netskope

White Paper

Su red del mañana

Cuatro principios para el diseño de redes modernas

Flexible

Segura

Índice

Índice

Prólogo:
Nota para los destinatarios

Estamos viendo cómo muchos clientes se encuentran en una encrucijada en cuanto a sus objetivos de red y piden ayuda sobre cómo adaptar la arquitectura actual a las necesidades del mañana. A lo largo de este camino, hemos trabajado con miles de clientes, y en esta guía se resumen los cuatro principios básicos para que los equipos de redes construyan su red del mañana.

La información es el sustento vital de las empresas. Para mantener su ventaja competitiva, las organizaciones diseñan redes empresariales que proporcionen un acceso rápido y fiable a las aplicaciones donde reside la información.

Hoy nos encontramos en una era de cambios rápidos, en la que factores tanto internos como externos generan unas condiciones que hacen que la flexibilidad, y no la eficiencia por sí sola, desempeñe un papel crucial para lograr el éxito o fracasar. Esto supone un cambio radical con respecto a los tiempos en los que se optimizaba la rentabilidad para mejorar los resultados. Para prosperar en estas condiciones, la dirección debe contar con estrategias de TI rentables, flexibles y que se adapten rápidamente a las nuevas exigencias a la misma velocidad a la que avanzan los negocios.

En los últimos años hemos sido testigos de cómo se manifiesta la inflexibilidad. En los inicios del trabajo híbrido, muchas organizaciones no fueron capaces de adaptarse con rapidez, y el capital quedó inmovilizado en diseños de red que suponían que los usuarios y las aplicaciones estaban principalmente en la LAN. Ante una serie de requisitos radicalmente nuevos, las organizaciones se apresuraron a adaptarse.

Existe presión para introducir cambios en la red, pero ¿cuáles son las principales prioridades? Utilice esta guía para planificar su camino hacia una red más rápida, segura y resistente, diseñada para las aplicaciones y los usuarios que dependen de usted.

LAS FUERZAS SECULARES QUE IMPULSAN EL CAMBIO

Para determinar cómo debe cambiar la red, es importante comprender el panorama general y saber por qué debe cambiar. Las siguientes fuerzas seculares están remodelando nuestra forma de vivir y trabajar, y repercuten directamente en las responsabilidades del equipo de TI. Cada factor añade presión para rediseñar la red, y no de una manera insignificante y gradual. Todo esto en su conjunto, está generando una obligación de transformar las cosas.

La transformación digital se ha afianzado en la mayoría de las organizaciones de todo el mundo. Según una encuesta reciente entre varios CIO, el 60 % de las empresas seguirá realizando importantes inversiones en digitalización para mejorar sus capacidades competitivas, permitir una mayor agilidad empresarial y ayudar en la toma de decisiones. [1]

Adopción de la nube

Uno de los aspectos de esta evolución es que las aplicaciones y los datos de las empresas están saliendo cada vez más de las redes y los centros de datos corporativos para trasladarse a la nube. Según Gartner, el 70 % de todas las cargas de trabajo empresariales, frente al 40 % en 2020, formará parte de los servicios de infraestructura y plataformas en la nube para 2028. [2] Además, más del 80 % de todo el tráfico empresarial se dirige a Internet y el 53 % de todo el tráfico web está relacionado con la nube. [3]

Más del 80 % de todo el tráfico empresarial se dirige a Internet y el 53 % de todo el tráfico web está relacionado con la nube.

Expansión de los datos

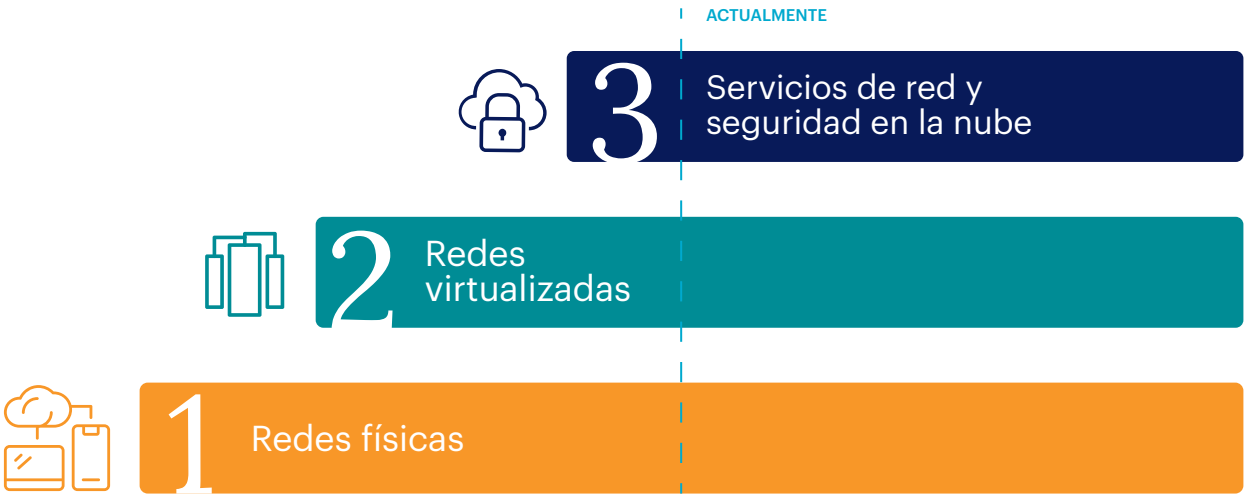
Otro factor crítico es el rápido crecimiento del volumen de datos que se generan. Entre 2020 y 2025, la cantidad de datos en el mundo pasará de 57 zettabytes (ZB) a la asombrosa cifra de 175 ZB. [4] Se están recopilando y compartiendo más datos a través de más puntos de acceso que nunca, y esta información está ampliamente distribuida en redes, nubes y una serie de dispositivos gestionados y no gestionados. Sin una protección específica, estas enormes cantidades de datos distribuidos son bastante vulnerables: más de un tercio (40 %) de las organizaciones sufrió el año pasado una filtración de datos en la nube. [5]

Trabajo híbrido

Un tercer factor que contribuye a la inestabilidad es que una parte importante de la población de usuarios seguirá trabajando fuera de una oficina corporativa tradicional con la expectativa de poder acceder a la información desde cualquier dispositivo y lugar, todo ello sin tener que hacer ninguna concesión de seguridad. A largo plazo se espera que el 50 % de la población activa estadounidense siga trabajando desde casa. [6]

Con estas fuerzas seculares impulsando las razones del cambio, ya va quedando claro qué debemos solucionar. Con este fin, el propio objetivo de la red y cómo debe implementarse está impulsando la tercera era de diseño de las redes empresariales. Ahora está claro que la red existente se ha optimizado para un conjunto de condiciones totalmente diferentes y que debemos resolver rápidamente los retos actuales. De hecho, aferrarse a las arquitecturas de red y seguridad antiguas puede obstaculizar la capacidad para aprovechar las ventajas de la nube y el trabajo híbrido, además de pasar por alto la importancia de conseguir una protección de datos adecuada en todo el panorama empresarial.

LAS TRES ERAS DE DISEÑO DE LAS REDES EMPRESARIALES



Ha habido tres grandes eras que han transformado radicalmente la forma de pensar en el diseño de redes:

1. Redes físicas (jerarquía de 3 niveles / conmutación *spine-leaf*)
2. Redes virtualizadas
3. Servicios de red y seguridad en la nube

La arquitectura básica que se encuentra en el corazón de la mayoría de las redes de nivel empresarial es la red de 3 niveles y sus variantes basadas en la conmutación *spine-leaf*. Se trata de un modelo de prestación de servicios de red probado y bien conocido, que sigue siendo relevante hoy en día.

Actualmente nos encontramos en plena adopción de la segunda era de diseño de redes, las redes virtualizadas , que responden a la creciente necesidad de introducir servicios de red y seguridad para el tráfico este-oeste. En lugar de enviar el tráfico este-oeste al núcleo, las redes virtualizadas implementan servicios de conmutación, enrutamiento y seguridad en el hipervisor o en un cortafuegos virtualizado en modo puente; de esta forma, las redes virtualizadas descargan (pero no eliminan ni sustituyen) la carga de los servicios de red del núcleo.

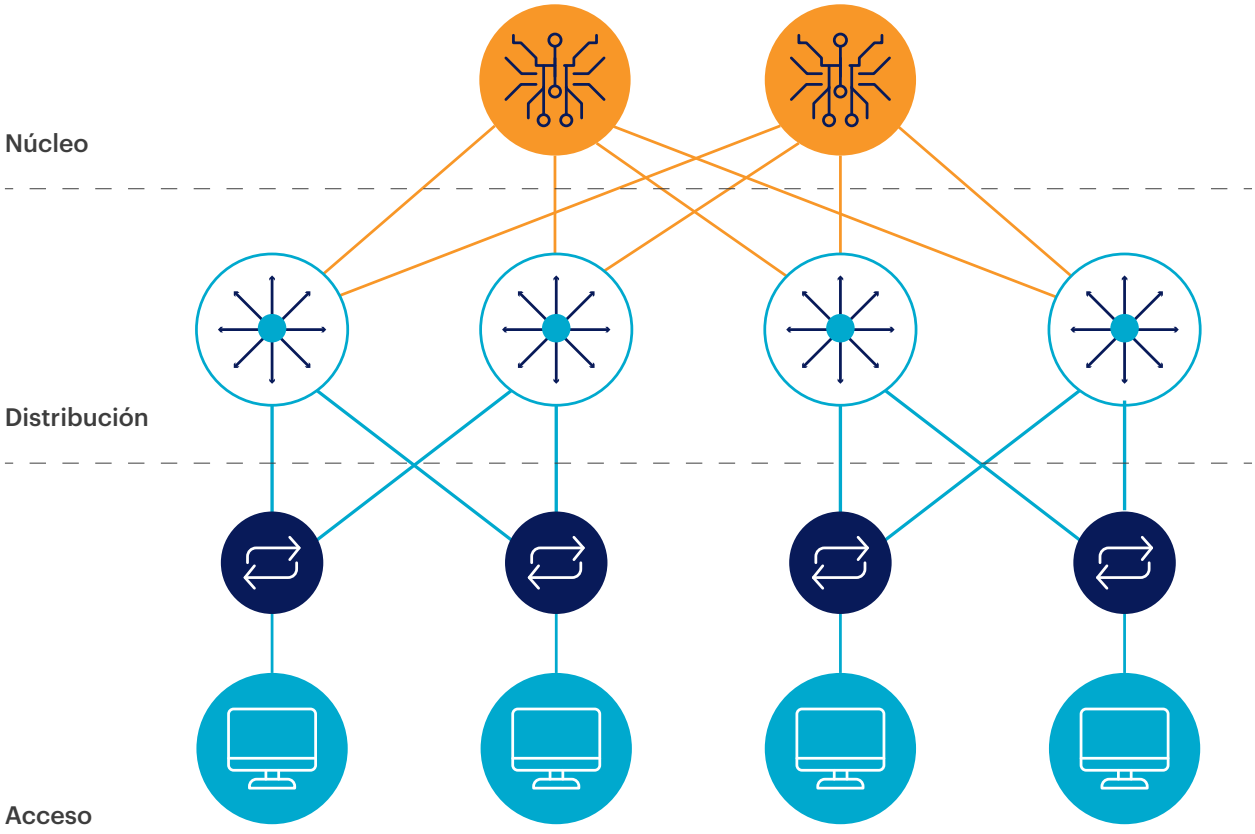
Uno de los aspectos destacables de las dos primeras eras de diseño de redes es que una no sustituye a la otra. La implementación de las redes virtualizadas coexiste con las anteriores redes físicas, pero no reduce ni elimina ninguna parte de su diseño. Por lo tanto, en términos de funcionalidad, la red virtualizada proporciona un enorme beneficio, pero permanece sobre la red física subyacente.

