

Por gentileza de:



SD-WAN moderna de SASE

para
dummies[®]
A Wiley Brand



Conecta, optimiza
y protege cualquier cosa

Garantiza una política y
experiencia coherentes en
cualquier lugar

Supervisa las redes
en tiempo real
con AIOps

Edición especial de
Netskope

Muhammad Abid
Parag Thakore

Acerca de Netskope

Netskope, líder mundial en SASE, ayuda a las organizaciones a integrar redes y seguridad a la perfección, aprovechar AIOps, aplicar los principios Zero Trust e innovaciones de IA/AA para proteger los datos con una conectividad de alto rendimiento y protección integral contra amenazas. Rápida y fácil de usar, la plataforma Netskope proporciona acceso optimizado y seguridad en tiempo real a personas, dispositivos y datos en cualquier lugar. Netskope ayuda a los clientes a reducir riesgos, acelerar el rendimiento y obtener una visibilidad inigualable de cualquier actividad de aplicaciones en la nube, web y privadas. Miles de clientes confían en Netskope y en su potente red NewEdge para hacer frente a las amenazas cambiantes, los nuevos riesgos, los cambios tecnológicos, los cambios organizativos y de red, y los nuevos requisitos normativos. Para saber cómo Netskope ayuda a los clientes a prepararse ante cualquier cosa en su andadura hacia SASE, visita [netskope.com](https://www.netskope.com).

Nos gustaría mostrar nuestro agradecimiento a una serie de personas que han hecho posible este libro:

De Netskope: Amanda Anderson, Robert Arandjelovic, Madhavan Arunachalam, Chad Berndtson, Jason Clark, Fan Gu, Kathy Jacobsen, Jessica Jostes, Naveen Palavalli, Gerry Plaza, Carolyn Robinson, James Yokota

De Evolved Media: Shay Ben-Dov, Theresa Ingles, David Penick, Karen Queen, Vincent Rossmeier, Evan Sirof, Lauren Wagner, Dan Woods

SD-WAN moderna de SASE

para
dummies[®]



SD-WAN moderna de SASE

Edición especial de Netskope

por **Muhammad Abid y
Parag Thakore**

para
dummies[®]

SD-WAN moderna de SASE para Dummies®, Edición especial de Netskope

Una publicación de

John Wiley & Sons, Inc.

111 River St., Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2024 de John Wiley & Sons, Inc., Hoboken, Nueva Jersey

No se permite la reproducción total o parcial de este libro, ni su incorporación a un sistema informático ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación, escaneado u otros métodos, salvo lo permitido en los apartados 107 o 108 de la Ley de derechos de autor de los Estados Unidos de 1976, sin el permiso previo y por escrito del editor. Si deseas solicitar el permiso del editor, debes escribir a Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, Estados Unidos. Tel.: +1 (201) 748 6011, fax +1 (201) 748 6008, o en línea en <http://www.wiley.com/go/permissions>.

Marcas comerciales: Wiley, Para Dummies, el logotipo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier y cualquier otra imagen comercial relacionada son marcas comerciales o marcas comerciales registradas de John Wiley & Sons, Inc. o sus empresas asociadas en los Estados Unidos y otros países, y no se pueden utilizar sin permiso por escrito. El resto de las marcas comerciales son propiedad de sus respectivos propietarios. John Wiley & Sons, Inc. no está asociada a ninguno de los productos o proveedores mencionados en este libro.

LÍMITE DE RESPONSABILIDAD/EXCLUSIÓN DE GARANTÍA: AUNQUE EL EDITOR Y LOS AUTORES HAN PUESTO TODO SU EMPEÑO EN LA ELABORACIÓN DE ESTE LIBRO, NO HACEN NINGUNA DECLARACIÓN NI GARANTÍA CON RESPECTO A LA PRECISIÓN O INTEGRIDAD DE SUS CONTENIDOS Y RENUNCIAN ESPECÍFICAMENTE A CUALQUIER GARANTÍA, INCLUIDAS, ENTRE OTRAS, GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN EN PARTICULAR. NO PODRÁ CREARSE NI AMPLIARSE NINGUNA GARANTÍA POR PARTE DE REPRESENTANTES DE VENTA, MATERIALES COMERCIALES POR ESCRITO NI DECLARACIONES PROMOCIONALES PARA ESTA OBRA. EL HECHO DE QUE SE HAGA REFERENCIA A UNA ORGANIZACIÓN, SITIO WEB O PRODUCTO EN ESTE LIBRO O SE LOS MENCIONE COMO UNA CITA O POSIBLE FUENTE DE INFORMACIÓN ADICIONAL NO SIGNIFICA QUE LOS AUTORES O EL EDITOR APRUEBEN LA INFORMACIÓN O SERVICIOS QUE PUEDA PROPORCIONAR DICHA ORGANIZACIÓN, SITIO WEB O PRODUCTO NI SUS POSIBLES RECOMENDACIONES. ESTA OBRA SE VENDE ENTENDIÉNDOSE QUE EL EDITOR NO SE DEDICA A PRESTAR SERVICIOS PROFESIONALES. ES POSIBLE QUE LOS CONSEJOS Y LAS ESTRATEGIAS QUE SE INCLUYEN EN ESTE LIBRO NO SEAN ADECUADOS PARA TODAS LAS SITUACIONES. DEBERÁS CONSULTAR CON UN ESPECIALISTA CUANDO PROCEDA. ASIMISMO, LOS LECTORES DEBEN SABER QUE LOS SITIOS WEB INDICADOS EN ESTE LIBRO PODRÍAN HABER CAMBIADO O DESAPARECIDO DESDE SU REDACCIÓN AL MOMENTO DE SU LECTURA. NI EL EDITOR NI LOS AUTORES SERÁN RESPONSABLES DE NINGUNA PÉRDIDA DE INGRESOS O CUALQUIER OTRO DAÑO COMERCIAL, INCLUIDOS, ENTRE OTROS, DAÑOS ESPECIALES, FORTUITOS, INDIRECTOS O DE CUALQUIER OTRO TIPO.

Para obtener información general sobre nuestros productos y servicios, o sobre cómo crear un libro *Para Dummies* personalizado para tu empresa u organización, ponte en contacto con el Departamento de Desarrollo Empresarial en EE. UU. en el teléfono +1 (877) 409 4177, ponte en contacto con info@dummies.biz, o visita www.wiley.com/go/custompub. Para obtener información sobre licencias de la marca *Para Dummies* para productos o servicios, ponte en contacto con BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-21954-4 (pbk); ISBN 978-1-394-21955-1 (ebk)

Agradecimientos del editor

Entre algunas de las personas que han ayudado a comercializar este libro figuran las siguientes:

Editora: Elizabeth Kuball

Editora de adquisiciones:
Traci Martin

Director editorial: Rev Mengle

Responsable de cuentas de clientes: Jeremith Coward

Editor de producción:
Sai Karthick Kumarasamy

Colaboración especial: Nicole Sholly

Índice

INTRODUCCIÓN	1
Acerca de este libro	1
Algunas suposiciones obvias.....	2
Iconos utilizados en este libro.....	2
Más allá del libro.....	2
CAPÍTULO 1: Por qué las redes están poniéndose al día con informática moderna	3
El mundo «de uno a uno»	4
Apoyando el mundo de uno a muchos	5
El reto «de muchos a muchos»: SD-WAN en un importante punto de inflexión	8
Aplicaciones y proliferación de los dispositivos del IoT	9
Trabajo híbrido	9
Conexión de los usuarios a varias nubes y conexión de las nubes en red	10
Inalámbrico primero (4G/5G).....	10
Microsucursal.....	10
Convergencia de la tecnología de la información y de la tecnología operativa (TI/TO).....	11
Limitaciones de la SD-WAN tradicional frente al mundo moderno	12
No se puede mejorar la red con parches.....	12
La SD-WAN no puede ampliarse	13
La SD-WAN carece de funciones clave.....	13
La SD-WAN no aprovecha la inteligencia artificial (IA) ni el aprendizaje automático (AA).....	14
La SD-WAN no puede ofrecer una experiencia de calidad a más de 60 000 aplicaciones	14
La SD-WAN no simplifica el uso del plano de control	15
La tecnología inalámbrica 4G/5G se pensó a posteriori.....	15
La arquitectura no nació en la nube.....	15
La SD-WAN no es ampliable.....	16
La SD-WAN es rígida e irrelevante	16
CAPÍTULO 2: Una visión para las SD-WAN plenamente realizadas: el futuro sin fronteras	17
Borderless SD-WAN: Redes para un mundo de muchos a muchos.....	18
SD-WAN seguras.....	19

	Microsucursal.....	21
	SD-WAN para endpoint.....	21
	WAN inalámbrica.....	23
	Redes multicloud.....	24
	Acceso inteligente al IoT.....	25
	Qué cabe esperar de estas nuevas funciones.....	27
CAPÍTULO 3:	Cómo funciona Borderless SD-WAN	29
	Por qué Borderless SD-WAN debe tener una arquitectura que da prioridad a la nube.....	30
	Reconfiguración de los planos de gestión, control y datos.....	31
	El plano de gestión.....	31
	El plano de control	32
	El plano de datos.....	33
	Espacio para la inteligencia artificial	35
CAPÍTULO 4:	Ventajas de Borderless SD-WAN para las empresas	37
	Un enfoque de una sola plataforma, un solo software y una sola política	38
	Borderless SD-WAN facilita la vida de los usuarios finales	39
	Qué obtienen los expertos en redes de Borderless SD-WAN	41
	Aumento de la confianza operativa con AIOps.....	42
	Mayor eficiencia y agilidad con una SD-WAN que tiene en cuenta el contexto.....	42
	Aumento de la productividad y mejora de la experiencia del usuario con un rendimiento garantizado de las aplicaciones.....	43
	Inversión a prueba de futuro con un controlador 100 % basado en SaaS.....	44
	Mayor alcance y flexibilidad con WAN inalámbrica.....	44
	Transforma tu empresa con SASE en la nube.....	45
	Garantiza la seguridad de tu empresa con una protección SASE de 360 grados	46
	Haz realidad el valor empresarial de los datos con el procesamiento perimetral.....	47
	Reducción de los costos generales de TI	47
CAPÍTULO 5:	Cómo acelerar la adopción de SASE	49
	El problema de la seguridad con SD-WAN en el mundo anterior a SASE	50
	La seguridad en la nube preparó el camino a SASE.....	52
	SASE: nacido para unir la red y la seguridad.....	52

SASE es un viaje: recorrido por todo el entorno	55
Zero Trust, SASE que tiene en cuenta el contexto	55
Política unificada y experiencia coherente en cualquier lugar	56
SASE en la nube con un alcance global sin precedentes.....	58
Operaciones de TI unificadas y simplificadas.....	59

CAPÍTULO 6: Las diez funciones principales que se necesitan para que las empresas adopten Borderless SD-WAN	61
Potencia tu empresa con la convergencia de SASE	62
Obtén toda la potencia de la nube con una solución que le da prioridad.....	63
Rampa de acceso a la nube: conectividad segura y optimizada «de cualquiera a cualquiera»	64
Acceso inteligente a la red y enrutamiento avanzado	65
Seguridad integral de redes híbridas	65
Una experiencia de primera clase al usar cualquier aplicación y en cualquier lugar	66
Contexto para validar la identidad de los usuarios, los dispositivos y los riesgos de las aplicaciones y para mejorar los controles	66
Operaciones simplificadas, automatizadas e impulsadas por la IA	67
Soporte a una estrategia que prioriza lo inalámbrico.....	68
Compatibilidad total con el procesamiento perimetral.....	69

Introducción

Durante décadas, las redes informáticas han impulsado nuestras empresas, nuestras comunidades y nuestras vidas en general. A medida que la informática y el mundo digital han ido evolucionando, las redes empresariales han tenido dificultades para seguir el ritmo. Las redes son dinámicas y están vivas, impulsadas por las necesidades empresariales, la innovación tecnológica disponible y el ingenio humano. A veces, las redes se adelantan a las aplicaciones prácticas y, otras veces, una tecnología que antaño fue deslumbrante agota su vida útil y surgen nuevas tecnologías para cubrir necesidades incipientes.

En este libro se examina tanto la historia como el futuro de las redes empresariales. Se explica cómo las redes empresariales pueden ponerse al día y seguir el ritmo de un mundo centrado en la nube, impulsado por el Internet de las cosas (IoT) y que da prioridad a la movilidad. Las prácticas de trabajo en red del pasado tienen muchos aspectos positivos. Pero esos modelos y la tecnología que empleaban ya no son los mejores para las empresas actuales, que operan en un mundo en el que cada vez hay menos fronteras.

Necesitamos un nuevo tipo de redes y una nueva forma de pensar. Las funciones tecnológicas no interconectarán por sí solas a las personas que utilizan multitud de dispositivos con una gran variedad de destinos y aplicaciones ampliamente distribuidos. Necesitamos una visión de redes sin fronteras que sean compatibles con un mundo sin fronteras e hiperconectado.

Acerca de este libro

La red de área extensa definida por *software* (SD-WAN) sin fronteras es una forma de crear una arquitectura de red más segura, fiable y de mayor rendimiento que se adapta al entorno tecnológico actual, difuso y basado en la nube. Este libro puede ayudarte a entender cómo elaborar un plan para implementar esta solución de red orientada al mundo moderno. Y como está «definida por *software*», también puede evolucionar a medida que cambian los requisitos de la empresa. Mejor aún, también te ayudará a trabajar de forma más productiva y a ahorrar dinero.

Algunas suposiciones obvias

No eres ajeno a los fundamentos de las redes empresariales y a cómo Internet se ha convertido en un elemento central para ellas. Puedes ver fácilmente por qué las empresas han pasado de una WAN tradicional de conmutación por etiquetas multiprotocolo (MPLS) a una SD-WAN más moderna. Pero probablemente te preguntes qué va a pasar en el futuro. Puedes ver cómo los supuestos sobre dónde trabajarán las personas han cambiado permanentemente y cómo los dispositivos móviles y la infraestructura del IoT, junto con el mundo en continua expansión de las aplicaciones de *software* como servicio (SaaS) y los servicios en la nube, están provocando aún más cambios. Quieres dejar de ir siempre por detrás con tu arquitectura de red y aprovechar Borderless SD-WAN para poder funcionar en este mundo en continua evolución.

Iconos utilizados en este libro

A lo largo de este libro, aparecen iconos en los márgenes para llamar la atención sobre información importante.



CONSEJO

Cualquier cosa marcada con el icono «Consejo» es un atajo para facilitar una tarea concreta.



RECUERDA

El icono «Recuerda» te señala información que es especialmente importante conocer.



CUESTIONES
TÉCNICAS

La información muy técnica que puedes omitir la hemos marcado con el icono «Cuestión técnica».



ADVERTENCIA

Presta atención a cualquier cosa que lleve el icono «Advertencia» para ahorrarte algún que otro dolor de cabeza.

Más allá del libro

Aunque este libro está repleto de ideas, si cuando lo termines todavía piensas: «¿Dónde puedo encontrar más información?», visita www.netskope.com.

EN ESTE CAPÍTULO

- » Analizamos la evolución de la red de área extensa (WAN - Wide Area Network)
- » Exploramos cómo la WAN definida por *software* (SD-WAN) ha mejorado la WAN
- » Tratamos de entender el principal reto de la conexión remota a las redes SD-WAN tradicionales
- » Vemos por qué las SD-WAN no pueden ser tan efectivas como necesitamos que sean

Capítulo 1

Por qué las redes están poniéndose al día con informática moderna

En la historia de las redes informáticas ha habido muchos puntos de inflexión: olvidémonos de lo antiguo y demos la bienvenida a lo nuevo. Las redes de área local (LAN) dieron paso a las WAN y las WAN dieron paso a las SD-WAN, una era que parece estar llegando a su fin. En su lugar, las SD-WAN sin fronteras se perfilan como la próxima gran novedad en las redes empresariales. Esta evolución permite ofrecer una conectividad segura y adaptada al contexto desde cualquier lugar a cualquier lugar, de una forma diseñada específicamente para la era del trabajo en la nube y centrado en lo híbrido. Las organizaciones que se embarquen en este viaje de actualización más pronto que tarde se situarán por delante de sus competidores con una infraestructura de TI más flexible, segura y eficaz.

El mundo «de uno a uno»

Hace mucho tiempo, en un universo muy parecido al nuestro, las galaxias de empresas tenían que sobrevivir en un mundo estático y orientado al *hardware*. Las redes empezaron con las LAN, que conectaban los usuarios y los dispositivos dentro de un edificio, generalmente la sede central o las sucursales de una empresa. Todos los empleados acudían a la oficina todos los días. Las LAN permitían a cualquier persona que se encontrara en la misma ubicación física trabajar conjuntamente en la misma red. Cualquier aplicación que prestaba servicio a esos usuarios tenía que estar conectada a un centro de datos en una ubicación central, y cada acción que tenía lugar en la red tenía que enrutarse a través de ese centro de datos. Esto funcionó bien... hasta que dejó de hacerlo.



RECUERDA

Las LAN tenían sus limitaciones, sobre todo el hecho de que requerían que todos los usuarios estuvieran en el mismo lugar.

Cuando pasamos de las LAN a las WAN, pudimos colocar más dispositivos en más ubicaciones y conectarlos a centros de datos conectados a Internet que estaban protegidos por un *firewall*. Cada dispositivo estaba en un perímetro físico que llevaba a cabo funciones de red.

Con las WAN, los empleados de las sucursales que querían conectarse a las aplicaciones de la empresa tenían que atravesar la red privada de la empresa —normalmente a través de conmutación por etiquetas multiprotocolo (MPLS— y volver al centro de datos central. (MPLS es una tecnología de red muy utilizada para redes privadas). Contar con aplicaciones en cada instalación remota era sencillamente demasiado difícil y poco práctico. La ubicación centralizada permitía adoptar un control uniforme y garantizar la seguridad de las aplicaciones y la red. Esto obligaba a todas las sucursales a conectarse a través de la WAN con el centro de datos o la sede corporativa.

Si era necesario acceder a Internet, los usuarios eran encaminados hacia y desde cualquier aplicación empresarial alojada en Internet desde la oficina central. Este sistema, que consistía en redirigir el tráfico, lo que también se conoce como «*hairpinning*», era engorroso.

Y lo era incluso para empresas con presencia mundial, como instituciones financieras internacionales, sistemas sanitarios en varios hospitales y cadenas de restaurantes con equipos de punto de venta, como Taco Bell o McDonald's.

En la década de 2000, las conexiones MPLS permitieron a los operadores converger voz, vídeo y datos en la misma red. Incluso hoy en día, MPLS proporciona conexiones de red fiables respaldadas por acuerdos de nivel

de servicio (SLA), pero es caro y puede llevar meses planificarlo y suministrarlo (consulta la figura 1-1).

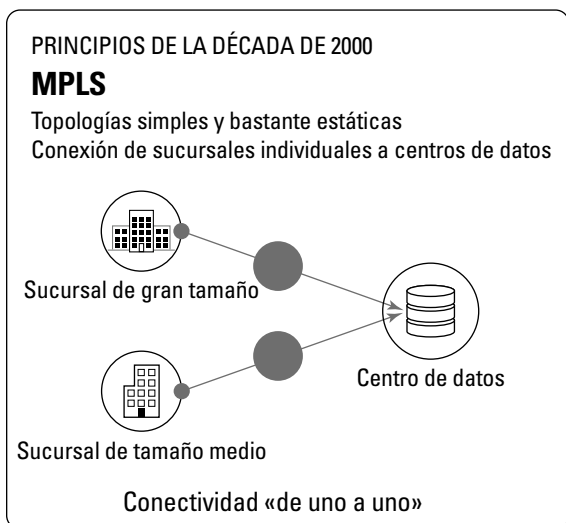


FIGURA 1-1: En el mundo «de uno a uno», las sucursales utilizan MPLS para conectarse a una ubicación centralizada denominada centro de datos, donde se alojan todas las aplicaciones.

Sin embargo, cuando las empresas empezaron a utilizar aplicaciones más inmersivas como el vídeo, MPLS simplemente no podía proporcionar el ancho de banda suficiente en una sucursal. Además, la implementación y mantenimiento de MPLS resultaba caro, y utilizarlo para cubrir las grandes necesidades de ancho de banda del consumo de vídeo era prohibitivo. Por ello, las empresas buscaban un transporte alternativo y rentable. Lo encontraron, y es bien conocido por nosotros como *transporte por Internet*.

Apoyando el mundo de uno a muchos

El gasto en ancho de banda de MPLS y la ralentización del suministro de una WAN fueron los primeros indicios de que las estructuras de red del pasado no estaban a la altura de las exigencias actuales. Pero también había muchas otras señales.

