GUÍA PARA LA ADOPCIÓN de Secure Access Service Edge (SASE)

¿Está su arquitectura lista para SASE?

¿Está su arquitectura lista para SASE?

Desafíos del mercado

Las infraestructuras IT de las empresas se encuentran inmersas en una gran transformación para reestructurar la manera en la que sus empleados, aplicaciones informáticas y datos se implementan y utilizan. Las iniciativas de transformación digital han acelerado el movimiento de datos corporativos a la nube, el cual se ha complicado por el creciente número de empleados móviles que siguen necesitando un acceso seguro y una experiencia de usuario consistente. Durante este proceso, las empresas han llegado a la conclusión de que su infraestructura física de red y seguridad debe evolucionar para poder proteger un entorno con un perímetro cada vez menos delimitado. La rápida convergencia entre seguridad, redes y servicios en la nube está creando un nuevo modelo en el que la seguridad y las redes ya no están compuestas de appliances o dispositivos, sino de servicios de software y aplicaciones basadas en la nube. De ese modo, las organizaciones dispondrán de un entorno simplificado basado en la nube cimentado en la consolidación de múltiples tecnologías de seguridad y en una experiencia de usuario mucho más optimizada con un coste menor.

El término «SASE» (Secure Access Service Edge), acuñado recientemente por Gartner, describe este nuevo marco de redes y seguridad. El modelo SASE de Gartner está diseñado para hacer frente al nuevo contexto de seguridad que está cambiando a causa de la transformación digital. Cada vez es más común que los usuarios, los datos y las aplicaciones estén en la nube en vez de en el tradicional centro de datos, y es necesario gestionar y garantizar la seguridad en consecuencia. Los servicios de seguridad necesarios, como los Secure Web Gateways (SWG, por sus siglas en inglés), los Cloud Access Security Brokers (CASB), las soluciones de prevención de pérdida de datos (DLP) y la protección contra amenazas avanzada (ATP), convergen en este modelo nativo en la nube y utilizan una red perimetral global de gran capacidad y baja latencia para ofrecer una experiencia de usuario optimizada.

Netskope ha sido nombrado líder del sector en el informe de Gartner «El futuro de la seguridad en la red está en la nube», el cual describe sus estudios, análisis y recomendaciones. Netskope ha desarrollado una plataforma de seguridad nativa de la nube y ya preparada para SASE con el objetivo de escalar de forma dinámica y proporcionar servicios de seguridad tanto a las empresas como a sus usuarios en todo el mundo.

LA VISIÓN DE NETSKOPE DEMUESTRA QUE SON CONSCIENTES DE LA IMPORTANCIA DEL EMERGENTE MERCADO SASE Y QUE ACTUALMENTE SE SITÚAN POR DELANTE DE CUALQUIER OTRO PROVEEDOR CASB CON ESTE ENFOQUE.

Gartner Magic Quadrant for Cloud Access Security Brokers, octubre de 2019, de los analistas Steve Riley y Craig Lawson

Pilares del valor de SASE

De acuerdo con Gartner, los líderes en seguridad informática deberían considerar las siguientes recomendaciones a la hora de desarrollar una arquitectura lista para SASE:

- **Utilice una arquitectura nativa de la nube:** comprenda que SASE facilita la transformación digital al ofrecer una mayor velocidad, agilidad y disponibilidad. Cambie la gestión de cajas de seguridad por servicios de seguridad basados en políticas mediante un entorno nativo de la nube y basado en microservicios.

- **Consolide las defensas de seguridad:** considere la convergencia de tecnologías de seguridad en la web y la nube para simplificar la configuración y las operaciones, además de reducir costes (por ejemplo, SWG, CASB, ZTNA, DLP).

- **Siga un modelo centrado en los datos:** implemente controles conscientes del contexto para detectar y prevenir de inmediato el movimiento de datos sensibles desde o hacia la web y la nube, así como entre instancias personales y corporativas de las aplicaciones en la nube.

- **Protéjase frente a las amenazas de la nube:** el panorama actual de las ciberamenazas es muy diferente con respecto al de hace algunos años debido a que predominan las amenazas originadas en la nube, como el *phishing*. Familiarícese con los riesgos propios de la nube y combine las capacidades para inspeccionar amenazas y datos para desarrollar una solución de inspección eficiente y en un único paso.

- **Desarrolle la estrategia de acceso remoto:** las anticuadas VPN que necesitan una comunicación *hairpinning* con una sede principal resultan ineficaces, costosos y difíciles de mantener. Considere la adopción de un enfoque *zero trust* con el que se puedan conectar de manera segura los usuarios y las aplicaciones desde cualquier ubicación, en vez de proporcionar simplemente un acceso a la red menos seguro.

