# GLOBALPROTECT

## Prevención de infracciones y protección de la plantilla móvil

GlobalProtect lleva la protección característica de la plataforma de seguridad de nueva generación de Palo Alto Networks a su plantilla móvil, allí donde estén.

### *Ventajas y situaciones de uso clave*

**VPN de acceso remoto**

- Permite acceder de forma segura a aplicaciones empresariales basadas en la nube e internas.

**Prevención de amenazas avanzadas**

- Protege el tráfico de Internet.
- Impide que las amenazas lleguen al endpoint.
- Protege del phishing y del robo de credenciales.

**Filtrado de URL**

- Aplica políticas de uso aceptables.
- Filtra el acceso a dominios maliciosos y a contenido para adultos.
- Impide el uso de herramientas de evasión.

**Protección del acceso a aplicaciones SaaS**

- Controla el acceso a aplicaciones SaaS y aplica políticas en ellas a la vez que bloquea las aplicaciones no autorizadas.

**BYOD**

- Admite el uso de VPN al nivel de las aplicaciones para conservar la privacidad del usuario.
- Permite un acceso seguro sin necesidad de cliente a socios, asociados comerciales y contratistas.

**Refuerzo de la segmentación de la red interna**

- Ofrece una identificación de usuario fiable.
- Proporciona información precisa e inmediata del host para favorecer la visibilidad y la aplicación de políticas.
- Aplica una autenticación multifactor superior para acceder a recursos confidenciales.

La realidad que necesita proteger sigue en expansión, pues tanto los usuarios como las aplicaciones cambian de lugar y traspasan el perímetro tradicional de la red. Los equipos de seguridad se enfrentan a dificultades a la hora de mantener la visibilidad del tráfico de la red y aplicar políticas de seguridad para poner freno a las amenazas. Las tecnologías que se han venido usando para proteger los endpoints móviles, como el software antivirus de los endpoints del host y las VPN de acceso remoto, no pueden detener las avanzadas técnicas que emplean los atacantes de hoy en día, que cuentan con un mayor grado de sofisticación.

El cliente de seguridad de red para endpoints GlobalProtect™ de Palo Alto Networks® permite a las organizaciones proteger la plantilla móvil ampliando la plataforma de seguridad de nueva generación a todos los usuarios, con independencia de su ubicación. Este cliente protege el tráfico empleando la capacidad que presenta la plataforma para comprender el uso de las aplicaciones, asociar el tráfico a usuarios y dispositivos, y aplicar políticas de seguridad con tecnologías de nueva generación.

### Ampliación de la protección de la plataforma hacia el exterior

GlobalProtect vela por la seguridad de la plantilla móvil inspeccionando todo el tráfico mediante los cortafuegos de nueva generación de la organización, que se implementan como puertas de enlace de Internet, ya sea en el perímetro, la DMZ o la nube. Los ordenadores portátiles, los teléfonos inteligentes y las tablets que incorporan la aplicación de GlobalProtect establecen automáticamente una conexión VPN IPSec/SSL segura con el cortafuegos de nueva generación que ofrece el mejor rendimiento en una ubicación determinada. De esta forma, la organización goza de total visibilidad en lo que respecta a todo el tráfico de red, a las aplicaciones, a los puertos y a los protocolos. Al eliminar los ángulos muertos del tráfico de la plantilla móvil, la organización mantiene una perspectiva coherente de las aplicaciones.

### Protección de la red a nivel interno

No todos los usuarios necesitan acceder a todos los recovecos de la red empresarial. Los equipos de seguridad están adoptando medidas de segmentación de la red para dividirla y aplicar controles precisos de acceso a recursos internos. GlobalProtect facilita la identificación de usuario más fiable y rápida para la plataforma, lo que posibilita a las organizaciones elaborar políticas precisas que permitan o restrinjan el acceso en función de las necesidades de la empresa. Y eso no es todo: GlobalProtect también proporciona información del host, que sirve para establecer criterios de dispositivos asociados a políticas de seguridad. Con estas medidas, las organizaciones pueden emprender acciones preventivas para proteger sus redes internas, instaurar controles de red Zero Trust y reducir la superficie expuesta a ataques.

Cuando GlobalProtect se implementa de esta manera, las puertas de enlace de red internas se pueden configurar para su uso con o sin un túnel VPN.