Con la llegada de los servicios de red y seguridad en la nube, ha llegado la tercera era de diseño moderno de redes. A diferencia de las dos primeras eras, los servicios de red y seguridad prestados en la nube brindan a las organizaciones una enorme oportunidad de eliminar la complejidad de las redes empresariales. En lugar de que la organización corra con todos los costes operativos y de capital de los servicios de la red empresarial, la tercera era utiliza servicios prestados en la nube para aumentar la WAN. En el proceso de adopción de los servicios basados en la nube, hay muchas oportunidades de hacer que las redes empresariales sean más eficientes, fiables y seguras restando, en lugar de añadiendo, complejidad. Esto es posible porque los servicios de red y seguridad pueden implementarse como servicios prestados en la nube sin tener que reinventar o rediseñar el diseño de la WAN.

En esta guía, exploraremos el arco del diseño de redes y proporcionaremos orientación a medida que las organizaciones avanzan en su trayectoria con la red.

La primera era: redes físicas (3 niveles / *spine-leaf*)

El concepto básico de la red de 3 niveles concentra los servicios de red de alta potencia en la red central, a la vez que utiliza capas de distribución para establecer la conectividad en todos los lugares donde opera la organización. Desde el punto de vista de las redes, es una arquitectura probada para la conectividad.



Ejemplo de una red física

El diseño tradicional de 3 capas intenta minimizar los costes maximizando la utilización de enrutadores y cortafuegos centralizados, potentes (y caros) en el núcleo. Como tal, la capa central conecta los segmentos de la WAN y sirve de demarcación entre las redes que son fiables y las que no lo son.

La implementación de la seguridad en la red de 3 niveles introduce una serie de complejidades. La seguridad debe inspeccionar sin ralentizar la red. Esto plantea retos arquitectónicos, como dónde introducirse en la arquitectura física. A medida que evolucionan los requisitos, se añaden al diseño de la red otros productos para el cortafuegos, la prevención de intrusiones y los servicios de prevención de pérdida de datos, lo que genera más complejidad operativa y puntos de fallo.

Con la evolución del centro de datos y la necesidad cada vez mayor de acceso a las aplicaciones, la red física de las empresas pasó a adoptar la arquitectura *spine-leaf*. Las arquitecturas *spine-leaf* reducen la latencia en el tráfico este-oeste interconectando los conmutadores *leaf* en una malla completa. En la práctica, *spine-leaf* simplifica un aspecto de la arquitectura (al reducir tres niveles a dos), pero sigue siendo igual de compleja o incluso más en lo que respecta a la seguridad. Incluso con mejoras en la conmutación, ¿en qué punto debe llevarse a cabo la inspección?

La primera era de las redes empresariales destaca por ofrecer conectividad, pero la seguridad sigue siendo difícil de introducir. Se diseñó para facilitar el acceso en lugar de limitarlo. Aislar *hosts* es fácil, pero conectar *hosts* aislados e implementar controles precisos e inspección de contenidos es difícil. La necesidad de un mejor aislamiento marca la pauta de la segunda era de las redes empresariales.

La primera era de las redes empresariales destaca por ofrecer conectividad, pero la seguridad sigue siendo difícil de introducir. Se diseñó para facilitar el acceso en lugar de limitarlo.

La segunda era: redes virtualizadas

Fueron varios los avances importantes que contribuyeron a catalizar y definir la era de las redes virtualizadas. En primer lugar, la virtualización cambió radicalmente la estructura de los centros de datos, aumentando la densidad de *hosts* e introduciendo al mismo tiempo tráfico de máquina a máquina que nunca llega al cable físico. En segundo lugar, el riesgo de que personas malintencionadas dentro de la organización y atacantes se aprovechen de máquinas comprometidas hizo que se prestara más atención al problema del movimiento lateral a través de sistemas con niveles de confianza similares. En tercer lugar, los principios de diseño de confianza cero impulsaron la necesidad de un mayor aislamiento y controles de acceso granulares en comparación con la red plana o la segmentación de red tradicional.

Las redes virtualizadas fueron el nacimiento de la segunda era de diseño de redes. En lugar de intentar forzar todo el tráfico a través del núcleo, las organizaciones empezaron a utilizar una serie de tecnologías superpuestas para añadir controles de red, como la segmentación, sin depender de cambios en la red subyacente. Además, al utilizar la superposición, la red virtualizada mejoraba la red física al permitir introducir la inspección de seguridad en el tráfico este-oeste sin forzar el tráfico por cable. La implementación de estos servicios podría realizarse utilizando redes virtualizadas para dirigir el tráfico a través de cortafuegos virtualizados o añadiendo servicios de seguridad que se enlazan al hipervisor.

Sin embargo, en muchos sentidos la red virtualizada mejoró la capacidad de la organización para poner en práctica más tipos de seguridad, pero seguía enfrentándose a un problema de complejidad. La red virtualizada es una superposición donde coexisten la complejidad de los servicios de red físicos y virtualizados.

La tercera era: servicios de red y seguridad en la nube

Las dos primeras eras de diseño de redes eran totalmente endógenas, lo que significa que el departamento de TI diseñaba, construía y operaba la infraestructura que proporcionaba los servicios de red. Sin embargo, ¿qué ocurre cuando los recursos que se conectan son exógenos a la red empresarial? Esto es precisamente lo que ocurrió cuando los efectos de la nube y el trabajo híbrido cambiaron la propia naturaleza de lo que la red necesitaba conectar y asegurar.

Estas condiciones plantean una pregunta obligada: «¿podrían prestarse los principales servicios de red y seguridad desde la nube, y funcionar conjuntamente con la red empresarial clásica?».

Muchas, si no la mayoría, de las aplicaciones empresariales utilizan la nube de una manera u otra. Forzar el tráfico a través de la red empresarial para llegar a las aplicaciones en la nube es problemático, ya que la organización dispone de un número limitado de puntos de salida y una cantidad fija de capacidad de cortafuegos. En la mayoría de los casos, forzar el tráfico a través de la pila de seguridad de la empresa crea un enrutamiento subóptimo que aumenta la latencia y perjudica a la experiencia del usuario, que se siente frustrado mientras espera que respondan sus aplicaciones.

Mediante el uso de servicios de red y seguridad desde la nube, las organizaciones pueden facilitar a los usuarios acceso a las aplicaciones independientemente de su ubicación, sin forzar el tráfico hacia los recursos locales. Sin embargo, en lugar de tratar el acceso a la nube como un caso de uso aparte, lo que no resulta evidente es que la tercera era brinda la oportunidad de reducir en gran medida la complejidad heredada de las dos primeras eras de diseño de redes.

Tratar la nube como una extensión de la red empresarial (es decir, una red de distribución de redes y seguridad entre iguales) ofrece la oportunidad de eliminar fuentes de complejidad que estaban integradas en la red local. De hecho, los servicios de red y seguridad en la nube desvinculan la necesidad de «añadir» más cosas a la red, porque se elimina la necesidad de forzar el tráfico a través de un dispositivo para implementar nuevos servicios.

El modelo basado en la nube reduce el problema de la red a un primer salto al centro de datos del proveedor de la nube, que ofrece microservicios de seguridad que pueden activarse sin más cambios en la red. Al desvincular los servicios de seguridad de la red, la organización puede poner en marcha redes empresariales más ligeras y fiables con seguridad desde la nube.

«¿podrían prestarse los principales servicios de red y seguridad desde la nube, y funcionar conjuntamente con la red empresarial clásica?».

