WHITE PAPER

Más allá de la SD-WAN:

Seguridad Zero Trust e Internet como WAN corporativa

Por qué la tecnología SD-WAN, el acceso seguro y la protección contra amenazas van de la mano

Akamai

El futuro de la red de área extensa empresarial

Las redes de área extensa (WAN) han estado presentes desde la década de 1960, los comienzos de la comunicación entre ordenadores, y continúan desarrollándose y mejorando a medida que evoluciona la tecnología y que aumenta la demanda de tráfico. Para las empresas actuales, las WAN son la infraestructura que permite una red unificada en todas las ubicaciones.

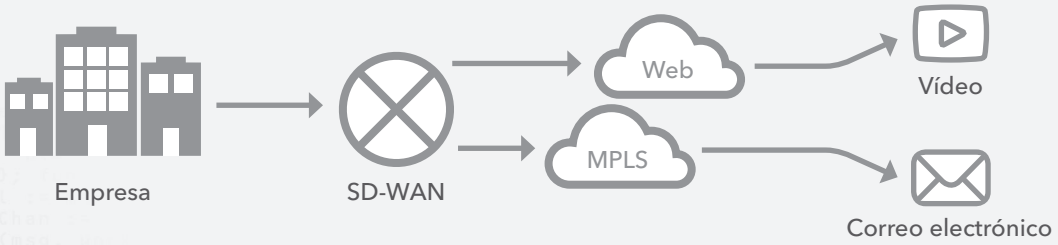
Sin embargo, esta estructura subyacente tan importante no está exenta de limitaciones. Con frecuencia, las WAN proporcionan un ancho de banda bajo o insuficiente, generan problemas relacionados con el rendimiento de aplicaciones específicas, ofrecen una fiabilidad fluctuante y pueden constituir un riesgo para la seguridad de su empresa. Además, las WAN se suelen crear a partir de líneas dedicadas, o bien se alquilan de proveedores de servicios cuya infraestructura utiliza métodos de conmutación de circuitos o paquetes, como el modo de transferencia asíncrona (ATM) y la conmutación por etiquetas multiprotocolo (MPLS), además del Internet público. Aunque esta última es una opción algo menos costosa, sigue tratándose de una solución muy cara y que no se presta a la escalabilidad.

Las redes corporativas están experimentando una transformación

En respuesta a estos desafíos económicos, de seguridad y de rendimiento, las empresas están adoptando un modelo de red WAN definida por software (SD-WAN), que permite reducir los costes y posibilita una mayor agilidad.

Procedentes de la innovación de las redes definidas por software (SDN) y la virtualización de las funciones de red (NFV) utilizadas originalmente en los centros de datos, los departamentos de TI adoptaron rápidamente la tecnología para las redes que conectaban las distintas divisiones internas.

En pocas palabras, el modelo SD-WAN separa los planos de datos y control de la red de área extensa. La SD-WAN supervisa el rendimiento de la combinación de conexiones de datos WAN (MPLS, ATM e Internet), al tiempo que selecciona la conexión más adecuada para cada tipo de tráfico según el rendimiento actual del enlace, el coste de la conexión y las necesidades de la aplicación o del servicio.



SD-WAN en acción

Una SD-WAN puede enrutar el correo electrónico a través de una MPLS porque la latencia no es un problema importante y el coste por bit enviado es el más bajo. Asimismo, la red SD-WAN podría dirigir el tráfico de videoconferencia a través de Internet para garantizar un rendimiento óptimo y una latencia mínima, pero con un coste por bit enviado más alto.

¿Podría Internet llegar a convertirse en la nueva WAN corporativa?

Las redes SD-WAN pueden llegar a ofrecer una verdadera flexibilidad, eficacia y rentabilidad si utilizan varios servicios de transporte, incluido el Internet público. Sin embargo, dado que no existe ninguna garantía de rendimiento ni acuerdo de nivel de servicio (SLA) para dichas opciones de transporte, los modelos SD-WAN utilizan Internet únicamente para aquellas aplicaciones cuyo rendimiento no sea crítico.

Para aumentar el uso de Internet con el fin de ofrecer un mayor tráfico WAN corporativo eficiente, rentable y seguro (y de forma que pueda coexistir con las implementaciones actuales de SD-WAN), debe adoptar un enfoque que elimine las limitaciones subyacentes de Internet. Para ello, puede emplear una plataforma en el borde de Internet con el objeto de proporcionar unas aplicaciones empresariales seguras, rápidas y fiables a través de Internet, y todo ello sin exponerlas públicamente en la Red. De esta manera, podrá maximizar su inversión actual en un modelo SD-WAN, al tiempo que reduce aún más los costes conforme transfiere más tráfico a Internet.

