivos y trabajos de impresión). Las relaciones de compresión aumentan a medida que se llena el historial de compresión, lo que aumenta la cantidad de datos que se pueden comparar con los datos nuevos. La compresión de Virtual Apps proporciona una reducción de datos varias veces mayor que Virtual Apps no asistido, a menudo superior a 50:1 en transferencias masivas repetitivas, como imprimir o guardar versiones sucesivas del mismo documento.

La compresión de Virtual Apps logra una alta utilización de enlaces sin congestión, ya que evita que los usuarios interfieran entre sí.

Para habilitar la aceleración de Virtual Apps

1. Compruebe la directiva de clase de servicio ICA. En la página Configuración: Clases de Servicio, la clase de servicio ICA debe mostrar el disco en la columna Aceleración y Prioridades ICA en la columna Modelado de Tráfico. Si no es así, modifique la definición de clase de servicio.
2. Actualice los servidores y clientes de Virtual Apps 4.x. (No es necesario en Virtual Apps 5.0 o posterior). Utilice Presentation Server 4.5 con paquete acumulativo de revisiones PSE450W2K3R03 (Beta) o posterior. Esta versión incluye el siguiente software de servidor y cliente, ambos deben estar instalados para la compresión de Virtual Apps:
   a) Paquete de servidor PSE450R03W2K3WS.msp o posterior.
   b) Versión de cliente 11.0.0.5357 o posterior.
3. Actualice los servidores y clientes de Virtual Desktops a la versión 4.0 o posterior.
4. Compruebe la configuración del Registro del servidor de Virtual Apps. (No es necesario en Virtual Apps 5.0 o posterior.) En los servidores de Virtual Apps, compruebe estos parámetros y corríjalos o créelos según sea necesario:


```
pre codeblock HKLM\System\CurrentControlSet\Control\Citrix\
WanScaler\EnableForSecureIca = 1 HKLM\System\CurrentControlSet
\Control\Citrix\WanScaler\EnableWanScalerOptimization = 1 HKLM\
System\CurrentControlSet\Control\Citrix\WanScaler\UchBehavior = 2
 <!--NeedCopy-->
```

Todos estos son valores DWORD.

5. Abra y utilice conexiones Virtual Apps, entre clientes y servidores de aplicaciones virtuales actualizados, que pasan por el WANOP actualizado de Citrix SD-WAN. De forma predeterminada, estas sesiones usan CGP. Para ICA, en el cliente, en Citrix Program Neighborhood, desmarque la casilla Conexiones ICA personalizadas. A continuación, haga clic con el botón secundario en un icono de conexión, vaya a **Propiedades** > **Opciones** y haga clic en la casilla de verificación **Habilitar confiabilidad de sesión**. Multi-Stream ICA y AutoQoS requieren que se habilite la confiabilidad de la sesión.
6. Verifica la aceleración.

   Después de iniciar las sesiones de Virtual Apps a través del vínculo acelerado, las conexiones ICA aceleradas deberían aparecer en la página Supervisión: Conexiones del dispositivo. Una relación de compresión superior a 1:1 indica que se está produciendo compresión.

Optimizar Citrix Receiver para HTML5

December 14, 2022

Aplicación que debe servir contenido dinámico funciona en HTML5 WebSockets. Citrix Receiver para Chrome y Citrix Receiver para HTML5 son aplicaciones compatibles con WebSockets HTML5. Estas aplicaciones tienen acceso simplificado a Virtual Desktops, ya que pueden integrarse con los exploradores web más recientes que admiten WebSockets HTML5.

> **Nota**
>
> No es necesario que realice ningún cambio en la configuración del dispositivo para utilizar esta función.

Cómo un dispositivo Citrix SD-WAN WANOP optimiza Citrix Receiver para HTML5

En la configuración típica de una sucursal y centro de datos, los recursos compartidos como Virtual Desktop Agent (VDA) se instalan en un servidor Citrix Hypervisor del centro de datos. Los clientes de las sucursales acceden a estos recursos compartidos a través de la red mediante Citrix Receiver.

En la configuración típica de una sucursal y centro de datos, los recursos compartidos como Virtual Desktop Agent (VDA) se instalan en un servidor Citrix Hypervisor del centro de datos. Los clientes de las sucursales acceden a estos recursos compartidos a través de la red mediante Citrix Receiver.

Al ser compatible con HTML, VDA utiliza un agente de escucha WebSocket que se ejecuta en el puerto 8008. Al acceder a una aplicación, el cliente inicia una conexión TCP en el puerto 8008 y la utiliza para enviar una solicitud HTTP al servidor para actualizar la conexión y utilizar el protocolo WebSocket. Después de que el cliente negocia la conexión WebSocket con VDA, comienzan las negociaciones de Independent Computing Architecture (ICA) y el cliente y el servidor utilizan ICA a través de HTML5 para intercambiar datos. Para obtener más información acerca de la secuencia de mensajes intercambiados entre el cliente y el servidor, vea Mensajes intercambiados entre el cliente y el servidor.

Una vez establecidas las conexiones entre los clientes y el servidor, el dispositivo Citrix SD-WAN WANOP comienza a optimizar las conexiones acelerando el tráfico a través de la red y acelerando la página web y otras aplicaciones mediante Citrix Receiver para HTML5. La funcionalidad de optimizar las conexiones de Citrix Receiver para HTML5 es similar a la aceleración HTTP.

> **Nota**
>
> - Para obtener más información acerca de HTML5, consulte Cómo funciona HTML5.
> - Para obtener más información acerca de Citrix Receiver para HTML5, consulte http://support.citrix.com/pro
> html5.html.
> - Para obtener más información acerca de los requisitos del sistema de Receiver para HTML5, consulte http://support.citrix.com/proddocs/topic/receiver-html5-14/receiver-html5-sys-req.html.

Configurar un dispositivo Citrix SD-WAN WANOP para optimizar Citrix Receiver para HTML5

La optimización de las conexiones de Citrix Receiver para HTML5 es una función de configuración cero. No es necesario que realice ningún cambio de configuración en el dispositivo. Al actualizar el software Citrix SD-WAN WANOP para la versión CB 7.3.1 o posterior, se crea el clasificador de aplicaciones alt-http en el dispositivo y se asigna este clasificador de aplicaciones al puerto 8008, que es el predeterminado para Virtual Desktops. Tan pronto como actualice el software del dispositivo, estará listo para optimizar las conexiones nativas de Chrome que utilizan Citrix Receiver para HTML5.

Si utiliza cifrado SSL para conexiones a través de Citrix Receiver para HTML5, las conexiones utilizan ICA a través de SSL. Para habilitar la aceleración ICA sobre SSL con Citrix Receiver para HTML5, debe configurar la aceleración SSL estándar, que incluye la dirección IP de destino adecuada en la clase de servicio y la asignación de perfiles SSL. Si planea implementar el dispositivo en modo proxy ICA, debe asignar la dirección VIP de StoreFront a los certificados de StoreFront. Del mismo modo, si planea implementar el dispositivo en cualquier modo de implementación de cifrado SSL de extremo a extremo,

debe asignar la dirección IP de VDA a certificados VDA.

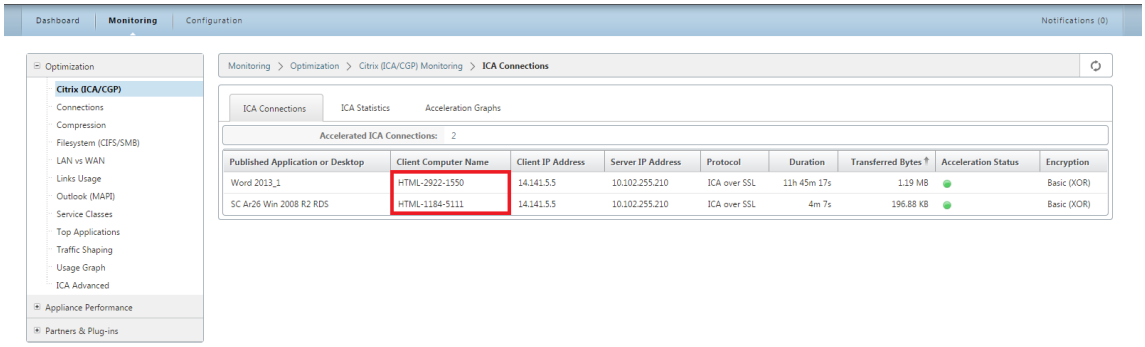
> **Advertencia**
>
> Asegúrese de no cambiar el número de puerto de la aplicación alt-http a ningún otro número de puerto. Si elimina este clasificador de aplicaciones o necesita realizar cambios en él, debe agregar el puerto 8008 al clasificador de aplicaciones HTTP.

Verificar las conexiones de Citrix Receiver para HTML5

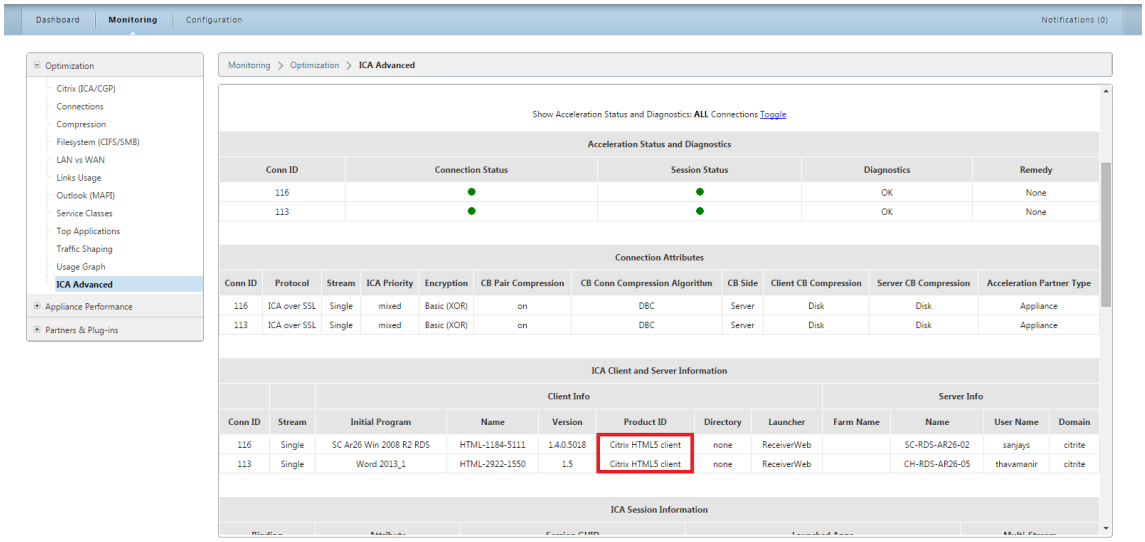
Para comprobar que el dispositivo está optimizando las conexiones de Citrix Receiver para HTML5, puede comprobar si las conexiones aparecen en las páginas de supervisión avanzada de Citrix (ICA/CGP) e ICA. La existencia de conexiones HTML5 en las páginas de supervisión indica que el dispositivo está optimizando las conexiones de Citrix Receiver para HTML5.

