GLOBALPROTECT

Prevenga brechas y garantice la fuerza de trabajo móvil

GlobalProtect extiende la protección de la Security Operating Platform de Palo Alto Networks a los miembros de su fuerza laboral móvil, sin importar a dónde vayan.

Principales escenarios de uso y beneficios

VPN de acceso remoto

- Provee acceso seguro a aplicaciones comerciales internas y basadas en la nube.

prevención de amenazas avanzada

- Protege el tráfico de Internet.
- Detiene las amenazas para evitar que lleguen al endpoint.
- Protege contra phishing y robo de credenciales.

URL Filtering

- Ejecuta políticas de uso aceptables.
- Filtra el acceso a dominios malintencionados y contenido para adultos.
- Previene el uso de herramientas de elusión y evasión.
- Asegura el acceso a aplicaciones SaaS.
- Controla el acceso y ejecuta políticas para aplicaciones SaaS mientras bloquea aplicaciones no sancionadas.

BYOD

- Brinda soporte para el VPN a nivel de la aplicación para la privacidad del usuario.
- Habilita el acceso seguro sin cliente para socios, asociados comerciales y contratistas.
- Admite la identificación automatizada de dispositivos no gestionados.
- Admite mecanismos de autenticación personalizados para dispositivos gestionados y no gestionados.

Implementación de la confianza cero

- Ofrece identificación confiable del usuario.
- Entrega información inmediata y precisa sobre el host para aportar visibilidad y cumplimiento con las políticas.
- Implementa una configuración de autenticación de varios factores para el acceso a recursos confidenciales.

El mundo que debe proteger continúa expandiéndose mientras que los usuarios y las aplicaciones se mueven a ubicaciones fuera del perímetro tradicional de la red. Los equipos de seguridad enfrentan desafíos para mantener la visibilidad del tráfico de red y ejecutar políticas de seguridad orientadas a detener las amenazas. Las tecnologías tradicionales utilizadas para proteger los endpoints móviles, como el software antivirus del endpoint host y la virtual private network (Red privada virtual – VPN) de acceso remoto, no pueden detener las técnicas avanzadas empleadas por los sofisticados atacantes de hoy en día.

La seguridad de red de Palo Alto Networks GlobalProtect™ para endpoints permite a las organizaciones proteger a la fuerza laboral móvil mediante la extensión de Security Operating Platform® a todos los usuarios, independientemente de su ubicación. Protege el tráfico al aplicar las capacidades de la plataforma para entender el uso de las aplicaciones, asociar el tráfico con usuarios y dispositivos, y ejecutar políticas de seguridad con tecnologías de nueva generación.

Extender la protección de la plataforma de forma externa

GlobalProtect protege la fuerza de trabajo móvil, ya que inspecciona todo el tráfico con los firewall de nueva generación de la organización que se implementan como gateway de Internet, ya sea en el perímetro, en la zona desmilitarizada (DMZ) o en la nube. Las computadoras portátiles, los teléfonos inteligentes y las tabletas con la aplicación de GlobalProtect establecen automáticamente una conexión IPsec/SSL VPN segura con el firewall de nueva generación con el uso del mejor gateway, lo que proporciona a la organización una visibilidad completa de todo el tráfico de la red, las aplicaciones, los puertos y los protocolos. Al eliminar los puntos ciegos en el tráfico de la fuerza laboral móvil, su organización mantiene una vista consistente de las aplicaciones.

Implementación de confianza cero en su red

No todos los usuarios necesitan acceso a todos los activos de su red corporativa. Los equipos de seguridad están adoptando los principios de confianza cero para segmentar sus redes y aplicar controles precisos para el acceso a los recursos internos. GlobalProtect proporciona la identificación de usuarios más rápida y acreditada para la plataforma, lo que posibilita a las organizaciones para escribir políticas precisas que permitan o restrinjan el acceso en función de las necesidades comerciales. Además, GlobalProtect proporciona información del host para establecer criterios de cumplimiento de dispositivos asociados con políticas de seguridad. Estas medidas le permiten tomar medidas preventivas para proteger sus redes internas, adoptar controles de red de confianza cero y reducir el riesgo de ataques.

Cuando GlobalProtect se implementa de esta manera, los gateways internos pueden configurarse con o sin un túnel de VPN.