El enrutamiento de una porción mayor de tráfico empresarial a Internet es la opción lógica: no hay más que ver la trayectoria de las redes corporativas modernas. Dado el aumento de las cargas de trabajo en la nube, junto con la diversificación de usuarios y dispositivos móviles, los flujos de trabajo ya dependen en gran medida de Internet. Y esta tendencia continúa difundiéndose.

¿Y si pudiera avanzar un paso más gracias a una WAN corporativa segura, escalable y eficiente a través de Internet?

En este documento, analizaremos los procesos de transformación de su red con un modelo SD-WAN y de seguridad Zero Trust. También veremos cómo puede posicionarse su organización para evolucionar más allá de la SD-WAN, gracias a la adopción de una red corporativa totalmente basada en Internet.

Una plataforma situada en el borde de Internet permite ofrecer aplicaciones empresariales seguras, rápidas y fiables a través de Internet, sin exponerlas públicamente a la Red.

> *A finales del año 2023, más del 90 % de las iniciativas de actualización de infraestructuras perimetrales de WAN se basarán en plataformas de equipo local del cliente virtualizado (vCPE) o en dispositivos o software de una red WAN definida por software (SD-WAN) frente a routers tradicionales (respecto del 40 % actual)."*
>
> *Gartner, Magic Quadrant for WAN Edge Infrastructure, octubre de 2018*

El valor de un modelo SD-WAN

Una red SD-WAN proporciona principalmente balanceo de enlaces, configuración automática de dispositivos e inserción de servicios de seguridad de terceros. El valor de estas funciones (la mejora de la experiencia del usuario, la reducción de los costes de enlace y la reducción de los gastos operativos) puede tener un impacto notable. Su aceptación es evidente y su adhesión es un buen ejemplo de ello.

Las capacidades SD-WAN ofrecidas varían según el proveedor, pero, a grandes rasgos, pueden clasificarse en tres categorías:

1. *Control de enlaces flexible*
2. *Capacidad de gestión*
3. *Inserción de servicios*

Control de enlaces flexible

La primera capacidad, un control de enlaces flexible, es la principal prestación de la SD-WAN. Puesto que la nube es un destino principal para muchas organizaciones, no resulta práctico redirigir el tráfico a través de una red privada a un centro de datos, que hace las veces de punto de control centralizado *de facto*. SD-WAN soluciona este desafío mediante el control inteligente del tráfico, incluida la selección dinámica de rutas. Además, la tecnología SD-WAN establece salidas a Internet locales o de sucursales, también conocidas como acceso directo a Internet (DIA), que enrutan el tráfico a la nube en lugar de hacerlo a través de un centro de datos. En este sentido, todas las aplicaciones heredadas, incluidas las de voz y vídeo, están diseñadas para enlaces MPLS; mientras que las aplicaciones en la nube y el tráfico de Internet se dirigen directamente a la Red.