### Inspección del tráfico y aplicación de políticas de seguridad

GlobalProtect hace que los equipos de seguridad puedan crear políticas que se apliquen de manera coherente, con independencia de que el usuario sea interno o remoto. Para prevenir los ciberataques, los equipos de seguridad pueden servirse de todas las funciones de la plataforma, entre las que se incluyen las siguientes:

- **Tecnología App-ID™**. Identifica el tráfico de las aplicaciones, sea cual sea el número de puerto, y permite a las organizaciones establecer políticas para gestionar el uso de las aplicaciones en función de los usuarios y los dispositivos.
- **Tecnología User-ID™**. Identifica los usuarios y su pertenencia a grupos para disfrutar de visibilidad total y aplicar políticas de seguridad de la red basadas en funciones.
- **Descifrado**. Inspecciona y controla las aplicaciones cifradas con tráfico SSL/TLS/SSH. Además, detiene las amenazas que se encuentran dentro del tráfico cifrado.
- **Servicio de análisis de amenazas basado en la nube de WildFire™**. Automatiza el examen de contenido para detectar malware nuevo, desconocido y altamente específico por su comportamiento, y articula la inteligencia sobre amenazas precisa para frenarlo casi en tiempo real.
- **Prevención de amenazas para IPS y antivirus**. La prevención de intrusiones bloquea los exploits basados en la red que tienen como objetivo aplicaciones y sistemas operativos vulnerables, los ataques de DoS y los análisis de puertos. Los perfiles de antivirus impiden que el malware y el spyware lleguen al endpoint gracias a un motor basado en flujos de datos.
- **Filtrado de URL con PAN-DB**. PAN-DB categoriza las URL en función del contenido a nivel de dominio, de archivo y de página, y recibe actualizaciones de WildFire de modo que, cuando el contenido web cambia, también cambian las categorizaciones.
- **Bloqueo de archivos**. Impide la transferencia de archivos peligrosos y no deseados, y examina más a fondo los permitidos con WildFire.
- **Filtrado de datos**. Esta función permite a los administradores aplicar políticas que sirven para frenar el movimiento no autorizado de datos, como la transferencia de información de clientes o de cualquier otro contenido confidencial.

### Condiciones de host personalizadas (p. ej., identificación de usuarios y dispositivos)

#### *Autenticación de usuarios*

GlobalProtect es compatible con todos los métodos de autenticación PAN-OS® que existen, incluidos Kerberos, RADIUS, LDAP, SAML 2.0, certificados de clientes y una base de datos de usuario local. Una vez que GlobalProtect ha autenticado al usuario, transmite de inmediato al cortafuegos de nueva generación la asignación de usuario y dirección IP que se utiliza para User-ID.

#### *Opciones de autenticación sólida*

GlobalProtect es compatible con numerosos métodos de autenticación multifactor de terceros, entre los que se incluyen los testigos de contraseña de un solo uso, los certificados y las tarjetas inteligentes mediante la integración de RADIUS.

Estas características ayudan a las organizaciones a lograr que la prueba de identidad para acceder al centro de datos interno o a las aplicaciones de SaaS sea más estricta.

GlobalProtect incluye opciones que permiten que la autenticación, aunque sólida, sea incluso más sencilla de utilizar e implementar:

- **Autenticación basada en cookies:** una vez realizada la autenticación, la organización puede optar por usar una cookie cifrada para los posteriores accesos a un portal o una puerta de enlace mientras dure dicha cookie.
- **Compatibilidad con protocolos de inscripción de certificados simple:** GlobalProtect puede automatizar la interacción con una PKI de empresa para gestionar, emitir y distribuir certificados a los clientes de GlobalProtect.

#### *Perfil de información de host*

GlobalProtect comprueba el endpoint para obtener un inventario de sus ajustes y crea un perfil de información de host que se comparte con el cortafuegos de nueva generación. Este último utiliza dicho perfil para ejecutar políticas de aplicación que solo permiten el acceso cuando el endpoint está correctamente configurado y protegido. Estos principios ayudan a exigir el cumplimiento de las políticas que rigen en qué medida un usuario concreto debe acceder a un dispositivo determinado.