Para verificar la conexión de Citrix Receiver para HTML5 en un dispositivo Citrix SD-WAN WANOP:

1. Vaya a la página **Supervisión** > **Optimización** > **Citrix (ICA/CGP)**.
2. En la ficha **Conexiones ICA**, compruebe que se muestran las conexiones HTML5. Una conexión HTML5 se muestra con HTML como prefijo en la columna Nombre del equipo cliente, como se muestra en la siguiente captura de pantalla:



3. Acceda a la página **Supervisión > Optimización > ICA Advanced**.
4. En la ficha **Información de conexión**, desplácese hacia abajo hasta la sección Información de cliente y servidor ICA. Las entradas para conexiones HTML5 tienen cliente Citrix HTML5 en la columna ID del producto, como se muestra en la siguiente captura de pantalla:

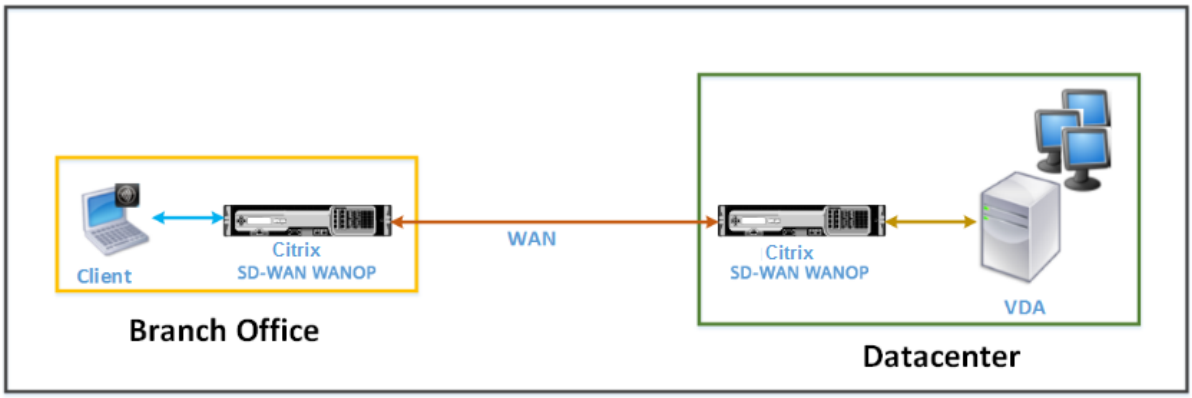


Modos de implementación

April 23, 2021

En una implementación típica de Citrix SD-WAN WANOP, los dispositivos WANOP de Citrix SD-WAN están emparejados entre sucursales y centros de datos. Instalar recursos compartidos, como VDA, en el centro de datos. Los clientes de varias sucursales acceden a los recursos del centro de datos mediante Citrix Receiver, como se muestra en la siguiente imagen.

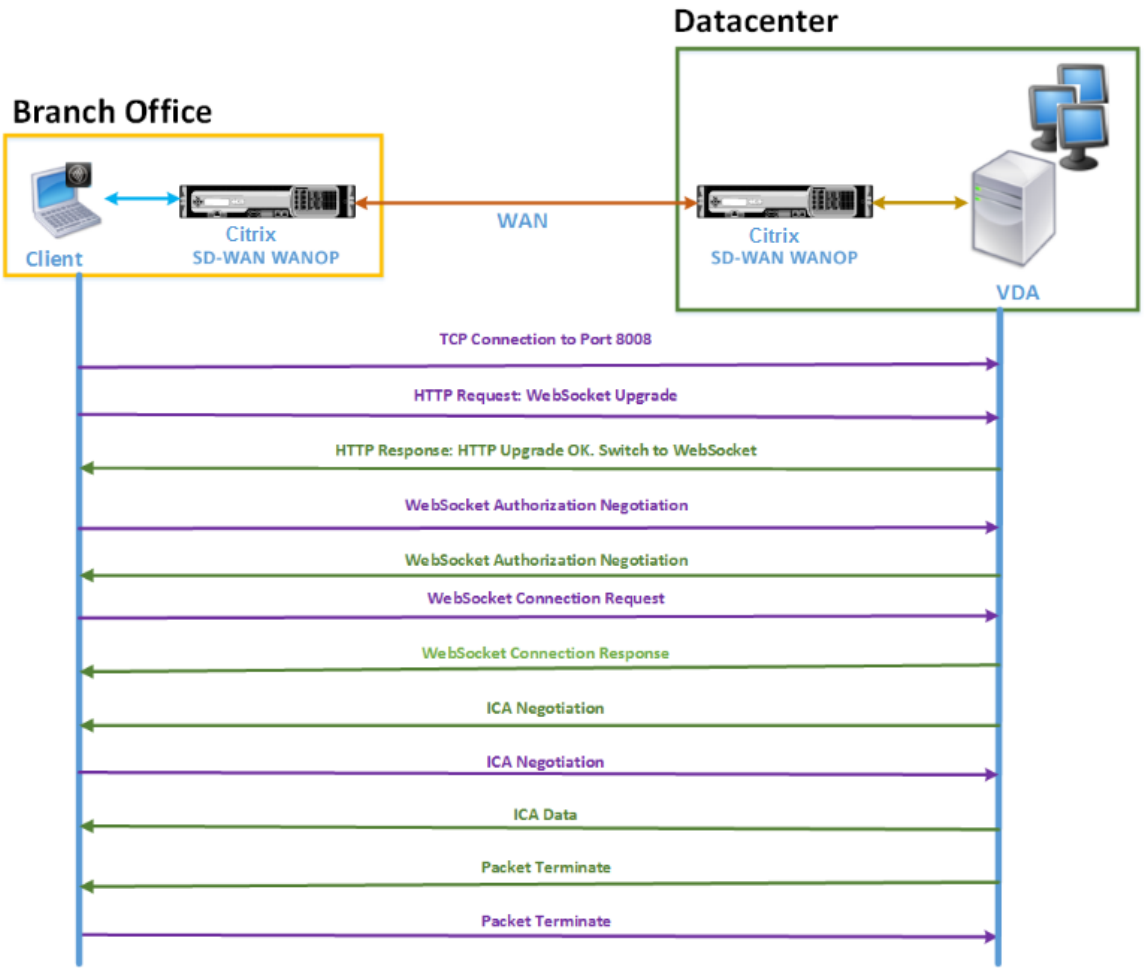
Una topología de implementación WANOP típica de Citrix SD-WAN



Los clientes instalan un producto de software Citrix Receiver, como Citrix Receiver para HTML5, en sus equipos locales y lo utilizan para acceder a los recursos del centro de datos. Las conexiones a través del par de dispositivos Citrix SD-WAN WANOP están optimizadas.

Comprender los mensajes intercambiados entre el cliente y el servidor

Al igual que con cualquier tipo de conexión de red, un cliente que utiliza Citrix Receiver para HTML5 intercambia varios mensajes con el servidor. La siguiente imagen muestra un flujo típico de mensajes entre el cliente y el servidor cuando se establece una conexión entre ellos.



Como se muestra en la imagen anterior, la siguiente secuencia de mensajes se intercambia entre el cliente y el servidor cuando un cliente de una sucursal desea acceder a los recursos del servidor del centro de datos:

1. El cliente utiliza Citrix Receiver para HTML5 para enviar una solicitud de conexión TCP al VDA en el puerto 8008.
2. Después de establecer la conexión TCP, el cliente envía una solicitud de actualización de WebSocket al VDA.
3. VDA responde a la solicitud de actualización y cambia al protocolo WebSocket.
4. El cliente y el VDA negocian la autorización de WebSocket.
5. El cliente envía una solicitud de conexión WebSocket al VDA.

6. VDA responde a la solicitud de conexión WebSocket.
7. VDA inicia la negociación ICA con el cliente.
8. Después de la negociación ICA, VDA comienza a transmitir datos ICA.
9. VDA envía un mensaje de finalización de paquetes.
10. El cliente responde con el mensaje de finalización del paquete.

> **Nota**
>
> El ejemplo anterior enumera los mensajes de ejemplo intercambiados por ICA a través de WebSocket. Si está utilizando ICA sobre el protocolo de puerta de enlace común (CGP), el cliente y el servidor negocian CGP en lugar de WebSocket. Sin embargo, para ICA sobre TCP, el cliente y el servidor negocian ICA.

Dependiendo de los componentes que haya implementado en la red, la conexión termina en diferentes puntos. La imagen anterior representa una topología que no tiene componentes adicionales implementados en la red. Como resultado, el cliente se comunica directamente con VDA en el puerto 8008. Sin embargo, si ha instalado una puerta de enlace, como Citrix Gateway, en el centro de datos, la conexión se establece con la puerta de enlace y proxies VDA. Hasta que la Gateway negocie la autorización de WebSocket, no hay comunicación con VDA. Después de que la puerta de enlace haya negociado la autorización de WebSocket, abre una conexión con VDA. A partir de entonces, la Gateway actúa como intermediario y pasa mensajes del cliente al VDA y viceversa.

Del mismo modo, si se crea un túnel VPN entre un complemento de Citrix Gateway instalado en el cliente y Citrix Gateway instalado en el centro de datos, la puerta de enlace reenvía de forma transparente todos los mensajes del cliente, inmediatamente después de establecer una conexión TCP, a VDA, y viceversa.

> **Nota**
>
> Para optimizar una conexión que requiere cifrado SSL de extremo a extremo, se establece una conexión TCP en el puerto 443 del VDA.

Modos de implementación compatibles

Al configurar un dispositivo Citrix SD-WAN WANOP para optimizar Citrix Receiver para HTML5, puede considerar cualquiera de los siguientes modos de implementación, dependiendo de los requisitos de red. Para optimizar las conexiones de Citrix Receiver para HTML5, los dispositivos Citrix SD-WAN WANOP admiten los siguientes modos de implementación:

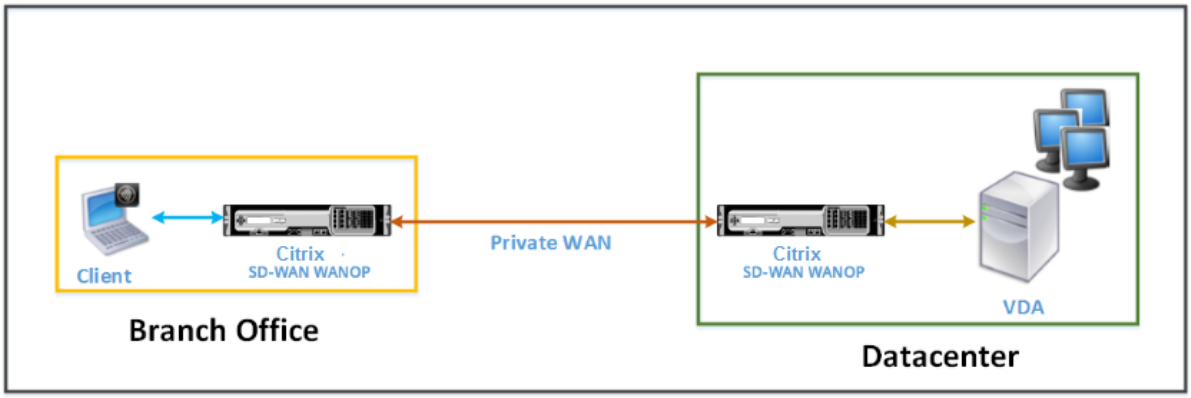
- Acceso directo
- Acceso directo con cifrado SSL de extremo a extremo

- Modo de proxy ICA
- Modo de proxy ICA con cifrado SSL de extremo a extremo
- Modo de red privada virtual completa (VPN)
- Modo de red privada virtual completa (VPN) con cifrado SSL de extremo a extremo

Acceso directo:

La siguiente imagen muestra la topología de implementación de Citrix Receiver para HTML5 instalada en el cliente en el modo de acceso directo.

