Guía del administrador de GlobalProtect

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 4, 2020

Table of Contents

Descripción general de GlobalProtect 7

Acerca de los componentes de GlobalProtect 9
- Portal GlobalProtect 9
- Puertas de enlace de GlobalProtect 9
- Aplicación de GlobalProtect 9

¿Qué versiones de sistema operativo admite GlobalProtect? 11
Acerca de las licencias de GlobalProtect 12

Comenzar 15

Creación de interfaces y zonas para GlobalProtect 17
Habilitación de SSL entre componentes de GlobalProtect 20
- Acerca de la implementación de certificados GlobalProtect 20
- Recomendaciones para certificados de GlobalProtect 20
- Implementación de certificados de servidores en los componentes de GlobalProtect 23

Autenticación 29

Acerca de la autenticación de usuarios de GlobalProtect 31
- Métodos de autenticación de GlobalProtect admitidos 31
- ¿Cómo sabe la aplicación qué credenciales proporcionar? 33
- ¿Cómo sabe la aplicación qué certificado proporcionar? 35

Configuración de autenticación externa 36
- Configuración de autenticación LDAP 36
- Configuración de autenticación SAML 38
- Configuración de autenticación Kerberos 44
- Configuración de autenticación RADIUS o TACACS+ 46

Configuración de la autenticación de certificado de cliente 49
- Implementación de certificados de cliente compartidos para autenticación 49
- Implementación de certificados de equipo para autenticación 49
- Implementación de certificados de cliente específicos del usuario para autenticación 54

Configuración de la autenticación en dos fases 58
- Habilitación de la autenticación en dos fases con perfiles de autenticación y certificado 58
- Habilitación de la autenticación en dos fases mediante contraseñas de un solo uso (OTP) 60
- Habilitación de autenticación en dos fases mediante tarjetas inteligentes 65
- Habilitación de la autenticación de doble factor mediante una aplicación de token de software 67

Configuración de la autenticación para endpoints strongSwan Ubuntu y CentOS 72
- Habilitación de la autenticación con un perfil de certificado 72
- Habilitación de la autenticación con un perfil de autenticación 74
- Habilitación de la autenticación con una autenticación en dos fases 76

Configuración de GlobalProtect para facilitar las notificaciones de autenticación multifactor 79
Habilitación de envío de VSA a un servidor RADIUS 82
Habilitación de la asignación de grupo 83

Puertas de enlace de GlobalProtect....87
Descripción general de puertas de enlace de GlobalProtect....89
Conceptos de puertas de enlace de GlobalProtect....90
Tipos de puertas de enlace....90
Prioridad de la puerta de enlace en una configuración de varias puertas de enlace....90
Soporte MIB de GlobalProtect....92
Tareas de requisito previo para la configuración de la puerta de enlace de GlobalProtect....93
Configuración de una puerta de enlace de GlobalProtect....94
Tráfico de división de túnel (Split Tunnel) en puertas de enlace de GlobalProtect....106
Configuración de división de túnel (Split Tunnel) basada en la ruta de acceso....106
Configure de una división de túnel (Split Tunnel) basada en el dominio y la aplicación....110
Exclusión de tráfico de vídeo del túnel VPN de GlobalProtect....111

Portales de GlobalProtect....115
Descripción general del portal de GlobalProtect....117
Tareas de requisito previo para la configuración del portal de GlobalProtect....118
Configuración del acceso al portal de GlobalProtect....119
Definición de las configuraciones de autenticación de cliente de GlobalProtect....122
Definición de las configuraciones de agente de GlobalProtect....124
Personalización de la aplicación de GlobalProtect....131
Personalización de las páginas de inicio de sesión, bienvenida y ayuda del portal de GlobalProtect....148

Aplicaciones de GlobalProtect....157
Implementación de la aplicación de GlobalProtect para usuarios finales....159
Descarga de la aplicación de GlobalProtect....161
Alojamiento de actualizaciones de la aplicación en el portal....162
Alojamiento de actualizaciones de la aplicación en un servidor web....163
Comprobación de la instalación de la aplicación....163
Descarga e instalación de la aplicación móvil de GlobalProtect....167
Implementación de la configuración de la aplicación de forma trasparente....170
Ajustes personalizables de la aplicación....170
Implementación de los ajustes de la aplicación para los endpoints de Windows....180
Implementación de los ajustes de la aplicación para los endpoints de macOS....192

VPN sin cliente de GlobalProtect....195
Descripción general de VPN sin cliente....197
Tecnologías compatibles....199
Configuración de VPN sin cliente....201
Solución de problemas de VPN sin cliente....208

Gestión de dispositivos móviles....213
Descripción general de la gestión de dispositivos móviles....215
Configuración de la integración de MDM con GlobalProtect....218
Gestión de la aplicación de GlobalProtect con proveedores de MDM aptos....218
Gestión de la aplicación de GlobalProtect con MDM externo....309

GlobalProtect para dispositivos IoT....317
Requisitos de GlobalProtect para IoT....319
Configuración de los portales y puertas de enlace de GlobalProtect para dispositivos IoT....320
Instalación de GlobalProtect para IoT en Android....324
Instalación de GlobalProtect para IoT en Raspbian....327
Instalación de GlobalProtect para IoT en Ubuntu....329
Instalación de GlobalProtect para IoT en Windows....331
Descarga e instalación el archivo MSIEXEC en el dispositivo IoT....331
Modificación de las claves de registro en el dispositivo IoT (On-Demand (Bajo demanda) o Always On (Siempre activado))....331
Modificación de las claves de registro en el dispositivo IoT (siempre activado, anterior al inicio de sesión)....332

Información de host....335
Acerca de la información del host....337
¿Qué datos recopila la aplicación de GlobalProtect?....337
¿Qué datos recopila la aplicación de GlobalProtect en cada sistema operativo?....340
Cómo usa la puerta de enlace la información del host para aplicar las políticas....349
¿Cómo pueden saber los usuarios si sus sistemas cumplen los requisitos?....349
¿Cómo puedo consultar el estado de los endpoints?....350
Configuración de la aplicación de políticas basadas en HIP....351
Recopilación de datos de procesos y aplicaciones de endpoints....360
Redistribución de informes de HIP....367
Bloqueo del acceso al endpoint....369
Configurar el agente de User-ID de Windows para recopilar información de host....371
Resumen de la integración de MDM....371
Información recopilada....371
Requisitos del sistema....373
Configuración de GlobalProtect para recuperar información del host....373
Solucionar problemas del servicio de integración de MDM....377
Dispositivos en cuarentena que utilizan información del host....378
Descripción general de la identificación y cuarentena de dispositivos en riesgo y requisitos de licencia....378
Visualización de información del dispositivo en cuarentena....379
Adición y eliminación de dispositivos manualmente de la lista de cuarentena....380
Cuarentena automática para un dispositivo....382
Uso de políticas de seguridad y de GlobalProtect para bloquear el acceso a los dispositivos en cuarentena....385
Redistribución de la información de cuarentena del dispositivo desde Panorama....386

Certificaciones....391
Habilitación y verificación del modo FIPS-CC....393
Habilitación y verificación del modo FIPS-CC con el registro de Windows....393
Habilitación y verificación del modo FIPS-CC con la lista de propiedades de macOS....396
Funciones de seguridad de FIPS-CC....400
Solución de problemas del modo FIPS-CC....401
Consulta y recopilación de logs de GlobalProtect....401
Solución de problemas del modo FIPS-CC....402

Configuraciones rápidas de GlobalProtect....405
VPN de acceso remoto (Perfil de autenticación)....407
VPN de acceso remoto (perfil del certificado)....411
VPN de acceso remoto con autenticación en dos fases....414
Configuración de VPN siempre activada....419
VPN de acceso remoto con función anterior al inicio de sesión....420
Configuración de varias puertas de enlace de GlobalProtect....426
GlobalProtect para comprobación de HIP interna y acceso basado en usuario....430
Configuración de puerta de enlace externa e interna combinada....435
Portal cautivo y uso obligatorio de GlobalProtect para acceder a la red....441

Arquitectura de GlobalProtect....445
Topología de la arquitectura de referencia de GlobalProtect....447
Portal GlobalProtect....447
Puertas de enlace de GlobalProtect....447
Características de la arquitectura de referencia de GlobalProtect....449
Experiencia del usuario final....449
Gestión y registro....449
Control y alta disponibilidad....450
Configuraciones de la arquitectura de referencia de GlobalProtect....451
Configuración de puerta de enlace....451
Configuración portal....451
Configuraciones de política....451

Criptografía de GlobalProtect....453
Acerca de la selección de cifrado de GlobalProtect....455
Intercambio de cifrado entre la puerta de enlace y la aplicación de GlobalProtect....456
Referencias de criptografía de GlobalProtect....458
Referencia: Funciones criptográficas de la aplicación de GlobalProtect....458
Conjuntos de cifrados TLS compatibles con las aplicaciones de GlobalProtect....459
Cifrados utilizados para configurar túneles de IPsec....465
API para SSL....466

Descripción general de GlobalProtect

Así consulten el correo electrónico desde su casa o actualicen documentos corporativos desde un aeropuerto, la mayoría de los empleados actuales trabajan fuera de los límites corporativos físicos. Esta movilidad de recursos aumenta la productividad y flexibilidad mientras que introduce importantes riesgos de seguridad al mismo tiempo. Cada vez que los usuarios abandonan el edificio con sus ordenadores portátiles o teléfonos inteligentes, anulan el cortafuegos corporativo y las políticas asociadas que están diseñadas para proteger al usuario y a la red. GlobalProtect™ resuelve los retos planteados por los usuarios itinerantes al extder las mismas políticas de última generación basadas en cortafuegos que se aplican a todos los usuarios dentro del perímetro físico de la empresa, independientemente de su ubicación.

Las siguientes secciones brindan información conceptual sobre lo que ofrece GlobalProtect de Palo Alto Networks y describen los componentes y diferentes situaciones de implementación de GlobalProtect:

> Acerca de los componentes de GlobalProtect
> ¿Qué versiones de sistema operativo admite GlobalProtect?
> ¿Qué funciones admite GlobalProtect?
> Acerca de las licencias de GlobalProtect

© 2020 Palo Alto Networks, Inc.

Acerca de los componentes de GlobalProtect

GlobalProtect ofrece una infraestructura completa para la gestión de su fuerza de trabajo itinerante a fin de garantizar a todos sus usuarios un acceso seguro, independientemente de los endpoints que usen o de donde se encuentren. Esta infraestructura incluye los siguientes componentes:

- Portal GlobalProtect
- Puertas de enlace de GlobalProtect
- Aplicación de GlobalProtect

Portal GlobalProtect

El portal de GlobalProtect proporciona las funciones de gestión para su infraestructura de GlobalProtect. Todos los endpoints que participan en la red de GlobalProtect reciben información de configuración desde el portal, incluida la información sobre las puertas de enlace disponibles, así como certificados cliente que pueden ser necesarios para conectarse a las puertas de enlace de GlobalProtect. Además, el portal controla el comportamiento y la distribución del software de la aplicación de GlobalProtect para los endpoints de macOS y Windows (en endpoints móviles, la aplicación de GlobalProtect se distribuye mediante la App Store de Apple para endpoints de iOS, Google Play para endpoints de Android y Chromebooks, y Microsoft Store para endpoints de Windows 10 UWP). Si usa la función del Perfil de información del host (Host Information Profile, HIP), el portal también define qué información se recopila desde el host, incluida la información personalizada que necesite. Puede configurar el acceso al portal de GlobalProtect en la interfaz de cualquier cortafuegos de última generación de Palo Alto Networks.

Puertas de enlace de GlobalProtect

Las puertas de enlace de GlobalProtect permiten aplicar la seguridad al tráfico de aplicaciones de GlobalProtect. Además, si la función de HIP está habilitada, la puerta de enlace genera un informe de HIP a partir de los datos sin procesar del host que envían las aplicaciones y puede usar esta información para la aplicación de políticas. Puede configurar diferentes Tipos de puertas de enlace para proporcionar seguridad y/o acceso a la red privada virtual (VPN) para sus usuarios remotos, o para aplicar una política de seguridad para acceder a los recursos internos.

Puede configurar una puerta de enlace de GlobalProtect en la interfaz de cualquier cortafuegos de última generación de Palo Alto Networks. Puede ejecutar tanto una puerta de enlace como un portal en el mismo cortafuegos, o puede tener varias puertas de enlace distribuidas en toda la empresa.

