Enterprise Strategy Group | Getting to the bigger truth.™

INFORME TÉCNICO DE ESG

# Modernice su puerta de enlace web segura con SASE

Autor: John Grady, analista sénior de ESG

Enero de 2022

Informe técnico de ESG encargado por Palo Alto Networks y distribuido con la licencia de ESG.

## Contenido

## Resumen ejecutivo

Las empresas actuales necesitan garantizar la protección de sus usuarios en todo momento, así como el acceso seguro a los recursos que les hacen falta para desempeñar su labor, trabajen donde trabajen. Los modelos de seguridad tradicionales dependen de dispositivos locales aislados, lo que se traduce en ineficiencias operativas, unas experiencias del usuario que dejan bastante que desear y una seguridad incoherente. Buen ejemplo de ello son las puertas de enlace web seguras (SWG, por sus siglas en inglés). No cabe duda de que son un componente importante de la estrategia de seguridad de las organizaciones, pero insuficientes para satisfacer las exigencias modernas por sí solas.

El principal objetivo de las arquitecturas de servidor perimetral de acceso seguro (SASE, por sus siglas en inglés) es proporcionar una herramienta que permita, además de aplicar las políticas de manera distribuida y coherente, unificar la gestión de unas tecnologías de seguridad que hasta ahora funcionaban por separado. El problema de este tipo de arquitecturas es que requieren rediseñar la infraestructura de red y seguridad. Como primer paso, muchas organizaciones están priorizando la seguridad de las soluciones SASE y están concentrando sus esfuerzos en converger las herramientas de puerta de enlace web segura, acceso Zero Trust (confianza cero) a la red y agente de seguridad de acceso a la nube. Cloud SWG, que forma parte de la plataforma Prisma Access de Palo Alto Networks, protege todo el tráfico de las aplicaciones (incluido el de las aplicaciones web) y, ahora, permite a las organizaciones utilizar soluciones antiguas basadas en *proxy* para migrar fácilmente a una arquitectura SASE en la nube moderna y convergente.

## La brecha de la seguridad de la red se agranda

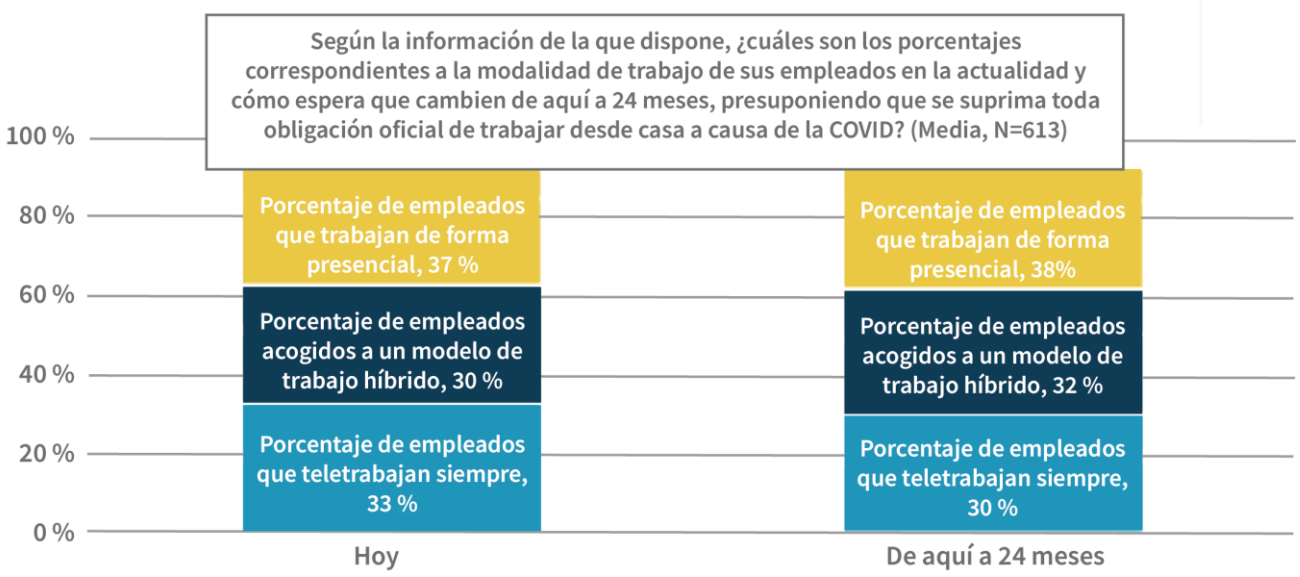
Hoy en día, la empresa está en pleno proceso de transformación digital y muchas organizaciones están condensado años de cambios en tan solo unos meses. Las iniciativas de migración a la nube se han acelerado con el fin de aumentar la resiliencia empresarial y mejorar la agilidad de las organizaciones. En concreto, un estudio de ESG reveló que el 95 % de las organizaciones utilizan actualmente aplicaciones de software como servicio o de infraestructura como servicio (SaaS e IaaS, respectivamente, por sus siglas en inglés).[1]

