Presentado por

Servicios de acceso seguro en el borde (SASE)

para dummies

Edición especial de Cisco

Explore las redes SASE

Amplíe la seguridad nativa de la nube en todos lados

Reduzca los costes y la complejidad

Lawrence Miller, CISSP

Información acerca de Cisco

Cisco diseña y vende amplias líneas de productos, proporciona servicios y ofrece soluciones integradas para desarrollar y conectar redes de todo el mundo, creando Internet.

Como líderes del mercado global en nuestro sector, ayudamos a nuestros empleados a conectarse, digitalizar y avanzar. Juntos, cambiamos la forma en que el mundo trabaja, vive, juega y aprende.

Durante más de 30 años, hemos ayudado a nuestros clientes a diseñar redes, automatizar, orquestar, integrar y digitalizar productos y servicios basados en la tecnología de la información (TI).

En un mundo cada vez más conectado, Cisco ayuda a marcar el camino a la hora de transformar negocios, gobiernos y ciudades de todo el mundo con una innovación diferenciada.

Introducción a los servicios de acceso seguro en el borde (SASE)

umbrella.cisco.com/sase

Con todas las soluciones de seguridad distintas (y sus acrónimos) que hay (DNS, SIG, SWG, CASB, FWaaS, SASE), puede resultar complicado decidir qué enfoque es el mejor, así como qué tecnologías necesita para reducir la complejidad, mejorar la velocidad y la agilidad y, en esencia, proteger su red. Visite nuestra página web para saber más sobre SASE y los pasos que puede empezar a dar para mantener su organización sana y salva.

www.twitter.com/CiscoUmbrella

www.facebook.com/CiscoUmbrella

www.linkedin.com/company/OpenDNS

www.youtube.com/c/CiscoUmbrella

Servicios de acceso seguro en el borde (SASE)

Edición especial de Cisco

por Lawrence Miller, CISSP

para dummies®

Servicios de acceso seguro en el borde (SASE) para dummies®, edición especial de Cisco

Publicado por **John Wiley & Sons, Inc.**
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-73562-5 (libro en rústica); ISBN 978-1-119-73547-2 (libro electrónico)

Fabricado en Estados Unidos de América

10 9 8 7 6 5 4 3 2 1

Agradecimientos del editor

Algunas de las personas que contribuyeron a comercializar este libro son:

Editora del proyecto: Jennifer Bingham

Editora de compras: Ashley Coffey

Director editorial: Rev Mengle

Representante de Desarrollo Empresarial: Karen Hattan

Editor de producción: Umar Saleem

Ayuda especial: Rachel Ackerly, Lorraine Bellon, Robert Clarke, Josh DeButts, Tori Devereux, Meg Diaz, Barry Fisher, Kiran Ghodgaonkar, David Gormley, Rachel Haag, Kate MacLean, Jonny Noble, Iloyd Noronha, Natalie Pino, Nicole Smith, Christina Soriano, Cynthia Turner-De Vries

Índice

Introducción

Los equipos de TI actuales se enfrentan a un desafío común: cómo hacer realidad de manera segura el universo cada vez mayor de usuarios itinerantes, dispositivos y aplicaciones de software como servicio (SaaS) sin que aumente la complejidad ni se reduzca el rendimiento del usuario final, al tiempo que se aprovechan las inversiones en seguridad existentes. De la misma manera, los usuarios de las oficinas remotas y sucursales necesitan el mismo nivel de rendimiento y seguridad de la red que el resto de los usuarios que se encuentran en las sedes centrales. El departamento de TI debe desarrollar estrategias para proteger a los usuarios (en los lugares en que trabajen y en los dispositivos que utilicen) de una gran variedad de amenazas, incluidas las infecciones de malware, las devoluciones de llamadas de control y mando, los ataques de suplantación de identidad, el acceso no autorizado y el uso indebido, entre otras.

En este libro, se analiza el paisaje cambiante de las redes y la seguridad, las brechas en las acumulaciones de seguridad existentes y los pasos que puede dar para mantener su organización sana y salva a medida que la red evoluciona. Estos cambios están preparando el terreno para una nueva categoría de soluciones que proporciona múltiples funciones de seguridad en la nube que son simples, escalables y flexibles para cumplir con las necesidades únicas de su negocio y su arquitectura de red cambiante.

El objetivo de este libro es ayudarle a entender las últimas tendencias en redes y seguridad, los desafíos más complicados que ofrecen estos cambios y cómo han evolucionado las tecnologías de seguridad y redes con el tiempo. Por último, el libro le presenta una nueva categoría de productos que ha surgido para ayudar a resolver estos problemas y la forma en que el enfoque de Cisco puede ayudar a su negocio hoy y en el futuro.

Acerca de este libro

Este libro consta de cinco capítulos que exploran:

- Tendencias clave sobre seguridad y redes y los retos que conllevan (Capítulo 1)
- Distintas opciones de seguridad y redes y reflexiones clave (Capítulo 2)

- ¿Cómo abordan las arquitecturas SD-WAN los retos de las redes modernas? (Capítulo 3)
- ¿De qué forma un servicio de seguridad multifunción nativa de la nube complementa a SD-WAN y afronta los retos de seguridad actuales? (Capítulo 4)
- Puntos clave de la seguridad en la nube y SD-WAN (Capítulo 5)

Cada uno de los capítulos se puede leer independientemente del resto, por lo que, si hay un tema que le llama la atención, puede pasar directamente a dicho capítulo. Puede leer este libro en el orden que prefiera (aunque no le recomendamos que lo lea del final al principio ni del revés).

Suposiciones ingenuas sobre los lectores

Siempre se ha dicho que la mayoría de las suposiciones sobreviven a los sinsentidos, pero de todos modos le dejamos algunas de estas suposiciones.

Tiene formación técnica y trabaja para una organización que, como muchas otras, busca una forma mejor de gestionar los desafíos de seguridad y redes de una empresa híbrida y con varias nubes. Como tal, este libro está escrito para lectores técnicos con conocimientos generales de los conceptos de seguridad, redes y nube.

Tal vez usted sea un gerente o ejecutivo de TI, como un director de información (CIO), un director de tecnología (CTO) o un director de seguridad de la información (CISO), el vicepresidente de TI, el director de TI o un administrador de redes o seguridad. O tal vez sea un ingeniero o un arquitecto de seguridad, redes o de la nube.

Si cualquiera de estas suposiciones le define, este libro es para usted. Si ninguna de estas suposiciones le describe, siga leyendo. Es un libro maravilloso y cuando acabe de leerlo sabrá bastante sobre seguridad en la nube y SD-WAN.

A lo largo de este libro, encontrará iconos especiales para llamar la atención sobre información importante. Estos son los iconos que encontrará:

RECUERDE

Este icono señala la información importante que debe guardar en su memoria no volátil, su materia gris o su coco, junto a los cumpleaños y aniversarios.

MATERIA TÉCNICA

Si lo que quiere es alcanzar el séptimo nivel del NERDvana, ¡preste atención! Este icono explica la jerga más allá de la jerga y es el material del que están hechos los nerds.

CONSEJO

Los consejos inesperados se agradecen: esperamos que aprecie estas perlas de sabiduría.

ADVERTENCIA

Estas señales son todo aquello sobre lo que le advirtió su madre (bueno, tal vez no), pero ofrecen consejos prácticos para ayudarle a evitar posibles errores frustrantes o costosos.

Más allá del libro

Hay tanta información que no cabe en un resumen de 48 páginas, así que, si termina el libro y piensa "Dios mío, este libro es increíble. Quiero saber más", consulte la página `https://umbrella.cisco.com/sase`.

EN ESTE CAPÍTULO

- Veremos cómo han cambiado la seguridad y las redes
- Abordaremos los retos en seguridad y redes actuales

Capítulo 1
Redes y seguridad: tendencias y retos

La red empresarial ha sufrido una gran transformación durante la última década. Como resultado, los productos de seguridad también evolucionan. El mercado está pasando de productos especializados con un único propósito a soluciones de seguridad multifunción integradas en ofertas de servicios en la nube. El objetivo es sencillo: implementar servicios de seguridad como y donde elija, con la posibilidad de controlar y proteger el acceso directo a Internet, las aplicaciones en la nube y a los usuarios de las sedes centrales, remotos e itinerantes por igual, sin necesidad de hardware adicional.

En este capítulo, se analizan los retos y las tendencias actuales que impulsan la necesidad de un nuevo enfoque para las redes y la seguridad.

Nuestra forma de trabajar ha cambiado

Varias tendencias clave han evolucionado a lo largo de los últimos diez años para reestructurar el panorama de la seguridad y las redes.

Adopción de la nube

El uso de aplicaciones y servicios de la nube pública se ha disparado en la última década. Cada año las empresas generan más datos y estos datos se almacenan cada vez con más frecuencia en aplicaciones de software como servicio (SaaS) en la nube pública. El informe de 2019 del Enterprise Strategy Group, *The Rise of Direct Internet Access* (El auge del acceso directo a Internet), prevé que un 60 % de las organizaciones van a utilizar aplicaciones SaaS para más de la mitad de sus necesidades empresariales durante los próximos dos años, especialmente en organizaciones altamente distribuidas.