Las empresas se enfrentaban a un nuevo reto en un mundo en el que el *software* y el almacenamiento se trasladaban a Internet, un modelo conocido como informática en la nube y *software* como servicio (SaaS). Necesitaban asegurarse de que podían entregar y mantener aplicaciones

(como Microsoft 365 para la productividad, Amazon Web Services (AWS) para la potencia de cálculo y el almacenamiento de datos, y Google Cloud para Google Docs y otros servicios en la nube) de forma segura y con un funcionamiento fiable. A medida que aumentaba la dependencia del número de aplicaciones inmersivas basadas en vídeo, en la nube y SaaS, y a medida que cambiaba el tipo de aplicaciones, añadir simplemente más ancho de banda MPLS resultaba increíblemente caro. ¿Qué debían hacer las empresas? Necesitaban que llegara un héroe de brillante armadura digital, y rápido.

Afortunadamente, SD-WAN apareció justo a tiempo, proporcionando la siguiente evolución lógica en la arquitectura WAN. SD-WAN era una tecnología moderna que permitía el control centralizado dentro de una infraestructura distribuida, resolviendo así muchas de las presiones que las aplicaciones en la nube ejercían sobre la WAN tradicional.

SD-WAN prometió aprovechar una variedad de transportes diferentes (MPLS, Internet o sistemas celulares) y ofrecer un rendimiento de nivel empresarial a través de uno o más enlaces. Al abstraer la capa de red y enrutar el tráfico conforme a políticas definidas y gestionadas de forma centralizada, SD-WAN optimizó el enrutamiento y la priorización del tráfico de aplicaciones. SD-WAN prometió conectividad entre los usuarios de la sucursal con el centro de datos y las aplicaciones en la nube (consulta la figura 1-2).

En concreto, SD-WAN:

- » Facilitó una conexión segura y cifrada a través del Internet público, sistemas celulares y MPLS a aplicaciones y datos tanto a nivel local como en la nube.
- » Permitió conectar una ubicación central, como un centro de datos, a muchas ubicaciones distribuidas, como las distintas sucursales de las empresas.
- » Permitió a las empresas enrutar y priorizar el tráfico en función del tipo de aplicación que se utilizaba y de los datos que ese tráfico contenía.

SD-WAN ofreció a las empresas más opciones y control. Les permitía utilizar el transporte por Internet de forma dinámica y eficiente, sin dejar de ofrecer la opción de utilizar MPLS cuando fuera necesario. Como el uso de conexiones a Internet era mucho más barato que el de MPLS, los costos eran mucho menores.

El uso de SD-WAN también aportó ventajas de rendimiento. Aunque el Internet público puede ser a veces menos fiable que MPLS, SD-WAN

cuenta con funciones que mejoran la experiencia del usuario y mantienen una alta fiabilidad. Por ejemplo, podría ofrecer funciones de calidad de servicio que dan prioridad a los datos. También dispone de funciones de corrección de enlaces, como la conexión de error de reenvío, que puede ayudar a solucionar problemas y mejorar la conexión.

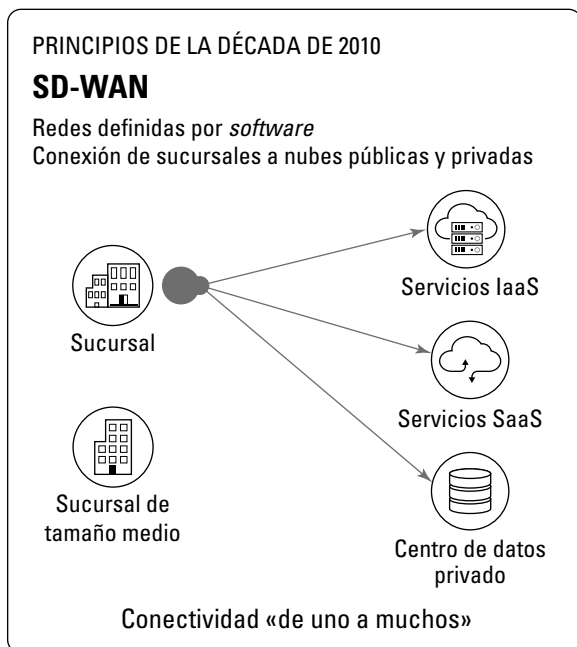


FIGURA 1-2: En el mundo de «uno a muchos», las sucursales dirigen el tráfico no solo al centro de datos centralizado mediante MPLS, sino también a múltiples nubes mediante MPLS e Internet de bajo costo aprovechando SD-WAN.

¿El resultado? En cuanto las empresas pudieron experimentar la potencia y facilidad de las aplicaciones SaaS basadas en Internet (en lugar de las aplicaciones que residían en el centro de datos), ya no hubo marcha atrás.

Se podría pensar que esto habría conducido a un mundo utópico en el que todas las empresas fueran capaces de utilizar plenamente el poder de la nube a través de una red flexible y asequible, ¿verdad?

Bueno, así *habría sido*... pero el mundo volvió a cambiar.

El reto «de muchos a muchos»: SD-WAN en un importante punto de inflexión

Hoy en día, hemos entrado en una nueva era de empresa sin fronteras (consulta la figura 1-3), en la que usuarios, dispositivos, sitios y nubes están todos conectados de numerosas maneras. Tenemos una perspectiva remota y hemos traspasado las cuatro paredes de la oficina corporativa tradicional. El crecimiento de las microsucursales, la *multicloud*, el trabajo remoto, la telemedicina, la flota móvil y los activos del Internet de las cosas (IoT) son ejemplos de cómo se ha ampliado el perímetro de red de la empresa.

● Empresa sin fronteras

Interconexión de hogares, dispositivos, sucursales y nubes



FIGURA 1-3: En el entorno «de muchos a muchos», la empresa sin fronteras requiere una conectividad sencilla, flexible, segura y de alto rendimiento en cualquier lugar, desde todo tipo de sucursales, trabajadores remotos y dispositivos del IoT hasta centros de datos y *multicloud*.

Lo bueno de SD-WAN era que permitía a una empresa controlar el flujo de tráfico desde los usuarios de las sucursales hasta los destinos a los que querían conectarse. Pero todo el sistema estaba ligado a una serie de supuestos que empezaron a desmoronarse a medida que las múltiples

oleadas de innovación cambiaban el mundo. En los apartados siguientes, encontrarás una breve visión general de las tendencias clave que han reducido la eficacia de SD-WAN.

Aplicaciones y proliferación de los dispositivos del IoT

La SD-WAN tradicional era capaz de funcionar con algunos miles de aplicaciones, lo que era suficiente en sus inicios. Pero con la explosión del volumen de aplicaciones en la nube y dispositivos del IoT, sus capacidades se vieron cuestionadas. SD-WAN no se construyó para reconocer y categorizar estas nuevas aplicaciones y dispositivos basándose en un contexto enriquecido ni para establecer políticas razonables para ellos. Es imposible priorizar o asegurar lo que no se puede entender ni clasificarlo en categorías significativas.

La proliferación de dispositivos del IoT importa ahora más que nunca. Las arquitecturas de red actuales no están diseñadas para la convergencia del IoT, la tecnología operativa y la tecnología de la información. La falta de visibilidad detallada y control granular de los dispositivos del IoT plantea riesgos para la red. Para ello, se requiere una segmentación precisa basada en inteligencia artificial (IA) / aprendizaje automático (AA) que es distinta a la segmentación tradicional basada en el protocolo de Internet (IP).

Trabajo híbrido

Los trabajadores de hoy en día no están confinados en sucursales y no pueden ser protegidos por redes SD-WAN que fueron diseñadas pensando en los trabajadores de oficina. Ahora, cada usuario y cada dispositivo es una sucursal individual. Además, el número de personal que trabaja fuera de las sucursales, especialmente tras la pandemia de COVID-19, ha aumentado drásticamente a una escala para la que SD-WAN nunca había sido diseñada. Los trabajadores esperan y se merecen una experiencia de usuario segura y de alta calidad, comparable a la de la oficina central, independientemente de dónde estén trabajando.

Cuando se envió a los empleados a casa durante la pandemia, los arquitectos informáticos se centraron principalmente en asegurar la conectividad de acceso remoto. A menudo, se pensaba poco en la planificación de la arquitectura a largo plazo. Debido a ello, muchas empresas se esfuerzan ahora por gestionar múltiples soluciones de conectividad remota basadas en puntos, como redes privadas virtuales (VPN) de acceso remoto, servicio de seguridad perimetral (SSE), acceso Zero Trust (confianza cero) a la red (ZTNA), puerta de enlace web segura (SWG), agente de seguridad para el acceso a la nube (CASB), prevención de pérdida de datos (DLP) y dispositivos SD-WAN.

Conexión de los usuarios a varias nubes y conexión de las nubes en red

Establecer conexiones entre usuarios, dispositivos y sitios a una o varias nubes es una tarea complicada. A menudo, este proceso resulta enormemente fastidioso, ya que abarca aspectos como la seguridad, la velocidad y la eficiencia de la red que deben integrarse de forma inherente en lugar de añadirse de forma retroactiva. Esto hace necesaria la evolución progresiva del diseño arquitectónico. Los casos de uso incluyen, entre otros:

- » Permitir a los usuarios un acceso seguro y optimizado a aplicaciones locales o en la nube a través de un Internet poco fiable.
- » Permitir que las empresas faciliten una comunicación segura y basada en políticas entre aplicaciones a través de varias nubes.
- » Permitir a las sucursales distribuidas por todo el mundo acceder a aplicaciones a través de conexiones de red de «media milla» poco fiables.

El denominador común de estos casos de uso es la necesidad de una red dispersa de puntos de presencia (PoP) en la nube, estratégicamente situados para proporcionar seguridad y optimización en las proximidades de los usuarios, dispositivos, sitios y diversos entornos en la nube. Esta disposición estratégica garantiza una experiencia de usuario superior. Por ejemplo, un PoP situado en San Francisco no ofrecería una experiencia satisfactoria a los usuarios de Bangalore.

Inalámbrico primero (4G/5G)

Un entorno «de muchos a muchos» en el que las personas necesitan poder trabajar en cualquier lugar y en cualquier momento requiere más capacidad inalámbrica/celular integrada que la que ha proporcionado SD-WAN. Se necesita una conectividad rápida y fiable en cualquier lugar, ya sea un vehículo de campo en constante movimiento, un lugar de obras o un emplazamiento de exploración, sobre todo allí donde la banda ancha no está disponible o tarda mucho en instalarse. Por lo tanto, las conexiones inalámbricas son necesarias en distintas situaciones, y la ampliación de la compatibilidad con 4G/5G inalámbrica debe ser una prioridad, no algo que se plantee *a posteriori*.

Microsucursal

El significado de la palabra *sucursal* ha cambiado desde que se introdujo por primera vez. Al principio, las sucursales hacían referencia casi siempre a grandes conjuntos de usuarios. En nuestro mundo masivamente distribuido, una sucursal puede estar formada por cinco o diez personas

en una pequeña oficina, en un banco o en una obra. La SD-WAN tradicional es demasiado torpe y pesada para gestionar rápidamente un gran número de microsucursales.

Lo que se necesita es una pequeña puerta de enlace móvil «todo en uno» que integre SD-WAN, seguridad, procesamiento perimetral, sistemas celulares, punto de acceso y conmutación. Las microsucursales o sucursales deben admitir aplicaciones de procesamiento perimetral ligeras propias o creadas por socios para eliminar así la necesidad de servidores adicionales y reducir los gastos de capital en *hardware* (CapEx) y los gastos operativos (OpEx). Piensa en esto como si se tratara de una tienda de aplicaciones que te permite ejecutar tus propias aplicaciones personalizadas o una de las aplicaciones de un catálogo de socios.

Convergencia de la tecnología de la información y de la tecnología operativa (TI/TO)

La proliferación de los dispositivos del IoT, la construcción de dispositivos de fabricación inteligentes y los activos de alto valor han transformado por completo la sucursal del mundo sin fronteras. Ya no existe la situación en la que imaginamos a los humanos accediendo a las aplicaciones con una experiencia de usuario óptima habilitada por SD-WAN. La nueva sucursal está compuesta por activos de alto valor que necesitan acceder a las aplicaciones de forma similar. Estas máquinas podrían ser un cajero automático, una grúa, un robot en una fábrica o cualquier otro sensor del IoT que recopile datos que deben transportarse de forma eficaz y analizarse automáticamente mediante técnicas de IA para desbloquear el valor empresarial y predecir cualquier fallo.

La ejecución de operaciones eficientes requiere capacidades informáticas en el extremo de la red que alimenten cualquier aplicación ligera en contenedores, personalizada específicamente para un uso previsto. Por ejemplo, en un yacimiento petrolífero, un cable de fibra óptica solo informa de la temperatura en función de un umbral predefinido al servicio de análisis en la nube. Pensemos en una planta de fabricación inteligente con una máquina de control numérico por ordenador (CNC) que informa continuamente de los valores de comprobación del funcionamiento a una herramienta de inteligencia artificial capaz de anticiparse a un problema antes de que este se produzca. El personal de operaciones de red puede conectarse a distancia al dispositivo, solucionar cualquier problema y encargarse de cualquier mantenimiento predictivo, lo que ahorra los costos asociados a los desplazamientos en camiones. Estas capacidades innovadoras permiten la convergencia de las TI con la TO.

Limitaciones de la SD-WAN tradicional frente al mundo moderno

Hoy en día, las arquitecturas de red tradicionales van por detrás de los requisitos empresariales y suponen una sobrecarga para las empresas. La red empresarial nunca se diseñó para el panorama actual del trabajo remoto. Tenemos que replantearnos cómo creamos las redes modernas para que estas y la seguridad se integren estrechamente y ofrezcan seguridad desde la nube basada en los principios de Zero Trust. Estos principios establecen que, en lugar de asumir que todo lo que hay detrás del *firewall* corporativo es seguro, la seguridad debe basarse en el principio de «no confiar nunca, verificar siempre». Las actuales tecnologías de redes y seguridad son como ladrillos viejos en un moderno edificio de cristal: se han metido con calzador en las infraestructuras empresariales, perturbando el diseño en lugar de mejorarlo. Crean o simplemente no están hechos para superar los retos actuales. Y eso es un problema.

Todos los retos mencionados anteriormente ponen a prueba la SD-WAN. Al igual que la SD-WAN se desarrolló porque la WAN no podía gestionar un entorno basado en sucursales, ahora la SD-WAN ha alcanzado un importante punto de inflexión (algunos incluso dirían punto de ruptura) porque no puede gestionar un entorno «de muchos a muchos».

En los apartados siguientes se exponen las razones por las que la SD-WAN ha llegado a sus límites.

No se puede mejorar la red con parches

La SD-WAN no fue creada para el mundo moderno, y ninguna pequeña actualización cambiará eso. Imagina tener un dispositivo SD-WAN «voluminoso» para cada trabajador remoto, activo del IoT o aplicación perimetral. Es el equivalente a que todos los pasajeros de un vuelo intenten embarcar con una maleta anticuada de grandes dimensiones, demasiado grande y difícil de manejar si pensamos en los compartimentos superiores que existen hoy en día en los aviones. Es inviable. Tradicionalmente, los equipos de redes han abordado las necesidades empresariales emergentes añadiendo nuevas soluciones individuales y a medida. Antes, cada nueva idea obtenía una nueva caja negra; ahora, cada idea obtiene una nueva máquina virtual (MV). Todos encajan en este patrón: los dispositivos SD-WAN, las puertas de enlace celulares en las sucursales para obtener conectividad, los productos adicionales para obtener conectividad de aplicación a aplicación en la *multicloud* y los clientes VPN tradicionales. Este enfoque ha creado silos tecnológicos, contruidos con soluciones puntuales poco integradas y gestionadas por separado.

En última instancia, el departamento de TI debe proporcionar un rendimiento constante y una seguridad sólida para todos los recursos empresariales globales, y debe hacerlo de forma rentable para cada conexión. Se trata de un reto arquitectónico (y no de un problema funcional) que exige la eliminación de los silos informáticos y las «tiritas» de las soluciones puntuales para hacer frente a los nuevos requisitos empresariales. El paradigma de «añadir otra caja o máquina virtual» no será compatible con las nuevas formas de funcionamiento de las empresas.

La SD-WAN no puede ampliarse

La SD-WAN no puede ampliarse para responder ante el volumen de usuarios, aplicaciones y dispositivos. Las sucursales varían en tamaño; pueden estar formadas por pocas personas, cientos de personas o miles de personas. En el extremo superior de este rango, las soluciones SD-WAN deben ejecutarse en un gran clúster con equilibrio de carga para funcionar con eficacia. Imagina una empresa con decenas de miles de trabajadores remotos repartidos por todo el mundo, o un entorno de fabricación con más de 100 000 máquinas habilitadas para el IoT que hay que gestionar. En estos casos, la SD-WAN tiene dificultades para gestionar el enorme volumen de tráfico, la multitud de conexiones o la complejidad de las políticas y reglas de calidad de servicio que deben definirse y aplicarse.

La SD-WAN carece de funciones clave

Si nos fijamos en cómo funciona el mundo ahora, está claro que el punto de control ya no reside en el perímetro de una sucursal. La capacidad de definir y gestionar una red no puede vincularse a un perímetro físico. Y debemos saber mucho más sobre cada conexión para poder gestionar la red y la calidad de servicio.

La SD-WAN desconoce el contexto. No puede entender a qué aplicaciones intentan acceder los usuarios y los riesgos potenciales que pueden plantear, ni tampoco cuál es la gama de dispositivos en uso y hasta qué punto pueden verse comprometidos. Las empresas necesitan este conocimiento exhaustivo para tomar decisiones informadas sobre la priorización de aplicaciones. En la práctica, esto significa que se necesita un conjunto mucho más rico de información sobre usuarios, aplicaciones y dispositivos. Este conocimiento permite a los administradores establecer normas específicas no solo sobre usuarios y dispositivos concretos, sino también que permitan gestionar los riesgos en categorías más amplias utilizando los principios de Zero Trust.

En la SD-WAN tradicional, la seguridad estaba atornillada, no integrada. La SD-WAN tradicional permitía a las sucursales comunicarse directamente a través de Internet con varias nubes, abriendo una enorme

brecha de seguridad en el proceso. Algunas empresas optaron por la seguridad distribuida en cada sucursal, lo que resultaba difícil de gestionar y no se podía ampliar. Además, no permite que la seguridad siga a los usuarios y las aplicaciones móviles dondequiera que estén. Los proveedores de SD-WAN incluso han empezado a utilizar el término «seguridad suficientemente buena» para referirse a las sucursales. Una seguridad de red «suficientemente buena» no puede sustituir a la mejor seguridad de su clase que ofrece el servidor perimetral de acceso seguro (SASE), una arquitectura basada en la nube que ofrece servicios de red y seguridad destinados a proteger a los usuarios, las aplicaciones y los datos con independencia de su ubicación. El tiempo ha demostrado que la seguridad en la nube es el enfoque correcto. El SASE de un único proveedor permite contar con una arquitectura unificada con simplificación y uso compartido del contexto entre SD-WAN y la seguridad proporcionada por la nube. (Hablaremos de SASE con más detalle en el capítulo 5).

La SD-WAN no aprovecha la inteligencia artificial (IA) ni el aprendizaje automático (AA)

La SD-WAN tradicional no aprovechó el AA ni los análisis predictivos avanzados que podrían dar lugar a operaciones eficaces y automatizadas que pongan las cosas fáciles y hagan eficaces a los equipos de red que buscan resolver problemas antes de que ocurran y ofrecer una experiencia inigualable desde cualquier usuario a cualquier aplicación. Se espera que la SD-WAN moderna recopile todos los datos necesarios en toda la red —por usuario remoto, por sucursal y por carga de trabajo en la nube— y aproveche la IA y el AA para ofrecer información predictiva en toda la empresa que permita a los ingenieros de red garantizar un mayor rendimiento de la red mientras los usuarios finales obtienen una mayor productividad.

La SD-WAN no puede ofrecer una experiencia de calidad a más de 60 000 aplicaciones

Una implementación típica de SD-WAN puede haber comprendido las características de 3000 o 4000 aplicaciones, pero en el entorno actual, existen 60 000 aplicaciones o más. Conocer las características y lo críticas que son estas aplicaciones permite priorizar las soluciones que mejoran la experiencia del usuario. Por ejemplo, una persona que utiliza Zoom para sus negocios necesita una optimización, mientras que alguien que utiliza YouTube o aplicaciones de juegos desde el trabajo no necesita una optimización.

