netskope

White Paper

Evolucione su seguridad de red del hoy al mañana

Cómo pasar a la seguridad de red y web nativa en la nube

Índice

INTRODUCCIÓN: EL PROBLEMA DE SEGURIDAD DE LAS REDES HEREDADAS

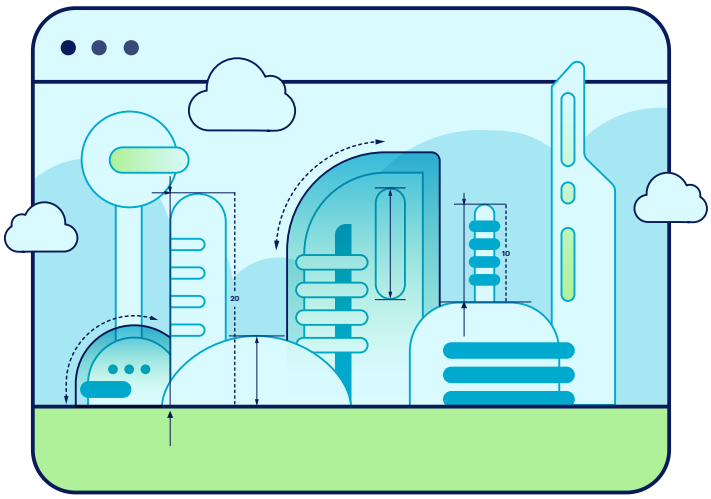
Tanto los equipos de redes como el grupo más general de infraestructuras y operaciones (I&O) son responsables del rendimiento y seguridad de la red en una organización. Un aspecto clave de ese trabajo es la seguridad de las redes en línea; es decir, supervisar y bloquear el tráfico de datos potencialmente maliciosos en tiempo real.

Durante muchos años, el debate sobre la mejor forma de hacerlo se ha centrado en las ventajas de los cortafuegos frente a las puertas de enlace *proxy*. Ciertos profesionales preferían uno u otro según las circunstancias de su organización, pero sus opciones se quedaban ahí.

Sin embargo, últimamente esa conversación se ha visto totalmente sobrepasada por los acontecimientos. El trabajo híbrido y las arquitecturas en la nube se han convertido en la nueva realidad para millones de organizaciones de todo el mundo debido a un proceso acelerado por la pandemia de covid, aunque enraizado en cambios tecnológicos que ya venían de largo.

En este contexto, quedan claras las carencias de los sistemas de seguridad de las redes heredadas. Los cortafuegos y puertas de enlace *proxy* tradicionales presentan problemas con la adaptabilidad, el rendimiento y la visibilidad en los entornos de *cloud-first* (la nube primero) y de teletrabajo. lo que provoca falta de eficiencia y brechas de seguridad. Es muy sencillo: los sistemas heredados no sirven para los objetivos que exige nuestra época de trabajo híbrido y teletrabajo.

Las organizaciones de hoy en día necesitan con urgencia seguridad nativa en la nube —como las soluciones de servicio de seguridad perimetral (SSE)— que ofrecen adaptabilidad y flexibilidad y se alinean con los principios del Zero Trust o confianza cero. Todas las respuestas tecnológicas están ahí, pero el desafío para los equipos responsables se encuentra en cómo pasar de forma prudente de los sistemas heredados a soluciones modernas como SSE sin aumentar la inversión actual ni abrir brechas de seguridad al migrar a nuevas formas de trabajo.



VISIÓN GENERAL DE LAS SOLUCIONES DE SEGURIDAD PARA REDES NATIVAS EN LA NUBE

Las soluciones de seguridad para redes nativas en la nube como SSE facilitan adaptabilidad, rendimiento y seguridad en organizaciones cada vez más diseminadas

En estas arquitecturas de red modernas hay tres elementos que tienen particular importancia.

Acceso Zero Trust a la red (ZTNA): Refuerza la premisa de que no se confía a ciegas en nadie y se aplican accesos con el menor privilegio posible; es decir, se concede un acceso de forma selectiva solo a los recursos que necesita una persona o un grupo, ni más ni menos.