Dispositivos Citrix SD-WAN WANOP implementados en modo de acceso directo



En el modo de acceso directo, se instala un par de dispositivos Citrix SD-WAN WANOP en una sucursal y en el centro de datos en modo inline. Un cliente accede a los recursos de VDA a través de Citrix Receiver para HTML5 a través de la WAN privada. Las conexiones desde el cliente a los recursos de VDA se protegen mediante el cifrado en el nivel ICA. Los mensajes intercambiados entre el cliente y el VDA se explican en Descripción de los mensajes intercambiados entre el cliente y el servidor.

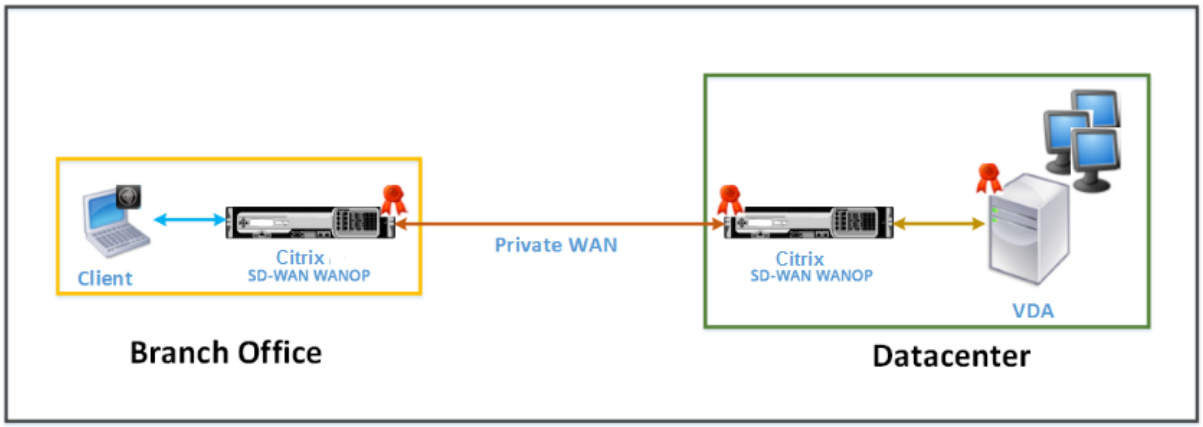
Los dispositivos Citrix SD-WAN WANOP instalados entre el cliente y el centro de datos VDA optimizan las conexiones de Citrix Receiver para HTML5 establecidas entre ellos.

Una implementación de acceso directo es adecuada para una intranet corporativa en la que los clientes se conectan sin usar Citrix Gateway ni ningún otro firewall. Implementar una configuración con acceso directo cuando los dispositivos Citrix SD-WAN WANOP se implementan en modo en línea y un cliente de una WAN privada se conecta a los recursos del VDA.

Acceso directo con cifrado SSL de extremo a extremo:

La siguiente imagen muestra la topología de implementación de Citrix Receiver para HTML5 instalada en el cliente en el modo de acceso directo protegido con cifrado SSL de extremo a extremo.

Dispositivos Citrix SD-WAN WANOP implementados en modo de acceso directo protegidos con cifrado SSL de extremo a extremo



El acceso directo con el modo de cifrado SSL de extremo a extremo es similar al modo de acceso directo, con la diferencia de que la conexión entre el cliente y los recursos de VDA está protegida por el cifrado SSL y utiliza el puerto 443 en lugar del puerto 8008 para la conexión.

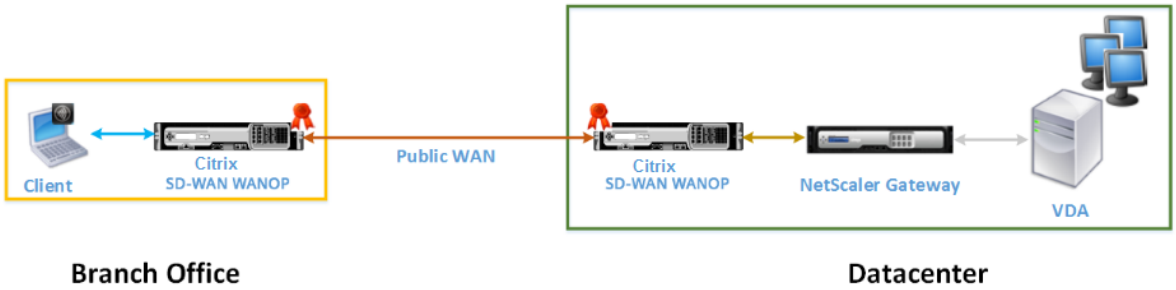
En esta implementación, la comunicación entre un par de dispositivos Citrix SD-WAN WANOP se asegura al hacer que los dos dispositivos sean socios seguros. Esta implementación es adecuada para una red corporativa en la que las conexiones entre el cliente y los recursos de VDA están protegidas mediante el cifrado SSL.

> **Nota**
>
> Debe configurar los certificados adecuados en los dispositivos para crear asociados seguros. Para obtener más información acerca de la asociación segura, consulte Peering seguro.

Modo de proxy ICA:

La siguiente imagen muestra la topología de implementación de Citrix Receiver para HTML5 instalada en el cliente en modo proxy ICA.

Dispositivos Citrix SD-WAN WANOP implementados en modo proxy ICA



En el modo proxy ICA, se instala un par de dispositivos Citrix SD-WAN WANOP en toda la sucursal y un centro de datos en modo en línea. Además, instale Citrix Gateway, que es proxy de VDA, en el centro de datos. Un cliente accede a los recursos de VDA a través de Citrix Receiver para HTML5 a través de

la WAN pública. Dado que la puerta de enlace es proxy del VDA, se establecen dos conexiones: una conexión SSL entre el cliente y Citrix Gateway y una conexión segura ICA entre Citrix Gateway y VDA. Citrix Gateway establece una conexión con recursos VDA en nombre del cliente. Las conexiones desde la Gateway a los recursos de VDA se protegen mediante el cifrado en el nivel ICA.

Los mensajes intercambiados entre el cliente y el VDA se explican en Descripción de los mensajes intercambiados entre el cliente y el servidor.Sin embargo, en este caso, la conexión finaliza en Citrix Gateway. La puerta de enlace hace de proxy en el VDA y abre una conexión a VDA solo después de que haya negociado la autorización de WebSocket. A continuación, la Gateway pasa de forma transparente los mensajes del cliente al VDA y viceversa.

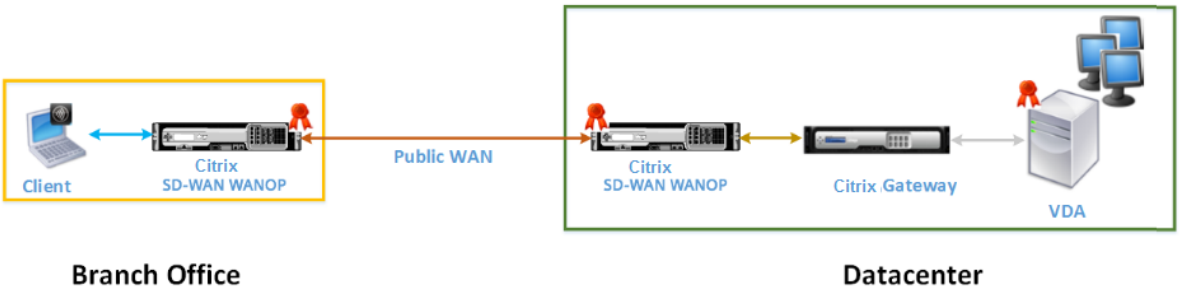
Si espera que los usuarios accedan a los recursos de VDA desde una WAN pública, puede considerar la implementación de la configuración del modo de proxy ICA.

> **Nota**
>
> Debe configurar los certificados adecuados en los dispositivos para crear asociados seguros. Para obtener más información acerca de la asociación segura, consulte Peering seguro.

Modo proxy ICA con cifrado SSL de extremo a extremo:

La siguiente imagen muestra la topología de implementación de Citrix Receiver para HTML5 instalada en el cliente en modo proxy ICA protegido con cifrado SSL de extremo a extremo.

Dispositivos WANOP de Citrix SD-WAN implementados en modo proxy ICA protegidos con cifrado SSL de extremo a extremo



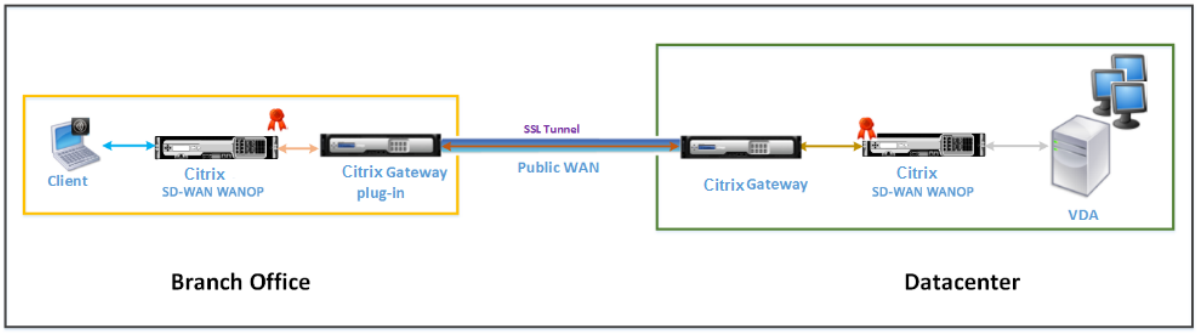
El modo Proxy ICA con modo de cifrado SSL de extremo a extremo es similar al modo Proxy ICA normal, con la diferencia de que la conexión entre Citrix Gateway y VDA está asegurada mediante cifrado SSL en lugar de utilizar una conexión segura ICA. En este escenario, debe instalar los certificados adecuados en el dispositivo Citrix SD-WAN WANOP y en el VDA. La conexión entre Citrix Gateway y VDA utiliza el puerto 443 en lugar del puerto 8008, como en el caso del modo Proxy ICA ordinario.

Esta implementación es adecuada para una red en la que debe proteger la comunicación integral entre los clientes y el VDA, incluida la conexión entre Citrix Gateway y VDA.

Modo de red privada virtual completa (VPN):

En la siguiente imagen se muestra la topología de implementación de Citrix Receiver para HTML5 instalada en el cliente en el modo de red privada virtual (VPN) completo.