- **Utilice una red periférica global y resistente:** debido a que los proveedores de servicios de internet y de nube proporcionan redes basándose en reducir sus propios costes, es fundamental considerar una arquitectura lista para SASE que proporcione una red de alto rendimiento y de alta capacidad a nivel global sin poner en riesgo la seguridad. Compruebe la infraestructura de red que ofrece su proveedor de seguridad para verificar si realmente está listo para SASE y si es capaz de soportar las comunicaciones con una importante presencia en la nube. Si utiliza soluciones de red de área amplia definida por software (SD-WAN, por sus siglas en inglés), conéctelas con esta red periférica para una mayor eficiencia y rendimiento.

- **Integre controles en la nube:** como hemos explicado anteriormente, no solo es fundamental consolidar el uso de las tecnologías de seguridad, como CASB, SWG o CSPM, para estar listo para SASE, sino que es igualmente importante conjugar e integrar sus herramientas de gestión y administración para reducir la complejidad y aumentar la eficiencia. Las soluciones que realmente integran consolas e interfaces de usuario, además de clientes de puntos terminales (agentes), ofrecen una mayor simplicidad frente al caos.

Esta guía de adopción profundiza en estos puntos que acabamos de exponer para ayudarle a entender qué debe tener en cuenta a la hora de evaluar e implementar una arquitectura de seguridad lista para SASE.

Cloud-Native Architecture

Desafíos del mercado

SASE opera en la nube para proteger los datos, los usuarios y las aplicaciones de las empresas en la nube. Para ello, necesita un marco nuevo en el que se integren de forma nativa funciones avanzadas de red y seguridad en la nube. Esto requiere un enfoque de microservicios en la arquitectura para poder construir y entregar rápidamente nuevas características, además de escalar elásticamente para ajustarse a la demanda. También debe ser diseñado para una alta resistencia y una baja latencia. Una arquitectura que depende de herramientas de red y seguridad tradicionales que simplemente se convierten a software en la nube no está preparada para adoptar SASE. Este enfoque —tan generalizado como enmarañado— no permite escalar, presenta problemas de interoperabilidad, es incapaz de desarrollar nuevas funcionalidades rápidamente y proporciona servicios de seguridad con una mayor latencia.

Beneficios de SASE

Una arquitectura nativa de la nube, que haya sido desarrollada desde cero, garantiza que su proveedor SASE comprende cómo y por qué utilizar una arquitectura de software basada en microservicios permite proporcionar servicios de seguridad fluidos que responderán a sus necesidades a la hora de reducir riesgos. Además, este enfoque garantiza el futuro de su inversión en una arquitectura que se adapta rápidamente a los cambios del mercado de redes y seguridad de las empresas, que construye nuevos productos de forma nativa y que proporciona servicios de seguridad que no interfieren con la productividad del negocio o afectan a la experiencia de usuario.

¿Qué preguntas debe hacer?

- Pregúntele a su proveedor SASE cómo ha construido su plataforma en la nube. ¿Su arquitectura tiene garantías de futuro en la nube?
- ¿Ha migrado sin más sus appliances y software de seguridad a la nube?
- ¿O ha construido su plataforma de forma nativa desde cero en una arquitectura de software basada en microservicios?
- ¿Cómo se puede optimizar para desarrollar nuevas funcionalidades de forma rápida?
- ¿Su infraestructura de red subyacente es capaz de proporcionar una baja latencia y una alta capacidad a nivel mundial?

LAS ARQUITECTURAS TRADICIONALES DE REDES Y DE SEGURIDAD DE REDES QUE TIENEN COMO PRINCIPAL PUNTO DE ACCESO LOS CENTROS DE DATOS DE LAS EMPRESAS RESULTAN CADA VEZ MÁS INEFICACES Y COMPLICADAS EN UN MUNDO MÓVIL Y EN LA NUBE.

Gartner, The Future of Network Security Is in the Cloud, agosto de 2019, de los analistas Neil MacDonald, Lawrence Orans y Joe Skorupa

Next Generation Secure Web Gateway (NG SWG)

Desafíos del mercado

Los Proxy Web o Secure Web Gateways (SWG) sirven para impedir que los usuarios de una empresa accedan a sitios web maliciosos capaces de mermar la seguridad general de una organización. Con una solución SWG, los responsables de seguridad pueden identificar, clasificar y bloquear contenido o malware para que no entren en la red corporativa a través del tráfico web. El mercado de los SWG se está transformando: los appliances físicos están dejando paso a las capacidades SWG en la nube. De ahora en adelante, una solución SWG deberá construirse de forma nativa en la nube para identificar, gestionar y garantizar la seguridad del tráfico web, entre otras funciones, de forma escalable.

