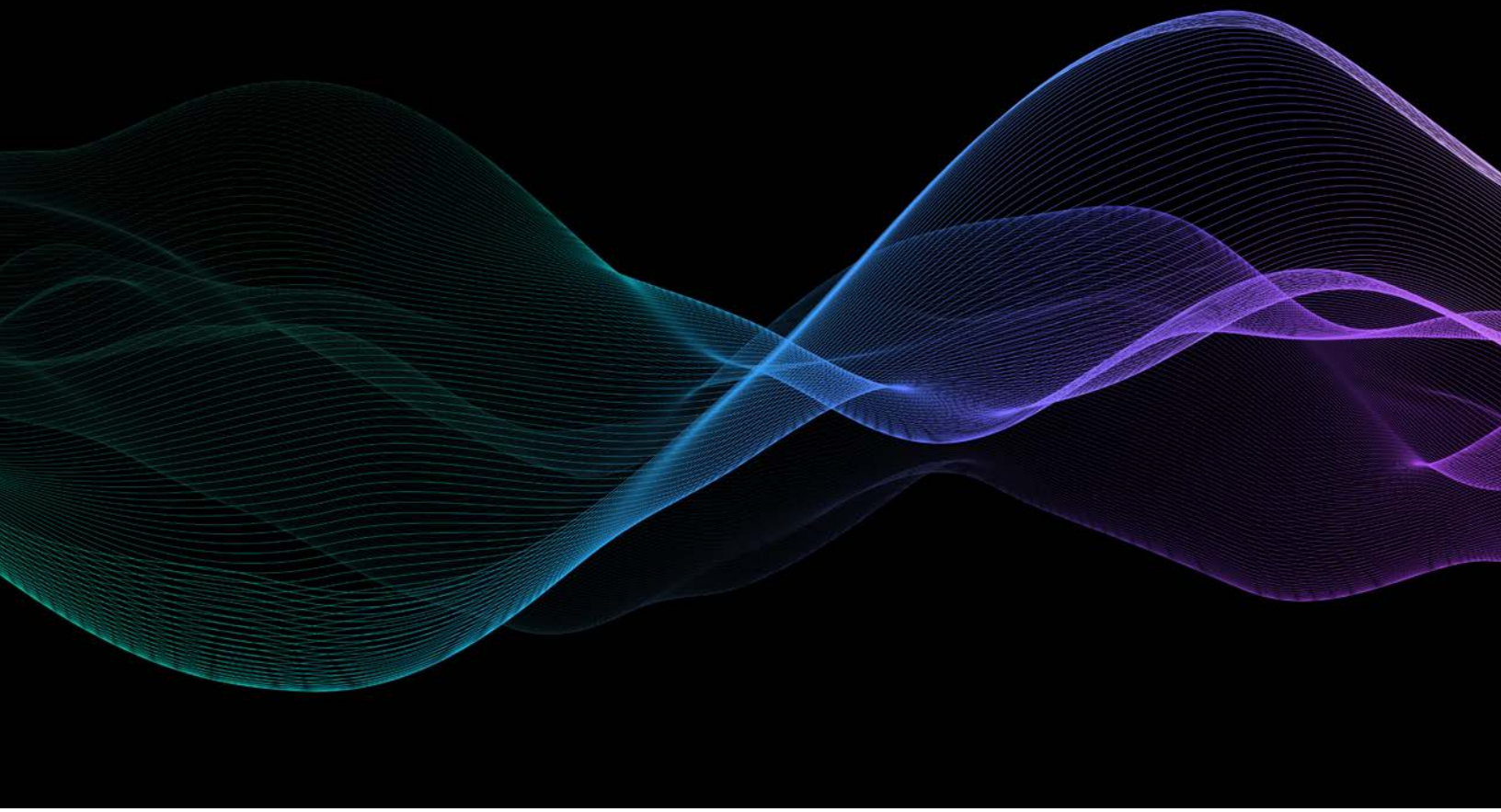
Guía del comprador del SD-WAN



Forcepoint

Guía del comprador

forcepoint.com/es



Qué buscar cuando elige una solución de SD-WAN

La arquitectura tradicional de las Software-Defined Wide Area Network(WAN) utiliza un modelo de "hub-and-spoke" (centro y distribución) en el que el tráfico se dirige a través costosas Multiprotocol Label Switching (MPLS) a un data center central, con fines de seguridad. Esta tecnología se enfrenta a problemas de escalabilidad con costos operativos y de rendimiento, y el rápido cambio de muchas empresas tanto hacia un modelo de fuerza laboral híbrido y como hacia aplicaciones basadas en la nube hace que sea difícil encontrar el equilibrio adecuado entre seguridad y eficiencia.