Aplicación de GlobalProtect

El software de la aplicación de GlobalProtect se ejecuta en endpoints y habilita el acceso a sus recursos de red mediante los portales y puertas de enlace de GlobalProtect que implementó.

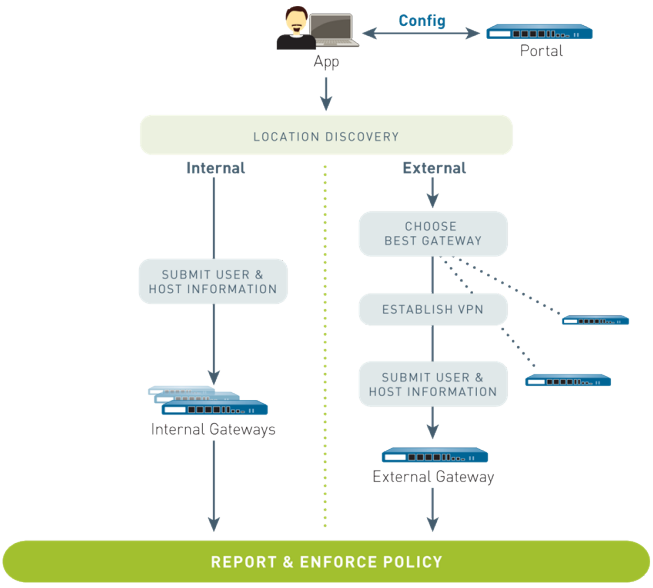
La aplicación de GlobalProtect para los endpoints de Windows y macOS se implementa desde el portal de GlobalProtect. Su comportamiento (por ejemplo, qué pestañas pueden ver los usuarios) se especifica en la configuración de clientes que defina en el portal. Consulte Definición de las configuraciones del agente de GlobalProtect, Personalización de la aplicación de GlobalProtect e Implementación del software de la aplicación de GlobalProtect para obtener más detalles.

La aplicación de GlobalProtect para endpoints móviles (iOS, Android y Windows UWP) está disponible a través de la tienda oficial del endpoint: App Store de Apple para iOS, Google Play para Android y Microsoft Store para Windows UWP. De manera alternativa, puede implementar la aplicación móvil de GlobalProtect con AirWatch, que es un sistema de gestión de endpoint móviles de terceros.

Consulte ¿Qué versiones de sistema operativo admite GlobalProtect? para obtener más detalles.

© 2020 Palo Alto Networks, Inc.

El siguiente diagrama ilustra el modo en que los portales, puertas de enlace y aplicaciones de GlobalProtect se coordinan para ofrecer a todos sus usuarios un acceso seguro, independientemente de los endpoints que usen o de donde se encuentren.



© 2020 Palo Alto Networks, Inc.

¿Qué versiones de sistema operativo admite GlobalProtect?

La aplicación de GlobalProtect se admite en ordenadores comunes, ordenadores portátiles, tabletas y teléfonos inteligentes. Le recomendamos que configure GlobalProtect en cortafuegos que ejecuten PAN-OS 6.1 o versiones posteriores y que los usuarios finales instalen solo versiones compatibles de la aplicación de GlobalProtect en sus endpoints. La versión mínima de la aplicación de GlobalProtect varía según el sistema operativo; para determinar la versión mínima de la aplicación de GlobalProtect para un sistema operativo específico, consulte los siguientes temas en la Matriz de compatibilidad de Palo Alto Networks®:

- ¿Dónde puedo instalar la aplicación de GlobalProtect?
- ¿Qué clientes IPSec de autenticación extendida (X-Auth) son compatibles?

Las versiones anteriores de la aplicación de GlobalProtect aún son compatibles con los sistemas operativos y las versiones de PAN-OS con las que se lanzaron. Para conocer la compatibilidad de la versión mínima de PAN-OS, consulte las notas de la versión de la aplicación de GlobalProtect correspondientes a la versión específica en el sitio de Actualizaciones de software.

© 2020 Palo Alto Networks, Inc.

Acerca de las licencias de GlobalProtect

Si desea usar GlobalProtect para proporcionar una solución segura de red privada virtual (virtual private network, VPN) o de acceso remoto a través de una o varias puertas de enlace externas, no necesita licencia de GlobalProtect. Sin embargo, para usar algunas de las características más avanzadas (tales como las comprobaciones de HIP y las actualizaciones de contenido asociadas, soporte para la aplicación móvil de GlobalProtect o soporte IPv6) debe comprar una suscripción anual de GlobalProtect. Esta licencia debe instalarse en cada cortafuegos que contenga puertas de enlace que:

- Realicen comprobaciones HIP
- Admitan la aplicación de GlobalProtect para los endpoints móviles
- Admitan la aplicación de GlobalProtect para los endpoints de Linux
- Admitan la aplicación de GlobalProtect para los endpoints de IoT.
- Proporciona conexiones IPv6
- Dividan el tráfico de los túneles sobre la base del dominio de destino, el nombre de proceso de la aplicación o la aplicación de transmisión de vídeo HTTP/HTTPS.
- Admitan añadir un dispositivo en riesgo a la lista de cuarentena.
- Admitan la identificación de dispositivos gestionados mediante el número de serie del endpoint en las puertas de enlace

Para la VPN sin cliente de GlobalProtect, también debe instalar una suscripción de GlobalProtect en el cortafuegos que aloje la VPN sin cliente del portal de GlobalProtect. También necesita las actualizaciones dinámicas de **GlobalProtect Clientless VPN (VPN sin cliente de GlobalProtect)** para usar esta función.

Función:	¿Requiere suscripción?
Una puerta de enlace externa (Windows y macOS)	—
Una o varias puertas de enlace internas	—
Varias puertas de enlace externas	—
Dispositivos de Internet de las cosas (Internet of Things, IoT)	✓
Comprobaciones HIP	✓
Identificación de dispositivos administrados mediante el número de serie del punto final en las puertas de enlace	✓
Aplicación de políticas basadas en HIP según el estado del endpoint	✓
Aplicación para los endpoints que ejecutan Windows o macOS	—
Aplicación móvil para los endpoints que ejecutan iOS, Android, Chrome OS y Windows 10 UWP	✓
Aplicación para los endpoints que ejecutan Linux	✓
Aplicación para los endpoints que ejecutan IoT	✓

© 2020 Palo Alto Networks, Inc.

Función:	¿Requiere suscripción?
IPv6 para puertas de enlace externas	✓
IPv6 para puertas de enlace internas (Cambio al comportamiento predeterminado. A partir de la versión de aplicación GlobalProtect 4.1.3. No se requiere una suscripción a GlobalProtect para este caso de uso)	—
VPN sin cliente	✓
Túneles divididos sobre la base del dominio de destino, proceso de cliente y aplicación de transmisión de vídeo	✓
DNS dividido	✓
Adición de un dispositivo en riesgo a la lista de cuarentena	✓

Consulte Activación de licencias para obtener información sobre la instalación de licencias en el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Comenzar

Para que GlobalProtect™ se ejecute, debe configurar la infraestructura que permite que todos los componentes se comuniquen. Básicamente, esto implica configurar las interfaces y zonas que a las que se conectarán los usuarios finales de GlobalProtect para acceder al portal y las puertas de enlace en la red. Puesto que los componentes de GlobalProtect se comunican a través de canales seguros, debe adquirir e implementar los certificados SSL necesarios de los distintos componentes. Las siguientes secciones brindan una guía de la configuración de la infraestructura de GlobalProtect:

> Creación de interfaces y zonas para GlobalProtect
> Habilitación de SSL entre componentes de GlobalProtect

© 2020 Palo Alto Networks, Inc.

Creación de interfaces y zonas para GlobalProtect

Debe configurar las siguientes interfaces y zonas para la infraestructura de GlobalProtect:

- **GlobalProtect portal (Portal de GlobalProtect)**: requiere una interfaz de bucle invertido o capa 3 para la conexión de las aplicaciones de GlobalProtect. Si el portal y el gateway se encuentran en el mismo cortafuegos, pueden usar la misma interfaz. El portal debe estar en una zona que se pueda acceder desde afuera de su red, como DMZ.
- **Puertas de enlace de GlobalProtect**: los requisitos de interfaz y zona para la puerta de enlace dependen de si la puerta de enlace que configura es externa o interna, como se indica a continuación:
  - **External gateways (Puertas de enlace externas)**: requieren una interfaz de bucle invertido o capa 3 y una interfaz de túnel lógica para que la aplicación establezca una conexión. La interfaz de bucle invertido o capa 3 debe estar en una zona externa, como DMZ. Una interfaz de túnel puede estar en la misma zona que la interfaz que se conecta a su recursos internos (por ejemplo, **`trust`**). Para mayor seguridad y mejor visibilidad, puede crear una zona separada, tal como **`corp-vpn`**. Si crea una zona separada para su interfaz de túnel, debe crear políticas de seguridad que habiliten el flujo del tráfico entre la zona VPN y la zona fiable.
  - **Puertas de enlace internas**: Requiere una interfaz de bucle o de capa 3 en su zona fiable. También puede crear una interfaz de túnel para acceder a sus puertas de enlace internas, pero no es necesario.

Para encontrar consejos sobre cómo usar una interfaz de bucle invertido para proporcionar acceso a GlobalProtect a través de diferentes puertos y direcciones, consulte ¿Se puede configurar la página del portal de GlobalProtect para acceder a ella desde cualquier puerto?

Si desea más información sobre portales y puertas de enlace, consulte Acerca de los componentes de GlobalProtect.

STEP 1 | Configure una interfaz de capa 3 para cada portal o puerta de enlace que planea implementar.

Si la puerta de enlace y el portal se encuentran en el mismo cortafuegos, puede usar una sola interfaz para ambos.

Se recomienda usar direcciones IP estáticas para el portal y la puerta de enlace.

No vincule un perfil de gestión de interfaces que permita HTTP, HTTPS, Telnet o SSH en las interfaces donde haya configurado un portal o una puerta de enlace de GlobalProtect, ya que franquearía el acceso a la interfaz de gestión desde internet. Siga las recomendaciones de las Prácticas recomendadas para proteger el acceso administrativo *para garantizar la seguridad del acceso administrativo a sus cortafuegos, de forma que evitará ataques efectivos.*

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** o **Network (Red)** > **Interfaces (Interfaces)** > **Loopback (Bucle invertido)** y, luego, seleccione la interfaz que desea configurar para GlobalProtect. En este ejemplo, configuramos **`ethernet1/1`** como la interfaz del portal.
2. (Solo para Ethernet) Configure **Interface Type (Tipo de interfaz)** en **Layer3 (Capa 3)**.
3. En la pestaña **Config (Configuración)**, seleccione la **Security Zone (Zona de seguridad)** a la cual pertenece la interfaz del portal o la puerta de enlace, de la siguiente manera:

© 2020 Palo Alto Networks, Inc.

- Coloque los portales y las puertas de enlace externas en una zona no fiable para acceder mediante hosts desde fuera de su red, como **`l3-untrust`**.
- Coloque puertas de enlace internas en una zona interna, como **`l3-trust`**.
- Si todavía no creó la zona, añada una **New Zone (Zona nueva)**. En el cuadro de diálogo Zona, defina un **Name (Nombre)** para una nueva zona y, a continuación, haga clic en **OK (Aceptar)**.

4. Seleccione el **Virtual Router (Enrutador virtual)** predeterminado.
5. Asigne una dirección IP a la interfaz:
   - Para una dirección IPv4, seleccione **IPv4** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 203.0.11.100/24.
   - Para una dirección IPv6, seleccione **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 2001:1890:12f2:11::10.1.8.160/80.
6. Haga clic en **OK (Aceptar)** para guardar la configuración de interfaz.

STEP 2 | En los cortafuegos que alojen las puertas de enlace de GlobalProtect, configure la interfaz de túnel lógica que finalizará los túneles VPN establecidos por las aplicaciones de GlobalProtect.

No se requieren direcciones IP en la interfaz de túnel a menos que requiera enrutamiento dinámico. Además, asignar una dirección IP a la interfaz de túnel puede resultar útil para solucionar problemas de conexión.

