APRENDIZAJE SENCILLO

Puerta de enlace web segura en la nube para Dummies

Edición Palo Alto Networks

El mundo ha cambiado. El trabajo ya no es un lugar al que vamos, sino algo que hacemos. Aunque trabajar de forma remota o móvil no es nada nuevo, la pandemia mundial ha acelerado necesariamente la adopción generalizada de un modelo de trabajo desde casa y desde cualquier lugar en las empresas actuales. Tras la pandemia, muchas organizaciones han adoptado esta «nueva normalidad», y parece que este modelo de trabajo híbrido ha llegado para quedarse. Según el estudio *The State of Hybrid Workforce Security 2021* de Palo Alto Networks, más de tres cuartas partes de los empleados quieren seguir trabajando desde casa al menos parte del tiempo.

Los trabajadores no son los únicos que han «abandonado el edificio». Muchas aplicaciones empresariales básicas, alojadas tradicionalmente en centros de datos corporativos a nivel local, han sido sustituidas por aplicaciones de *software* como servicio (SaaS). El informe *2022 State of the Cloud Report* de Flexera concluyó que el 49 % de todas las cargas de trabajo empresariales se ejecuta actualmente en la nube pública, y según *30 SaaS Industry Statistics [2023]:Trends + Analysis* de Zippia.com, las organizaciones utilizan ya una media de 110 aplicaciones SaaS y el 99 % de las empresas utilizarán una o más soluciones SaaS para finales de 2023.

Como resultado de estas importantes tendencias, la mayoría de los trabajadores y las aplicaciones a las que acceden se utilizan ahora fuera del perímetro de la empresa. Hoy en día, la World Wide Web es el nuevo perímetro de la red. En esta guía, descubrirás cómo una puerta de enlace web segura (SWG) ofrece seguridad

completa en una única plataforma en la nube para proteger a todos tus usuarios y aplicaciones, estén donde estén.

Protección del tráfico de Internet con una puerta de enlace web segura

Una SWG es una solución de seguridad de red local o en la nube que filtra el *software* o *malware* no deseado del tráfico de Internet e impone el cumplimiento de las políticas corporativas y normativas. En lugar de conectarse directamente a un sitio web o aplicación, un usuario accede a SWG, que se encarga después de conectar al usuario al sitio web/aplicación deseado y de llevar a cabo funciones como el filtrado web, la visibilidad web, la inspección de contenidos maliciosos, los controles de acceso web y otras medidas de seguridad.

Cuando las SWG se definieron por primera vez como categoría en el mercado de la seguridad, la mayoría de ellas (si no todas) consistían en soluciones de proveedores *proxy*. Sin embargo, las SWG y los *proxies* no son lo mismo: un *proxy* es una función de red, mientras que una SWG es una solución de seguridad. Un *proxy* es un ordenador o *software* dedicado que se sitúa entre un cliente final (como un ordenador de sobremesa o un dispositivo móvil) y un destino deseado (como un sitio web, un servidor o una aplicación web o basada en la nube).

Al actuar como intermediarios entre el cliente y el destino, los *proxies* pueden ocultar la dirección del protocolo de Internet (IP) del cliente al destino, lo que proporciona así una capa de privacidad. Como se muestra en la figura 1, un *proxy*:

- Recibe una petición web de un cliente
- Finaliza la conexión
- Establece una nueva conexión con el destino deseado
- Envía los datos en nombre del cliente

Figura 1: Un *proxy* funciona como intermediario entre un cliente final y un recurso del destino.

Algunas de las principales limitaciones asociadas a los dispositivos *proxy* web locales tradicionales son:

- **Seguridad incompleta:** los dispositivos *proxy* web locales y otros productos heredados de varios proveedores nunca se diseñaron para la nube y no proporcionan una seguridad completa y coherente a todos los usuarios, ubicaciones y dispositivos. La incapacidad de los dispositivos *proxy* web locales para proteger todas las

aplicaciones (web y no web), la falta de inspección del tráfico en línea y la escasa integración con los ecosistemas en la nube aumentan el riesgo organizativo.