SASE – UNA IMPLEMENTACIÓN PRÁCTICA DE LOS SERVICIOS EN LA NUBE
SERVICIOS DE RED Y SEGURIDAD

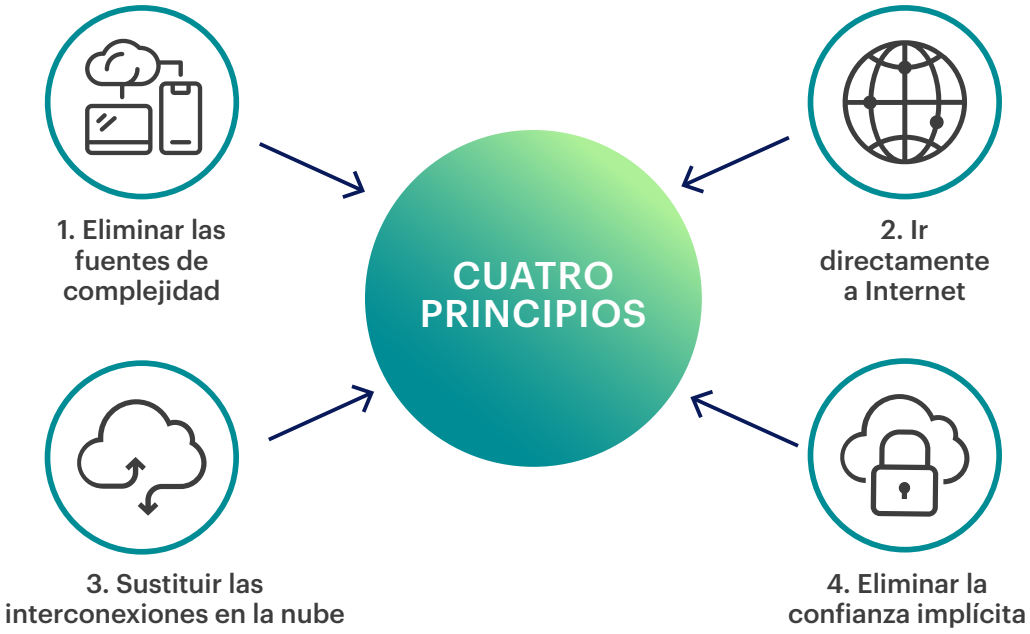
El servidor perimetral de acceso seguro (SASE) es una arquitectura basada en la nube que ofrece servicios de red y seguridad destinados a proteger a usuarios, aplicaciones y datos. Dado que muchos usuarios y aplicaciones ya no residen ni operan en una red corporativa, el acceso y las medidas de seguridad no pueden depender de los dispositivos de *hardware* convencionales del centro de datos corporativo.

SASE ofrece las capacidades de red y seguridad necesarias en forma de servicios en la nube. En lugar de dirigir el tráfico a un dispositivo de seguridad, los usuarios se conectan al servicio en la nube SASE para acceder y utilizar de forma segura servicios web, aplicaciones y datos con un cumplimiento coherente de las políticas de seguridad.

CUATRO PRINCIPIOS PARA IMPLEMENTAR SERVICIOS EN LA NUBE
SERVICIOS DE RED Y SEGURIDAD

A medida que nos adentramos en el comienzo de la tercera era de las redes empresariales, ¿cómo deberían enfocar los arquitectos de redes su estado en el futuro?

Esta guía le ayudará durante el proceso. Estos cuatro principios ayudan a las organizaciones a comprender dónde aplicar cambios significativos para mejorar sus servicios de red:



PRINCIPIO 1: ELIMINAR LAS FUENTES DE COMPLEJIDAD

SASE cambia las reglas del juego en el diseño de redes y abre las puertas a nuevas posibilidades.

Simplifique su arquitectura

Una red bien diseñada debe tener siempre capacidad adicional, porque si funciona cerca de su punto de ruptura, es una receta para el fracaso. Una red resistente tiene que ser capaz de absorber los impactos derivados de su uso, como cuando la mayor parte del equipo de ventas de la empresa se encuentra en la sede central para una conferencia, o cuando la empresa migra hacia o desde una política de trabajo remoto. Incluso en el ciclo normal de funcionamiento de la empresa, cualquier ubicación de la red puede estar relativamente inactiva durante 16 horas fuera de la jornada laboral normal. Pero la capacidad adicional conlleva un coste, porque las redes infrautilizadas siguen necesitando equipos, servicios y personal que, en el mejor de los casos, no se utilizan.

Del mismo modo, la fiabilidad también tiene un coste. La redundancia duplica los gastos en equipos de red, así como en servicios de conmutación por error, que idealmente NO se utilizan si son repuestos en frío o conmutaciones por error pasivas.

Como consecuencia, cada servicio introducido en la red requiere un sobreaprovisionamiento y una sobreingeniería para tener en cuenta la estabilidad, la usabilidad, la fiabilidad y la escalabilidad. Esto no es malo, ya que las organizaciones deben asegurarse de que haya capacidad y fiabilidad en el diseño. La cuestión, sin embargo, es si la introducción en la red es la mejor manera de implementar esos servicios. Si se pudiera «trasladar» la capacidad y el sobreaprovisionamiento y la ingeniería relacionados a la capa SASE, entonces solo se pagaría por lo que se usa cuando realmente se usa.

Una red bien diseñada debe tener siempre capacidad adicional, porque si funciona cerca de su punto de ruptura, es una receta para el fracaso.

La simplificación aumenta la disponibilidad y resistencia de la red existente. Es más fácil conseguir la fiabilidad y elasticidad de un operador si hay menos cosas que se puedan romper.

Para simplificar la red, las organizaciones deben pensar en cómo racionalizar su diseño, conseguir que los servicios y las capacidades se desplieguen más rápidamente, saber cómo abordar nuevas oficinas, sucursales o trabajadores remotos, ir directas a la red para una conectividad más barata y un acceso más rápido a SaaS, o aprovechar nuevas tecnologías, como SD-WAN. Desde este punto de vista, la red empresarial debe centrarse en una conexión sencilla, rápida y fiable, aprovechando al mismo tiempo la capa SASE para una conectividad segura a la nube.

Modernizar diseños anticuados

En las dos primeras eras de los modelos de redes empresariales, los servicios de seguridad en línea requerían la instalación de dispositivos físicos y virtuales en línea. Con el tiempo, la acumulación de distintos servicios de seguridad hizo ineficiente el enrutamiento, como la complejidad creada por el encadenamiento *proxy* de productos de seguridad heredados o la necesidad de tunelizar el tráfico para llegar a una pila de seguridad distante. Estas prácticas siguen utilizándose hoy en día, y muchos proveedores desarrollan productos que utilizan encadenamientos y reenvíos ineficaces en un segundo plano.

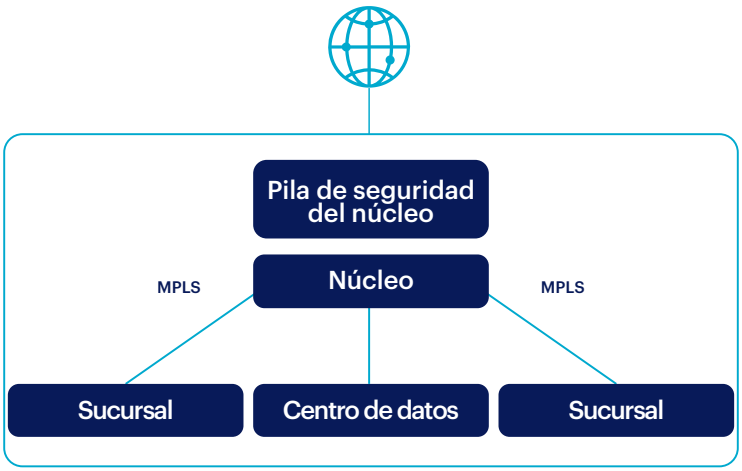
Para modernizar la arquitectura, utilice SASE como red del mismo nivel para implementar servicios en lugar de volver a cablear constantemente la red. Por ejemplo, en lugar de implementar múltiples puertas de enlace encadenadas para abordar los múltiples carriles de tráfico de Internet, web y nube, la capa SASE ofrece SWG, Cloud Firewall y CASB que pueden implementarse desde el mismo primer salto. El despliegue del primer producto en línea permite añadir otros activando servicios en lugar de introducir más dispositivos de seguridad en la red.

Tenga en cuenta que a medida que la prestación de servicios de seguridad se desplaza a la capa SASE, la red subyacente se vuelve más segura en virtud de la eliminación de rutas y excepciones de políticas. Esto se debe a que los controles de acceso a la red heredados dependían de la aplicación de decisiones sobre políticas en la red, mientras que la red moderna las elimina. Por ejemplo, los controles de acceso a la red heredados suelen basarse en políticas de cortafuegos para segmentos o zonas de la red. Cada «permiso» puede tener consecuencias imprevistas, especialmente si se tiene en cuenta el «grano grueso» de las segmentaciones de red. Al eliminar las decisiones políticas de la capa de red, la superficie de ataque se reduce y se contrae para adaptarse a las decisiones políticas de «grano fino» de SASE.

A medida que las organizaciones evolucionan para añadir nuevas capacidades de seguridad, como la protección de datos y la protección frente a amenazas, dichos servicios pueden activarse desde la plataforma SASE.

PRINCIPIO 2: IR DIRECTAMENTE A INTERNET

Las redes de área extensa utilizan diseños radiales por varias razones. En parte, antes era necesario enrutar todo el tráfico a través del núcleo para llegar al centro de datos interno. También era un diseño lógico introducir seguridad en el limitado número de puntos de salida.



Con el traslado de las aplicaciones a la nube, las empresas empezaron a esforzarse por adoptar un enfoque directo a Internet. Mediante una conexión a Internet en la sucursal, el tráfico destinado a la nube e Internet podría descargarse de la red MPLS. El problema es que los cortafuegos de bajo coste de las sucursales rara vez ofrecen el mismo nivel de seguridad que el cortafuegos perimetral, lo que hace que las políticas de seguridad se apliquen de forma incoherente. Incluso si la organización compra el mismo cortafuegos perimetral para la sucursal, el trabajo de mantenimiento de las cajas de la sucursal sobrecarga a los equipos de red. O peor aún, se pone en manos de empleados de la sucursal sin conocimientos técnicos y sin experiencia en la gestión de cortafuegos o el control de la seguridad física de los dispositivos. Como consecuencia, resolver un problema en la red crea otro problema operativo, posiblemente peor.

Utilizar SASE para ir directamente a Internet

Son varios los aspectos del modelo SASE que permiten lograr sencillez, modernización y optimización en las redes de sucursales mediante la implementación de una conexión directa a Internet. Hay que tener en cuenta que los dos principales obstáculos a la hora de sustituir MPLS son: (1) la inestabilidad y los problemas de fiabilidad de la Internet abierta, y (2) la aplicación de una seguridad coherente sin equipos caros y de alto mantenimiento en la sucursal. Estos retos se superan ofreciendo los servicios de red y seguridad a través de SASE.