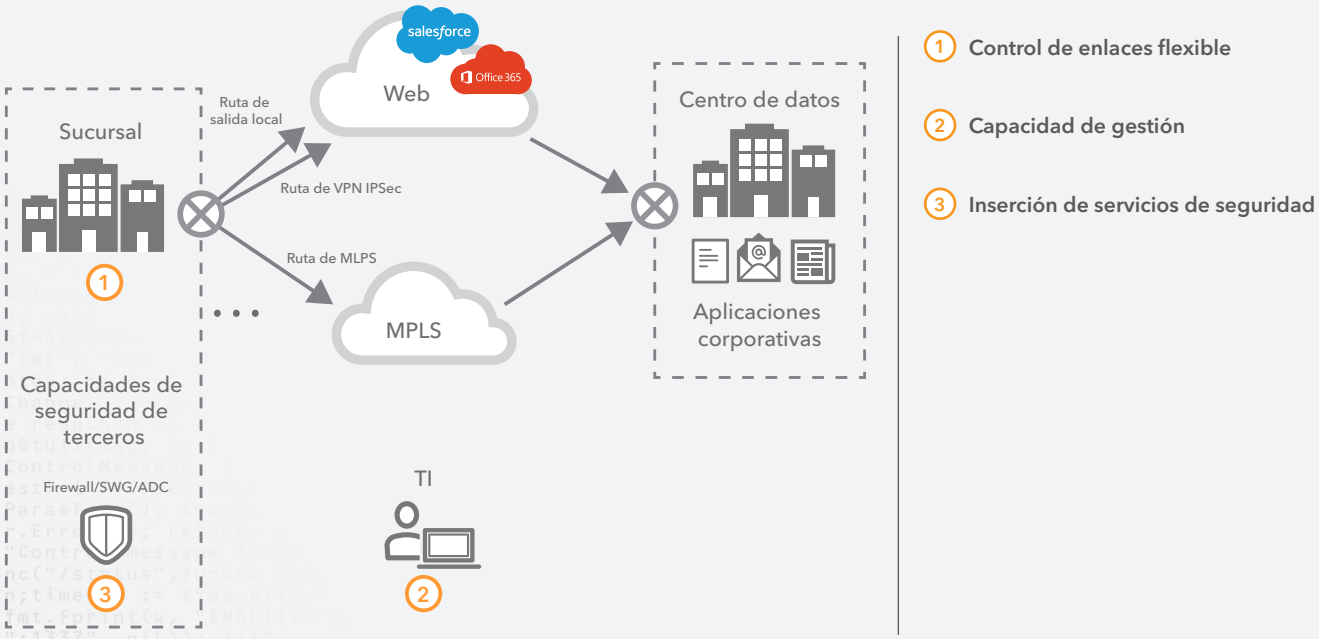
Capacidad de gestión

Los proveedores de SD-WAN también pueden ofrecer capacidad de gestión, lo que simplifica el funcionamiento y la administración de los dispositivos de red. Desde la década de 1990, las WAN empresariales se han compuesto de dispositivos de red como conmutadores y routers multicapa. Estos dispositivos se han gestionado mayormente por separado, por terminal. En otras palabras, los administradores tienen que configurar y mantener de varios cientos a varios miles de dispositivos de forma individual, supervisando la pila de software de cada uno de ellos, en toda la empresa. Aunque los dispositivos intercambien información de enrutamiento dinámicamente o establezcan una alta disponibilidad mediante protocolos de enrutamiento, el esfuerzo es enorme. Con un modelo SD-WAN, toda la gestión de los dispositivos se puede realizar en una única consola centralizada.

Inserción de servicios

Por último, algunos proveedores de SD-WAN están especializados en la inserción de servicios. El requisito mínimo para una WAN es la accesibilidad mediante IP, es decir, la conectividad de red de capa 3, en toda la organización. Sin embargo, a medida que las conexiones de red han evolucionado, también lo han hecho las funciones de seguridad: firewalls, sistemas de prevención de intrusos (IPS) y controladores de distribución de aplicaciones, por nombrar algunos. En el pasado, era necesario elaborar un complicado diseño de enrutamiento para agregar estas capacidades a la red, ya que los dispositivos que proporcionaban dichos servicios normalmente no podían comunicarse con protocolos de enrutamiento dinámico (primera trayectoria abierta más corta [OSPF], Border Gateway Protocol [BGP]), lo que generaba una compleja combinación de redistribución y enrutamiento estático. La SD-WAN hace que estas tecnologías, a menudo distribuidas a través de terceros, sean fáciles de configurar y sencillas de gestionar a través de un portal unificado.

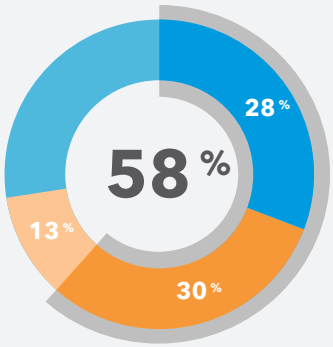
Valor empresarial de SD-WAN



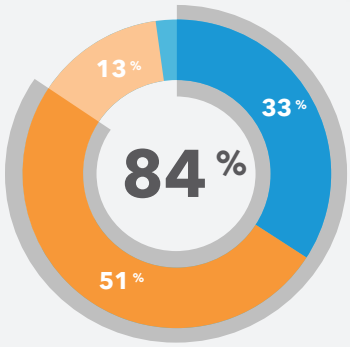
Un nuevo modelo: la seguridad Zero Trust

Una nueva arquitectura requiere un nuevo modelo de seguridad. Conforme las transacciones se trasladan a la nube y a Internet, las redes se han vuelto altamente distribuidas, lo que se traduce en la creación de superficies de ataque adicionales. Las aplicaciones, los usuarios, los datos y los dispositivos se han desplazado fuera de la zona de control tradicional, lo que ha hecho desaparecer lo que antes era el perímetro empresarial de confianza. Y así es: la creación y aplicación de un modelo de seguridad basado en el perímetro de la empresa ya no es viable. Una estrategia de defensa moderna debe resolver las cargas y fuerzas de trabajo distribuidas de hoy en día.

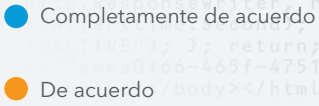
¿Hasta qué grado está de acuerdo o en desacuerdo?