- **Cobertura limitada de la aplicación:** más de la mitad de las amenazas a las que se exponen los trabajadores remotos corresponden a aplicaciones no web, que son invisibles para los *proxies* web. Los equipos de seguridad no pueden bloquear lo que no pueden ver, por lo que el riesgo de que se produzca una filtración de datos aumenta si no hay seguridad tanto para las aplicaciones web como para las que no lo son.
- **Mala experiencia del usuario final:** los cuellos de botella en el rendimiento se producen cuando las organizaciones reenvían el tráfico de Internet de los trabajadores remotos a dispositivos *proxy* web en centros de datos para garantizar el acceso y la seguridad. Además, los trabajadores remotos utilizan con frecuencia una red privada virtual (VPN), no una SWG, para obtener acceso a aplicaciones privadas, lo que puede causar confusión y problemas de conectividad, dando lugar a más llamadas al servicio de asistencia de TI.
- **Limitaciones de los dispositivos de varios proveedores:** el uso de dispositivos de varios proveedores da lugar a una falta de gestión centralizada, políticas de seguridad incoherentes, un rendimiento lento y una visibilidad deficiente de las amenazas a la red en toda la organización. Los dispositivos en silos de varios proveedores dan lugar a políticas incoherentes, aumentan los costes de mantenimiento y limitan la visibilidad y la colaboración entre los equipos de redes y seguridad.

RECUERDA

El acceso a las aplicaciones de las oficinas centrales se hace a través de una VPN de acceso remoto. Cuando los usuarios acceden a las aplicaciones en la nube, se desconectan de la VPN y quedan expuestos a riesgos. Esta es una de las razones por las que las organizaciones utilizan las SWG: para proporcionar un acceso seguro a Internet cuando los usuarios están desconectados de la VPN.

Muchas organizaciones confían en SWG en la nube para asegurar el acceso a Internet de los usuarios remotos y desde la oficina, así como el acceso a servidores, infraestructura de escritorio virtual (VDI) y dispositivos del Internet de las Cosas (IoT) en sucursales, e incluso en oficinas centrales/

campus universidades con requisitos de ancho de banda elevados en los que es necesario hacer descargas de la instalación local a la nube. Además, una SWG en la nube proporciona visibilidad al acceso de los usuarios, las amenazas basadas en Internet y al tráfico web, además de controles de Internet y aplicación de la normativa con controles de acceso, control de funciones, controles de SaaS y protección de datos, así como capacidades de navegación segura por Internet. Por último, una SWG en la nube puede utilizarse para mejorar la experiencia del usuario final. En lugar de redirigir todo el tráfico web a un centro de datos corporativo, lo que introduce latencia, el rendimiento de la red puede mejorarse drásticamente conectándose directamente a la nube.

CUESTIÓN TÉCNICA

Las SWG tampoco sustituyen a los cortafuegos. Los cortafuegos de primera generación solo inspeccionaban direcciones IP, puertos u otros protocolos basados en enrutadores (capas 2 y 3). Los *proxies* web locales funcionan en la capa 7, y los cortafuegos de nueva generación operan tanto en la capa de la red como en la de la aplicación (capas 3 y 7, respectivamente). Una SWG en la nube traslada estas capacidades a la nube y admite arquitecturas basadas en *proxy*.

Comienza tu viaje SASE con una puerta de enlace web segura

Uno de los retos de la implementación de las funciones de SWG es que normalmente se configuran como un entorno independiente sin coordinar los flujos de trabajo, los informes o el registro con otras infraestructuras de seguridad de la organización. Esto puede aumentar la complejidad con el paso del tiempo, ya que las organizaciones a menudo tienen varios productos de seguridad puntuales, lo que disminuye la eficiencia y eficacia de sus operaciones de seguridad.