Una solución de Software-Defined Wide Area Network (SD-WAN) resuelve estos desafíos mediante el uso de la tecnología de Software-Defined Networking (SDN), para crear una superposición que virtualiza y abstrae las conexiones de red, en lugar de emplear hardware, como enrutadores y conmutadores. Esto permite el uso agnóstico de diferentes tipos de conexión, incluidos los servicios de MPLS, LTE e Internet de banda ancha, en combinación, para conectar de manera flexible a los usuarios remotos con aplicaciones y recursos de TI. El enrutamiento efectivo del tráfico puede optimizar la velocidad y el ancho de banda, lo que lleva a un mejor rendimiento y menores costos operativos en comparación con la arquitectura WAN tradicional.

SD-WAN juega un papel crucial en la ciberseguridad al permitir que las funciones de seguridad se distribuyan a endpoints remotos y de sucursales, en lugar de requerir que el tráfico se envíe en retroceso a un data center central para su inspección. Los proveedores ofrecen una variedad de soluciones, incluidos los servicios de SD-WAN y los servicios administrados, además de los dispositivos físicos y virtuales y las licencias de software.

Al seleccionar una solución de SD-WAN, los evaluadores deben tener en cuenta estas cinco consideraciones clave:

1. Rendimiento
2. Costos operativos
3. Protección contra amenazas
4. Escalabilidad

Rendimiento

Una solución de SD-WAN debe poder dirigir automáticamente el tráfico de red para garantizar que las aplicaciones de misión crítica reciban los recursos necesarios para un rendimiento óptimo. El enrutamiento avanzado del tráfico, el monitoreo dinámico de enlaces y la identificación detallada de aplicaciones son funcionalidades que pueden ayudar a diferenciar las soluciones líderes. El enrutamiento en función de las aplicaciones ocurre cuando una solución de SD-WAN reconoce los requisitos de ancho de banda de diferentes aplicaciones y garantiza que las aplicaciones de misión crítica reciban el ancho de banda necesario para operar sin latencia o pérdida de paquetes.

Las soluciones de SD-WAN utilizan el monitoreo continuo y el autoaprendizaje para responder automáticamente en tiempo real a cualquier cambio en el estado de la red, enrutando el tráfico alrededor de cuellos de botella o servicios de transporte que están experimentando problemas. El monitoreo del estado de las aplicaciones es el proceso de aplicar este enfoque a las aplicaciones que se ejecutan en la red, y cualquier buena solución de SD-WAN debe recopilar datos sobre el rendimiento de las aplicaciones para anticipar las necesidades cambiantes y los posibles problemas.

La conectividad de rutas múltiples mejora el rendimiento y reduce los costos al equilibrar de manera inteligente el tráfico entre la banda ancha de ISP y las líneas privadas de MPLS. Este abordaje ofrece el máximo rendimiento para reducir el tiempo de inactividad y eliminar cualquier barrera a la productividad de los empleados. Las



Figura 1: Monitoreo del estado de las aplicaciones

capacidades mencionadas anteriormente ofrecen maneras de profundizar en las afirmaciones sobre el rendimiento mejorado para calificar cómo funciona una solución de SD-WAN para ofrecer conexiones más rápidas con menos latencia o tiempo de inactividad.

Forcepoint Secure SD-WAN optimiza el rendimiento de las aplicaciones mediante el aprovechamiento de las capacidades de dirección dinámica de aplicaciones, como la identificación detallada de aplicaciones y el monitoreo preciso de enlaces. La dirección dinámica de aplicaciones enruta el tráfico en función del rendimiento de la red y los requisitos de las aplicaciones, lo que garantiza que las aplicaciones de misión crítica siempre reciban los recursos necesarios para un rendimiento óptimo. La capacidad de conmutación por error automática garantiza que las aplicaciones permanezcan disponibles y con buen rendimiento, incluso en caso de problemas de red.