"El perímetro de la red es indefendible en el ecosistema tecnológico actual de redes de nube distribuidas y usuarios móviles o remotos."



"La transformación digital requiere ajustes en las estrategias de seguridad tradicionales (basadas en el perímetro)."



Forrester Research, Build Your Zero Trust Security Strategy With Microsegmentation, septiembre de 2018

Un modelo de seguridad Zero Trust asume que nada queda dentro y que ningún dispositivo o usuario son de confianza. Todas las solicitudes de acceso requieren autenticación y autorización. Las aplicaciones y los datos solo se distribuyen después de la verificación, e, incluso entonces, de forma transitoria y con alcance limitado. Este marco de seguridad trata todas las aplicaciones como si estuvieran orientadas a Internet y considera que la red está en peligro y es hostil. Además, la visibilidad es fundamental; los análisis de comportamiento y registros completos son aspectos imprescindibles.

Los principios básicos del modelo de seguridad Zero Trust son los siguientes:

- *Garantizar que el acceso a todos los recursos sea seguro, independientemente de la ubicación o el modelo de alojamiento.*
- *Adoptar una estrategia de "privilegios mínimos" y "denegación predeterminada" al implantar el acceso a las aplicaciones.*
- *Inspeccionar y registrar el tráfico, tanto para las aplicaciones que controla como para las que no, con objeto de identificar actividades maliciosas.*

Hay dos componentes principales que respaldan la implementación de un modelo de seguridad Zero Trust:

- *Proxy con reconocimiento de identidades, para un acceso seguro a las aplicaciones.*
- *Puerta de enlace de Internet segura, para proteger a los usuarios.*

Proxy con reconocimiento de identidades para un acceso seguro a las aplicaciones.

Si los usuarios, los datos y las aplicaciones están en la nube, y el DIA habilitado por SD-WAN proporciona la conexión, ¿por qué no cambiar también la pila de DMZ y seguridad a la nube? De esta forma, puede aprovechar las prestaciones de un modelo Zero Trust para garantizar un acceso seguro a las aplicaciones que controla, al tiempo que reduce el riesgo asociado a los usuarios que acceden a las aplicaciones que no controla.

Si actualmente es de los que utilizan una configuración de VPN sencilla para proporcionar acceso a las aplicaciones corporativas, probablemente esté permitiendo que los usuarios que han iniciado sesión tengan acceso a la totalidad de su red a nivel de IP. Sin embargo, esto es muy arriesgado y es un modelo contrario a los principios del modelo de seguridad Zero Trust. ¿Por qué los teleoperadores tienen permisos de acceso a repositorios de código fuente? ¿Por qué un contratista que utiliza su sistema de facturación debe tener derechos de acceso a los terminales de procesamiento de tarjetas de crédito? A los usuarios solo se les debe conceder acceso a las aplicaciones que necesiten para desempeñar su trabajo. La VPN tradicional no permite este acceso granular, sino que requiere una dependencia continuada de un modelo de red radial.

Una arquitectura de proxy con reconocimiento de identidades (IAP) proporciona acceso a las aplicaciones a través de un proxy basado en la nube. La autenticación y la autorización se producen en el borde de Internet y se basan en los principios de privilegios mínimos "necesarios", que son similares al acceso a través de perímetros definidos por software (SDP), pero que, en su lugar, utilizan protocolos HTTPS estándar en la capa de aplicación (capa 7).

Las dos formas en las que un IAP puede funcionar

Se integra una CDN en las transacciones a escala internacional para mejorar la respuesta de las aplicaciones.

O BIEN

Se utiliza un firewall de aplicaciones web (WAF) para proteger los servidores web corporativos frente a vulnerabilidades comunes, como la inyección SQL y las secuencias de comandos en sitios cruzados.

Un componente clave de un IAP es una fuente de identidades que verifica la confianza de los usuarios y los dispositivos (autenticación) y a lo que tienen permiso para acceder (autorización). Esta fuente de identidades puede basarse en directorios corporativos, o bien en proveedores de identidades basados en la nube. Incluso antes de validar la identidad de un usuario, comprobar el dispositivo en sí puede garantizar que el dispositivo que intenta obtener acceso cumpla unos determinados criterios de seguridad; por ejemplo, tener un certificado, ejecutar el sistema operativo más reciente, estar protegido por contraseña o tener instalada y operativa la solución de detección y respuesta de terminales adecuada.

