

**FORTINET®**

# **QUÉ SE DEBE TENER EN CUENTA AL EVALUAR LAS OPCIONES DE SD-WAN**

# CONTENIDO

## INTRODUCCIÓN

1

## SECCIÓN 1: PROBLEMAS CON SOLUCIONES WAN TRADICIONALES

2

- TCO ELEVADO
- ADOPCIÓN Y VISIBILIDAD DE LA NUBE
- SEGURIDAD EN EL CENTRO DE DATOS
- RESILIENCIA/CONTINUIDAD DEL NEGOCIO

## SECCIÓN 2: SEIS ASPECTOS QUE SE DEBEN TENER EN CUENTA AL EVALUAR

### SUS OPCIONES DE SD-WAN

4

- ADOPCIÓN DE APLICACIONES DE LA NUBE
- RECONOCIMIENTO DE APLICACIONES
- INTELIGENCIA DE RECONOCIMIENTO DE RUTAS
- SEGURIDAD Y CUMPLIMIENTO
- COMPATIBILIDAD DE ANCHO DE BANDA MÚLTIPLE
- TCO

## RESUMEN

11

# INTRODUCCIÓN

En la actualidad, las empresas se enfrentan a desafíos relacionados con el precio, el rendimiento y la flexibilidad de las redes de área extensa (WAN) tradicionales. El crecimiento agresivo en la adopción de servicios de nube pública (crecimiento del 28,6 % año tras año en 2017)<sup>1</sup> está forzando a las organizaciones a buscar una solución de red más eficaz en otro lugar para abordar el tráfico distribuido entre sitios remotos y subsidiarias.

Entre los problemas específicos a los que se enfrentan las organizaciones con sus WAN tradicionales se incluyen los siguientes:

- Coste total de la propiedad (TCO) elevado
- Largos ciclos de aprovisionamiento

- Degradación del rendimiento con el crecimiento del tráfico de red
- Redundancia y resiliencia inadecuadas
- Falta de conectividad para aplicaciones

Para gestionar mejor las inversiones WAN, las empresas están adoptando un nuevo enfoque para sus redes de subsidiarias distribuidas. La **WAN definida por software (SD-WAN)** ofrece mejora del rendimiento, agilidad y flexibilidad operativa, así como importantes ahorros en el coste. Sin embargo, no todas las soluciones SD-WAN están creadas de la misma manera.

<sup>1</sup> "Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017", IDC, 6 de noviembre de 2017.

# 01 PROBLEMAS CON SOLUCIONES WAN TRADICIONALES

El rendimiento WAN tradicional es costoso porque está casi limitado a caros circuitos como la conmutación de etiquetas multiprotocolo (MPLS). Al mismo tiempo, el aumento rápido de las aplicaciones de nube que se están usando en aplicaciones distribuidas ha originado un agudo repunte en las demandas de ancho de banda de red. A medida que aumentan estas necesidades de rendimiento, las infraestructuras WAN tradicionales se vuelven considerablemente más caras, complejas de implementar y difíciles de gestionar. Como prueba de este problema, **según una encuesta llevada a cabo en la conferencia del centro de datos de 2016 de Gartner, “una proporción de 6:1 de encuestados describió su WAN como «frágil y lenta, propensa a interrupciones o demasiado cara», frente a la calificación de «rentable y ágil»”.**<sup>2</sup>

<sup>2</sup> Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzo de 2017.

## TCO elevado

- Las soluciones WAN tradicionales tienen un **ancho de banda caro**. Mantienen conectividad entre sitios y calidad de servicio al depender de costosos circuitos MPLS. MPLS también requiere tiempos prolongados de implementación, lo que inhibe el crecimiento de la empresa y la productividad general.
- También se produce una **mayor complejidad**. Las funciones de red y seguridad dispares implican que hay más partes de las que se debe realizar un seguimiento. La gestión mediante una interfaz de la línea de comandos (CLI) agrava este problema. CLI requiere mucho tiempo de dedicación al seguimiento de la gestión de registros, aumenta la oportunidad de error humano y disminuye la productividad general del personal.