Beneficios de SASE

SASE permite la implementación de capacidades SWG, además de otros servicios de red y seguridad en la nube, como CASB, DLP o ATP. Netskope define a estos servicios de seguridad consolidados como Next Generation Security Web Gateways (NG SWG, por sus siglas en inglés). Esta solución identifica y decodifica el tráfico web y las aplicaciones basadas en la nube para extraer el contexto de forma detallada, como por ejemplo las instancias personales o corporativas de la misma aplicación en la nube (Office 365, Gmail o Slack). Las empresas se benefician de una visión general del tipo de ciberamenazas que sufren las organizaciones al incorporar el contexto obtenido de los servicios integrados de seguridad y red dentro de la plataforma lista para SASE. Con la ayuda de un motor de aplicación de políticas unificado, la NG SWG proporciona una mayor protección al identificar, gestionar y garantizar la seguridad del tráfico web y de las aplicaciones basadas en la nube, al detectar y atenuar las amenazas cloud y, por último, al reforzar las capacidades de protección de pérdida de datos.

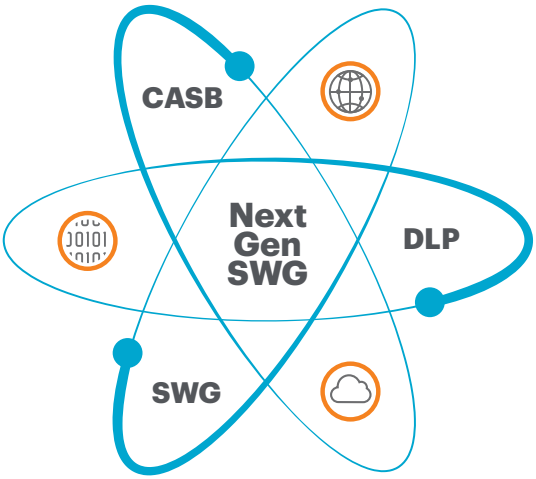
¿Qué preguntas debe hacer?

- ¿Su proveedor admite todas las capacidades de una solución Next Generation Secure Web Gateway dentro de su arquitectura SASE?
- ¿Su proveedor SASE comprende el contexto a nivel granular de las instancias de aplicaciones, como la distinción entre instancias personales o instancias corporativas en las aplicaciones cloud (por ejemplo, en Office365, G Suite, Slack)?
- Si la respuesta es negativa, ¿cómo se protege su proveedor SASE de la filtración de datos sensibles dentro de las aplicaciones en la nube autorizadas?
- Si la respuesta es negativa, ¿cómo se protege de la filtración de datos fuera del perímetro corporativo por parte de un usuario interno malicioso o un cibercriminal?

VALORE HOY MISMO LAS OPORTUNIDADES A CORTO PLAZO PARA LA CONSOLIDACIÓN Y COMPLEJIDAD DE LOS SERVICIOS SASE, COMO LA INTEGRACIÓN PARCIAL O COMPLETA DE CASB, SWG, ZTNA, VPN O LAS CAPACIDADES DE AISLAMIENTO DE LOS NAVEGADORES REMOTOS.

Gartner, The Future of Network Security Is in the Cloud, agosto de 2019, de los analistas Neil MacDonald, Lawrence Orans y Joe Skorupa

Netskope Next Generation Secure Web Gateway



CASB + SWG + DLP unificados y nativos de la nube

Cloud Access Security Broker (CASB)

Desafíos del mercado

Al transferir sus aplicaciones a la nube, las empresas ya no pueden depender de cortafuegos en un servidor local para proteger sus datos, ya que dichos sistemas no detectan el tráfico actual de la nube, como las solicitudes de API o la notación de objeto de JavaScript (JSON, por sus siglas en inglés). Además, los datos corporativos se están transfiriendo principalmente desde un centro de datos centralizado dentro del perímetro de la empresa a un número cada vez mayor de soluciones SaaS y servicios de nube pública/IaaS fuera del perímetro, lo cual complica la capacidad de los equipos de operaciones de seguridad (SecOps, en inglés) para gestionar las políticas de seguridad de una manera consistente y coherente. Los vectores de ataque de los cibercriminales ahora ponen el punto de mira en los datos corporativos alojados en las aplicaciones SaaS y IaaS, que a menudo disponen de controles de seguridad nativos limitados. Los clientes necesitan un conjunto de controles de seguridad de mayor profundidad para tener una mejor visibilidad detallada de las actividades realizadas en los servicios SaaS, web o IaaS, independientemente de si se han realizado en dispositivos gestionados o no gestionados.

Beneficios de SASE

Los CASB basados en SASE pueden ayudar a las organizaciones a llevar a cabo controles de seguridad consistentes en los servicios SaaS, Web o IaaS para así reducir la superficie de ataque y proteger los datos más sensibles. Los CASB pueden ayudar a los clientes a activar los controles de seguridad de los datos en tránsito y los datos en reposo mediante una combinación de modos de implementación. Al utilizar una mezcla de defensas capacitadas para API y defensas integradas, los CASB modernos detectan las aplicaciones en la nube en uso y evalúan sus riesgos potenciales, además de garantizar la protección ante pérdidas de datos sensibles y la propagación de amenazas utilizando capacidades DLP y ATP. Dado que protegen los datos corporativos más sensibles en las aplicaciones en la nube, tanto gestionadas como no gestionadas, los CASB son la base de una arquitectura lista para SASE y suponen un complemento para otras tecnologías de seguridad necesarias.