Inspección de tráfico y ejecución de políticas de seguridad

GlobalProtect permite a los equipos de seguridad crear políticas que se ejecutan de forma consistente, tanto para usuarios internos o remotos. Los equipos de seguridad pueden evitar los ciberataques eficaces con el uso de todas las capacidades de la plataforma:

- **Tecnología App-ID™**: identifica el tráfico de las aplicaciones, independientemente de la cantidad de puertos, y permite a las organizaciones establecer políticas para gestionar el uso de las aplicaciones con base en usuarios y dispositivos.
- **Tecnología User-ID™**: identifica los usuarios y membresías de grupos para mayor visibilidad como también para la ejecución de políticas de seguridad de red basadas en funciones.
- **Descifrado de SSL:** inspecciona y controla las aplicaciones que están cifradas con el tráfico SSL/TLS/SSH y detiene las amenazas dentro del tráfico cifrado.
- **El servicio de prevención de malware WildFire® automatiza** el análisis del contenido para identificar malware nuevo, desconocido hasta ahora y altamente segmentado por su comportamiento y genera la inteligencia de amenazas para detenerlo en tiempo casi real.
- **Threat Prevention (Prevención de amenazas) para IPS y antivirus** bloquea los exploits basados en la red dirigidos a aplicaciones y sistemas operativos vulnerables, ataques de denial-of-service (denegación de servicio – DOS) y análisis de puertos. Los perfiles de antivirus evitan que malware y spyware alcancen el endpoint al utilizar un motor basado en flujos de tráfico.
- **El URL Filtering con PAN-DB** categoriza las URL basadas en su contenido a nivel del dominio, los archivos y la página, y recibe actualizaciones de WildFire para que cuando el contenido web se modifique, también se modifiquen las categorías.
- **El bloqueo de archivos** detiene la transferencia de archivos no deseados y peligrosos, mientras continúa examinando los archivos permitidos con WildFire.
- **El filtrado de Datos** permite a los administradores implementar políticas que pueden usarse para detener el movimiento de datos no autorizados, como la transferencia de información de clientes u otro contenido confidencial.

Control de acceso seguro

Autenticación del usuario

GlobalProtect es compatible con todos los métodos de autenticación de PAN-OS® existentes, como Kerberos, RADIUS, LDAP, SAML 2.0, certificados de clientes, inicio de sesión biométrico, y una base de datos de usuarios local. Una vez que GlobalProtect autentica el usuario, proporciona inmediatamente el mapeo de la dirección usuario-a-IP como User-ID para el firewall de nueva generación.

Fuertes opciones de autenticación

GlobalProtect es compatible con un amplio rango de métodos de autenticación de terceros (MFA), de varios factores, como tokens de one-time password (contraseña única – OTP), certificados y tarjetas inteligentes a través de la integración con RADIUS y SAML.

Estas opciones ayudan a las organizaciones a fortalecer la prueba de identidad para el acceso al centro de datos interno o las aplicaciones de software como servicio (SaaS).

GlobalProtect tiene opciones para facilitar aún más el uso y la implementación de la autenticación segura:

- **Autenticación basada en cookies:** Luego de la autenticación, puede optar por el uso de una cookie cifrada para el acceso posterior a un portal o gateway durante la vida útil de esa cookie
- **Compatibilidad simplificada con el protocolo de inscripción de certificados:** GlobalProtect puede automatizar la interacción con un PKI de empresa para gestionar, emitir y distribuir certificados a los clientes de GlobalProtect.
- **MFA:** Antes de que un usuario pueda acceder a una aplicación, se le puede exigir que presente una forma adicional de autenticación.

Host information profile (perfil de información de host – HIP)

GlobalProtect verifica el endpoint para obtener un inventario de cómo está configurado y crea un host information profile (perfil de información de host – HIP) que se comparte con el firewall de nueva generación. El firewall de nueva generación utiliza el HIP para ejecutar las políticas de aplicaciones que solo permiten el acceso cuando el endpoint está correctamente configurado y protegido. Estos principios ayudan a hacer cumplir las políticas que rigen la cantidad de accesos que un usuario dado debe tener con un dispositivo en particular.