Puerta de enlace web segura (SWG): Proporciona un control y seguridad minuciosos en el acceso a internet al mismo tiempo que se enfrenta a las amenazas y a los riesgos de datos en casos personales de aplicaciones gestionadas, miles de aplicaciones informáticas en la sombra y servicios en la nube.

Cortafuegos como servicio (FWaaS): Ofrece una seguridad de red uniforme en todos los puertos y protocolos de salida para obtener un acceso a internet directo y seguro por medio de un agente en dispositivos gestionados o, en el caso de las oficinas, por medio de Encapsulamiento Genérico de Enrutamiento (GRE) y Seguridad de Protocolo de Internet (IPsec). Entre los componentes que se suelen integrar se incluye la Seguridad DNS y los Sistemas de Prevención contra Intrusiones (IPS) para detectar y evitar ataques iniciados en los DNS e identificar amenazas en tiempo real, respectivamente.

Las soluciones de seguridad para redes nativas en la nube como SSE facilitan adaptabilidad, rendimiento y seguridad en organizaciones cada vez más diseminadas.

BENEFICIOS EN LA VIDA REAL

Cuatro formas de aportar valor empresarial mediante infraestructuras de seguridad modernas

El cambio a la SSE nativa en la nube permite a las organizaciones reforzar la seguridad de su red. Pero sus numerosas ventajas no se acaban ahí. Al modernizar su infraestructura, en realidad las arquitecturas SSE reducen costes, simplifican y hacen más eficientes los procesos operativos y mejoran el rendimiento de la red para mejorar la experiencia del usuario. Todas estas ventajas en conjunto ayudan a las organizaciones a mejorar su posición en el camino hacia el éxito en esta época digital.

BENEFICIO	IMPACTO
Consolidación de la infraestructura Al consolidar la infraestructura de seguridad de red dentro de un sistema moderno basado en la nube, las organizaciones podrán ir retirando sus sistemas y soluciones heredados.	y se aprovecharán de la reducción de costes relacionados con los servidores físicos, los equipos de redes y su mantenimiento. Forrester estima que el cambio de la seguridad heredada a las soluciones de servicio de seguridad perimetral (SSE) de Netskope en una organización normal genera un ROI del 109 % en un plazo de tres años, recupera la inversión en menos de seis meses y supone unos ahorros consolidados de 5,4 millones de dólares* solamente en infraestructuras.
Simplificación de las operaciones y gestión de seguridad La simplificación y automatización de los flujos de trabajo permite a los equipos centrarse en las iniciativas estratégicas y no en los problemas técnicos del día a día.	Como los procesos se vuelven más sencillos, las organizaciones pueden ahorrar tiempo a sus equipos de redes e I&O y al personal en general. Forrester calcula que las soluciones SSE de Netskope ayudan a los equipos de seguridad a recuperar más de 35 000 horas laborables, valoradas en 1,5 millones de dólares, lo que les permite dedicarse a actividades con mucho mayor impacto. Y, al mismo tiempo, se evitan unas 30 000 horas de trabajo por parte de los usuarios remotos de toda la organización, puesto que ya no necesitan perder el tiempo constantemente en procesos VPN*.
Mejora del rendimiento de la red La infraestructura en la nube moderna es más rápida y fiable; sufre menos tiempo de inactividad, menos interrupciones y goza de una mayor tasa de detección.	Según Forrester, con la adopción de sistemas modernos y ágiles, las organizaciones pueden llegar a reducir en un 80 % los volúmenes del servicio de asistencia y en un 60 % el tiempo medio de resolución (MTTR) de incidentes gracias a la SSE de Netskope. La SSE de Netskope ofrece una mayor visibilidad en el entorno del usuario, lo que en última instancia mejora la protección de la red y evita las pérdidas de datos. Netskope también ofrece una reducción del 15 % en los tiempos de inactividad imprevistos.
Refuerzo de las defensas Las soluciones nativas en la nube entienden y bloquean de forma más eficaz las ciberamenazas	Las soluciones modernas de SSE de Netskope pueden reducir en hasta un 80 % el riesgo de una infracción grave causada por un ataque externo, según Forrester.

*Cálculos basados en una organización mixta que sea una firma multimillonaria con 60 000 empleados (o su equivalente en jornada completa) en todo el mundo, la mitad de los cuales necesitarían acceder en remoto a las aplicaciones privadas de la empresa.