POR TERCER AÑO CONSECUTIVO, GARTNER CONSIDERA A NETSKOPE COMO UN LÍDER DEL SECTOR EN EL «MAGIC QUADRANT FOR CLOUD ACCESS SECURITY BROKERS» POR SU VISIÓN GLOBAL Y SU CAPACIDAD PARA LA EJECUCIÓN.

Gartner Magic Quadrant for Cloud Access Security Brokers, octubre de 2019, de los analistas Steve Riley y Craig Lawson

¿Qué preguntas debe hacer?

- ¿Su proveedor SASE ofrece controles capacitados para API (para los datos en reposo) e integrados (para los datos en tránsito)?
- ¿Puede aplicar las mismas políticas de prevención de pérdida de datos (DLP) en aplicaciones en la nube y sitios web con un marco de políticas y una consola de administración únicos?
- ¿Puede decodificar información (usuario, ubicación, actividad, aplicación, entre otros) para favorecer los controles de políticas detallados y conscientes del contexto?
- ¿Puede distinguir entre instancias de las mismas aplicaciones en la nube, como por ejemplo diferenciar las instancias personales y corporativas de Gmail u Office365?

Prevención de pérdida de datos (DLP)

Desafíos del mercado

A las empresas siempre les ha resultado difícil gestionar el incremento y control de los datos sensibles. Esta problemática se ha agravado por el rápido crecimiento de las aplicaciones y los servicios en la nube, así como por el aumento de usuarios móviles que trabajan en remoto. El principal problema para las empresas se concentra en escalar la clasificación de datos para que los datos sensibles estén etiquetados correctamente de manera que la política de DLP pueda detectar y prevenir de forma precisa la salida de datos sensibles de la empresa. En un entorno actual de «cloud first», las soluciones DLP anticuadas no logran rastrear la pérdida ni la exfiltración de datos sensibles a servicios o dispositivos personales en la nube, y además siguen dando un excesivo número de falsos positivos. Para complicar aún más su tarea, las empresas deben cumplir con regulaciones (como PCI, PHI, HIPAA, RGPD) que obligan a la protección de datos de los clientes, con el riesgo de recibir multas cuantiosas y ver dañada su imagen en caso de incumplimiento. Las empresas han comprendido que las soluciones DLP tradicionales en servidores locales no están diseñadas para gestionar el rápido aumento de los datos y su migración hacia la nube.

Beneficios de SASE

Con SASE, la protección de datos es una parte integrada dentro del marco de seguridad en la nube. Las soluciones DLP modernas en la nube ofrecen una visibilidad completa y, en el mejor de los casos, un conocimiento contextual del movimiento de datos en la nube, además de una reducida pérdida y exfiltración de datos. Para poder escalar y optimizar su DLP, las políticas deben estar basadas en datos. El énfasis debe estar puesto en los propios datos independientemente de la aplicación. La gestión de las políticas DLP se simplifica ya que se aplican las mismas políticas en todas las aplicaciones en la nube y sitios web. Se emplea el mismo conjunto de políticas DLP tanto en los datos en reposo como en los datos en tránsito para que haya una protección siempre activa dondequiera que se muevan los datos. Un entorno listo para SASE debe identificar, clasificar y comprender de forma efectiva los datos para así proporcionar una comprensión granular que favorezca las políticas basadas en el contexto, como usuario, tipo de dispositivo, tipo de archivo, identificadores de datos, etc. Por último, para que las empresas puedan cumplir con las regulaciones, es fundamental contar con un sistema de monitorización y de generación de informes intuitivo y personalizable.

LOS PRINCIPALES DESAFÍOS DE SEGURIDAD EN LA NUBE PARA LOS PROFESIONALES DE CIBERSEGURIDAD SON LA PRIVACIDAD DE LOS DATOS (52 %) Y LA FUGA DE DATOS (51 %).

2019 Cloud Security Report, Cybersecurity Insiders, marzo de 2019

¿Qué preguntas debe hacer?

- ¿Su proveedor de SASE tiene un número limitado de aplicaciones o servicios compatibles con su DLP?
- ¿El motor de DLP es capaz de identificar y procesar los patrones de datos que son relevantes para su empresa?
- ¿Se puede aplicar la misma política DLP a los datos en reposo y a los datos en tránsito?
- ¿Utiliza inteligencia artificial o aprendizaje automático (AI/ML, en inglés) para mejorar su DLP? ¿De qué manera las utiliza?
- ¿La solución DLP de su proveedor SASE ofrece protección para cualquier usuario, dispositivo o ubicación, incluido el uso de navegadores, clientes de sincronización y aplicaciones móviles?
- ¿Durante cuánto tiempo mantienen los metadatos completos sobre el tráfico web y los servicios en la nube para poder proporcionar un análisis más optimizado? *(Consejo:* el periodo mínimo debería ser 90 días).