A su vez, los trabajadores han empezado a regresar a las oficinas, y muchos lo están haciendo según un modelo híbrido que los encuestados del estudio de ESG esperan que dure por lo menos otros 24 meses (véase la figura 1).[2]Para hacer posibles estos cambios, muchas empresas han priorizado las actualizaciones de la infraestructura de la red mediante, por ejemplo, la adopción de tecnologías SD-WAN. Sin embargo, actualizar las estrategias de seguridad para responder mejor a estas cambiantes dinámicas sigue siendo un trabajo pendiente para muchas organizaciones.

[1]Fuente: Informe de investigación de ESG, *2022 Technology Spending Intentions Survey* (disponible en inglés), noviembre de 2021.

[2]Fuente: Resultados de la encuesta completa de ESG, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased* (disponible en inglés), diciembre de 2021.

**Figura 1. Porcentaje de empleados que trabajan en modalidad de teletrabajo, trabajo híbrido y trabajo presencial**




*Fuente: Enterprise Strategy Group*

## Las estrategias de seguridad web y acceso seguro tradicionales no se ajustan a las dinámicas actuales y generan más problemas

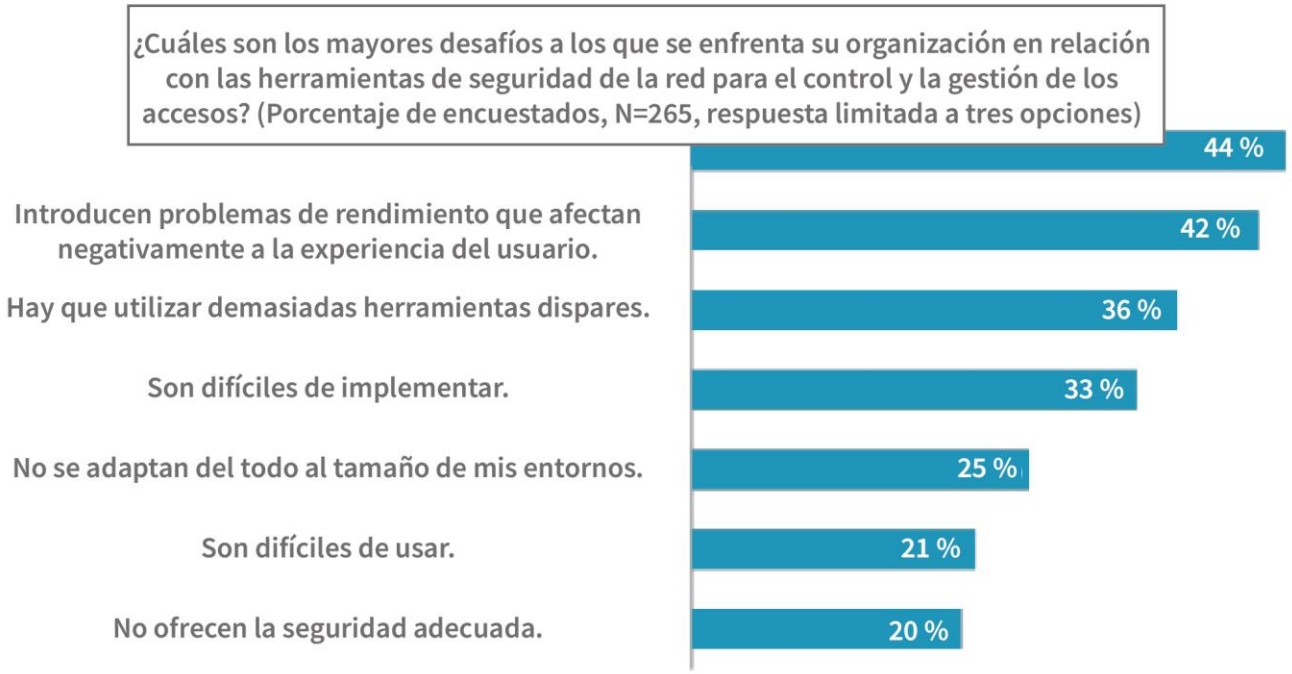
Las estrategias de seguridad de la red tradicionales están pensadas para aplicarse a perímetros estáticos bien definidos en los que el tráfico se deriva desde las sucursales y los usuarios remotos hasta las soluciones de seguridad local centralizada que lo inspecciona. Con el progresivo abandono de las ubicaciones corporativas físicas por parte de los usuarios y los recursos empresariales, muchas organizaciones han empezado a recurrir a soluciones en la nube para responder a las nuevas situaciones que se les planteaban y proteger determinados vectores de amenazas. Sin embargo, este modelo se ha revelado ineficiente y el uso de herramientas independientes que funcionan de manera aislada ha sido una fuente de problemas para las empresas (véase la figura 2).[3] En concreto:

- Ineficiencia operativa. A nadie se le escapa la escasez de competencias y personal de ciberseguridad. Como resultado, los equipos de seguridad y de red tienen cada vez más trabajo y no dan abasto. Aun así, se les pide que implementen y gestionen constantemente toda suerte de herramientas independientes, cada una con su propia consola y, a menudo, un buen número de políticas duplicadas. Esta manera de trabajar no solo es ineficiente, sino que además es caldo de cultivo para el error humano y aumenta el riesgo de la organización.
- Experiencia del usuario deficiente. El modelo radial según el cual el tráfico se desvía a una ubicación central en la que se analiza de manera secuencial con distintas herramientas de seguridad puede introducir latencia y afectar al rendimiento de las aplicaciones que utilizan los usuarios. Además, los modelos tradicionales de red privada virtual (VPN, por sus siglas en inglés), que obligan a los empleados a conectarse a determinadas puertas de enlace para acceder a ciertos recursos, resultan muy incómodos y los usuarios terminan por desactivar o eludir las herramientas de seguridad cada vez que pueden.

[3] Fuente: Informe de investigación de ESG, *The State of Network Security: A Market Poised for Transition* (disponible en inglés), marzo de 2020.

- Seguridad incoherente. La velocidad con la que aparecen nuevas aplicaciones en los entornos, sean aplicaciones IaaS introducidas por desarrolladores internos o aplicaciones SaaS desconocidas a las que acceden los usuarios, es impresionante. Por lo general, no hay una fuente de información fidedigna única que proporcione visibilidad clara de lo que se está ejecutando en la red y ayude a los administradores a identificar las aplicaciones con precisión, aplicar las políticas correctas y priorizar las alertas conforme surgen.

**Figura 2. Principales desafíos de las herramientas de seguridad de la red**




*Fuente: Enterprise Strategy Group*

Buen ejemplo de estas tendencias son las puertas de enlace web seguras (SWG) y los *proxy* web. Al principio, las organizaciones adoptaban *proxies* web físicos para proteger a los usuarios que accedían a recursos basados en Internet. Con todo, y pese a que se ha incrementado el uso de SWG en la nube para reducir la necesidad de desviar el tráfico en algunos casos, la mayoría de las organizaciones continúan simultaneándolas con SWG locales. De hecho, mientras que el 96 % de los encuestados del estudio de ESG reconocían utilizar puertas de enlace web seguras o soluciones de *proxy* web físicas, el 93 % afirma que su organización utiliza una puerta de enlace web segura en la nube.[4] Este nivel de solapamiento ilustra lo poco sistemáticas que han sido muchas organizaciones a la hora de migrar sus mecanismos de control de la seguridad a la nube.