La SD-WAN no simplifica el uso del plano de control

La SD-WAN ha avanzado enormemente en la separación entre el plano de datos y el plano de control, pero dejar el plano de control como algo que debes hacer tú mismo a nivel local se ha quedado corto a la hora de facilitar su uso. Lo que las organizaciones deben buscar es un controlador que esté 100 % basado en SaaS y que tenga capacidad para admitir un enrutamiento avanzado, como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF). Las organizaciones también deben buscar la infraestructura que impulsa las capacidades de SSE y explorar si esto proporciona cobertura global y seguridad de pila completa en cada ubicación, amplia interconexión con proveedores de nube y la latencia más baja posible para que los clientes no tengan que elegir entre la eficacia de la seguridad y el rendimiento, un problema muy difícil de resolver. Una configuración con un solo clic de las capacidades de tipo SSE para una caja SD-WAN en una sucursal encuentra automáticamente el punto de presencia (PoP) más cercano.

La tecnología inalámbrica 4G/5G se pensó a posteriori

La ampliación de la compatibilidad con la tecnología inalámbrica 4G/5G no debe ser un planteamiento *a posteriori*. En lugar de eso, debe ser compatible de muchas formas distintas: como opción de transporte integrada en el dispositivo SD-WAN y como solución WAN inalámbrica que amplíe el alcance de la puerta de enlace de SD-WAN que se ejecuta en el armario. Las sucursales pueden necesitar acceso inalámbrico, pero también lo necesitarán los equipos móviles como los camiones o robots. La tecnología inalámbrica desempeña un papel diferente en cada uno de estos contextos.

La arquitectura no nació en la nube

La abrumadora complejidad de las redes en la nube lleva a las organizaciones a experimentar una inmensa frustración cuando se trata de conectar usuarios, dispositivos y sitios a la nube o a varias nubes. La arquitectura tiene que evolucionar para que la seguridad, la velocidad y la optimización de la red se integren y formen partes esenciales de la conectividad y no ser algo accesorio. Los casos de uso pueden ir desde un usuario que obtiene un acceso seguro y optimizado a aplicaciones locales o en la nube mediante un Internet poco fiable, hasta sucursales distribuidas por todo el mundo que intentan acceder con seguridad a aplicaciones mediante una conectividad poco fiable de «media milla» o en varias nubes que va de una aplicación a otra. Pero conectarse a la

nube también exige acercar el PoP de la red al usuario para garantizar el rendimiento y una experiencia de alta calidad.

La SD-WAN no es ampliable

Hoy en día, las redes se trasladan a la nube y el procesamiento se sitúa más cerca del perímetro. Al principio, muchos proveedores de SD-WAN empezaron a encadenar máquinas virtuales de SD-WAN con máquinas virtuales de seguridad de socios locales alojadas en un gran dispositivo. Sin embargo, muchas de estas funciones de seguridad y redes se han trasladado ahora a la nube. En consecuencia, cada vez es más necesario disponer de funciones de procesamiento ligeras más cerca de la fuente de datos. Piensa en un minorista que desea que un sistema de punto de venta esté disponible de manera ininterrumpida: Movería el sistema de punto de venta como una aplicación de procesamiento perimetral para mantener una alta disponibilidad o, en el mundo del IoT, ejecutaría Azure IoT Edge en el perímetro. Otros ejemplos pueden ser tus propias aplicaciones personalizadas.

La SD-WAN es rígida e irrelevante

El éxito de cualquier tecnología depende de su relevancia en el panorama tecnológico actual. Todo es cuestión de contexto. A pesar de sus puntos fuertes, la SD-WAN no admite las conexiones «de cualquiera a cualquiera» ni «de muchos a muchos» que necesitan las organizaciones de hoy en día. Tampoco se amplía bien, algo imprescindible para cualquier sector.



RECUERDA

La SD-WAN tuvo su día de gloria. Pero ahora se ha vuelto demasiado rígida e inflexible para apoyar la transformación en nuestro mundo hiperconectado. Se irá desvaneciendo y será superada por la próxima generación de tecnología. Así es cómo funciona el ciclo de la innovación.



ADVERTENCIA

En algún momento, la falta de una experiencia segura con las aplicaciones o de una seguridad, visibilidad o gestión de aplicaciones uniforme se convierte en una presa con grietas cada vez más grandes que puede terminar rompiéndose de forma catastrófica. Los usuarios y los dispositivos se encuentran atrapados en una avalancha de flujo descendente, incapaces de acceder a recursos remotos con el nivel adecuado de rendimiento o políticas de ciberseguridad. Entonces, ante esta avalancha de nuevos requisitos, ¿qué se supone que debe hacer un arquitecto informático para frenar la marea? Organizaciones de todas las formas y tamaños necesitan ahora una SD-WAN construida para el entorno «de muchos a muchos» o «de cualquiera a cualquiera». Afortunadamente, para los que nos interesa la tecnología, esa forma de SD-WAN ha llegado. Netskope lo denomina *SD-WAN sin fronteras*, (*Borderless SD-WAN*) y va más allá de lo que ofrece la SD-WAN tradicional.

EN ESTE CAPÍTULO

- » Tratamos de entender las ventajas de Borderless SD-WAN de Netskope
- » La seguridad en una red de área extensa definida por *software* (SD-WAN)
- » Respuesta a las necesidades de la microsucursal
- » Apoyo a los usuarios finales, estén donde estén
- » Cómo conseguir una conectividad rápida y fiable con 4G/5G
- » Aprovechamiento máximo de las capacidades del Internet de las cosas (IoT)
- » Vemos lo que Borderless SD-WAN puede hacer por ti

Capítulo 2

Una visión para las SD-WAN plenamente realizadas: el futuro sin fronteras

La SD-WAN triunfó como tecnología porque los usuarios de las sucursales necesitaban disponer de un soporte mucho mejor para enrutar su tráfico y calidad de servicio a través de una combinación de enlaces de Internet de bajo costo y conmutación por etiquetas multiprotocolo (MPLS). Pero, como se resume en el capítulo 1, el mundo siguió expandiéndose de una forma que la SD-WAN no estaba preparada para afrontar. Cada una de las áreas que mencionamos en el capítulo 1, la explosión de la movilidad, la proliferación de las aplicaciones

y dispositivos del IoT y las redes *multicloud*, debe contar con redes inalámbricas, procesamiento perimetral y seguridad proporcionada por la nube. Estos requisitos ponen a prueba la SD-WAN tradicional y los productos que han surgido para ayudarla.

En este capítulo, nos sumergimos en estos problemas con más detalle y abordaremos específicamente cómo Borderless SD-WAN de Netskope los va a solucionar.

Borderless SD-WAN: Redes para un mundo de muchos a muchos

Ahora mismo, cuando los usuarios o los dispositivos se encuentran a la deriva en el mar digital, interactuando con numerosas nubes y un vasto abanico de aplicaciones, pueden sentirse como marineros que navegan por la inmensidad sin brújula ni mapa: la protección y la optimización pueden ser tan esquivas como un faro en medio de una tormenta. Incluso cuando se les lanza un salvavidas, resulta ser una mezcla de soluciones que son una pesadilla de mantener unidas. Eso no es lo que quieren las organizaciones.

El objetivo de Borderless SD-WAN es permitir que cualquier persona o dispositivo disponga de una conectividad segura y optimizada desde cualquier lugar. Suena genial, ¿no? Pero, ¿cómo funciona? ¿Cómo puede hacerse realidad esta promesa?

Para explicar plenamente lo que es Borderless SD-WAN (consulta la figura 2-1), debemos explorar cómo seis situaciones actuales en la informática, las redes y la seguridad están acabando con la SD-WAN tradicional:

- » SD-WAN segura
- » Microsucursal
- » SD-WAN para *endpoint*
- » Puerta de enlace WAN inalámbrica
- » Acceso inteligente al IoT
- » Redes *multicloud*

A medida que avanzamos por cada una de ellas, explicamos qué se necesita en el mundo de muchos a muchos, por qué la SD-WAN y las soluciones actuales se quedan cortas y cómo ayudará con todo esto Borderless SD-WAN.

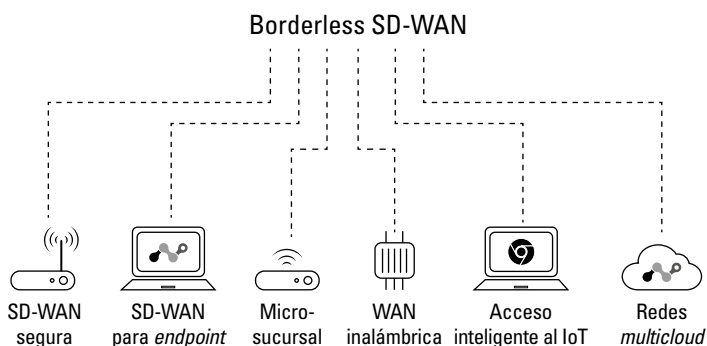


FIGURA 2-1: Borderless SD-WAN admite *software* en portátiles, puertas de enlace celulares y dispositivos de micro a grandes sucursales o centros de datos, y actúa como puerta de enlace virtual para redes *multicloud*.

SD-WAN seguras

La seguridad y las redes siempre han estado interrelacionadas. Como hemos comentado antes, los enlaces MPLS eran caros y estáticos, y carecían de visibilidad y control a nivel de aplicación. En respuesta al elevado costo de la MPLS, nació la SD-WAN. La SD-WAN optimizó la MPLS con enlaces a Internet de gran ancho de banda y bajo costo, lo que permitió a los usuarios de las sucursales conectarse directamente a aplicaciones distribuidas en las instalaciones y de *software* como servicio (SaaS). El objetivo de la SD-WAN era ofrecer el mismo nivel de rendimiento y seguridad a través de enlaces de banda ancha básicos, lo que se consiguió eficazmente con visibilidad y control de las aplicaciones. Esto permitía a los administradores definir políticas que garantizaran que Zoom tuviera mayor prioridad que Netflix.



RECUERDA

Nos encontramos en otro punto de inflexión en el que es hora de mirar más allá de la SD-WAN tradicional. El enorme volumen de aplicaciones en la nube y dispositivos del IoT se ha disparado, y las soluciones SD-WAN tradicionales con controles basados en políticas centradas en las aplicaciones no son suficientes, especialmente si la solución SD-WAN específica carece de los principios de Zero Trust.

La empresa en evolución necesita ahora una SD-WAN de Zero Trust y que sea consciente del contexto para proporcionar un acceso rápido, fiable y seguro a cualquier aplicación y dispositivo en cualquier ubicación con total visibilidad y el conjunto adecuado de controles. Esto es posible utilizando políticas contextuales que incluyan la comprensión de las aplicaciones, los riesgos de las aplicaciones, los usuarios, los riesgos de los usuarios, los dispositivos y los riesgos de los dispositivos, todo lo cual hace que las operaciones de red sean más inteligentes y seguras.

Las soluciones SD-WAN normalmente permitían a los administradores establecer políticas para unos pocos miles de aplicaciones, pero esto es ahora solo una fracción del número de aplicaciones que existen en la web y en la nube, que son más de varias decenas de miles. Si no sabes cuáles son las aplicaciones, ¿cómo puedes controlarlas? Algunas de estas aplicaciones pueden estar preparadas para la empresa, mientras que otras no. Asignar automáticamente prioridades de tráfico a todas las aplicaciones compatibles sigue siendo un gran reto. Los equipos de operaciones de red tienen que configurar estas aplicaciones manualmente de una en una. Ese proceso es extremadamente lento y propenso a errores, y no es escalable cuando se trata de decenas de miles de aplicaciones.

Una solución Borderless SD-WAN admite una base de datos de más de 60 000 aplicaciones. Los administradores de las tecnologías de la información (TI) no van a configurar las políticas de calidad del servicio para estas aplicaciones de una en una, por lo que es importante clasificar cada aplicación con un índice de confianza en la nube (CCI - Cloud Confidence Index). El CCI ofrece la puntuación de preparación para la empresa de una aplicación; esta puntuación se utiliza para producir valores predeterminados inteligentes listos para usar en la priorización del tráfico basada en la calidad del servicio. Esto elimina todo el trabajo manual del equipo de operaciones de red y da lugar a operaciones mucho más eficientes. (Por ejemplo, Zoom tiene un CCI de 82; está marcado con una prioridad alta por defecto. SureVoIP tiene un CCI de 38; se trata como prioridad baja desde el primer momento).

Las empresas aspiran a disponer de una supervisión continua de la salud de sus enlaces a las aplicaciones y de la flexibilidad necesaria para cambiar la aplicación de un enlace malo a otro bueno en una fracción de segundo. También buscan la reparación a la carta y la optimización del protocolo de control de transmisión (TCP).

La SD-WAN utilizaba una segmentación estática basada en direcciones/subredes del protocolo de Internet (IP). La seguridad se derivaba del conocimiento y control de la red. Esto funcionaba en el mundo de ayer. ¿Pero qué pasa con la microsegmentación de los dispositivos del IoT en el perímetro cuando se ven comprometidos y proporcionan una vía de acceso a la red de la empresa? La SD-WAN tradicional no proporciona visibilidad de los dispositivos del IoT, y debido a su proliferación, esto es cada vez más importante. Las capacidades que tienen en cuenta el contexto aprovechan la inteligencia artificial y el aprendizaje automático (IA/AA) para detectar automáticamente todos los dispositivos del IoT, gestionados y no gestionados, y microsegmentarlos para abordar los riesgos que pueden estar asociados a un dispositivo comprometido. Por ejemplo, un dispositivo del IoT como una cámara podría estar enviando un vídeo a una aplicación no autorizada. Esta cámara

puede bloquearse fácilmente mediante microsegmentación para reducir el radio de alcance si el dispositivo del IoT se ve comprometido, y puede remediarse fácilmente.

Borderless SD-WAN responde a estas necesidades porque recopila un conjunto mucho mayor de datos sobre usuarios, dispositivos, aplicaciones y redes. El contexto enriquecido permite aplicar políticas granulares de forma precisa.

Microsucursal

El término *microsucursal* hace referencia a una pequeña oficina, una cafetería o una tienda, que en la actual cultura del trabajo a distancia puede ser un lugar donde una persona está trabajando. En estas situaciones, puede que solo haya unos pocos usuarios o dispositivos; sin embargo, sus necesidades de conectividad, calidad de servicio y seguridad siguen siendo tan cruciales como lo serían en una oficina convencional. Necesitan una puerta de enlace fina que sea rentable y ofrezca conectividad y seguridad de calidad.

La WAN sin fronteras es compatible con el caso de uso de la microsucursal, proporcionando un *software* ligero que reside en una puerta de enlace compacta de servidor perimetral de acceso seguro (SASE), un dispositivo de *hardware* situado en una sucursal o en una microsucursal. En Borderless SD-WAN, convergen los servicios de red y de seguridad. Una puerta de enlace SASE consolidada es la forma más adecuada de ofrecer Borderless SD-WAN. Puede hacer converger capacidades como la conectividad celular, SD-WAN, Wi-Fi, seguridad y procesamiento perimetral de forma integral, todo operado desde una sola consola y gobernado por una sola política. La configuración ideal es la integración con un solo clic a través de una única consola con un servicio de seguridad perimetral (SSE) inteligente para proporcionar una seguridad completa. (Por cierto, el SASE de un único proveedor de Netskope ofrece precisamente esta combinación).



RECUERDA

Una Borderless SD-WAN distribuida significa poder ofrecer una experiencia de calidad de sucursal en cualquier ubicación, desde una pequeña oficina hasta el vehículo de una flota en un entorno hostil, como un campo petrolífero en Texas. Para ello, es necesario poder ofrecer varios servicios desde un único dispositivo en un formato fino y ligero. La mayoría de los proveedores de SD-WAN no pueden ofrecer esto; solo pueden proporcionar SD-WAN para sucursales tradicionales.

SD-WAN para endpoint

En el mundo actual, el acceso remoto seguro y de alto rendimiento se consigue a menudo a través de un dispositivo SD-WAN combinado con clientes de *software* de red privada virtual (VPN). Sin embargo, esta

configuración puede resultar incómoda para los usuarios remotos, que no disfrutaban de la misma experiencia de conectividad fluida que sus homólogos en la oficina. La doble dependencia de SD-WAN y VPN también significa que las empresas deben hacer malabarismos con múltiples proveedores, dispositivos y centros de costos, lo que hace que este enfoque no sea escalable.

Confiar únicamente en un cliente de *software* VPN sin un dispositivo SD-WAN conlleva muchos problemas. Las VPN, por ejemplo, adolecen de falta de visibilidad, conexiones estáticas de punto a punto, latencia al redirigir el tráfico e incapacidad para optimizar el tráfico de voz/vídeo. La incapacidad para reconocer quién accede a qué y desde dónde, combinada con variaciones inadvertidas en el rendimiento de la red, puede afectar directamente a la productividad de los usuarios.

Las VPN tradicionales están diseñadas para redirigir el tráfico a los concentradores de VPN, lo que supone una latencia añadida debida a la selección de una ruta subóptima. Las soluciones SD-WAN pueden superar algunos de estos problemas, pero dependen del *hardware* y carecen de la seguridad Zero Trust. No pueden adaptarse a las necesidades de cada usuario remoto.

Los trabajadores de hoy en día esperan seguridad Zero Trust y conectividad fiable, independientemente de su ubicación. Las organizaciones de TI, por su parte, necesitan simplicidad y mayor visibilidad para prestar un apoyo adecuado a los usuarios remotos. A pesar de su denominación «definida por *software*», la SD-WAN se basa en *hardware* especializado o servidores dedicados, principalmente ubicados en las sucursales.

Instalar SD-WAN en un ordenador portátil puede mejorar significativamente la experiencia del usuario, independientemente del lugar desde el que acceda a la red. Los operadores de red obtienen una visibilidad completa de todas las aplicaciones y enlaces que se están utilizando, lo que ayuda en la resolución de problemas. No importa dónde se encuentren los usuarios, aunque se trate de lugares con mala conexión a Internet, la SD-WAN instalada en un portátil mejorará la experiencia optimizando y creando políticas de calidad de servicio para priorizar el tráfico de aquellas aplicaciones sensibles a la latencia.

La naturaleza basada en *hardware* de la SD-WAN se vuelve problemática a medida que el volumen de conexiones de acceso remoto sigue creciendo. Pensemos en una gran compañía de seguros que tuvo que enviar dispositivos de SD-WAN físicos a más de 25 000 agentes de centros de atención al cliente remotos. Cuando aumentó la rotación de empleados, hubo más de 500 dispositivos al mes que no se devolvían, lo que provocaba riesgos de seguridad, mayores costos y quebraderos de cabeza

logísticos. Esta situación pone de manifiesto la necesidad de una solución como Borderless SD-WAN, que puede ejecutarse directamente en el portátil de un empleado.

En cuanto a las vías alternativas al acceso remoto, como los sistemas Zero Trust y el acceso Zero Trust a la red (ZTNA), también tienen sus inconvenientes. La mayoría de los clientes de Zero Trust/ZTNA no pueden ofrecer las ventajas de la optimización SD-WAN, y la mayoría de los proveedores de SD-WAN no ofrecen los elementos Zero Trust, además de necesitar el *hardware*. Una solución que unifique las capacidades de Zero Trust y las ventajas de optimización de las aplicaciones de SD-WAN en forma de *software* podría ofrecer lo mejor de ambos mundos sin necesidad de *hardware*. El moderno panorama laboral actual exige un cliente SASE unificado que esté basado en *software* al 100 % (consulta la figura 2-2).

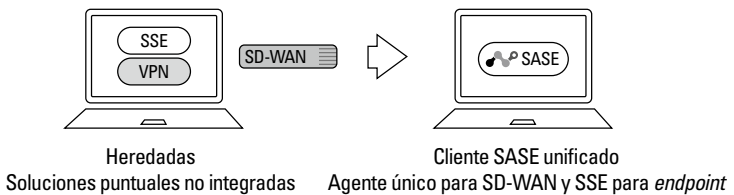


FIGURA 2-2: Borderless SD-WAN admite un cliente SASE unificado que aúna la optimización SD-WAN y la seguridad SSE para satisfacer las demandas de los trabajadores híbridos actuales.



RECUERDA

El acceso remoto solo es eficaz cuando proporciona una experiencia de usuario de alta calidad y seguridad Zero Trust en todos los lugares en los que trabaja el usuario. Algunas soluciones especializadas también pueden ofrecer esto, pero entonces el problema se convierte en tener que gestionar una plétora de productos en lugar de una única solución Borderless SD-WAN.

