Cloud SWG: el primer paso hacia la transición a la tecnología SASE

Contenido

Es el turno de las plantillas híbridas y las aplicaciones en la nube

En los últimos años, el número de empleados que se han reubicado desde las sedes centrales corporativas a oficinas remotas y en casa no ha hecho más que crecer, lo que abre un horizonte de nuevos desafíos para los equipos de redes y seguridad de todo el mundo. Las organizaciones ya tienen más que asumida la nueva normalidad y parece que el modelo de trabajo híbrido ha llegado para quedarse. Tanto es así que el 76 % de los empleados quieren seguir trabajando desde casa, al menos parcialmente.[1]

Sin embargo, los trabajadores no son lo único remoto en todo este asunto. El rápido crecimiento del software como servicio (SaaS, por sus siglas en inglés) ha contribuido a que el porcentaje de aplicaciones basadas en la nube sea bastante alto. Como resultado, la mayoría de los trabajadores y las aplicaciones a las que tienen acceso ahora residen fuera del centro de datos tradicional e Internet ha pasado a ser el nuevo perímetro de la red.

Los dispositivos proxy web no dan abasto

Este nuevo paradigma puede resultar especialmente problemático para aquellas organizaciones que utilizan dispositivos de seguridad locales de distintos proveedores que no están pensados para un mundo tan centrado en la nube como el actual, en el que los usuarios son híbridos y trabajan desde muy diversas ubicaciones. Según una encuesta de la consultora informática Enterprise Strategy Group (ESG Global), a la pregunta «¿Cuáles son los mayores desafíos a los que se enfrenta su organización en relación con las herramientas de seguridad de la red para el control y la gestión de los accesos?» la mayoría de los encuestados respondieron lo siguiente:[2]

- Hacen que la gestión de los entornos físicos y en la nube/virtuales sea incoherente.
- Introducen problemas de rendimiento que afectan negativamente a la experiencia del usuario.
- Hay que utilizar demasiadas.
- Son difíciles de implementar.

Además, según otro estudio de ESG Global, muchas organizaciones están abiertas a probar una nueva forma de proteger la puerta de enlace web, mientras que solo un 8 % de los encuestados indicaban estar muy satisfechos con su solución actual y no se planteaban cambiarla a corto plazo.[3]

Estas son algunas de las limitaciones clave asociadas a los dispositivos proxy web locales tradicionales:

- **Seguridad incompleta:** los dispositivos proxy web locales y otros productos obsoletos de varios proveedores nunca estuvieron pensados para la nube y no ofrecen el debido nivel de seguridad y coherencia para todos los usuarios, ubicaciones y dispositivos.
- **Cobertura limitada de las aplicaciones:** más de la mitad de las amenazas a las que se enfrentan los trabajadores remotos tienen como objetivo aplicaciones que no son web y que son invisibles para los proxies web. Los equipos de seguridad no pueden bloquear lo que no ven, por lo que la falta de protección aumenta el riesgo de sufrir una brecha de datos para las aplicaciones, tanto si son web como si no.
- **Experiencia del usuario final deficiente:** cuando, por motivos de acceso y seguridad, las organizaciones desvían el tráfico de Internet de los trabajadores remotos a dispositivos proxy web basados en centros de datos (figura 1), se producen cuellos de botella de rendimiento. Además, para obtener acceso a las aplicaciones privadas, los trabajadores remotos suelen utilizar redes privadas virtuales (VPN, por sus siglas en inglés) en lugar de puertas de enlace web seguras (SWG, por sus siglas en inglés). Esto puede ser una fuente de confusión y problemas de conectividad que acabe aumentando el volumen de llamadas al equipo de asistencia técnica.
- **Limitaciones del uso de dispositivos de varios proveedores:** el uso de dispositivos de distintos proveedores no solo ralentiza el rendimiento, sino que además impide centralizar la gestión, aplicar políticas de seguridad coherentes y tener visibilidad de las amenazas en la red que afectan a toda la organización (figura 2).