Asegúrese de habilitar User-ID en la zona donde finalizan los túneles VPN.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir una interfaz de túnel.
2. En el campo **Interfaz Name (Nombre de interfaz)**, especifique un sufijo numérico, como **`.2`**.
3. En la pestaña **Config (Configuración)**, seleccione la **Security Zone (Zona de seguridad)** para la finalización del túnel VPN, de la siguiente manera:
   - Para usar una zona fiable como punto de finalización del túnel, seleccione la zona en el menú desplegable.
   - (Recomendado) Para crear una zona separada para la finalización del túnel VPN, añada una **New Zone (Zona nueva)**. En el diálogo Zone (Zona), defina un **Name (Nombre)** para la zona nueva (por ejemplo, **`corp-vpn`**), haga clic en **Enable User Identification (Habilitar la identificación del usuario)** y en **OK (Aceptar)**.
4. Configure el **Virtual Router (Enrutador virtual)** en **None (Ninguno)**.
5. Asigne una dirección IP a la interfaz:
   - Para una dirección IPv4, seleccione **IPv4** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 203.0.11.100/24.
   - Para una dirección IPv6, seleccione **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 2001:1890:12f2:11::10.1.8.160/80.
6. Haga clic en **OK (Aceptar)** para guardar la configuración de interfaz.

STEP 3 | Si ha creado una zona separada para la finalización del túnel de las conexiones VPN, cree una política de seguridad para habilitar el flujo de tráfico entre la zona VPN y su zona fiable.

Por ejemplo, la siguiente regla de política habilita el tráfico entre la zona **`corp-vpn`** y la zona **`l3-trust`**.

© 2020 Palo Alto Networks, Inc.

	Name	Tags	Source				Destination		Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address			
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

© 2020 Palo Alto Networks, Inc.

Habilitación de SSL entre componentes de GlobalProtect

Toda la interacción entre los componentes de GlobalProtect se realiza a través de una conexión SSL/TLS. Por lo tanto, debe generar o instalar los certificados necesarios antes de configurar cada componente, de modo que pueda hacer referencia a los certificados adecuados en las configuraciones. En las siguientes secciones se describen los métodos compatibles de implementación de certificados, las descripciones y las directrices de recomendaciones para los diversos certificados de GlobalProtect, además de ofrecer instrucciones para la generación e implementación de los certificados necesarios:

- Acerca de la implementación de certificados GlobalProtect
- Recomendaciones para certificados de GlobalProtect
- Implementación de certificados de servidores en los componentes de GlobalProtect

Acerca de la implementación de certificados GlobalProtect

Existen tres métodos básicos para implementar certificados de servidor para los componentes de GlobalProtect:

- (Recomendado) **Combinación de certificados de terceros y certificados autofirmados**: dado que la aplicación de GlobalProtect accederá al portal antes de la configuración de GlobalProtect, esta debe confiar en el certificado para establecer una conexión HTTPS.
- **Entidad de certificación empresarial**: si ya cuenta con su propia CA empresarial, puede usar esta CA interna para emitir certificados de cada uno de los componentes de GlobalProtect y, a continuación, importarlos a los cortafuegos donde se alojan su portal y su(s) puerta(s) de enlace. En este caso, también debe asegurarse de que los endpoints confíen en el certificado de CA raíz que se usa para emitir los certificados de los servicios de GlobalProtect a los que deben conectarse.
- **Certificados autofirmados**: Puede generar un certificado de CA autofirmado en el portal y usarlo para emitir certificados de todos los componentes de GlobalProtect. Sin embargo, esta solución es menos segura que otras opciones y, por lo tanto, no se recomienda. Si aun así elige esta opción, los usuarios finales verán un error de certificado la primera vez que se conecten al portal. Para evitarlo, puede implementar el certificado de CA raíz autofirmado en todos los endpoints de forma manual o usar un tipo de implementación centralizada, como un Objeto de directiva de grupo (Group Policy Object, GPO) de Active Directory.

Recomendaciones para certificados de GlobalProtect

En la siguiente tabla se resumen los certificados SSL/TLS que necesitará, dependiendo de las funciones que pretenda usar:

Certificado	Uso	Proceso de emisión / Recomendaciones
Certificado de CA	Usado para firmar certificados emitidos para los componentes de GlobalProtect.	Si piensa usar certificados autofirmados, genere un certificado de CA con su servidor de CA dedicado o el cortafuegos de Palo Alto Networks y, a continuación, emita certificados de portal y puerta de enlace de GlobalProtect firmados por la CA o una CA intermedia.

© 2020 Palo Alto Networks, Inc.

Certificado	Uso	Proceso de emisión / Recomendaciones
Certificado de servidor del portal	Habilita las aplicaciones de GlobalProtect para establecer una conexión HTTPS con el portal.	• Este certificado está identificado con un perfil de servicio SSL/TLS. Usted asigna el certificado del servidor del portal al seleccionar su perfil asociado en una configuración de portal. • Utilice un certificado de servidor desde una CA externa conocida. Es la opción más segura y garantiza que los endpoints de los usuarios puedan establecer una relación de confianza con el portal sin necesidad de que implemente el certificado de CA raíz. • Si no usa una CA pública reconocida, debe exportar el certificado de CA raíz que se utilizó para generar el certificado de servidor del portal en todos los endpoints que ejecutan la aplicación de GlobalProtect. La exportación de este certificado evita que los usuarios finales vean las advertencias de certificados durante el inicio de sesión inicial en el portal. • Los campos de nombre común (Common Name, CN) y de nombre alternativo del asunto (Subject Alternative Name, SAN) del certificado deben coincidir exactamente con la dirección IP o con el FQDN de la interfaz donde está alojado el portal. • En general, cada portal debe tener su propio certificado de servidor. Sin embargo, si implementa una puerta de enlace y un portal únicos en la misma interfaz, debe usar el mismo certificado para ambos. • Si configura una puerta de enlace y un portal en la misma interfaz, también recomendamos que use el mismo perfil de certificado y perfil de servicio SSL/TLS para la puerta de enlace y el portal. Si no utilizan el mismo perfil de certificado y perfil de servicio SSL/TLS, la configuración de la puerta de enlace tendrá prioridad sobre la configuración del portal durante el protocolo de enlace SSL.
Certificado de servidor de la puerta de enlace	Habilita las aplicaciones de GlobalProtect para establecer una conexión HTTPS con la puerta de enlace.	• Este certificado está identificado con un perfil de servicio SSL/TLS. Asigne el certificado del servidor de la puerta de enlace cuando seleccione el perfil asociado en una configuración de puerta de enlace. • Genere un certificado de CA en el cortafuegos o servidor de CA, y utilice ese certificado de CA para generar todos los certificados de puertas de enlace. • Los campos de CN y de SAN del certificado deben coincidir con el FQDN o la dirección IP de la interfaz donde pretende configurar la puerta de enlace. • El portal puede distribuir el certificado de CA raíz de la puerta de enlace a la aplicación de

© 2020 Palo Alto Networks, Inc.

Certificado	Uso	Proceso de emisión / Recomendaciones
		GlobalProtect según la configuración (lista de CA raíz de confianza en la pestaña Agent (Agente) de la configuración del portal). Sin embargo, no es obligatorio que el certificado de CA raíz de la puerta de enlace se preinstale en el almacén de certificados de confianza del usuario o que una CA pública emita el certificado de puerta de enlace. • En general, cada puerta de enlace debe tener su propio certificado de servidor. Sin embargo, si implementa una puerta de enlace y un portal únicos en la misma interfaz para el acceso de VPN, debe usar un certificado de servidor único para ambos componentes. Lo recomendado es usar un certificado firmado por una CA pública. • Si configura una puerta de enlace y un portal en la misma interfaz, también recomendamos que use el mismo perfil de certificado y perfil de servicio SSL/TLS para la puerta de enlace y el portal. Si no utilizan el mismo perfil de certificado y perfil de servicio SSL/TLS, la configuración de la puerta de enlace tendrá prioridad sobre la configuración del portal durante el protocolo de enlace SSL.

(Opcional) Certificado de cliente	Se utiliza para habilitar la autenticación mutua cuando se establece una sesión HTTPS entre el portal y las puertas de enlace y las aplicaciones de GlobalProtect. Esto garantiza que solo los endpoints con certificados de cliente válidos puedan autenticarse y conectarse a la red.	• Para simplificar la implementación de certificados de clientes, configure el portal para que implemente el certificado de cliente a las aplicaciones luego del inicio de sesión correcto mediante uno de los siguientes métodos.
		  • Use un certificado de cliente único en todas las aplicaciones de GlobalProtect que reciban la misma configuración. Asigne el certificado del cliente **Local** mediante la carga del certificado al portal y, luego, selecciónelo en una configuración de agente del portal.
		  • Use el protocolo de inscripción de certificados simple (**SCEP**) para permitir que el portal de GlobalProtect implemente certificados de cliente únicos en las aplicaciones de GlobalProtect. Habilítelo mediante la configuración del perfil de SCEP y, luego, seleccione ese perfil en una configuración de agente del portal.
		• Cuando genere certificados de cliente para los terminales de GlobalProtect, use uno de estos siguientes algoritmos de resumen: SHA1, SHA256, SHA384 o SHA512.
		• Puede usar otros mecanismos para implementar certificados de cliente únicos para cada endpoint cuando se autentica el usuario final.
		• Tal vez deba probar su configuración primero sin el certificado de cliente y, a continuación, añadir el certificado del cliente cuando esté seguro de

© 2020 Palo Alto Networks, Inc.

Certificado	Uso	Proceso de emisión / Recomendaciones
		que el resto de ajustes de la configuración son correctos.
(Opcional) Certificado de máquina	Un certificado de máquina es un certificado de cliente que se emite a un endpoint reside en la tienda de máquinas local o en el llavero del sistema. Cada certificado de equipo identifica el endpoint en el campo del asunto (por ejemplo, CN=laptop1.example.com) en lugar de un usuario. El certificado garantiza que solo los endpoints confiables puedan conectarse a las puertas de enlace o al portal. Los certificados de equipo son necesarios para los usuarios configurados con el método de conexión de inicio de sesión previo.	• Cuando genere certificados de cliente para los terminales de GlobalProtect, use uno de estos siguientes algoritmos de resumen: SHA1, SHA256, SHA384 o SHA512. • Si planifica usar la función de inicio de sesión previo, use su propia infraestructura de PKI para implementar certificados en cada endpoint antes de habilitar el acceso a GlobalProtect. Este enfoque es importante para garantizar la seguridad. Para obtener más información, consulte VPN de acceso remoto con inicio de sesión previo.

Tabla: Requisitos de certificados para GlobalProtect

Si desea información detallada sobre los tipos de claves empleadas para establecer una comunicación segura entre el endpoint de GlobalProtect y los portales y puertas de enlace, consulte Referencia: Funciones criptográficas de la aplicación de GlobalProtect.

Implementación de certificados de servidores en los componentes de GlobalProtect

La siguiente tabla muestra los pasos recomendados para implementar certificados SSL/TLS en los componentes de GlobalProtect:

- Importe un certificado de servidor desde una CA externa conocida.

Use un certificado de servidor de una CA externa conocida para el portal de GlobalProtect. Esta práctica garantiza que los usuarios finales puedan establecer una conexión HTTPS sin ver advertencias sobre certificados no confiables.

El campo de nombre común (Common Name, CN) y, si corresponde, el campo de nombre alternativo del asunto (Subject Alternative Name, SAN) del certificado deben coincidir exactamente con el nombre de dominio completo (fully qualified domain name, FQDN) o la dirección IP de la interfaz donde planea configurar el portal o la interfaz de registro del dispositivo en el sistema de gestión de endpoints móviles externo. Admite coincidencias con comodines.

© 2020 Palo Alto Networks, Inc.

Antes de importar un certificado, asegúrese de que se pueda acceder a los archivos de clave y al certificado desde su sistema de gestión, y de que tiene la frase de contraseña para descifrar la clave privada.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)** para importar un certificado nuevo.
2. Use el tipo de certificado **Local** (predeterminado).
3. Introduzca un **Certificate Name (Nombre de certificado)**.
4. Introduzca la ruta y el nombre del **Certificate File (Archivo de certificado)** que recibió de la CA o seleccione **Browse (Examinar)** para buscar el archivo.
5. Configure el **File Format (Formato de archivo)** en **Encrypted Private Key and Certificate (PKCS12) (Certificado y clave privada cifrada [PKCS12])**.
6. Introduzca la ruta y el nombre en el archivo PKCS#12, en el campo **Key File (Archivo de clave)** o seleccione **Browse (Examinar)** para buscarlo.
7. Ingrese y vuelva a introducir la **Passphrase (Frase de contraseña)** que se usó para cifrar la clave privada.
8. Haga clic en **OK** para importar el certificado y la clave.

- Cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect.

Cree el certificado de CA raíz en el portal y úselo para emitir certificados de servidor para las puertas de enlace y, de manera opcional, clientes.