Protección contra amenazas avanzada (ATP)

Desafíos del mercado

Los equipos de operaciones de seguridad se encargan de desarrollar defensas de múltiples capas para ofrecer un modelo de seguridad en profundidad que cuente con múltiples fuentes de inteligencia de amenazas, protección de terminales, protección ante amenazas en la nube y defensas de red tradicionales. Esta estrategia generalizada presenta sus desafíos ya que normalmente los equipos de operaciones de seguridad siguen un enfoque de seguridad, el mejor de su clase, que resulta complejo, costoso y difícil de mantener (especialmente por el uso de productos diferentes, la falta de personal y de especialización); o recurren a una solución de un único proveedor que resulta menos compleja o costosa, pero que carece de las capacidades de seguridad necesarias (como controles granulares o descifrado SSL/TLS). Con el rápido auge de las amenazas capacitadas para la nube, como el *phishing*, las soluciones anticuadas cada vez tienen menos capacidad para detectar las amenazas y, por lo tanto, plantean un riesgo considerable. Será necesaria una solución basada en la nube capaz de escalar para ofrecer protección ante amenazas en tiempo real (escaneo rápido) o mediante escaneo profundo (entorno aislado o *sandboxing*) en la nube para exponer y mitigar de forma efectiva cualquier malware o amenaza.

Beneficios de SASE

Una solución ATP basada en un modelo SASE puede ayudar a reducir de forma significativa las complejidades y los costes a los que se enfrentan los equipos de operaciones de seguridad y los equipos de respuesta frente a incidencias, además de optimizar la eficacia ante las amenazas y la escalabilidad. Este tipo de solución ATP basada en SASE puede permitir centralizar todas las incidencias de seguridad recogidas en las nubes gestionadas y no gestionadas ya que proporcionará una vista consolidada y centralizada de todas las actividades mediante un enfoque de múltiples capas (por ejemplo, descompresión recursiva, heurística en preejecución, *sandboxing*, aprendizaje automático). Esta solución debe recopilar metadatos completos del tráfico en la web y en la nube para realizar un análisis y estudio en profundidad que ayude a los equipos internos de respuesta frente a incidencias o a los servicios administrados de detección y respuesta (MDR, por sus siglas en inglés). Por último, una solución ATP lista para SASE debe prevenir y detectar las amenazas utilizando los servicios modernos en la nube para acabar con los ciclos de vida de un ciberataque, lo cual no es posible con las defensas anticuadas o incluso con las defensas de terminales modernas.

LOS ATAQUES DE *PHISHING* EN SAAS/ WEBMAIL (UN 36 % DEL TOTAL) YA SUPERAN LAS AMENAZAS EN EL SECTOR DE PAGOS Y FINANZAS. PARA BLOQUEARLOS, ES NECESARIO SER CONSCIENTE DE LAS INSTANCIAS DE MILES DE SERVICIOS EN LA NUBE.

Phishing Activity Trends Report, Anti-Phishing Working Group, mayo de 2019

¿Qué preguntas debe hacer?

- ¿Su proveedor SASE puede inspeccionar un número limitado de servicios en la nube gestionados o no gestionados cifrados con TLS?
- ¿Puede describir cómo prevendrían una instancia personal o no autorizada proveniente de un servicio en la nube que estuviese haciendo un ataque de *phishing* en la nube?
- ¿Cómo proporciona la misma protección ante amenazas a oficinas y usuarios en remoto, tanto si usan navegadores como si emplean clientes de sincronización o aplicaciones?
- ¿Dispone de capacidades ATP que se optimizan con inteligencia artificial o aprendizaje automático?
- ¿Cuenta con integraciones de terceros con soluciones como EDR, RBI, SIEM, o SOAR, además de compartir inteligencia de amenazas?

Zero Trust Network Access (ZTNA)

Desafíos del mercado

Las organizaciones se han vuelto más globales y dispersas; esto requiere extender los perímetros de la empresa a los trabajadores de oficinas remotas. Los usuarios en remoto necesitan un acceso seguro a los recursos de la empresa sin que se ponga en riesgo su seguridad y sin que afecte a la experiencia de usuario. Hasta ahora, los equipos de seguridad habían utilizado implementaciones con dispositivos VPN (IPSec y SSL/TLS) complejos y costosos que no escalan, incurren en altos gastos de mantenimiento y resultan difíciles de gestionar. Debido al acceso «abierto» a la red que ofrece una VPN, se pueden producir fácilmente exfiltraciones de datos sensibles a aplicaciones en la nube. Además, las cuentas vulneradas y los usuarios internos pueden desplazarse lateralmente dentro de la red y llevar a cabo actividades maliciosas. Con la rápida transición de aplicaciones y datos a la nube, los equipos de operaciones de seguridad necesitan una solución moderna de acceso seguro que sea escalable fácilmente y que permita un acceso seguro a los usuarios en remoto a determinadas aplicaciones privadas en nubes y centros de datos públicos, independientemente de su ubicación.