Dispositivos Citrix SD-WAN WANOP implementados en modo VPN



En el modo VPN completo, se instala un par de dispositivos Citrix SD-WAN WANOP en una sucursal y en el centro de datos en modo en línea. Además de Citrix Receiver para HTML5, instale el complemento Citrix Gateway en el cliente y Citrix Gateway interconectando la red externa en el centro de datos. El complemento Citrix Gateway en el cliente y Citrix Gateway en el centro de datos crean un túnel SSL o VPN a través de la red cuando establecen una conexión. Como resultado, el cliente tiene un acceso seguro directo a los recursos del VDA, con una conexión transparente a través del dispositivo Citrix SD-WAN WANOP. Cuando la conexión del cliente finaliza en Citrix Gateway, la puerta de enlace abre una conexión transparente al puerto 8008 del VDA.

Los mensajes intercambiados entre el cliente y el VDA se explican en la sección Descripción de los mensajes intercambiados entre el cliente y el servidor. Sin embargo, en este caso, la conexión finaliza en Citrix Gateway. La Gateway hace proxy VDA y abre una conexión transparente a VDA en el puerto 8008, y pasa de forma transparente todos los mensajes del cliente al VDA y viceversa.

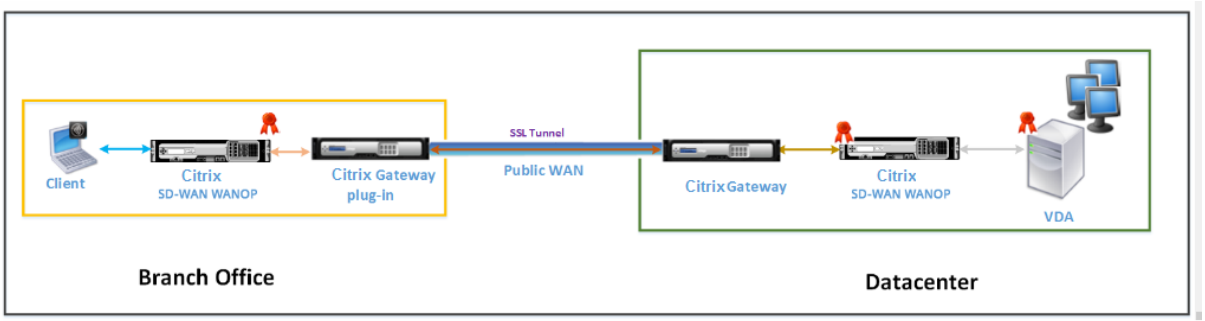
El complemento WANOP de Citrix SD-WAN permite al cliente acceder a los recursos independientemente de la ubicación del cliente. Cuando espera que los clientes necesiten acceso a los recursos de VDA desde ubicaciones distintas de sus escritorios, puede implementar la configuración en modo de red privada virtual (VPN) completa.

Esta implementación es adecuada para las organizaciones que esperan que sus empleados accedan a los recursos cuando viajan.

Modo de red privada virtual completa (VPN) con cifrado SSL de extremo a extremo:

La siguiente imagen muestra la topología de implementación de Citrix Receiver para HTML5 instalada en el cliente en el modo VPN completo protegido con cifrado SSL de extremo a extremo.

Dispositivos WANOP de Citrix SD-WAN implementados en modo VPN protegidos con cifrado SSL de extremo a extremo



El modo de red privada virtual completa (VPN) con implementación de cifrado SSL de extremo a extremo es similar al modo VPN completo normal, con la diferencia de que la comunicación entre Citrix Gateway y VDA está protegida mediante cifrado SSL y utiliza el puerto 443 en lugar del puerto 8008.

Esta implementación es adecuada para organizaciones que necesitan cifrado SSL de extremo a extremo para los recursos a los que acceden los empleados que viajan.

Interoperabilidad del transporte adaptable

April 23, 2021

El transporte adaptable es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops. Es más rápido y escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones de Internet y WAN difíciles de largo recorrido. El transporte adaptable mantiene la alta escalabilidad de servidores y un uso eficiente del ancho de banda. Al usar el transporte adaptable, los canales virtuales ICA responden automáticamente a las cambiantes condiciones de red. Cambian de forma inteligente el protocolo subyacente entre el protocolo de Citrix (denominado Enlightened Data Transport o EDT) y TCP para conseguir el mejor rendimiento.De forma predeterminada, el transporte adaptativo está habilitado y se utiliza EDT cuando es posible, con retroceso a TCP.

Citrix SD-WAN WANOP ofrece compresión tokenizada entre sesiones (deduplicación de datos), incluido el almacenamiento en caché de vídeo basado en URL. Proporciona una reducción significativa del ancho de banda si dos o más personas en la ubicación de la oficina ven el mismo vídeo obtenido por el cliente o transfieren o imprimen partes significativas del mismo archivo o documento. Además, al ejecutar los procesos de reducción de datos ICA y compresión de trabajos de impresión en el dispositivo de la sucursal, WANOP ofrece la descarga de la CPU del servidor VDA y permite una mayor escalabilidad del servidor de Citrix Virtual Apps and Desktops.

Cuando se utiliza TCP como protocolo de transporte de datos, Citrix SD-WAN WANOP admite la optimización como se describe anteriormente. Cuando utilice Citrix SD-WAN WANOP en conexiones de red, elija TCP y deshabilite EDT. Mediante el uso del control de flujo TCP y el control de congestión, Citrix SD-WAN WANOP garantiza la interactividad equivalente a EDT con una latencia alta y una pérdida

moderada de paquetes.

Para obtener información sobre cómo configurar el transporte adaptativo en Citrix Virtual Apps and Desktops, consulteTransporte adaptable.

Actualización de versión de Citrix Hypervisor 6.5

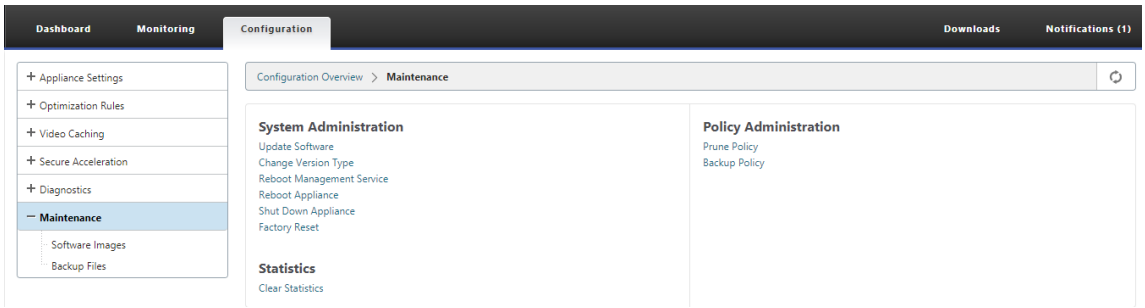
April 23, 2021

> **Importante**
>
> **Para actualizar a Citrix Hypervisor versión 6.5, los dispositivos deben ejecutar el software Citrix SD-WAN WANOP versión 9.0.x o posterior.**
>
> **Nota**
>
> No intente realizar la actualización cuando el dispositivo se esté ejecutando en una versión de software inferior a la versión 9.0.x para evitar problemas de actualización.

Cómo actualizar a Citrix Citrix Hypervisor 6.5

Para actualizar a Citrix Hypervisor 6.5 en dispositivos SD-WAN WANOP, asegúrese de que el dispositivo ejecuta la versión de software 9.0.x o posterior. Si los dispositivos están ejecutando una versión de versión de software anterior, actualice primero a la versión de software más reciente.

1. En Citrix SD-WAN WANOP GUI, vaya a **Configuración** > **Mantenimiento** > **Actualizar software**.Descargue el <Build_No> archivo *ns-sdw-wo- .upg* para actualizar el dispositivo.



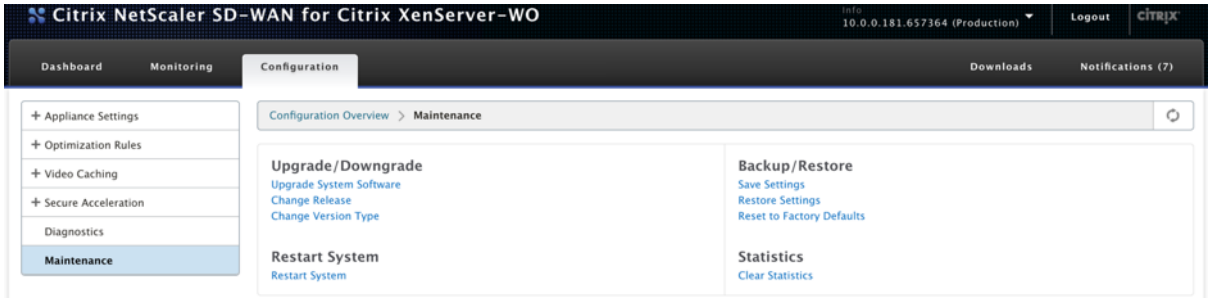
2. Después de actualizar a la última versión de software del software WANOP, vaya a **Configuración > Mantenimiento > Actualizar software** en la GUI.Cargue el archivo *ns-sdw-xen65-pkg_v1.5.upg*.

3. Espere aproximadamente 20 minutos para que se complete la actualización.El dispositivo se reinicia después de que la actualización se haya completado correctamente.

Mantenimiento

April 23, 2021

Utilice la página **Mantenimiento** para realizar actividades de mantenimiento como actualizar el software del sistema, realizar copias de seguridad y restaurar configuraciones y borrar estadísticas.



Actualizar/Bajar de categoría

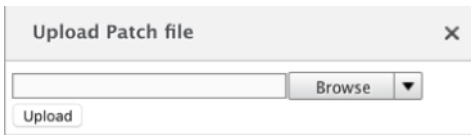
Actualizar el software del sistema

Existe un paquete de software de Citrix SD-WAN diferente para cada modelo de dispositivo. Debe descargar el paquete de software WANOP SD-WAN adecuado para un dispositivo que desee incluir en una red y guardarlo en la unidad local.

El software del dispositivo se actualiza mediante archivos de revisión que obtiene de Citrix.

> **NOTA**:
>
> Si los dispositivos ejecutan una versión de versión de software anterior, primero debe actualizar a la versión de software más reciente.

Para actualizar el software del sistema, vaya a **Configuración > Mantenimiento**. Seleccione **Actualizar software del sistema** en **Actualización/Desactualización**. Seleccione el archivo de revisión y cárguelo en el dispositivo.



El dispositivo examinará el archivo de revisión. Solo un archivo de revisión válido puede actualizar el sistema a una versión diferente de la que se está utilizando actualmente.

Una actualización conserva los archivos de licencia y la configuración del sistema. La unidad actualizada no requiere reconfiguración excepto para las funciones nuevas que se hayan agregado con la nueva versión.

Cambiar versión

La página de lanzamiento de cambios muestra la versión instalada actualmente. Si desea cambiar la versión de lanzamiento, haga clic en **Cambiar opción de lanzamiento**, seleccione la versión en la lista desplegable y haga clic en **Cambiar**.

Cambiar tipo de versión

La opción **Cambiar tipo de versión** le permite seleccionar una versión de depuración de la versión. Puede seleccionar el tipo de versión en la lista desplegable **Tipo** y hacer clic en **Cambiar**. Las siguientes son las posibles versiones de depuración:

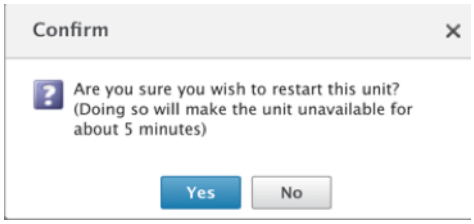
- Predeterminado
- Nivel 1
- Nivel 2
- MC predeterminado
- Nivel 1 MC
- Nivel 2 MC

Debe realizar esta acción según las instrucciones del equipo de soporte.