Para superar los problemas de inestabilidad y fiabilidad de la Internet abierta, utilice múltiples conexiones (incluida una Internet de bajo coste) que estén orquestadas y gestionadas a través de SD-WAN. SD-WAN mantiene la estabilidad de la sesión incluso cuando se produce una congestión o un fallo del enlace, ya que puede garantizar que la sesión permanezca activa mientras realiza los ajustes respectivos para optimizar el rendimiento. Como esto ocurre de forma transparente, las conexiones SD-WAN mantienen las aplicaciones en funcionamiento sin interrupciones, ya que el tráfico aprovecha la conexión directa a Internet.

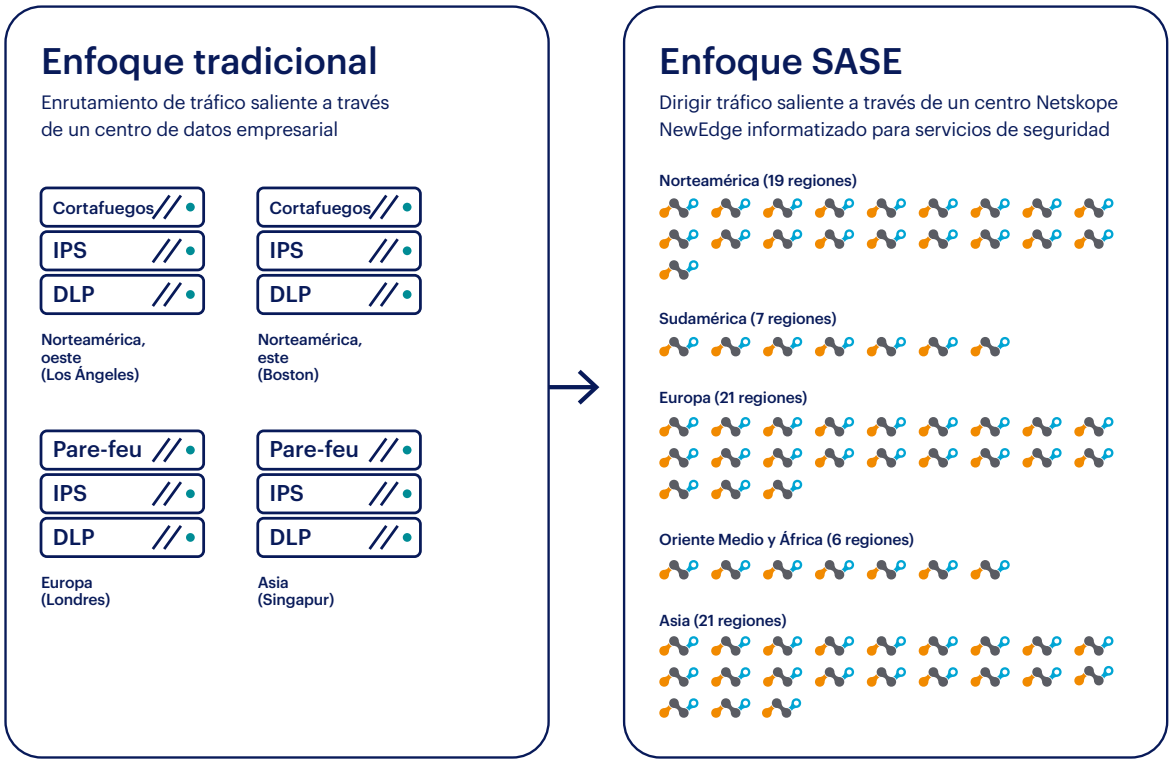
Para superar el problema de incoherencia en la seguridad, las organizaciones utilizan la implementación de SD-WAN con SASE para ofrecer seguridad en lugar de confiar en el cortafuegos local. Así, al descargar los servicios de seguridad de la sucursal, la labor principal del dispositivo local es mucho más sencilla. El dispositivo SD-WAN local establece la red para dar el primer salto a la nube SASE con el fin de establecer visibilidad y seguridad a medida que las organizaciones utilizan las aplicaciones. Así, las organizaciones no necesitan mantener costosos cortafuegos en la sucursal.

Tenga en cuenta que la aplicación de las tecnologías SD-WAN no se limita únicamente a la sucursal. Cada vez se depende más de aplicaciones en la nube, especialmente de aquellas que incluyen comunicaciones en tiempo real, como las funciones de colaboración y vídeo, lo que también tiene repercusiones sobre la conectividad a disposición de los usuarios cuando trabajan a distancia. A medida que su organización evalúe SD-WAN, piense si tiene sentido utilizar múltiples enlaces desde el terminal a Internet (como banda ancha junto con un módem 5G) para mejorar la estabilidad de las aplicaciones críticas.

Distribuir el acceso a los servicios de seguridad para reducir la latencia

En general, la mayoría de las organizaciones tienen límites físicos y económicos en cuanto al número de centros de datos que pueden operar y al número de puntos de salida que pueden mantener. Por ejemplo, una gran organización podría implementar cuatro grandes centros de datos para cubrir todo el mundo (dos en Norteamérica, uno en Europa y uno en Asia) y exigir que todas las sucursales se conecten a uno de estos centros. Añadir un quinto o sexto emplazamiento conllevaría un coste prohibitivo, lo que lleva a un tope de cobertura en el que la empresa simplemente tolera un enrutamiento subóptimo hasta que pueda justificar el coste de abrir otro centro de datos para aliviar la carga.

La consecuencia de un tope de cobertura es que solamente una parte de los miembros de la organización está cerca de un punto de salida, y todos los demás aceptan un cierto grado de latencia. Cuanto más lejos esté el usuario o la oficina del centro de datos, más latencia experimentarán los usuarios, lo que resulta especialmente problemático con trabajadores muy móviles.



Los datos más actualizados están disponibles en https://trust.netskope.com/

Prestación de servicios SASE

Con SASE, la carga de la creación y el aprovisionamiento de la cobertura se traslada al proveedor de SASE, que es el encargado de dar la cobertura que se ofrece a sus clientes. Esto permite superar el tope de cobertura, porque el proveedor de SASE suele tener centros en muchas más regiones que una empresa media. El resultado neto es que la organización tiene más cobertura global de la que podría mantener por sí sola, sin la carga de gestionar centros de datos globales.

PRINCIPIO 3: SUSTITUIR LAS INTERCONEXIONES EN LA NUBE

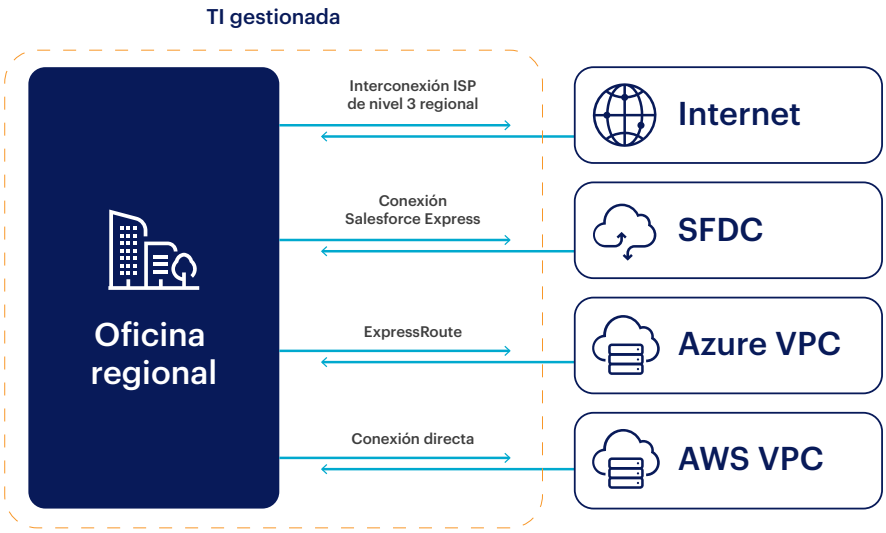
Los servicios de red que utilizan las organizaciones para conectarse a Internet, crear su WAN y ampliar el acceso a la nube dependen de servicios prestados por proveedores locales. Sin embargo, estos servicios no son universalmente homogéneos en todo el mundo. Los proveedores de servicios variarán de un mercado a otro, el nivel de servicio será diferente y los precios impondrán límites técnicos y económicos a la capacidad de la organización para prestar servicio en distintas zonas geográficas.

El enlace a Internet suele ser el más rentable, con la salvedad de que los servicios de Internet no son tan fiables ni llevan implícita la privacidad de un enlace dedicado. Con la explosión de la informática en la nube, las empresas tenían un número cada vez mayor de aplicaciones críticas para el negocio que eran externas a su red. Dada la incertidumbre que a menudo generaba el uso de Internet para acceder a la nube, las interconexiones en la nube como ExpressRoute para Azure, Direct Connect para AWS o Express Connect para Salesforce se hicieron populares para dar soporte a aplicaciones críticas en la nube.

La idea original era vincular las comunicaciones nube->centro de datos de forma similar a las comunicaciones centro de datos->centro de datos.

La primera oleada de interconexiones en la nube estableció el modelo de arquitectura de nube híbrida (es decir, el uso de la nube pública como extensión del centro de datos de la nube privada local). La idea original era vincular las comunicaciones nube->centro de datos de forma similar a las comunicaciones centro de datos->centro de datos.

Con el tiempo, el uso de las interconexiones se extendió. Por ejemplo, Salesforce es tan esencial para que las organizaciones realicen transacciones con sus clientes como una aplicación local, por lo que requiere un enlace dedicado para obtener velocidad y un acceso fiable desde la WAN. El problema es que las organizaciones tienen muchas aplicaciones SaaS y muchas de ellas son críticas para el negocio, por lo que cabría preguntarse cuáles deben tener una interconexión y cuáles una ruta a través de la Internet abierta. Además, la cobertura mundial también es un problema. Si una oficina regional no tiene una opción local para la interconexión en la nube, ¿debe esa organización dirigir internamente el tráfico a una ubicación que sí la tenga, o debe seguir adelante y utilizar la Internet abierta?



Interconexión de nube tradicional gestionada por TI a través de enlaces dedicados de alta disponibilidad

El argumento de la seguridad se utiliza a veces como justificación para añadir más enlaces de interconexión a la nube. Por ejemplo, si todo el tráfico a una aplicación se enruta a través de un enlace dedicado, el acceso a Internet podría eliminarse, reduciendo así la exposición a vulnerabilidades de preautenticación o intentos de rellenar la autenticación con credenciales. Si el origen del tráfico procede de la WAN interna y no de Internet, el acceso a la aplicación sería al menos tan seguro como la WAN.