Beneficios de SASE

Un proveedor SASE puede ofrecer una solución de seguridad en la nube que permita un acceso a nivel de aplicaciones a aplicaciones privadas basadas en principios Zero Trust. Esto incluye la autenticación de los usuarios y la comprobación y clasificación de la postura del dispositivo, *antes* de conectar a los usuarios para seleccionar aplicaciones privadas. Además, para reducir la superficie de ataque y ayudar a prevenir posibles ciberataques e intrusiones, las aplicaciones privadas publicadas no deberían ser visibles o accesibles por parte de usuarios no autorizados. Este enfoque reduce la necesidad de implementar servicios de protección costosos, como cortafuegos de aplicaciones web (WAF, en inglés) o ataques de denegación de servicio distribuido (DDoS, en inglés), para impedir que las actividades de ciberataque tengan un impacto en la operación y accesibilidad de las aplicaciones corporativas. Una solución de acceso lista para SASE debe simplificar y optimizar la experiencia de acceso remoto en general, al tiempo que utiliza la misma infraestructura de alto rendimiento disponible para otras tecnologías y controles de seguridad nativas de la nube.

MÁS DEL 75 % DE LOS ENTREVISTADOS CONSIDERA IMPORTANTE CONSOLIDAR LOS SERVICIOS DE SEGURIDAD ZTNA CON OTROS SERVICIOS DE SEGURIDAD EN LA NUBE, COMO CASB O SWG.

2020 Zero Trust Report, Cybersecurity Insiders, febrero de 2020

¿Qué preguntas debe hacer?

- ¿Su proveedor SASE ofrece una estrategia Zero Trust?
- En caso afirmativo, ¿cómo ha implementado su solución ZTNA? ¿Ha migrado un producto de un tercer proveedor en su plataforma?
- ¿Se puede acceder a las aplicaciones corporativas publicadas desde cualquier sitio en Internet?
- ¿Se necesitan o se utilizan conexiones entrantes en su solución de acceso remoto?
- ¿Necesitan servicios de protección WAF o DDoS para complementar la protección de aplicaciones publicadas?

Software-Defined WAN (SD-WAN)

Desafíos del mercado

El mercado de SD-WAN surgió como una alternativa para las empresas para hacer frente a la costosa implementación de mecanismos de conmutación de etiquetas multiprotocolo (MPLS, en inglés) utilizada para conectar de forma segura sus oficinas remotas a las redes corporativas. Para complicar aún más la situación, las oficinas remotas necesitan implementar múltiples dispositivos de red y seguridad físicos en cada ubicación que pueden incluir: SWG o Proxy Web, inspección SSL/TLS, *anti-malware*, cortafuegos de nueva generación, IPS, VPN, etc. Para una organización media, estos gastos pueden escalar rápidamente, lo cual puede ejercer una mayor presión sobre los límites presupuestarios en los gastos de capital (CapEx, en inglés) y los gastos de operación (OpEx) para operar la red corporativa. Los productos SD-WAN y las soluciones de seguridad que hayan sido integrados adecuadamente se complementan bien a la hora de proporcionar un acceso seguro.

Beneficios de SASE

El modelo SASE permite una integración fluida de la funcionalidad SD-WAN en una arquitectura basada en la nube, donde la funcionalidad SD-WAN ha sido construida de forma nativa e integrada con los servicios de seguridad. De esta manera, se puede escalar el rendimiento y la distribución para los usuarios en oficinas remotas. Las organizaciones pueden reducir los gastos y la complejidad que entraña la implementación de múltiples dispositivos de red y seguridad en toda la red corporativa. Las arquitecturas listas para SASE permiten que las soluciones periféricas SD-WAN se conecten directamente a la red periférica en la nube, por lo que se evita la compleja implementación de *hubs* SD-WAN físicas. Este modelo de acceso también puede ayudar a simplificar las múltiples superposiciones que complican aún más la gestión de las redes corporativas.

¿Qué preguntas debe hacer?

- ¿Cómo implementa su proveedor SASE su solución de conectividad entre sucursales mediante SD-WAN?
- ¿Cuántos dispositivos físicos debe implementar su proveedor SASE para ofrecer la funcionalidad SD-WAN? Si dicho número debe aumentar a medida que su negocio se expande, ¿está usted preparado para asumir el coste y el mantenimiento?
- ¿Su solución está integrada en una plataforma nativa de la nube o se encuentra en servicios de colocación diferentes con funciones de red y seguridad separadas que puedan afectar al rendimiento de los usuarios de su organización?