CONSEJO

El aumento de la adopción de la nube empresarial se evidenció aún más en el informe *RightScale State of the Cloud Report* de Flexera de 2019, que halló que la adopción de la nube pública, lo que incluye el SaaS y la infraestructura como servicio (IaaS), ha aumentado hasta un 91 % en las organizaciones. En la actualidad, un tercio de las cargas de trabajo de las empresas se ejecutan en nubes públicas y casi la mitad se ejecutan en nubes privadas (véase la figura 1-1).

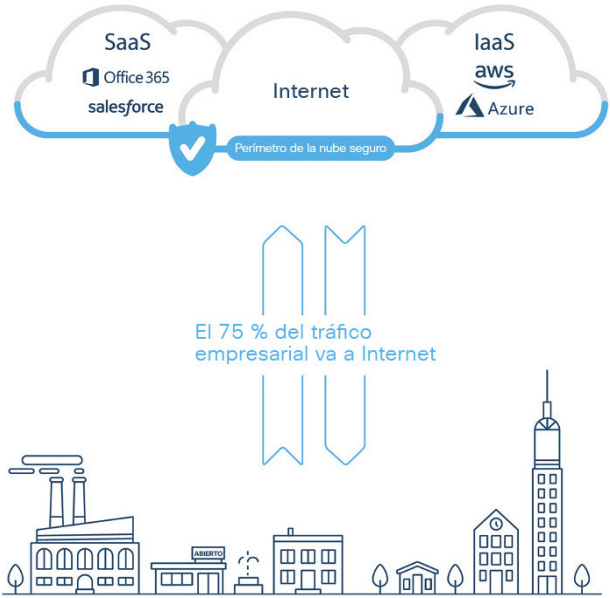


FIGURA 1-1: Es esencial contar con una seguridad sólida que proteja el volumen cada vez mayor del tráfico de IaaS, aplicaciones SaaS e Internet en todas las ubicaciones.

Oficinas remotas

Atrás quedan los días en que los empleados trabajaban juntos en el mismo lugar (la sede de la empresa). A medida que las organizaciones se expanden a nuevos mercados comprando empresas más pequeñas y sus oficinas, el número de sucursales y oficinas remotas también crece. Para la empresa media, las oficinas remotas o satélite generan la mayoría de los ingresos: las investigaciones del Enterprise Strategy Group sugieren que el 80 % de los usuarios se encuentra en oficinas remotas o sucursales. Estos usuarios necesitan protección del mismo modo que los compañeros de las oficinas principales, aunque su tráfico de red vaya directamente a Internet en vez de retornar al centro de datos corporativo.

RECUERDE

Una sucursal u oficina remota es la ubicación de una empresa de negocios (no doméstica) que tiene más de un empleado. Esta ubicación puede estar conectada a un centro de datos central mediante una red de área amplia (WAN) o directamente a Internet. Las oficinas remotas y las sucursales suelen recibir algún nivel de soporte tecnológica por parte de las sedes centrales y la mayoría (aunque no todas) generalmente tienen uno o varios servidores locales para ofrecer a los usuarios servicios de impresión, archivos y otros servicios de TI.

Algunas oficinas remotas pueden estar conectadas a una oficina principal mediante un enlace WAN de conmutación de etiquetas de protocolos múltiples (MPLS). Sin embargo, es cada vez más habitual que las oficinas remotas se conecten a la oficina principal a través de una red privada virtual (VPN) mediante un enlace de acceso directo a Internet (DIA) o que cuenten con un enlace DIA secundario que sirva como copia de seguridad del enlace MPLS principal.

CONSEJO

A medida que las empresas se descentralizan, la creciente población de trabajadores remotos y sucursales necesita un nuevo enfoque en materia de redes y seguridad.

Usuarios itinerantes

Los ordenadores portátiles han sustituido a los ordenadores de escritorio para convertirse en el terminal principal de muchos usuarios empresariales. Del mismo modo, la informática móvil se traduce en trabajadores independientes, ya que los dispositivos móviles son ahora más potentes que muchos ordenadores de escritorio y su uso ha proliferado. Debido a estas tendencias tecnológicas, la mayor parte del trabajo se puede realizar prácticamente desde cualquier sitio y las organizaciones modernas reconocen cada vez más que el trabajo es una actividad, no un lugar.

Según el Enterprise Strategy Group, el 50 % del personal será itinerante en 2021 y, en un artículo de Forbes de febrero de 2019, se señalaba que «el trabajo remoto ya no es un "beneficio", un "estilo de vida" o una "política". El trabajo remoto, el trabajo a distancia y la flexibilidad en el lugar de trabajo se han convertido oficialmente en un sector global».

RECUERDE

Un *usuario itinerante* es cualquier empleado que trabaja desde una oficina en casa o desde otra ubicación no corporativa (como en la oficina de un cliente o en carretera) al menos un día a la semana. Los usuarios itinerantes pueden utilizar dispositivos corporativos o personales y acceder a la red corporativa a través de una VPN o conectarse directamente a Internet para acceder a las aplicaciones en la nube y realizar sus tareas.

Más tráfico de red

Las nuevas aplicaciones, incluido el almacenamiento en la nube pública y las videoconferencias, requieren una gran cantidad de datos y de tráfico de red para satisfacer la creciente demanda de los empleados. Este aumento de la carga de tráfico está ejerciendo una presión cada vez mayor sobre la infraestructura de red existente y los procesos de seguridad centralizados, lo que conlleva una reducción del rendimiento, una productividad más baja y una experiencia de usuario deficiente en general.

Comprender los retos en materia de seguridad y redes

También han surgido numerosos retos en materia de seguridad y redes en la última década, que requieren nuevas soluciones innovadoras para abordarlos con eficacia.

Aumento de los costes de la arquitectura de red tradicional

La función tradicional de la WAN era conectar a los usuarios de la sucursal o el campus con aplicaciones alojadas en los servidores de un centro de datos centralizado. Por lo general, se utilizaban circuitos MPLS específicos para contribuir a garantizar la seguridad y la fiabilidad de la conectividad. Sin embargo, el aprovisionamiento y mantenimiento-deestoscircuitosespecíficosescostoso, especialmente en comparación con la amplia disponibilidad de otras opciones de DIA más baratas que actualmente están a disposición de las empresas.

MATERIA TÉCNICA

MPLS es una técnica de enrutamiento que utiliza etiquetas de ruta virtual en lugar de direcciones de terminal de red para dirigir el tráfico a través de la red, lo que reduce la carga en los routers y acelera la disponibilidad del tráfico. MPLS proporciona una calidad de servicio (QoS) más fiable para aplicaciones con un consumo elevado del ancho de banda o sensibles a la latencia. Las tecnologías MPLS se pueden aplicar a cualquier protocolo de capa de red (de ahí el nombre, "multiprotocolo") y las empresas las utilizan a menudo, por ejemplo, para devolver el tráfico de red vital para la empresa desde las sucursales al centro de datos.

Ineficiencias en el modelo de red centralizada

El modelo de red centralizada tenía sentido cuando el centro de datos de la empresa era el principal destino para que los usuarios accedieran a las aplicaciones y a los datos a través de la red. El tráfico de Internet era relativamente insignificante y podía gestionarse fácilmente a través de los circuitos MPLS existentes. El tráfico de red puede enrutarse y priorizarse según sea necesario para garantizar un rendimiento eficiente y fiable, mientras que los recursos de personal de TI limitados y caros, como los equipos de seguridad y redes, pueden administrar la red de forma centralizada en todas las ubicaciones.

Tradicionalmente, las organizaciones retornaban (es decir, redirigían) el tráfico de red de las sucursales a las sedes centrales para aplicar políticas de seguridad, a menudo utilizando enlaces MPLS. Sin embargo, en la era digital moderna, este enfoque no es eficiente. A medida que las empresas adoptan cada vez más las aplicaciones SaaS, así como la plataforma como servicio (PaaS) y las cargas de trabajo y los recursos de IaaS proporcionados desde varias nubes, la experiencia de usuario en las aplicaciones se ha visto afectada. Retornar el tráfico dirigido a Internet a través de redes MPLS diseñadas para ofrecer un acceso rápido y fiable al centro de datos es costoso y puede resultar lento. La conclusión es que las redes MPLS no son una forma eficaz o efectiva de gestionar la explosión sin precedentes del tráfico de Internet que conlleva la adopción de la nube.

MATERIA TÉCNICA

El tráfico destinado a Internet se devuelve de forma efectiva a través de la red MPLS a una cabecera (como una sede corporativa o un centro de datos) que lo dirige a través de un conjunto de comprobaciones de seguridad y, a continuación, proporciona acceso a Internet, pero, por desgracia, también actúa como un cuello de botella.

MATERIA TÉCNICA

Los enlaces WAN existentes que utilizan MPLS son incapaces de gestionar las crecientes demandas de ancho de banda de los usuarios que necesitan un acceso rápido y fiable a Internet, para poder ser lo más productivos posible. Para abordar la creciente necesidad de acceso directo a Internet para aplicaciones basadas en la nube, cada vez más organizaciones (el 79 % según el Enterprise Strategy Group) se están planteando utilizar, o ya utilizan, el DIA de banda ancha en las sucursales en lugar de redirigir el tráfico a través de MPLS. Aunque estos enlaces DIA abordan los problemas de rendimiento asociados con el retorno del tráfico a través de una ubicación de cabecera MPLS, a menudo los proporcionan los proveedores de servicios de Internet (ISP) locales como enlaces de banda ancha; es importante comprobar la resistencia, la priorización de la calidad de servicio (QoS) y las garantías de los acuerdos de nivel de servicio (SLA).