WAN inalámbrica

Para poder trabajar en cualquier lugar y en cualquier momento en un mundo de muchos a muchos, se necesita más de lo que una SD-WAN proporciona en el frente inalámbrico. Lo que se necesita es una conectividad rápida y fiable en todas las ubicaciones, ya sea en un vehículo de campo en continuo movimiento o en un punto de acceso empresarial fijo en una pared que proporcione una señal potente desde el interior de los armarios de TI.

La SD-WAN tradicional no puede hacer esto. Borderless SD-WAN sí puede. Desde la perspectiva del cliente, surgen dos escenarios o casos de uso.

El primer caso de uso implica a una organización que busca un dispositivo que consolide múltiples funciones, como SD-WAN, seguridad, procesamiento perimetral y puertas de enlace inalámbricas en un solo dispositivo todo en uno, aliviando los problemas que están asociados a la gestión de redes complejas y centros de costos. La puerta de enlace inalámbrica debe ser compatible con operadores de todo el mundo y ofrecer funciones de calidad de la experiencia para ajustar dinámicamente el ancho de banda de la aplicación y ahorrar costos en los ya de por sí caros enlaces celulares. Por ejemplo, puede ser aceptable tener Netflix como aplicación de prioridad media cuando se dispone de un enlace de banda ancha junto con el enlace celular, pero si el enlace de banda ancha falla, una política de calidad de servicio dinámica puede bloquear Netflix en los enlaces celulares.

El segundo caso de uso incorpora Borderless SD-WAN como dispositivo de puerta de enlace WAN inalámbrica. La puerta de enlace celular de Netskope puede montarse en una pared/techo y alimentarse mediante un cable de Ethernet (PoE). Proporciona una fuerte intensidad de señal a la puerta de enlace SASE de Borderless SD-WAN situada en el armario de TI. Esta configuración ayuda a las organizaciones a gestionar todos los dispositivos desde una única consola, evitando la necesidad de múltiples proveedores y consolas. Esta capacidad ahorra costos y ayuda a superar las limitaciones de las antenas externas, que pierden intensidad de señal en función de la distancia, lo que las hace casi inutilizables si la distancia entre el enrutador que se encuentra en el armario de TI y el tejado es demasiado grande.

Redes multicloud

La SD-WAN tradicional no gestiona correctamente las redes *multicloud* ni las operaciones automatizadas. Las empresas pueden acceder a docenas de nubes distintas, con cargas de trabajo distintas alojadas en cada una de ellas. Buscan una solución de red que proporcione una conectividad segura a todas estas nubes y, al mismo tiempo, permita una comunicación entre aplicaciones basada en políticas. Algunos proveedores nuevos ofrecen una solución de red en la nube que admite la visibilidad y el control de las conexiones entre nubes mediante un conjunto de políticas y la configuración automatizada de las conexiones. Estos proveedores de redes *multicloud* resuelven un problema importante: permiten a las empresas migrar sus cargas de trabajo a estas nubes desde un cuadro de mandos unificado que proporciona la información necesaria para una orquestación eficaz, lo cual está muy bien, dentro de sus limitaciones. Pero Borderless SD-WAN va más allá, proporcionando seguridad integrada y optimización para cada usuario, dispositivo, sitio y nube. Con Borderless SD-WAN, los clientes obtienen acceso a SSE con un solo clic, lo que garantiza la seguridad completa de cualquier nube.

Imagínate miles de servidores repartidos en varias nubes, que necesitan obtener actualizaciones de Internet. Dado que los servidores están expuestos a ciberamenazas, ¿cómo se puede garantizar su protección? Borderless SD-WAN utiliza un contexto enriquecido y su capacidad de integración con sistemas de automatización de la nube, como Terraform, para aplicar políticas que controlan la conectividad entre nubes, la optimización de la red y la seguridad. Esta red *multicloud* se gestiona desde una única consola unificada, que puede crear fácilmente instancias del *software* ligero de Borderless SD-WAN en todas las nubes. Desde esta única consola unificada, las operaciones automatizadas en la nube permiten la interoperabilidad de estas instancias del *software* de Borderless SD-WAN y que estas intercambien rutas con los principales proveedores en la nube, como Amazon Web Services (AWS) Transit Gateway, Azure Virtual Router y el enrutador de nube Cloud Router de Google Cloud Platform (GCP). Con el acceso de un solo clic a Netskope Intelligent SSE, las empresas también disponen de seguridad integrada de pila completa para protegerse de todos los ciberataques.

Borderless SD-WAN también amplía la WAN empresarial, lo que permite a los usuarios conectarse a varias nubes e integrar la infraestructura de nube pública en el tejido de Borderless SD-WAN. Esto permite a las aplicaciones que se ejecutan en dispositivos de usuarios consumir servicios prestados en la nube, como la infraestructura como servicio (IaaS), de forma segura y con un alto rendimiento.

El resultado: Borderless SD-WAN hace converger las redes y la seguridad de manera uniforme en todos los perímetros.



CONSEJO

Con la seguridad y la optimización integradas, las empresas pueden establecer políticas de manera uniforme en toda la red, abarcando todos los dispositivos y todos los usuarios en todas las nubes. Esto significa que las políticas serán coherentes independientemente de la nube a la que acceda el usuario. Lo que está optimizado, permitido y restringido no cambiará aunque cambie la nube en uso. Las nubes no solo pueden comunicarse entre sí (AWS necesita comunicarse con GCP, que a su vez necesita comunicarse con Azure, etc.), sino que las conexiones pueden enrutarse de forma segura a través de entornos *multicloud*. Así es como hay que hacer las redes *multicloud* en estos tiempos para seguir las mejores prácticas.

Acceso inteligente al IoT

Las empresas actuales necesitan un acceso inteligente al IoT desde su SD-WAN. Las organizaciones quieren que sus activos habilitados para el IoT y la tecnología operativa se conecten a la nube para que el procesamiento perimetral pueda ejecutarse en estos activos, reenviando a la nube solo los datos necesarios para analizar un problema y determinar

proactivamente una solución. También deben ser capaces de aprovechar las capacidades del IoT para la supervisión remota, la resolución de problemas, la recopilación de datos y el mantenimiento predictivo, al tiempo que reducen los desplazamientos innecesarios en camiones, es decir, las llamadas de servicio en persona que aumentan los gastos de mano de obra y gasolina, entre otros. Sin estas características, conseguir el retorno de la inversión (ROI) deseado de su ecosistema de activos del IoT será todo un reto.

El objetivo es proporcionar a un activo del IoT conectividad segura y de alta calidad con procesamiento perimetral e inalámbrico.

Por ejemplo, para una máquina de control numérico por ordenador (CNC) de una fábrica, los dispositivos Borderless SD-WAN reforzados no solo proporcionan Wi-Fi a los sensores, sino que también admiten capacidades de procesamiento perimetral para recopilar información, como los datos de temperatura y la vibración de los sensores. También recopilan selectivamente datos útiles en función de umbrales predefinidos, ofreciendo así una mayor eficacia operativa a un costo drásticamente reducido.

La puerta de enlace SASE de Netskope admite el aprovisionamiento sin intervención y el procesamiento perimetral integrado, lo que acerca el procesamiento a la fuente de datos. Puede recopilar y extraer datos de sensores del IoT y enviar a la nube del IoT solo los datos que superen umbrales preestablecidos, utilizando conexiones celulares u otros medios de transporte preferidos. Gracias a una gestión del ciclo de vida de las aplicaciones (ALM) escalable, ofrece servicios de contenedor listos para usar, como el tiempo de ejecución de Azure IoT Edge, así como la capacidad de ejecutar otros servicios de un catálogo de servicios para dispositivos móviles. Los clientes también pueden ejecutar sus propias aplicaciones personalizadas. La puerta de enlace SASE de Netskope, con su kit de desarrollo de *software* (SDK) y sus interfaces de programación de aplicaciones (API) de fácil uso para los desarrolladores, ofrece opciones y flexibilidad y permite a las empresas incluir sus propias aplicaciones.

Para proporcionar asistencia del día 2 y mantenimiento continuo, la puerta de enlace de Borderless SD-WAN permite el acceso desde el exterior a través de un gestor del IoT integrado de forma nativa a activos de alto valor, lo que acelera el tiempo de resolución de incidentes. Esta función evita los desplazamientos físicos a las instalaciones, ya que permite al informático solucionar problemas y establecer un diagnóstico a distancia. Al anticiparse a los fallos de un dispositivo, pueden enviar rápidamente la pieza adecuada para solucionar el problema, evitando o minimizando las interrupciones de la actividad.

Qué cabe esperar de estas nuevas funciones

Las empresas deberían tener las expectativas muy altas sobre las nuevas capacidades que Borderless SD-WAN puede proporcionarles. He aquí una lista de lo que Borderless SD-WAN debe hacer para garantizar la seguridad y el rendimiento, incluidos los elementos que ya hemos tratado y algunos elementos adicionales:

- » **Proporcionar visibilidad para tener en cuenta el contexto.** Controlar, priorizar o defender lo que no se ve es imposible. Una solución Borderless SD-WAN debe ofrecer la máxima visibilidad posible sobre usuarios, dispositivos, aplicaciones y redes en todo el flujo de tráfico. Cuando sea posible, esta información debe controlarse y actualizarse en tiempo real.
- » **Proporcionar acceso y enrutamiento inteligentes que eliminen la complejidad en la administración.** Busca una solución que permita configurar con un solo clic las capacidades de SSE y SD-WAN para un dispositivo SD-WAN en una sucursal, para los usuarios remotos, dispositivos del IoT y entornos *multicloud*. Esta solución debería localizar automáticamente el punto de presencia (PoP) más cercano. Además, busca un controlador de nube escalable que tenga capacidad para ofrecer interoperabilidad con enrutamiento avanzado, como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF).
- » **Ofrecer seguridad en la nube basada en los principios de Zero Trust.** Hoy en día, la seguridad debe seguir a la conectividad allá donde vaya y reaccionar en tiempo real a las condiciones cambiantes. Los sistemas SD-WAN tradicionales empezaron a abordar este problema con *firewalls* integrados, pero esto no permite a la seguridad seguir a los usuarios y aplicaciones móviles dondequiera que estén. Una solución Borderless SD-WAN que esté estrechamente integrada en SSE inteligente, ofrece SASE de un único proveedor. Permite contar con una arquitectura unificada con seguridad de red híbrida, lo que ofrece seguridad local como *firewall* este-oeste, sistema de prevención de intrusiones/sistema de detección de intrusiones (IPS/IDS) y segmentación en la sucursal, además de protección de 360 grados con seguridad en la nube.
- » **Ofrecer operaciones escalables basadas en IA.** Borderless SD-WAN aprovecha las operaciones basadas en IA para supervisar la red a todos los niveles, incluida la actividad a nivel de usuarios, sucursales y nubes, para permitir la resolución proactiva de problemas y el análisis exhaustivo. La identificación temprana de anomalías y señales de advertencia mediante IA y AA ayuda a reducir el número de

incidencias de soporte técnico y el tiempo medio hasta la resolución, lo que a su vez permite a los clientes ejecutar redes a gran escala. La IA y el AA también ayudan a rectificar automáticamente cualquier estado incorrecto de la red para ofrecer el máximo rendimiento de la misma.

- » **Proporcionar una experiencia de aplicación y una seguridad garantizadas para decenas de miles de aplicaciones y dispositivos del IoT.** Una implementación típica de SD-WAN puede comprender las características de 3000 o 4000 aplicaciones, pero la explosión de aplicaciones en la nube y el IoT exigen una solución Borderless SD-WAN que pueda detectar y priorizar automáticamente 60 000 o más aplicaciones y microsegmentar automáticamente dispositivos del IoT que puedan ser un riesgo.
- » **Ofrecer una mayor compatibilidad con la tecnología inalámbrica 4G/5G que no sea una opción añadida posteriormente y que sea compatible de muchas formas diferentes.** Con Borderless SD-WAN, los usuarios pueden acceder a las redes 4G y 5G de forma segura allí donde no se disponga de conexión de banda ancha o se tarde mucho en establecerla. Esta capacidad es crucial no solo para las sucursales, sino también para las flotas móviles, máquinas y robots.
- » **Proporcionar una rampa de acceso a la nube que aúne nube, red y seguridad.** Las organizaciones experimentan una inmensa frustración cuando se trata de conectar usuarios, dispositivos y sitios a la nube o a varias nubes, debido a la abrumadora complejidad de las redes en la nube. La arquitectura debe evolucionar para que la seguridad, la velocidad y la optimización de la red formen parte integrante de la conectividad, en lugar de ser un planteamiento *a posteriori*. Para ofrecer una solución Borderless SD-WAN y seguridad integrada, la conectividad de alta calidad debe estar cerca de los usuarios y dispositivos, estén donde estén. Una nube global con PoP en todas partes permite que la funcionalidad se ejecute en el perímetro y ofrezca conectividad y rendimiento de alta calidad para la rampa de acceso a la nube.
- » **Provisión de aplicaciones de procesamiento perimetral para habilitar nuevos servicios.** Cada vez se despliegan más aplicaciones en contenedores en el perímetro de la red. Este cambio crea importantes retos de gestión de las aplicaciones a los que el diseño de las arquitecturas SD-WAN actuales no puede hacer frente. Como ejemplo, piensa en un administrador de TI que quiere ejecutar una aplicación de supervisión de la experiencia digital de su elección en una sucursal.

- » Comprender la importancia de la arquitectura que da prioridad a la nube
- » Creación de planos de gestión, control y datos más sofisticados
- » Uso del aprendizaje automático y la inteligencia artificial para supervisar las redes en tiempo real

Capítulo 3

Cómo funciona Borderless SD-WAN

Hay un viejo dicho en el mundo de la tecnología, atribuido a Thomas Edison, que dice que la visión sin ejecución es una alucinación. O como dirían en Texas, si no se pasa a la acción, lo que hay es «mucho ruido y pocas nueces». Pues bien, la versión de Netskope de la red de área extensa definida por *software* (SD-WAN) sin fronteras se ha diseñado de arriba abajo para ofrecer una gran experiencia a las personas que utilizan la tecnología y a las que la configuran, ejecutan, optimizan y depuran. En otras palabras, Netskope pasa a la acción. No se queda en el ruido.

Con Borderless SD-WAN de Netskope, la ejecución tiene que abrir nuevos caminos, porque la tecnología amplía tanto el ámbito como el alcance de la SD-WAN tradicional y ha creado un conjunto de requisitos que rompen la arquitectura y las funciones administrativas utilizadas en la SD-WAN. En consecuencia, la arquitectura de la red también debe cambiar para permitir que los usuarios que trabajan desde cualquier parte del mundo tengan una experiencia agradable.

El gran alcance de los servicios que se prestan a una enorme población de usuarios, sucursales, dispositivos del Internet de las cosas (IoT) y la nube exige un cambio en el funcionamiento de los planos de gestión,

control y datos. Las antiguas configuraciones que se creaban solo para las sucursales se sustituyen por políticas que expresan el resultado deseado basándose en un contexto enriquecido sobre el usuario, el dispositivo, la aplicación, los datos y la red. Por estas razones, Borderless SD-WAN funciona de una forma completamente nueva, utilizando una arquitectura nativa de la nube. En este capítulo se examina lo que esto significa en la práctica.

Por qué Borderless SD-WAN debe tener una arquitectura que da prioridad a la nube

El mundo de muchos a muchos en el que vivimos hoy en día ha cambiado radicalmente el número de usuarios, dispositivos, sitios y nubes que necesitan una conectividad segura y optimizada con Borderless SD-WAN. Por ejemplo, si una empresa traslada a miles de trabajadores de centros de atención al cliente a un modelo de trabajo desde casa, la función SD-WAN debe ampliarse de forma masiva. Para prestar un servicio de alta calidad a todo este personal, es necesario contar con un punto de presencia (PoP) fiable cerca de cada persona. La única forma de conseguirlo pasa por trasladar la implementación a la nube y adoptar una nueva estrategia de conectividad. Eso es exactamente lo que hace Borderless SD-WAN.

Muchos proveedores afirman ofrecer la arquitectura nativa en la nube de Borderless SD-WAN, pero pocos lo hacen realmente. Los proveedores afirmarán: «Nuestro plano de gestión, plano de control y plano de datos se entregan en la nube». Pero, en realidad, ejecutan el *software* como servidores de respaldo activo en la nube. El problema de esta estrategia es que, cada vez que te quedas sin capacidad, los proveedores tienen que poner en marcha continuamente los servidores de reserva activos en la nube para atender las distintas necesidades de los clientes. Con tantos dispositivos, sitios y usuarios que conectar, esta arquitectura y este planteamiento no son ampliables. El mero hecho de trasladar una implementación de *software* para que se ejecute en la nube no significa que el sistema aproveche el potencial de ampliación de la tecnología de la nube.

Para aprovechar las ventajas de la nube, Borderless SD-WAN utiliza contenedores de *software* y microservicios, cada uno de los cuales puede ampliarse por separado utilizando los recursos flexibles que ofrece la nube. Esta arquitectura permite a Borderless SD-WAN implementar y gestionar miles de sitios, dispositivos del IoT y terminales de usuarios.



CUESTIONES
TÉCNICAS

Más concretamente, Borderless SD-WAN de Netskope funciona sobre una plataforma en la nube distribuida altamente redundante, con múltiples capas de redundancia, instantáneas de copia de seguridad y conmutación por error automática. Todos los componentes de la arquitectura Borderless SD-WAN se implementan en un clúster redundante y tolerante a fallos, con servicios de configuración activa-activa, lo que facilita el equilibrio de carga además de una alta disponibilidad.

Esto permite a Borderless SD-WAN no solo garantizar un elevado tiempo de actividad de forma independiente, sino también ampliar automáticamente cada servicio. Cada servicio se implementa detrás de un clúster de equilibradores de carga configurados para ofrecer alta disponibilidad, y la carga de cada uno de esos grupos se supervisa utilizando diversas métricas.

Si las máquinas de un grupo están sobrecargadas, se añaden máquinas adicionales para distribuir la carga. Los servicios de Borderless SD-WAN también están diseñados para no tener estado y, por lo tanto, pueden ampliarse con flexibilidad a través de instancias de servidor dentro de cada centro de datos y entre centros de datos, sin tiempo de inactividad ni impacto en el rendimiento.

Reconfiguración de los planos de gestión, control y datos

La arquitectura de Borderless SD-WAN permite que los planos de gestión, control y datos sean mucho más inteligentes y sofisticados. En este apartado, describimos los nuevos enfoques de cada plano y sus nuevas capacidades.

El plano de gestión

El *plano de gestión* en SD-WAN surgió de un servicio central, que normalmente se encontraba en una máquina virtual (MV) en un centro de datos o posiblemente en la nube. La tarea principal del plano de gestión consistía en administrar los dispositivos de las sucursales de SD-WAN en toda la red y garantizar que estuvieran actualizados, aprovisionados y controlados para que el *software* de SD-WAN funcionara correctamente en el *hardware* de la empresa. Eso funcionó hasta que dejó de hacerlo, cuando surgieron nuevos retos.

Ahora, las empresas deben dar cuenta de una gran cantidad de dispositivos del IoT y personales, así como de ordenadores portátiles que se conectan a la red y a entornos *multicloud*. Borderless SD-WAN tiene que

gestionar toda esta diversidad de casos de uso, así como todos los datos que generen y la configuración de las aplicaciones. Por eso, en Borderless SD-WAN, el plano de gestión ha sufrido una transformación radical. Es nativo de la nube, altamente redundante, multiusuario y fácil de usar, con una interfaz intuitiva basada en la web. Esta evolución fue fundamental, porque Borderless SD-WAN tiene que desempeñar varias funciones vitales:

- » **Gestión de *software* en casos de uso distribuidos:** El alto rendimiento y la conectividad segura deben ampliarse a todos los usuarios, dispositivos, sucursales y entornos *multicloud*. Borderless SD-WAN debe gestionar el *software* en estos casos de uso distribuidos, una tarea mucho mayor que la gestión del *software* en el menor número de cajas SD-WAN que las empresas tenían anteriormente.
- » **Gestión de datos y telemetría:** Debe gestionar todos los datos y la telemetría que recibe la red. Esto solo puede ocurrir con la escalabilidad que proporciona Borderless SD-WAN.
- » **Gestión del nuevo modelo de trabajo remoto:** Debe ser capaz de gestionar el nuevo modelo de trabajo remoto a escala, cuando las organizaciones ya no tratan de gestionar 400 oficinas remotas, sino que intentan gestionar y consumir a distancia los datos de miles de usuarios remotos de forma eficiente y segura.