## Adopción y visibilidad de la nube

- Las WAN tradicionales cuentan con **visibilidad de nube inferior** porque solo pueden ofrecer una vista de nivel de enrutamiento y de paquete, en lugar de la visibilidad sobre las aplicaciones.
- Además, las WAN tradicionales pueden crear **cuellos de botella de rendimiento** que afectan a la productividad y al rendimiento de los usuarios en todo el negocio, y esto ocurre especialmente con el aumento de las demandas basadas en la nube. Dado que el tráfico se enruta a través del centro de datos, viaja más allá y aumenta la latencia. Asimismo, **el tráfico WAN tradicional no es inteligente** y no se puede asignar por política al canal del ancho de banda adecuado.

## Seguridad en el centro de datos

- Las conexiones MPLS privadas que utilizan la mayoría de las WAN tradicionales permiten la seguridad centralizada. El tráfico se dirige al centro de datos (un proceso conocido como retorno) en una típica infraestructura de red radial donde todo lo que pasa por la red se puede comprobar y filtrar. Aunque el tráfico es seguro, cuenta con un **problema de rendimiento**.
- Por diseño, las WAN tradicionales no disponen de **acceso directo a Internet** mediante vínculos públicos, lo que a su vez limita el rendimiento disponible para el uso en continua expansión



de los servicios de nube como las aplicaciones Software como servicio (SaaS).

- Algunas organizaciones deciden comprar sus soluciones de seguridad y red de manera independiente, lo que origina **dispositivos almacenados en silos con consolas de gestión independientes** que **limitan la visibilidad transparente**. Esto hace que las operaciones sean más complejas y que tarden más tiempo.

## Resiliencia/continuidad del negocio

- Las opciones de conmutación por error de conectividad WAN para MPLS (redes 4G/3G) **no son fiables** y las organizaciones carecen de la **resiliencia** que su negocio requiere. Esto, a su vez, puede interrumpir operaciones de negocio periódicas con tiempo de inactividad e incurrir en pérdida de productividad.

# 02 SEIS ASPECTOS QUE SE DEBEN TENER EN CUENTA AL EVALUAR SUS OPCIONES DE SD-WAN

Con todos los problemas anteriores asociados a WAN tradicionales, las empresas necesitan una infraestructura de reemplazo con simplificación importante, una mejora de la ventaja del coste y un mejor soporte para la adopción de la nube.

A diferencia de las arquitecturas WAN tradicionales, las **redes de área extensa definidas por software (SD-WAN)** pueden distribuir el tráfico de manera dinámica en varias ubicaciones a la vez que responden automáticamente al cambio de las políticas de aplicaciones para lograr un mejor rendimiento. Esto, a su vez, permite una mejor agilidad y rentabilidad frente a las soluciones de redes tradicionales.

**Gartner prevé que el “25 % de las empresas adoptarán SD-WAN en los dos próximos años”.**<sup>3</sup>

Sin embargo, existen demasiadas diferencias entre los diferentes productos de proveedor que se encuentran en el mercado, desde la funcionalidad hasta la implementación, la gestión, la visibilidad que proporcionan y la relación precio/rendimiento y el coste.

Las siguientes son las seis ventajas clave que las personas que toman decisiones deben buscar a la hora de pensar en las alternativas de SD-WAN para sus organizaciones.

<sup>3</sup> Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzo de 2017.