Las políticas de perfiles de información de host se pueden basar en diversos atributos, entre ellos, los siguientes:

- El nivel del parche de la aplicación y el sistema operativo
- El estado y la versión del antimalware del host
- El estado y la versión del cortafuegos del host
- La configuración del cifrado del disco
- La configuración del producto de copia de seguridad de datos
- Las condiciones de host personalizadas (p. ej., entradas de registro y software en ejecución)

#### *Control del acceso a aplicaciones y datos*

Los equipos de seguridad pueden establecer políticas basadas en la aplicación, el usuario, el contenido y la información del host para mantener un control exhaustivo del acceso a cierta aplicación. Estas políticas se pueden asociar a determinados usuarios o grupos definidos en un directorio para garantizar que las organizaciones ofrecen los niveles de acceso correctos en función de las necesidades de la empresa. El equipo de seguridad puede establecer más políticas para una autenticación multifactor superior con el fin de proporcionar una prueba de identidad adicional antes de acceder a recursos y aplicaciones especialmente confidenciales.

### Protección y adopción de la iniciativa BYOD

Los efectos de la iniciativa BYOD están cambiando el número de permutaciones de casos de uso que los equipos de seguridad deben afrontar. Es necesario brindar acceso a las aplicaciones a un conjunto más amplio de empleados y contratistas mediante un gran abanico de dispositivos móviles.

La integración de soluciones de gestión de dispositivos móviles, como AirWatch® y MobileIron®, permite a las organizaciones implementar GlobalProtect, así como ofrecer medidas de seguridad adicionales por medio del intercambio de inteligencia y configuración del host. Al usarse en conjunto con GlobalProtect, la organización puede conservar la visibilidad y aplicar las políticas de seguridad

en cada una de las aplicaciones, al mismo tiempo que mantiene la separación de los datos de las actividades personales para ajustarse a las expectativas de privacidad de los usuarios cuando se utilicen dispositivos personales (BYOD).

GlobalProtect admite VPN SSL sin cliente para posibilitar un acceso seguro a las aplicaciones del centro de datos y la nube desde dispositivos no gestionados. Este enfoque ofrece comodidad y seguridad, ya que permite acceder a aplicaciones concretas por medio de una interfaz web sin necesidad de que el usuario tenga que instalar un cliente de antemano o configurar un túnel completo.

### La arquitectura importa

La arquitectura flexible de GlobalProtect ofrece numerosas posibilidades que ayudan a las organizaciones a superar una gran variedad de retos en materia de seguridad. Empezando por lo más básico, las organizaciones pueden servirse de GlobalProtect para sustituir la puerta de enlace de VPN tradicional, con lo que se olvidan de la complejidad y los quebraderos de cabeza que conlleva administrar una puerta de enlace de VPN independiente y de terceros.

Las opciones de conexión manual y selección de puerta de enlace permiten a las organizaciones personalizar la configuración para satisfacer los requisitos de la empresa como sea preciso.

En las implementaciones más completas para proteger el tráfico, GlobalProtect puede implementarse con una conexión VPN ininterrumpida con un túnel completo, lo que garantiza que siempre exista protección y que esta resulte transparente para el usuario.

#### *Puertas de enlace basadas en la nube*

La plantilla se mueve de un sitio a otro y eso genera cambios en la carga de tráfico. Esta afirmación se refuerza en especial cuando pensamos en la manera en la que evolucionan las empresas: temporalmente (como por una catástrofe natural en una región) o permanentemente (como introducirse en nuevos mercados).

El servicio en la nube de GlobalProtect ofrece una opción cogestionada para implementar cobertura en las ubicaciones que necesitan las organizaciones mediante sus políticas de seguridad. Se puede usar en combinación con los cortafuegos instalados, lo que permite adaptar la arquitectura a las cambiantes condiciones.

El servicio en la nube de GlobalProtect admite la escalabilidad automática, que asigna nuevos cortafuegos de manera dinámica en función de la carga y la demanda de una región determinada.

### Conclusión

Los métodos de protección que ofrece la plataforma de seguridad de nueva generación de Palo Alto Networks desempeñan un papel fundamental en la prevención de infracciones. Utilice GlobalProtect para llevar la protección de la plataforma a los usuarios vayan donde vayan. Con GlobalProtect, las organizaciones pueden lograr una aplicación coherente de políticas de seguridad para que, incluso cuando los usuarios salgan de las instalaciones, la protección frente a los ciberataques les acompañe.