Reiniciar el sistema

Una vez instalado un parche, aparecerá un mensaje emergente en el que se preguntará si se puede reiniciar el dispositivo. El parche no se aplicará hasta que se reinicie el dispositivo. Si selecciona no reiniciar el sistema inmediatamente, se colocará un recordatorio en la parte superior de cada página.

Haga clic en **Reiniciar sistema** para reiniciar el dispositivo WANOP SD-WAN. Este proceso toma varios minutos.



Configuración de copia de seguridad

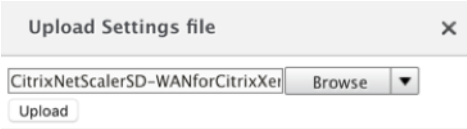
Puede realizar una copia de seguridad de la configuración del dispositivo guardándola como archivo de texto.

Haga clic en **Guardar configuración**, se descargará un archivo de texto en la unidad local. Los archivos de licencia, los parámetros SSH y las direcciones IP de la página IP de administración no se pueden guardar. El archivo es un archivo de texto ordinario, pero no debe modificarse manualmente.

Restaurar configuración

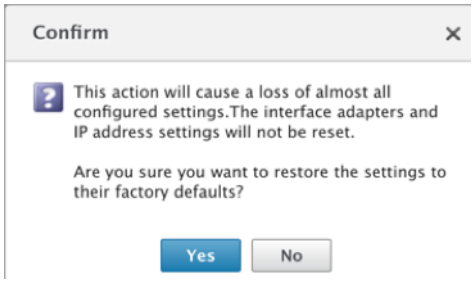
Una vez guardado el archivo, se puede restaurar en el mismo dispositivo WANOP SD-WAN.

El dispositivo mantiene copias de versiones anteriores. La opción**Restaurar configuración** ayuda a restaurar la configuración configurada. Los archivos de licencias, los parámetros SSH y las direcciones IP de la página Administración IP no se copian de la versión más reciente a la anterior. En su lugar, el dispositivo volverá a la configuración que estaba en vigor en el momento en que se actualizó la versión anterior.



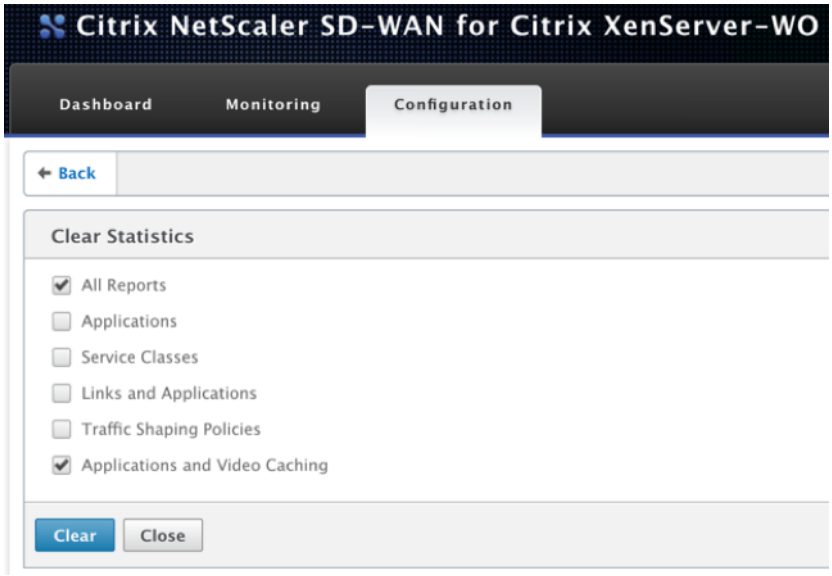
Restablecer los valores predeterminados de fábrica

La opción**Restablecer a los valores predeterminados de fábrica** permite restablecer los ajustes. Establece todos los parámetros excepto las direcciones IP, la configuración de ancho de banda y las licencias a sus valores predeterminados de fábrica. Haga clic en **Restablecer a los valores predeterminados de fábrica**, aparecerá un mensaje de confirmación. Haga clic en **Sí** si desea restaurar la configuración a los valores predeterminados de fábrica.



Borrar estadísticas

La página**Borrar estadísticas** permite restablecer las estadísticas del dispositivo SD-WAN WANOP. También permite crear informes que comienzan al principio de la ventana de muestreo deseada. Seleccione las opciones de estadística que desea borrar del dispositivo y haga clic en **Borrar**.



Diagnóstico

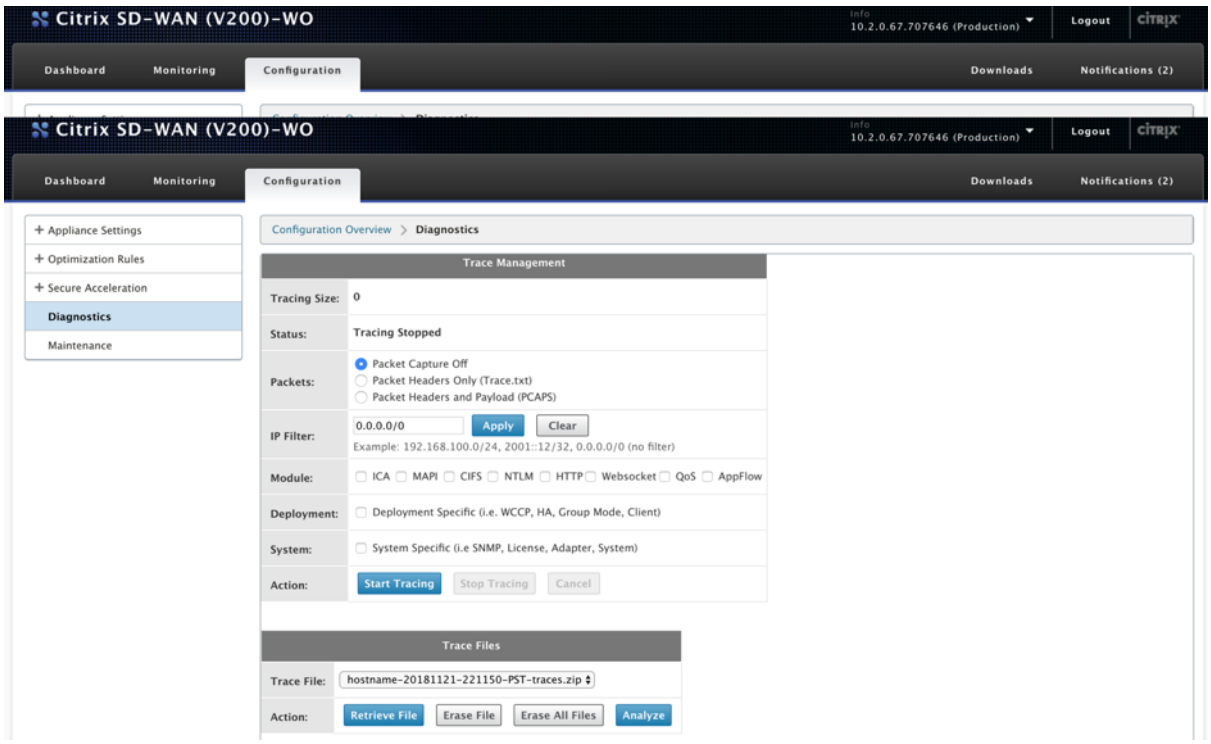
April 23, 2021

Esta sección proporciona herramientas de diagnóstico para identificar problemas de red en su red WANOP SD-WAN y solucionarlos. También puede obtener archivos de registro del sistema, información del sistema y otros detalles necesarios que ayuden al equipo de soporte de Citrix SD-WAN a diagnosticar y resolver problemas de red.

A continuación se muestra la herramienta de diagnóstico disponible en SD-WAN WANOP:

- Rastreo

- Analizador de paquetes
- Prueba de tarjeta de derivación
- Recuperar curso
- Probador de línea
- Ping
- Traceroute
- Información del sistema
- Datos de diagnóstico



Rastreo

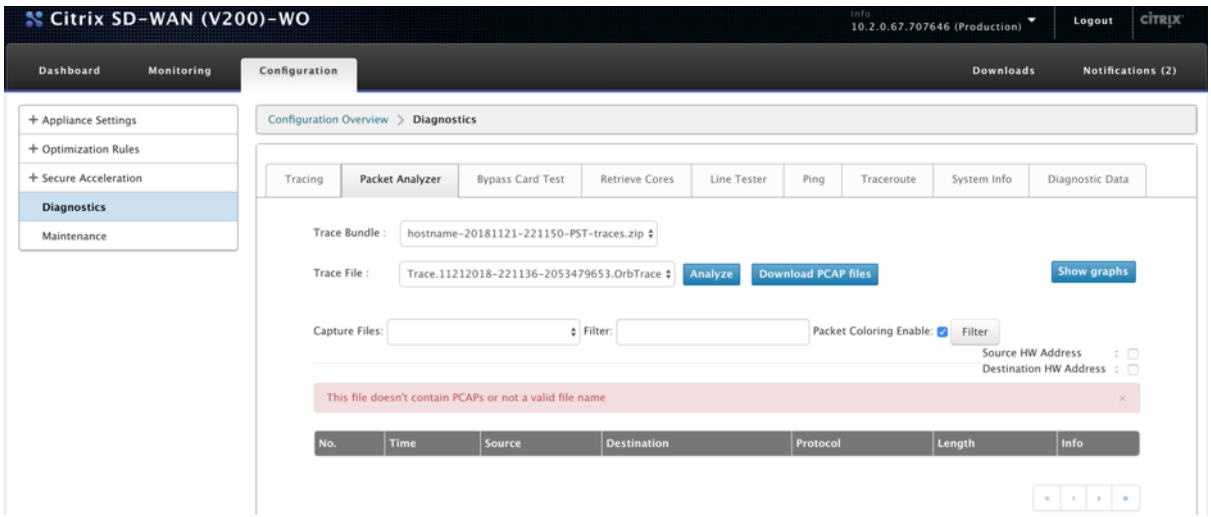
La herramienta de **seguimiento** se utiliza para observar los paquetes que fluyen a través de la red WANOP SD-WAN. Puede abrir cada paquete e identificar el protocolo utilizado, la dirección IP del origen y el destino y otra información de carga útil. El equipo de soporte de Citrix utiliza esta información para encontrar la causa raíz de los problemas de red.

Puede elegir realizar un seguimiento de **Solo encabezados de paquetes** o **Encabezados de paquetes y carga útil**. Puede elegir el módulo que desea realizar el seguimiento y especificar si el seguimiento debe ser específico de la implementación o específico del sistema.

Haga clic en **Iniciar seguimiento**, el dispositivo comienza a rastrear los paquetes. Los resultados se empaquetan
en un archivo ZIP al hacer clic en **Detener seguimiento**. Este archivo se puede descargar en su

computadora, mediante la opción **Recuperar archivo**. A continuación, puede reenviar estos archivos al equipo de soporte. Los archivos de seguimiento también proporcionan datos de análisis de fallos.