CONSEJO

Con Borderless SD-WAN, las empresas obtienen una configuración y visibilidad completas de todos sus dispositivos de red a través del plano de gestión. El plano de gestión de Borderless SD-WAN también puede suministrar información sobre el estado de las aplicaciones, así como actualizaciones de *software* automatizadas y seguras a todos los dispositivos de la red al mismo tiempo. Los productos SD-WAN tradicionales no pueden ofrecer una visión de la gestión tan completa de toda la red de una empresa y de todos sus dispositivos.

El plano de control

El *plano de control* hace referencia a la forma en que las empresas pueden construir y controlar la topología de la red; así es como una sucursal descubre otra sucursal. En la SD-WAN del pasado, este plano de control funcionaba normalmente en un dispositivo de *hardware* físico en el que también residía el plano de datos de la SD-WAN. Si el plano de datos fallaba, el plano de control fallaba con él, sin ofrecer ningún tipo de resiliencia. En otras situaciones, cuando el plano de control se quedaba sin capacidad de proximidad (para los gurús técnicos, si el plano de

control utiliza Border Gateway Protocol [BGP], es el BGP el que se queda sin capacidad de proximidad), era necesario instalar más dispositivos SD-WAN porque el plano de control y el plano de datos se ejecutaban en el mismo enrutador/*hardware*. Además, el plano de control de SD-WAN simplemente no estaba diseñado para manejar el enorme volumen de usuarios, dispositivos, sucursales y entornos *multicloud* que tendría que gestionar.

Con Borderless SD-WAN, el plano de control se traslada a la nube y se entrega mediante *software* como servicio (SaaS). Interactúa con un plano de control local como BGP y Open Shortest Path First (OSPF). Como resultado, un controlador ya no reside físicamente en el entorno local de una empresa. Es un servicio que utilizan las organizaciones, al igual que Salesforce, Workday o cualquier otro SaaS. La principal razón por la que esto era necesario es que, al hacer que el plano de control funcione como SaaS, Borderless SD-WAN tiene ahora la capacidad de ampliarse en función de la demanda. Otra ventaja es que las empresas ya no tienen que preocuparse de añadir más *hardware* para aumentar la capacidad del plano de control con el fin de añadir nuevas sucursales debido a su crecimiento.



CONSEJO

Este traslado del plano de control a la nube permite a Borderless SD-WAN gestionar la topología de una red de forma más detallada y sofisticada que antes. Esto es necesario a medida que las redes se amplían y hay que gestionar cada vez más dispositivos personales y del IoT, así como conexiones a puertos de enlace inalámbricas.

Borderless SD-WAN traslada los controladores completamente a la nube, ofreciendo niveles de control, simplicidad y ampliación que simplemente no eran posibles con SD-WAN.

El plano de datos

Con un controlador totalmente basado en SaaS que proporciona visibilidad de toda la red y de todos los dispositivos conectados a ella, las empresas obtienen una visión sin precedentes de los datos que circulan por su red y eliminan los complejos controladores locales «de andar por casa».

El *plano de datos* también ha cambiado significativamente bajo el paradigma de Borderless SD-WAN. La MPLS consistía en el enrutamiento de paquetes; la SD-WAN tradicional supuso un gran paso hacia adelante al tomar decisiones y políticas de enrutamiento basadas en aplicaciones sin tener en cuenta ningún contexto asociado a las aplicaciones, los usuarios y los dispositivos. En otras palabras, la SD-WAN tradicional no

dejaba lugar para las políticas basadas en los riesgos de las aplicaciones, riesgos entre usuarios o riesgos entre dispositivos. La seguridad se incorporó a SD-WAN, como se muestra en la figura 3-1, y era o «suficientemente buena» o estaba poco integrada, lo que la hacía compleja desde el punto de vista operativo e incapaz de compartir el contexto entre la red y la seguridad.

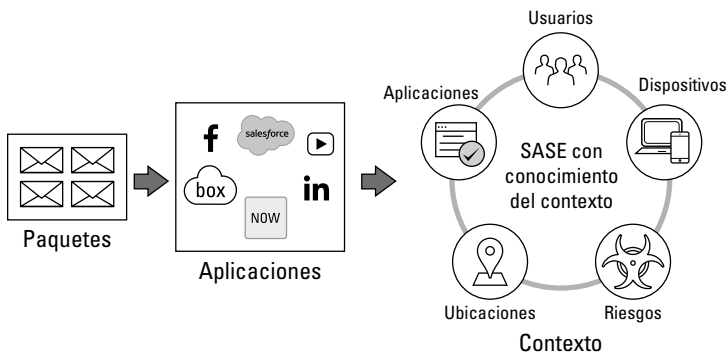


FIGURA 3-1: Las políticas contextuales de Borderless SD-WAN incluyen la comprensión de las aplicaciones y sus riesgos, los usuarios y sus riesgos, los dispositivos y sus riesgos, todo lo que hace que las operaciones de red sean inteligentes y seguras.

En el entorno actual, que también se muestra en la figura 3-1, las empresas necesitan establecer políticas coherentes en torno al rendimiento de las aplicaciones, el acceso Zero Trust y la seguridad para cada usuario remoto, sitio, dispositivo y nube. Borderless SD-WAN lleva estas capacidades a niveles completamente nuevos:

»» **Un solo clic al servicio de la seguridad perimetral (SSE) automatiza la conectividad desde Borderless SD-WAN a SSE.**

Además, facilita el consumo del servicio sin necesidad de crear configuraciones de enrutamiento del tráfico ni de utilizar archivos de configuración automática de proxy (PAC).

»» **Borderless SD-WAN amplía el contexto sobre el usuario, el dispositivo, los datos y la aplicación, lo que permite definir y aplicar políticas mucho más eficaces y sofisticadas.** Al calificar las soluciones para tomar decisiones de seguridad y enrutamiento del tráfico dentro de contextos relevantes en la nube, es posible gestionar mejor el riesgo de los usuarios y detectar y abordar el riesgo de los dispositivos con políticas segmentadas en tiempo real. Imagina detectar y priorizar y optimizar automáticamente

más de 60 000 aplicaciones o detectar el riesgo de los dispositivos del IoT basándose en la inteligencia artificial (IA) y el aprendizaje automático (AA).

» **Borderless SD-WAN también mantiene a los usuarios, sitios, dispositivos y entornos *multicloud* remotos cerca de una red global de PoP.** Borderless SD-WAN combinada con SSE se interpone entre los usuarios y las aplicaciones en estos PoP. Así es como pone en práctica su magia y proporciona los servicios necesarios para aplicar políticas y mejorar la calidad del servicio con seguridad integrada. Pero para que esto funcione, la conexión de red y los servicios de Borderless SD-WAN deben estar cerca del usuario en términos de red. Si toda la funcionalidad de Borderless SD-WAN y SSE se encuentra en un centro de datos de Seattle, y los usuarios o sucursales están en Bombay o Berlín, la experiencia será lenta e incoherente.

Por este motivo, Netskope creó una red global de PoP en todo el mundo llamada NewEdge.

NewEdge de Netskope es una nube privada creada específicamente que combina servicios de red y seguridad a gran escala, proporcionando rampas de entrada de baja latencia al tráfico en más de 70 regiones de todo el mundo. La red NewEdge permite una integración sin fisuras de los servicios de Borderless SD-WAN y SSE, y garantiza que los usuarios, sucursales, sitios, dispositivos y entornos *multicloud* a nivel global tengan muy cerca estos servicios convergentes. SSE en NewEdge ofrece varios servicios, como puerta de enlace web segura de nueva generación (NG-SWG), agente de seguridad para el acceso a la nube (CASB), acceso Zero Trust (confianza cero) a la red (ZTNA), gestión de la postura de seguridad SaaS (SSPM), gestión de la postura de seguridad en la nube (CSPM), *firewall* como servicio (FWaaS) y prevención de pérdida de datos (DLP). Borderless SD-WAN en NewEdge proporciona una vía optimizada para aplicaciones SaaS y servicios de «media milla» en la nube. En general, NewEdge con SSE y Borderless SD-WAN garantizan una conectividad segura y de alto rendimiento para aplicaciones en la nube, web, SaaS y privadas.

Espacio para la inteligencia artificial

En los planos de gestión de Borderless SD-WAN, se pueden implementar más operaciones basadas en IA en comparación con la SD-WAN tradicional. Las empresas consiguen una visión completa de su red, y la IA puede supervisar en tiempo real cómo tendría que ser un enlace

adecuado y seguro para los dispositivos externos que se conectan a la red. La IA puede identificar un enlace defectuoso, y también puede utilizar datos históricos y el contexto para predecir cuándo puede fallar un enlace. El AA y la IA también pueden proporcionar una solución automatizada cuando surge este tipo de problemas, como las correcciones de errores hacia adelante o *corrección automatizada de enlaces* (una corrección que permite cambiar automáticamente a los usuarios a un enlace mejor, actualmente disponible, para obtener una conexión más fiable). El AA y la IA también pueden detectar automáticamente los dispositivos del IoT y su comportamiento y poner en cuarentena los dispositivos problemáticos.

Asimismo, Borderless SD-WAN incluye valiosos análisis de flujo sobre el rendimiento de las aplicaciones en toda la red. En estos flujos, las empresas pueden ver cada dispositivo que está utilizando una aplicación concreta y el funcionamiento de ese dispositivo. Con estos datos, se pueden establecer referencias automáticamente. Básicamente, define lo que es un rendimiento «normal» de la red en cuanto a pérdida de paquetes o estadísticas de flujo de las aplicaciones. Las referencias también deben tener en cuenta la hora y la actividad de la red, ya que esta varía en función del horario laboral normal de las distintas sucursales y usuarios remotos.

Borderless SD-WAN también incluye una vista de rastreador de paquetes específicos integrada que supervisa cada usuario y sucursal, durante cada minuto. De este modo, busca problemas de funcionamiento en el nivel de servicio y señala las infracciones de los acuerdos de nivel de servicio (SLA) de los proveedores de servicios. El rastreador de paquetes simplifica la gestión con información sobre los flujos de tráfico (incluido dónde se produce el fallo), señala las infracciones de las políticas y realiza la detección de anomalías.

Además, Borderless SD-WAN va más allá de la información procesable sobre fallos basada en AA para solucionar realmente los problemas de los dispositivos de una sucursal. Por ejemplo, las funciones de detección automática pueden identificar los dispositivos reales que acceden a las aplicaciones desde el interior de la sucursal o el domicilio. El departamento de TI remoto puede utilizar el gestor del IoT integrado para solucionar a distancia los problemas de estos dispositivos, lo que reduce de manera considerable el tiempo medio de resolución.

- » Ventajas empresariales de Borderless SD-WAN
- » Exploramos las ventajas para el usuario final
- » Analizamos las ventajas para los expertos en redes
- » Cómo ahorrar dinero con Borderless SD-WAN

Capítulo 4

Ventajas de Borderless SD-WAN para las empresas

Borderless SD-WAN de Netskope ofrece un conjunto de funciones relacionadas con la red que responden a las necesidades del mundo actual. Es una red de área extensa definida por *software* (SD-WAN) creada para satisfacer las necesidades actuales de movilidad, flexibilidad, seguridad integrada y disponibilidad constante desde cualquier lugar, en cualquier momento y con cualquier dispositivo. Del mismo modo que la SD-WAN llevó la WAN al mundo de uno a muchos, Borderless SD-WAN hace evolucionar la red hacia la era de muchos a muchos.

Las ventajas de esta transformación no solo están al alcance de los expertos en redes. Son tangibles y se experimentan a diario en toda la empresa. Si eso no hace feliz al friki de las redes que llevas dentro, no sabemos qué puede hacerlo.

En este capítulo hablaremos de estas ventajas diarias para todos los usuarios, así como de algunas de las ventajas más avanzadas para los expertos en redes encargados de mantener la tecnología y la

infraestructura de red. Después de leer este capítulo, comprenderás que Borderless SD-WAN no es solo un conjunto de funciones para la red, sino que también proporciona conectividad de alto rendimiento e integra perfectamente la seguridad. Esto la convierte en una función esencial para las empresas, ya que ofrece la misma experiencia a todos los usuarios, independientemente del lugar al que quieran ir.

Un enfoque de una sola plataforma, un solo software y una sola política

Antes de continuar, analicemos el cambio filosófico más amplio que Borderless SD-WAN supone para la empresa. Este contexto ayudará a perfilar el resto del análisis que abordaremos en este capítulo. Hay un viejo dicho de innumerables programas de televisión que dice que cada persona necesita un código, una filosofía personal por la que regirse (esto parece ser así en todas las representaciones de bandas criminales y clanes nobles de alienígenas espaciales). Lo mismo ocurre con la conectividad. El mantra de Borderless SD-WAN gira en torno al «poder de solo uno» (consulta la figura 4-1) y al modo en que este enfoque ayuda a las organizaciones a agilizar las operaciones.

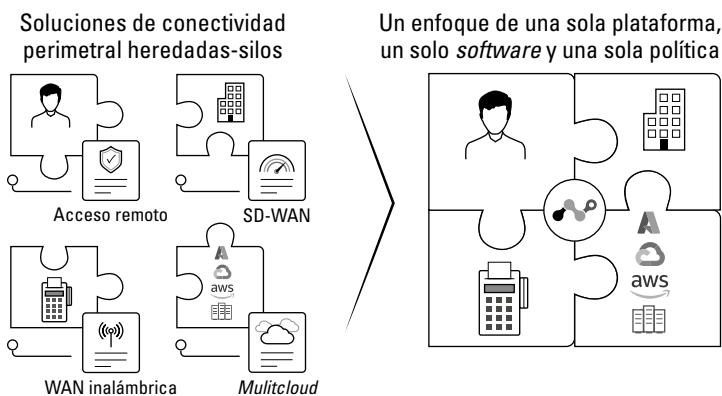


FIGURA 4-1: La arquitectura del «poder de solo uno» puede satisfacer distintos casos de uso, para integrar perfectamente la red con la seguridad, reducir costos y simplificar las operaciones.

Este «poder de solo uno» se manifiesta de diversas maneras:

- » Significa crear una experiencia de usuario coherente regida por políticas que sigan a los usuarios con independencia de su ubicación. Esta coherencia se consigue mediante un *software* ligero que ofrece el mismo conjunto de funciones SD-WAN en todas

partes, desde una sucursal de cualquier tamaño hasta un ordenador portátil en movimiento. El mismo *software* también habilita funciones WAN inalámbricas, permite la creación de redes *multicloud* para facilitar la conectividad de aplicación a aplicación a través de varias nubes, proporciona acceso inteligente al Internet de las cosas (IoT) para obtener valor empresarial a partir de multitud de fuentes de datos, y supervisa y soluciona de forma remota problemas de activos inteligentes.

- » **Todas las soluciones Borderless SD-WAN se gestionan a través de una única consola.**
- » **Engloba una única plataforma que integra perfectamente las redes con la seguridad, ofreciendo un acceso seguro optimizado y una experiencia unificada que reduce los costos y simplifica las operaciones.**

Una experiencia de usuario proporcionada por una plataforma integral que comparte un motor común Zero Trust, la gestión de la experiencia digital y el contexto entre la red y la seguridad: así es como el «poder de solo uno» ofrece en última instancia un verdadero marco de servidor perimetral de acceso seguro (SASE) de un único proveedor (te ofreceremos más información al respecto en este capítulo).

Suena bien, ¿no? Pues eso es solo el principio. Empecemos por las ventajas para los usuarios finales y luego hablemos de las ventajas más amplias de las soluciones Borderless SD-WAN para los equipos de operaciones de red y las empresas.

Borderless SD-WAN facilita la vida de los usuarios finales

Borderless SD-WAN beneficia a todos los usuarios independientemente del lugar desde donde trabajen, ya sea un empleado en una sucursal o un analista que esté en su casa con su portátil tratando de acceder a aplicaciones corporativas situadas en todo el mundo, o un agente de un centro de atención que quiere ofrecer un servicio óptimo a un cliente. Se amplía incluso a un técnico de servicio que esté en una plataforma de un yacimiento petrolífero, trabajando desde un camión. Entre las ventajas de Borderless SD-WAN para los usuarios empresariales cotidianos se incluyen las siguientes:

- » **Flexibilidad y capacidad de elección:** Los usuarios pueden trabajar desde cualquier lugar (ya sea una sucursal o una ubicación remota, como su casa, una cafetería, una autocaravana o un hotel)

y disponer de las mismas capacidades SASE (SD-WAN y servicio de seguridad perimetral [SSE]) en todas partes.

- » **Conectividad optimizada:** Cada usuario puede disfrutar de un acceso de alto rendimiento a varias nubes y centros de datos. Los fallos de rendimiento y de calidad de servicio son cosa del pasado. Incluso las aplicaciones más exigentes, como Zoom y Microsoft Teams, funcionan bien con conexiones irregulares.
- » **Continuidad de las actividades:** La protección de seguridad completa proporcionada por una puerta de enlace SASE y un cliente SASE unificado evita cualquier interrupción que puedan provocar los ciberataques. La seguridad sigue a los usuarios en las sucursales y en ubicaciones remotas.
- » **Acceso Zero Trust:** El mismo acceso Zero Trust que tiene en cuenta el contexto está disponible en cualquier ubicación, lo que permite a los usuarios seguir cumpliendo las políticas corporativas. El sistema garantiza que las políticas sigan a los usuarios y se adapten a su contexto.
- » **Fácil resolución de problemas:** Las operaciones basadas en inteligencia artificial (IA) con los conocimientos del aprendizaje automático (AA) permiten a los administradores de tecnologías de la información (TI) diagnosticar de forma remota los problemas de los usuarios finales y reducir el tiempo medio de resolución de las incidencias de soporte técnico, así como aumentar su productividad.

La experiencia del usuario mejora drásticamente con Borderless SD-WAN. Para los usuarios móviles, como los que viajan en los camiones de la flota de la empresa, la puerta de enlace SASE une la SD-WAN, conmutación, enrutamiento, Wi-Fi y funciones inalámbricas con una integración perfecta con SSE, lo que permite un acceso seguro y optimizado a cualquier aplicación empresarial, independientemente de dónde se encuentren los usuarios.

Los usuarios que trabajan desde ubicaciones remotas disfrutan de una productividad mejorada gracias a una conectividad fiable, incluso desde conexiones dudosas. Borderless SD-WAN es capaz de proporcionar todo esto porque optimiza constantemente la conexión del usuario a cualquier aplicación, incluidas las más exigentes aplicaciones de voz/vídeo sujetas a limitaciones temporales, como Zoom y RingCentral. Por ejemplo, mientras se utilizan estas aplicaciones, si las conexiones experimentan latencia, fluctuaciones y pérdida de paquetes, Borderless SD-WAN soluciona la situación de forma tan fluida que el usuario ni

quiera se da cuenta de que hay un problema. Esa experiencia coherente y de alta calidad y esa conectividad segura tienen lugar entre el usuario y cualquier nube o centro de datos, independientemente del dispositivo o del lugar en que se esté trabajando.

Además, los usuarios reciben políticas coherentes de seguridad y optimización de red con una SD-WAN para *endpoints* y SSE, todo integrado como parte de un cliente SASE unificado que se ejecuta en el portátil de un usuario, ofreciendo la misma experiencia de la sucursal a las ubicaciones remotas. El acceso y la productividad de los usuarios no se verán limitados si trabajan en la oficina, en casa, en una autocaravana o en la playa. Disfrutan de la misma seguridad y conectividad de alto rendimiento estén donde estén (¿entiendes de qué va todo esto?). La experiencia de la aplicación es siempre la misma.

El usuario dispone ahora de mayor flexibilidad y capacidad de elección sobre cómo y dónde quiere trabajar. No tiene que pensar dónde está ni qué dispositivo utiliza: puede acceder a las aplicaciones y trabajar del mismo modo que lo haría como si estuviera físicamente en la oficina. Esta es una función muy potente. Si estás trabajando desde la habitación de un hotel con conexión a Internet y quieres dirigir una reunión de Zoom, tu portátil puede convertirse en el dispositivo SD-WAN que optimiza la última milla para ofrecer una gran experiencia de vídeo de forma automática.

La gestión de la posición de seguridad del *software* como servicio (SSPM) del SSE supervisa continuamente los entornos Zoom para descubrir y corregir cualquier error de configuración que debilite la seguridad, con el fin de mantener el cumplimiento de los parámetros de referencia del sector y los marcos normativos.

Lo mejor de todo es que el usuario ni siquiera sabe que se está realizando un trabajo de optimización y seguridad: solo sabe que su conexión es estable, segura y está optimizada. Consigue un alcance sin precedentes con conectividad en cualquier lugar. Borderless SD-WAN está hecha para el mundo actual de muchos a muchos.