Problemas de rendimiento con aplicaciones de ejecución de negocios de SaaS

Muchas de las aplicaciones SaaS actuales se han convertido en las principales aplicaciones empresariales de ejecución de negocios. Algunos ejemplos son Salesforce, Office 365 y Workday. El retorno del tráfico de SaaS a través de costosos enlaces WAN MPLS a una cabecera corporativa genera congestión y latencia de red. Esto, a su vez, genera problemas de rendimiento que desembocan en una pérdida de productividad y en la frustración del usuario. La complejidad de la WAN puede provocar problemas de rendimiento adicionales debido a decisiones de enrutamiento de calidad inferior a la óptima, a una clasificación y una priorización del tráfico incorrectas y a una falta de aplicación de las políticas.

Cuando los usuarios experimentan problemas de rendimiento con las aplicaciones aprobadas por la empresa, suelen recurrir a aplicaciones no autorizadas y potencialmente peligrosas para realizar su trabajo. Esta cultura de TI en la sombra en la que se elude el departamento de TI (y por ende los controles de seguridad) es un gran problema. En la actualidad, se utilizan más de 1200 servicios en la nube de media en las empresas grandes y Enterprise Strategy Group informa de que hasta el 98 % de dichos servicios son aplicaciones SaaS no autorizadas y no analizadas.

ADVERTENCIA

Aunque muchas organizaciones implementan políticas de seguridad que requieren que los usuarios remotos o itinerantes redirijan su tráfico de red a través de túneles VPN, el 85 % de las organizaciones cree que sus usuarios infringen estas políticas de VPN corporativas, según Enterprise Strategy Group.

Exceso de retos de integración y herramientas de seguridad aisladas

Los equipos de seguridad se ven desbordados con frecuencia por montones de datos de productos de seguridad independientes y puntuales que no se integran con otros productos y que requieren diferentes niveles de conocimiento y competencias para su funcionamiento y mantenimiento. Enterprise Strategy Group informa de que el 31 % de las organizaciones utiliza más de 50 herramientas diferentes y la investigación de Cisco indica que a la mayoría de ellas les resulta difícil organizar las alertas de las distintas herramientas. Esta falta de integración e interoperabilidad dificulta, si no imposibilita, que los analistas de seguridad supervisen y correlacionen la información sobre amenazas y seguridad en tiempo real.

RECUERDE

Estos retos han crecido exponencialmente a medida que las sucursales conectadas y las oficinas remotas han proliferado. Cada ubicación requiere normalmente un router y un firewall como mínimo. En ubicaciones remotas y sucursales, a menudo se adquieren como componentes básicos que proporcionan funciones limitadas y capacidades de gestión remota. Al cambiar al DIA en las ubicaciones remotas, existe la necesidad de ofrecer el nivel adecuado de seguridad a los usuarios: seguridad web, firewalls, prevención de pérdida de datos, etc. Sin embargo, no resulta práctico comprar una pila independiente de dispositivos de seguridad para cada una de las ubicaciones. Aunque algunos de estos componentes de las sucursales incluyan herramientas de seguridad, normalmente no hay personal de TI en estas ubicaciones para mantenerlos. Con el tiempo, el hardware no podrá hacer frente a las cargas de tráfico cada vez mayores, por lo que las herramientas de seguridad tendrán que desplazarse de estos dispositivos a la nube, donde pueden aplicarse y gestionarse de forma centralizada.

CONSEJO

Hay luz al final del túnel. Según el estudio comparativo sobre CISO de Cisco, el 93 % de los CISO está de acuerdo en que trasladar la seguridad a la nube ha aumentado la eficacia, lo que permite a los equipos de seguridad centrarse en otras áreas.

Escasez de personal de seguridad y aumento de los costes del personal

La escasez mundial de profesionales de la seguridad y la gran inversión continua necesaria para formar y conservar a personal de seguridad cualificado es un problema muy real para las organizaciones de todo el mundo. Según Cybersecurity Ventures, en 2021 quedarán sin cubrir

3,5 millones de puestos de trabajo de ciberseguridad en todo el mundo. Enterprise Strategy Group e ISSA informan además de que el 74 % de los encuestados afirma que la escasez de trabajadores cualificados en ciberseguridad ha afectado de manera significativa a sus organizaciones.

Nuevas ciberamenazas que aprovechan las brechas de seguridad

Las ciberamenazas avanzadas, incluido el ransomware, los troyanos de acceso remoto (RAT) y las amenazas avanzadas persistentes (APT), han evolucionado para aprovechar la falta de visibilidad y control en la red distribuida moderna. Los usuarios remotos y de sucursales son especialmente vulnerables a muchas de estas amenazas, porque las organizaciones se han alejado de un modelo de seguridad centralizado y, a menudo, son incapaces de aplicar políticas de seguridad uniformes en la red. Las funciones de seguridad limitadas y el hecho de que el personal de TI se encuentre en ubicaciones remotas hacen que estos usuarios sean aún más vulnerables a sufrir un ataque o brecha que prospere. Los ciberdelincuentes saben que los trabajadores remotos suelen ser más vulnerables y, por tanto, tienen como objetivo ubicaciones remotas y a usuarios itinerantes.

ADVERTENCIA

Según el Enterprise Strategy Group, el 68 % de las organizaciones ha sufrido ataques en los últimos 12 meses en los que una sucursal o un usuario itinerante ha sido la fuente de riesgo.

CONSEJO

Las organizaciones actuales deben tener en cuenta las nuevas e innovadoras opciones de redes y seguridad para abordar con éxito los retos de la red empresarial actual. Puede encontrar más información al respecto en el capítulo 2.

EN ESTE CAPÍTULO

- Reconoceremos las limitaciones de MPLS
- Innovaremos con SD-WAN
- Abordaremos las amenazas de seguridad con SWG y SIG
- Presentaremos los servicios de acceso seguro en el borde (SASE)

Capítulo 2
La evolución de las soluciones de seguridad y redes

El panorama de las redes y la seguridad está evolucionando desde numerosas soluciones puntuales dispares a plataformas de redes y seguridad totalmente integradas, multifunción y basadas en la nube. Este cambio se está produciendo porque las empresas necesitan cada vez más la flexibilidad y la capacidad para implementar servicios de seguridad y redes como y donde elijan. Necesitan controlar y proteger el acceso a Internet, gestionar el uso de aplicaciones en la nube y proporcionar protección a los usuarios itinerantes, a la vez que reducen la presión sobre los recursos y eliminan la necesidad de hardware.

En este capítulo, aprenderá cómo evolucionaron la red y la seguridad desde las redes de área amplia (WAN) tradicionales a la WAN definida por software (SD-WAN) y desde puertos web seguros (SWG) a gateways de Internet seguras (SIG). También se aporta información sobre el nuevo concepto combinado de servicios de acceso seguro en el borde (SASE).

Un vistazo a la tecnología WAN tradicional

Durante casi dos décadas, la tecnología WAN de referencia para infraestructura de redes de TI, voz y datos ha sido la arquitectura de red de conmutación de etiquetas de protocolos múltiples (MPLS). Las redes MPLS proporcionan una red troncal de red resistente para conectar la sede central de la empresa y las sucursales remotas. MPLS ofrece la posibilidad de priorizar el tráfico de voz, vídeo y datos en su red para cumplir requisitos empresariales únicos y los paquetes pueden enviarse a través de una red privada MPLS.

Sin embargo, las empresas actuales necesitan más control, flexibilidad y administración centralizada de sus entornos de WAN que la que ofrece MPLS, lo que está impulsando la necesidad de un cambio. Los costes asociados al aprovisionamiento y el mantenimiento de enlaces WAN MPLS privados por sí solos pueden ser un catalizador suficiente para el cambio. Las redes MPLS suelen proporcionarlas los proveedores de servicios de Internet (ISP) y otros proveedores de servicios, tanto las conocidas empresas de telecomunicaciones como empresas más pequeñas no tan conocidas.

Además, las ineficiencias de una red MPLS que redirige el tráfico con destino a Internet a través de enlaces de sucursales a una cabecera corporativa incrementan los costes, la complejidad, los problemas de rendimiento y la latencia. Muchas organizaciones, inevitablemente, acaban instalando un enlace de acceso directo a Internet (DIA) secundario en sus sucursales para descargar parte del tráfico de Internet. Dicha solución aumenta los costes recurrentes e introduce aún más complejidad. Es posible que el tráfico de red no se enrute necesariamente a través del mejor enlace en un momento dado y que el ancho de banda de uno u otro enlace esté infrautilizado.

En cuanto a la seguridad, el tráfico con destino a Internet debe estar mínimamente protegido mediante seguridad en la capa de DNS o un firewall, pero también puede requerir filtrado del contenido web, prevención de pérdida de datos, detección de malware en tiempo real y otros servicios de seguridad. La falta de visibilidad y un punto de aplicación de políticas centralizado dificultan, si no imposibilitan, que los equipos de seguridad garanticen un entorno operativo seguro y compatible (consulte la figura 2-1).

FIGURA 2-1: Los retos con las arquitecturas WAN actuales son la complejidad, los costes, los retrasos y las interrupciones.