Sin embargo, esta seguridad es solo relativa, ya que sigue siendo posible que un actor malintencionado opere en la WAN y pueda desplazarse lateralmente a la interconexión. Así, las organizaciones siguieron complicando aún más la arquitectura de interconexión de la nube añadiendo *hosts* bastión delante de la interconexión de la nube y exigiendo a los usuarios externos que utilizaran VPN para llegar a ella.

Lo que ha quedado claro es que conectar la WAN a la nube a través de interconexiones no es escalable ni sólido desde el punto de vista de la arquitectura. Un mejor enfoque es aprovechar la seguridad y las redes de la capa SASE para obtener un acceso seguro y de alto rendimiento a las aplicaciones en la nube en distintas partes del mundo.

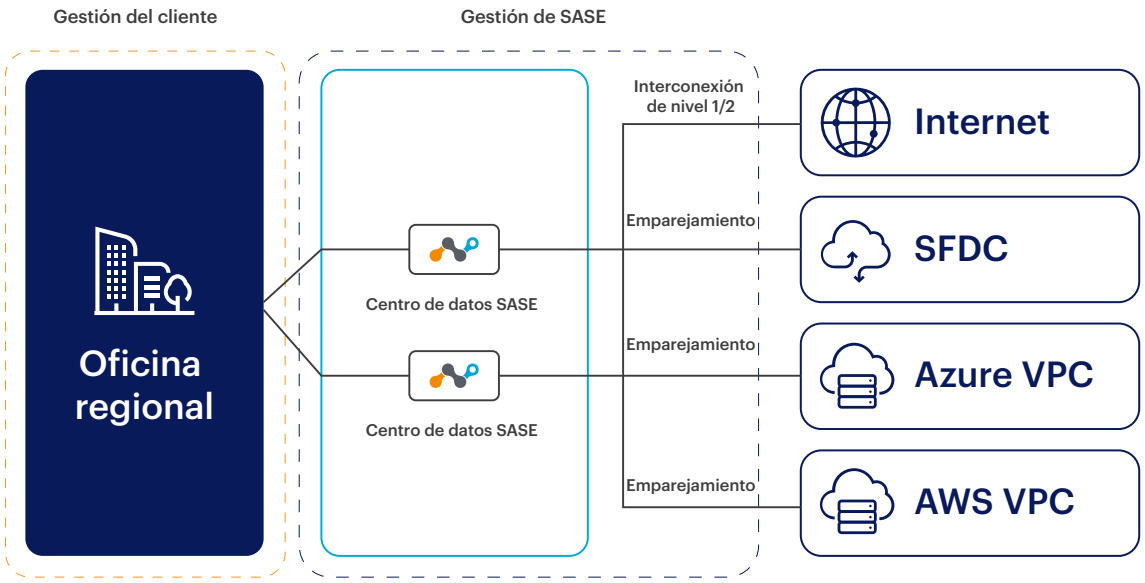
Con la explosión de la informática en la nube, las empresas tenían un número cada vez mayor de aplicaciones críticas para el negocio que eran externas a su red.

Uso de emparejamiento SASE como alternativa a las interconexiones en la nube

En lugar de obtener y mantener interconexiones en la nube de una multitud de proveedores de servicios regionales, plantéese la posibilidad de utilizar el emparejamiento SASE con proveedores de nube para obtener un acceso fiable, seguro y de baja latencia a las aplicaciones de la nube. Este enfoque reduce en gran medida el coste y la complejidad al descargar la complicada arquitectura de prestación de servicios al proveedor de SASE.

No todos los proveedores de SASE son iguales en este sentido. Por ejemplo, un proveedor podría optimizar únicamente el tiempo de procesamiento dentro de su propio centro de datos, sin pensar en cómo ofrecer el mejor tiempo de ida y vuelta al usuario. Como resultado, no todas las salidas del centro de datos SASE son iguales. Es importante verificar que el proveedor de SASE elegido optimice la seguridad y el rendimiento de la red.

Cuando se hace correctamente, TI dirige el tráfico al centro de datos de un proveedor de SASE para aprovechar sus interconexiones y el emparejamiento a los principales proveedores de nube, así como al resto de Internet. Puede ofrecer una cobertura y unas velocidades constantes en comparación con las variaciones a las que normalmente se enfrenta TI con los proveedores de redes regionales.



PRINCIPIO 4: ELIMINAR LA CONFIANZA IMPLÍCITA

La seguridad perimetral separa las entidades externas y no fiables de Internet de las de la red interna. Este modelo es razonable en el nivel más grueso de segmentación (interno frente a externo) porque puede utilizarse para controlar la política entre actores externos y recursos internos, y actores internos con recursos externos.

Sin embargo, una vez que el usuario está dentro del perímetro, hay pocos controles que impidan el acceso a los recursos internos. Como subproducto, la red interna a menudo tiene niveles excesivos de confianza implícita que asume que todos los usuarios internos son «dignos de confianza». Por supuesto, confianza es un término relativo, dado que se asume, aunque no se garantiza, que los usuarios internos no perjudican a la empresa.

Para corregir los problemas de la confianza implícita, muchas empresas han intentado introducir una serie de tecnologías de seguridad en la red para mantener el control:

1. NAC para imponer la autenticación a nivel de dispositivo y la aplicación de políticas L2 para el acceso a la red
2. VPN para conectar dispositivos remotos a la red local a través de un túnel
3. Segmentación de red para una separación de granularidad gruesa de las funciones de red y las zonas de seguridad, como el centro de datos frente a LAN, o el servidor web frente al servidor de base de datos
4. VLAN para la separación lógica de grupos funcionales, por ejemplo, separar el marketing de la contabilidad
5. Políticas de comprobación de *host* para verificar la configuración del dispositivo y el nivel de parches
6. Autenticación de dos factores para reducir el riesgo de robo de credenciales

Todas estas tecnologías, aunque bienintencionadas, pretenden eliminar parte de la confianza implícita, pero como consecuencia añaden más complejidad a la red. Peor aún, siguen existiendo lagunas de seguridad. Por ejemplo, si las políticas de autenticación de dispositivos y de identidad de usuarios se aplican por separado, es posible que un dispositivo controlado de forma remota realice un escaneado de puertos de la red e identifique servidores con vulnerabilidades sin parches incluso sin ninguna credencial de identidad. Y muchas de estas tecnologías de seguridad, como NAC y VPN, no son relevantes cuando se accede a aplicaciones en la nube.

En términos de objetivos de diseño, eliminar la confianza implícita en realidad hace que la red sea más sencilla de manejar, por varias razones.

Hoy en día, lo que ha quedado claro es que no se puede añadir suficiente seguridad para eliminar la confianza implícita. En primer lugar, se debe crear confianza a partir de la red. En lo que respecta a los objetivos de diseño, eliminar la confianza implícita en realidad hace que la red sea más sencilla de manejar, por varias razones.

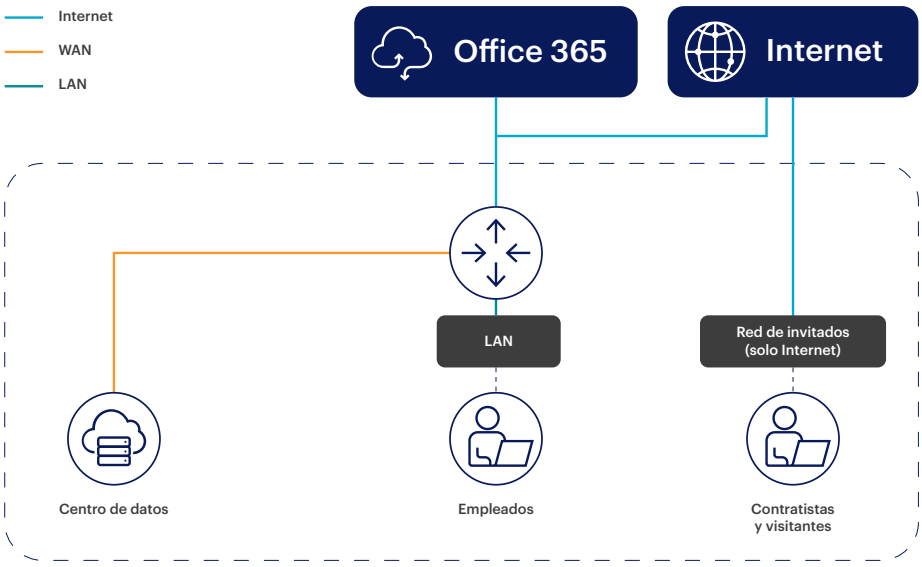
- Los controles de políticas pueden implementarse desde la capa de seguridad en lugar de intentar tomar decisiones de permiso/denegación en el diseño de la red.
- La red es más fiable si hay menos aparatos o servicios de seguridad que deban gestionarse.
- Muchas rutas de salida a diferentes segmentos de red y aplicaciones pueden consolidarse en un primer salto a la capa de los servicios de seguridad.
- Muchas rutas de entrada pueden eliminarse por completo, reduciendo así la capa de superficie de ataque expuesta y el potencial de errores de política o abuso de credenciales robadas.