Antes de implementar certificados autofirmados, debe crear un certificado de CA raíz que firme los certificados de componentes de GlobalProtect del siguiente modo:

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Generate (Generar)** para generar un certificado nuevo.
2. Use el tipo de certificado **Local** (predeterminado).
3. Introduzca un **Certificate Name (Nombre de certificado)**, como GlobalProtect_CA. El nombre de certificado no puede contener espacios.
4. No seleccione un valor en el campo **Signed By**. Sin una selección para **Signed By (Firmado por)**, el certificado se autofirma.
5. Habilite la opción **Certificate Authority (Entidad de certificación)**.
6. Haga clic en **OK (Aceptar)** para generar el certificado.

- Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado.

Genere certificados de servidor para cada puerta de enlace que planifica implementar y, opcionalmente, para la interfaz del sistema de gestión de endpoints móviles de terceros (si esta interfaz es donde las puertas de enlace recuperan los informes HIP).

En los certificados de servidor de puerta de enlace, los valores de los campos CN y SAN deben ser idénticos. Si los valores difieren, el agente de GlobalProtect detecta la discrepancia y no confía en el certificado. Los certificados autofirmados solo contendrán un campo SAN si usted añade un atributo de Host Name (Nombre de host).

De manera alternativa, puede usar el Protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) para solicitar un certificado de servidor desde su CA empresarial.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Generate (Generar)** para generar un certificado nuevo.
2. Use el tipo de certificado **Local** (predeterminado).
3. Introduzca un **Certificate Name (Nombre de certificado)**. Este nombre no puede contener espacios.
4. Introduzca el FQDN (recomendado) o la dirección IP de la interfaz donde planea configurar la puerta de enlace en el campo **Common Name (Nombre común)**.
5. En el campo **Signed By**, seleccione el GlobalProtect_CA que ha creado.
6. En el área Certificate Attributes (Atributos del certificado), haga clic en **Add (Añadir)** y defina los atributos que identifican de manera única la puerta de enlace. Tenga en cuenta que si añade un atributo **Host Name (Nombre de host)** (que cumplimenta el campo SAN del certificado), debe coincidir con el valor que haya definido en el campo **Common Name (Nombre común)**.
7. Configure los ajustes criptográficos para el certificado del servidor, incluido el **Algorithm (Algoritmo)** de cifrado, la extensión de la clave (**Number of Bits [Cantidad de bits]**), el algoritmo de **Digest (Resumen)** y el **Expiration (Vencimiento)** (días).
8. Haga clic en **OK (Aceptar)** para generar el certificado.

- Use el protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) para solicitar un certificado de servidor de la CA de su empresa.

Configure perfiles SCEP separados para cada portal y puerta de enlace que planea implementar. Luego use el perfil SCEP específico para generar el certificado de servidor para cada componente de GlobalProtect.

En los certificados de portal y puerta de enlace, el valor del campo CN debe incluir el FQDN (recomendado) o la dirección IP de la interfaz donde planea configurar el portal y la puerta de enlace, y debe ser idéntico al campo SAN.

Para cumplir con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) de EE. UU., usted también debe habilitar la autenticación SSL mutua entre el servidor SCEP y el portal de GlobalProtect. (La operación de FIPS-CC se indica en la página de inicio de sesión del cortafuegos y en su barra de estado).

Una vez guardada la configuración, el portal intenta solicitar un certificado de CA con los ajustes del perfil SCEP. Si se obtiene el certificado, el cortafuegos que aloja el portal guarda el certificado CA y lo muestra en la lista de **Device Certificates (Certificados de dispositivos)**.

1. Configure un perfil SCEP para cada portal o puerta de enlace de GlobalProtect.
   1. Introduzca un **Name (Nombre)** que identifique el perfil SCEP y el componente en el cual implementará el certificado del servidor. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.
   2. (Opcional) Configure una **SCEP Challenge (comprobación de SCEP)**, que es un mecanismo de respuesta entre la PKI y el portal de cada solicitud de certificado. Use una contraseña **Fixed (Fija)** que obtenga del servidor SCEP o una contraseña **Dynamic (Dinámica)** en la que el cliente del portal envíe un nombre de usuario y OTP de su elección al servidor SCEP. Para una comprobación de SCEP dinámica, esto pueden ser las credenciales del administrador de PKI.
   3. Configure la **Server URL (URL de servidor)** que usa el portal para conectarse con el servidor SCEP en la PKI (por ejemplo, `http://10.200.101.1/certsrv/mscep/`).
   4. Introduzca una cadena (hasta 255 caracteres de extensión) en el campo **CA-IDENT Name (Nombre CA-IDENT)** para identificar el servidor SCEP.

© 2020 Palo Alto Networks, Inc.

5. Escriba un nombre de **Subject (Asunto)** para los certificados generados por el servidor SCEP. El asunto debe incluir una clave de nombre común (common name, CN) con el formato **`CN=<value>`**, donde **`<value>`** es el FQDN o la dirección IP del portal o la puerta de enlace.
6. Seleccione el tipo de nombre de asunto alternativo en **Subject Alternative Name Type**. Para introducir el nombre del correo electrónico en la extensión de nombre alternativo de asunto o en el asunto de un certificado, seleccione **RFC 822 Name (Nombre RFC 822)**. También puede introducir el **DNS Name (Nombre de DNS)** para usar en la evaluación de certificados o el **Uniform Resource Identifier (Identificador uniforme de recursos)** para identificar el recurso desde el cual el cliente obtendrá el certificado.
7. Configure los ajustes criptográficos adicionales, incluida la extensión de la clave (**Number of Bits [Cantidad de bits]**) y el algoritmo de **Digest (Resumen)** para la solicitud de firma del certificado.
8. Configure los usos permitidos del certificado, ya sea para firma (**Use as digital signature**) o cifrado (**Use for key encipherment**).
9. Para garantizar que el portal se conecte al servidor SCEP correcto, introduzca la huella digital de certificado CA en **CA Certificate Fingerprint**. Obtenga esta huella en el campo Thumbprint (Huella digital) de la interfaz del servidor SCEP.
10. Habilite la autenticación SSL mutua entre el servidor SCEP y el portal GlobalProtect.
11. Haga clic en **OK (Aceptar)** y luego en **Commit (Confirmar)** para aplicar la configuración.

2. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Generate (Generar)**.
3. Introduzca un **Certificate Name (Nombre de certificado)**. Este nombre no puede contener espacios.
4. Seleccione el **SCEP Profile (Perfil SCEP)** para usarlo a fin de automatizar el proceso de emisión de un certificado de servidor que esté firmado por la CA de la empresa a un portal o puerta de enlace, y luego haga clic en **OK (Aceptar)** para generar el certificado. El portal de GlobalProtect utiliza los ajustes del perfil SCEP para enviar una CSR a la PKI de la empresa.

- Asigne el certificado de servidor que importó o generó a un perfil de servicio SSL/TLS.
  1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil del servicio SSL/TLS)** y haga clic en **Add (Añadir)** para añadir un perfil de servicio SSL/TLS nuevo.
  2. Ingrese un **Name (Nombre)** para identificar el perfil y seleccione el certificado del servidor que importó o generó en **Certificate (Certificado)**.
  3. Defina el intervalo de las versiones de SSL/TLS (**Min Version** a **Max Version**) para la comunicación entre los componentes de GlobalProtect.

     La versión máx. permitida es TLSv1.2.

     Para brindar la seguridad más estricta, configure Min Version (Versión mínima) en TLSv1.2.
  4. Haga clic en **OK (Aceptar)** para guardar el perfil de servicio SSL/TLS.
  5. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

- Implemente los certificados de servidor autofirmados.

  - *Exporte los certificados de servidor autofirmados emitidos por la CA raíz al portal e impórtelos desde las puertas de enlace.*
  - *Asegúrese de emitir un único certificado de servidor para cada gateway.*
  - *Al especificar certificados autofirmados, debe distribuir el certificado de CA raíz a los clientes finales en las configuraciones de clientes del portal.*

© 2020 Palo Alto Networks, Inc.

Exporte el certificado desde el portal:

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.
2. Seleccione el certificado de la puerta de enlace que desea implementar y, luego, haga clic en **Export Certificate (Exportar certificado)**.
3. Configure el **File Format (Formato de archivo)** en **Encrypted Private Key and Certificate (PKCS12) (Certificado y clave privada cifrada [PKCS12])**.
4. Ingrese y confirme una **Passphrase (Frase de contraseña)** para cifrar la clave privada.
5. Haga clic en **OK** para descargar el archivo PKCS12 en la ubicación que desee.

Importe el certificado en la puerta de enlace:

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)** para importar el certificado.
2. Introduzca un **Certificate Name (Nombre de certificado)**.
3. Seleccione **Browse (Examinar)** para buscar y seleccionar el **Certificate File (Archivo de certificado)** que descargó en el paso anterior.
4. Configure el **File Format (Formato de archivo)** en **Encrypted Private Key and Certificate (PKCS12) (Certificado y clave privada cifrada [PKCS12])**.
5. Ingrese y confirme la **Passphrase (Frase de contraseña)** que usó para cifrar la clave privada cuando la exportó desde el portal.
6. Haga clic en **OK** para importar el certificado y la clave.
7. Haga clic en **Commit (Confirmar)** para aplicar los cambios en la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

Autenticación

El portal y la puerta de enlace de GlobalProtect™ deben autenticar a los usuarios finales para permitirles acceder a los recursos de GlobalProtect. Debe configurar los mecanismos de autenticación antes de configurar la puerta de enlace y el portal. En las siguientes secciones se detallan los mecanismos de autenticación compatibles y el modo de configurarlos:

- Acerca de la autenticación de usuarios de GlobalProtect
- Configuración de autenticación externa
- Configuración de la autenticación de certificado de cliente
- Configuración de la autenticación en dos fases
- Configuración de la autenticación para endpoints strongSwan Ubuntu y CentOS
- Configuración de GlobalProtect para facilitar las notificaciones de autenticación multifactor
- Habilitación de envío de VSA a un servidor RADIUS
- Habilitación de la asignación de grupo

© 2020 Palo Alto Networks, Inc.

Acerca de la autenticación de usuarios de GlobalProtect

La primera vez que se conecta la aplicación de GlobalProtect al portal, se solicita al usuario que se autentique en el portal. Si la autenticación es correcta, el portal de GlobalProtect envía la configuración de GlobalProtect, que incluye una lista de puertas de enlace a las que se puede conectar la aplicación y, opcionalmente, un certificado de cliente para conectarse a las puertas de enlace. Luego de descargar y almacenar en caché la configuración de manera correcta, la aplicación intentará conectarse a una de las puertas de enlace especificadas en la configuración. Puesto que estos componentes ofrecen acceso a sus recursos y configuraciones de red, también requieren la autenticación del usuario final.

El nivel apropiado de seguridad necesario en el portal y las puertas de enlace varía según la importancia de los recursos que protege la puerta de enlace. GlobalProtect proporciona un marco de autenticación flexible que le permite elegir el perfil de autenticación y el perfil de certificado apropiados para cada componente.

- Métodos de autenticación de GlobalProtect admitidos
- ¿Cómo sabe la aplicación qué credenciales proporcionar?

Métodos de autenticación de GlobalProtect admitidos

Los siguientes temas describen los métodos de autenticación compatibles con GlobalProtect y proporcionan pautas de uso para cada método.

- Autenticación local
- Autenticación externa
- Autenticación de certificación de cliente
- Autenticación de dos factores
- Autenticación multifactor para aplicaciones que no están basadas en navegador
- Inicio de sesión único

Autenticación local

Tanto las credenciales de cuenta de usuario como los mecanismos de autenticación se encuentran en el cortafuegos. Este mecanismo de autenticación no es adaptable, ya que requiere una cuenta para cada usuario final de GlobalProtect y, por lo tanto, solo se recomienda para implementaciones muy pequeñas.

Autenticación externa

Los servicios externos LDAP, Kerberos, TACACS+, SAML o RADIUS llevan a cabo las funciones de autenticación del usuario (e incluyen soporte para los mecanismos de autenticación en dos fases y basados en token, como la autenticación con Contraseña de un solo uso [one-time password, OTP]). Para habilitar la autenticación externa:

- Cree un perfil de servidor con ajustes para el acceso al servicio de autenticación externo.
- Cree un perfil de autenticación que haga referencia al perfil de servicio.
- Especifique la autenticación de cliente en el portal y las configuraciones de puerta de enlace y opcionalmente especifique el SO del endpoint que usará estos ajustes.

Puede usar diferentes perfiles de autenticación para cada componente de GlobalProtect. Consulte Configuración de autenticación externa para obtener instrucciones. Consulte VPN de acceso remoto (Perfil de autenticación) para obtener un ejemplo de configuración.