Explorar las soluciones SD-WAN

La configuración de varios routers conectados a diferentes circuitos (por ejemplo, un enlace MPLS y un enlace a Internet de banda ancha) para enrutar el tráfico de red de forma eficiente y óptima puede suponer un reto. En muchos casos, puede que se limite a una opción de equilibrio de carga round-robin, especialmente si no dispone de personal de red en sus distintas ubicaciones remotas.

Más allá del simple equilibrio de carga, la capacidad de ancho de banda disponible puede no utilizarse durante los periodos de congestión. Por ejemplo, la conexión a Internet de banda ancha puede funcionar con lentitud durante un periodo de tiempo determinado, mientras que el costoso enlace MPLS no está congestionado relativamente y puede proporcionar una conectividad a Internet más rápida. La imposibilidad de incorporar diferentes enlaces supone una pérdida de capacidad de ancho de banda y una menor satisfacción de los empleados.

EJEMPLO DE CISCO SD-WAN

Cisco SD-WAN es una arquitectura segura, a escala de nube, abierta, programable y escalable. Le permite establecer rápidamente un fabric de superposición de SD-WAN para conectar centros de datos, sucursales, campus e instalaciones de coubicación. Esta conexión puede mejorar la velocidad, la seguridad y la eficiencia de la red. Cisco SD-WAN es compatible con (consulte la siguiente figura):

- **Cualquier implementación:** gestión de WAN flexible para entornos multitenant, en las instalaciones y en la nube.
- **Cualquier servicio:** un conjunto completo de servicios, entre ellos, seguridad de la sucursal, seguridad de la nube, calidad de la experiencia en aplicaciones, voz y colaboración y onramp en la nube.
- **Cualquier método de transporte:** implemente su WAN en cualquier tipo de conexión, lo que incluye vía satélite, Internet, MPLS y 5G/evolución a largo plazo (LTE).
- **Cualquier ubicación:** las plataformas físicas o virtuales están disponibles para sucursales, coubicación y nube.

Arquitectura segura de SD-WAN a medida de la nube

Fuente: Cisco.

CONSEJO

Una solución SD-WAN puede abordar estos escenarios y ofrecer otras funciones de enrutamiento avanzadas para optimizar el tráfico de su red según sea necesario. Otras consideraciones y funciones adicionales son:

- Enrutamiento del tráfico a través de diferentes enlaces en función del destino

- Enrutamiento del tráfico a través de diferentes enlaces en función del coste
- Incorporación de varios enlaces para proporcionar un mayor ancho de banda total
- Nuevo enrutamiento del tráfico a través de un enlace alternativo cuando un enlace está congestionado, es inestable o está inactivo
- Priorización de determinado tráfico de aplicaciones, como voz y vídeo, para garantizar la calidad del servicio

SD-WAN combina y optimiza las tecnologías WAN tradicionales, como MPLS y las conexiones a Internet de banda ancha. Esto permite a las organizaciones enrutar de manera eficiente el tráfico de red a varias sucursales remotas a la vez que ofrece funciones mejoradas de supervisión y gestión. SD-WAN supervisa el tráfico de red en todos los enlaces disponibles en tiempo real y selecciona de forma dinámica la mejor ruta para cada paquete de datos que circula por la red.

CONSEJO

La International Data Corporation prevé que el mercado global de SD-WAN alcanzará los 8 mil millones de dólares en 2021 y la investigación de Forrester revela que el 64 % de las organizaciones de EE. UU. tiene previsto implementar SD-WAN el próximo año.

Hacer frente a las amenazas de seguridad de Internet

Durante la mayor parte de los últimos 25 años, la seguridad de la red se ha centrado en la detección y prevención de amenazas de malware (como virus, ransomware, spam y suplantación de identidad), la identificación y el bloqueo del uso no autorizado de Internet (como navegar por contenido inapropiado y descargar contenido pirateado) y la garantía del rendimiento de la red (con proxy de almacenamiento en caché y productos frente a la denegación de servicio distribuida [DDoS]).

RECUERDE

En 2017, varios proveedores y analistas del sector definieron un nuevo concepto: la gateway de Internet segura (SIG). Mientras que el SWG está diseñado principalmente para el tráfico web, este nuevo tipo de solución nativa de la nube ofrecía varias funciones en más tipos de tráfico, como seguridad del sistema de nombre de dominio (DNS), SWG, firewall como servicio (FWaaS) y agente de seguridad de acceso a la nube (CASB), para mejorar la seguridad y el rendimiento al mismo tiempo que se reducen los costes y las tareas de mantenimiento. Una SIG proporciona un amplio conjunto de seguridad de la nube para que las organizaciones

puedan proteger a los usuarios sin importar dónde se encuentren. Puede ampliarse fácilmente para cubrir el tráfico adicional y a los usuarios de forma más eficiente que el antiguo enfoque de dispositivo SWG en las instalaciones.

Échele SASE a la vida

En 2019, Gartner publicó un informe titulado *El futuro de la seguridad de la red está en la nube*. En este informe, Gartner introdujo el concepto de servicios de acceso seguro en el borde (SASE). El concepto SASE incluye un conjunto aún más amplio de funciones de seguridad que una SIG e incluye también la convergencia de las funciones de red. Una solución SASE puede proteger la nube, el centro de datos y los extremos de la red de sucursales y ofrecer un fabric de SD-WAN seguro a través de conexiones diferentes (consulte la figura 2-2).

En *El futuro de la seguridad de la red está en la nube*, Gartner compartió su pronóstico de que «[e]n 2023, el 20 % de las empresas habrá adoptado las capacidades de SWG, CASB, [acceso a la red Zero Trust] y FWaaS en las sucursales del mismo proveedor con respecto al 5 % de 2019».

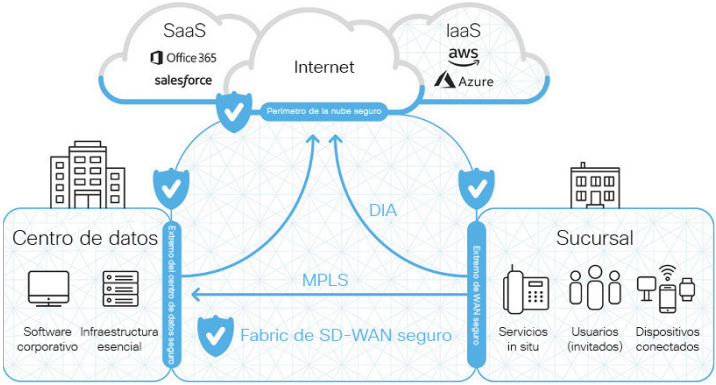


FIGURA 2-2: SD-WAN es un elemento de red fundamental en las soluciones SASE que puede dirigir el tráfico para la protección de la nube, el centro de datos y las redes de perímetro de las sucursales.

EN ESTE CAPÍTULO

- Analizaremos los retos de seguridad en la era de la nube
- Reconoceremos las características clave y ventajas de SASE
- Presentaremos los SASE

Capítulo 3
SASE: funciones de redes y seguridad combinadas

En este capítulo, conocerá los retos de seguridad surgidos en el nuevo modelo de arquitectura de red, la funcionalidad que necesita en una solución de seguridad, los problemas que debe tener en cuenta al implementar una solución y cómo pueden ayudar los servicios de acceso seguro en el borde (SASE).

Reconocer los retos de seguridad

La seguridad de la red ya no se limita al centro de datos, sino a la nube. A medida que el trabajo se traslada fuera de la oficina y la seguridad se traslada a la nube, el modelo de seguridad basado en el perímetro probado no está a la altura. Para conseguirlo, los equipos de TI deben identificar un nuevo enfoque para controlar y proteger a los usuarios, las aplicaciones, los dispositivos y los datos en cualquier lugar.

En la actualidad, el uso a gran escala de aplicaciones en la nube se ha vuelto fundamental para las operaciones empresariales de todas las ubicaciones. Según la investigación del Enterprise Strategy Group, el 32 % de las organizaciones afirma que la mayoría de sus aplicaciones se basan ahora en software como servicio (SaaS) y que se prevé que el número aumente al 60 % en dos años. El enfoque de la seguridad centralizada

se ha vuelto inviable debido al alto coste de redirigir el tráfico y a los problemas de rendimiento que genera en las sucursales.

Para superar estos problemas de rendimiento y coste, muchas organizaciones están adoptando un enfoque de redes más descentralizado para optimizar el rendimiento en ubicaciones remotas. Esto permite una ruta de acceso directo a Internet (DIA) más eficiente para estas oficinas, pero también saca a la luz nuevos retos de seguridad, entre los que se incluyen:

- **Brechas en la visibilidad y la cobertura:** las políticas de seguridad centralizadas no se pueden administrar y aplicar de forma eficaz en una red descentralizada. Esto se debe a que la mayor parte del tráfico que va de las sucursales a la nube y a Internet no cruza un punto centralizado de aplicación de políticas. Esto se traduce en brechas de visibilidad y cobertura, que aumentan el riesgo de que una brecha llegue a buen puerto o de que se produzca una infracción de cumplimiento.
- **Volumen y complejidad de las herramientas de seguridad:** los equipos de seguridad ya están teniendo problemas para mantenerse al día de las amenazas de ciberseguridad. Muchos de ellos cuentan con una gran cantidad de soluciones centradas en un momento específico que son difíciles de integrar y administrar. Estos productos puntuales generan cientos de alertas haciendo que sea muy difícil, si no imposible, mantener al día los análisis. En consecuencia, con muchas de las alertas no se llega a hacer nada.
- **Presupuestos y recursos de seguridad limitados:** los presupuestos de TI y seguridad ya son limitados. La implementación de varias soluciones de seguridad puntuales costosas, como firewalls, puertos web seguros (SWG), sistemas de prevención y detección de intrusiones (IDS e IPS) y prevención de pérdida de datos (DLP), en varias ubicaciones y la gestión remota de estas soluciones con recursos de seguridad limitados son poco prácticas e ineficaces.