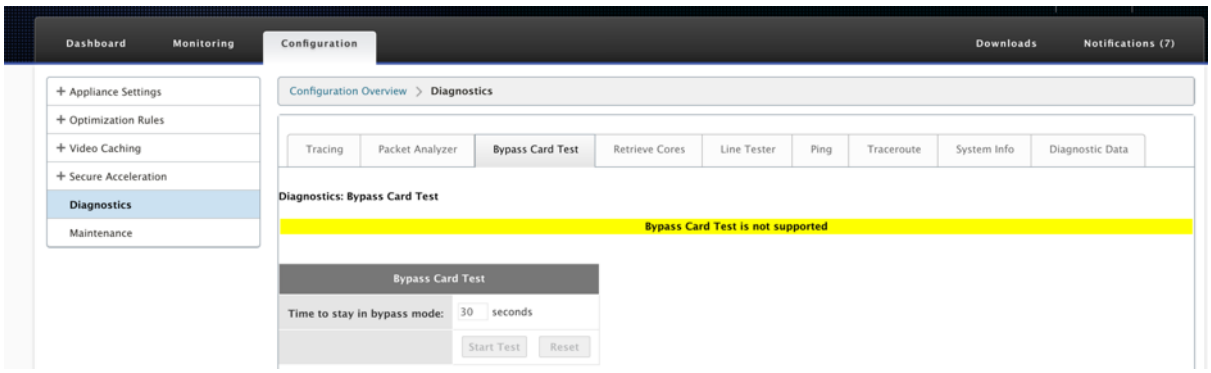
Haga clic en **Analizar** para ver más información sobre los paquetes en la ficha **Analizador de paquetes**.



Puede ver la hora, la dirección de origen, la dirección de destino, el protocolo, la longitud y la información de carga útil.

Prueba de tarjeta de derivación

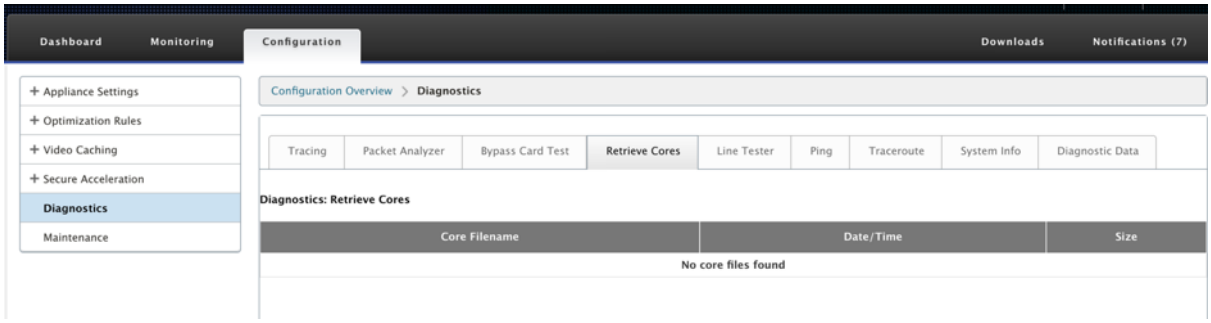
Puede probar la funcionalidad de conmutación por error de cables de la interfaz Ethernet para la implementación de un dispositivo en modo en línea (Fail-to-Wire). Introduzca el número de segundos para que el dispositivo permanezca en modo de omisión y haga clic en **Iniciar prueba**. Durante este período, se omite el dispositivo. La operación normal se reanudará después de eso.



Recuperar núcleos

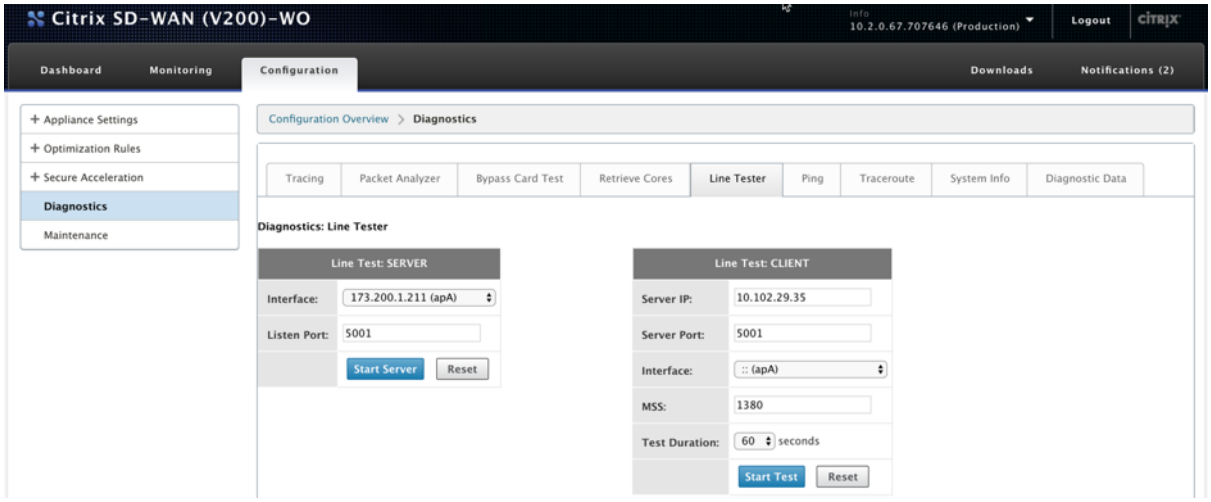
Los archivos**principales** se crean cuando el dispositivo WANOP SD-WAN sale de forma anormal o se bloquea. El dispositivo se reinicia automáticamente después de un bloqueo. En caso de bloqueos persistentes, la aceleración se inhabilita pero la interfaz de administración permanece activa.

Puede seleccionar y recuperar los archivos principales necesarios que se crearon durante el bloqueo del dispositivo o cuando el dispositivo se comportó de forma anormal. Los archivos recuperados se guardan en un archivo ZIP. Puede compartirlo con el equipo de soporte para un análisis más detallado.

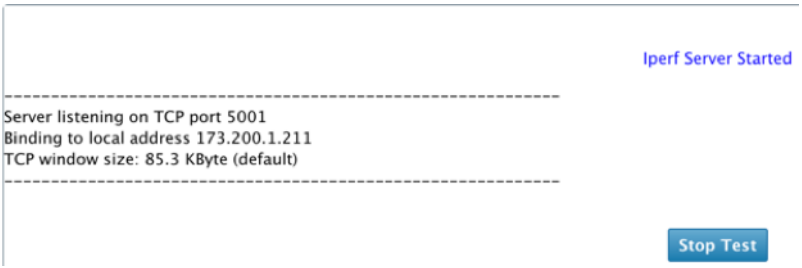


Probador de línea

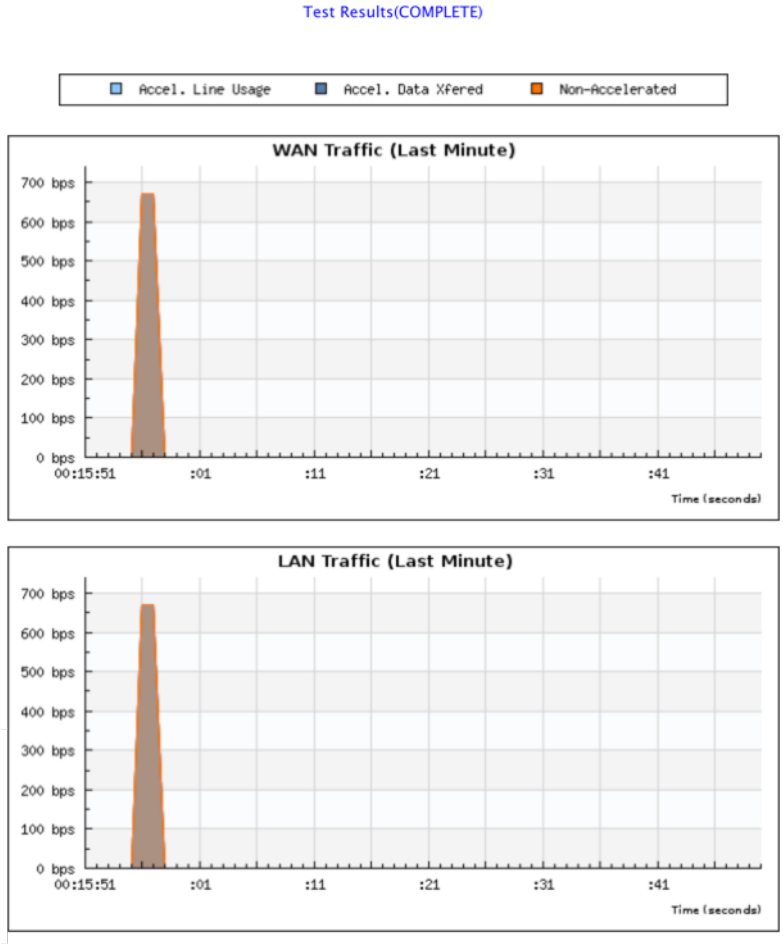
La función **Prueba de línea: SERVER** inicia un servidor iperf en el dispositivo, que se ejecuta en modo TCP. Esta opción se puede utilizar para comprobar la conectividad entre los dispositivos WANOP y solucionar problemas del tráfico de red. Para ejecutar las pruebas iperf, un sistema (un dispositivo u otro host) debe ejecutar iperf como servidor y otro debe conectarse a él como cliente.



Puede utilizar la interfaz y el número de puerto predeterminados **del servidor del probador de línea**. Haga clic en **Iniciar servidor** para iniciar un servidor iperf en el dispositivo.

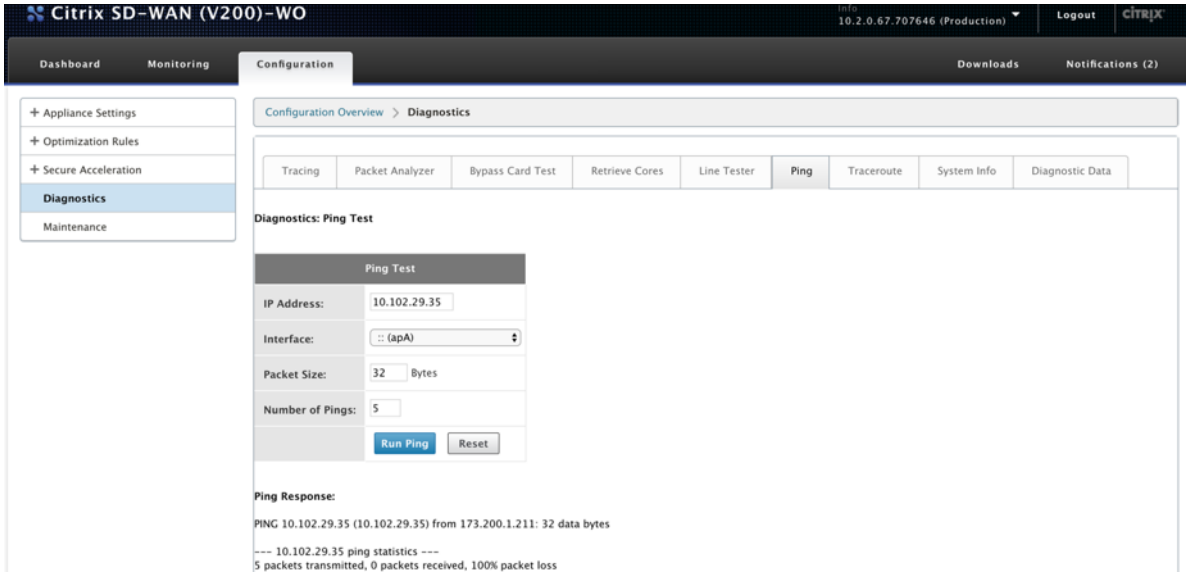


La función **Line Test: CLIENT** inicia un cliente iperf en la unidad, ejecutándose en modo TCP. También puede especificar el número de puerto del servidor iperf y la duración de la prueba. Una vez finalizada la prueba, se informará de la velocidad de conexión. Haga clic en **Iniciar prueba** para ver el resultado del tráfico WAN y LAN.