Una ventaja notable del IAP en comparación con otras tecnologías de acceso: no solo se verifican los usuarios, sino que también se inspecciona el tráfico de estos y se pueden cancelar, examinar y autorizar solicitudes de aplicaciones individuales. Una vez terminada una transacción en el proxy, se pueden integrar servicios adicionales, lo que permite mejorar la experiencia del usuario y la protección de las aplicaciones.

Proxy con reconocimiento de identidades (IAP)

El IAP también se basa en controles de acceso a nivel de aplicación, no solo en reglas de firewall; las políticas configuradas pueden reflejar la intención del usuario y de la aplicación, no solo los puertos y las IP. Al igual que los SDP, este enfoque puede ocultar las aplicaciones y otros activos en la nube o detrás del firewall, y no emplea clientes para las aplicaciones web.

A medida que crece la adopción de soluciones basadas en la nube, el reto de migrar las aplicaciones corporativas ha cobrado mayor conciencia. Muchas organizaciones se esfuerzan por aprovechar las prestaciones de la nube para aplicaciones tradicionales y nativas de la nube por igual. El IAP no solo se puede utilizar para autenticar usuarios para aplicaciones SaaS nativas, sino que también se puede emplear para, en esencia, "convertir" aplicaciones heredadas en aplicaciones SaaS dentro del centro de datos. Además, un proxy facilita la migración a la nube y la modernización de las aplicaciones sin tener que recurrir a una estrategia completa de sustitución y eliminación. Como resultado, las empresas pueden adoptar un enfoque metódico y gradual para implementar un modelo Zero Trust, al tiempo que reducen la deuda técnica asociada a los controles basados en perímetros heredados y a las VPN tradicionales.

Puerta de enlace de Internet segura, para proteger a los usuarios.

Un aspecto fundamental de la transición a un modelo de seguridad Zero Trust consiste en garantizar el mantenimiento de la seguridad de los usuarios mientras acceden a las aplicaciones que no controla. Un gran número de ciberamenazas acechan cada vez que hace clic en Internet. Anteriormente, cuando los usuarios estaban vinculados a la red corporativa y a los dispositivos gestionados, protegerse contra malware, ransomware y phishing era tan sencillo como implementar antivirus en los terminales, instalar una pila de dispositivos en un centro de datos y redireccionar el tráfico para su inspección y control.

Con usuarios en diferentes ubicaciones, Internet se convierte en la red corporativa preferida; una SIG basada en la nube le proporciona una vía de acceso segura, al proteger de forma proactiva a los usuarios en cualquier lugar.

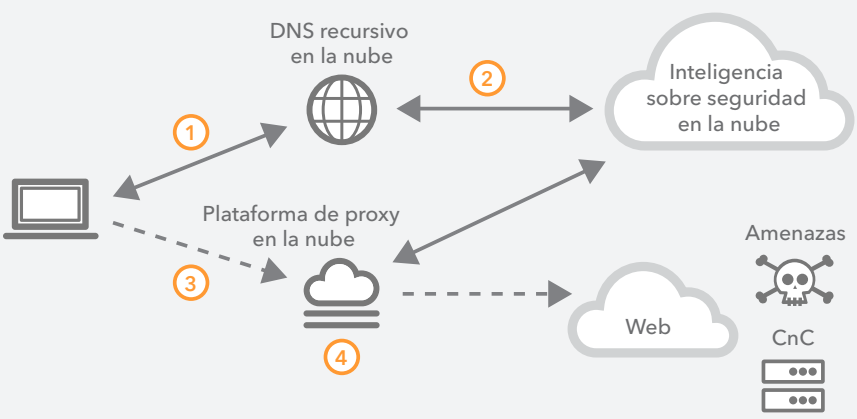
Sin embargo, los usuarios ya no siempre están en la oficina, los dispositivos no se gestionan e Internet se está convirtiendo en la red corporativa preferida. Una conectividad de DIA deja obsoletas las soluciones de seguridad mediante inspección y control centrales. Como alternativa, puede replicar la pila de dispositivos de seguridad en cada salida a Internet. Sin embargo, para la mayoría de las empresas, se trata de algo imposible, tanto desde el punto de vista logístico como desde el financiero. Y, lo que quizás sea aún más importante, la complejidad inherente de este enfoque introduce defectos de seguridad, concebidos según premisas totalmente opuestas a las prácticas recomendadas de un modelo Zero Trust.

Un método más sencillo, rápido y rentable de proteger el tráfico de DIA es utilizar una puerta de enlace de Internet segura (SIG) basada en la nube. Una SIG es una vía de acceso segura a Internet que protege de forma proactiva a los usuarios, independientemente de su ubicación, contra amenazas avanzadas filtrando el tráfico malicioso para su control e inspección. Esto se consigue examinando cada una de las solicitudes DNS, bloqueando las solicitudes a dominios maliciosos, permitiendo que las solicitudes a dominios seguros procedan con normalidad y reenviando las solicitudes de dominios de riesgo a un proxy en la nube para su posterior inspección.