## 1. ADOPCIÓN DE APLICACIONES DE NUBE

Según IDC, la adopción de servicios de nube pública está creciendo a un ritmo del 28,6 % año tras año.<sup>4</sup> Este crecimiento da lugar a una proliferación de nubes en toda la empresa. En la actualidad, la empresa media ya usa en torno a 30 aplicaciones SaaS diferentes en toda su organización.<sup>5</sup>

Para complicar aún más las cosas, un porcentaje cada vez mayor de las personas que compran y gestionan aplicaciones SaaS no son responsables de TI. En 2017, los compradores de línea de negocio gastarán más en aplicaciones de software (150.700 millones de \$) que los compradores de TI (64.700 millones de \$).<sup>6</sup>

Teniendo en cuenta la previsión de que el número de aplicaciones de nube activa continuará en aumento, SD-WAN puede ayudar a las empresas a adoptar más aplicaciones SaaS sin crear un cuello de botella en el rendimiento de la red o sin afectar a la productividad de los usuarios finales. De manera específica, SD-WAN elimina el retorno del tráfico de la aplicación de nube a través del centro de datos al permitir el acceso directo a Internet a las redes remotas. De esta manera se reduce drásticamente la latencia y la pérdida de paquetes.

<sup>4</sup> "Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017", IDC, 6 de noviembre de 2017.

<sup>5</sup> Nirav Shah and Bill McGee, "[Empowering Distributed Enterprises with Secured SD-WAN](#)", Fortinet, acceso del 16 de diciembre de 2017.

<sup>6</sup> "[Technology Purchases from Line of Business Budgets Forecast to Grow Faster Than Purchases Funded by the IT Organization](#)", IDC, 23 de marzo de 2017.



Varios sectores se pueden beneficiar de la SD-WAN, aunque los posibles resultados son mayores para algunos sectores determinados, como los siguientes:

- **Atención sanitaria.** Las organizaciones sanitarias suelen disponer de numerosos sitios remotos que constan de usuarios que necesitan acceso a servicios SaaS que se usan para registros médicos electrónicos (EMR), atención al paciente, contabilidad y finanzas, entre otras funciones. Debido a que cada uno de estos servicios requiere un importante ancho de banda, las WAN tradicionales simplemente no pueden mantener el ritmo de las necesidades de rendimiento basadas en la nube cada vez mayores en una infraestructura sanitaria ampliada. Una solución SD-WAN segura proporciona ancho de banda flexible y asequible para abordar mejor las crecientes necesidades de aplicaciones de nube de los profesionales sanitarios a la vez que sirve mejor a los resultados de los pacientes y a mantener la seguridad de la información médica privada.

- **Comercio minorista.** Combinando los establecimientos tradicionales y las ventas basadas en Internet, las cadenas minoristas actuales dependen cada vez más de un conjunto convergido de herramientas de comercio electrónico basadas en la nube para coordinar todos los aspectos de su negocio, desde la gestión del inventario hasta el procesamiento de pagos y el análisis de datos de clientes. Con tiendas remotas que pueden llegar a ser cientos e incluso miles, las organizaciones minoristas pueden depender de SD-WAN para lograr un mejor rendimiento de aplicaciones de red de gran volumen en geografías ampliamente distribuidas, incluso en horas de venta punta.
- **Fabricación.** Al igual que el comercio minorista, las organizaciones industriales y de fabricación modernas se aprovechan de aplicaciones SaaS coordinadas para ejecutar mejores y diferentes funciones de trabajo entre territorios diversos e incluso fronteras internacionales. Las rigurosas condiciones y la naturaleza crítica de alguna de estas operaciones implican que las aplicaciones en red no se pueden restringir por límites de rendimiento sin graves consecuencias. Una solución SD-WAN segura ofrece un ancho de banda ágil y asequible para admitir funciones como la gestión automática de la cadena de suministro, las ventas internacionales y los controles industriales que mantienen tanto la seguridad de los trabajadores como una productividad óptima.

## 2. RECONOCIMIENTO DE APLICACIONES

La naturaleza estática de una infraestructura WAN tradicional puede perjudicar seriamente el rendimiento de las aplicaciones en una operación distribuida. Su solución SD-WAN puede admitir la necesidad cada vez más urgente de una **visibilidad completa de las aplicaciones** para ayudar a los administradores a supervisar y gestionar patrones de tráfico, equilibrar necesidades de ancho de banda y ampliar el rendimiento en toda la empresa distribuida. En este escenario, la SD-WAN mantiene la información actual de todas las aplicaciones y optimiza su función al enrutar de manera inteligente y priorizar aplicaciones en función de su ancho de banda y de qué usuarios necesitan acceso a cada una ellas. La información de cada aplicación incluye su estado y requisitos de recursos.