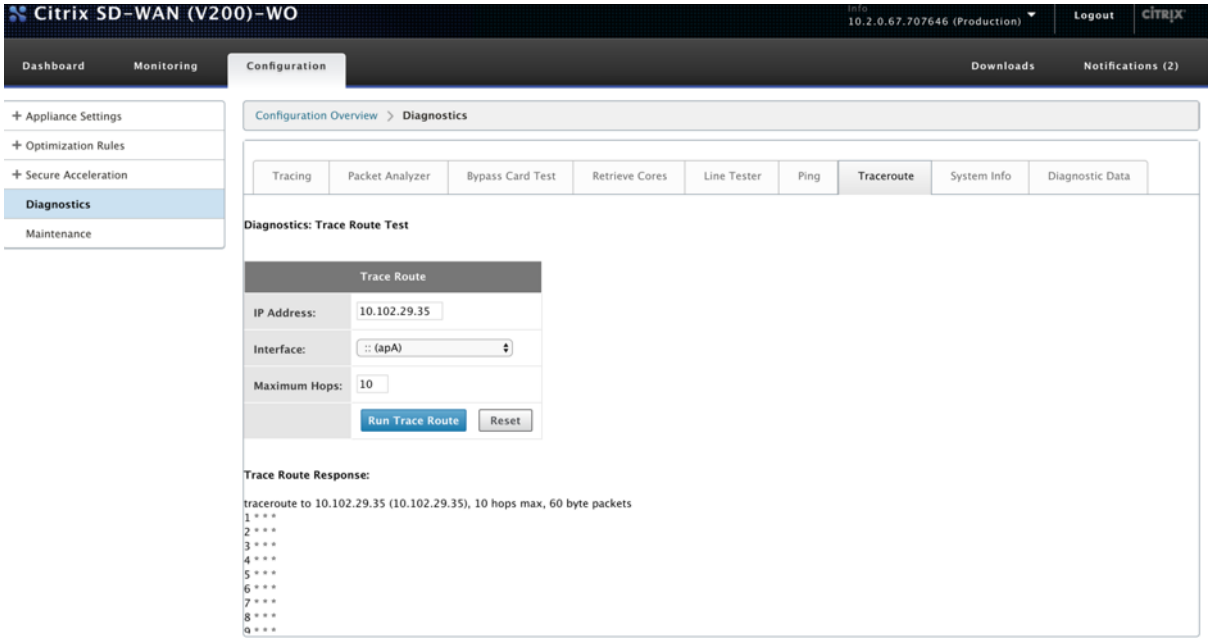
Ping

Ping le permite comprobar la conectividad de los elementos de red en su red SD-WAN. Introduzca la dirección IP del elemento de red y haga clic en **Ejecutar ping** para ver el resultado.



Traceroute

Traceroute permite registrar la ruta entre el dispositivo SD-WAN y cualquier otro elemento de red de la red SD-WAN o en Internet. Calcula y muestra la cantidad de tiempo que tomó cada salto.

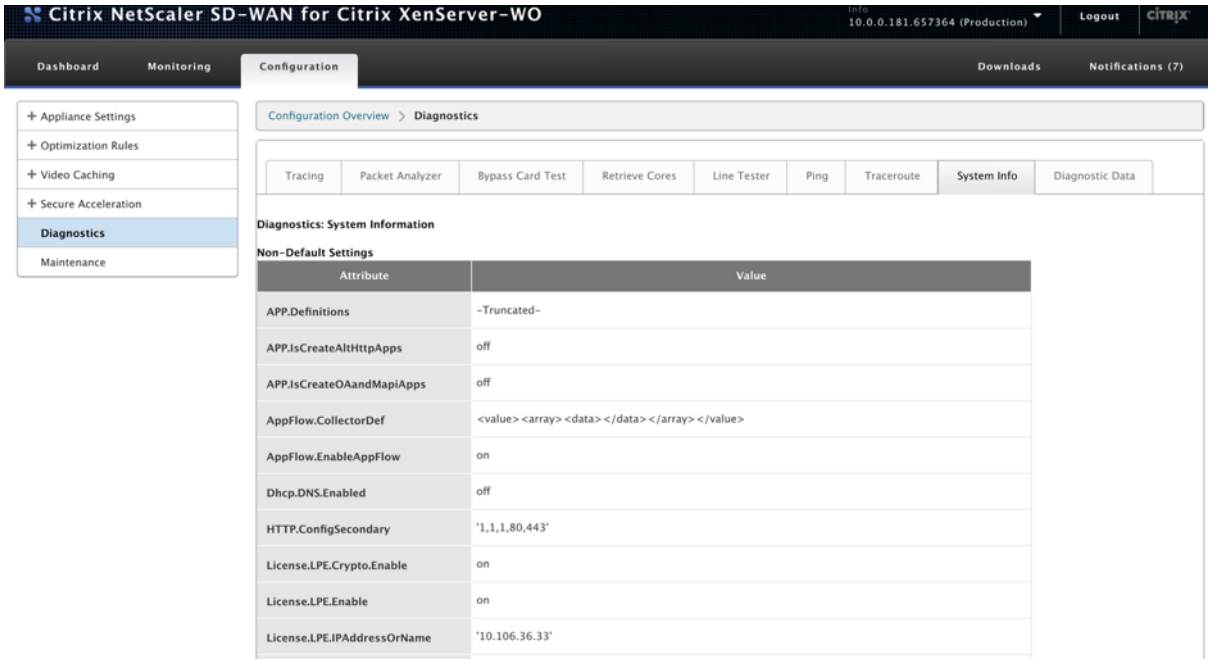


Información del sistema

La **información del sistema** muestra todos los parámetros que no están establecidos en sus valores predeterminados. Esta información es de solo lectura. Es utilizado por el soporte técnico cuando se

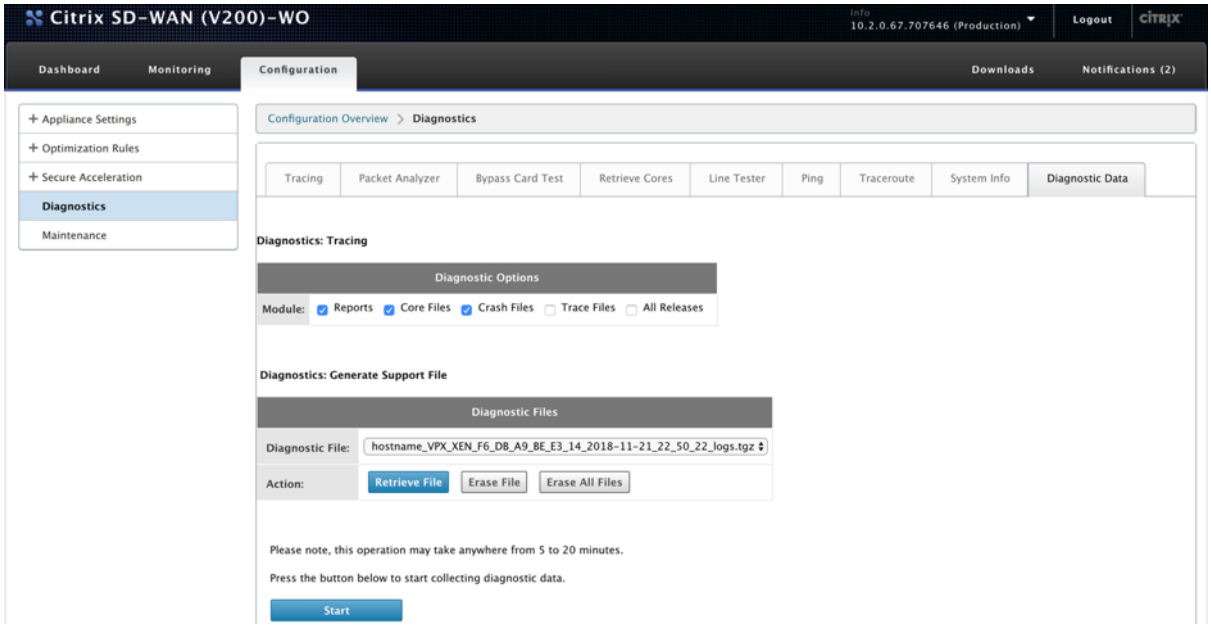
sospecha algún tipo de configuración incorrecta. Cuando informe un problema, es posible que se le pida que compruebe uno o más valores en esta página.

Proporciona **ajustes no predeterminados, información detallada para adaptador principal, información detallada para adaptador apA.2**e **información detallada para adaptador apA.1**.



Datos de diagnóstico

Datos de diagnóstico le permite empaquetar datos de diagnóstico para su análisis por parte del equipo de soporte de Citrix. Seleccione los archivos de diagnóstico necesarios y haga clic en **Inicio**. A continuación, puede hacer clic en **Recuperar archivo** para descargar el archivo zip y compartirlo con el soporte técnico de Citrix.



Solucionar problemas

April 23, 2021

En los temas siguientes se proporciona una lista de problemas, la causa del problema y los pasos de resolución para algunas funciones de Citrix SD-WAN WANOP.

CIFS y MAPI

Plug-in de Citrix SD-WAN WANOP

RPC sobre HTTPS

Almacenamiento en caché de vídeo

Aceleración de Citrix Virtual Apps and Desktops

CIFS y MAPI

April 23, 2021

- **Problema**: se quita un Controller de dominio de la red. Sin embargo, el dispositivo Citrix SD-WAN WANOP no puede abandonar el dominio.

  Causa: se trata de un problema conocido con el dispositivo.

Solución alternativa: desde la página Dominio de Windows, cambie el DNS por el que pueda resolver el dominio deseado. A continuación, utilice la opción
Volver a unirse al dominio para que el dispositivo Citrix SD-WAN WANOP se una a ese dominio. Ahora intenta salir del dominio.

- **Problema**: las conexiones MAPI no están optimizadas y aparece el siguiente mensaje de error:

  configuración no predeterminada en Outlook no es compatible

  Causa: se trata de un problema conocido con la versión 6.2.3 y versiones anteriores.

  Resolución: actualice el dispositivo a la versión más reciente.

- **Problema**: el dispositivo optimizó las conexiones MAPI. Sin embargo, las páginas de supervisión muestran el número de bytes enviados y recibidos como cero.