1. *Estado de la seguridad de las plantillas híbridas (2021)*, Palo Alto Networks, 15 de agosto de 2021, https://start.paloaltonetworks.es/state-of-hybrid-workforce-security-2021.
2. *Modernize Your Secure Web Gateway with SASE* (disponible en inglés), Enterprise Strategy Group, enero de 2022, https://www.paloaltonetworks.com/resources/whitepapers/modernize-your-secure-web-gateway-with-sase.
3. *Ibid*.

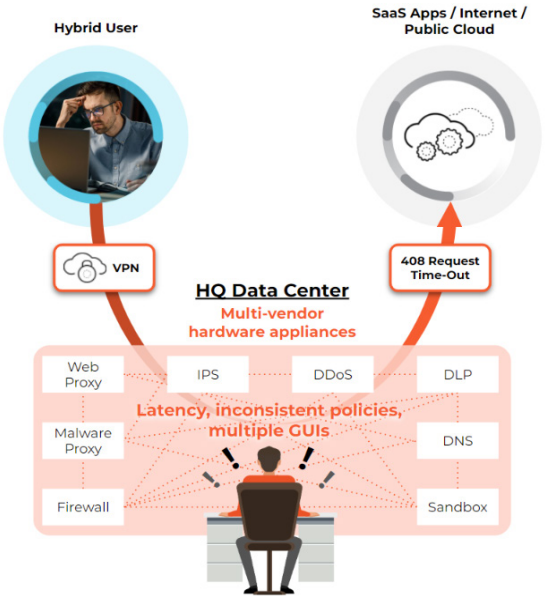


Figura 1: Desvío del tráfico al centro de datos para controlar el acceso e inspeccionarlo

Dispositivos de distintos proveedores:
difíciles de gestionar y seguridad incoherente

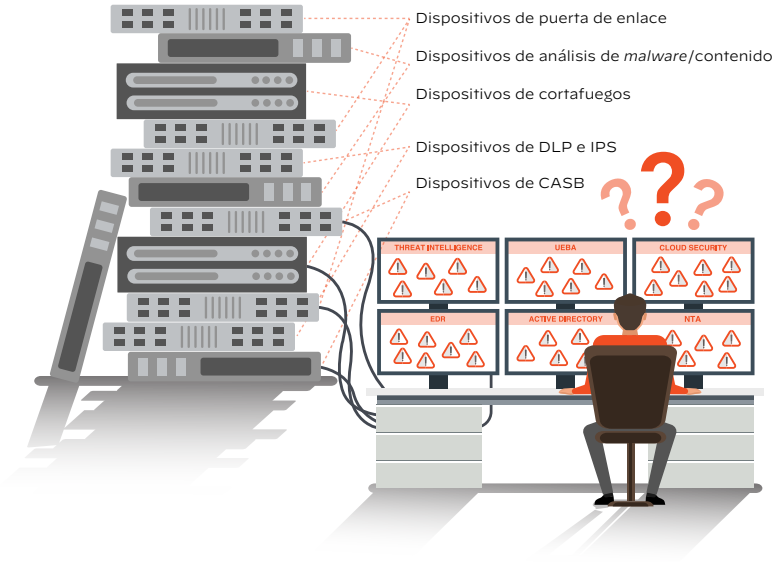


Figura 2: Dispositivos de seguridad de distintos proveedores

Una solución en la nube moderna y completa

Hoy en día, las organizaciones requieren una solución de seguridad web moderna que, además de ofrecerles visibilidad profunda, gestión centralizada y políticas unificadas, blinde a sus usuarios, datos y aplicaciones frente a cualquier amenaza con independencia de dónde residan. Dado que la seguridad web es una parte esencial de una arquitectura moderna de servidor perimetral de acceso seguro (SASE, por sus siglas en inglés), no debería gestionarse de manera aislada. Cloud SWG, la puerta de enlace web segura en la nube de Palo Alto Networks, proporciona seguridad total en la nube a través de Prisma Access.