¿Cómo apoyan las soluciones nativas en la nube los hábitos de trabajo modernos?

Los cambios en los comportamientos implican nuevos enfoques de cara a la seguridad.

Los años anteriores a la pandemia de covid, como media, menos del 20 % de los empleados y trabajadores de las organizaciones trabajaban en remoto. Actualmente hay muchas organizaciones en las que esa cantidad se sitúa entre el 50 % y el 100 % ciertos días de la semana, ya que las políticas de trabajo híbrido se han generalizado.

Y, por tanto, también ha cambiado fundamentalmente el acceso remoto, web y SaaS (y todas sus funciones de seguridad asociadas). Las organizaciones confían cada vez más en puertas de enlace web seguras (SWG) basadas en la nube y en componentes de cortafuegos como servicio (FWaaS) suministrados dentro de plataformas de servicios de seguridad perimetral (SSE). Aunque sigue siendo necesario contar con cortafuegos para gestionar los requisitos de acceso entrante (en centros de datos y nubes públicas donde están instaladas las aplicaciones), ya no hacen falta en las ubicaciones externas: tiendas, sucursales u oficinas regionales.

Además, el Zero Trust Network Access (ZTNA) está sustituyendo a las VPN como el enfoque estándar para ofrecer un acceso seguro a servicios aprovechables de cara al público de forma remota y para permitir movimientos laterales una vez dentro. El modelo de conexión de «dentro hacia afuera» del ZTNA es más seguro y ofrece a los usuarios un acceso directo solo a las aplicaciones o recursos deseadas, limitando el alcance de cualquier agente malicioso.

El contenido y el contexto son ahora esenciales para lograr un control de acceso adaptativo en tiempo real

Las redes modernas, diseñadas en torno al principio ZTNA, adoptan un enfoque más contextual y en tiempo real para analizar el contenido y tomar decisiones de seguridad que sus equivalentes heredadas. Estas redes más adaptables e inteligentes resultan apropiadas para nuestra nueva generación de agilidad comercial, teletrabajo y acceso en la nube.

La inspección en línea del contenido y el contexto del software como servicio (SaaS) y de la infraestructura como servicio (IaaS) en tiempo real es el futuro del control de acceso para las soluciones SSE. En épocas tecnológicas anteriores, los cortafuegos perfeccionaron la inspección del tráfico en las redes y los SWG hicieron lo mismo con el tráfico web. Ahora, SSE unifica todos esos controles y además añade en línea un agente de seguridad para el acceso a la nube (CASB) e inspección según el contexto.

Según el riesgo de la aplicación, el riesgo de comportamiento, la posición del dispositivo, la actividad, la sensibilidad de los datos u otras variables, se aplica un control de acceso adaptativo a cada transacción comercial en función de su contenido y contexto.

Si un usuario desea borrar 100 archivos de datos confidenciales de la empresa, el acceso adaptativo puede solicitar una autenticación escalonada o pedir una justificación al usuario. Si otro usuario quiere acceder a una aplicación de almacenamiento en la nube no gestionada y de riesgo para mover archivos, el acceso adaptativo puede proporcionar una advertencia y ofrecer opciones de almacenamiento en la nube más seguras y aprobadas por la empresa.

Este enfoque de «orientación en tiempo real» se parece mucho al uso que le damos ahora a la navegación satélite o al GPS al conducir: alerta a los usuarios de posibles rutas erróneas y los redirige hacia alternativas más seguras siempre que se pueda. Los usuarios de las empresas modernas se benefician de esta especie de guía al desplazarse por sus redes.

MIGRACIÓN CON CONFIANZA

Un marco para la aplicación del SSE por fases

No hay por qué pasar de golpe de los sistemas de seguridad para redes heredadas a las modernas soluciones de SSE. De hecho, no se debería. Adoptar un enfoque por fases, con una transición gradual con el paso del tiempo acumulando metódicamente sucesivas implementaciones de éxito, es la mejor forma de conseguir mejorar los resultados sin poner en riesgo el rendimiento y, al mismo tiempo, sacándole el máximo partido a la inversión existente.