La cambiante composición del tráfico empresarial añade una consideración más con respecto a la tecnología SWG. En lugar de hacer un uso genérico de la web, los usuarios ahora dedican gran parte del tiempo a acceder a aplicaciones en la nube. Aunque los *proxies* web pueden proporcionar accesos con controles generales para las aplicaciones HTTP, la falta de visibilidad de los puertos y protocolos hace que pasen por alto las aplicaciones no basadas en la web. Como resultado, el uso de agentes de seguridad de acceso a la nube y herramientas de acceso Zero Trust a la red (CASB y ZTNA, respectivamente, por sus siglas en inglés) se ha visto incrementado para facilitar el acceso seguro a aplicaciones SaaS públicas, de centros de datos privados o IaaS. Aun así, el solapamiento que se produce entre estas herramientas suele derivar en la duplicación de la gestión de las políticas y las configuraciones, con las consecuencias que mencionábamos antes. Como resultado, muchas organizaciones están abiertas a probar una nueva forma de proteger la puerta de enlace

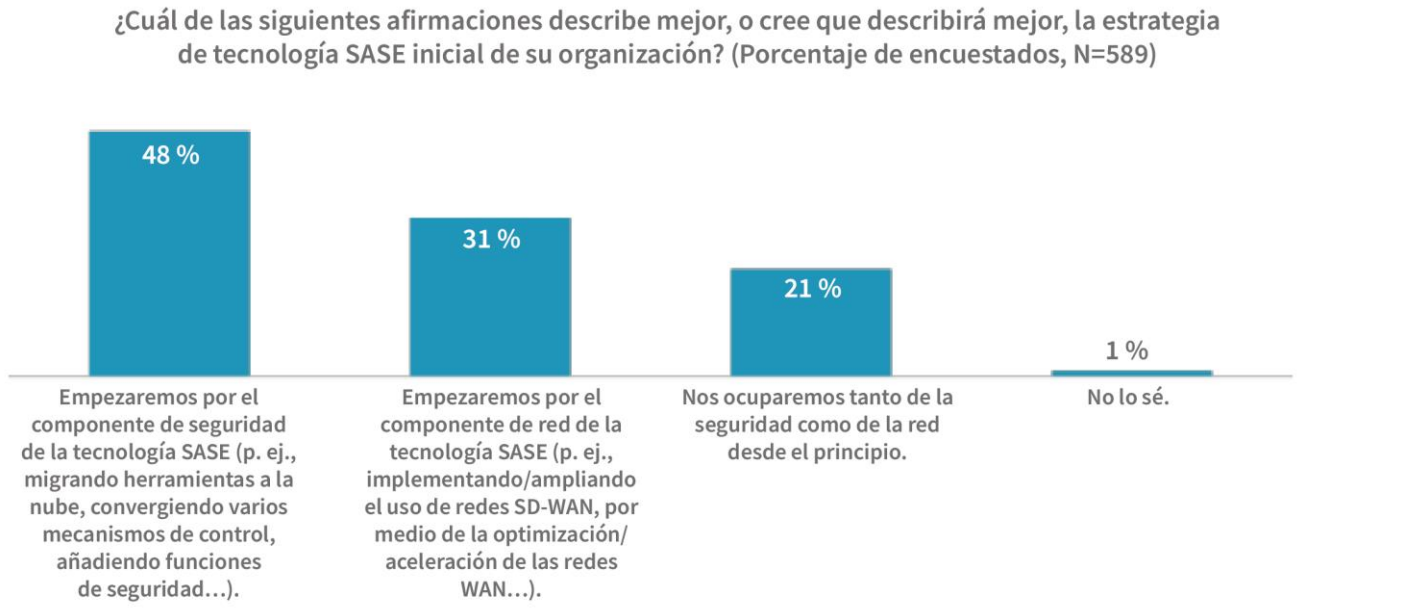
[4] Fuente: Resultados del estudio de ESG, *Network Security Trends* (disponible en inglés), marzo de 2020.

web, mientras que solo un 8 % de los encuestados por ESG indicaban estar muy satisfechos con su solución actual y no se planteaban cambiarla a corto plazo.[5]

## Tecnología SASE: un trampolín a la modernización de la puerta de enlace web segura

El concepto de servidor perimetral de acceso seguro (SASE) ha suscitado gran interés como manera de responder a muchos de los problemas mencionados a lo largo de este documento. La tecnología SASE converge herramientas de red y mecanismos de control de la seguridad que antes estaban aislados en una arquitectura en la nube completa que, por un lado, permite aplicar las políticas de manera coherente y distribuida a los usuarios que acceden desde el perímetro, y por el otro lado ofrece una gestión unificada a los administradores. Aunque esto representa una evolución necesaria que, además, es aplicable a organizaciones de todos los tipos y tamaños, lo cierto es que la gran variedad de iniciativas SASE exige una metodología por fases. Según las investigaciones de ESG, la mayoría de las organizaciones coinciden en este punto y casi la mitad de los encuestados (el 48 %) afirma que la primera prioridad de su organización serán los aspectos de seguridad del modelo SASE (véase la figura 3).[6]