Nuestro servicio de prevención de amenazas no tiene parangón en el mercado, ya que permite ver todo el tráfico web y protegerlo frente al *malware*, los ataques sin archivo, el *phishing* y un largo etcétera de amenazas. Las tecnologías de prevención de pérdida de datos (DLP, por sus siglas en inglés) para empresas y de agente de seguridad de acceso a la nube (CASB, por sus siglas en inglés) de nueva generación se integran de forma nativa para proporcionar visibilidad completa de las aplicaciones SaaS y garantizar la confidencialidad de los datos en todo momento. A todo esto hay que añadir el filtrado de URL integrado, el análisis de *malware*, la seguridad de la capa del sistema de nombres de dominio (DNS, por sus siglas en inglés) y el aislamiento remoto del navegador (RBI, por sus siglas en inglés): una combinación con la cual es muy fácil llevar una seguridad coherente a todos sus empleados, se conecten desde donde se conecten y sea cual sea el dispositivo que utilicen.

Nuestra puerta de enlace web segura en la nube ofrece una seguridad completa y moderna a través de Prisma Access que incluye:

- **Protección de todo el tráfico de las aplicaciones:** nuestra SWG en la nube no solo da acceso a todas las aplicaciones, sino que también las protege de todo tipo de amenazas (no solo de las dirigidas a las aplicaciones web o procedentes de Internet) y reduce hasta un 45 % el riesgo de sufrir una brecha de datos.[4]
- **Una seguridad completa y de primera:** combina funciones líderes en el sector en una sola plataforma basada en la nube cuya cobertura de seguridad supera a la de cualquier otra solución. Ofrecemos más de 4,3 millones de actualizaciones de seguridad al día (24,5 veces más que nuestro competidor más cercano).
- **Una experiencia del usuario excepcional:** los usuarios finales disfrutan de la mejor experiencia digital posible gracias a que nuestra red tiene poquísima latencia, es sumamente escalable y está sujeta a acuerdos de nivel de servicio (SLA, por sus siglas en inglés) líderes en el sector. Ofrecemos un rendimiento total en túneles cifrados diez veces superior al de nuestro competidor más cercano y nuestros SLA son diez veces mejores que los de cualquier otro servicio en la nube.

Además, Palo Alto Networks es el primer proveedor en introducir funciones de seguridad con aprendizaje automático (AA) en nuestro ya de por sí impresionante arsenal de mecanismos de protección de primer nivel. Prisma Access, que utiliza el aprendizaje automático para ofrecer protección de día cero integrada en tiempo real de manera proactiva, ha sido el primer producto del sector en lograr unos resultados tan impresionantes como estos:

- bloqueo de hasta un 95 % de las amenazas desconocidas basadas en archivos y en la web gracias al aprendizaje automático integrado;
- bloqueo de otras amenazas desconocidas en tiempo casi real mediante actualizaciones de firmas sin demora;
- uso del AA para garantizar la visibilidad y la seguridad de todos los dispositivos, incluidos los de IdC nunca vistos, sin necesidad de sensores adicionales;
- recomendación automática de políticas para ahorrar tiempo y reducir la posibilidad de que se produzcan errores humanos.