Los equipos de red pueden tomar medidas para eliminar las fuentes de confianza implícita:

- Desarrollar la LAN: minimizar o eliminar el acceso externo y no conceder ningún privilegio adicional por conectarse desde la LAN.
- Enrutar todo el tráfico de aplicaciones gestionadas a través de SASE.
- Acceso con intermediarios y cumplimiento de la autenticación / identificación con SASE en lugar de depender de NAC/802.1x/VPN.
- Replantearse la DMZ

Desarrollar la LAN

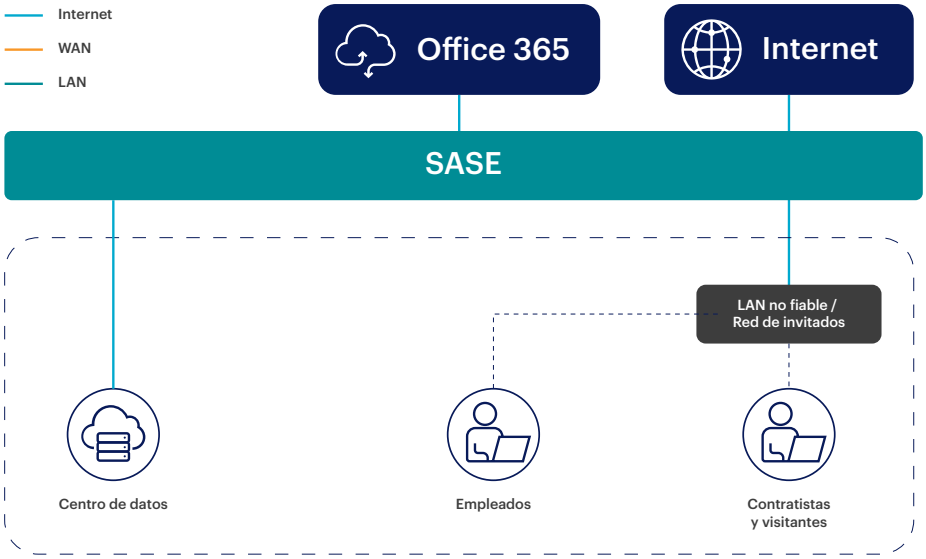
La LAN es la puerta de entrada para que los *hosts* locales accedan a la red corporativa y al centro de datos y, sin embargo, sigue siendo una fuente problemática de confianza implícita. Durante años, la única protección de la LAN era el vigilante de recepción y el lector de tarjetas de acceso al edificio. Sin embargo, una vez dentro del edificio, un dispositivo podía conectarse a la LAN con amplios niveles de acceso a la red, normalmente por encima de lo que el usuario realmente necesitaba. Aunque se ha trabajado para controlar los dispositivos en las redes, muchas redes empresariales son sumamente vulnerables a los ataques desde dentro, ya sea por parte de una persona con información privilegiada o de un atacante que opera desde un dispositivo comprometido. Una vez dentro de la LAN, un malhechor suele encontrar poca resistencia a la hora de mapear el resto de la red y comprometer otros *hosts*.



¿Son necesarios hoy en día amplios niveles de acceso a la red en la LAN? En el pasado, era habitual utilizar la LAN para llegar a las aplicaciones del centro de datos y habilitar funciones de grupo de trabajo, como archivos compartidos, herramientas de colaboración y comunicaciones en tiempo real. Hoy en día, en general, estos servicios han evolucionado hasta convertirse en equivalentes basados en la nube que ya no requieren amplios ni excesivos servicios LAN.

Modelar la LAN como red de invitados para todos los usuarios

Afortunadamente, el modelo para eliminar la confianza implícita de la LAN ya existe en la mayoría de las redes empresariales. Es la red de invitados. La función de la red de invitados es proporcionar conexión a Internet a personas que no son empleados, como contratistas y visitantes. No permite el acceso al centro de datos ni a otros recursos de la LAN.



Hoy en día, la conectividad a Internet es en realidad lo único que necesita la mayoría de los empleados locales para utilizar sus aplicaciones. Con el trabajo híbrido, la oficina no es diferente del usuario remoto, dado que se accede a las aplicaciones en la nube.

Por tanto, no es necesario conceder a los usuarios más acceso a la red solamente porque trabajen desde la oficina. De hecho, con el trabajo híbrido la red de la oficina empieza a parecerse a espacios de trabajo compartidos en los que usuarios de diferentes organizaciones utilizan una red compartida sin confianza implícita entre *hosts*.

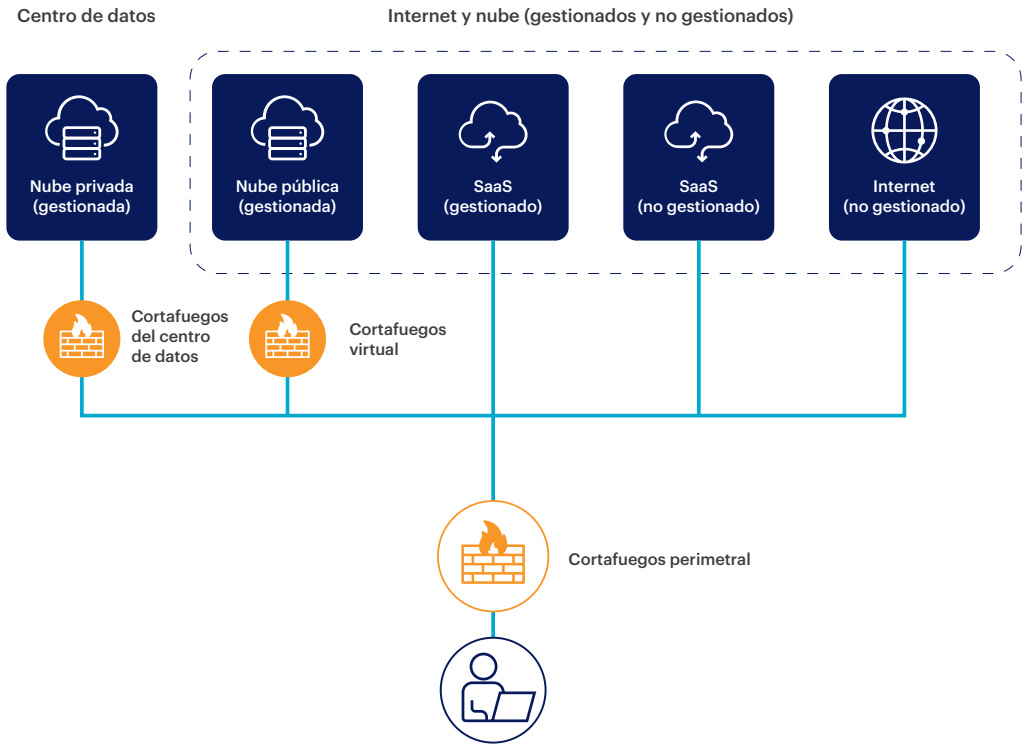
Al permitir a los empleados trabajar desde cualquier lugar, está desapareciendo la distinción entre estar en una red fiable y otra que no lo es.

Al permitir a los empleados trabajar desde cualquier lugar, está desapareciendo la distinción entre estar en una red fiable y otra que no lo es. Al trabajar desde casa, una cafetería o un espacio de trabajo compartido, el usuario pasa la mayor parte del tiempo en redes que no son fiables. Es lo mismo que tener a los empleados en una LAN no fiable o en una red de invitados mientras están en la oficina.

Aplicaciones gestionadas y no gestionadas entremezcladas

En el pasado, tenía sentido delimitar el perímetro como la frontera entre la red fiable y la no fiable. Con los datos, el perímetro se desplaza ahora para aplicar controles entre aplicaciones fiables y no fiables, por lo que tiene que asegurarse de que sus datos no se muevan a lugares donde no pueda controlarlos.

Sin embargo, los dispositivos de seguridad convencionales no están bien preparados para distinguir entre las aplicaciones o instancias que se gestionan y las que no. El creciente número de excepciones a la visibilidad crea una situación peligrosa en la que las aplicaciones gestionadas y no gestionadas son indistinguibles entre sí, y no existen controles para detener el movimiento de datos no deseados.



Usar SASE como perímetro para aplicaciones gestionadas

En lugar de intentar forzar el tráfico gestionado a través de un cortafuegos en el centro de datos, piense primero en lo que sus aplicaciones gestionadas necesitan para la seguridad y dónde residen esas aplicaciones.

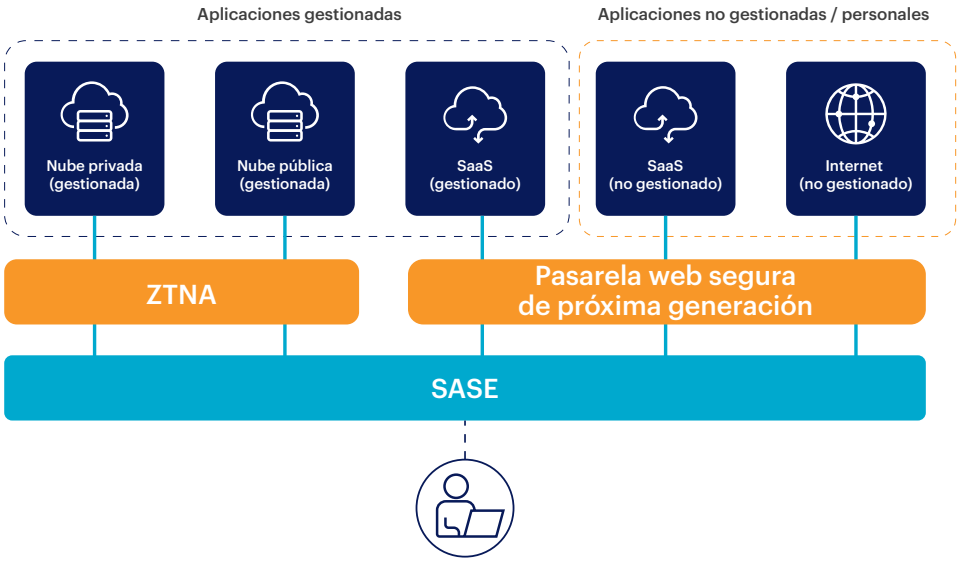
Por ejemplo, si clasifica sus aplicaciones como gestionadas o no gestionadas, queda bastante claro que muchos servicios de seguridad deben prestarse en el centro de datos, la nube pública y SaaS.

El creciente número de excepciones a la visibilidad crea una situación peligrosa en la que las aplicaciones gestionadas y no gestionadas son indistinguibles entre sí, y no existen controles para detener el movimiento de datos no deseado.

Ejemplos de asignaciones: aplicaciones gestionadas frente a aplicaciones no gestionadas

TIPO DE APLICACIÓN	UBICACIÓN	EJEMPLOS DE APLICACIONES	REQUISITOS CLAVE DE SEGURIDAD
APLICACIONES GESTIONADAS	Centro de datos	Base de datos Oracle	• Acceso seguro • Protección de datos • Análisis del comportamiento
	Nube pública	AWS/Azure	
	SaaS	Office 365 Google Workspace Salesforce Workday GitHub	
APLICACIONES NO GESTIONADAS / PERSONALES	SaaS	Microsoft 365 Google Workspace Dropbox Zippyshare	• Calificación del riesgo • Política basada en el riesgo • Detección de instancias • Protección frente a amenazas • Protección de datos • Análisis del comportamiento • Orientación para el usuario final
	Internet	Web Fuera de la web (FTP, SSH, RSH, etc.)	