En esta fase final, cuando el proxy recibe una solicitud HTTPS, compara la URL solicitada con una base de conocimiento en la nube (de inteligencia frente a amenazas) y bloquea las URL maliciosas. Para todas las demás URL solicitadas que estén clasificadas como peligrosas, el proxy envía el contenido web para el análisis de carga en línea a través de varios motores de análisis de malware. Estos motores utilizan una amplia gama de técnicas de detección (firma, sin firma y aprendizaje automático) para identificar y bloquear amenazas conocidas y amenazas de día cero desconocidas. Al contar con una amplia gama de métodos de detección, puede dirigir una carga al motor (o motores) más adecuado en función del tipo de contenido, lo que garantiza unos índices de detección óptimos y ofrece un índice bajo de falsos positivos.

Es importante tener en cuenta que este enfoque es bastante diferente del enfoque adoptado por dispositivos de seguridad heredados, como las puertas de enlace web seguras (SWG). En concreto, las SWG utilizan el proxy para filtrar todo el tráfico de Internet, inspeccionando tanto el tráfico legítimo como el malicioso, lo que puede ser especialmente perjudicial para las páginas web complejas y el contenido HTTPS más pesado. Este enfoque degrada el rendimiento, introduce latencia y aumenta el volumen de sitios web y aplicaciones con problemas, que son la consecuencia de utilizar el proxy para todo el tráfico. Las SWG suelen generar más incidentes de seguridad y falsos positivos, lo que se traduce en solicitudes de asistencia técnica y monopoliza los recursos de TI.

Arquitectura de puerta de enlace de Internet segura



1. **Búsqueda de DNS**
2. **Categorización del dominio en términos de benigno, malicioso y sospechoso**
3. **Dominios sospechosos redirigidos al proxy en la nube**
4. **Análisis de carga e inteligencia frente a amenazas de URL**

Un proxy selectivo inteligente puede utilizar el DNS como vía de acceso a Internet y como primera capa de seguridad. Al dirigir el tráfico seguro directamente a Internet, bloquear el tráfico malicioso y redirigir a un proxy únicamente el tráfico que puede plantear riesgos, este enfoque le ofrece:

- *una seguridad simplificada;*
- *menor latencia y mejor rendimiento; y*
- *un menor número de problemas con páginas web y aplicaciones.*

Transformación de la red con menos riesgo: implementación del modelo Zero Trust en un entorno SD-WAN

Muchas organizaciones que están migrando a arquitecturas basadas en Internet consideran que la SD-WAN es el factor clave, gracias a su control de enlaces y su capacidad para reducir potencialmente los costes de propiedad de MPLS. Pueden utilizar redes de banda ancha o inalámbricas para ampliar o complementar las conexiones MPLS, lo que crea una WAN híbrida. Pero, si ya han adoptado un DIA, seguramente tenga sentido emplear un modelo de seguridad con el mismo enfoque.

A medida que se adopta la tecnología SD-WAN, las empresas deben hacer que su seguridad evolucione de un marco perimetral a un marco Zero Trust en el borde de Internet. En este sentido, ¿dónde nos encontramos actualmente y qué vendrá después?

Las redes con SD-WAN suelen ubicarse en una de estas tres situaciones, en función de la mentalidad y la estrategia a largo plazo de la empresa:

1. *WAN privada tradicional con salida centralizada; es decir, se plantean utilizar la tecnología de red SD-WAN, pero no la han implementado aún.*
2. *Implementación híbrida de WAN privada tradicional en las instalaciones existentes y de SD-WAN en las nuevas sucursales.*
3. *Principalmente SD-WAN.*

Un enfoque de seguridad Zero Trust encaja perfectamente en todas estas situaciones. No obstante, si la empresa ya está considerando o implementando la tecnología SD-WAN, puede que ya haya adoptado Internet como una herramienta de red empresarial viable y, por lo tanto, esté preparada para aplicar una estrategia de seguridad Zero Trust a su entorno de red corporativa.

Examinemos las posibles arquitecturas actuales para identificar cómo cada una de ellas podría implementar Zero Trust y, posteriormente, progresar hacia el futuro estado que desea.