© 2020 Palo Alto Networks, Inc.

Si configura la autenticación de usuarios mediante SAML en el portal o la puerta de enlace, los usuarios que ejecutan GlobalProtect 4.1.8 o una versión anterior no pueden cerrar la sesión en dicha aplicación si deshabilita el cierre de sesión único (single logout, SLO). En cambio, sí pueden cerrarla si ejecutan GlobalProtect 4.1.9 o una versión posterior en la aplicación, tanto si habilita como si deshabilita SLO.

Si configura la autenticación de usuarios mediante Kerberos en el portal o la puerta de enlace, los usuarios no pueden cerrar la sesión en la aplicación de GlobalProtect una vez autenticados con este método.

Si no habilita la opción Save User Credentials (Guardar credenciales de usuarios) de Network (Red) > GlobalProtect > Portals (Portales) > <portal-config> > Agent (Agente) > <agent-config> > Authentication (Autenticación) en la aplicación de GlobalProtect, los usuarios no pueden cerrar la sesión en la aplicación una vez que se realiza la correcta autenticación mediante LDAP, TACACS+ o RADIUS.

Autenticación de certificación de cliente

Para mayor seguridad, puede configurar el portal o la puerta de enlace para que utilicen un certificado de cliente para obtener el nombre de usuario y autenticar al usuario antes de permitirle acceder al sistema.

- Para autenticar al usuario, uno de los campos del certificado, tal como el campo Subject Name, debe identificar el nombre de usuario.
- Para autenticar el endpoint, el campo Subject del certificado debe identificar el tipo de dispositivo en lugar del nombre de usuario. (Con los métodos de conexión de inicio de sesión previo, el portal o la puerta de enlace autentica el endpoint antes de que el usuario inicie sesión).

Si configura la autenticación de usuarios mediante certificados de cliente en el portal o la puerta de enlace, los usuarios no pueden cerrar la sesión en la aplicación de GlobalProtect una vez autenticados solo con este método.

Para un perfil de configuración de agente que especifica los certificados de cliente, cada usuario recibe un certificado de cliente. El mecanismo para brindar los certificados determina si un certificado es único para cada usuario o el mismo para todos los usuarios de esa configuración de agente:

- Para implementar certificados de cliente que son únicos para cada usuario y endpoint, use **SCEP**. La primera vez que un usuario inicia sesión, el portal solicita un certificado de la PKI de la empresa. El portal obtiene un certificado único y lo implementa en el endpoint.
- Para implementar el mismo certificado de cliente en todos los usuarios que reciben una configuración de cliente, implemente un certificado que sea local para el cortafuegos.

Use un perfil de certificado opcional para verificar el certificado del cliente que el endpoint presenta con una solicitud de conexión. El perfil de certificado especifica el contenido del nombre de usuario y los campos de dominio de usuario; enumera los certificados de CA; los criterios para bloquear una sesión; y ofrece maneras de determinar el estado de revocación de los certificados de CA. Debido a que el certificado es parte de la autenticación del endpoint o del usuario para una nueva sesión, debe implementar previamente en los endpoints los certificados utilizados en los perfiles de certificados, antes del inicio de sesión inicial de los usuarios en el portal.

El perfil del certificado especifica el campo del certificado que contiene el nombre de usuario. Si el perfil del certificado especifica Subject (Asunto) en el campo Username (Nombre de usuario), el certificado presentado por el endpoint debe contener un nombre común para que el endpoint se conecte. Si el perfil del certificado especifica Subject-Alt (Asunto alternativo) con un correo electrónico o nombre principal como el campo Username (Nombre de usuario), el certificado del endpoint debe contener los campos correspondientes, que se usarán como el nombre de usuario cuando la aplicación de GlobalProtect se autentique con el portal o la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

GlobalProtect también es compatible con la autenticación con tarjeta de acceso común (common access cards, CAC) y con tarjetas inteligentes, que se basan en un perfil del certificado. Con estar tarjetas, el perfil del certificado debe contener el certificado de CA raíz que emitió el certificado en la tarjeta inteligente o CAC.

Si especifica la autenticación del certificado del cliente, no debe configurar un certificado de cliente en la configuración del portal, ya que el endpoint lo brindará cuando se conecte el usuario. Para obtener un ejemplo de cómo configurar la autenticación del certificado de cliente, consulte VPN de acceso remoto (perfil de certificado).

Autenticación de dos factores

Con la autenticación en dos fases, el portal o la puerta de enlace utiliza dos mecanismos para autenticar usuarios, tal como una contraseña de una sola vez, además de las credenciales de inicio de sesión Active Directory (AD). Puede habilitar la autenticación en dos fases al configurar y añadir tanto un perfil de certificado como un perfil de autenticación a la configuración de portal o puerta de enlace.

Puede configurar el portal y las puertas de enlace para que utilicen los mismos métodos de autenticación o para que utilicen métodos diferentes. De cualquier manera, los usuarios deben autenticarse correctamente mediante los dos mecanismos que el componente exige antes de poder obtener acceso a los recursos de red.

Si el perfil del certificado especifica un **Username Field (Campo de nombre de usuario)** del cual GlobalProtect puede obtener un nombre de usuario, el servicio de autenticación externa utiliza automáticamente el nombre de usuario para autenticar al usuario en el servicio de autenticación especificado en el perfil de autenticación. Por ejemplo, si el **Username Field (Campo de nombre de usuario)** en el perfil del certificado se ha definido como **Subject (Asunto)**, el valor en el campo de nombre común del certificado se usará como el nombre de usuario cuando el servidor de autenticación intente autenticar al usuario. Si no quiere obligar a los usuarios a autenticarse con un nombre de usuario del certificado, asegúrese de que **Username Field (Campo de nombre de usuario)** en el perfil del certificado se definió como **None (Ninguno)** Consulte VPN de acceso remoto con autenticación en dos fases para obtener un ejemplo de configuración.

Autenticación multifactor para aplicaciones que no están basadas en navegador

(Solo en Windows y macOS) En el caso de los recursos de red confidenciales que no están basados en navegador (por ejemplo, aplicaciones financieras o aplicaciones de desarrollo de software) y que exigen autenticación adicional, la aplicación de GlobalProtect solicita al usuario que lleve a cabo la autenticación multifactor oportuna para acceder a ellos.

Inicio de sesión único

(Solo en Windows) Si habilita el inicio de sesión único (single sign-on, SSO), la aplicación de GlobalProtect emplea las credenciales de inicio de sesión en Windows del usuario para autenticarse automáticamente y conectarse al portal y a la puerta de enlace de GlobalProtect. También puede configurar la aplicación de modo que ajuste las credenciales externas para garantizar que los usuarios de Windows se puedan autenticar y conectar por medio de un proveedor externo de credenciales.

Si habilita SSO, los usuarios que ejecutan GlobalProtect 4.1.9 o una versión posterior no pueden cerrar la sesión en dicha aplicación una vez autenticados con este método.

¿Cómo sabe la aplicación qué credenciales proporcionar?

De manera predeterminada, la aplicación de GlobalProtect intenta usar las mismas credenciales de inicio de sesión para la puerta de enlace que las que se usaron en el inicio de sesión del portal. En el caso más

© 2020 Palo Alto Networks, Inc.

simple, donde la puerta de enlace y el portal usan el mismo perfil de autenticación o perfil de certificado, la aplicación se conecta a la puerta de enlace de forma transparente.

Usted también puede personalizar qué portal y puertas de enlace (internas, externas o solo manuales) de GlobalProtect requerirán diferentes credenciales (tales como OTP únicos), con una configuración basada en cada aplicación. Esto permite que el portal o la puerta de enlace de GlobalProtect solicite la OTP única sin solicitar primero las credenciales especificadas en el perfil de autenticación.

Existen dos opciones para modificar el comportamiento de la autenticación de la aplicación predeterminada de modo que sea más segura y rápida:

- Autenticación de cookies en el portal o la puerta de enlace
- Reenvío de credenciales a algunas o todas las puertas de enlace

Autenticación de cookies en el portal o la puerta de enlace

La autenticación de cookies simplifica el proceso de autenticación para usuarios finales, puesto que ya no tendrán que iniciar sesión sucesivamente tanto en el portal como en la puerta de enlace o introducir varias OTP para autenticarse en ambas. Por lo tanto, se mejora la experiencia del usuario al minimizar la cantidad de veces que los usuarios deben introducir las credenciales. Además, las cookies habilitan el uso de una contraseña temporal para volver a habilitar el acceso VPN tras la caducidad de la contraseña del usuario.

Puede configurar los ajustes de autenticación de cookies de manera independiente para el portal y para las puertas de enlace individuales (por ejemplo, puede imponer un periodo de vigencia menor para las cookies en las puertas de enlace que protegen recursos confidenciales). Una vez que el portal o las puertas de enlace implementan una cookie de autenticación en el endpoint, el portal y las puertas de enlace dependerán de la misma cookie para autenticar al usuario. Cuando la aplicación presenta la cookie, el portal o la puerta de enlace evalúan si la cookie es válida sobre la base del periodo de vigencia configurado para la cookie. Si la cookie caduca, GlobalProtect solicita automáticamente al usuario que se autentique con el portal o la puerta de enlace. Si la autenticación se realiza correctamente, el portal o la puerta de enlace emiten la cookie de autenticación de reemplazo para el endpoint y el periodo de validez comienza nuevamente.

Considere el siguiente ejemplo cuando configure el periodo de vigencia de la cookie para el portal (que no protege información confidencial) en 15 días, pero configure el periodo de vigencia de la cookie para las puertas de enlace (que sí protegen información confidencial) en 24 horas. Cuando el usuario se autentica por primera vez en el portal, el portal emite la cookie de autenticación. Si después de cinco días el usuario intenta conectarse al portal, la cookie de autenticación seguirá siendo válida. Sin embargo, si después de cinco días el usuario intenta conectarse a la puerta de enlace, la puerta de enlace evaluará el periodo de vigencia de la cookie y determinará que caducó (5 días >24 horas). Entonces el agente indicará automáticamente al usuario que se autentique con la puerta de enlace y, tras la autenticación correcta, recibirá una cookie de autenticación de reemplazo. La nueva cookie de autenticación será válida por otros 15 días en el portal y otras 24 horas en las puertas de enlace.

Para obtener un ejemplo sobre cómo usar esta opción, consulte Configuración de autenticación en dos fases.

Reenvío de credenciales a algunas o todas las puertas de enlace

Con la autenticación en dos fases, usted puede especificar el portal o los tipos de puertas de enlace (internas, externas o solo manuales) que solicitan su propio conjunto de credenciales. Esta opción acelera el proceso de autenticación cuando el portal y la puerta de enlace requieren credenciales distintas (ya se trate de OTP distintas o credenciales de inicio de sesión completamente diferentes). Para cada portal o puerta de enlace que seleccione, la aplicación no reenvía las credenciales, lo que le permite personalizar la seguridad para diferentes componentes de GlobalProtect. Por ejemplo, usted puede tener la misma seguridad en sus portales y en las puertas de enlace internas, y al mismo tiempo solicitar una OTP como segunda fase o una contraseña diferente para acceder a esas puertas de enlace que permiten llegar a los recursos más importantes.

© 2020 Palo Alto Networks, Inc.

Para obtener un ejemplo sobre cómo usar esta opción, consulte Configuración de autenticación en dos fases.

¿Cómo sabe la aplicación qué certificado proporcionar?

Cuando configura GlobalProtect para usar certificados de cliente para la autenticación en endpoints de macOS o Windows, GlobalProtect debe presentar un certificado de cliente válido para autenticarse con el portal o las puertas de enlace.

Para que un certificado de cliente sea válido, debe cumplir los requisitos siguientes:

- Debe estar emitido por la autoridad de certificación (certificate authority, CA) que definió en el perfil de certificado de las configuraciones del portal y la puerta de enlace.
- Debe especificar el propósito de la autenticación del cliente, que el administrador del certificado especifica cuando crea el certificado.
- Debe estar ubicado en el almacén de certificados, como se estableció en la configuración del agente del portal de GlobalProtect. Por defecto, la aplicación de GlobalProtect primero busca un certificado de cliente válido en el almacén del usuario. Si no existe uno, la aplicación busca en el almacén del equipo. Si la aplicación de GlobalProtect localiza un certificado en el almacén del usuario, no buscará en el almacén del equipo porque el almacén del usuario tiene prioridad. Para forzar a la aplicación de GlobalProtect a buscar certificados en solo un almacén de certificados, configure la opción **Client Certificate Store Lookup (Búsqueda del almacén de certificados de cliente)** en la configuración de agente de portal de GlobalProtect adecuada.
- El certificado coincide con objetivos adicionales especificados en la configuración de agente de portal de GlobalProtect. Para especificar un objetivo adicional, debe identificar el identificador de objeto (OID) para el certificado y configurar el valor de **Extended Key Usage OID (OID de uso de clave extendida)** en la configuración de agente de portal de GlobalProtect adecuada. Un OID es un valor numérico que identifica la aplicación o servicio para el cual se utiliza un certificado y que se adjunta automáticamente a un certificado cuando una autoridad de certificación (CA) lo crea. Para obtener más información sobre cómo especificar un OID común o personalizado, consulte Selección de certificado por OID.