Global Edge Network

Desafíos del mercado

A medida que las organizaciones se han ido haciendo más globales y dispersas, se han dado cuenta de que el despliegue de aplicaciones desde un lugar centralizado no es escalable. Los usuarios que necesitan acceso desde ubicaciones remotas o menos pobladas suelen tener una experiencia de usuario de mala calidad. La productividad se reduce ya que los usuarios finales deben esperar o repetir tareas innecesarias en la aplicación. Es esencial superar las limitaciones de rendimiento de los servicios públicos de Internet y de la primera línea, ya que cada vez más datos, aplicaciones y usuarios se mueven a la nube. Estas limitaciones ejercen una gran presión sobre los equipos de IT, que son responsables de proporcionar una infraestructura segura para las aplicaciones y los datos a nivel mundial. La arquitectura de red global de un proveedor determina el tiempo que tardan en transitar los datos del cliente desde y hasta los puntos de presencia (PoP) más cercanos antes de ser procesados, lo cual puede causar un potencial aumento de latencia de extremo a extremo. A la larga, la infraestructura de red subyacente afecta a la escala y la eficacia de los controles de seguridad. Las redes tradicionales e irregulares no resultan adecuadas para las organizaciones con una estrategia cloud-first.

EL TRÁFICO DE LAS EMPRESAS NO DEBERÍA CRUZARSE CON EL INTERNET PÚBLICO CON DEMASIADA FRECUENCIA. INTERNET DEBE USARSE COMO UNA PASARELA PARA LA INFRAESTRUCTURA SASE, DONDE SE INSPECCIONA BASÁNDOSE EN POLÍTICAS Y SE OPTIMIZA PARA UN MEJOR RENDIMIENTO CON LA AYUDA DE UN RUTEO DE RECORRIDO RÁPIDO Y ACUERDOS DE *PEERING*.

Gartner, The Future of Network Security Is in the Cloud, agosto de 2019, de los analistas Neil MacDonald, Lawrence Orans y Joe Skorupa

Beneficios de SASE

Un proveedor listo para SASE implementará sus servicios mediante una red periférica global en la nube que proporcione servicios de seguridad lo más cerca posible del usuario final, que optimice el ruteo y la disponibilidad, y que permita (o incluso acelere) las funciones de seguridad integradas, como DLP y ATP. De esta manera, el procesamiento se realizará rápidamente con una latencia e interrupciones mínimas para el usuario final. Si el proveedor transmite mediante sistemas *backhaul* el tráfico de los clientes a centros de datos centralizados, significa que no está siguiendo el modelo SASE y que es incapaz de ofrecer los servicios de red y seguridad necesarios para las empresas. Como consecuencia, se crearán embotellamientos que provocarán una latencia que debilitará la protección y causará frustración a los usuarios. Para poder escalar a demanda, en cualquier lugar y en cualquier momento, las arquitecturas SASE necesitan una distribución global e inteligente de PoP y centros de datos con funciones de tolerancia automática frente a fallos para poder ofrecer la mejor experiencia posible a los usuarios en cualquier parte del mundo. Los acuerdos principales de *peering* con los proveedores de servicios de Internet (ISP, por sus siglas en inglés) y los proveedores de servicios de nube (CSP) de primer nivel ayudan a optimizar las rutas entre usuarios finales y los proveedores de aplicaciones gestionadas, de modo que resulte en una experiencia de usuario en general satisfactoria.

¿Qué preguntas debe hacer?

- ¿Qué tan dependiente es su proveedor de SASE de la Internet pública para su servicio de seguridad en la nube?
- ¿Qué capacidad sobrante tiene para su servicio de seguridad en la nube?
- ¿Cómo define un PoP? ¿Son todos sus PoP consistentes y tienen una capacidad y un umbral de latencia similar?
- ¿Estos PoP están disponibles para clientes en todo el mundo o existen limitaciones?
- ¿Cuáles son los proveedores ISP de primer nivel con los que tienen acuerdos de *peering*?
- ¿Gestionan y optimizan toda la infraestructura de la nube, incluyendo la primera, media y última milla?

Una única consola, un único agente, una única nube

Desafíos del mercado

Durante mucho tiempo, los equipos de operaciones de seguridad han tenido dificultades con la gestión y el mantenimiento de múltiples productos y consolas de varios proveedores de seguridad. Esta variedad requiere un diseño, una configuración y una gestión de su infraestructura de seguridad cada vez más complejos. Además, los equipos de operaciones de seguridad tienen que enfrentarse con una maraña de consolas de seguridad centradas en el producto físico. Esto amplifica la complejidad y aumenta tanto el tiempo como el esfuerzo invertidos en desenmarañar este «caos de consolas». Y el mismo desafío se presenta también para los agentes en los endpoints. Un sinfín de agentes diferentes compiten por los recursos de los puntos terminales y ralentizan las funciones de seguridad como DLP, Endpoint Protection (EPP) y el acceso a las aplicaciones privadas. Lamentablemente, la mayoría de las grandes empresas de seguridad ofrecen un portfolio de productos basados en hardware y software que han sido implementados juntos mediante adquisiciones. Y aunque existan integraciones, los resultados serán los mismos: un conjunto desigual de productos que no mejora la situación de seguridad, sino que la complica y debilita.