Más recientemente, ha surgido un nuevo enfoque ante la infraestructura de seguridad. Según la definición de Gartner, un servicio perimetral de acceso seguro (SASE) combina servicios de red y seguridad en una solución unificada y suministrada desde la nube que incluye lo siguiente, tal y como se resume en la figura 2:

- **Red**
  - Red de área extensa definida por *software* (SD-WAN):
  - VPN
  - Calidad del servicio (QoS)
  - Enrutamiento
  - Aceleración SaaS
- **Seguridad**
  - SWG en la nube

- Agente de seguridad para el acceso a la nube (CASB)
- Cortafuegos como servicio (FWaaS)
- Prevención de pérdida de datos (DLP)
- Seguridad del sistema de nombre de dominio (DNS)
- Prevención de amenazas

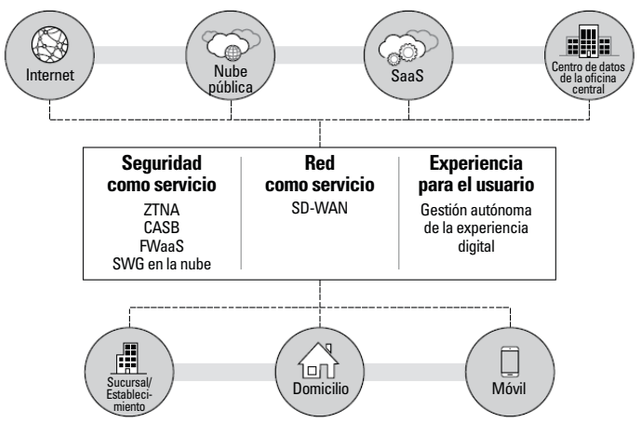

Figura 2: SASE ofrece capacidades avanzadas de red y seguridad en una solución convergente en la nube.

Esto permite a las empresas ofrecer varios tipos de servicios de seguridad desde la nube, como SWG, prevención avanzada de amenazas, FWaaS, seguridad DNS, CASB, DLP y otros.

Una SWG es tan solo uno de los muchos servicios de seguridad que debe proporcionar una solución SASE. A medida que las organizaciones crecen y añaden un número cada vez mayor de usuarios remotos, la cobertura y la protección se hacen más difíciles. Estos retos se ven agravados por el rápido crecimiento y la adopción generalizada de aplicaciones SaaS, la proliferación de dispositivos personales gestionados y no gestionados que acceden a las aplicaciones empresariales, y la naturaleza descentralizada de las distintas aplicaciones empresariales que se ejecutan en el centro de datos corporativo y en la nube pública. Una solución SASE traslada la SWG a la nube, ofreciendo protección en la nube a través de una plataforma unificada que permite obtener una visibilidad y control completos de toda la red.

RECUERDA

Una solución SASE debe incluir SWG para que las organizaciones puedan controlar el acceso web y aplicar políticas de seguridad que protejan a los usuarios de sitios web maliciosos, *malware*, ataques de *phishing*, ataques a plataformas SaaS, ataques de intermediarios, etc.

SASE ofrece muchas ventajas a las organizaciones, entre ellas:

- **Protección de tus trabajadores remotos:** protege a tus usuarios, aplicaciones y datos con una inspección de seguridad en línea basada en inteligencia artificial (IA) / aprendizaje automático (ML) para todo el tráfico web y no web.

- **Agilización de la gestión y operaciones de la red:** centraliza la gestión y la aplicación de las políticas de seguridad, y unifica múltiples productos y proveedores puntuales con una única plataforma.
- **Mejora de la experiencia de los usuarios:** proporciona un acceso constante a los usuarios y mejora su experiencia con una visibilidad completa y un control preciso de la conexión de extremo a extremo.

CONSEJO

Consulta los siguientes recursos de Palo Alto Networks que te ayudarán a proteger el tráfico de Internet con una SWG en la nube:

- **Libro electrónico:** *SASE para Dummies, 2.ª edición especial*
- **Página web:** Puerta de enlace web segura
- **Libro blanco:** *Moderniza tu puerta de enlace web segura con SASE*

paloalto NETWORKS

9781394227273