Características clave y ventajas de SASE

En su informe de agosto de 2019, *El futuro de la seguridad de la red está en la nube*, Gartner definió el concepto de servicios de acceso seguro en el borde (SASE) como «una oferta emergente que combina capacidades integrales [de red de área amplia] con funciones integrales de seguridad de la red (como SWG, [agente de seguridad de acceso a la nube], [firewall como servicio] y [acceso a la red Zero Trust]) para satisfacer las necesidades de acceso seguro dinámico de las empresas digitales».

Estas son cuatro características clave de las organizaciones con transformación digital que están sentando las bases de este nuevo concepto:

- **Centrada en la identidad:** Gartner sugiere que «la transformación empresarial digital invierte los patrones de diseño de servicios de red y seguridad, cambiando el foco a la identidad del usuario y/o el dispositivo, no al centro de datos». Además, la «identidad del usuario/dispositivo/servicio es uno de los elementos de contexto más significativos que se puede tener en cuenta en la política que se aplica».
- **Nativa de la nube:** Gartner dice que las empresas digitales modernas tienen «[m]ás datos confidenciales ubicados fuera del centro de datos de la empresa en servicios en la nube que dentro» y «[m]ás tráfico de usuarios destinado a servicios en la nube pública que al centro de datos de la empresa».
- **Informática perimetral:** para respaldar el concepto de SASE, Gartner describe un «fabric/malla mundial de red y capacidades de seguridad de la red que se pueden aplicar cuando y donde sea necesario para conectar entidades a las capacidades de red a las que necesiten acceder».
- **Distribuida de forma global:** Gartner describe la necesidad de una «centralita inteligente» en la que «las identidades se conecten a las capacidades de red a través del fabric mundial de capacidades de acceso seguro del proveedor de SASE».

RECUERDE

El concepto SASE consolida numerosas funciones y capacidades de seguridad y redes, que tradicionalmente se ofrecían en varias soluciones puntuales aisladas, en una única plataforma nativa de la nube totalmente integrada.

Entre las principales ventajas para la empresa del concepto SASE, se encuentran las siguientes:

- Reducir los costes y la complejidad
- Habilitar el acceso remoto y móvil seguro
- Proporcionar enrutamiento basado en políticas y optimizado para la latencia
- Mejorar el acceso seguro y sin interrupciones para los usuarios
- Mejorar la seguridad con políticas uniformes
- Actualizar las políticas y la protección contra amenazas sin actualizaciones de hardware y software

- Restringir el acceso en función de la identidad del usuario, el dispositivo y la aplicación
- Aumentar la eficacia del personal de redes y seguridad con una gestión centralizada de políticas

CÓMO AVRIL AMPLÍA LA PROTECCIÓN DE LAS SUCURSALES CON CISCO UMBRELLA

En la actualidad, el DIA permite a las sucursales mejorar significativamente el rendimiento de la red, gracias a la eliminación de la latencia al acabar con la necesidad de redirigir el tráfico al centro de datos. Sin embargo, como resultado, el tráfico de Internet procedente de estas ubicaciones no se ve ni se protege mediante la pila de seguridad centralizada, lo que puede exponer a los usuarios y los datos confidenciales.

Para aprovechar el uso cada vez mayor del DIA, los equipos de TI necesitan un servicio simplificado basado en la nube que unifique la potencia de las soluciones de seguridad de varios puntos en una única consola. Esta solución es Cisco Umbrella.

Avril, un grupo agroindustrial francés, necesitaba proporcionar a sus sucursales una solución de seguridad fiable que pudiera seguir ampliándose a medida que Avril adquiriera nuevos negocios y divisiones. Para proteger estas ubicaciones mientras seguían proporcionándoles un DIA rápido, necesitaban un servicio de seguridad basado en la nube que pudiera funcionar en los extremos externos de la red, proporcionando una primera línea de protección.

Al utilizar la red integrada y la arquitectura de seguridad de Cisco Umbrella, Avril puede proteger a los usuarios de las sucursales, los dispositivos conectados y el uso de aplicaciones en decenas de miles de grupos con DIA. Al aprovechar la seguridad de Umbrella para ampliar la protección en todas partes, Avril ha podido reducir considerablemente el riesgo de fuga de datos y malware en todos los puertos y protocolos. Además de ser fácil de implementar y gestionar desde la nube, Umbrella también permite que Avril siga ampliando la protección para mantenerse al día con las nuevas necesidades y el continuo crecimiento.

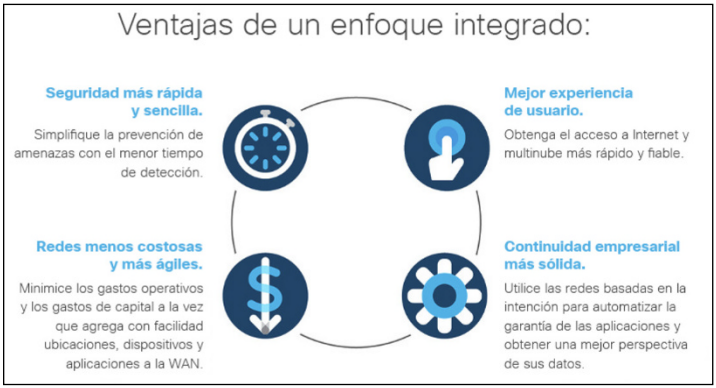
Con Cisco Umbrella, el grupo Avril pudo reducir el ransomware en un 100 %, proteger a los usuarios móviles que trabajan fuera de la red y reducir el tiempo de gestión de la seguridad en comparación con las soluciones anteriores.

Marc Tournier, gerente de cumplimiento normativo y seguridad de la información (CISO) de Avril, quedó impresionado con el reducido tiempo necesario para la rentabilización. "Umbrella protegió toda la red de la empresa en 10 minutos".

Estas ventajas son fundamentales para las organizaciones que necesitan abordar los actuales retos de las redes y la seguridad de un personal cada vez más centrado en la nube, distribuido, móvil y global.

Comienzo de su transición a SASE

SASE es un concepto amplio. Para simplificar las cosas, debe buscar una forma flexible de comenzar y lograr un progreso demostrable hacia los objetivos de su organización. Dicho esto, dos conceptos principales de SASE son la consolidación y la simplificación, por lo que tiene sentido trazar un rumbo que incluya elementos de red y de seguridad de un único proveedor. Este tipo de enfoque combinado ofrece muchas ventajas técnicas, de coste y de rendimiento para el usuario final (consulte la figura 3-1).



Fuente: Cisco

FIGURA 3-1: Las ventajas de un enfoque integrado de redes y seguridad.

Teniendo en cuenta estas ventajas combinadas, tiene sentido fijar la vista en el primer paso lógico en la red y la seguridad.

Primeros pasos en redes

Comience analizando las numerosas ventajas que tiene la red de área amplia definida por software (SD-WAN) y comience una prueba para conocer el impacto que podría tener en los costes de los servicios de red, el rendimiento y las tareas de gestión. A medida que desarrolla un plan para la SD-WAN, también debe decidir cuál es la mejor forma de proteger los nuevos flujos de tráfico, especialmente desde el creciente número

de sucursales remotas y usuarios itinerantes. Busque un proveedor con una sólida cartera de tecnología de red que ofrezca una amplia gama de capacidades de la red como servicio en el futuro.

Primeros pasos en seguridad

Busque una solución nativa de la nube que se pueda sustituir con flexibilidad e incluso mejorar en las capacidades de su pila de seguridad actual. Busque una solución que pueda gestionar un amplio conjunto de tareas de seguridad y presente los datos en una única consola para simplificar la implementación, las investigaciones y las continuas tareas de mantenimiento.

ADVERTENCIA

No vuelva a generar los retos que se derivaron de las pilas de seguridad en las instalaciones con un gran número de soluciones puntuales independientes.

EN ESTE CAPÍTULO

- Sabremos qué buscar en una solución SASE
- Conoceremos cómo abordan Cisco SD-WAN y Cisco Umbrella los requisitos principales de SASE

Capítulo 4
Los componentes de SASE y el enfoque de Cisco

En este capítulo, conocerá los componentes clave que debe buscar en una solución de servicios de acceso seguro en el borde (SASE) y leerá un ejemplo del enfoque que Cisco está adoptando para la convergencia de la seguridad de la nube y la red.

Componentes clave de la solución de SASE

Eche un vistazo a los componentes clave que conforman una solución SASE. (Puede obtener más información sobre SASE en el capítulo 3).