PASOS CLAVE	MEJORES PRÁCTICAS
Evaluación y planificación iniciales Lo primero es lo primero: analice su posición de seguridad actual e identifique las lagunas que podría mejorar el SSE. Evalúe la arquitectura de su red, las soluciones de seguridad existentes y las necesidades comerciales específicas para descubrir dónde le puede ser de más ayuda el SSE.	Elabore una estrategia clara para la aplicación del SSE que incluya la definición de objetivos, los resultados esperados y los indicadores clave de rendimiento (KPI).
Elección del proveedor de SSE adecuado Evalúe los posibles proveedores de SSE según su capacidad para cumplir sus requisitos y casos de uso concretos. Tenga en cuenta factores como la exhaustividad de sus servicios de seguridad, la arquitectura subyacente, la facilidad de integración con los sistemas existentes, su servicio de atención al cliente y la relación calidad-precio.	Haga una selección inicial de proveedores y, con los que la pasen, realice una prueba piloto en su entorno para ver cómo la solución SSE gestiona sus necesidades de seguridad, patrones de tráfico de redes y requisitos de visibilidad concretos.
Despliegue por fases Colabore con el proveedor que elija hasta alcanzar una configuración de la solución SSE que se adapte a sus necesidades de seguridad y requisitos de conformidad concretos. Esta personalización puede suponer el establecimiento de unas reglas de seguridad, la configuración de unos ajustes de prevención de pérdida de datos (DLP) y la definición de unos controles de acceso.	Integre la solución SSE a su estructura informática actual, como sistemas de gestión de identidad, infraestructura de red y otras herramientas de seguridad. Una integración adecuada es vital para conseguir un funcionamiento impecable y maximizar el valor de su solución SSE, así que evalúe a los vendedores basándose en su ecosistema de socios e integraciones.
Énfasis en la experiencia de usuario Ofrezca una formación completa antes de cada fase del despliegue. Comunique los cambios con bastante antelación y supervise los comentarios de los usuarios para abordar cuanto antes cualquier problema.	Use herramientas de análisis para ir supervisando la eficacia de la seguridad y su adopción por parte de los usuarios. Establezca un seguimiento de auditorías para demostrar la mejora en la seguridad a lo largo del tiempo.

Los pilares para el éxito a largo plazo

¿Por qué son tan importantes los marcos de confianza cero?

A medida que el perímetro de red tradicional se ha ido disolviendo y con el aumento del teletrabajo y los servicios en la nube, el enfoque Zero Trust se ha vuelto fundamental para conseguir una seguridad de red eficaz. Los principios de confianza cero pretenden eliminar el acceso implícito, perfeccionar el acceso de privilegio mínimo y supervisar de manera continua. Es un reflejo del aumento de la sofisticación de las ciberamenazas y ofrece una mejor visibilidad y control a los profesionales de la seguridad.

De media, las organizaciones usan más del triple de aplicaciones de IA generativa (y tienen casi tres veces más usuarios activos) en 2024 que en el año anterior.

Sin embargo, el enfoque Zero Trust se suele malinterpretar, ya que muchas explicaciones se centran únicamente en el acceso seguro de confianza cero y pasan por alto el hecho de que los datos fluyen a través de todos los demás componentes de confianza cero (usuarios, aplicaciones, dispositivos y redes).

Las soluciones SSE combinan las capacidades CASB y SWG en un *proxy* principal en línea con FWaaS y ZTNA para redefinir las funciones tradicionales del NGFW y la VPN a fin de respaldar los principios de confianza cero. El resultado: una infraestructura más resiliente y segura. Otro elemento importante es que el SSE adapta su tamaño y rendimiento según cada usuario, dispositivo o ubicación para ofrecer una gran experiencia de usuario, además de eliminar la disyuntiva entre rendimiento y seguridad en lo que respecta a la visibilidad del contenido.

La divulgación de código fuente privado en cuentas de aplicaciones de IA generativa supone el 46 % de todas las vulneraciones de políticas de datos.

Las empresas que cuenten con un marco de confianza cero y una solución moderna de SSE ya gozarán de unos pilares sólidos sobre los que construir una seguridad sostenible que puede flexibilizar su escala y adaptarse a medida que dichas empresas crezcan y se transformen, sin dejar de mantener unos controles de seguridad constantes en todos los entornos y casos de uso.