Forcepoint Secure SD-WAN aprovecha la tecnología Forcepoint Multi-Link™ para mejorar la resiliencia de la red y el rendimiento de las aplicaciones. Al combinar dinámicamente múltiples conexiones, como MPLS, LTE y banda ancha, Forcepoint Secure SD-WAN ofrece una conectividad perfecta en toda la red, lo que garantiza que las aplicaciones críticas reciban la mejor conectividad posible.

Forcepoint Secure SD-WAN también incorpora el dashboard de Monitoreo del estado de las aplicaciones, que permite a los administradores monitorear las métricas de calidad (tráfico, latencia, jitter y pérdida de paquetes) para aplicaciones de red, enlaces de ISP y túneles de VPN, todo en una sola vista. Monitoreo del estado de las aplicaciones también proporciona un historial de estado para detectar cualquier malfuncionamiento. Contar con el historial del estado de salud de los enlaces de ISP en la misma pantalla que el estado de salud de las aplicaciones de red permite a los administradores identificar si hay conexiones causales entre la calidad del enlace y las aplicaciones, o si hay problemas más aislados con respecto a una aplicación en particular o la conectividad de una sucursal.

Preguntas para hacer cuando evalúe soluciones

- → ¿Qué funcionalidad integrada proporciona esta solución para priorizar las aplicaciones críticas para la empresa?
- → ¿Qué capacidades, como el monitoreo del estado de las aplicaciones y la dirección del tráfico, ofrece esta solución para evitar cuellos de botella y maximizar el rendimiento?
- → ¿Esta solución proporciona conectividad Multi-Link?
- → ¿Cuánto tiempo de inactividad se puede esperar típicamente con una solución como esta?

Costos operativos

Además de mejorar el rendimiento, una buena solución de SD-WAN debe contribuir a mantener los costos operativos de tu organización bajos. Como se discutió anteriormente, el primer paso es el uso agnóstico de diferentes tipos de conexión con conectividad Multi-Link, lo que evita tener que depender exclusivamente de conexiones MPLS de mayor costo.

Dentro de SD-WAN, el clúster de alta disponibilidad es una capacidad crítica para mitigar el tiempo de inactividad de la red y los costos asociados. El agrupamiento de alta disponibilidad minimiza las interrupciones de red al redirigir rápidamente el tráfico durante los fallos de enlace, lo que garantiza una conectividad ininterrumpida. El tiempo de inactividad en cualquier empresa implica pérdida de ingresos, productividad y satisfacción del cliente.

Las soluciones de SD-WAN pueden reducir en gran medida el tiempo y la mano de obra al aprovechar la configuración en la nube para un despliegue sin intervención en cualquier ubicación. Esto aplica a la implementación inicial de una nueva infraestructura de red, pero también tiene el efecto continuo de simplificar las actualizaciones de políticas y software. Los despliegues sin intervención no solo son más rápidos, sino que liberan al personal para que se concentre en problemas y objetivos más críticos para la misión. Estos efectos se traducen en menores costos operativos en todos los ámbitos, y una solución adecuada debe proporcionar múltiples vías para mantener los gastos bajo control.

Forcepoint Secure SD-WAN proporciona la flexibilidad para desplegar en la nube (con integraciones con AWS, Microsoft y más). Con el despliegue y la administración sin intervención de los dispositivos de red, las organizaciones pueden reducir los gastos de capital (CapEx) y los gastos operativos (OpEx), al tiempo que se permiten escalar su infraestructura de red de manera rápida y rentable.

La capacidad de agrupación de alta disponibilidad dentro de Forcepoint Secure SD-WAN garantiza la continuidad empresarial mediante la eliminación los puntos únicos de falla. En el caso de alguna falla, el dispositivo de respaldo tomará el control sin interrupciones, lo que reducirá el tiempo de inactividad y mantendrá una conectividad perfecta. La función de agrupación en clústeres permite a los administradores administrar múltiples dispositivos desde una única interfaz, lo que simplifica la administración de la red y reduce los costos operativos.

Multi-Link™ en Forcepoint Secure SD-WAN no solo optimiza el rendimiento de las aplicaciones, sino que también ayuda a las organizaciones a ahorrar en costos de red. Con la capacidad de enrutar dinámicamente el tráfico por la ruta más eficiente y rentable, las organizaciones pueden evitar costosos enlaces y reducir los gastos de red.