## 3. INTELIGENCIA DE RECONOCIMIENTO DE RUTAS

La inteligencia de reconocimiento de rutas implica que su solución debe **priorizar automáticamente el enrutamiento de aplicaciones** en todo el ancho de banda en función del usuario y aplicación específicos. Ofreciendo un SLA de nivel por aplicación, la inteligencia de reconocimiento de rutas selecciona dinámicamente la mejor conexión o vínculo WAN para la situación. Esto permite a las organizaciones priorizar



las aplicaciones en función de su criticidad, hora del día y otras funciones.

A diferencia del servicio WAN basado en MPLS (con conectividad cara y limitada), las SD-WAN proporcionan un reemplazo ligero de los routers WAN tradicionales y son independientes del transporte WAN (MPLS, Internet, LTE, etc.). Las soluciones SD-WAN permiten el uso compartido de la carga inteligente del tráfico entre varias conexiones de ancho de banda para lograr una mayor eficiencia de red y un funcionamiento dinámico en una empresa distribuida. La inteligencia de reconocimiento de rutas ayuda a aumentar los beneficios de la ventaja de la conectividad de SD-WAN.



#### 4. CUMPLIMIENTO Y SEGURIDAD INTEGRADOS

Sin la protección centralizada proporcionada por el retorno del tráfico a través del centro de datos, el paso de MPLS a las conexiones de ancho de banda de Internet directas requiere seguridad adicional dentro de la infraestructura empresarial, especialmente considerando que los ciberataques continúan creciendo en volumen y sofisticación.

Se ha demostrado que las capacidades de seguridad y red distribuidas en las WAN son ineficaces e ineficientes. En la actualidad, de acuerdo con Gartner, “Los productos WAN definidos por software (SD-WAN) incorporan ahora seguridad de perímetro de Internet, pero más del 90 % de los proveedores SD-WAN

no son proveedores de seguridad tradicionales, lo que hace que los clientes se pregunten si pueden depender solo de la seguridad integrada”.<sup>7</sup> Esto ofrece el potencial de costes de configuración más elevados y de un aumento del TCO, por no mencionar un riesgo superior de las posibles brechas entre las dispares tecnologías para red y seguridad. Y, conforme el tráfico empresarial cifrado con SSL aumente por encima del 50 % en los próximos años, el tráfico cifrado se deberá comprobar minuciosamente para ver el malware oculto sin crear un cuello de botella del rendimiento de la red.<sup>8</sup>

<sup>7</sup> Gartner, Four Architectures to Secure SD-WAN, Bjarne Munch, Greg Young, octubre de 2017.

<sup>8</sup> Nirav Shah and Bill McGee, “[Empowering Distributed Enterprises with Secured SD-WAN](#)”, Fortinet, acceso del 16 de diciembre de 2017.



La **seguridad del firewall de próxima generación (NGFW)** es un requisito clave para permitir el acceso de Internet directo en una arquitectura de SD-WAN. La protección de NGFW resulta fundamental para reducir la exposición a los riesgos en una red extensa. Entre sus funciones de seguridad preparadas para SD-WAN se deben incluir las siguientes:

- **Una solución única** que combina funciones tanto de red como de seguridad en un dispositivo puede fortalecer la protección en todo el entorno distribuido a la vez que simplifica los controles y reduce los costes de inversión.
- **Inspección SSL** para proteger su red distribuida frente al malware y otras amenazas ocultas en

el tráfico web cifrado. La inspección SSL puede desbloquear sesiones, mirar en paquetes cifrados, encontrar amenazas y bloquearlas.