  Causa: se trata de un problema conocido con el dispositivo.

  Resolución: Este es un problema benigno y no afecta a la funcionalidad del dispositivo. Puedes ignorarlo.

- **Problema**: No se puede establecer un peering seguro entre los dispositivos Citrix SD-WAN WANOP.

  Causa: el emparejamiento seguro con el dispositivo asociado no está configurado correctamente.

  Resolución: Haga lo siguiente:

  1. Compruebe que ha cargado la combinación adecuada de certificados de CA y servidor en el dispositivo.
  2. Vaya a la página**Citrix SD-WAN WANOP**> **Configuración** > Configuración > **Configuración de SSL** > **Socios seguros**.
  3. En la sección **Seguridad de socios**, en **Verificación de certificados**, seleccione **Ninguna: permitir todas las solicitudes** para asegurarse de que el certificado nunca caduca.
  4. Compruebe que el dispositivo puede establecer la interconexión segura con el dispositivo asociado.
  5. Compruebe que la sección **Escuchar en** tiene una entrada para la dirección IP del dispositivo Citrix SD-WAN WANOP deseado.

- **Problema**: Al conectarse a un clúster de Exchange, los usuarios de Outlook con conexiones optimizadas se omitan ocasionalmente o se les pide credenciales de inicio de sesión.

  Causa: la optimización MAPI requiere que cada nodo del clúster de Exchange esté asociado con el nombre principal de servicio (SPN) de ExchangeMDB. Con el tiempo, a medida que necesite más capacidad, agregue nodos adicionales al clúster. Sin embargo, a veces, es posible que la

tarea de configuración no se complete, dejando algunos nodos en el clúster sin la configuración de SPN. Este problema es más frecuente en clústeres de Exchange con Exchange Server 2003 o Exchange Server 2007.

Resolución: realice lo siguiente en cada servidor Exchange en la configuración:

1. Acceder al Controller de dominio.
2. Abra el símbolo del sistema.
3. Ejecute los comandos siguientes:

```
pre codeblock setspn -A exchangeMDB/Exchange1 Exchange1
setspn -A exchangeMDB/Exchange1.example.com Exchange1 <!--
NeedCopy-->
```

- **Problema**: Al intentar conectarse a Outlook, se muestra el mensaje Intentando conectar y, a continuación, se termina la conexión.

  Causa: el dispositivo Citrix SD-WAN WANOP del lado cliente tiene entradas de lista de bloqueados que no existen en el dispositivo del lado servidor.

  Resolución: elimine las entradas de la lista de bloqueados de ambos dispositivos o actualice (recomendado) el software de los dispositivos a la versión 6.2.5 o posterior.

- **Problema**: el dispositivo no puede unirse al dominio incluso después de pasar las comprobaciones previas al dominio.

  Causa: Se trata de un problema conocido.

  Resolución: Haga lo siguiente:

  1. Acceda al dispositivo mediante una utilidad SSH.
  2. Inicie sesión en el dispositivo mediante las credenciales raíz.
  3. Ejecute el comando siguiente:

     /opt/comparecido/bin/domainjoin-cli join <Domain_Name> administrador

- **Problema**: El mensaje de error LDAperError aparece cuando agrega un usuario delegado al dispositivo Citrix SD-WAN WANOP.

  Resolución: realice una de las siguientes acciones:

  - En el servidor DNS del dispositivo Citrix SD-WAN WANOP, compruebe que esté configurada una zona de búsqueda inversa para cada dirección IP del controlador de dominio.
  - Compruebe que el reloj del sistema del equipo cliente está sincronizado con el reloj del sistema del servidor de Active Directory. Cuando se utiliza Kerberos, estos relojes deben sincronizarse.

  - Actualice el usuario delegado en la página Dominio de Windows proporcionando una vez más la contraseña para el usuario delegado.

- **Problema**: aparece el mensaje de error de sesgo de tiempo cuando agrega un usuario delegado al dispositivo Citrix SD-WAN WANOP.

  Resolución: compruebe que el dispositivo está unido al dominio. Si no es así, une el dispositivo al dominio. Esto sincroniza la hora del dispositivo con la hora del servidor de dominio y resuelve el problema.

- **Problema**: El cliente está temporalmente excluido para la aceleración. Aparece el mensaje de error Último error (error Kerberos.) cuando agrega un usuario delegado al dispositivo Citrix SD-WAN WANOP.

  Causa: el usuario delegado está configurado para la autenticación **Usar solo Kerberos**.

  Resolución: compruebe que, en el Controller de dominio, la configuración de autenticación del usuario delegado es **Usar cualquier protocolo de autenticación**.

- **Problema**: aparece el mensaje de error Delegate user not ready cuando agrega un usuario delegado al dispositivo Citrix SD-WAN WANOP.

  Resolución: si el mensaje solo aparece en el dispositivo del cliente, omítelo. Sin embargo, si el mensaje se muestra en el dispositivo del lado del servidor, ejecute la herramienta de comprobación previa del usuario delegado, disponible en la página **Dominio de Windows** y, a continuación, configure el usuario delegado en el dispositivo del lado del servidor.

- **Problema**: Último error (el servidor no está delegado para la autenticación Kerberos. Agregue el usuario delegado, la lista de comprobación de servicios y el servidor permitido para la delegación.) Aparece un mensaje de error UR:4 cuando agrega un usuario delegado al dispositivo de Citrix SD-WAN WANOP.

  Resolución: Compruebe que el usuario delegado está configurado correctamente en el Controller de dominio y que ha agregado los servicios adecuados al Controller de dominio.

- **Problema**: el dispositivo no puede unirse al dominio.

  Resolución: Ejecute la herramienta de comprobación previa del dominio, disponible en la página Dominio de Windows, y resuelva los problemas, si los hay. Si la herramienta de comprobación previa del dominio no informa de ningún problema, póngase en contacto con el Soporte técnico de Citrix para obtener más ayuda para resolver el problema.

Plug-in de Citrix SD-WAN WANOP

April 23, 2021

- **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 Citrix del dispositivo WANOP.
  2. Acceda a la página **Gestión del tráfico** > **Equilibrio de carga** > **Servidores virtuales** > BR_LB_VIP_SIG.

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.

RPC sobre HTTPS

April 23, 2021

- **Problema**: Después de actualizar el software del dispositivo a la versión 7.3, los informes de supervisión no tienen una categoría especial para las conexiones RPC a través de HTTPS.

  Causa: cuando actualiza el dispositivo a la versión 7.3, las aplicaciones RPC sobre HTTPS no pertenecen a su propia clase de servicio. Como resultado, todas las conexiones RPC a través de HTTPS aparecen como conexiones TCP Otras en los informes.

  Resolución: Para categorizar estas conexiones como RPC sobre conexiones HTTPS, cree una clase de servicio para las aplicaciones.

- **Problema**: Después de crear una clase de servicio para RPC sobre HTTPS, todo el tráfico HTTP y HTTPS se clasifica como RPC sobre HTTP.

  Causa: no ha agregado la dirección IP de destino a la clase de servicio que ha creado para RPC a través de aplicaciones HTTPS.

  Resolución: modifique la clase de servicio que ha creado para RPC a través de aplicaciones HTTPS, agregando las direcciones IP de destino de sus servidores.

Almacenamiento en caché de vídeo

April 23, 2021

- **Problema**: Después de agregar una entrada a la lista de tareas de prerrellenado, la entrada sigue en el estado Configurado.

  Causa: una tarea de prerrellenado tarda aproximadamente un minuto en pasar al estado Descargando.

  Resolución: Compruebe el estado de la entrada después de un minuto o actualice la página para comprobar que el estado cambia a Descarga.

- **Problema**: Después de agregar una entrada a la lista de tareas de prerrellenado, el estado de la entrada muestra ERROR 403. Sin embargo, el sitio web funciona bien en un explorador web.

  Causa: la dirección IP de Citrix SD-WAN WANOP AP no tiene acceso al servidor de vídeo.

  Solución: Para resolver este problema, compruebe y actualice lo siguiente:

  - Reglas de acceso a través de los firewalls
  - Limitaciones basadas en la dirección IP de origen en el archivo httpd.conf del servidor de vídeo

  Causa: el servidor de vídeo no es compatible con el método HEAD.

  Resolución: el servidor de vídeo debe permitir la dirección IP WANOP de Citrix SD-WAN para este método.

  Causa: la lista de directorios para carpetas no está habilitada en el servidor de vídeo.

  Resolución: El servidor de vídeo debe habilitar la lista de directorios para las carpetas.

- **Problema**: Después de crear entradas para tareas de prerrellenado, no puede modificar ni suprimir entradas.

  Causa: es posible que haya hecho clic en **Iniciar ahora** para la entrada.

  Resolución: Esto es por diseño. No puede modificar ni eliminar una entrada después de haber hecho clic en **Iniciar ahora** para la entrada y la entrada está en el estado de cola, de inicio o de descarga. Puede eliminar la entrada solo después de completar la descarga.

- **Problema**: Después de crear entradas para tareas de prepoblación, el vídeo no se descarga ni se almacena en caché. El estado de la entrada muestra Error al descargar.

  Causa: la entrada de prerrellenado no tiene URL absoluta para el vídeo.

  Resolución: Para resolver este problema, siga el procedimiento siguiente:

  1. Compruebe que la entrada de prerrellenado tenga la dirección URL real del vídeo, por ejemplo `http://10.102.29.16/Citrix SD-WAN WANOP\\_demo.mp4`, y no un archivo HTML. El dispositivo Citrix SD-WAN WANOP no puede buscar en el contenido del archivo HTML para encontrar el vínculo de vídeo.

2. Compruebe que el protocolo HTTP se utiliza para publicar el vídeo. Puede comprobarlo mediante la opción Ver origen del explorador web.
3. Puede obtener la URL absoluta del vídeo mediante la opción Herramientas para desarrolladores del explorador web.

Aceleración de Citrix Virtual Apps and Desktops

April 23, 2021

- **Problema**: Después de actualizar un dispositivo a la versión 7.3.1, las conexiones ICA no se clasifican como conexiones Citrix Receiver para HTML5 en las páginas de supervisión de ICA.

  Causa: la clase de servicio definida en el dispositivo es **HTTP (privado)** en lugar de web (privado). Cuando actualiza un dispositivo a la versión 7.3.1, la aplicación **ALTHTTP** no se agrega a esta clase de servicio. Como resultado, aunque las conexiones ICA a través de Citrix Receiver para HTML5 están optimizadas, éstas no se clasifican como conexiones de Citrix Receiver para HTML5 en las páginas de supervisión de ICA.

  Resolución: Para categorizar las conexiones ICA a través de Citrix Receiver para HTML5, complete el siguiente procedimiento:

  1. Acceda a la página **Configuración** > **Reglas de Optimización** > **Clases de Servicio**.
  2. Modifique la clase de servicio **HTTP (privado)**.
  3. Haga clic en **Agregar regla**.
  4. En Reglas de filtro, en Aplicaciones, haga clic en **Cualquiera**.
  5. En la lista Aplicaciones, seleccione **ALTHTTP**.
  6. Haga clic en **Agregar**.
  7. Haga clic en **Guardar**.
  8. Realice otros cambios en la regla de filtro, según sea necesario.
  9. Haga clic en **Guardar**.