Cuando solo un certificado de cliente cumple con los requisitos anteriores, la aplicación usa automáticamente ese certificado de cliente para la autenticación. Sin embargo, cuando los certificados de múltiples clientes cumplen con estos requisitos, GlobalProtect solicita al usuario que seleccione el certificado de cliente de una lista de certificados de cliente válidos en el endpoint. Si bien GlobalProtect requiere que los usuarios seleccionen el certificado de cliente solo cuando se conectan por primera vez, es posible que los usuarios no sepan qué certificado seleccionar. En este caso, le recomendamos que limite la lista de certificados de cliente disponibles por objetivo del certificado (como lo indica el OID) y el almacén de certificados. Para obtener más información sobre estos y otros ajustes que puede configurar para personalizar su aplicación, consulte Personalización del agente de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación externa

En los siguientes flujos de trabajo se describe el modo de configurar el portal y las puertas de enlace de GlobalProtect para usar un servicio de autenticación externo. Los servicios de autenticación compatibles son LDAP, Kerberos, RADIUS, SAML y TACACS+.

GlobalProtect también es compatible con la autenticación local. Para usar la autenticación local, cree una base de datos de usuario local (Device [Dispositivo] > Local User Database [Base de datos de usuario local]) que contenga los usuarios y grupos a los que desea permitirles el acceso a GlobalProtect y, luego, haga referencia a esa base de datos en el perfil de autenticación.

Para obtener más información, consulte Métodos de autenticación de GlobalProtect admitidos.

Las opciones para configurar la autenticación externa incluyen:

- Configuración de autenticación LDAP
- Configuración de autenticación SAML
- Configuración de autenticación Kerberos
- Configuración de autenticación RADIUS o TACACS+

Configuración de autenticación LDAP

Con frecuencia, las organizaciones usan LDAP como un servicio de autenticación y un repositorio central para la información de usuario. También se puede usar para almacenar la información del rol para los usuarios de aplicaciones.

STEP 1 | Cree un perfil de servidor.

El perfil de servidor identifica el servicio de autenticación externo e indica al cortafuegos cómo conectarse con dicho servicio de autenticación y acceder a las credenciales de autenticación para sus usuarios.

Cuando utiliza LDAP para conectarse a Active Directory (AD), debe crear un perfil de servidor LDAP diferente para cada dominio de AD.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **LDAP** y, luego, haga clic en **Add (Añadir)** para añadir un perfil de servidor de LDAP.
2. Introduzca un **Profile Name (Nombre de perfil)**, como `GP-User-Auth`.
3. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.
4. Haga clic en **Add (Añadir)** en el área **Server List (Lista de servidores)** y luego introduzca la información requerida para conectarse al servidor de autenticación, incluido el **Name (Nombre)**, la dirección IP o FQDN del **LDAP Server (Servidor LDAP)** y el **Port (Puerto)**.
5. Seleccione el **Type (Tipo)** de servidor LDAP.
6. Introduzca **Bind DN (DN de enlace)** y **Password (Contraseña)** para permitir que el servicio de autenticación autentique el cortafuegos.
7. (Opcional) Si desea que el endpoint use SSL o TLS para una conexión más segura con el servidor del directorio, habilite la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)** (está habilitada por defecto). El protocolo que usa el endpoint depende del puerto del servidor:
   - 389 (predeterminado): TLS (específicamente, el dispositivo usa la operación StartTLS, que actualiza la conexión de texto no cifrado inicial a TLS).

© 2020 Palo Alto Networks, Inc.

- 636—SSL
- Cualquier otro puerto: El dispositivo intenta primer usar TLS. Si el servidor de directorio no admite TLS, el dispositivo cambia a SSL.

8. (Opcional) Para mayor seguridad, habilite la opción **Verify Server Certificate for SSL sessions (Verificar el certificado del servidor para las sesiones SSL)** de modo que el endpoint verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar la verificación, debe seleccionar también la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)**. Para que la verificación se realice correctamente, el certificado debe reunir una de las siguientes condiciones:
   - Está en la lista de certificados de dispositivo: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Si es necesario, importe el certificado al dispositivo.
   - El firmante del certificado está en la lista de autoridades de certificación confiables: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Default Trusted Certificate Authorities (Autoridades de certificados de confianza por defecto)**.
9. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | (Opcional) Cree un perfil de autenticación.

El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios. En un portal o puerta de enlace, puede asignar uno o más perfiles de autenticación en uno o más perfiles de autenticación de cliente. Para obtener descripciones de la manera en que un perfil de autenticación dentro de un perfil de autenticación de usuario admite la autenticación de usuario pormenorizada, consulte Configuración de una puerta de enlace de GlobalProtect y Configuración del acceso al portal de GlobalProtect.

Para permitir que los usuarios se conecten y cambien sus contraseñas caducadas sin intervención administrativa, considere usar la VPN de acceso remoto con inicio de sesión previo.

Si la contraseña de un usuario venció, puede asignar una contraseña de LDAP temporal que permita a los usuarios iniciar sesión en GlobalProtect. En este caso, la contraseña temporal puede usarse para autenticar el portal, pero el inicio de sesión de la puerta de enlace puede fallar porque la misma contraseña temporal no puede reutilizarse. A fin de evitar este problema, habilite una cancelación de autenticación en la configuración del portal (Network [Red] > GlobalProtect > Portal) para permitir que la aplicación use una cookie para autenticarse en el portal y la contraseña temporal para autenticarse en la puerta de enlace.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y haga clic en **Add (Añadir)** para añadir un perfil nuevo.
2. Introduzca un **Name (Nombre)** para el perfil.
3. Configure el tipo de **Authentication (Autenticación)** en **Type (Tipo)** como **LDAP**.
4. Seleccione el **Server Profile (Perfil de servidor)** de la autenticación LDAP que creó en el paso 1.
5. Introduzca **sAMAccountName** como el **Login Attribute (Atributo de inicio de sesión)**.
6. Configure la **Password Expiry Warning (Advertencia de vencimiento de la contraseña)** para especificar la cantidad de días de antelación con la que se comunicará a los usuarios la caducidad de la contraseña. Por defecto, a los usuarios se les notificará siete días antes de la caducidad de la contraseña (el intervalo es de 1 a 255). Debido a que los usuarios deben cambiar la contraseña antes del final del período de vencimiento, debe proporcionar un período que sea adecuado para su base de usuarios, a fin de garantizar el acceso continuado a GlobalProtect. Para usar esta función, debe especificar uno de los siguientes tipos de servidores LDAP en su perfil de servidor LDAP: **active-directory**, **e-directory**, o **sun**.

© 2020 Palo Alto Networks, Inc.

Salvo que habilite el inicio de sesión previo, los usuarios no pueden acceder a GlobalProtect cuando se vencen sus contraseñas.

7. Especifique el **User Domain (Dominio de usuario)** y el **Username Modifier (Modificador de nombre de usuario)**. El endpoint combina los valores de **User Domain (Dominio de usuario)** y **Username Modifier (Modificador de nombre de usuario)** para modificar la cadena de dominio/nombre de usuario que introduce un usuario durante el inicio de sesión. El endpoint usa la cadena modificada para la autenticación y usa el valor de **User Domain (Dominio de usuario)** para la asignación de grupos de User-ID. La modificación de la entrada del usuario es útil cuando el servicio de autenticación requiere cadenas de dominio/nombre de usuario en un formato particular pero usted no desea depender de los usuarios para introducir correctamente el dominio. Puede seleccionar una de las siguientes opciones:
   - Para enviar solamente la información de usuario sin modificar, dejar en blanco el **User Domain (Dominio de usuario)** (predeterminado) y definir el **Username Modifier (Modificador de nombre de usuario)** con la variable **%USERINPUT%** (predeterminado).
   - Para que un dominio preceda a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina el **Username Modifier (Modificador de nombre de usuario)** como **%USERDOMAIN%\%USERINPUT%**.
   - Para anexar un dominio a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina **Username Modifier (Modificador de nombre de usuario)** como **%USERINPUT%@ %USERDOMAIN%**.

   Si Username Modifier (Modificador de nombre de usuario) incluye la variable %USERDOMAIN%, el valor de User Domain (Dominio de usuario) sustituye cualquier cadena de dominio que introduzcan los usuarios. Si el campo User Domain (Dominio de usuario) está en blanco, el dispositivo elimina toda cadena de dominio introducida por el usuario.
8. En la pestaña **Advanced (Avanzada)**, haga clic en **Add (Añadir)** para añadir una **Allow List (Lista de permitidos)** y seleccione los usuarios y grupos de usuarios que pueden autenticarse con este perfil. La opción **all (todo)** permite que todos los usuarios se autentiquen con este perfil. Por defecto, la lista no tiene entradas, lo que significa que ningún usuario puede autenticarse.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.

Configuración de autenticación SAML

El lenguaje de marcado de aserción de seguridad (Security Assertion Markup Language, SAML) es un formato de datos abierto basado en XML usado para intercambiar datos de autenticación y autorización entre partes, en particular, entre un proveedor de identidad (identity provider, IdP) y un proveedor de servicios. SAML es un producto del Comité Técnico de Servicios de Seguridad de OASIS.

STEP 1 | Cree un perfil de servidor.

El perfil de servidor identifica el servicio de autenticación externo e indica al cortafuegos cómo conectarse con dicho servicio de autenticación y acceder a las credenciales de autenticación para sus usuarios.

Los siguientes pasos describen cómo usted importa un archivo de metadatos de SAML desde el IdP, de manera que el cortafuegos pueda crear automáticamente un perfil de servidor y completar la información de conexión, registro y certificado de IdP. Si el IdP no proporciona un archivo de metadatos, seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider**

© 2020 Palo Alto Networks, Inc.

(Proveedor de identidad SAML) y luego haga clic en **Add (Añadir)** para añadir un perfil de servidor manualmente

1. Exporte el archivo de metadatos SAML desde el IdP a un endpoint que el cortafuegos pueda acceder.

   Consulte su documentación de IdP para obtener instrucciones sobre cómo exportar el archivo.
2. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)**.
3. Haga clic en **Import (Importar)** para importar el archivo de metadatos en el cortafuegos.
4. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor, como **`GP-User-Auth`**.
5. Haga clic en **Browse (Examinar)** para buscar el archivo de metadatos.
6. (Recomendado) Seleccione **Validate Identity Provider Certificate (Validar certificado de proveedor de identidad)** (valor predeterminado) para que el cortafuegos valida el certificado de IdP.

   La validación se produce después de asignar el perfil del servidor a un perfil de autenticación y haga clic en **Commit (Confirmar)** para guardar los cambios. El cortafuegos utiliza el perfil de certificado en el perfil de autenticación para validar el certificado.
7. Introduzca **Maximum Clock Skew (Desplazamiento de reloj máximo)**, que es la diferencia de tiempo permitida del sistema (en segundos) entre el IdP y el cortafuegos cuando este valida los mensajes IdP. El valor predeterminado es 60 segundos y el rango es de 1 a 900 segundos. Si la diferencia supera este valor, la autenticación falla.
8. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | (Opcional) Cree un perfil de autenticación.

El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios. En un portal o puerta de enlace, puede asignar uno o más perfiles de autenticación en uno o más perfiles de autenticación de cliente. Para obtener más información sobre cómo un perfil de autenticación dentro de un perfil de autenticación de cliente admite la autenticación de usuario granular, consulte Configuración de una puerta de enlace de GlobalProtect y Configuración del acceso al portal de GlobalProtect.