- **Filtrado web** para ofrecer una primera línea de defensa frente a los ataques basados en web. Protege a las organizaciones bloqueando el acceso a sitios web malintencionados, pirateados o inadecuados.
- La **VPN de IPsec de alto rendimiento** resulta fundamental para implementaciones de SD-WAN seguras. La seguridad de protocolo de Internet (IPsec) permite la comunicación de dos o más hosts de una manera segura al autenticar y cifrar cada paquete IP de una sesión de comunicación de red privada virtual (VPN).
- Las **funciones de informes y de seguimiento de cumplimiento** ayudan a garantizar la adherencia a la normativa y los estándares del sector a la vez que reducen los riesgos colaterales de multas y costes legales en el caso de una fuga. Su NGFW debe incluir funciones de informes que realicen un seguimiento de la actividad de amenazas en tiempo real para facilitar la evaluación de riesgos, así como para detectar y mitigar posibles problemas. También debe supervisar políticas y reglas de firewall, además de automatizar auditorías de cumplimiento.

## 5. COMPATIBILIDAD DE ANCHO DE BANDA MÚLTIPLE

Como se ha mencionado anteriormente en referencia a la inteligencia de reconocimiento de rutas, su controlador SD-WAN debe poder mezclar y emparejar varias conexiones de ancho de banda (Internet, MPLS, LTE, etc.) para admitir el uso directo de conexiones de Internet públicas. Dado que SD-WAN es independiente del transporte y del operador, su conectividad ya no depende tan solo de las conmutaciones de red MPLS y 4G/3G no confiables, que pueden poner a las operaciones empresariales en riesgo de tiempo de inactividad. Al aprovechar la Internet pública como opción de conmutación por error, SD-WAN ofrece una **resiliencia y redundancia superiores** para evitar las interrupciones y la degradación del rendimiento.

## 6. TCO

El paso al ancho de banda público significa que las conexiones MPLS caras se pueden reemplazar con opciones más rentables, como el Internet público o la evolución a largo plazo (LTE). Esto puede proporcionar ahorros en el coste operativo medibles frente a la WAN tradicional.

Además, con las funciones de control de seguridad y red integradas en **un solo panel**, SD-WAN reduce la complejidad y simplifica la gestión. El personal de



seguridad puede pasar menos tiempo gestionando los diversos aspectos de las operaciones de seguridad y red, así como correlacionando eventos.

Su solución SD-WAN también debe admitir **implementación sin intervención** para lograr una mayor eficiencia al conectar nuevas subsidiarias. Estas funciones ayudan a las empresas a crecer a través del aprovisionamiento rápido, la configuración agilizada y la autenticación automática, así como el soporte y la supervisión automática. La implementación sin intervención ahorra mucho tiempo en comparación con los procesos más implicados de añadir subsidiarias en un entorno WAN tradicional.

# RESUMEN

La WAN tradicional ya no es una solución eficaz para la empresa distribuida actual. Las organizaciones están superando los importantes problemas de seguridad y red pasando a SD-WAN. Gartner indica que “para el 2018, más del 40 % de las iniciativas de actualización de la infraestructura de borde WAN se basarán en aplicaciones vCPE o SD-WAN frente a routers tradicionales”.<sup>9</sup>

<sup>9</sup> Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzo de 2017.

En la actualidad hay muchas SD-WAN diferentes en el mercado y los VP de TI deben revisar con cuidado cada una de ellas. Aquí es donde la publicación “Seis aspectos que se deben tener en cuenta” puede resultar de ayuda. En ese respecto, Fortinet Secure SD-WAN integra las características de SD-WAN mejoradas en capacidades de seguridad probadas, proporcionando capacidades de redes y protección de última generación que mejoran la eficiencia de la red sin poner en peligro la seguridad.



**FORTINET**®

[www.fortinet.com](http://www.fortinet.com)

Copyright © 2018 Fortinet, Inc. Todos los derechos reservados. 02.02.18

154319-A-0-EN