Beneficios de SASE

Una solución lista para SASE debe estar completamente integrada y no integrada «con pinzas». Tenga cuidado con los productos que necesitan configuraciones y paneles de instrumentos separados para conectar múltiples productos en flujos de trabajo comunes. Una arquitectura SASE que ha sido diseñada desde el principio con una consola, un motor de políticas, y un agente para SWG, CASB y más ZTNA garantiza una gestión simplificada, una implementación de políticas consistente y un enfoque optimizado y centralizado que proporciona un acceso seguro y rápido a la nube y a la web. De esta manera, los equipos de seguridad informática solo deben aprender a utilizar una consola/interfaz gráfica de usuario (GUI, por sus siglas en inglés) que tenga un flujo de trabajo intuitivo para configurar, operar y monitorizar su postura de seguridad.Por último, la integración con herramientas de seguridad de terceros es fundamental. Una solución lista para SASE debe ofrecer APIs de transferencia de estado representacional (REST, por sus siglas en inglés) y compartir inteligencia de amenazas, basándose en estándares, para así amplificar sus capacidades.

¿Qué preguntas debe hacer?

- ¿Cuántas consolas necesita su proveedor SASE para configurar su portfolio de seguridad para aplicaciones en la web, la nube pública, la nube privada y los centros de datos? ¿Estas consolas son meros paneles de instrumentos que conectan múltiples sistemas sin ningún flujo de trabajo ni integración de aplicación de políticas?
- ¿Cuántas de sus defensas de seguridad están diseñadas para la nube (y no meramente alojadas en la nube) e integradas?
- ¿Tienen un motor de políticas único y exhaustivo?
- ¿Cómo gestionan las integraciones con herramientas de terceros? ¿Es un método complicado?

Qué puede hacer Netskope por su empresa

Netskope es el proveedor de seguridad en la nube líder del mercado. Su plataforma Security Cloud ofrece servicios de seguridad en la nube, *cloud-smart*, a clientes de todo el mundo sin comprometer el rendimiento. Netskope ayuda a sus clientes a resolver los problemas de seguridad más críticos, además de proteger sus aplicaciones y datos frente a amenazas evasivas. Con un diseño centrado en los datos, la plataforma de seguridad en la nube de Netskope ha sido creada para comprender y proteger los entornos SaaS, web y IaaS durante los accesos desde cualquier dispositivo. Gracias a la tecnología Cloud XD™, Netskope permite el control contextual de sus políticas de seguridad basadas en el tipo de usuario, dispositivo, aplicación, instancia, actividad, categoría de datos, etc. Este control sienta las bases para aplicar los controles de seguridad granulares en los entornos SaaS, web y IaaS, todos ellos gestionados desde una única consola con un motor unificado de aplicación de políticas.

Los puntos siguientes son los beneficios que su organización obtendrá de la plataforma Netskope preparada para SASE:

Centrada en los datos

- Ofrece una protección consciente del contexto y centrada en los datos que hace un seguimiento de los datos dondequiera que vayan.
- Proporciona visibilidad allí donde la tecnología de seguridad tradicional no es capaz de detectar amenazas.
- Protege los datos sensibles independientemente de donde transiten: Cloud, Web y IaaS.

Cloud-Smart

- Entiende el lenguaje de la nube, como las solicitudes de API y JSON.
- La tecnología Cloud XD™ ofrece un contexto en profundidad que permite los controles de seguridad granulares.
- Aplica controles de seguridad universales en la nube, la web y IaaS.

Rápida

- La tecnología NewEdge™ ofrece una infraestructura de red global de alta capacidad y alto rendimiento para una experiencia de usuario optimizada.
- Proporciona funciones de seguridad en tiempo real (por ejemplo, inspección SSL/TLS, DLP) y a escala sin limitar el rendimiento.
- Ofrece una experiencia de acceso a Internet sin interrupciones, segura y de alto rendimiento.

Para más información acerca de cómo puede ayudarle Netskope a prepararse para SASE, visite las siguientes páginas web o contacte con uno de los agentes de ventas locales de Netskope.

SASE: https://www.netskope.com/es/about-SASE

Plataforma de seguridad en la nube Netskope: https://www.netskope.com/platform

GUÍA PARA LA ADOPCIÓN

Para más información acerca de cómo puede ayudarle Netskope a prepararse para SASE, visite las siguientes páginas web o contacte con uno de los agentes de ventas locales de Netskope.

SASE: https://www.netskope.com/es/about-SASE

Plataforma de seguridad en la nube Netskope: https://www.netskope.com/platform

netskope

Netskope security cloud proporciona una visibilidad incomparable, así como protección de datos y amenazas en tiempo real durante el acceso a servicios en la nube, sitios web o aplicaciones privadas desde cualquier lugar y desde cualquier dispositivo. Solo Netskope es capaz de entender la nube y adoptar un enfoque centrado en los datos que permita a los responsables de seguridad obtener el equilibrio adecuado entre la protección y la velocidad que necesitan para asegurar su viaje hacia la transformación digital.

Para más información, visite https://www.netskope.com.