El camino a seguir consiste en pensar en cómo controlar los datos de sus aplicaciones gestionadas y ofrecer la seguridad necesaria allí donde sea preciso. Al enrutar todas sus aplicaciones gestionadas a través de SASE, puede garantizar un acceso seguro, protección de datos y capacidades de análisis de comportamiento. De forma similar, todo el tráfico de las demás aplicaciones puede tratarse como no gestionado o personal, con políticas establecidas para evitar el movimiento de datos no deseado.



Acceso con intermediarios y cumplimiento de la autenticación / identificación con SASE en lugar de depender de NAC/802.1x/VPN

El matrimonio entre identidad y trabajo en red tiene una larga y accidentada historia. Hoy en día, las redes aplican políticas de identidad en diferentes capas de la conexión de red. Metafóricamente, cada medida de seguridad actúa como una puerta antes de permitir que una conexión se lleve a cabo, con poco o ningún conocimiento de la decisión política anterior o posterior. Por ejemplo, NAC establece si un dispositivo tiene permiso para conectarse a la capa de acceso de la red, pero en la capa 2 no podría determinar si el usuario del dispositivo está autorizado a acceder a una aplicación determinada. Así, el campo de visión de NAC es únicamente determinar si un dispositivo está permitido en la red, pero no lo que puede hacer en ella.

En efecto, estas tecnologías intentan mitigar la confianza implícita en la red creando barreras adicionales a los recursos protegidos. Esto sigue siendo problemático por varias razones:

1. Cualquier nivel de acceso deja la red abierta a abusos. Por ejemplo, el mero hecho de estar conectado a la red sin las credenciales de la aplicación deja la puerta abierta a la vigilancia, el escaneado de puertos de otros *hosts*, la comprobación de software sin parches, el robo de credenciales y las vulnerabilidades de preautenticación en sistemas vulnerables.
2. Colocar controles de identidad en las capas de red no es útil cuando ni el usuario ni la aplicación están en la red. Sería ineficaz enrutar el tráfico a través de la red para obtener estos servicios de identidad. Por lo tanto, el uso de controles de identidad con las aplicaciones gestionadas debe tener en cuenta los escenarios de trabajo desde cualquier lugar.

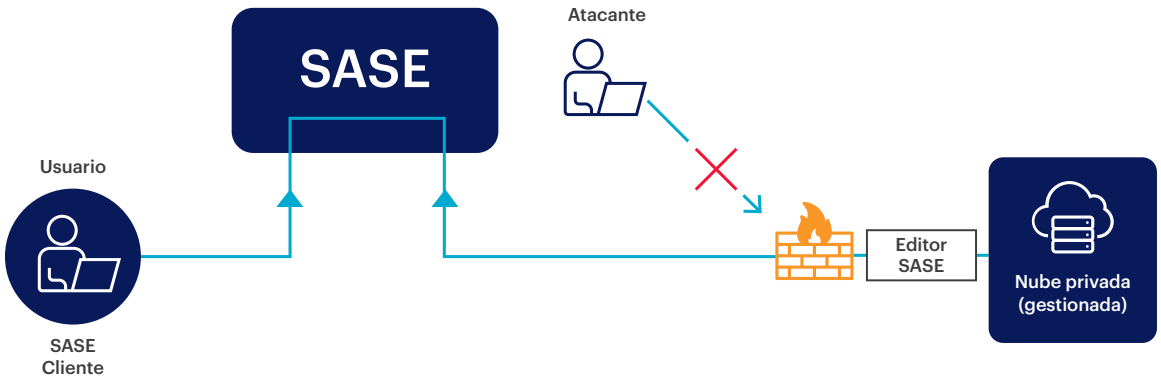
Usar SASE para aplicar políticas basadas en la identidad

En lugar de bloquear las conexiones de red a una aplicación, tiene más sentido aplicar el acceso de red de confianza cero (ZTNA) a las conexiones mediante intermediarios con criterios de identidad a fin de ofrecer controles de usuario->aplicaciones y crear conectividad a través de la infraestructura SASE.

Como ya se ha mencionado, al reducir la confianza depositada en la LAN interna, la organización reduce drásticamente la superficie de ataque. Con todos los usuarios limitados únicamente a Internet y sin enrutamiento interno a las aplicaciones gestionadas, no hay que recuperar ninguna confianza implícita.

El puente entre los usuarios y las aplicaciones es la superposición SASE para implementar ZTNA, que no solo comprueba las políticas de identidad y los criterios para permitir el acceso, sino que también conecta dos conexiones de salida. Lo bueno del enfoque de acceso la red de confianza cero es que las políticas de cortafuegos de la red también resultan mucho más sencillas en el centro de datos. Por parte de la aplicación, basta con bloquear todo el tráfico entrante. Esto significa que no hay ninguna puerta de enlace para sondear, ningún servidor visible expuesto ni nada para escanear los puertos. Si no hay ningún tráfico entrante, la superficie de ataque desaparece.

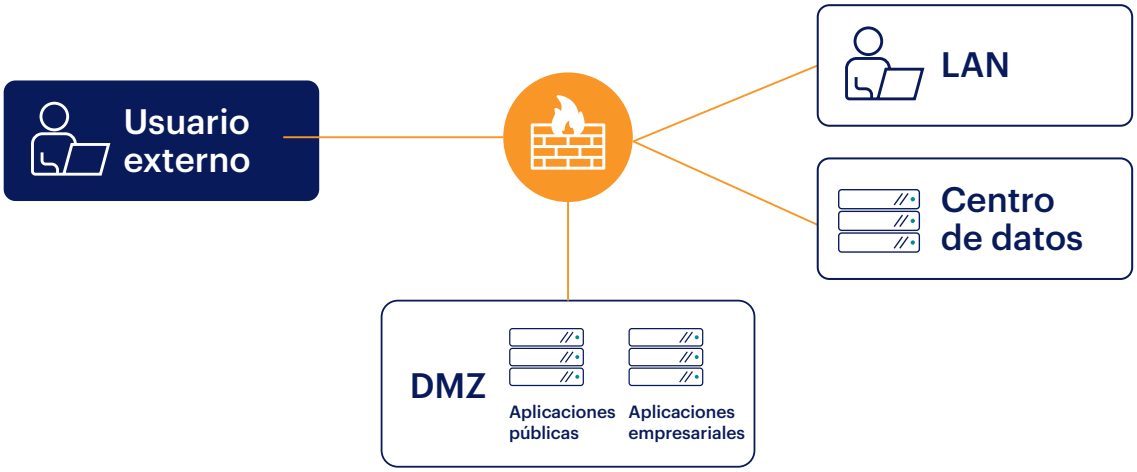
Lo bueno del enfoque de acceso a la red de confianza cero es que las políticas de cortafuegos de la red también resultan mucho más sencillas en el centro de datos.



Replantearse la DMZ

La DMZ de red proporciona un método para exponer los recursos internos al público, pero, ¿es realmente necesaria hoy en día? En su momento, fue una forma útil, aunque imperfecta, de exponer una red gestionada a Internet para permitir una serie de casos de uso, entre ellos:

- **Para aplicaciones personalizadas de cara al público:** los servidores web y de aplicaciones situados en la DMZ podían ser utilizados por el público.
- **Para aplicaciones empresariales utilizadas por empleados y contratistas:** aplicaciones que se ejecutan en la DMZ o que proporcionan un acceso limitado al centro de datos.



Pero la DMZ es un lugar peligroso, ya que permite al público interactuar con servidores que tienen acceso a recursos internos. Cualquier vulnerabilidad de seguridad o error de configuración de las políticas que sea público podría ser el catalizador de una filtración. Como consecuencia, las organizaciones tienen que dedicar un enorme capital a configurar y mantener la DMZ:

- Uno o varios pares de cortafuegos de red de alta disponibilidad para establecer la red de DMZ
- Equilibradores de carga para soportar y distribuir el tráfico legítimo
- Filtrado DDoS en la red, así como en fases anteriores, para filtrar los intentos de saturar las interfaces de los servidores en la DMZ
- Prevención de intrusiones para eliminar los intentos de explotar una vulnerabilidad no parcheada
- Cortafuegos de aplicaciones para filtrar las entradas maliciosas a las aplicaciones, como la inyección de SQL y *scripting entre* sitios

Incluso una DMZ bien gestionada, con una supervisión cuidadosa y una configuración basada en las mejores prácticas puede sufrir vulnerabilidades. Cualquier sistema en la DMZ forma parte de la superficie de ataque, que podría ser explotada externamente por usuarios no autenticados.

Alternativas arquitectónicas a la DMZ

En lugar de gestionar y proteger la DMZ, resulta práctico evaluar si sus aplicaciones necesitan operar desde la DMZ en primer lugar. En general, la nube ha cambiado el panorama de las aplicaciones DMZ tradicionales, especialmente en el caso de las aplicaciones de cara al público. Esto se debe a que los servicios creados con fines específicos, como las aplicaciones alojadas o SaaS, ofrecen capacidades de aplicación similares o iguales sin tener que gestionar el entorno operativo.

No obstante, la cuestión sigue siendo qué hacer con las aplicaciones empresariales para empleados y contratistas. Las aplicaciones personalizadas pueden trasladarse a la nube pública o privada, pero el acceso a la aplicación normalmente sigue exigiendo algún tipo de método expuesto públicamente para establecer la conexión, como una VPN, un *host* bastión, un *proxy* o un servidor terminal. Aunque cada una de estas tecnologías pretende proporcionar un acceso seguro al servidor interno, hay puertas de enlace expuestas que siguen corriendo el peligro de ser escaneadas por puertos, mal configuradas o vulneradas.

En general, la nube cambió el panorama de las aplicaciones DMZ tradicionales.