Qué obtienen los expertos en redes de Borderless SD-WAN

Pasemos ahora a los expertos en redes más sofisticados y técnicos (aquí hablamos de ti), que obtienen ocho ventajas principales con Borderless SD-WAN.

Aumento de la confianza operativa con AIOps

Los arquitectos de red y los equipos de operaciones se benefician de funciones administrativas que unifican y preparan una optimización, seguridad y visibilidad de la red a prueba de futuro. Un panel de vidrio (o, en otras palabras, una consola) define las políticas, supervisa y facilita la resolución de problemas para todas las ubicaciones, usuarios y dispositivos de la red. Las sucursales y los usuarios obtienen la misma experiencia y se gestionan de la misma manera. La misma orquestación Borderless SD-WAN y SSE de la sucursal, incluidas las políticas Zero Trust que tienen en cuenta el contexto y que utilizan y gestionan los equipos de red en la actualidad, puede aplicarse ahora a los usuarios individuales que ejecutan el cliente SASE unificado. El mismo soporte desde un único panel de vidrio se amplía a las redes *multicloud*, WAN inalámbrica y soluciones de acceso inteligente del IoT.

Con el aprovisionamiento sin intervención, puedes poner en línea a toda tu red —incluidos usuarios, dispositivos, sitios y nubes— en cuestión de minutos. Pueden establecerse políticas para toda la red y, a continuación, distribuirse a través de todas las puertas de enlace y *endpoints* de Borderless SD-WAN que ejecuten las mismas funciones de SD-WAN y SSE. A la hora de supervisar y optimizar la red, la IA y el AA hacen sonreír a los expertos en redes porque detectan anomalías en la utilización del ancho de banda, permiten la solución automatizada de problemas, proporcionan asistencia proactiva y ofrecen información sobre los flujos y las políticas del tráfico.

Los resultados son tangibles. Tener una visión consolidada de las principales soluciones de la red bajo una misma consola permite a los equipos de operaciones de red agilizar todos los aspectos de la supervisión, la generación de informes y la gestión de la red, así como utilizar eficazmente su tiempo centrándose en proyectos más estratégicos a largo plazo que añadirán valor al crecimiento global de la empresa.

Mayor eficiencia y agilidad con una SD-WAN que tiene en cuenta el contexto

Borderless SD-WAN proporciona visibilidad completa de los datos y las aplicaciones que forman parte de una red híbrida, conectando cada sitio, usuario remoto, dispositivo del IoT y entorno *multicloud*. Esta visibilidad de las aplicaciones es crucial cuando se presta asistencia a usuarios que utilizan diversas aplicaciones, como SaaS y otras aplicaciones personales y profesionales en la nube o en el entorno local. La empresa en evolución necesita ahora una SD-WAN con Zero Trust y que tenga en cuenta el contexto para proporcionar un acceso rápido, fiable y seguro a

cualquier aplicación y dispositivo en cualquier ubicación, con total visibilidad y los controles adecuados.

Borderless SD-WAN puede clasificar el tráfico por aplicación en todos los puertos de forma predeterminada. El truco está en proporcionar la mejor calidad de servicio a las aplicaciones críticas y evitar gastar recursos, ancho de banda y tiempo de funcionamiento en aplicaciones menos importantes. Puesto que existen decenas de miles de aplicaciones SaaS, los equipos de operaciones de red no pueden configurar políticas de calidad de servicio para cada una de ellas. El SASE de Netskope admite una base de datos de más de 60 000 aplicaciones (como comentamos en el capítulo 1 y en otros apartados) categorizadas según un índice de confianza en la nube (CCI) que determina la puntuación de lo preparada que está la aplicación para la empresa. El CCI ayuda a asignar automáticamente las aplicaciones al nivel adecuado de políticas de calidad del servicio. En el capítulo 5 trataremos este tema con más detalle en el contexto de la adopción del SASE.

Netskope dispone de una base de datos de las políticas sobre la calidad del servicio que se asignan a las aplicaciones en función del CCI y otros criterios. Esta asignación automática reduce drásticamente el trabajo manual del equipo de operaciones de red, lo que se traduce en unas operaciones mucho más eficientes.

Las funciones de Netskope que tienen en cuenta el contexto pueden ampliarse para detectar automáticamente todos los dispositivos del IoT, gestionados y no gestionados, y microsegmentos para hacer frente a los riesgos asociados a un dispositivo comprometido.

Aumento de la productividad y mejora de la experiencia del usuario con un rendimiento garantizado de las aplicaciones

Borderless SD-WAN aumenta la productividad y mejora la colaboración al proporcionar un acceso optimizado y de alta fiabilidad a todas las aplicaciones, incluida cualquier función de las comunicaciones unificadas como servicio (UCaaS). Con muy poco esfuerzo, los expertos en redes pueden ofrecer una mejor experiencia a los usuarios que trabajan desde casa, en una sucursal o en un lugar ajeno a la oficina (como un hotel o una cafetería) con funciones de SD-WAN que se ejecutan en la sucursal, en la nube y en sus portátiles. Borderless SD-WAN puede mejorar el rendimiento de la red con una conmutación por error en una fracción de segundo en entornos de enlaces múltiples o mediante una corrección bajo demanda, incluso a través de una única conexión a Internet de banda ancha inestable.

Inversión a prueba de futuro con un controlador 100 % basado en SaaS

Los administradores de TI implementaban manualmente los controladores de SD-WAN a nivel local. Este enfoque «hágalo usted mismo» es complejo en cuanto a implementación y ampliación. Con los controladores Borderless SD-WAN 100 % basados en SaaS que admiten un enrutamiento avanzado, como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF), las organizaciones pueden poner en marcha rápidamente nuevas ubicaciones y conectar sitios remotos. Esta función del controlador en la nube permite a los expertos en redes ampliar fácilmente de uno a miles los sitios, los usuarios y los activos del IoT todo ello con una configuración, gestión y visibilidad sin complicaciones en todos los sitios a nivel mundial.

Los expertos en redes pueden dejar que sus redes crezcan tanto como sea necesario. No tienen que predecir de antemano la capacidad (medida en número de sitios que admite la red SD-WAN). Se puede añadir una puerta de enlace o cliente SASE cada vez que una nueva sucursal o usuario remoto necesite acceder a la red. También de dispondrá de una ampliación infinita porque el controlador funciona como un servicio SaaS. Ahora la red puede ampliarse según la demanda. ¡Toma ya! A prueba de futuro.

Mayor alcance y flexibilidad con WAN inalámbrica

El mundo de los negocios va mucho más allá del alcance de las redes con cable tradicionales. Pero que haya conectividad inalámbrica no significa que vayas a obtener la conectividad, la calidad de servicio y la seguridad necesarias para gestionar una empresa moderna. Con las puertas de enlaces inalámbricas gestionadas en la nube de Borderless SD-WAN, puedes convertir la conectividad inalámbrica en una red sólida como una roca, segura y optimizada, tanto si estás configurando una red puntual en un sitio remoto u oficina temporal como si quieres proporcionar una conectividad inalámbrica rápida, fiable y sin esfuerzo.

La puerta de enlace inalámbrica Borderless SD-WAN puede integrarse en tu infraestructura existente y emparejarse con cualquier solución SD-WAN para ofrecer un soporte celular principal o de respaldo. Esto facilita una creación rápida de los servicios de red, lo que aumenta la productividad y la agilidad empresarial.

Transforma tu empresa con SASE en la nube

La SD-WAN tradicional tiene dificultades a la hora de ofrecer visibilidad total y rampas de acceso optimizadas desde cualquier usuario o sitio a cualquier nube, SaaS o aplicaciones privadas. Incluso si añadimos “creatividad” con una combinación de instalaciones de concentradores SD-WAN que hayas creado tú mismo, esto hará que los entornos de los proveedores sufran latencias y no ofrezcan una conectividad de alto rendimiento. Ahí es donde realmente cuenta la calidad de la infraestructura de la red.

NewEdge de Netskope es la nube privada de seguridad mejor conectada del mundo, con cobertura en más de 70 regiones y convergencia de servicios de red y seguridad a escala. Ofrece rampas de entrada de baja latencia al tráfico distribuidas por todo el mundo, está altamente interconectada y dispone de un sistema informático completo en cada región para el procesamiento del tráfico. Tiene una disponibilidad de cinco nueves (99,999 %) y ofrece los mejores acuerdos de nivel de servicio (SLA) del sector. La red NewEdge permite a cada usuario, sucursal, sitio, dispositivo y entorno *multicloud* de todo el mundo estar cerca de una Borderless SD-WAN convergente con servicios SSE. Los concentradores de nube Borderless WAN y SSE en la infraestructura NewEdge distribuida globalmente proporcionan ventajas a distintos niveles:

»» **Borderless SD-WAN de Netskope amplía el tejido SD-WAN de las ubicaciones locales a todos los recursos SaaS y en la nube.**

Por ejemplo, al utilizar una SD-WAN de *endpoint* con un cliente SASE unificado, el tráfico de Zoom puede optimizarse para un usuario que está conectado desde una ubicación remota del mismo modo que se haría para un usuario que trabaja en una sucursal corporativa y utiliza la puerta de enlace SASE de Netskope. Otro ejemplo es aprovechar un servicio de media milla que conecte sucursales dispersas geográficamente con una aplicación ubicada en la sede central en otro continente.

»» **Gracias a su perfecta integración con SSE, Borderless SD-WAN ofrece una protección completa contra todas las amenazas de ciberseguridad y una red de alto rendimiento, lo que garantiza la continuidad de las operaciones empresariales.**

»» **Borderless SD-WAN puede aprovecharse para conectar los recursos empresariales distribuidos en entornos de varias nubes, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP), a un tejido de red unificado.** A través del enrutamiento avanzado y la integración nativa dentro de los

proveedores de nube, Borderless SD-WAN permite la interconexión de diferentes regiones y facilita la integración con un solo clic con Netskope Intelligent SSE para las cargas de trabajo en la nube.

Al proporcionar estas funciones, Borderless SD-WAN permite a las empresas acelerar la adopción de la nube tanto con una conectividad de alto rendimiento como con la posición de seguridad adecuada. Alojarse algunos activos en el entorno local mientras otros están en la nube ya no genera ninguna preocupación. La migración gradual de más infraestructuras a la nube está totalmente respaldada sin tener que pensar en las limitaciones del entorno SD-WAN existente. La limitada compatibilidad con varias nubes que ofrece la SD-WAN tradicional provoca a menudo enormes quebraderos de cabeza logísticos, algo que no queremos que sufran los expertos en redes.



RECUERDA

Con Borderless SD-WAN, las empresas pueden controlar cómo habla e interactúa cada nube con las demás, lo que constituye una excelente estrategia de nube empresarial.

Garantiza la seguridad de tu empresa con una protección SASE de 360 grados

Borderless SD-WAN ofrece un completo paquete de funciones de seguridad integradas. Desde el punto de vista de la red, Borderless SD-WAN proporciona la seguridad de la red híbrida perimetral al introducir servicios como *firewalls* y un sistema de prevención de intrusiones (IPS) para la segmentación este-oeste. Gracias a la integración con Netskope Intelligent SSE, obtendrás una protección de 360 grados con funciones para la puerta de enlace web segura (SWG), agente de seguridad para el acceso a la nube (CASB), acceso Zero Trust (confianza cero) a la red (ZTNA), prevención de pérdida de datos (DLP), SSPM, gestión de la posición de seguridad en la nube (CSPM), *firewall* en la nube y otros servicios de seguridad.

Tanto los servicios de red como los de seguridad que componen el SASE de Netskope se basan en NewEdge, una plataforma nativa en la nube que es rápida, fiable y convergente y que ofrece la cobertura geográfica más amplia del sector (más de 70 regiones). Esto se traduce en una latencia de milisegundos de un solo dígito para la gran mayoría de los trabajadores de conocimiento del mundo. Las empresas están protegidas frente a todo tipo de ciberataques y filtración de datos, lo que evita interrupciones y protege la reputación de la marca. Las puertas de enlaces y los clientes SASE eligen automáticamente el punto de presencia (PoP) de SSE óptimo para la seguridad y la optimización. Los expertos en redes están encantados con la posibilidad de implementar SSE con un solo clic, tanto en las sucursales como para los usuarios remotos. El resultado es

una nueva forma de avanzar en la conectividad, construida en la nube, que ofrece una increíble agilidad empresarial.

Haz realidad el valor empresarial de los datos con el procesamiento perimetral

Borderless SD-WAN admite de forma nativa funciones de procesamiento perimetral y la capacidad de ejecutar servicios de contenedor listos para usar, como el tiempo de ejecución de Azure IoT Edge, la gestión de la experiencia digital, etc. Los administradores de TI pueden elegir un servicio de un catálogo o usar sus propias aplicaciones personalizadas. Con las funciones de gestión del ciclo de vida de las aplicaciones (ALM), las empresas pueden implementar estos servicios a gran escala y ofrecer estas aplicaciones en miles de dispositivos de puerta de enlace SASE con un solo clic.

Reducción de los costos generales de TI

Mientras tanto, las ventajas que ofrece Borderless SD-WAN se traducen en una huella de red consolidada. Una solución única y centralizada sustituye la configuración de múltiples proveedores de SD-WAN por un producto de un único proveedor. No es de extrañar que un menor número de proveedores equivalga a una reducción significativa de los costos de prestación de asistencia a la red. El costo de formar al personal operativo en una multitud de productos puntuales puede superar rápidamente los gastos operativos y de capital de la organización en estos productos.

Borderless SD-WAN allana el camino para eliminar las soluciones aisladas y no integradas con el fin de reducir costos y lograr un mayor retorno de la inversión. Borderless SD-WAN reduce la complejidad al sustituir varios productos y consolas por un único *software* ligero que responde a las principales necesidades de los clientes. Los expertos en redes amplían su control con Borderless SD-WAN. (No estamos diciendo que seamos unos maniáticos del control, pero vale, sí, lo somos. Es parte del trabajo, ¿no?) Borderless SD-WAN reduce la carga administrativa al proporcionar una gestión centralizada nativa de la nube para toda la red.

Con Borderless SD-WAN, las empresas pueden ahorrar en gastos de capital (CapEx) y en las operaciones generales de TI. Con una sola consola, una automatización y un *software* que gobierna toda la red, las empresas gastan menos y aumentan el retorno de la inversión (ROI). Por ejemplo, Borderless SD-WAN de Netskope ha supuesto un ahorro de al menos diez veces el costo total de propiedad (TCO) a los clientes que han construido una arquitectura convergente con esta tecnología.

- » **Cómo superar los retos de seguridad de una red de área extensa definida por *software* (SD-WAN)**
- » **El servidor perimetral de acceso seguro (SASE) para combinar redes y seguridad**
- » **Recorrido hasta SASE**

Capítulo 5

Cómo acelerar la adopción de SASE

Ahora, tenemos que hablar de cómo se integra la seguridad en la Borderless SD-WAN de Netskope más amplia como parte de una arquitectura SASE más amplia. El camino hasta SASE se ha visto acelerado por las empresas que buscan innovaciones digitales para diferenciarse. Esto ha creado la necesidad de generar nuevas funciones digitales, como la informática en la nube y la convergencia de redes y seguridad a los niveles de producto, arquitectura y organización.

SASE combina conceptos como Zero Trust, SD-WAN y el servicio de seguridad perimetral (SSE) para guiarnos hacia una posición de seguridad y redes que protege y gobierna la nube y el nuevo entorno de trabajo desde cualquier lugar. Para llegar a SASE, tanto las redes como la seguridad deben estar definidas por *software* y entregarse en la nube. Una forma de conseguir el SASE es mediante la consolidación y la integración de las funciones de seguridad, la esencia propia del SSE.

El SSE reubica los puntos de inspección y control críticos en la nube que pone en marcha tu negocio. Este cambio coloca a la seguridad junto al lugar donde se encuentran los datos, se ejecutan las aplicaciones y trabajan las personas, y también donde está el posible peligro. SSE funciona bien con Borderless SD-WAN porque está definido por *software* y sus

servicios críticos se entregan en la nube de forma nativa. Esto optimiza la conectividad para cada usuario, dispositivo, sitio, aplicación y pieza de la infraestructura corporativa sin que se ralentice el negocio.

Por tanto, combinar la SD-WAN con el SSE permite a las empresas conseguir un SASE, algo necesario para que Borderless SD-WAN sea verdaderamente seguro. En este capítulo, hablaremos de los problemas de la seguridad en un entorno SD-WAN tradicional y de cómo han surgido nuevas tecnologías para que las empresas puedan mantener su seguridad en una arquitectura en la nube.

El problema de la seguridad con SD-WAN en el mundo anterior a SASE

Borderless SD-WAN se centra en capacitar a los empleados actuales para que trabajen desde cualquier lugar y dispositivo. Los usuarios deben poder acceder a cualquier aplicación, que, a su vez, puede encontrarse en cualquier lugar. Para ello, tienen que saber con seguridad que, independientemente de dónde se encuentren y a qué aplicaciones accedan, las funciones clave de la empresa estarán disponibles y podrán trabajar sin interrupciones. Pero la seguridad también debe garantizarse para estos usuarios, dispositivos, sitios y aplicaciones. Por tanto, Borderless SD-WAN debe integrarse con una pila de seguridad adecuada que proteja a cada usuario, dispositivo, sitio, aplicación, y pieza de la infraestructura de la empresa.

Para comprender los retos derivados de una integración fluida de la seguridad con Borderless SD-WAN, tenemos que saber dónde nos encontrábamos y dónde estamos ahora en relación con la SD-WAN tradicional y la seguridad.

Con la SD-WAN tradicional, todas las conexiones parten de los perímetros físicos de una sucursal del mundo real hacia uno o más proveedores de infraestructura como servicio (IaaS), plataforma como servicio (PaaS) o *software* como servicio (SaaS), y hacia cualquier proveedor de comunicaciones unificadas como servicio (UCaaS). Todas estas conexiones se basan en las necesidades de los usuarios y en las aplicaciones a las que quieren acceder. Uno de los principales problemas que surgió de la SD-WAN tradicional fue cómo mantener la seguridad. La seguridad se convirtió en el legendario talón de Aquiles de la SD-WAN tradicional. Hagamos un inciso para aclarar lo siguiente: cuando se trata de aplicaciones, la SD-WAN tradicional se diseñó para detectar, priorizar y proteger solamente unos cuantos miles de aplicaciones. Esto es algo muy restrictivo en una época en la que proliferan las aplicaciones.

Y todo esto funcionó bien... hasta que dejó de hacerlo.

A medida que las empresas eliminaron sus fronteras, el perímetro se transformó y extendió más allá de las sucursales para incluir a microsucursales, ubicaciones remotas de los usuarios y dispositivos del Internet de las cosas (IoT) ubicados en los bordes de la *multicloud*. Aquí la necesidad común es que todas estas cosas deben protegerse. Los arquitectos de redes comenzaron a implementar múltiples productos puntuales dirigidos a la seguridad y la conectividad para incluir estos nuevos bordes o perímetros. Este enfoque condujo a una red llena de tecnologías dispares e inconexas que se vieron obligadas a funcionar juntas. Con frecuencia, esto dio lugar a complicaciones excesivas para los usuarios y las operaciones de TI. Una arquitectura fragmentada no puede aplicar las políticas de seguridad ni de calidad de la experiencia de manera coherente para todos los usuarios, dispositivos, sitios y nubes. Es más, hoy en día, hay decenas de miles de aplicaciones que residen en la nube, un modelo para el que no se había diseñado la SD-WAN tradicional y con el que no es compatible. Y como suele decirse: «Lo que no se detecta, no se puede priorizar ni proteger». Así que la SD-WAN tradicional tuvo problemas con todas las nuevas aplicaciones que no podía detectar.

Además, la falta de visibilidad y control granular del IoT plantea riesgos para la empresa. La SD-WAN tradicional no pudo reducir el efecto de los dispositivos comprometidos. Por tanto, añadir más contexto al modelo con una seguridad Zero Trust se convirtió en algo fundamental para prestar servicios de SD-WAN que pudieran satisfacer las necesidades de la empresa actual en el perímetro y en toda la WAN.

Para conseguir una seguridad integral adecuada que evitara los ciberataques a la SD-WAN, algunas organizaciones tuvieron que redirigir todo el tráfico a una ubicación centralizada, como un centro de datos. Desde ahí, se conectarían a Internet y a distintas nubes para utilizar los servicios IaaS, PaaS y SaaS. Aunque se contaba con seguridad, la experiencia de usuario estaba una vez más comprometida, ya que existían problemas de latencia inherentes al redireccionamiento del tráfico. Para evitar redirigir el tráfico y la latencia resultante, algunas empresas optaron por una seguridad distribuida en cada sitio. Algunas incorporaron dispositivos de seguridad independientes a las soluciones de SD-WAN existentes. Aunque otras se decantaron por el uso de servicios complejos que combinaban distintos métodos en los mismos dispositivos denominadas soluciones SD-WAN «gruesas», esto resultaba caro y era complejo de gestionar y ampliar. Algunos proveedores de SD-WAN con funciones de *firewall* básicas comenzaron a utilizar el término «seguridad suficientemente buena» a nivel de sucursal. Pero una seguridad de redes «suficientemente buena» no podía sustituir a la seguridad de más alto nivel que necesitaba la empresa.