Red de área amplia definida por software

Una red de área amplia definida por software (SD-WAN) es una red de área amplia (WAN) virtual que permite a las empresas utilizar cualquier combinación de servicios de transporte, incluida la conmutación de etiquetas de protocolos múltiples (MPLS), la evolución a largo plazo (LTE) y el 5G de los móviles y la banda ancha, para conectar de forma segura a los usuarios con las ubicaciones de red. Puede seleccionar el método de comunicación más eficiente a la vez que reduce los costes y simplifica la gestión.

Seguridad de la capa del sistema de nombres de dominio

La resolución del sistema de nombres de dominio (DNS) es el primer paso cuando un usuario intenta acceder a un sitio web u otro servicio en Internet. Por lo tanto, reforzar la seguridad en las capas de DNS e IP es la primera línea de defensa contra las amenazas y es una excelente manera de detener los ataques antes de que los usuarios se conecten a destinos perjudiciales.

Gateway web segura

Un proxy web basado en la nube o un puerto web seguro (SWG) proporcionan funciones de seguridad como la detección de malware, el sandboxing de archivos y la inteligencia de amenazas dinámica, el descifrado de la capa de conexión segura (SSL), el filtrado de contenido y aplicaciones, y la prevención de pérdida de datos (DLP).

El firewall como servicio

El firewall como servicio (FWaaS) es la prestación de la funcionalidad del firewall basada en la nube para proteger otro tipo de tráfico de Internet distinto al tráfico web. Esto normalmente incluye control y visibilidad de capa 3 y capa 4 (IP, puerto y protocolo), junto con las reglas de capa 7 (control de aplicaciones) y anonimización de IP.

Agente de seguridad de acceso a la nube

Los agentes de seguridad de acceso a la nube (CASB) ayudan a controlar y proteger el uso del software como servicio (SaaS) basado en la nube. Las soluciones CASB permiten a las organizaciones aplicar sus políticas de seguridad y normativas de cumplimiento internas. El valor de los CASB radica en su capacidad para proporcionar información sobre el uso de aplicaciones basadas en la nube a través de plataformas de la nube e identificar el uso no autorizado. Los CASB utilizan la detección automática para detectar las aplicaciones en la nube que hay en uso e identificar las aplicaciones y los usuarios de alto riesgo, además de otros factores de riesgo clave. Por lo general, incluyen la funcionalidad de DLP y la capacidad para detectar y enviar alertas cuando se produce una actividad anómala de los usuarios para ayudar a detener las amenazas internas y externas.

Acceso a la red Zero Trust

El marco de seguridad Zero Trust de Forrester adopta un enfoque de seguridad de "nunca confiar, siempre verificar". El acceso a la red Zero Trust (ZTNA) verifica las identidades de los usuarios y establece la confianza del dispositivo antes de conceder acceso a aplicaciones

autorizadas, lo que ayuda a las organizaciones a evitar accesos no autorizados, contener las brechas y limitar el movimiento lateral de un atacante en su red. ZTNA requiere un enfoque de autenticación de varios factores, sólido y basado en la nube.

Enfoque de Cisco para SASE

Cisco ofrece funciones principales y adicionales de SASE a través de varios componentes clave de seguridad y red.

Cisco SD-WAN: red flexible gestionada en la nube

El enfoque de Cisco para SASE aprovecha una arquitectura SD-WAN a escala de nube (consulte la figura 4-1) diseñada para satisfacer las complejas necesidades de las WAN actuales a través de tres áreas clave:

- optimización avanzada de las aplicaciones que ofrece una experiencia con las aplicaciones predecible a medida que la estrategia empresarial de aplicaciones evoluciona
- Seguridad de varias capas que proporciona la flexibilidad necesaria para implementar la seguridad adecuada en el lugar adecuado, ya sea en las instalaciones o en la nube
- Simplicidad a escala empresarial, que permite una política integral del usuario a la aplicación en miles de sitios

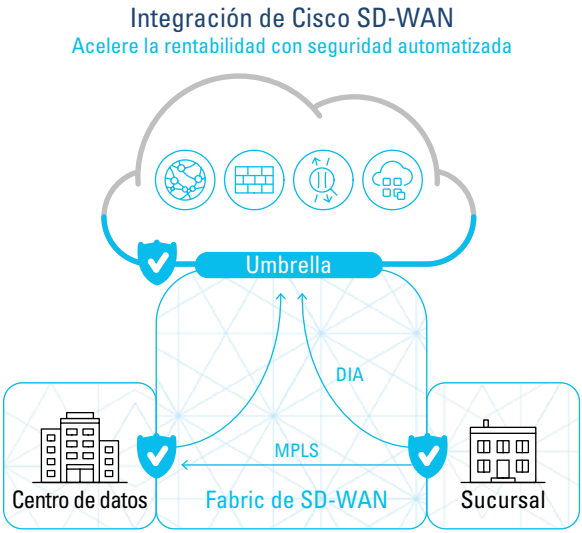


FIGURA 4-1: Arquitectura a escala de nube de Cisco SD-WAN.

La solución Cisco SD-WAN contiene los cuatro componentes clave indicados a continuación que funcionan en conjunto para formar el fabric de Cisco SD-WAN (consulte la figura 4-2):

- **Cisco vManage** (plano de gestión)
- **Cisco vBond** (plano de organización)
- **Cisco vSmart** (plano de control)
- **Routers Cisco WAN Edge** (fabric de red)

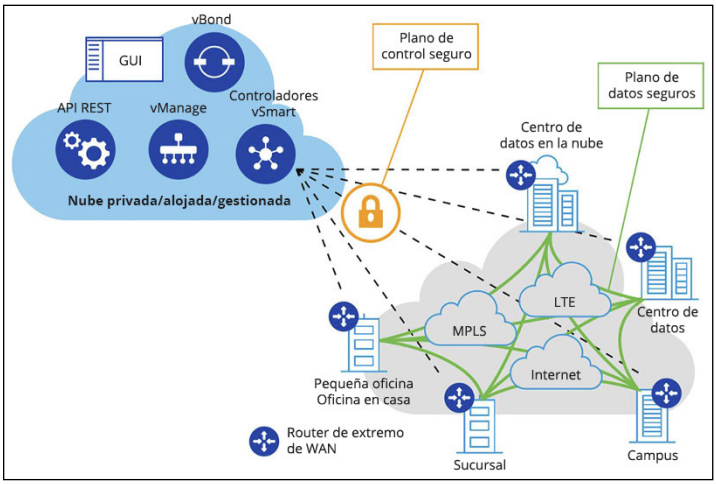


FIGURA 4-2: Integración de Cisco SD-WAN.

Cisco Umbrella: seguridad multifunción nativa de la nube

Cisco Umbrella es un servicio de seguridad en la nube que ofrece una experiencia de Internet segura, fiable y rápida. Al unificar varias funciones de seguridad en un único servicio, Umbrella ayuda a empresas de todos los tamaños a adoptar el acceso directo a Internet (DIA), proteger las aplicaciones en la nube y ampliar la protección a los usuarios itinerantes y las sucursales.

RECUERDE

Al habilitar estas funciones de forma conjunta en lugar de a través de soluciones puntuales, Umbrella reduce significativamente el tiempo, el dinero y los recursos que normalmente se requieren para la implementación, la configuración, la integración y la gestión de una pila de productos de seguridad independientes.

Cisco Umbrella ofrece un conjunto básico de funciones de seguridad en una consola basada en la nube (consulte la figura 4-3):

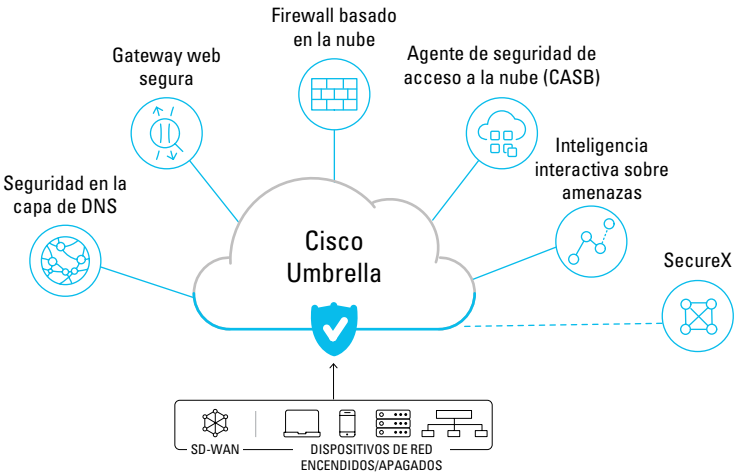


FIGURA 4-3: Cisco Umbrella ofrece funciones de seguridad de SASE y mucho más.

Seguridad en la capa de DNS

Cisco Umbrella bloquea las solicitudes de destinos maliciosos y no deseados, incluso antes de que se establezca una conexión, con lo que se detienen las amenazas en cualquier puerto o protocolo antes de que alcancen su red o sus terminales. Como un servicio basado en la nube, Umbrella:

- ofrece la visibilidad necesaria para proteger el acceso a Internet en todos los dispositivos de red, oficinas y usuarios itinerantes.
- Registra y categoriza la actividad de DNS por tipo de amenaza de seguridad o contenido web y la medida tomada, tanto si se ha bloqueado o como si se ha permitido.
- Se puede implementar de forma rápida para cubrir cientos de ubicaciones y usuarios en tan solo unos minutos para ofrecer un retorno inmediato de la inversión.