Las políticas de HIP pueden basarse en una serie de atributos, como:

- Identificación de dispositivos gestionados/no gestionados
- Certificados de máquina presentes en el dispositivo
- Información sobre dispositivos recibida del administrador de dispositivos móviles
- Nivel de parches del sistema operativo y la aplicación
- Versión y estado del antimalware del host
- Versión y estado del firewall del host
- Configuración de cifrado del disco
- Configuración del backup de los datos del producto
- Condiciones personalizadas del host (por ejemplo, entradas de registro, software en ejecución)

Controlar el acceso a las aplicaciones y a los datos

Los equipos de seguridad pueden establecer políticas basadas en aplicaciones, usuarios, contenido, e información de host para mantener el control granular sobre el acceso a una aplicación dada. Estas políticas pueden asociarse con usuarios específicos o grupos definidos en un directorio para asegurar que las organizaciones proporcionen los niveles de acceso correctos en función de sus necesidades comerciales. El equipo de seguridad puede definir otras políticas de configuración de MFA a fin de proporcionar pruebas adicionales de identidad antes de acceder a recursos y aplicaciones particularmente confidenciales.

Solución de problemas y visibilidad mejorados

Los widgets, los informes y el nuevo registro del Application Command Center (Centro de comando de aplicación – ACC) de la Aplicación de GlobalProtect proporcionan una visibilidad completa del uso de GlobalProtect en su implementación. El registro detallado del flujo de trabajo de conexión por etapas simplifica enormemente la solución de problemas de conexión del usuario. Este registro permite a los administradores identificar fácilmente la etapa/evento en el proceso de conexión donde un usuario determinado tiene un problema.

BYOD seguro y habilitado

Los efectos de las políticas de Bring-Your-Own-Device (trae tu propio dispositivo – BYOD) están modificando la cantidad de permutaciones de casos de uso que los equipos de seguridad deben respaldar. Resulta necesario ofrecer acceso a aplicaciones a un mayor espectro de empleados y contratistas que utilizan un amplio rango de dispositivos móviles.

La integración con ofertas de mobile device management (gestión de dispositivos móviles – MDM), como AirWatch® y MobileIron®, puede contribuir a que implemente GlobalProtect y, además, ofrecen medidas de seguridad adicionales a través del intercambio de inteligencia y configuración de hosts. Cuando se utiliza en forma conjunta con GlobalProtect, su organización puede mantener la visibilidad y el cumplimiento con la política de seguridad bajo una modalidad por aplicación mientras mantiene la separación de datos de las actividades personales, a fin de cumplir con las expectativas de privacidad de los usuarios en situaciones de BYOD.

GlobalProtect es compatible con SSL VPN sin cliente para el acceso seguro a aplicaciones en el centro de datos y en la nube desde dispositivos no gestionados. Este enfoque permite a los clientes habilitar el acceso seguro para los usuarios y empleados de terceros que se conectan desde dispositivos BYOD, lo que proporciona acceso a aplicaciones específicas a través de una interfaz web, tanto sin la necesidad de que los usuarios instalen un cliente como sin la necesidad de configurar un túnel de VPN.

La arquitectura importa

La arquitectura flexible de GlobalProtect proporciona muchas capacidades que pueden ayudarlo a resolver una selección de desafíos de seguridad. En el nivel más básico, puede usar GlobalProtect como reemplazo de un gateway VPN tradicional, eliminar la complejidad y las complicaciones de administrar un gateway VPN de terceros independiente.

Las opciones para la selección manual de conexiones y gateways le permiten personalizar la configuración de acuerdo con los requisitos comerciales, según se necesite.

En una implementación más extensa para asegurar el tráfico, GlobalProtect puede implementarse con una conexión VPN permanente con un túnel completo, lo que asegura que la protección siempre esté presente y sea transparente para la experiencia del usuario. Se pueden definir excepciones para el tráfico confidencial a la latencia por aplicación, nombres de dominio y rutas, o tráfico de video.

Gateways basados en la nube

El movimiento de las fuerzas de trabajo de una ubicación a otra genera cambios en las cargas de tráfico. Esto es especialmente cierto cuando se considera cómo evolucionan las compañías, ya sea de manera temporal (como ante un desastre natural) o permanente (como al ingresar en nuevos mercados).

Prisma™ Access de Palo Alto Networks ofrece una opción de administración conjunta para implementar la cobertura en las ubicaciones que precisan las organizaciones, a través de sus políticas de seguridad. Puede utilizarse de manera conjunta con sus firewalls existentes, lo que hace que su arquitectura se ajuste a condiciones de constante cambio.

Prisma Access incluye el escalamiento automático, que asigna nuevos firewalls de manera dinámica en función de la carga y la demanda en una región determinada.