Decir que la convergencia de red y seguridad para cada usuario remoto, sucursal, IoT y entorno multicloud se convirtió en un mero acto de malabarismo sería quedarse corto. Se parecía más a sacar toda la arena de la playa grano a grano, es decir, una tarea propia de Sísifo. (Nos habíamos propuesto incluir tantas metáforas como fuera posible en dos frases, y creo que lo hemos conseguido).

La seguridad en la nube preparó el camino a SASE

La aparición y gran popularidad de la seguridad en la nube marcó un cambio en la estrategia de los proveedores de SD-WAN. Comenzaron a asociarse con los proveedores de seguridad en la nube para reducir los riesgos que presentaba el acceso directo a Internet a través de la nube. Esto contrastaba con la práctica anterior de dirigir el tráfico de SD-WAN a través de los centros de datos de la empresa para las inspecciones de seguridad, lo que creaba la «horquilla» de tráfico que provocaba una gran latencia o la distribución de una pila de seguridad completa en cada sucursal.

El tiempo ha demostrado que la seguridad en la nube es el enfoque correcto y ha allanado el camino hacia SASE. Las empresas tratan de unificar sus arquitecturas de red y seguridad para simplificar las operaciones y facilitar la tarea de compartir contexto entre SD-WAN y la seguridad en la nube con el fin de conseguir unos controles más eficaces y granulares.

SASE: nacido para unir la red y la seguridad

SASE y SSE representan el modo en que la seguridad se traslada a la nube para convertirse en lo más eficaz que hemos tenido hasta la fecha. SSE es la forma en que todos los servicios de seguridad necesarios para SASE (que anteriormente eran aplicaciones, productos o servicios independientes, a menudo de distintos proveedores) se unen de una manera unificada e integrada para proporcionar mayor capacidad, mejorar la eficiencia y reducir la complejidad y el costo. SASE es una visión general para la transición de las capacidades de la red y la seguridad a la nube. SSE consolida todas las funciones de seguridad necesarias, mientras que Borderless SD-WAN consolida todas las funciones de red necesarias y, a continuación, SASE converge la red y la seguridad.

SASE ofrece un conjunto de servicios de red y seguridad integrados que se convierten en el principal punto de inspección de todo el tráfico, garantizando una seguridad coherente para todos los usuarios, datos,

dispositivos, sitios y aplicaciones. SASE conecta todos tus «sentidos» de red y seguridad a un solo cerebro que conecta, optimiza, interpreta los datos, comprende el alcance de los riesgos presentes y negocia el nivel de acceso adecuado en cualquier momento determinado y en cualquier situación.

Netskope Intelligent SSE hace uso de todo el valor de la nube al integrar las funciones de seguridad críticas de la empresa, como el agente de seguridad para el acceso a la nube (CASB), la puerta de enlace web segura (SWG), el acceso Zero Trust (confianza cero) a la red (ZTNA), la prevención de la pérdida de datos (DLP), la gestión de la posición de seguridad en la nube (CSPM), la gestión de la posición de seguridad en SaaS (SSPM), la gestión de la experiencia digital (DEM), *firewall* como servicio (FWaaS), etc., garantizando que funcionan conjuntamente. Mediante el uso de la integración con un clic y NewEdge de Netskope, Borderless SD-WAN puede ayudar a ofrecer estos servicios SSE tan cerca como sea posible del punto de acceso con personas, datos y aplicaciones. Asimismo, los puntos de presencia (PoP) distribuidos globalmente de NewEdge garantizan la menor latencia posible cuando los usuarios acceden a cualquier aplicación desde cualquier lugar para ofrecer una conectividad de alto rendimiento y gran calidad que acelere la adopción de SASE. NewEdge de Netskope ofrece también seguridad con SSE y una rampa de acceso a cualquier nube con Borderless SD-WAN, incluida la optimización de aplicaciones UCaaS críticas para la empresa.

Entonces, ¿qué ocurre con el perímetro de la empresa, donde se encuentra la puerta de enlace SASE y desde donde trabajan los usuarios y dispositivos? La puerta de enlace SASE, que utiliza el *software* de Borderless SD-WAN, ofrece de forma nativa *firewalls* avanzados en la capa 7 y un sistema de prevención de intrusiones (IPS).

A continuación, te ofrecemos más información sobre las funciones de seguridad integradas del SASE de Netskope:

- » **Clasificación:** Identifica y etiqueta información confidencial, de forma ideal cuando se crea, pero también mediante análisis periódicos de los almacenes de datos.
- » **CASB:** Funciona como un punto de aplicación de políticas de seguridad situado entre los consumidores de servicios en la nube y los proveedores de servicios en la nube para aplicar políticas de seguridad empresarial cuando se accede a los recursos en la nube.
- » **SWG:** Controla el acceso y protege ante amenazas web solamente. La SWG de Netskope también protege frente a amenazas y riesgos de datos en la nube para instancias personales de aplicaciones

gestionadas, miles de aplicaciones de tecnología de la información (TI) en la sombra y servicios en la nube.

- » **ZTNA:** Hace cumplir la premisa de que no se confía en nadie a ciegas ni se le permite acceder a los activos de la empresa hasta que haya sido validado como persona auténtica y autorizada. El acceso de privilegio mínimo solo concede el acceso a los recursos que necesita el usuario y a nada más.
- » **Aislamiento remoto del navegador (RBI):** Separa los dispositivos de los trabajadores de la navegación por Internet alojando y ejecutando toda la actividad de navegación en un contenedor remoto en la nube. Este espacio seguro protege los datos, los dispositivos y las redes frente a todos los tipos de amenazas que se originan en sitios web maliciosos.
- » **FWaaS:** Ofrece seguridad para todos los puertos y protocolos de salida a fin de proporcionar un acceso seguro y directo a Internet mediante un agente en dispositivos gestionados o a través de la encapsulación de enrutamiento genérico (GRE) y el protocolo de seguridad de Internet (IPSec) para las oficinas.
- » **DLP:** DLP evita la exfiltración de datos accidental y no intencionada que se lleva a cabo mediante un uso indebido intencionado y no intencionado. Netskope DLP ofrece una detección precisa de todos los datos confidenciales en cualquier formato con el menor grado de error posible.
- » **Conocimiento y neutralización de amenazas (también llamada protección avanzada contra amenazas [ATP]):** Identifica indicios de que un entorno se ha visto comprometido y toma medidas para reducir o eliminar la probabilidad de ataques futuros.
- » **CSPM:** Identifica y corrige los problemas que causan los errores de configuración entre las organizaciones y el proveedor de servicios en la nube (CSP) en distintos entornos de nube IaaS como Amazon Web Services (AWS), Microsoft Azure, y Google Cloud Platform (GCP).
- » **SSPM:** Evalúa la configuración de las aplicaciones SaaS y elimina las configuraciones erróneas que puedan permitir la exfiltración, suplantación de identidad y otros tipos de ataque.
- » **Seguridad en el entorno local:** Los servicios de seguridad también pueden incluirse a nivel local. El tráfico este-oeste también puede hacer uso del *firewall* de próxima generación (NGFW) local, del sistema de detección de intrusiones (IDS)/IPS, entre otros, con la puerta de enlace SASE de Borderless SD-WAN.

SASE es un viaje: recorrido por todo el entorno

Una arquitectura SASE robusta que integra Borderless SD-WAN puede adoptar muchas formas, en función de las necesidades de cada empresa individual. Por definición, un SASE que logra sus objetivos implica menos proveedores, operaciones más sencillas, menos complejidad, menos costos y un rendimiento más rápido y fluido de la red con seguridad de pila completa. Esta mejora exhaustiva no tiene lugar en un abrir y cerrar de ojos.



RECUERDA

SASE es un viaje y no un «arrancar y reemplazar»;; en la mayoría de los casos, la consolidación de los proveedores tendrá lugar con el tiempo.

Muchas empresas utilizan ya la seguridad en la nube de proveedores de SSE y podrían elegir una SD-WAN que se integre mejor con sus soluciones de seguridad existentes. Por otro lado, si la organización ya tiene un producto Borderless SD-WAN, podría integrarlo a su solución de seguridad en la nube preferida. No hay un enfoque correcto o incorrecto. Lo que más importa está relacionado con las necesidades particulares de cada organización y lo que mejor le funcionará para lograr sus objetivos comerciales.

En los apartados siguientes se describen las ventajas específicas de tener un solo proveedor de SASE. Te recomendamos que las tengas presentes antes de iniciar tu viaje y decidir qué camino seguir. A veces, $1 + 1$ no son siempre 2.

Zero Trust, SASE que tiene en cuenta el contexto

En la era de la nube, la visibilidad no es suficiente. Incluso con una imagen de la más alta resolución, todavía pueden perderse pequeños detalles si no se sabe cómo y adónde mirar, o qué buscar exactamente. Un contexto enriquecido centrado en los usuarios, los dispositivos, las aplicaciones y sus riesgos asociados es un ingrediente necesario para poder definir las políticas de SASE granulares. Un contexto así también es crucial para implementar Zero Trust.

Para las funciones de red y de seguridad del SASE de Netskope, el contexto llega de la mano de Netskope Cloud XD (Xtreme Definition) que ejecuta el motor de Zero Trust. El SSE de Netskope, como parte de la arquitectura SASE de Netskope, comparte el mismo motor de Zero Trust que Borderless SD-WAN. Esto permite compartir el contexto entre los servicios de red y seguridad unidos e incluye políticas granulares que se basan en detectar aplicaciones e identificar sus riesgos, detectar dispositivos e identificar sus riesgos y detectar usuarios e identificar sus riesgos.

A modo de ejemplo, SSE y Borderless SD-WAN de Netskope comparten un motor de base de datos de aplicaciones común que identifica más de 60 000 aplicaciones. Netskope califica cada aplicación con un índice de confianza en la nube (CCI), que ofrece una puntuación de lo preparada que está cada aplicación para la empresa. Con el SSE de Netskope, los administradores de TI pueden hacer uso del CCI para identificar y evaluar el riesgo asociado a distintos servicios en la nube y tomar decisiones informadas sobre permisos o bloqueos de aplicaciones concretas dentro de su entorno. Esto facilita un afinamiento del control de uso de los servicios en la nube, garantizando el cumplimiento de los requisitos de seguridad y gobernanza. Borderless SD-WAN aprovecha la información contextual que ofrece el CCI para establecer unos valores predeterminados y listos para usar de la calidad de la experiencia para la puerta de enlace SASE de Netskope. Esto elimina la difícil y laboriosa tarea de configurar manualmente reglas de calidad de la experiencia para decenas de miles de aplicaciones. Al aprovechar la información del CCI, Borderless SD-WAN puede asignar dinámicamente los recursos de la red, como el ancho de banda y la prioridad, garantizando un rendimiento óptimo de las aplicaciones esenciales (consulta la figura 5-1).



FIGURA 5-1: Un contexto enriquecido centrado en los usuarios, los dispositivos, las aplicaciones y sus riesgos asociados es un ingrediente necesario para poder definir las políticas de SASE granulares.

Política unificada y experiencia coherente en cualquier lugar

En el mundo actual en el que operan la mayoría de las empresas, las sucursales y los usuarios remotos no se gestionan de forma unificada. El

soporte de la SD-WAN tradicional a los usuarios de las sucursales carece de conocimientos del contexto y de seguridad Zero Trust, mientras que la puerta de enlace Borderless SD-WAN de Netskope permite habilitar políticas con una SD-WAN que incluye políticas contextuales de Zero Trust granular. Las redes privadas virtuales (VPN) utilizadas normalmente para prestar soporte a los usuarios remotos carecen de visibilidad y optimización, mientras que la SD-WAN para *endpoints* de Netskope aborda ambas necesidades. De esta manera, con las funciones de integración de Borderless SD-WAN y SSE, una empresa moderna puede ofrecer un SD-WAN de alto rendimiento que tiene en cuenta el contexto a los usuarios de las sucursales y remotos (consulta la figura 5-2).

El resultado es un marco de políticas unificado que ofrece una experiencia y una seguridad coherentes que siguen a los usuarios. Las arquitecturas de red y los equipos de operaciones se benefician de la única plataforma, única consola y única política de Borderless SD-WAN para configurar y gestionar las políticas de las sucursales que pueden aplicar ahora a usuarios individuales en ubicaciones remotas. No importa dónde estén los usuarios, las aplicaciones o los servicios, desde una sola plataforma unificada, los departamentos de TI de la empresa pueden ahora gestionar las sucursales y a los usuarios remotos individuales con una política Zero Trust y de rendimiento de la red uniforme en toda la infraestructura corporativa. Este enfoque unificado ofrece una arquitectura ampliable, operaciones agilizadas, conectividad de alto rendimiento y seguridad inquebrantable según unos principios Zero Trust que tienen en cuenta el contexto.

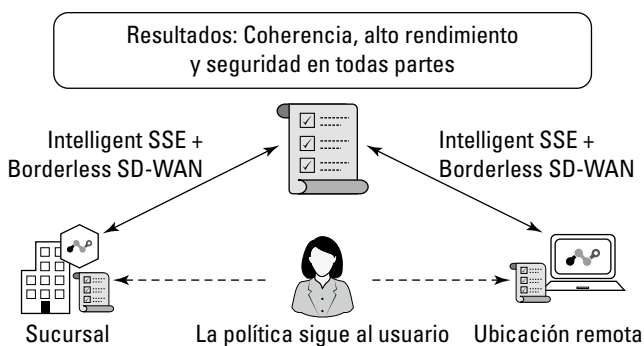


FIGURA 5-2: Desde una sola plataforma unificada, los equipos de TI pueden ahora gestionar las sucursales y a los usuarios remotos individuales mediante una política de seguridad y de rendimiento de la red uniforme que sigue al usuario.

SASE en la nube con un alcance global sin precedentes

Históricamente, los ingenieros de seguridad y de redes se han enfrentado siempre a un ejercicio de equilibrio muy conocido: más seguridad frente a un mayor rendimiento. La ley no escrita de la seguridad de la red es que no se puede tener todo: siempre hay que llegar a un compromiso entre rendimiento, disponibilidad y seguridad. La plataforma NewEdge de Netskope rompe esta regla y ofrece los tres requisitos sin exigir ningún compromiso.

Como dijimos en el capítulo 3, NewEdge de Netskope es hoy en día la nube privada más destacada para la seguridad, con una amplia cobertura en más de 70 regiones del mundo. Combina con éxito los servicios de red y seguridad a gran escala, ofreciendo rampas de entrada de baja latencia al tráfico por todo el mundo. Gracias a la amplia interconexión e infraestructura de procesamiento exhaustiva en cada región, NewEdge procesa el tráfico con eficacia. Asimismo, garantiza una disponibilidad excepcional con un tiempo de actividad del 99,999 %, y cuenta con los mejores acuerdos de nivel de servicio (SLA) del sector para ofrecer un rendimiento y fiabilidad óptimos.

Con la red NewEdge (consulta la figura 5-3), cada usuario, sucursal, sitio, dispositivo y entorno *multicloud* de todo el mundo puede acceder sin interrupción a Borderless SD-WAN integrado con servicios SSE. Los servicios de SSE disponibles en NewEdge incluyen una gran cantidad de ofertas, como la puerta de enlace web segura de próxima generación (NG-SWG), CASB, ZTNA, SSPM, CSPM, FWaaS y DLP. Los servicios de Borderless SD-WAN de Netskope en la red NewEdge amplían con eficacia el alcance de SD-WAN para añadir los recursos de la nube y del SaaS. Esto facilita la optimización del tráfico de la nube para los usuarios remotos y las sucursales. También ofrece un servicio de media milla que garantiza una conectividad fiable entre las sucursales distribuidas geográficamente y las aplicaciones centralizadas en un continente distinto.

Esta combinación de la red NewEdge, los servicios SSE y Borderless SD-WAN garantiza una conectividad segura y de alto rendimiento para aplicaciones en la nube, web, SaaS y privadas. Proporciona a las organizaciones una infraestructura robusta que consigue un alto rendimiento y un acceso protegido a los recursos críticos en distintos entornos.



70 regiones
Accesos al tráfico distribuidos globalmente y de baja latencia



Más de 100 zonas de localización
Mayor resistencia en la experiencia localizada



Más de 2000 proximidades de red
Altamente interconectadas, Microsoft y Google en todas las regiones posibles



Procesamiento completo
En cada región, procesamiento del tráfico mediante la pila SASE completa



Los mejores SLA del sector
Tiempo de actividad del 99,999 %, procesamiento 10 veces más rápido, tasa de captura de malware del 100 %



FIGURA 5-3: NewEdge combina con éxito los servicios de red y seguridad a escala, ofreciendo rampas de entrada de baja latencia al tráfico por todo el mundo.

Operaciones de TI unificadas y simplificadas

Los usuarios, los dispositivos, los sitios y las nubes exigen un alto rendimiento y conexiones seguras «de cualquiera a cualquiera». Los enfoques actuales dan como resultado muchos productos puntuales y

disparos que aumentan los costos y la complejidad. Gracias a su enfoque sumamente integrado hacia la seguridad y los servicios de red, SASE aporta muchas ventajas rentables.

Desde el punto de vista de la red, un solo *software* Borderless SD-WAN ligero puede ayudar a eliminar muchos productos puntuales (por ejemplo, SD-WAN de sucursales, VPN de acceso remoto, puertas de enlace inalámbricas, perímetro *multicloud*, etc.), por lo que reduce la complejidad (consulta la figura 5-4). El SSE integra distintas funciones de seguridad en una sola solución, eliminando así la necesidad de contar con varios productos que no comparten entre ellos la información sobre amenazas y debilitan la postura de seguridad. Además, como hemos dicho antes, Borderless SD-WAN y SSE se integran entre sí a la perfección y comparten el mismo motor Zero Trust. Con un SASE que consolida a los proveedores hay menos sistemas que controlar y mantener, y se consiguen unos mejores diseños de la red, lo que reduce los gastos operativos. Y al hacer uso de las operaciones generadas por la inteligencia artificial (IA) y la automatización de gran parte de la actividad de detección y respuesta, se reduce el número de incidencias de soporte técnico y disminuye considerablemente el tiempo medio de respuesta para la resolución de problemas.

Operaciones basadas en IA

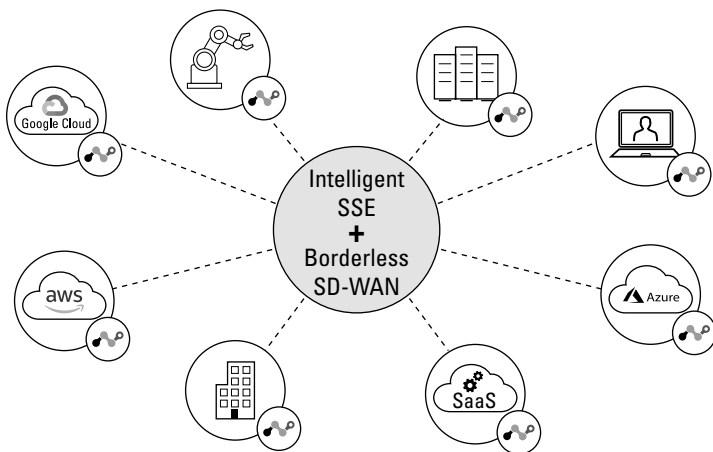


FIGURA 5-4: SASE consolida a múltiples proveedores, por lo que hay menos sistemas que controlar, se simplifican los diseños de la red y se consiguen ventajas en lo que respecta a la rentabilidad.

EN ESTE CAPÍTULO

- » Cómo fortalecer tu empresa con diversas arquitecturas de red
- » La adopción de una solución creada para la nube
- » Seguridad y optimización de la conectividad
- » Exploramos el acceso inteligente a la red y el enrutamiento avanzado
- » Más información sobre la seguridad integral de las redes híbridas
- » Aplicaciones de máxima categoría en cualquier lugar
- » Mayor conocimiento del contexto
- » Cómo aprovechar el poder de las operaciones basadas en la inteligencia artificial (IA)
- » Implantación de una estrategia que prioriza lo inalámbrico
- » Flexibilidad y eficacia con la orquestación de contenedores

Capítulo 6

Las diez funciones principales que se necesitan para que las empresas adopten Borderless SD-WAN

Si has llegado hasta aquí, probablemente estés pensando seriamente en adoptar Borderless SD-WAN de Netskope, ya sea ahora o en un futuro próximo. Y también es probable que te estés preguntando (teniendo en cuenta todas las formas en que hemos demostrado que Borderless SD-WAN supera a la red de área extensa definida por

software (SD-WAN) tradicional) cuáles son las funciones diferenciadas que deberías buscar en una solución Borderless SD-WAN para asegurarte de que es la adecuada para tu empresa.