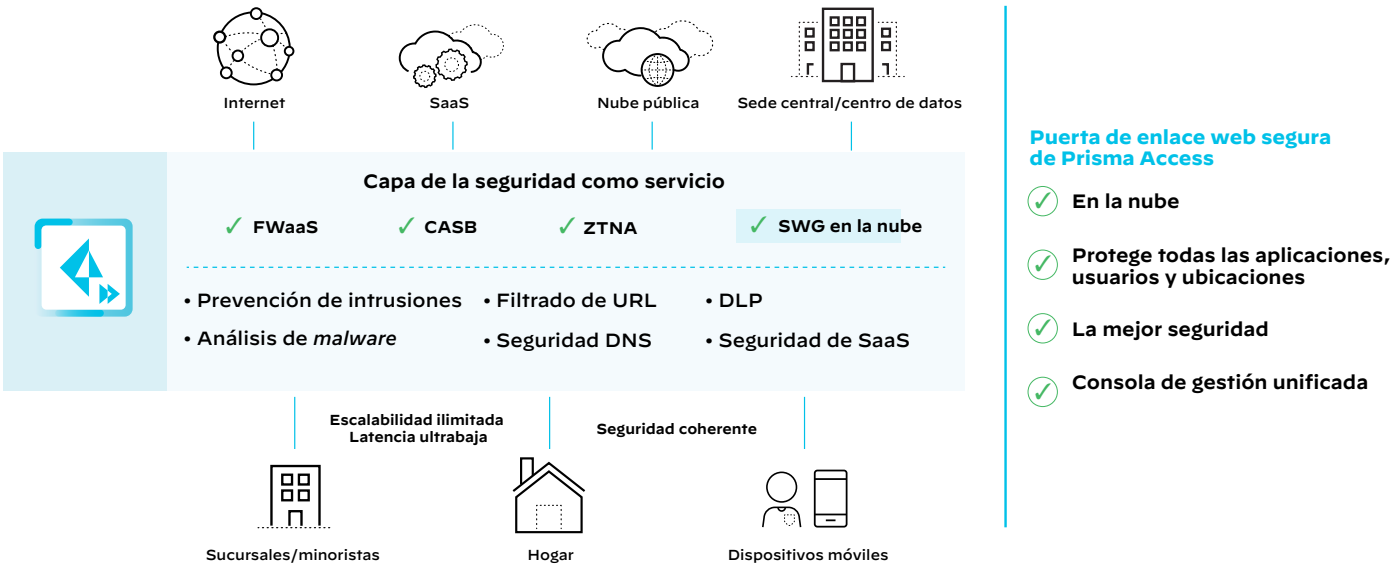


Figura 3: Puerta de enlace web segura (SWG) en la nube para Prisma Access de Palo Alto Networks

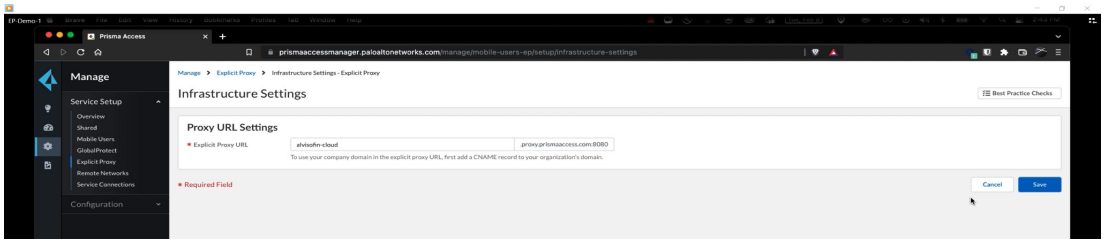
4. *Provide Secure Remote Access And Gain Peace Of Mind With Palo Alto Networks Prisma Access* (disponible en inglés), un informe Total Economic Impact™ realizado por encargo por Forrester Consulting para Palo Alto Networks, enero de 2021. https://start.paloaltonetworks.es/forrester-tei-prisma-access-spotlight.html.