El impacto de la IA

La inteligencia artificial (IA) y el aprendizaje automático (AA) se llevan utilizando en segundo plano durante muchos años en motores de defensa contra amenazas, clasificación de datos, clasificaciones dinámicas de URL y planificación de operaciones de TI, entre otras áreas. Ahora las defensas basadas en IA y AA se están integrando en línea para funcionar en tiempo real y detectar nuevas amenazas de día cero desconocidas e identificar datos confidenciales en documentos e imágenes.

Los datos regulados, regidos por normativas sectoriales o requisitos de cumplimiento, suponen el 35 % de todas las vulneraciones de políticas de datos y la propiedad intelectual supone el 15 %.

El propio auge de la IA permite a los agentes, tanto buenos como malos, desarrollar rápidamente nuevos códigos y contenido además de aprender con rapidez. En este sentido, el auge de la IA también puede ser peligroso, ya tiene potencia de dejar expuestos datos confidenciales. Por ejemplo, el contenido más popular que se envía a aplicaciones de IA como ChatGPT es el código fuente.

Las defensas heredadas no están en condiciones de permitir instancias empresariales de IA frente al control de instancias públicas y personales para los usuarios; tampoco pueden proporcionar la capacidad de identificar contenido como el código fuente del que se alimentan las aplicaciones de IA.

En cambio, las defensas en línea basadas en IA/AA ya son capaces hoy en día de detectar archivos ejecutables maliciosos y ataques de suplantación de identidad, además de poder clasificar docenas de documentos e imágenes, incluido el código fuente. A medida que las empresas van adoptando rápidamente las aplicaciones de IA y sus diferentes usos, cualquier estrategia de seguridad de red a prueba de futuro debe ser capaz de responder a estos tipos de riesgos.

CONCLUSIÓN: LA EVOLUCIÓN DE LA SEGURIDAD ES UN IMPERATIVO

La tecnología empresarial y el comportamiento individual están en constante evolución. En los últimos años hemos visto de cerca esa realidad, a medida que el cambio hacia la nube, la explosión del teletrabajo y el trabajo híbrido así como el auge de la IA han transformado nuestras vidas diarias.

Para los profesionales de redes y de infraestructuras y operaciones, el requisito más urgente en este momento es modernizar las arquitecturas en consonancia con los cambios que suceden a su alrededor. Ese proceso tiene dos caras.

En primer lugar, los equipos deberían analizar cuidadosamente sus sistemas heredados. Se está produciendo un cambio constante hacia la inspección en línea de SaaS e IaaS, más defensas en línea de IA/AA y la oferta de accesos adaptativos con formación en tiempo real para los usuarios. En este contexto, renovar las soluciones NGFW, SWG y VPN podría suponer un error muy caro.

En segundo lugar, las organizaciones deberían trazar un mapa de migración hacia soluciones SSE modernas. Desglosarlo en varias fases es la mejor forma de hacerlo más manejable y efectivo. Evita tener que abandonar los sistemas existentes sin más y ayuda a los equipos de redes a ganar confianza en nuevas formas de hacer las cosas a través de toda la empresa.

El entorno informático no deja de evolucionar y, seguramente, lo que definirá el éxito de una organización será lo rápido que pueda adaptarse a esos continuos cambios para capitalizar su impacto. En el caso de los profesionales de las redes e infraestructuras y operaciones, aunque pueda parecer una transición complicada, también es posible simplificarla y, al final, promete recompensas muy jugosas en cuanto a rendimiento, productividad y reducción de costes.

¿Le gustaría obtener más información?

Solicite una demostración

Netskope, líder en seguridad y redes modernas, atiende las necesidades tanto de los equipos de seguridad como de redes proporcionando acceso optimizado y seguridad basada en contexto en tiempo real para las personas, dispositivos y datos estén donde estén. Miles de clientes, incluidas más de 30 empresas de Fortune 100, confían en la plataforma Netskope One, su motor Zero Trust y su potente red NewEdge para reducir riesgos y obtener una visión completa de cualquier actividad en la nube, la IA, la web y las aplicaciones privadas, ofreciendo siempre seguridad y acelerando el rendimiento sin renunciar a nada.