**Figura 3. Aproximaciones iniciales al modelo SASE**




*Fuente: Enterprise Strategy Group*

Converger el acceso seguro a la web, las aplicaciones públicas y las aplicaciones privadas es un punto de partida lógico hacia el modelo SASE

**Para los usuarios, el proceso de acceder a un sitio web, una aplicación SaaS o una aplicación privada suele ser siempre el mismo: abrir un navegador y buscar el**

[5]Fuente: Resultados de la encuesta de ESG, *Transitioning Network Security Controls to the Cloud* (disponible en inglés), julio de 2020.

[6]Fuente: Resultados de la encuesta completa de ESG, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased* (disponible en inglés), diciembre de 2021.

**recurso. Esta experiencia debería ser siempre igual, sin que el usuario tenga que pararse a pensar a qué está accediendo ni desde dónde.**

Las arquitecturas de seguridad creadas a lo largo de muchos años no pueden actualizarse por completo de la noche a la mañana. Por eso, aunque establecer la seguridad como prioridad es un buen primer paso, hay que seguir profundizando, pues hay muchas opciones que considerar en relación con la seguridad de la tecnología SASE. Aumentar la coherencia con la que los usuarios están protegidos, independientemente de dónde estén o a qué accedan, debería ser la prioridad número uno para casi cualquier organización. Dadas las circunstancias, no es de extrañar que el 69 % de los encuestados por ESG indicaran que, a la hora de implementar su solución SASE, la puerta de enlace web segura (SWG) será el punto de partida o una consideración secundaria.[7]

Para los usuarios, el proceso de acceder a un sitio web, una aplicación SaaS o una aplicación privada suele ser siempre el mismo: abrir un navegador y buscar el recurso. Esta experiencia debería ser siempre igual, sin que el usuario tenga que pararse a pensar a qué está accediendo ni desde dónde. Tener que conectarse a puertas de enlace VPN específicas para acceder a ciertos recursos supone un inconveniente para los empleados, es complicado en dispositivos no gestionados y puede degradar la seguridad cuando los usuarios deciden eludir la VPN. Así pues, converger las tecnologías de puerta de enlace web segura, CASB y ZTNA tiene todo el sentido para muchas organizaciones. De hecho, ESG descubrió que estas herramientas solían citarse entre las más difíciles de aprovisionar con un solo proveedor en el contexto de un modelo SASE (véase la figura 4).[8]

[7] *Ibid.*
[8] Ibid.

**Figura 4. Principales 10 herramientas SASE que comprar a un solo proveedor**


*Fuente: Enterprise Strategy Group*

## Aspectos clave que deben tenerse en cuenta a la hora de elegir una SWG como parte de una arquitectura SASE

A la hora de barajar con qué proveedores trabajar para implementar una iniciativa SASE basada inicialmente en las tecnologías SWG, CASB y ZTNA, las organizaciones deberían hacerse las siguientes preguntas clave:

- ¿Qué proceso de migración tengo que seguir para pasar a los usuarios de mi SWG actual a la nueva solución? La necesidad de implementar agentes adicionales o de cambiar el enrutamiento en función de las políticas genera una sobrecarga de trabajo y puede ralentizar la transición. Esta posible complejidad es lo que ha hecho que algunas organizaciones se hayan resistido durante tanto tiempo a modernizar sus SWG. Utilizar los agentes que ya tienen o los archivos de configuración automática del *proxy* (PAC, por sus siglas en inglés) ya implementados puede facilitar y agilizar la transición en gran medida.

- ¿Tiene el proveedor otras funciones SASE que puedan servir a otros casos de uso en el futuro? Lo normal es que, al principio, las iniciativas SASE se centren en un caso de uso particular, como proteger a los teletrabajadores. Sin embargo, pasado un tiempo, la mayoría de las organizaciones querrán ampliar su solución SASE. En relación con la consolidación inicial de las tecnologías SWG, CASB y ZTNA, los usuarios deben asegurarse de que los proveedores que están estudiando les vayan a servir para un amplio abanico de casos de acceso en los dispositivos gestionados, no gestionados y móviles utilizados tanto por los empleados como por terceros. En general, los proveedores capaces de proporcionar una arquitectura SASE que, a su vez, permita proteger los dispositivos IdC e incorporar funciones de red y SD-WAN ofrecerán una flexibilidad a largo plazo que podrá ampliar la iniciativa con el tiempo.

