

**VISIÓN DE FORTINET**

# Es hora de dejar atrás los routers en las delegaciones

## 4 grandes ventajas de Secure SD-WAN.



Cada vez más organizaciones se están alejando de los routers en las delegaciones y están optando por Secure SD-WAN para estar preparadas para la nube y mejorar la experiencia del usuario. Las soluciones Secure SD-WAN no sólo son seguras sino que también simplifican las operaciones de la WAN en general.

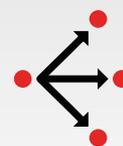
Las organizaciones deberían adoptar soluciones de Secure SD-WAN para ayudar a los usuarios de las sedes remotas a aprovechar mejor la colaboración y las comunicaciones unificadas, a utilizar aplicaciones SaaS críticas y a acceder fácilmente a los recursos almacenados en la nube. Secure SD-WAN ofrece cuatro ventajas clave frente a los tradicionales routers en las delegaciones:

### 1. Mayor agilidad de las aplicaciones

Los routers operan en base a paquetes. Como resultado, no pueden proporcionar una visibilidad profunda de las aplicaciones. Dado que la mayoría de las organizaciones tienen una inversión en aplicaciones y servicios en la nube, el hecho de no poder identificar esas aplicaciones críticas para el negocio y aplicar protocolos para respaldar sus necesidades únicas de ancho de banda y conectividad puede degradar la experiencia del usuario.

Las soluciones SD-WAN pueden hacer lo mismo que un router tradicional, como proporcionar conectividad WAN y enrutamiento avanzado. Sin embargo, más allá de las funciones de enrutamiento tradicionales, las soluciones SD-WAN:

- Identifican y orientan las aplicaciones con la selección de rutas dinámicas para lograr una calidad constante de la experiencia.
- Pueden identificar aplicaciones y crear SLA para miles de aplicaciones como O365, Salesforce.com y comunicaciones unificadas.
- Tienen la capacidad de actualizar las aplicaciones comerciales a diario para garantizar que las aplicaciones se identifiquen con precisión y toman el camino más deseado.



Las soluciones Secure SD-WAN son fáciles de gestionar y simplifican las operaciones de la WAN en general.

## 2. Facilidad de ampliación, con un ahorro considerable de gastos operativos y de capital

Los volúmenes y velocidades de conexión MPLS están predeterminados y son costosos, lo que significa que un repentino pico en el tráfico —como las múltiples conexiones de comunicaciones unificadas de alta velocidad o la necesidad de procesar una gran cantidad de datos— puede afectar a todos. La adición de nuevos sitios de router de sedes remotas también es un proceso costoso y que requiere mucho tiempo.

Sin embargo, las soluciones SD-WAN pueden ayudar a los clientes a migrar de MPLS a la banda ancha (DSL, 4G/5G, Ethernet) y a obtener un 40 % de ahorro en gastos operativos en muchos casos. SD-WAN permite a las organizaciones escalar de forma dinámica y segura a decenas de miles de sedes remotas, interoperar sin problemas con las infraestructuras físicas y de nube existentes, y proporcionar solución de problemas a distancia para eliminar las costosas intervenciones físicas llevadas a cabo por técnicos cualificados. Secure SD-WAN también consolida una gama de productos especializados —entre los que se incluyen routers, cortafuegos y herramientas de optimización de la WAN— en un solo producto, lo que favorece un considerable ahorro de gastos de capital.

## 3. Gestión y orquestación simplificadas

Los routers de sedes remotas suelen ser complejos de instalar, actualizar y mantener, incluso cuando se supone que son una solución de esfuerzo mínimo. La configuración requiere experiencia con la interfaz de la línea de comandos (CLI) de un router y, debido a su complejidad, rara vez puede realizarse por cualquier persona que se encuentre en las instalaciones de una sede remota.

La gestión de Secure SD-WAN centralizada garantiza que los nuevos servicios y políticas se centren en las aplicaciones y que las configuraciones de conectividad y seguridad, así como los cambios de políticas, se puedan propagar sin problemas por toda la WAN ampliada, eliminando la necesidad de configurar o gestionar cada dispositivo o servicio de forma individual. Secure SD-WAN centralizada también proporciona análisis detallados que muestran el rendimiento histórico y en tiempo real de las aplicaciones, lo que permite a los equipos solucionar problemas rápidamente y mejorar los indicadores de rendimiento clave, como el promedio de tiempo para responder.

## 4. Seguridad y redes integradas

Los routers de las sedes remotas no son de ningún modo soluciones de redes y seguridad totalmente integradas. Cuando el MPLS se complementa con canalización por túnel para permitir el acceso directo a Internet, los routers de sedes remotas proporcionan poca o ninguna gestión de vínculos o conexiones. Incluso cuando el tráfico conmuta por error o se desplaza a una ruta alternativa, carecen de la dirección proactiva de subsegundos necesaria para evitar la caída de conexiones y no tienen la capacidad de mitigar problemas de transporte o de proporcionar cuestiones como el búfer dinámico de fluctuaciones. Tampoco pueden regular de manera activa el tráfico antes de que la congestión se convierta en un problema. Peor aún, debido a que los routers carecen de una seguridad efectiva, estas conexiones que no son MPLS exponen a su organización a un riesgo adicional.

Sin embargo, es importante señalar que la mayoría de las soluciones SD-WAN no están exentas de desafíos de seguridad; de hecho, uno de los requisitos críticos para el éxito de SD-WAN es la seguridad totalmente integrada. Los firewalls de última generación (NGFW), cuyos componentes clave incluyen IPS, filtrado web, inspección SSL y antimalware, son un ejemplo de solución integrada. Sin una seguridad totalmente integrada, SD-WAN se convierte en otro conducto para que el malware y los ciberdelincuentes ataquen la red.

Una verdadera plataforma necesita herramientas explícitamente diseñadas para interoperar como un solo sistema, idóneamente con cada elemento que se ejecuta en el mismo sistema operativo y gestionado mediante una interfaz de un solo panel de cristal. De esta manera se garantiza que todas las transacciones sean vistas e inspeccionadas, y que cualquier amenaza o comportamiento anómalo sea compartido entre cada solución para una máxima protección. Como parte de un sistema integrado de este tipo, las funcionalidades de redes y conectividad de una SD-WAN no solo están más estrechamente asociadas con las soluciones de seguridad instaladas en la plataforma, sino que son lo mismo.

## Consideraciones de siguiente etapa

Es fundamental no solo reconocer la necesidad de abandonar una estrategia tradicional de WAN basada en routers, sino también seleccionar cuidadosamente una solución Secure SD-WAN diseñada para proporcionar el espectro completo de funcionalidad y el mayor número posible de casos de uso. Esto ayuda a garantizar que su nueva implementación de SD-WAN no solo satisfaga las necesidades actuales de su organización, sino que también pueda adaptarse a sus requisitos de rápida evolución.



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