Utilizando los mismos principios comentados en el uso del acceso a la red de confianza cero y SASE para intermediar en las conexiones, las organizaciones pueden ampliar el acceso a aplicaciones privadas sin necesidad de una DMZ. A diferencia de la VPN tradicional, que conecta el dispositivo del usuario final a la red de confianza, el acceso a la red de confianza cero ofrece un acceso seguro específicamente entre usuarios y aplicaciones.

En una situación ideal, se pueden maximizar los beneficios de costes y seguridad eliminando todo el tráfico de entrada. Esto puede ser viable o no cuando se compara con los requisitos de su organización, pero está claro que incluso una reducción en el número de sistemas colocados en la DMZ reducirá la superficie de ataque y hará que su red sea más fácil de gestionar.

ACERCA DE LA PLATAFORMA NETSKOPE ONE

Netskope One es una plataforma convergente de seguridad y red como servicio. A través de su motor patentado Zero Trust Engine, las innovaciones de IA y la mayor nube de seguridad privada, facilitamos a nuestros clientes la defensa de sus empresas y datos a la vez que ofrecemos una extraordinaria experiencia de usuario final.

El poder de One

Reduzca costes y complejidad con la única plataforma convergente que ofrece un motor, un cliente, una pasarela y una nube de seguridad privada.

Visibilidad y protección potenciadas por la IA

Descifre y descodifique toda la actividad de los usuarios de la nube, SaaS y web con innovaciones de IA patentadas y la incomparable visibilidad y precisión del motor Zero Trust para impedir la pérdida de datos y las amenazas.

Una experiencia de usuario extraordinaria

Acelere la empresa híbrida con la infraestructura de nube de seguridad privada más rápida y fiable del sector y gestione de forma proactiva la experiencia, desde el usuario hasta la aplicación y todo lo que haya en medio.

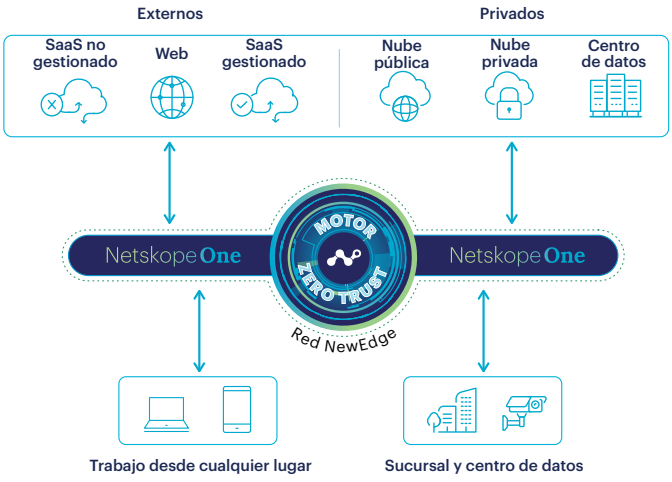
COMPONENTES DE LA PLATAFORMA NETSKOPE ONE

Motor Zero Trust

El motor Zero Trust se encuentra en el corazón de la plataforma Netskope One, facilitando las implementaciones de confianza cero mediante la recopilación continua de telemetría de riesgos sobre los usuarios, los dispositivos, las aplicaciones, las transacciones y los datos para ampliar la confianza adaptativa integral y precisa que minimiza el riesgo a la vez que ofrece una experiencia de usuario rápida y que inspira confianza.

Red NewEdge

Netskope NewEdge es la mayor infraestructura de nube de seguridad privada, con centros de datos ultrarrápidos con cobertura en todos los países para que los usuarios y las oficinas se conecten al motor Zero Trust, así como amplias relaciones de interconexión con los principales proveedores web y de nube del mundo para garantizar la mejor experiencia de usuario de extremo a extremo.



Netskope One Client

Netskope One Client es el primer cliente SASE del sector, que unifica el acceso remoto de los usuarios a la web, la nube y las aplicaciones privadas, junto con la DLP y la SD-WAN para puntos de conexión, lo que da como resultado una huella de agente único para casos de uso de SASE y de confianza cero que simplifica enormemente la administración del escritorio y la experiencia del usuario.

Puerta de enlace Netskope One

La puerta de enlace Netskope One facilita la transformación de la sucursal en una sucursal ligera con la conectividad segura y optimizada de Borderless SD-WAN, una rampa de acceso sin problemas a Intelligent SSE y la consolidación de varios dispositivos inconexos de cada sucursal en un único dispositivo.

Usar Netskope para su red del mañana

Netskope SASE ayuda a las organizaciones a conseguir su red del mañana aplicando los principios descritos en esta guía. Implementa los servicios de seguridad y redes para proporcionar una cobertura completa desde cualquier lugar donde opere la empresa. La red y nube privada Netskope NewEdge es la nube privada de seguridad más grande y de mayor rendimiento del mundo y la tecnología base de la plataforma Netskope One. Diseñada por expertos del sector que anteriormente habían presentado y ampliado en la nube algunos de los mayores servicios y redes de distribución de contenidos del mundo, NewEdge es una arquitectura de hiperescala preparada para SASE que ofrece a los clientes una cobertura de servicios, rendimiento y resistencia sin precedentes.

Con el aprovisionamiento de todos los servicios informáticos y de seguridad disponibles en cada una de nuestras más de 75 regiones y más de 100 centros (en agosto de 2024), NewEdge garantiza un rendimiento sin concesiones. Esto permite el despliegue de medidas de seguridad allí donde se encuentren los empleados y los dispositivos, eliminando la dependencia de puntos de presencia virtuales o redireccionamiento de tráfico. Todo esto se traduce en una conectividad más rápida a cualquier aplicación y en una experiencia de usuario excepcional.

Nuestro modelo de servicio en la nube procesa el tráfico con velocidad y disponibilidad instantáneas. Nuestro SLA de 5 nueves garantiza el tiempo de actividad y la disponibilidad de nuestros servicios en línea. Netskope sobreaprovisiona masivamente la red NewEdge, capaz de alcanzar 2 terabits por segundo en cada centro de datos o más de 100 terabits a nivel global. Todo esto forma parte del diseño NewEdge, que ayuda a nuestros clientes a simplificar sus propias redes.

El enfoque SASE, tal y como lo ofrece Netskope, proporciona una serie de ventajas de diseño con respecto a las redes empresariales convencionales:

Ventajas de la red

1. **Operaciones simplificadas:** Trasladar la red de *back-end* a Netskope significa que su organización solo tiene que gestionar los túneles al centro de datos de NewEdge. Esto se simplifica aún más gracias a Netskope Client, que puede utilizarse para negociar las conexiones de túnel para los usuarios, además de Borderless SD-WAN, que mantiene y optimiza las conexiones tanto para los usuarios como para las oficinas de forma automática mediante políticas.
2. **Altas velocidades:** Al hacer uso de NewEdge, su organización tiene acceso a una conectividad en la nube sin igual y a una red de alto rendimiento, sin la red de retorno al centro de datos corporativo para la salida.
3. **Más cobertura de aplicaciones en la nube:** La mayoría de las organizaciones mantienen un número reducido de interconexiones en la nube. Por ejemplo, una tienda de AWS podría adquirir Direct Connect para dar soporte al equipo de desarrollo de AWS, pero depender de la impredecible Internet abierta para otras nubes o aplicaciones SaaS. Con Netskope, puede dar soporte a una gama más amplia de aplicaciones con velocidad y seguridad.
4. **Mayor cobertura geográfica:** El servicio de Internet en todo el mundo sigue estando muy fragmentado, con una calidad y velocidad de servicio impredecibles por parte de los proveedores de las distintas regiones. Normalmente, las organizaciones pueden mejorar su conectividad global general a través de un primer salto a través de NewEdge.
5. **Consolidación de un solo proveedor:** Cada región tiene diferentes proveedores de servicios de red, lo que supone una difícil carga para una empresa típica. Incluso dentro de una misma región, la calidad del servicio varía, sobre todo en continentes tan diversos como Europa y Sudamérica. Gracias a Netskope, las organizaciones pueden garantizar una experiencia de usuario de alta calidad en todo el mundo sin tener que mantener relaciones con varios proveedores en cada región.
6. **Mayor seguridad:** En lugar de confiar en un conjunto mixto de dispositivos de red y excepciones a las políticas, las organizaciones pueden mejorar su seguridad utilizando Netskope. Netskope SASE ofrece protecciones que incluyen la protección frente a amenazas, la protección de datos y el acceso a la red de confianza cero como servicios. Cambiar las protecciones a través de Netskope ayuda a la organización a simplificar y reducir la superficie de ataque dentro de sus propias redes, como se ilustra en esta guía.

Para obtener más información sobre Netskope, visite http://www.netskope.com y esté al tanto de más contenidos en esta serie que le ayudarán a construir su red del mañana.

ÍNDICE DE REFERENCIAS

[1] «CIOs, CTOs and technology leaders: Latest findings from PwC's Pulse Survey», PwC, 27 de enero de 2022.

[2] «Gartner, Hype Cycle™ for Cloud Security, 2021», por Tom Croll, Jay Heiser, 27 de julio de 2021.

[3] «Cloudy With a Chance of Malice», Netskope, 23 de febrero de 2021.

[4] «Volumen de datos/información creados, capturados, copiados y consumidos en todo el mundo de 2010 a 2025», Statista, 18 de marzo de 2022.

[5] «40% of organizations have suffered a cloud-based data breach», Security Magazine, 29 de octubre de 2021.

[6] «A Stanford Economist Who Studies Remote Work Says Half of All Workers Will Make This Big Change in 2022», Inc., 8 de enero de 2022.

¿Le gustaría obtener más información?

Solicite una demostración

Netskope, líder mundial en SASE, ayuda a las organizaciones a aplicar los principios de Zero Trust y las innovaciones de IA/AA para proteger los datos y defenderse frente a las ciberamenazas. Rápida y fácil de usar, la plataforma Netskope One y su motor patentado Zero Trust proporciona acceso optimizado y seguridad en tiempo real a personas, dispositivos y datos en cualquier lugar. Miles de clientes confían en Netskope y en su potente red NewEdge para reducir riesgos y obtener una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas, ofreciendo siempre seguridad y acelerando el rendimiento sin concesiones. Más información en netskope.com.