- ¿Están unificadas la gestión de políticas y la visibilidad en las distintas funciones SASE? No basta con tener un amplio catálogo de funciones SASE. La gestión unificada es un componente clave de la arquitectura para eliminar las ineficiencias operativas comentadas anteriormente. Es fundamental que la gestión esté basada en una interfaz gráfica de usuario (GUI, por sus siglas en inglés) que optimice la creación de políticas en componentes de SASE solapados y reduzca el error humano. Además, la visibilidad centralizada de todos los usuarios y ubicaciones en un solo panel puede ayudar a los equipos de seguridad a identificar los problemas y priorizar las medidas de respuesta de manera más eficiente.

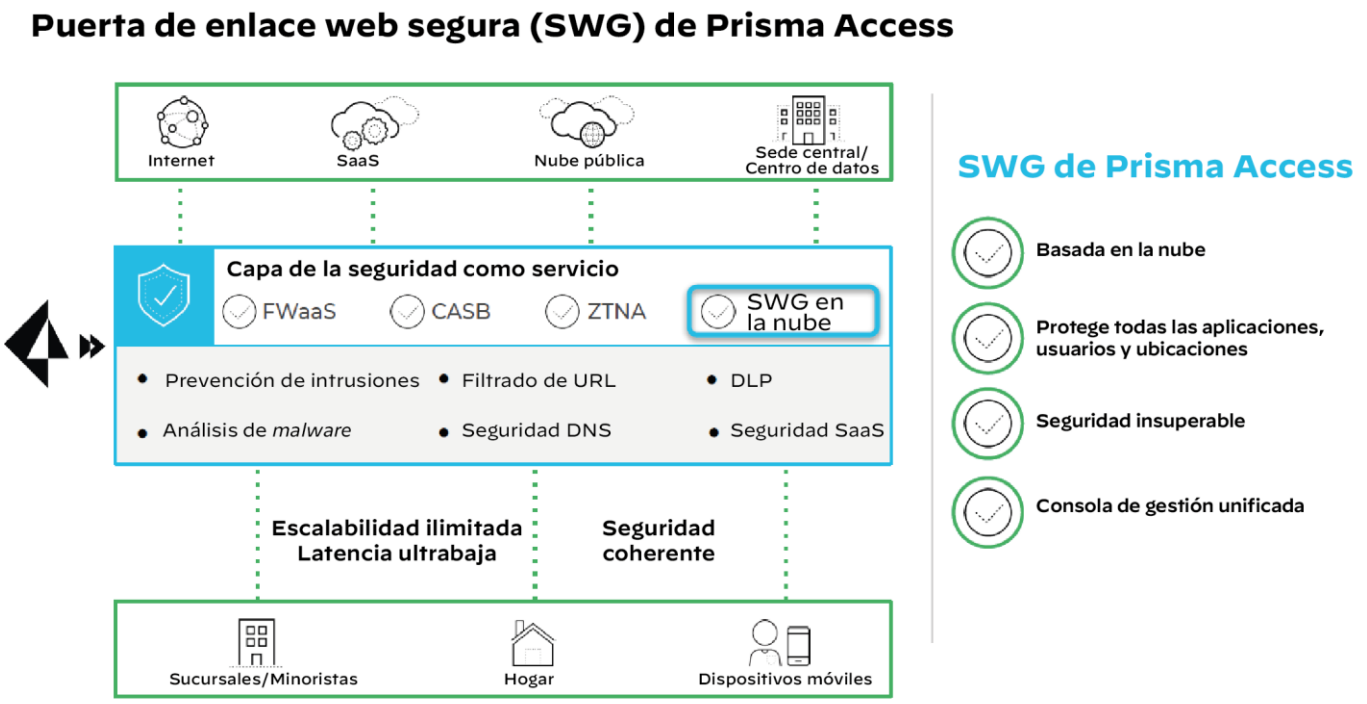
- ¿Qué capacidad de red e infraestructura de conexión tiene el proveedor? Las soluciones SASE deben ser escalables y muy fiables. Esto requiere una red resiliente global. Contar con una red distribuida con puntos de presencia en las principales geografías y relaciones directas significativas es fundamental para garantizar un rendimiento robusto y una experiencia del usuario positiva. Algunos proveedores cooperan con proveedores de servicios en la nube con el fin de utilizar sus redes troncales privadas para las conexiones privadas e impedir que el tráfico termine en la red Internet pública, disminuyendo al mismo tiempo la posibilidad de que la congestión de la web afecte al rendimiento.