Conclusión

Security Operating Platform de Palo Alto Networks cumple una función importante en la prevención de brechas. Use GlobalProtect para extender la protección de la plataforma a los usuarios donde quiera que vayan. Al usar GlobalProtect, puede ejecutar de forma consistente las políticas de seguridad para que, incluso cuando los usuarios dejan el edificio, su protección contra ciberataques siga funcionando.

Tabla 1: Funciones de GlobalProtect	
Categoría	**Especificación**
Conexión VPN	IPsec
	SSL
	VPN sin cliente
	VPN por aplicación en Android®, iOS
Selección de gateway	Selección automática
	Selección manual
	Selección de gateway preferida
	Selección de gateway externo por ubicación de origen
	Selección de gateway interno por IP de origen
Métodos de conexión	Inicio de sesión de usuario (siempre activo)
	A petición
	Anterior al inicio de sesión (siempre activado)
	Anterior al inicio de sesión, luego a petición
	Anterior al inicio de sesión por el usuario
Modo de conexión	Modo interno
	Modo externo
Protocolos de capa 3	IPv4
	IPv6
Single sign-on (registro único – SSO)	SSO (proveedor de credenciales de Windows)
	SSO Kerberos
	SSO para macOS ®
Túnel dividido	Incluye rutas, dominios, aplicaciones
	Excluye rutas, dominios, aplicaciones
Métodos de autenticación	SAML 2.0
	LDAP
	Certificados de cliente
	Kerberos
	RADIUS
	Autenticación de dos factores
	Selección del método de autenticación a partir de la propiedad del sistema operativo o del dispositivo
Informe HIP, cumplimiento de políticas y notificaciones	Gestión de parches
	Antispyware del host
	Antimalware del host
	Firewall del host
	Cifrado del disco
	Backup del disco
	Data loss prevention (prevención de pérdida de datos – DLP)
	Condiciones personalizadas del host information profile (perfil de información de host – HIP) (p. ej. entradas de registro, software en ejecución)
Identificación del dispositivo gestionado	Por certificados de máquina
	Por número de serie del hardware
MFA	En el momento de la conexión y en el momento del acceso a los recursos
Otras funciones	User-ID
	Último recurso de IPSec a SSL VPN
	Implemente la conexión de GlobalProtect para el acceso a la red

Tabla 1: Funciones de GlobalProtect (continuación)	
Categoría	**Especificación**
Otras funciones	Configuración de túnel basada en la ubicación del usuario
	Redistribución del informe HIP
	Verificación de certificados en HIP
	Gestión automática de certificados de usuario basada en SCEP
	Secuencias de acciones que se ejecutan antes y después de las sesiones
	Personalización dinámica de aplicaciones de GlobalProtect
	Configuración de aplicaciones basadas en usuarios, grupos o sistemas operativos
	Detección automática interna/externa
	Actualización manual/automática de la aplicación de GlobalProtect
	Selección de certificados por OID
	Bloqueo de acceso por dispositivos perdidos, robados o desconocidos
	Compatibilidad con tarjeta inteligente para su conexión/desconexión
	Distribución transparente de CA raíz confiable para el descifrado de SSL
	Deshabilitación del acceso directo a redes locales
	Páginas de bienvenida y de ayuda personalizables
	Conexión RDP a cliente remoto
	Notificaciones nativas del sistema operativo
	Restricción de cierre de sesión de usuario
	Admisión de proxy
	Aplicación de las exclusiones de GlobalProtect
	Conexión solo con SSL
	Integración de tokens de software RSA
Integración MDM/EMM	AirWatch
	MobileIron
	Microsoft InTune®
Herramientas de Gestión y API	Firewalls de nueva generación de Palo Alto Networks, incluidos los dispositivos físicos y virtuales
	Prisma Access
	Gestión de seguridad de red Panorama™
Plataformas compatibles con la aplicación de GlobalProtect	Microsoft® Windows y Windows UWP
	Apple macOS
	Apple iOS e iPadOS™
	Google Chrome® OS
	Android OS
	Linux OS (Red Hat®, CentOS®, Ubuntu)
	Dispositivos IoT
IPsec XAuth	Cliente Apple iOS IPSec
	Cliente Android OS IPSec
	Cliente de VPNC y StrongSwan de terceros
Localización de la aplicación de GlobalProtect	Chino, Inglés, Francés, Alemán, Japonés, Español

3000 Tannery Way
Santa Clara, CA 95054

Teléfono principal: +1.408.753.4000
Ventas: +1.866.320.4788
Asistencia: +1.866.898.9087

www.paloaltonetworks.com

globalprotect-ds-102919