Preguntas para hacer cuando evalúe soluciones

- ¿Esta solución utiliza el agrupamiento de alta disponibilidad para reducir el tiempo de inactividad y optimizar la conectividad?
- ¿Esta solución permite capacidades de despliegue sin intervención para ahorrar tiempo e incorporar ubicaciones remotas fácilmente?

Protección contra amenazas

No todas las soluciones de SD-WAN proporcionan características de seguridad integradas. Si bien la mayoría incluyen el cifrado para proteger la privacidad de datos, esta opción de conectividad puede convertirse en un vector de ataque adicional cuando no se integra adecuadamente con otras funcionalidades de seguridad. Las tecnologías superiores de SD-WAN también proporcionan capacidades de seguridad adicionales.

A medida que los usuarios remotos se conectan directamente a aplicaciones en la nube, la seguridad que solía ser proporcionada por gateways on-premises ahora debe implementarse en cada ubicación remota o en la nube. Las soluciones de Secure SD-WAN lo hacen posible a través de la incorporación de funciones clave de seguridad:

- → La tecnología de control de acceso y prevención de intrusiones evita que los atacantes penetren las defensas. Por lo general, lo hacen a través de Next-Generation Firewalls (NGFW).
- → Las características de seguridad web ofrecen protección en tiempo real contra amenazas avanzadas dentro de las páginas web o el contenido descargado.
- → Las soluciones de monitoreo en la nube rastrean y protegen las aplicaciones y los datos almacenados en la nube, para evitar abusos.

Con soluciones superiores de SD-WAN, las empresas pueden permitir a los usuarios conectarse fácilmente a los recursos en la nube que necesitan, a la vez que protegen las redes, los usuarios y los datos contra robos, pérdidas y ataques.

Las últimas generaciones de soluciones de Secure SD-WAN se construyen con la idea de priorizar la seguridad y capacidades clave, como Quality of Service (QoS) y Network Encryption & Decryption.

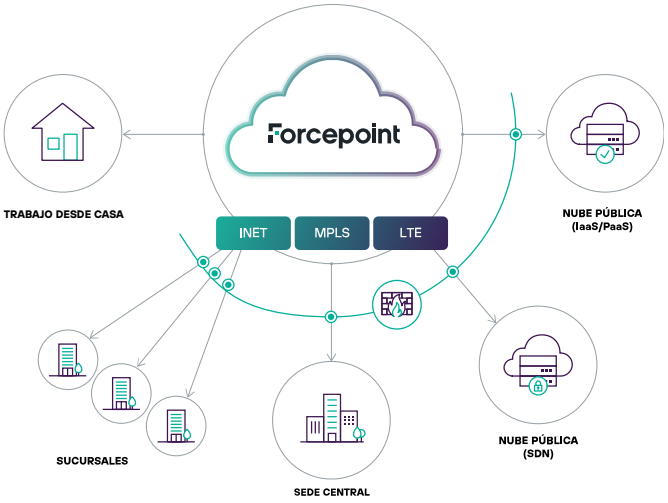


Figura 2: Arquitectura de Forcepoint Secure SD-WAN

Forcepoint Secure SD-WAN proporciona detección y protección en tiempo real contra una variedad de amenazas, que incluyen malware, tráfico de botnets y ataques de comando y control (C2), junto con otros tipos de explotaciones. Con una inspección detallada de paquetes y capacidades avanzadas de detección de amenazas, los administradores obtienen una visión integral de la actividad de la red y pueden responder rápidamente para mitigar las amenazas. Los paquetes sospechosos son identificados y bloqueados, las sesiones de TCP son terminadas y el contenido malicioso es eliminado de la red. Todas estas acciones se pueden tomar en tiempo real y de acuerdo con los requisitos de su política de seguridad, lo que garantiza que sus datos y aplicaciones más críticos estén protegidos contra daños.

La inspección de multicapa es una función esencial de Forcepoint Secure SD-WAN que proporciona un enfoque flexible e integral a la seguridad. Al combinar el control de acceso, la identificación de aplicaciones, la inspección profunda y el filtrado de archivos, las organizaciones pueden optimizar la seguridad y el rendimiento del sistema.

Preguntas para hacer cuando evalúe soluciones

- › ¿Qué funciones de seguridad integrada ofrece esta solución?
- › ¿Cómo se integra la solución con soluciones de seguridad externas para proteger los datos transmitidos a aplicaciones basadas en la nube?