Cómo migrar la seguridad a la nube en solo tres pasos

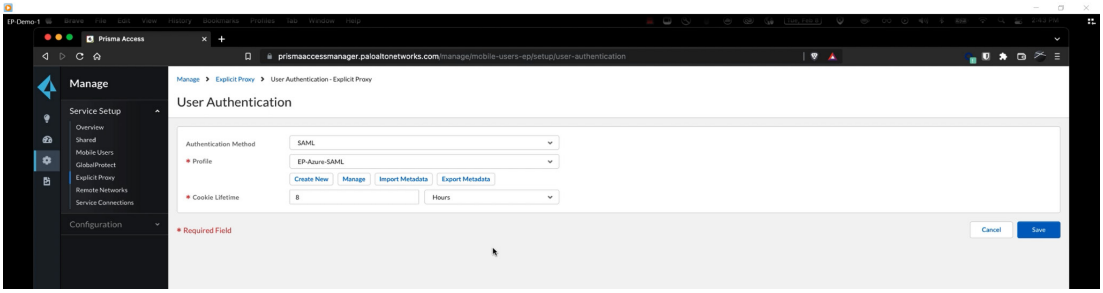
Gracias a la posibilidad de utilizar un proxy explícito en la nube, las organizaciones que mantienen dispositivos proxy web convencionales pueden pasarse fácilmente a Prisma Access, nuestra plataforma de seguridad en la nube moderna. Este enfoque permite actualizar los archivos PAC rápidamente sin necesidad de realizar cambios en la arquitectura de red con el fin de dirigir el tráfico de Internet a nuestro proxy explícito en la nube para controlar el acceso de los usuarios y proteger a la organización de las amenazas de Internet.

Con la gestión en la nube de Prisma Access, aplicar un proxy explícito en la nube es tan fácil como configurar los tres siguientes ajustes: los de la infraestructura, los de la autenticación de usuarios y los de las ubicaciones de Prisma Access. El proceso de configuración dura tan solo unos minutos e incluye una interfaz de administrador tan intuitiva como la ilustrada en las capturas de pantalla siguientes. Encontrará más información en los recursos en línea de TechDocs relativos a la configuración de un proxy explícito en la nube.

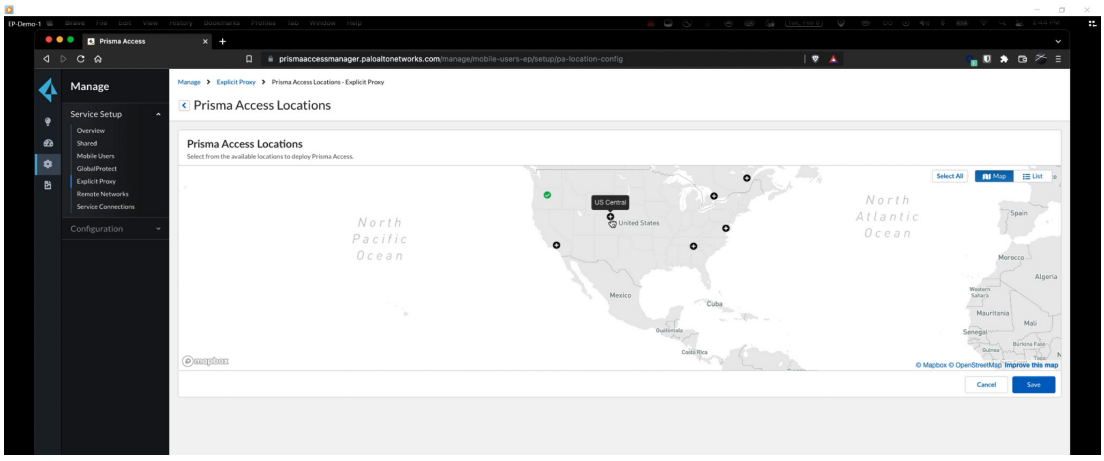
1. Ajustes de la infraestructura



2. Ajustes de la autenticación de usuarios



3. Ajustes de las ubicaciones de Prisma Access



La gestión en la nube de Prisma Access optimiza la configuración de nuestra puerta de enlace web segura en la nube e incluye un panel de prácticas recomendadas, evaluaciones, comprobaciones de campo e informes para mejorar su estrategia de seguridad y aumentar la productividad de los usuarios. Esto permite a las organizaciones evaluar su entorno de forma fácil y continua a través de estas comprobaciones integradas. Las comprobaciones de prácticas recomendadas se aplican a los componentes siguientes:

- su base de reglas de políticas de seguridad (para comprobar cómo se organizan y gestionan las políticas de seguridad, incluidos los ajustes de configuración que se aplican a muchas reglas);
- las reglas de seguridad en sí.