Puerto web seguro (SWG)

Cisco Umbrella incluye un proxy basado en la nube que puede registrar e inspeccionar todo su tráfico web para ofrecerle una mayor transparencia, control y protección. Esto incluye:

- Inspección en tiempo real de archivos de entrada en busca de malware y otras amenazas utilizando el motor de Protección frente a malware avanzado (APM) de Cisco y recursos de terceros
- Sandboxing de archivos avanzado por parte de Cisco Threat Grid
- Descifrado de SSL completo o selectivo para seguir protegiendo contra ataques ocultos
- Bloqueo de actividades de usuario específicas en aplicaciones determinadas (por ejemplo, cargas de archivos, adjuntar archivos y publicaciones propias o compartidas)
- Filtrado del contenido por categoría o localizadores uniformes de recursos (URL) específicos para bloquear destinos que infrinjan las políticas o reglas de cumplimiento

MATERIA TÉCNICA

Los túneles de protocolo de seguridad de Internet (IPsec), los agentes de AnyConnect, los archivos de configuración automática de proxy (PAC) y el encadenamiento de proxy se pueden utilizar para reenviar el tráfico web a Cisco Umbrella.

Firewall basado en la nube

Con el firewall de Cisco Umbrella, toda la actividad se registra y el tráfico no deseado se bloquea mediante el uso de normas de protocolo, IP y puertos. Para desviar el tráfico, solo debe configurar un túnel IPset desde cualquier dispositivo de red. La administración se maneja mediante el panel de Umbrella y a medida que se crean nuevos túneles, las políticas de seguridad se pueden aplicar de forma automática para una configuración sencilla y una aplicación consistente en todo el entorno.

El firewall basado en la nube de Cisco Umbrella ofrece:

- Visibilidad y control sobre el tráfico de Internet en todos los puertos y protocolos
- Políticas de IP, puerto y protocolo personalizables en el panel de Umbrella
- Visibilidad y control de aplicaciones de capa 7

Funciones del agente de seguridad para el acceso a la nube (CASB)

Cisco Umbrella revela la TI en la sombra al ofrecer la capacidad de detectar e informar sobre las aplicaciones en la nube que están en uso en su entorno. App Discovery de Umbrella ofrece:

- Una mayor visibilidad de las aplicaciones en la nube en uso y del volumen de tráfico
- Detalles de la aplicación e información de riesgos
- Capacidad para bloquear o permitir aplicaciones específicas

CONSEJO

La información de los CASB permite una mejor gestión de la adopción de la nube, reducir los riesgos y tener la capacidad de bloquear el uso de aplicaciones en la nube inapropiadas u ofensivas en el entorno de trabajo.

Inteligencia de amenazas interactiva

Cisco Umbrella analiza más de 200 000 millones de solicitudes DNS diarias, tomadas de la red global de Cisco en una base de datos gráfica masiva. También funciona continuamente con modelos estadísticos y de machine learning. Esta información la analizan de forma constante investigadores de seguridad de Umbrella y se complementa con inteligencia de Cisco Talos para detectar y bloquear de forma eficiente una extensa gama de amenazas. Umbrella está impulsado por esta inteligencia de amenazas y Cisco brinda acceso a dichos datos para permitirle acelerar la detección de amenazas y la respuesta ante ellas.

Los analistas pueden aprovechar Umbrella Investigate para conseguir una inteligencia rica sobre dominios, IP y malware en Internet. Investigate ofrece:

- Amplia visibilidad de las amenazas actuales y futuras
- Mejor priorización de las investigaciones de incidentes
- Investigaciones de incidentes y respuesta más rápidas

CONSEJO

El punto de vista de Internet único de Cisco permite a Umbrella descubrir dominios, IP y URL maliciosos antes de que se utilicen en ataques y ayuda a los analistas a acelerar las investigaciones.

Integración de Umbrella y SD-WAN

Con la integración de Cisco Umbrella y Cisco SD-WAN, puede implementar Umbrella en su red y obtener una potente seguridad basada en la nube para la protección contra amenazas en Internet. Umbrella ofrece la flexibilidad para crear políticas de seguridad según el nivel de visibilidad y protección que necesite, todo en un único panel.

CONSEJO

Umbrella se puede implementar en cientos de dispositivos con una única configuración en el panel vManage de Cisco SD-WAN para aumentar la seguridad en la capa de DNS. Para conseguir una mayor seguridad y mayor control granular, las capacidades del SWG de Umbrella y del firewall basado en la nube se pueden implementar con un sencillo túnel IPsec. Cisco ha abierto nuevos caminos en la automatización, la conexión y la implementación de los túneles, que conectan el tráfico de SD-WAN con los servicios de seguridad basados en la nube. Este enfoque integrado protege de forma eficiente a los usuarios de su sucursal, a los dispositivos conectados y el uso de la aplicación desde todas las conexiones de DIA.

Cisco SecureX

La plataforma Cisco SecureX conecta toda la cartera de seguridad integrada de Cisco y otras herramientas de terceros para ofrecer una experiencia coherente y simplificada que unifique la visibilidad, facilite la automatización y refuerce la seguridad. Reúne datos de AMP para terminales, Umbrella, SWE, SWC, ESA/WSA a través de SMA, NGFW Eventing a través de SSE, Orbital, Threat Grid, Duo, CDO y Tetration para mejorar la inteligencia y acelerar el tiempo de respuesta.

Puede visualizar la amenaza y su impacto en la organización al instante y obtener un veredicto rápido de los observables que está investigando a través de un gráfico de relaciones visualmente intuitivo. Le permite clasificar, priorizar, supervisar y responder a alertas de alta fidelidad a través del administrador de incidentes integrado. Además, puede adoptar medidas de respuesta rápida en varios productos de seguridad: aislar hosts, bloquear archivos y dominios y bloquear IP, todo desde una interfaz práctica (consulte la figura 4-4).

SecureX dota a los equipos de su centro de operaciones de seguridad (SOC) de una única consola para disfrutar de corrección directa, acceso a la inteligencia de amenazas y herramientas como el registro y el administrador de incidentes. Supera numerosos desafíos haciendo que las investigaciones de amenazas sean más rápidas, sencillas y efectivas.

FIGURA 4-4: Cisco SecureX simplifica la seguridad con una mejor visibilidad y automatización.

Zero Trust con Cisco Duo

Para las organizaciones de todos los tamaños que necesitan proteger datos confidenciales a escala, la solución de acceso fiable de Cisco Duo es una plataforma de seguridad Zero Trust centrada en el usuario y destinada a todos los usuarios, todos los dispositivos y todas las aplicaciones. La autenticación de varios factores (MFA) de Duo le permite verificar la identidad de todos los usuarios antes de conceder acceso a las aplicaciones corporativas. También puede garantizar que los dispositivos cumplan los estándares de seguridad, desarrollar y gestionar políticas de acceso y optimizar el acceso remoto y el inicio de sesión único (SSO) en aplicaciones empresariales.

Ventajas combinadas exclusivas de Cisco

Haciendo uso de los conocimientos de Cisco Talos, uno de los equipos de inteligencia de amenazas comerciales más grandes del mundo con más de 300 investigadores, Cisco Umbrella descubre y bloquea un amplio espectro de dominios maliciosos, IP, URL y archivos que se utilizan en los ataques. Cisco Umbrella también informa de los enormes volúmenes de actividad global de Internet (más de 200 000 solicitudes al día) en una combinación de modelos estadísticos y de machine learning para identificar nuevos ataques perpetrados en Internet.

Umbrella tiene una infraestructura de nube muy resistente que cuenta con cerca de un 100 % de tiempo de actividad desde 2006. Con el enrutado de Anycast, cualquiera de los más de 30 centros de datos de Cisco en todo el mundo está disponible mediante la misma dirección IP única. Como resultado, las solicitudes se envían de manera transparente al centro de datos más cercano y rápido y la conmutación por error es automática. Umbrella trabaja de manera conjunta con más de 900 de los principales proveedores de servicios de Internet (ISP), redes de entrega de contenido (CDN) y plataformas de SaaS del mundo para proporcionar la ruta más rápida para cualquier solicitud, lo que da como resultado una velocidad superior, una seguridad efectiva y una experiencia de usuario excelente.

CONSEJO

Para obtener más información sobre la solución de SASE de Cisco Umbrella, visite `https://umbrella.cisco.com/sase`.

EN ESTE CAPÍTULO

- Reconocer la naturaleza cambiante del trabajo y las redes
- Manejar aplicaciones y servicios basados en la nube
- Abordar las amenazas actuales y atraer y conservar a las personas de más talento en seguridad
- Introducción a SASE

Capítulo 5
Diez conclusiones clave

Hay que tener en cuenta diez puntos clave sobre la red de área amplia definida por software (SD-WAN) y la seguridad en la nube.

Más oficinas remotas y usuarios itinerantes

El número de usuarios de oficinas remotas, móviles e itinerantes está aumentando y estos usuarios suelen ser algunos de los objetivos más susceptibles a sufrir un atacante. La oportunidad de cometer errores, como hacer clic en un enlace de correo electrónico malicioso o visitar un sitio web malicioso, también está aumentando. Debido a que estos usuarios remotos e itinerantes pueden no tener acceso a un recurso de TI local, pueden ser menos proclives a ponerse en contacto con el soporte técnico o el equipo de seguridad cuando surge un problema.