La autenticación mediante SAML admite las redes privadas virtuales (virtual private network, VPN) de acceso remoto con función anterior al inicio de sesión con la aplicación de GlobalProtect 5.0 y las versiones posteriores.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y, luego, haga clic en **Add (Añadir)** para añadir un perfil nuevo de autenticación.
2. Introduzca un **Name (Nombre)** para el perfil de autenticación.
3. Configure el tipo de **Authentication (Autenticación)** en **Type (Tipo)** como **SAML**.
4. Seleccione el **IdP Server Profile (Perfil de servidor IdP)** de SAML que creó en el paso 1.
5. Configure las siguientes opciones para permitir la autenticación de certificado entre el cortafuegos y el proveedor de identidad de SAML. Consulte Autenticación SAML 2.0 para obtener más detalles.
   - Las **Certificate for Signing Requests (Certificado para solicitudes de firma)** que el cortafuegos utiliza para firmar los mensajes que envía al IdP.
   - El **Certificate Profile (Perfil de certificado)** que el cortafuegos utiliza para validar el certificado de IdP.
6. Especifica los formatos de nombre de usuario y función de administración.
   - Especifica el **Username Attribute (Atributo de nombre de usuario)** y **User Group Attribute (Atributo del grupo de usuarios)**.

© 2020 Palo Alto Networks, Inc.

A diferencia de otros tipos de autenticación externa, el perfil de autenticación de SAML no tiene un atributo de User Domain (Dominio de usuario).

- (Opcional) Si va a utilizar este perfil para autenticar cuentas administrativas que gestiona en el almacén de identidades IdP, especifique el **Admin Role Attribute (Atributo de función de administración)** y el **Access Domain Attribute (Atributo de dominio de acceso)**.

7. En la pestaña **Advanced (Avanzada)**, haga clic en **Add (Añadir)** para añadir una **Allow List (Lista de permitidos)** y seleccione los usuarios y grupos que pueden autenticarse con este perfil. La opción **all (todo)** permite que todos los usuarios se autentiquen con este perfil. Por defecto, la lista no tiene entradas, lo que significa que ningún usuario puede autenticarse.

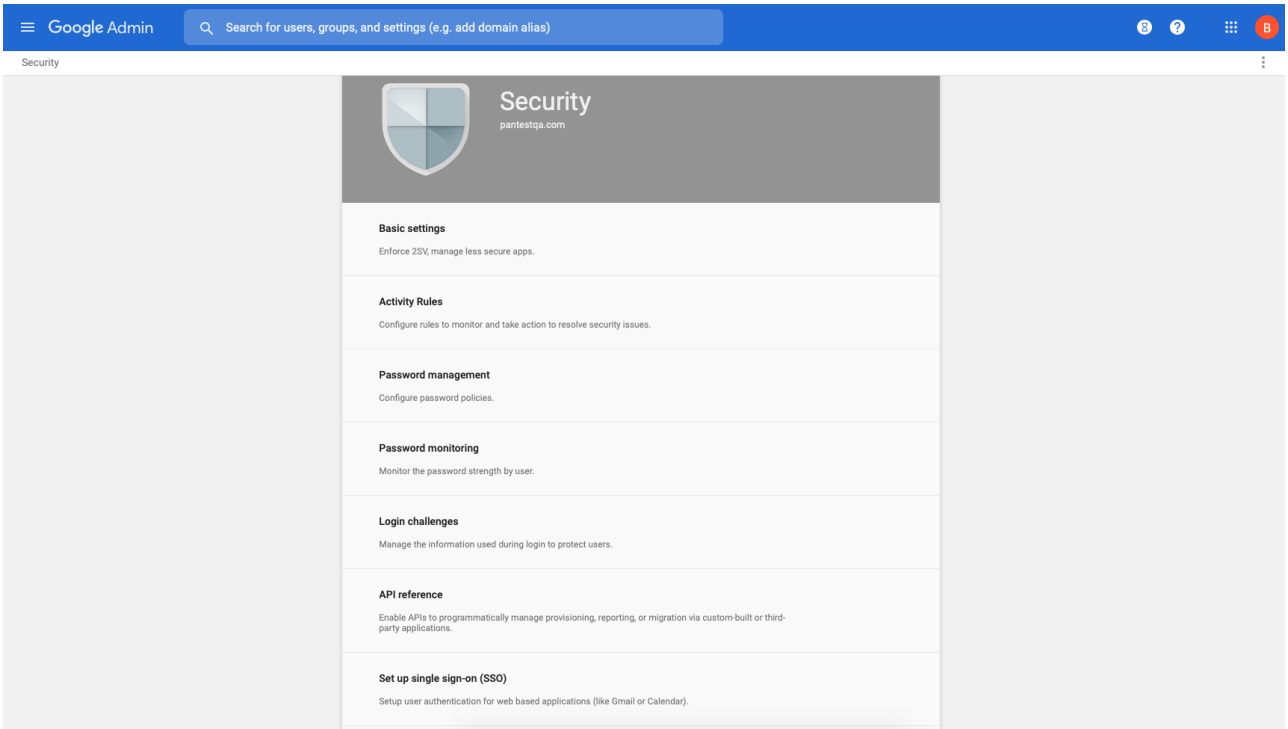
   Asegúrese de que el nombre de usuario en la **Allow List (Lista de permitidos)** coincida con el nombre de usuario devuelto por el servidor SAML IdP.
8. Haga clic en **OK (Aceptar)**.

STEP 3 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 4 | (Solo Chromebooks) Habilite el SSO SAML para Chromebooks.

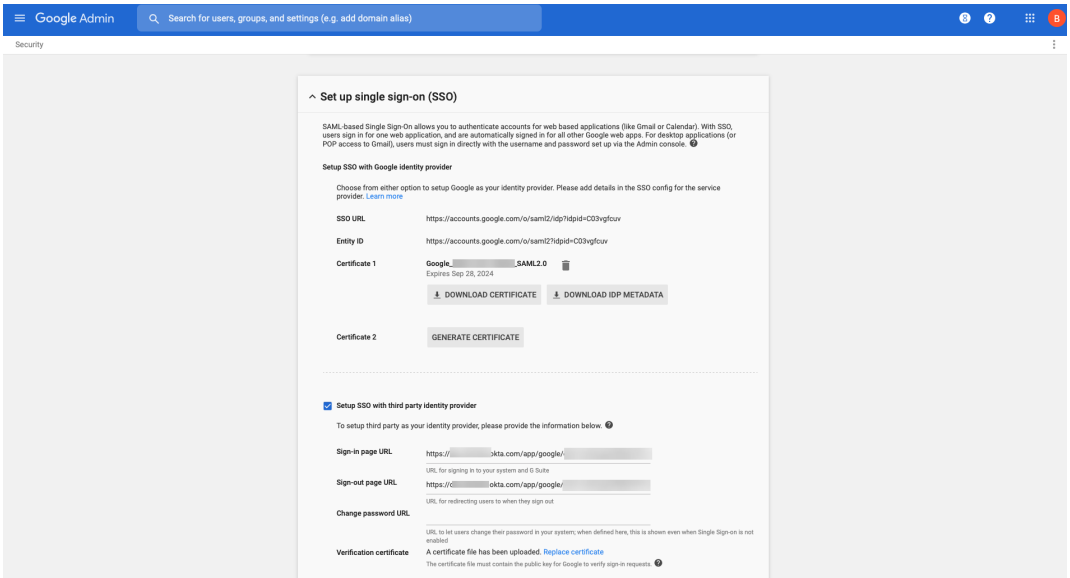
Estos pasos le permiten configurar el SSO SAML para la aplicación de GlobalProtect para Android en Chromebooks.

1. Inicie sesión en la Consola del administrador de Google y seleccione **Security (Seguridad)**.

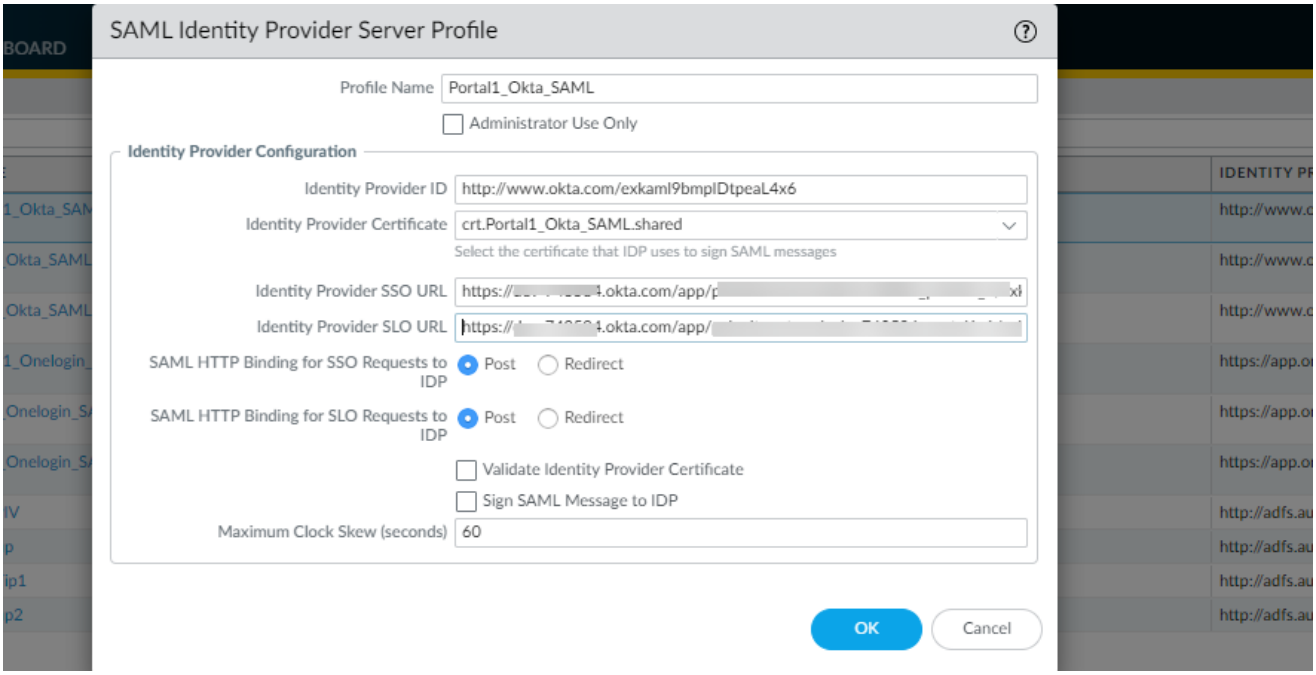


2. Seleccione **Set up single sign-on (SSO) (Configurar inicio de sesión único (SSO))**.
3. (Optcional) Si desea configurar el SSO con cualquier otro proveedor además de Google, seleccione **Setup SSO with third party identity provider (Configurar SSO con un proveedor de identidad de terceros)** y especifique la **URL de página de inicio de sesión** y la **URL de página de cierre de sesión**, y cargue un **certificado de validación** válido.

© 2020 Palo Alto Networks, Inc.



4. Configure el proveedor de identidad SAML en GlobalProtect.
   1. En la consola de GlobalProtect, seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)**.
   2. Haga que los valores que especificó para el IdP en la Consola del administrador de Google coincidan.



Uso del navegador del sistema predeterminado para la autenticación SAML

Si ha configurado el portal de GlobalProtect para autenticar los usuarios a través de la autenticación SAML, los usuarios finales pueden conectarse a la aplicación u otras aplicaciones habilitadas para SAML sin tener que volver a especificar sus credenciales para una experiencia de inicio de sesión único sin problemas (SSO, Single Sign-On). Los usuarios finales pueden beneficiarse del uso del navegador del sistema predeterminado

© 2020 Palo Alto Networks, Inc.

para la autenticación SAML porque pueden aprovechar el mismo inicio de sesión para GlobalProtect con sus credenciales de usuario guardadas en el navegador del sistema predeterminado, como Chrome, Firefox o Safari.

Además, en cualquier navegador que admita la API de autenticación web (WebAuthn), puede utilizar los tokens de seguridad Univeral 2nd Factor (U2F) como YubiKeys para la autenticación multifactor (MFA, Multi-Factor Authentication) para identificar proveedores (IdP, Identify Providers) como Onelogin u Okta.

Esta función es compatible con Windows, macOS, Linux y dispositivos Android e iOS a partir de la aplicación de GlobalProtect™ 5.2.

STEP 1 | Cambie la configuración previamente implementada en Windows, macOS, Linux y los endpoints de Android e iOS para usar el navegador del sistema predeterminado para la autenticación SAML.

Debe establecer la configuración implementada previamente en los endpoints del cliente para poder habilitar el navegador del sistema predeterminado para la autenticación SAML. GlobalProtect recupera estas entradas solo una vez, cuando se inicializa la aplicación de GlobalProtect.