## Funciones de GlobalProtect

| Categoría | Especificación |
|---|---|
| **Conexión VPN** | IPSec |
| | SSL |
| | VPN sin cliente |
| | VPN por aplicación en Android™, iOS y Windows® 10 |
| **Selección de puerta de enlace** | Selección automática |
| | Selección manual |
| | Selección de puerta de enlace externa según ubicación de origen |
| | Selección de puerta de enlace interna según IP de origen |
| **Métodos de conexión** | Inicio de sesión de usuario (siempre activado) |
| | A petición |
| | Anterior al inicio de sesión (siempre activado) |
| | Anterior al inicio de sesión, después a petición |
| **Modo de conexión** | Modo interno |
| | Modo externo |
| **Protocolos de capa 3** | IPv4 |
| | IPv6 |
| **Inicio de sesión único** | SSO (proveedor de credenciales de Windows) |
| | SSO de Kerberos |

| Categoría | Especificación |
|---|---|
| **División de túneles** | Inclusión de rutas |
| | Exclusión de rutas |
| **Métodos de autenticación** | SAML 2.0 |
| | LDAP |
| | Certificados de cliente |
| | Kerberos |
| | RADIUS |
| | Autenticación de dos factores |
| **Perfil de información de host, elaboración de informes, aplicación de políticas y notificaciones** | Gestión de parches |
| | Antispyware de host |
| | Antivirus de host |
| | Cortafuegos de host |
| | Cifrado de disco |
| | Copia de seguridad de disco |
| | Prevención de pérdida de datos |
| | Condiciones de perfil de información de host personalizadas (p. ej., entradas de registro y software en ejecución) |
| **Autenticación multifactor** | Autenticación avanzada para el acceso a recursos confidenciales |
| **Otras funciones** | User-ID |
| | Reserva de VPN de IPSec a SSL |
| | Aplicación de conexión de GlobalProtect para el acceso a redes |
| | Gestión automática de certificados de usuarios basada en SCEP |
| | Acciones de script que se ejecutan antes y después de las sesiones |
| | Personalización dinámica de la aplicación de GlobalProtect |
| | Configuración de la aplicación en función de los usuarios, grupos o sistemas operativos |
| | Detección automática interna o externa |
| | Actualización manual o automática de la aplicación de GlobalProtect |
| | Selección de certificado según OID |
| | Bloqueo del acceso desde dispositivos perdidos, robados y desconocidos |
| | Compatibilidad de tarjetas inteligentes para conexión y desconexión |
| | Distribución transparente de CA raíz de confianza para descifrado SSL |
| | Desactivación del acceso directo a redes locales |
| | Páginas de bienvenida y de ayuda personalizables |
| | Conexión RDP a un cliente remoto |

| Categoría | Especificación |
|---|---|
| **Integración de MDM/EMM** | AirWatch |
| | MobileIron |
| **API y herramientas de gestión** | Plataforma de seguridad de nueva generación de Palo Alto Networks, incluidos formatos físicos (como PA-7000 Series, PA-3000 Series y PA-200) y virtuales (VM-Series) |
| | Microsoft InTune® |
| | Servicio en la nube de GlobalProtect |
| **Plataformas compatibles con la aplicación de GlobalProtect** | Microsoft® Windows y Windows UWP |
| | Apple® Mac® OS X® |
| | Apple iOS |
| | Google® Chrome® OS |
| | Android® OS |
| | Linux® compatible mediante VPNC de terceros y cliente de StrongSwan |
| **XAUTH de IPSec** | Cliente de IPSec de Apple iOS |
| | Cliente de IPSec de Android |
| **Localización de la aplicación de GlobalProtect** | Inglés |
| | Español |
| | Alemán |
| | Francés |
| | Japonés |
| | Chino |

3000 Tannery Way
Santa Clara, CA 95054 (EE. UU.)

Línea principal: +1 408 753 4000
Ventas: +1 408 753 4000
Asistencia técnica: +1 408 753 4000

www.paloaltonetworks.com


**globalprotect-ds-082817**