WAN privada tradicional con salida centralizada

Si las motivaciones de la migración a la SD-WAN son el coste, la agilidad y la flexibilidad, ventajas que puede ofrecer una arquitectura de red basada en Internet, podría tener sentido omitir la adopción de la tecnología de red SD-WAN y pasar directamente a un marco de trabajo Zero Trust. El IAP permite el acceso Zero Trust a las aplicaciones, independientemente de su ubicación, mientras que la SIG proporciona a los usuarios un acceso seguro a Internet; todo ello sin que las organizaciones tengan que crear pilas de seguridad en cada salida a Internet.

Un aspecto que tener en cuenta: si la empresa ya admite servicios en tiempo real como VoIP y videoconferencia a través de un proveedor de servicios en la nube de Internet, se encuentra en una posición ideal para adoptar de manera íntegra una arquitectura de acceso y red basada en Internet. Si estos servicios siguen alojados principalmente a nivel local, puede ser oportuno mantener cierto nivel de redes "privadas" entre ubicaciones, ya sean verdaderamente privadas (por ejemplo, basadas en MPLS) o basadas en SD-WAN.

Híbrida con WAN tradicional y SD-WAN

En este caso, las organizaciones ya han dado el primer paso hacia una arquitectura más eficiente basada en Internet.

En estos entornos, es importante saber cómo se gestiona el tráfico de usuarios:

- *¿Tienen los usuarios acceso directo a Internet desde oficinas remotas, o se utiliza el enlace de Internet solo para conectarse en red a las instalaciones principales?*
- *¿Dónde se encuentran ubicadas las principales aplicaciones de usuario? ¿En las instalaciones, en un centro de datos o en la nube?*
- *Si se utiliza la nube, ¿cómo se conectan los usuarios a esas aplicaciones? ¿Se facilita la conexión a través de un DIA desde una sucursal, o se redirige a través de un enlace de conexión directa?*
- *¿Cómo está extendido el uso de las aplicaciones SaaS?*
- *En el caso de utilizar un DIA en las sucursales, ¿hasta qué punto es completa la pila de seguridad en cada ubicación?*

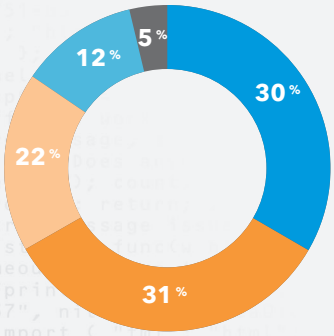
Evidentemente, las respuestas variarán en función del tratamiento del tráfico del usuario y, como tal, la migración de la red tendrá distintos grados de complejidad. Pero existen dos constantes: se producirá un aumento del uso de Internet y de la necesidad de pasar de la seguridad perimetral a un modelo Zero Trust.

Tomemos como ejemplo una situación en la que exista alguna conectividad de DIA desde una oficina remota. Una SIG puede ofrecer protección adicional a la pila de seguridad centralizada, así como sustituir parte de la pila, con la consiguiente reducción de la complejidad y los costes.

Si los usuarios acceden a aplicaciones en la nube, un enfoque basado en un IAP puede reforzar la estrategia de seguridad de la organización, al tiempo que mejora la experiencia del usuario. También puede incrementar el rendimiento de las aplicaciones, al permitir el acceso directo a las aplicaciones a través de Internet con una CDN.

Puede continuar la transición de una WAN tradicional a un entorno SD-WAN mediante la habilitación de un DIA para oficinas remotas y la adopción de los principios del modelo de seguridad Zero Trust.

¿Cuáles son sus planes empresariales para utilizar hoy mismo la tecnología de red definida por software (SD-WAN)?



- Utilizarla desde hoy mismo
- Probar en el próximo año
- Planificar su adopción en los próximos dos años
- Consideramos su uso, pero sin ningún plan
- No consideramos su uso ni hay ningún plan

Forrester Research, Digital Transformation Drives Distributed Store Networks to the Breaking Point, abril de 2018