Escalabilidad

Las capacidades de despliegue sin intervención mencionadas anteriormente ayudan a que una solución de SD-WAN sea escalable mediante el aprovisionamiento de servicio remoto a nuevas ubicaciones de todo el mundo. La administración centralizada es otro factor crucial que hace posible escalar rápidamente, ya que los administradores de red pueden establecer políticas de mayor nivel una vez y aplicarlas automáticamente en toda la organización. Idealmente, esta administración centralizada debe poder operar en la nube para proporcionar la velocidad y la flexibilidad necesarias para la resolución efectiva de problemas.

Uno de los desafíos que enfrentan las organizaciones cuando escalan es administrar múltiples regiones con diferentes proveedores de ISP. Tales escenarios pueden requerir demasiado tiempo en la configuración manual de nuevas conexiones y hardware costoso; estas consideraciones pueden hacer que las organizaciones incurran en costos más altos de los anticipados al escalar las operaciones. Una solución de SD-WAN que pueda hacer este proceso más eficiente y menos costoso, por ejemplo, mediante la creación de numerosas puertas de enlace sin la necesidad de conectividad directa, puede aumentar en gran medida la escalabilidad para las organizaciones.

Con Forcepoint SD-WAN, los administradores pueden supervisar y mantener miles de sitios desde el Centro de Gestión de Seguridad para administrar y monitorear toda la red en tiempo real. Además, el orquestador de Forcepoint SD-WAN simplifica la configuración de nuevas ubicaciones de SD-WAN. Simplemente añade una nueva ubicación al orquestador de SD-WAN y automáticamente se comunicará con los sitios nuevos y existentes.

El orquestador de Forcepoint SD-WAN también administra la conectividad de malla completa entre miles de puertas de enlace, lo que permite a las organizaciones escalar operaciones a múltiples ubicaciones.

Preguntas para hacer cuando evalúe soluciones

- ¿Cómo facilita esta solución la visualización y administración centralizadas de los flujos de tráfico de red?
- ¿Esta solución proporciona asistencia con la administración de múltiples regiones a la vez que minimiza los requisitos de configuración manual y aprovecha el hardware asequible?



Figura 3: Enlaces de banda ancha de productos básicos seguros de SD-WAN

Consideraciones clave para seleccionar una solución de SD-WAN

Las soluciones de SD-WAN que son capaces de abordar las necesidades de redes y seguridad de las empresas modernas proporcionan lo siguiente:

- → Rendimiento | Dirige automáticamente el tráfico de red y emplea el monitoreo continuo y el autoaprendizaje para evitar cuellos de botella y reducir la latencia y el tiempo de inactividad.
- → Costos operativos | Reduce los gastos de tiempo, mano de obra e infraestructura con medidas como el despliegue sin intervención directa, el uso agnóstico de diferentes tipos de conexión y el agrupamiento de alta disponibilidad.
- → Protección contra amenazas | Incluye características de seguridad integradas, como el cifrado, la prevención de intrusiones y la inspección de múltiples capas.
- → Escalabilidad | Facilita la administración centralizada, así como la configuración y el despliegue eficientes para nuevas ubicaciones en todo el mundo.

Forcepoint Secure SD-WAN maximiza el rendimiento y la escalabilidad, reduce los costos operativos y admite las mejores prácticas de seguridad de datos.

Si quieres ver a Forcepoint Secure SD-WAN en acción o si deseas conocer nuestras ofertas de SASE, regístrese para obtener una demo gratuita.

Forcepoint

forcepoint.com/contact

Acerca de Forcepoint

Forcepoint simplifica la seguridad para empresas y gobiernos de todo el mundo. La plataforma todo en uno y realmente nativa en la nube, de Forcepoint, facilita la adopción de un enfoque de Zero Trust y evita el robo o la pérdida de datos confidenciales y propiedad intelectual sin importar desde donde trabajen las personas. Forcepoint, con sede en Austin, Texas, crea entornos seguros y confiables para los clientes y sus empleados en más de 150 países. Interactúe con Forcepoint en www.forcepoint.com, Twitter y LinkedIn.

© 2025 Forcepoint. Forcepoint y el logotipo de FORCEPOINT son marcas comerciales de Forcepoint. Todas las demás marcas comerciales utilizadas en este documento son propiedad de sus respectivos dueños. [FP-Brochure-Software-Defined Wide Area Network Buyer's Guide-ES] 06May2025