En el capítulo 5, mostramos cómo una solución de servidor perimetral de acceso seguro (SASE) de un único proveedor simplifica el viaje y ofrece una conectividad segura, fiable y optimizada para cada sitio, nube, usuario remoto o dispositivo del Internet de las cosas (IoT). Esto permite a todos los miembros de una empresa disfrutar de las ventajas de una plataforma SASE verdaderamente convergente que simplifica las operaciones, aplica una seguridad uniforme, mantiene el rendimiento de la red y garantiza el éxito de SASE.

Quienes adoptan la solución SASE de proveedor único de Netskope pueden simplificar su arquitectura con el «poder de solo uno» (consulta el capítulo 4), es decir, una sola plataforma, un solo *software* ligero y una sola política para controlar todas las redes y la seguridad. Para poder resumir las ventajas de Borderless SD-WAN, presentamos diez funciones que pueden ayudar a impulsar el viaje de una organización hacia su adopción.



CONSEJO

Si eres una de esas personas que leen los libros sin ningún orden (es tentador saber cuál es el final desde el principio, ¿no?) y este es el primer capítulo que estás leyendo, ten en cuenta que estas funciones proporcionan el marco adecuado para implementar las soluciones Borderless SD-WAN de las que ya hemos hablado a lo largo del libro. Estas son las diez funciones *principales*, pero no las *únicas*; la lista de lo que puede hacer Borderless SD-WAN es mucho más larga y muy adaptable a las necesidades de cada empresa. Utiliza esta lista como contexto para poder tomar otras decisiones a la hora de adoptar una solución.

Potencia tu empresa con la convergencia de SASE

No hay una forma incorrecta de construir tu arquitectura de seguridad y Borderless SD-WAN. Lo que importa es que se adapte a las necesidades de tu empresa, ayudándote a alcanzar los objetivos técnicos y comerciales que tu organización esté tratando de alcanzar. Al adoptar un enfoque unificado a través de Borderless SD-WAN e Intelligent Security Service Edge (SSE) de Netskope, las organizaciones pueden eliminar la necesidad de múltiples productos puntuales y lograr eficiencia operativa. Esta convergencia de conectividad y seguridad aborda diversos casos de uso, como entornos *multicloud*, sucursales de cualquier tamaño, usuarios remotos y el IoT. A través de una única solución de *software* ligera,

Borderless SD-WAN se integra a la perfección con Intelligent SSE de Netskope para conseguir una red sumamente segura, optimizada y de alto rendimiento para cada usuario remoto, dispositivo, sitio y nube. Este enfoque integrado simplifica la gestión y reduce la complejidad, lo que permite a las organizaciones agilizar sus operaciones con eficacia.

Obtén toda la potencia de la nube con una solución que le da prioridad

Para implementar eficazmente servicios SASE de alto rendimiento, es fundamental adoptar un enfoque que priorice la nube, tanto para los servicios de SD-WAN como de SSE. Esto garantiza flexibilidad y escalabilidad.

Borderless SD-WAN con gestión alojada en la nube simplifica las operaciones mediante un control centralizado y permite la rápida conectividad de usuarios, dispositivos, sitios y recursos en la nube, a menudo en cuestión de minutos. Con una visibilidad completa y la información que proporciona la IA y el aprendizaje automático (AA) en toda la red (consulta el capítulo 4), los problemas pueden identificarse rápidamente, lo que reduce las incidencias de soporte técnico y minimiza el tiempo necesario para resolverlas. En última instancia, esto ayuda a mantener la productividad para los clientes.

Borderless SD-WAN también emplea una separación clara entre el plano de datos y el plano de control, lo que permite escalabilidad y resistencia. El plano de control, que puede interactuar con protocolos de enrutamiento como Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), se entrega como *software* como servicio (SaaS), lo que elimina las complejidades asociadas a las instalaciones de controladores «hazlo tú mismo» a nivel local, simplificando así la gestión y reduciendo la complejidad. En el capítulo 3 hablamos de este tema con más detalle.

Al establecer una superposición segura independiente de los operadores y transportes, Borderless SD-WAN crea un tejido que tiene en cuenta el contexto para conectar a usuarios remotos, dispositivos del IoT, sucursales/centros de datos y entornos *multicloud*. Además, los servicios de Borderless SD-WAN y SSE se alojan en NewEdge de Netskope con puntos de presencia (PoP) distribuidos geográficamente. Esta proximidad a los usuarios y a las aplicaciones se traduce en rampas de acceso seguro y optimizado a las nubes públicas y privadas, incluidas optimizaciones para aplicaciones exigentes como Zoom y Microsoft 365.

Rampa de acceso a la nube: conectividad segura y optimizada «de cualquiera a cualquiera»

Borderless SD-WAN garantiza una visibilidad completa y una rampa de acceso optimizado para cualquier usuario o sitio, lo que permite una conectividad perfecta a diversas aplicaciones en la nube, de SaaS y aplicaciones privadas.

A través de concentradores en la nube sumamente distribuidos dentro de NewEdge de Netskope, Borderless SD-WAN amplía el tejido SD-WAN de una organización desde las ubicaciones locales (como sucursales, centros regionales, campus, centros de datos, ubicaciones remotas y oficinas móviles) y lo acerca lo máximo posible a los servicios de SaaS y los servicios en la nube para optimizar el rendimiento.

Por ejemplo, tanto si un usuario accede a Zoom desde una ubicación remota con una SD-WAN para *endpoint* como si lo hace desde una sucursal corporativa utilizando la puerta de enlace SASE de Netskope, el tráfico se optimizará para garantizar una experiencia de usuario de alta calidad. Del mismo modo, Borderless SD-WAN en NewEdge proporciona un servicio de media milla altamente optimizado y de baja latencia que conecta sucursales dispersas geográficamente con aplicaciones ubicadas en sedes situadas en distintos continentes.

La estrecha integración de Borderless SD-WAN con SSE, como parte de un marco SASE completo, garantiza una protección integral frente a las ciberamenazas, lo que reduce el riesgo de interrupciones del negocio.

Además de proporcionar funciones de SD-WAN a sucursales y usuarios remotos, Borderless SD-WAN también puede conectar recursos empresariales dispersos en múltiples entornos de nube, incluidos Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP), en un tejido de red unificado. Aprovechando el enrutamiento avanzado y la integración nativa en los proveedores de nube, Borderless SD-WAN establece conexiones sin problemas entre diferentes regiones desde estas plataformas de nube. Además, permite la integración sin esfuerzo con Intelligent SSE de Netskope para las cargas de trabajo en la nube mediante un solo clic.

Acceso inteligente a la red y enrutamiento avanzado

La flexibilidad debe ser un aspecto clave para las empresas a la hora de seleccionar un producto. Borderless SD-WAN de Netskope ofrece un alto nivel de flexibilidad al integrarse perfectamente con Intelligent SSE mediante el acceso inteligente con un solo clic. Esto permite la integración perfecta de Borderless SD-WAN con varios servicios de seguridad, como la puerta de enlace web segura (SWG), el agente de seguridad para el acceso a la nube (CASB), el acceso Zero Trust (confianza cero) a la red (ZTNA), la prevención de pérdida de datos (DLP), la gestión de la posición de seguridad en SaaS (SSPM), la gestión de la posición de seguridad en la nube (CSPM), *firewall* como servicio (FWaaS), etc., proporcionando una protección completa contra los ciberataques.

La integración de la seguridad está disponible tanto a nivel de sucursal, a través de la puerta de enlace SASE, como en cualquier ubicación remota a través de un *software* cliente SASE unificado y ligero que se ejecuta en los portátiles de los usuarios y se usa en los entornos *multicloud*. Esto garantiza la aplicación de medidas de seguridad coherentes y sólidas con independencia de la ubicación o el dispositivo que se utilice. La compatibilidad de Borderless SD-WAN con protocolos de enrutamiento avanzados como OSPF y BGP también permite una integración fluida con la infraestructura empresarial existente. Además, tanto la separación del plano de control y del plano de datos como la distribución de claves a escala de la nube garantizan la simplicidad y escalabilidad del plano de control, que puede entregarse con eficiencia desde la nube.

Seguridad integral de redes híbridas

Esta es la cuestión: adoptar SD-WAN sin seguridad integrada puede resultar muy complejo. Las empresas acaban haciendo malabarismos con dos soluciones distintas, lo que puede ser una pesadilla logística. Esto no solo crea dolores de cabeza en términos de gestión, sino que también puede comprometer la eficacia de los componentes de seguridad y de SD-WAN.

Pero no temas. Borderless SD-WAN adopta un enfoque de seguridad de red híbrida al integrar la seguridad a nivel local y en la nube. Dispone de servicios de seguridad esenciales como el *firewall* de próxima generación (NGFW) y un sistema de prevención de intrusiones/sistema de

detección de intrusiones (IPS/IDS) directamente en la puerta de enlace SASE. Esto significa que el tráfico este-oeste recibe protección justo donde la necesita.

Pero eso no es todo. Borderless SD-WAN va más allá al proporcionar una protección integral de 360 grados mediante servicios de seguridad avanzados que se entregan desde la nube. Piensa en la próxima generación de SWG (NG-SWG), CASB, ZTNA, SSPM, CSPM, FWaaS y mucho más. Es como tener una fortaleza de seguridad que rodea tu red y la defiende desde todos los flancos.

Una experiencia de primera clase al usar cualquier aplicación y en cualquier lugar

Las empresas siempre deben dar prioridad a poder ofrecer a sus usuarios una experiencia coherente, fiable y de alto rendimiento cuando usan las aplicaciones. Esta es precisamente la razón por la que resulta fundamental adoptar Borderless SD-WAN. Permite a las empresas replantearse sus estrategias de red, seguridad y optimización para alcanzar este objetivo.

Borderless SD-WAN ofrece una serie de funciones, como la selección dinámica de rutas, la conmutación por error en una fracción de segundo, la calidad de la experiencia granular teniendo en cuenta el contexto, la corrección de enlaces y la optimización del protocolo de control de transmisión/protocolo de datagramas de usuario (TCP/UDP). Estas funciones funcionan juntas para garantizar un rendimiento y una experiencia de usuario óptimos. Es importante que las empresas no pongan en peligro estas capacidades. Al adoptar Borderless SD-WAN, las empresas pueden transformar su enfoque de las redes y optimizarlo para ofrecer una experiencia de excepcional durante el uso de las aplicaciones.

Contexto para validar la identidad de los usuarios, los dispositivos y los riesgos de las aplicaciones y para mejorar los controles

Borderless SD-WAN se ha diseñado para tener en cuenta el contexto, proporcionando una validación en tiempo real de la identidad del usuario, la información del dispositivo y los riesgos de las aplicaciones. Este conocimiento del contexto permite establecer un verdadero marco de

confianza cero dentro de la red. Borderless SD-WAN destaca además por su capacidad para simplificar la configuración de políticas de calidad de servicio. Las soluciones SD-WAN tradicionales solo detectarían unos pocos miles de aplicaciones, y los administradores de tecnologías de la información (TI) tendrían que configurar individualmente las políticas de calidad de servicio para esas aplicaciones, lo que lleva mucho tiempo.

El motor Zero Trust de Netskope puede detectar hoy en día más de 60 000 aplicaciones, asignando a cada una de ellas un índice de confianza en la nube (CCI) (consulta el capítulo 2). Esta clasificación CCI ofrece una puntuación de lo preparada que está la aplicación para ser utilizada en la empresa. Con Borderless SD-WAN, Netskope aprovecha estas clasificaciones CCI para proporcionar valores predeterminados e inteligentes de la calidad de servicio desde el primer momento. Esto significa que el equipo de operaciones de red ya no necesita configurar manualmente las políticas de calidad de servicio para cada aplicación, lo que ahorra un tiempo y un esfuerzo valiosos.

Las funciones de Netskope para detectar el contexto van más allá de la mera identificación de usuarios y aplicaciones. Se amplían a la detección automática de todos los dispositivos del IoT, ya sean gestionados o no, lo que significa que Netskope puede identificar y gestionar los riesgos asociados a los dispositivos del IoT que se vean comprometidos. Con este nivel de conocimiento del contexto, Netskope puede microsegmentar eficazmente la red basándose en la IA y el AA, aislando y controlando el acceso y el comportamiento de los dispositivos del IoT. Esto ayuda a reducir el impacto que podría tener un dispositivo comprometido, lo que reduce a su vez el riesgo de que se produzca un acceso no autorizado o una violación de la seguridad de los datos.

Operaciones simplificadas, automatizadas e impulsadas por la IA

Imagínate esto: la solución Borderless SD-WAN es tu fiel compañera, siempre dispuesta a echarte una mano. Es como tener un asistente personal que se ocupa de todas las tareas cotidianas, para que tú puedas centrarte en lo que realmente importa. Al automatizar los procesos y aprovechar las operaciones basadas en la IA, esta solución aporta un nuevo nivel de simplicidad a tus tareas de gestión. Ya se trate de dar de alta a clientes, configurar puertas de enlace SASE, gestionar SD-WAN para *endpoints* o lidiar con entornos *multicloud*, puedes hacerlo todo fácilmente desde una plataforma de gestión centralizada.

Pero eso no es todo. El poder del AA entra en juego para hacer que esta solución Borderless SD-WAN sea realmente extraordinaria. La solución aprende de tu red, analiza los flujos de tráfico y entiende tus políticas, lo que significa que puede identificar y resolver problemas de manera proactiva antes incluso de que se conviertan en problemas. Es como tener un equipo de expertos trabajando las 24 horas del día para que todo funcione a la perfección.

Ah, ¿y te hemos hablado de las ventajas de ahorrar tiempo? Con la supervisión autónoma, las anomalías se detectan en un abrir y cerrar de ojos, y tú puedes predecir las posibles infracciones del acuerdo de nivel de servicio (SLA) del proveedor de servicios antes de que estas se produzcan. Podrás resolver los problemas más rápidamente, minimizando el tiempo de inactividad, y volver a la actividad en un santiamén.

Soporte a una estrategia que prioriza lo inalámbrico

Una completa solución Borderless SD-WAN te cubre las espaldas en lo que a conectividad se refiere, ya que brinda un diseño independiente del transporte que se adapta a tus necesidades. Ofrece la flexibilidad de añadir opciones de conectividad 4G/5G, lo que garantiza una conectividad fiable y sin esfuerzo desde cualquier lugar. Una de las grandes ventajas de esta solución es su capacidad para optimizar la intensidad de la señal celular. Así, incluso si te encuentras en una oficina remota o en un espacio de trabajo temporal sin acceso de banda ancha por cable, puedes contar con una conexión sólida y fiable. Esto es ideal en situaciones en las que una conexión de banda ancha por cable puede no estar disponible, no ser la mejor o ni siquiera existir.

Además, esta solución Borderless SD-WAN se ha diseñado teniendo en cuenta la interoperabilidad global de los operadores. Funciona bien con diferentes operadores de todo el mundo, lo que te permite elegir el que mejor se adapte a tus necesidades o funcione mejor en tu ubicación. Tanto si se trata de microsucursales, oficinas de tamaño medio o de grandes entornos corporativos, esta solución tiene la flexibilidad y escalabilidad necesarias para satisfacer tus requisitos de conectividad.

Compatibilidad total con el procesamiento perimetral

Con Borderless SD-WAN, todo gira en torno a la flexibilidad y la eficiencia. Por eso, la orquestación de contenedores cambia las reglas del juego. Te permite gestionar e implementar fácilmente nuevos servicios en la puerta de enlace sin la molestia de mantener un montón de servidores en cada sucursal. Imagina disponer de un contenedor de gestión de la experiencia digital en tu puerta de enlace SASE: supervisar en tiempo real las experiencias de los usuarios se convierte en un juego de niños. También te puede permitir profundizar en los datos del IoT como un profesional. Es compatible con entornos *multicloud* como AWS IoT Greengrass y Azure IoT Hub, para que puedas descubrir y analizar todo lo bueno del IoT en el mismo borde. ¡Eso sí que es bordarlo!

En la figura 6-1 se muestra las diez funciones tratadas en este capítulo.

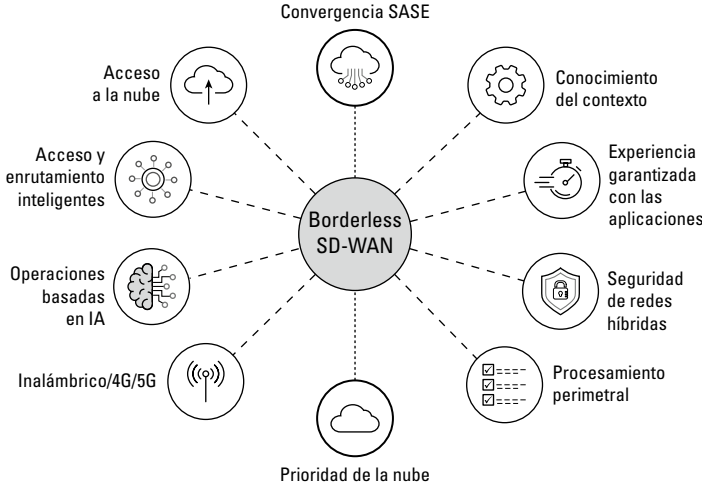


FIGURA 6-1: Diez funciones que pueden ayudar a impulsar el viaje de una organización hacia la adopción de Borderless SD-WAN.

Ready for Anything



Borderless SD-WAN

Netskope, un líder global en SASE, ayuda a las organizaciones a integrar de manera fluida la red y la seguridad, aprovechando AIOps, aplicando principios de confianza cero e innovaciones de inteligencia artificial/aprendizaje automático para asegurar datos con conectividad de alto rendimiento y una protección integral contra amenazas. Rápida y fácil de usar, la plataforma de Netskope proporciona acceso optimizado y seguridad en tiempo real para personas, dispositivos y datos, estén donde estén. Netskope ayuda a los clientes a reducir el riesgo, acelerar el rendimiento y obtener una visibilidad sin igual en cualquier actividad de aplicaciones en la nube, web y privadas. Miles de clientes confían en Netskope y su potente red NewEdge para hacer frente a amenazas en evolución, nuevos riesgos, cambios tecnológicos, organizativos y de red, y nuevos requisitos regulatorios. Para conocer cómo Netskope ayuda a los clientes a estar preparados para cualquier cosa en su viaje SASE, visita netskope.com/es/

Cumple las exigencias de la empresa sin fronteras con Borderless SD-WAN

El perímetro de red de la empresa se ha ampliado con el crecimiento de las microsucursales, la *multicloud*, el trabajo remoto, la telesalud, la flota móvil y el Internet de las cosas (IoT). Hoy en día, los usuarios, los dispositivos, los sitios y las nubes están dispersos, pero conectados de numerosas maneras. Te presentamos Borderless SD-WAN y sus nuevas funciones que te ofrecen conectividad segura, fiable y rápida (basada en los principios Zero Trust), operaciones ampliables que utilizan la IA, experiencia y seguridad de aplicaciones garantizadas para más de 60 000 aplicaciones, compatibilidad ampliada con redes inalámbricas 4G/5G y mucho más.

En el interior...

- Consigue una conectividad rápida y fiable
- Integra la red y la seguridad a la perfección y acelera SASE
- Encuentra seis soluciones y diez funciones para una empresa sin fronteras
- Reduce los costos de TI y gestiona los presupuestos
- Simplifica las arquitecturas y ejecuta operaciones eficientes



Los líderes de Netskope, **Parag Thakore** y **Muhammad Abid**, son expertos reconocidos con múltiples patentes en la informática en la nube, la ciberseguridad y las redes. Con décadas de experiencia en organizaciones globales como Cisco, VeloCloud/VMWare, Infot, Fortinet y T-systems, han sido figuras fundamentales a la hora de redefinir la WAN empresarial e impulsar la adopción de SD-WAN y SASE.

Visita **Dummies.com**[®]

para ver vídeos, fotografías paso a paso, artículos con instrucciones o para comprar.

ISBN: 978-1-394-21954-4

Prohibida la venta



para
dummies[®]

WILEY END USER LICENSE AGREEMENT

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