De manera similar, los usuarios móviles e itinerantes a menudo no piensan dos veces antes de conectarse a una zona Wi-Fi pública. Los ciberdelincuentes aprovechan todas las oportunidades para aprovechar las vulnerabilidades de la red Wi-Fi y la confianza inherente que un cliente de una cafetería o un cliente de un hotel deposita en una conexión Wi-Fi "segura".

DIA es la nueva normalidad

Con la llegada de la era de la nube, las arquitecturas de red diseñadas para proporcionar una conectividad sólida a un centro de datos corporativo están obsoletas y deben evolucionar. Actualmente, la mayoría del tráfico de red se produce dentro del propio centro de datos (tráfico este-oeste) o desde las distintas ubicaciones de una organización a la nube a través de Internet (tráfico norte-sur). Como resultado, el retorno del tráfico de red desde ubicaciones remotas o sucursales a través de enlaces de red de área amplia (WAN) de conmutación de etiquetas de protocolos múltiples (MPLS) o del tráfico de usuarios itinerantes a través de conexiones de red privada virtual (VPN) ya no es una opción eficaz ni viable. Las organizaciones proporcionan cada vez más enlaces de banda ancha con acceso directo a Internet (DIA) para que sus usuarios remotos, de sucursales e itinerantes accedan a sus aplicaciones de software como servicio (SaaS) sin el rendimiento lento y la latencia asociada al retorno del tráfico a una oficina corporativa con una única pila de seguridad.

Las aplicaciones SaaS están tomando el control

Las aplicaciones SaaS, antes limitadas a las aplicaciones personales que los empleados descargaban en sus smartphones, se han convertido en aplicaciones empresariales esenciales que admiten funciones empresariales fundamentales en el lugar de trabajo digital actual. Salesforce permite la gestión de relaciones con los clientes (CRM), Workday ofrece servicios de nóminas y Concur facilita la gestión de los gastos. Otras aplicaciones como Office 365 ofrecen correo electrónico y colaboración, y otras aplicaciones como Box, Dropbox, Google Drive y OneDrive proporcionan almacenamiento y administración de archivos.

Por supuesto, parte del atractivo de las aplicaciones SaaS es su facilidad de uso. Para ofrecer esta cómoda experiencia de usuario, muchas aplicaciones SaaS ofrecen solo mecanismos débiles de control de acceso y seguridad... o ninguno. Otras tienen un control de acceso y una seguridad sólidos, pero a costa de la comodidad.

Una solución de seguridad multifunción nativa de la nube puede ofrecer servicios de agente de seguridad de acceso a la nube (CASB) para garantizar que se apliquen políticas de control de acceso y seguridad sólidas y coherentes a todas las aplicaciones, por ejemplo, mediante el inicio de sesión único (SSO) y la inteligencia de amenazas integrada.

Las redes antiguas son lentas y caras

Los costosos enlaces WAN MPLS que conectan sucursales remotas y redirigen todo su tráfico a una cabecera corporativa son ineficientes e introducen problemas de complejidad, rendimiento y satisfacción del usuario.

La arquitectura de red satisface las nuevas exigencias

SD-WAN, como solución de red independiente, es ideal para resolver los retos de las redes empresariales, especialmente en ubicaciones remotas y sucursales. SD-WAN permite a las organizaciones configurar nuevos sitios rápidamente, sin tener que esperar semanas o meses para configurar nuevos enlaces WAN MPLS. En su lugar, un proveedor de servicios de Internet (ISP) local puede proporcionar un enlace DIA, a menudo en solo un par de días.

Sin embargo, la agilidad y la simplicidad presentan nuevos retos para los equipos de seguridad de las empresas. En el apuro por conectarse, la seguridad puede ser una ocurrencia de última hora para la empresa. Una vez que la conexión a Internet está activa, la empresa está lista para funcionar, con o sin seguridad. Además, si la solución SD-WAN no cuenta con funciones de seguridad integradas, el equipo de seguridad puede necesitar enviar un firewall independiente u otros dispositivos de seguridad a la oficina remota. Conectar un dispositivo está bien, pero dos o tres, bueno, es pedir demasiado.

Busque una solución que reduzca la complejidad y los costes

En un pasado no muy lejano, los equipos de seguridad de las empresas implementaban de forma rutinaria las mejores soluciones de seguridad puntuales de diferentes proveedores para abordar las necesidades con un único fin: firewalls, puertos web seguros (SWG), sistemas de detección y prevención de intrusiones (IDS e IPS), el filtrado de contenido web, la seguridad del sistema de nombres de dominio (DNS), la prevención de pérdida de datos (DLP), la prevención de denegación de servicio distribuida (DDoS) y la protección frente a malware, por nombrar solo algunos. Estos productos independientes cuentan con diferentes sistemas operativos y consolas de administración y normalmente ofrecen

una integración limitada, si es que la ofrecen, con otros productos de seguridad.

Desafortunadamente, en la búsqueda de una estrategia de "defensa en profundidad", muchas organizaciones terminan con una "defensa hasta la saciedad", ya que estas diversas herramientas de seguridad aisladas incrementan la complejidad y a menudo crean problemas de rendimiento en la red.

No comprometa el rendimiento de la red

En definitiva, la experiencia de usuario es lo que impulsa la adopción con éxito de iniciativas de transformación digital en una organización. Un rendimiento deficiente de la red garantiza una experiencia de usuario negativa e impulsa a los empleados frustrados a recurrir a soluciones y aplicaciones de TI en la sombra potencialmente peligrosas.

Asegúrese de que su red y su plataforma de seguridad puedan ofrecer el rendimiento (y la seguridad) que los usuarios necesitan para seguir siendo productivos, tanto si se encuentran en la sede central, en una oficina remota o sucursal o en un dispositivo móvil.

Mantenga siempre la seguridad como su prioridad

Las ciberamenazas son cada vez más avanzadas y los atacantes emplean nuevas técnicas para explotar vulnerabilidades y vulnerar las redes objetivo. Los correos electrónicos de suplantación de identidad que antes se identificaban con facilidad por sus errores gramaticales y de ortografía se han vuelto mucho más difíciles de detectar. El ransomware también se ha vuelto mucho más frecuente, con el ransomware como servicio (RaaS) facilitando que prácticamente cualquiera pueda lanzar un ataque. Y estas son algunas de las amenazas menos sofisticadas que existen en la actualidad. El crimen organizado y los Estados nación lanzan ataques mucho más avanzados con vastos recursos que pueden tardar años en detectarse y erradicarse.

Facilítele la vida a su equipo de operaciones

La escasez mundial de profesionales de la seguridad cualificados es una tendencia que continuará en el futuro inmediato. La buena noticia para los profesionales de la seguridad es que habrá trabajos de seguridad bien remunerados en los próximos años. La mala es que el trabajo ya de por sí complicado de proteger una red empresarial se está dificultando a medida que las amenazas se vuelven más avanzadas y la proliferación de herramientas de seguridad aisladas requiere conocimientos y experiencia especializados que deben actualizarse constantemente.

Atraiga y conserve a las personas de más talento implementando soluciones innovadoras de redes y seguridad que integren la funcionalidad en una única plataforma basada en la nube y le faciliten la vida a todo su equipo de operaciones.

Cada viaje empieza con un solo paso

Con Cisco Umbrella, puede empezar paso a paso con la seguridad de la capa de DNS y desarrollar funciones adicionales a partir de ahí cuando su organización esté preparada.

Una solución de seguridad nativa de la nube y SD-WAN totalmente integrada puede ayudar a las organizaciones a abordar los retos relativos a la seguridad y las redes de la era de la informática móvil y la nube. Estos productos de servicios de acceso seguro en el borde (SASE) ofrecen funciones avanzadas de red y seguridad en un único panel, lo que permite a los equipos de seguridad y redes empresariales crear sus redes con confianza y con la agilidad que requieren las empresas modernas.

CONSEJO

Obtenga más información sobre el enfoque de Cisco en cuanto a los SASE en `https://umbrella.cisco.com/sase`.

Notas

Notas

Notas

Notas

Descubra la seguridad multifunción nativa de la nube

Las redes empresariales se enfrentan a una transformación importante. Tradicionalmente, todo el tráfico de Internet de las sucursales se ha enrutado de vuelta a una ubicación central donde se llevan a cabo las funciones de seguridad. Actualmente, las aplicaciones en la nube fundamentales para la empresa hacen que no sea práctico retornar el tráfico de las sucursales debido a problemas de rendimiento y coste. Las empresas necesitan una solución de seguridad y redes totalmente integrada diseñada para la nube. En este libro, aprenderá la forma en la que SASE afronta los retos de seguridad y redes actuales.

Descubrirá cómo...

- Aprovechar las funciones de SD-WAN
- Optimizar el rendimiento de la red perimetral
- Proteger el acceso remoto y móvil
- Simplificar la gestión de la red y la seguridad
- Consumir funciones de seguridad como servicio
- Acceder a la inteligencia de amenazas interactiva
- Implementar el acceso a la red Zero Trust

Lawrence Miller sirvió como suboficial en la Armada de EE. UU. y ha trabajado en tecnología de la información de diversos sectores durante más de 25 años. Es el coautor de CISSP para dummies y ha escrito más de 150 libros de la colección "For Dummies" sobre varios temas de seguridad y tecnología.

ISBN: 978-1-119-73562-5

para dummies®

También disponible en formato electrónico

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.