## Palo Alto Networks proporciona una puerta de enlace web segura flexible a través de Prisma Access

Aunque Palo Alto Networks es más conocido por sus productos de cortafuegos de nueva generación, las empresas llevan años utilizando los mecanismos de control y la visibilidad de capa 7 que ofrece Palo Alto en estas herramientas de seguridad web cuando no se necesitaban ni deseaban arquitecturas *proxy*. Ahora que las estrategias de nube híbrida y los modelos de teletrabajo flexibles están tan extendidos, las organizaciones están recurriendo cada vez más a las soluciones en la nube para proteger todas sus aplicaciones en todos los puertos, protocolos y usuarios. Si bien Prisma Access ha ayudado a las organizaciones a proteger el tráfico de las aplicaciones, incluido el de las aplicaciones web, desde sus inicios, la migración desde las herramientas de SWG basadas en *proxy* tradicionales exigía grandes cambios en la arquitectura de red. Para facilitar la transición, Palo Alto ha añadido un *proxy* explícito a su SWG en la nube de Prisma Access que permite a los clientes migrar fácilmente desde sus soluciones tradicionales basadas en *proxy* a toda una plataforma de seguridad en la nube sin obligarlos a cambiar la arquitectura de red.

Prisma Access de Palo Alto Networks ofrece Cloud SWG (véase la figura 5). Proporciona opciones de conectividad flexibles para distintas situaciones de uso. Los dispositivos móviles gestionados pueden seguir conectándose a Prisma Access a través del agente GlobalProtect, mientras que los no gestionados pueden utilizar la opción VPN sin cliente de Palo Alto. De manera similar, las sucursales pueden conectarse a Prisma Access a través de VPN IPsec. Por último, gracias a la implementación de *proxy* explícito, los clientes pueden migrar con mayor facilidad desde sus herramientas tradicionales de *proxy* web sin necesidad de cambiar la arquitectura. Los archivos de configuración automática del *proxy* (PAC) pueden actualizarse para dirigir el tráfico web al *proxy* explícito en la nube de Prisma Access y que las organizaciones puedan empezar a migrar a una arquitectura SASE moderna.

**Figura 5. Puerta de enlace web segura de Prisma Access**




*Fuente: Palo Alto Networks*

La inclusión de Cloud SWG en la plataforma Prisma Access ofrece a los usuarios distintas ventajas, siendo estas las más importantes:

1. Una hoja de ruta clara para adoptar una solución SASE moderna y completa. Prisma Access es una plataforma de seguridad nativa en la nube totalmente integrada, lo que significa que Cloud SWG funciona perfectamente con las funciones de cortafuegos como servicio (FWaaS, por sus siglas en inglés), CASB y ZTNA de Palo Alto para ayudar a los clientes a dar el primer paso en su transición a la tecnología SASE. Además, las organizaciones disponen de una herramienta de gestión autónoma de la experiencia digital (ADEM, por sus siglas inglés) para asegurarse de que la experiencia del usuario sea la misma en las sucursales y las ubicaciones remotas, y que les resulte más fácil diagnosticar los problemas que les surjan. Gracias a las integraciones nativas con Prisma SD-WAN, es posible converger las arquitecturas de red y seguridad. Además, Prisma Access ofrece dos posibilidades para unificar la gestión: o bien a través de una consola en la nube unificada para Prisma Access que permite optimizar la gestión de la configuración y la incorporación, o bien a través de la gestión de la seguridad de la red de Panorama para facilitar la implementación y gestión de Prisma Access a los clientes actuales de los cortafuegos de nueva generación.