- Perfiles de seguridad
  - » *Antispyware*
  - » Protección frente a vulnerabilidades
  - » WildFire y antivirus
  - » Gestión de acceso a URL
  - » Seguridad DNS
- Autenticación
- Descifrado
- GlobalProtect

Las instrucciones para seguir las prácticas recomendadas incluidas permiten a las organizaciones simplificar la gestión y aumentar la productividad de los usuarios. Prisma Access, que compara sus configuraciones y políticas con las comprobaciones de prácticas recomendadas constantemente, también le permite tomar medidas inmediatas para reforzar su estrategia de seguridad.

Además de nuestra opción de proxy explícito en la nube, Cloud SWG proporciona opciones de conectividad adicionales que permiten a las organizaciones proteger fácilmente todas las aplicaciones y a todos los usuarios, residan donde residan. Esta protección cubre:

- los dispositivos móviles gestionados, que pueden protegerse a través del agente GlobalProtect para garantizar la seguridad de todos los puertos y protocolos y, por extensión, del tráfico web y no web;
- los dispositivos no gestionados que pueden utilizar nuestro acceso sin agente para disfrutar de la protección más completa;
- las sucursales, desde donde los usuarios pueden conectarse fácilmente a través de IPsec.

Seguridad SASE completa por la vía fácil

Las plantillas híbridas y las arquitecturas de acceso directo a las aplicaciones no solo han dejado obsoletas las arquitecturas de seguridad de las organizaciones, sino que además han aumentado escandalosamente sus superficies de ataque. Aunque han surgido distintas ofertas de seguridad basada en la nube, lo único que son capaces de ofrecer son unos mecanismos de protección incoherentes e incompletos con un rendimiento y unas experiencias del usuario que dejan bastante que desear.

Prisma® Access de Palo Alto Networks protege su plantilla híbrida con la seguridad avanzada del ZTNA 2.0 y, al mismo tiempo, ofrece una experiencia del usuario excepcional. Todo, con un producto de seguridad sencillo y unificado. Solo el ZTNA 2.0 de Prisma Access —una solución creada en la nube para ofrecer seguridad a la escala de la nube— protege todo el tráfico de las aplicaciones con las mejores funciones y blinda los accesos y los datos para reducir drásticamente el riesgo de sufrir una brecha de datos. Gracias a un marco de políticas común y a un único panel de gestión, esta plataforma ofrece protección para las plantillas híbridas actuales sin renunciar al rendimiento. Además, Prisma Access combina la gran flexibilidad de los principales proveedores de nube del mundo y el acceso a redes de fibra de calidad prémium independientes para ofrecer los acuerdos de nivel de servicio (SLA, por sus siglas en inglés) más competitivos del sector aplicables al procesamiento de la seguridad, al rendimiento de las aplicaciones y a la experiencia del usuario.

Otro aspecto importante es que Prisma Access propone un proceso claro para las organizaciones que deseen implementar una solución SASE moderna y completa. Según un estudio llevado a cabo por la consultora ESG, *el 69 % de los encuestados indicaron 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.*[5] Nuestra puerta de enlace web segura en la nube se integra perfectamente con nuestro CASB, nuestro cortafuegos como servicio (FWaaS, por sus siglas en inglés) y el acceso Zero Trust (confianza cero) a la red (ZTNA, por sus siglas en inglés) 2.0, todas ellas tecnologías de nueva generación, para ayudar a los clientes a pasarse a un modelo SASE lo antes posible. Si desea más información, consulte el informe técnico sobre cómo modernizar su puerta de enlace web segura con la tecnología SASE elaborado por la consultora ESG.

Descubra cómo Prisma Access y sus funciones de puerta de enlace web segura en la nube pueden ayudar hoy a su organización a proteger todas sus aplicaciones y a todos sus usuarios en todas partes.

5. *Modernize Your Secure Web Gateway with SASE* (disponible en inglés), Enterprise Strategy Group, enero de 2022, https://www.paloaltonetworks.com/resources/whitepapers/modernize-your-secure-web-gateway-with-sase.

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es