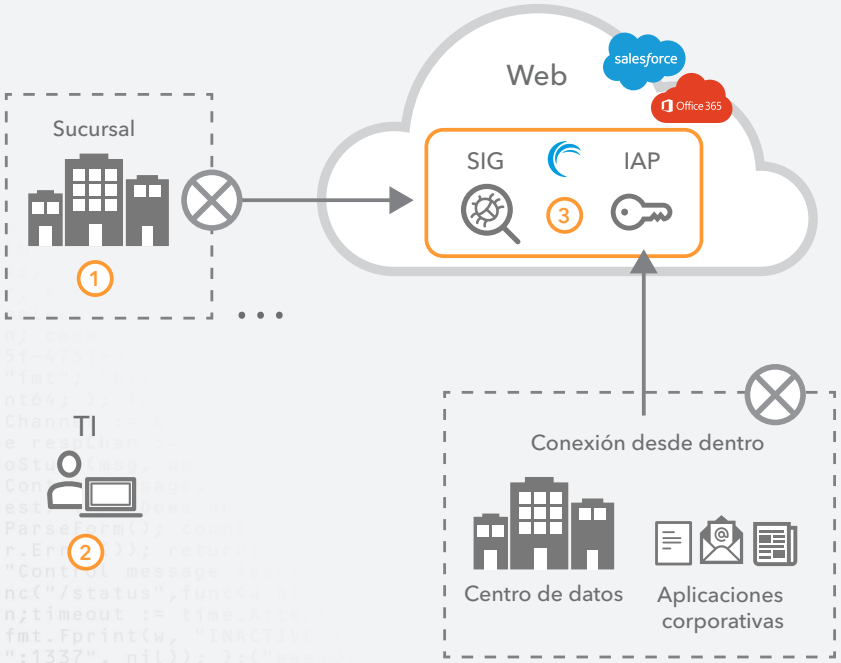
Principalmente SD-WAN

En este estado, es probable que las organizaciones se hayan alejado de una red WAN privada tradicional, utilizando el enrutamiento inteligente a través de enlaces de Internet entre instalaciones para la comunicación entre oficinas, aprovechando al máximo las ventajas del DIA. Estas empresas ya se basan en el acceso a Internet en la mayoría de las instalaciones, por lo que la evolución de la red más allá de una red SD-WAN resulta lo más coherente.

¿Cuál es el siguiente paso? Comenzar a reducir la dependencia de los enlaces MPLS trasladando las aplicaciones a Internet para ofrecer agilidad y rentabilidad. Se puede acceder a las aplicaciones corporativas a través de un IAP, incluso en un entorno con DIA. Si las aplicaciones ya están en un entorno de nube, no tiene sentido acceder a ellas mediante el redireccionamiento del tráfico a un centro de datos antes de su división en una ubicación central (por ejemplo, mediante una topología de tipo de conexión directa).

Por último, este entorno está bien adaptado para un futuro estado de conectividad y acceso basados totalmente en Internet. Se puede acceder a todas las aplicaciones corporativas a través de un IAP, tanto si se encuentran en las instalaciones como en la nube. Todo el tráfico de usuarios se puede proteger mediante una SIG. Además, si los proveedores basados en Internet ofrecen comunicación en tiempo real, como voz y vídeo, puede que sea posible eliminar por completo la SD-WAN, e incluso la WAN corporativa. Así se podría reducir los costes y la complejidad, además de reforzar la seguridad gracias un modelo de arquitectura Zero Trust.

Valor de la arquitectura basada en Internet con un modelo de seguridad Zero Trust



1. **Acceso a la red más sencillo**
   - Solo acceso a Internet
   - Sin acceso desde fuera
2. **Capacidad de gestión**
   - Un único punto de gestión
   - Supervisión de dispositivos
   - Supervisión de usuarios
3. **Mayor control de seguridad**
   - Prevención de ataques de día cero
   - Centralización de AAA (autenticación, autorización y contabilización)
   - Control del nivel de seguridad del cliente
   - Prevención de phishing, malware y CnC

Transforme su negocio

La realidad actual de las empresas aumenta la exposición en un entorno que ya se ha visto sometido a riesgos y complejidad. Un modelo de red regulado por transacciones radiales en una WAN privada está tan obsoleto como la defensa empresarial basada en el perímetro; tanto las arquitecturas de red como las de seguridad deben evolucionar. Si bien la tecnología SD-WAN actualmente permite a la red corporativa gestionar de forma eficaz el tráfico y mover cargas de trabajo a la nube, este modelo de red debe seguir iterando. Internet es la WAN corporativa del futuro cercano.

Akamai cree que el uso de la tecnología de red SD-WAN, combinado con los servicios de acceso y seguridad adecuados y compatibles con un modelo Zero Trust, es el primer paso para la transición a Internet como red corporativa. Combine la tecnología SD-WAN con Akamai Intelligent Edge Platform y podrá aplicar políticas de acceso y seguridad de forma universal, así como garantizar una experiencia de usuario final con las aplicaciones rápida y fiable a través de Internet.

Akamai puede ayudarle a dirigir la evolución de su red y su seguridad. Póngase en contacto con el equipo de su cuenta para obtener más información sobre la evaluación Zero Trust de Akamai. Recibirá recomendaciones tangibles de nuestros expertos en seguridad sobre dónde empezar o cómo avanzar en la transformación a un modelo Zero Trust. O bien, visite *3 maneras sencillas de iniciar la implementación de la seguridad Zero Trust hoy mismo* para obtener recursos que le permitan iniciar rápidamente su transición.