2. Una seguridad sólida de varias capas. Prisma Access proporciona visibilidad completa de todos los puertos y protocolos. Mientras que los *proxies* web solo ven el tráfico web, la inclusión de CASB y ZTNA ofrece una visibilidad detallada de las aplicaciones, y los cortafuegos FWaaS protegen a los usuarios de las amenazas que no están basadas en la web. La prevención de amenazas por capas incluye prevención de intrusiones, filtrado de URL y seguridad DNS. Además, Palo Alto combina su motor de análisis de *malware* WildFire con la prevención de amenazas sin firmas con aprendizaje automático para garantizar que las amenazas de día cero y otras amenazas avanzadas se bloqueen en tiempo real. A continuación, esta inteligencia sobre amenazas se distribuye de

inmediato a todos los clientes de Palo Alto, quienes, según la empresa, tienen acceso a más de 4,3 millones de actualizaciones de seguridad únicas al día. Por último, las integraciones con Enterprise DLP proporcionan una visibilidad coherente del contenido al que acceden y que comparten los usuarios, lo que permite a las organizaciones recuperar el control sobre los datos confidenciales.

3. Rendimiento a nivel de proveedor de servicios en la nube. Prisma Access utiliza Google Cloud Platform (GCP) y su red troncal privada para establecer las conexiones privadas entre las ubicaciones de Prisma Access. La plataforma se basa en más de 100 puntos de presencia distribuidos por 77 países. Como resultado, Palo Alto Networks ofrece una disponibilidad de cinco nueves (un 99,999 %), garantiza una latencia de procesamiento inferior a los 10 ms y ofrece un acuerdo de nivel de servicio (SLA, por sus siglas en inglés) para la latencia de las aplicaciones SaaS. La plataforma utiliza un plano de gestión de varios inquilinos que se combina con un plano de datos de un único inquilino y una arquitectura de análisis en un solo paso para garantizar el rendimiento y la seguridad.

4. Una seguridad más eficiente y coherente gracias a la consolidación. La estrategia consolidada de Prisma Access permite a las organizaciones disfrutar de una seguridad más coherente, una eficiencia operativa mejor y unas experiencias del usuario de mayor calidad. La protección coherente frente a las amenazas, sean web o no, unida a que la gestión se centraliza a través de un solo panel ayuda a reducir el riesgo de que se produzcan incidentes de seguridad. El personal de TI es más eficiente gracias a que tarda menos en detectar los incidentes y darles respuesta, y disminuyen los costes asociados con la gestión y el mantenimiento de distintos productos independientes, así como con el tiempo necesario para familiarizarse con ellos. Por último, un motor de análisis en un paso distribuido que acerca los mecanismos de protección a los usuarios y recursos ofrece una experiencia del usuario positiva que elimina la necesidad de desviar el tráfico al centro de datos para inspeccionarlo con herramientas de distintos proveedores.

## Conclusión

El adagio que señala la futilidad de hacer lo mismo una y otra vez y esperar resultados distintos cobra especial relevancia en el mundo de la ciberseguridad. Puede que, de un modo u otro, las estrategias hayan evolucionado a lo largo de los años, pero los cimientos siguen siendo esencialmente los mismos. Aun antes de que se produjeran los enormes cambios que están experimentando la mayoría de las organizaciones en relación con las aplicaciones y los usuarios, estas estrategias eran insuficientes para protegerlas, potenciar su crecimiento y dar autonomía a los usuarios. Visto lo visto, y con una aceleración digital cada vez más acusada, ¿por qué iban a funcionar hoy estas estrategias de seguridad? En resumen, no lo hacen.

La tecnología SASE es una iniciativa crucial que deberían adoptar todas las organizaciones para pasar de una seguridad perimetral a un modelo de aplicación de políticas distribuida en la nube que garantice una seguridad más coherente, una eficiencia operativa superior y mejores experiencias del usuario. A menudo, el punto de partida lógico de este proyecto consistirá en converger el acceso seguro a la web, las aplicaciones públicas y las aplicaciones privadas, lo que requiere una estrategia moderna que proteja las puertas de enlace seguras con funciones de CASB y ZTNA. Prisma Access no solo lo hace posible, ayudando a las organizaciones a migrar desde los *proxies* web tradicionales, sino que también ofrece las bases de una implementación SASE completa que incluye tecnologías FWaaS, CASB, ZTNA, ADEM y SD-WAN.

**Enterprise Strategy Group** es una empresa especializada en estrategias, validación, investigación y análisis de TI que ofrece inteligencia de mercado y otra información útil a la comunidad global de TI.



www.esg-global.com

contact@esg-global.com

+1 508 482 0188