La aplicación abrirá un navegador integrado en lugar del navegador del sistema predeterminado si no hay un valor preimplementado especificado en los endpoints de Windows o macOS de los usuarios finales cuando se use el navegador del sistema predeterminado para la autenticación SAML, la opción **Use Default Browser for SAML Authentication (Usar el navegador predeterminado para la autenticación SAML)** está establecida en **Yes (Sí)** en la configuración del portal y los usuarios actualizan la aplicación desde la versión 5.0.x o la versión 5.1.x a la versión 5.2.0 por primera vez. Una vez que los usuarios se conecten a la aplicación de GlobalProtect y la opción **Use Default Browser for SAML Authentication (Usar navegador predeterminado para la autenticación SAML)** se establezca en **Yes (Sí)** en la configuración del portal, la aplicación abrirá el navegador del sistema predeterminado en Windows y endpoints de macOS en el próximo inicio de sesión.

Si el valor **default browser** se establece en **Yes (Sí)** en la configuración preinstalada de la máquina cliente y la opción **Use Default Browser for SAML Authentication (Usar el navegador predeterminado para la autenticación SAML)** está establecida en **No** en la configuración del portal, los usuarios finales no disfrutarán de la mejor experiencia de usuario. La aplicación abrirá el navegador del sistema predeterminado para la autenticación SAML por primera vez. Debido a que los valores predeterminados del navegador difieren entre la máquina cliente y el portal, la aplicación detectará una falta de coincidencia y abrirá un navegador integrado en el siguiente inicio de sesión.

La opción Use Default Browser for SAML Authentication (Usar navegador predeterminado para autenticación SAML) del portal de GlobalProtect y la configuración preinstalada en la máquina cliente deben tener el mismo valor para ofrecer la mejor experiencia de usuario.

- En los endpoints de Windows, puede usar System Center Configuration Manager (SCCM) para preimplementar la aplicación de GlobalProtect 5.2 y establecer el valor **DEFAULTBROWSER** en **yes (sí)** desde Windows Installer (Msiexec) mediante la siguiente sintaxis:

```
msiexec.exe /i GlobalProtect.msi DEFAULTBROWSER=YES
```

- En los endpoints de macOS, configure el valor **default-browser** en **yes (sí)** en macOS plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) para la aplicación de GlobalProtect con la siguiente sintaxis:

```
sudo defaults write /Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist '{"Palo Alto Networks"
 ={GlobalProtect={Settings={default-browser=yes;};};};}'
```


© 2020 Palo Alto Networks, Inc.

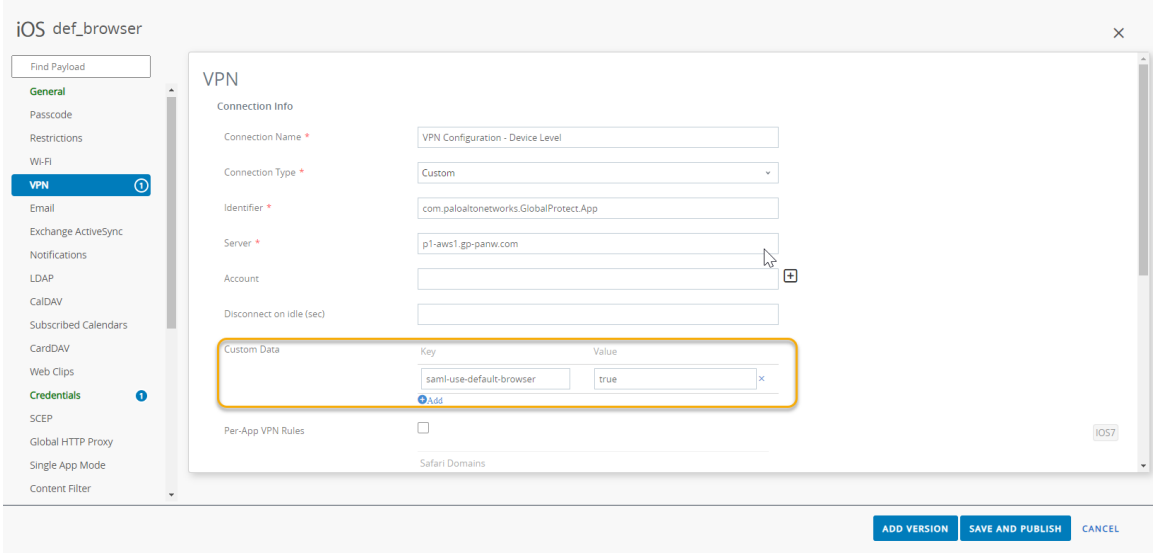
Debe especificar la clave plist para iniciar el navegador del sistema predeterminado para la autenticación SAML después de instalar la aplicación de GlobalProtect 5.2

Después de añadir la clave plist, debe reiniciar el endpoint de macOS para que la clave plist surta efecto. Después de reiniciar el sistema, se iniciará el navegador del sistema predeterminado para la autenticación SAML.

- En los endpoints de Linux, establezca el valor **default-browser** en **yes (sí)** en el archivo de configuración previa a la implementación `/opt/paloaltonetworks/globalprotect/pangps.xml` en `<Settings> (<Configuración>)`. Después de añadir el valor **default-browser**, debe reiniciar el endpoint de Linux para que el cambio surta efecto.
- En los endpoints de Android e iOS, cree un perfil de VPN mediante el sistema de gestión de dispositivos móviles (MDM, Mobile Device Management System) compatible, como AirWatch.
  - Inicie sesión en AirWatch como administrador.
  - Seleccione un perfil VPN existente (**Devices [Dispositivos]** > **Profiles & Resources [Perfiles y recursos]** > **Profiles [Perfiles]**) en la lista.
  - Seleccione **VPN** para añadir un perfil de VPN.

    En los endpoints de Android, especifique la **clave de datos personalizada** (**use_default_browser_for_saml**). Especifique el **valor de datos personalizado** (**true**).

    En los endpoints de iOS, especifique la **clave de datos personalizada** (**saml-use-default-browser**). Especifique el **valor de datos personalizado** (**true**).



  - Haga clic en **Save and Publish (Guardar y publicar)** para guardar los cambios.

STEP 2 | Configure la autenticación SAML para autenticar usuarios.

Para que el navegador del sistema predeterminado para la autenticación SAML no abra varias pestañas para cada conexión, le recomendamos que configure una anulación de autenticación. Para obtener más información, consulte Autenticación de cookies en el portal o la puerta de enlace.

STEP 3 | Habilite la aplicación de GlobalProtect para que los usuarios finales puedan aprovechar el mismo inicio de sesión para GlobalProtect y su navegador del sistema predeterminado para la autenticación SAML.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Agent (Agente)** *<agent-config>* > **App (Aplicación)** > **Use Default Browser for SAML Authentication (Usar el navegador predeterminado para la autenticación SAML)**.
2. Seleccione **Yes (Sí)** para permitir que la aplicación de GlobalProtect abra el navegador del sistema predeterminado para la autenticación SAML.

   Si el inicio de sesión único (SSO, Single-Sign-On) está habilitado, le recomendamos que lo deshabilite. Establezca Use Single Sign-On (Windows) [Usar inicio de sesión único (Windows)] o Use Single Sign-On (macOS) [Usar inicio de sesión único (macOS)] en No para deshabilitar el inicio de sesión único cuando utilice el navegador del sistema predeterminado para la autenticación SAML.

STEP 4 | Haga clic en **OK** dos veces.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 6 | Verifique que los usuarios finales puedan autenticarse con éxito en el IdP mediante sus credenciales guardadas.

1. Seleccione **Refresh Connection (Actualizar conexión)**, **Connect (Conectar)** o **Enable (Habilitar)** en la aplicación de GlobalProtect para iniciar la conexión.

   Se abrirá una nueva pestaña en el navegador predeterminado del sistema para la autenticación SAML.
2. Inicie sesión con el nombre de usuario y la contraseña para autenticarse en el IdP.
3. Una vez que los usuarios finales puedan autenticarse correctamente en el IdP, haga clic en **Open GlobalProtect (Abrir GlobalProtect)**.
4. Conéctese a la aplicación de GlobalProtect u otras aplicaciones habilitadas para SAML sin volver a introducir las credenciales de usuario.

Configuración de autenticación Kerberos

Kerberos es un protocolo de autenticación de red informática que usa *vales* para permitir que los nodos se comuniquen a través de una red no segura para demostrar su identidad entre sí de forma segura.

La autenticación Kerberos es compatible con endpoints de Windows (7, 8 y 10) y macOS (10.10 y versiones posteriores). La autenticación Kerberos para endpoints de macOS requiere como mínimo la versión 4.1.0 de la aplicación de GlobalProtect.

STEP 1 | Cree un perfil de servidor.

El perfil de servidor identifica el servicio de autenticación externo e indica al cortafuegos cómo conectarse con dicho servicio de autenticación y acceder a las credenciales de autenticación para sus usuarios.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Kerberos** y haga clic en **Add (Añadir)** para añadir un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)**, como `GP-User-Auth`.
3. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.
4. Haga clic en **Add (Añadir)** en el área **Servers (Servidores)** y, luego, introduzca la siguiente información para conectarse al servidor de autenticación:
   - Nombre del servidor en **Name (Nombre)**
   - Dirección IP de FQDN del **Kerberos Server (Servidor Kerberos)**
   - **Puerto**

© 2020 Palo Alto Networks, Inc.

5. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | (Opcional) Cree un perfil de autenticación.

El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios. En un portal o puerta de enlace, puede asignar uno o más perfiles de autenticación en uno o más perfiles de autenticación de cliente. Para obtener información sobre cómo un perfil de autenticación dentro de un perfil de autenticación de cliente admite la autenticación de usuario granular, consulte Configuración de una puerta de enlace de GlobalProtect y Configuración del acceso al portal de GlobalProtect.

Para permitir que los usuarios se conecten y cambien sus contraseñas caducadas sin intervención administrativa, considere usar la VPN de acceso remoto con inicio de sesión previo.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y haga clic en **Add (Añadir)** para añadir un perfil nuevo.
2. Introduzca un **Name (Nombre)** para el perfil y, a continuación, seleccione **Kerberos** como el tipo de autenticación en **Type (Tipo)**.
3. Seleccione el **Server Profile (Perfil de servidor)** de la autenticación Kerberos que creó en el paso 1.
4. Especifique el **User Domain (Dominio de usuario)** y el **Username Modifier (Modificador de nombre de usuario)**. El endpoint combina estos valores para modificar la cadena de dominio/nombre de usuario que introduce un usuario durante el inicio de sesión. El endpoint usa la cadena modificada para la autenticación y usa el valor de **User Domain (Dominio de usuario)** para la asignación de grupos de User-ID. La modificación de las entradas del usuario es útil cuando el servicio de autenticación requiere cadenas de dominio/nombre de usuario en un formato particular, pero usted no desea depender de los usuarios para introducir correctamente el dominio. Puede seleccionar una de las siguientes opciones:
   - Para enviar la información de usuario sin modificar, deje en blanco el **User Domain (Dominio de usuario)** (predeterminado) y defina el **Username Modifier (Modificador de nombre de usuario)** con la variable **%USERINPUT%** (predeterminado).
   - Para que un dominio preceda a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina el **Username Modifier (Modificador de nombre de usuario)** como **%USERDOMAIN%\%USERINPUT%**.
   - Para anexar un dominio a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina **Username Modifier (Modificador de nombre de usuario)** como **%USERINPUT%@%USERDOMAIN%**.

   Si Username Modifier (Modificador de nombre de usuario) incluye la variable %USERDOMAIN%, el valor de User Domain (Dominio de usuario) sustituye cualquier cadena de dominio que introduzcan los usuarios. Si el campo User Domain (Dominio de usuario) está en blanco, el dispositivo elimina toda cadena de dominio introducida por el usuario.
5. Configure el inicio de sesión único (single sign-on, SSO) de Kerberos si su red lo admite.
   - Introduzca el **Kerberos Realm (Dominio Kerberos)** (hasta 127 caracteres) para especificar la parte del nombre de host del nombre de inicio de sesión del usuario. Por ejemplo, en el nombre de cuenta de usuario usuario@EJEMPLO.LOCAL, el dominio es EJEMPLO.LOCAL.
   - Haga clic en **Import (Importar)** para importar un archivo de **Kerberos Keytab (Keytab de Kerberos)**. Cuando se le indique, seleccione **Browse (Examinar)** para buscar el archivo de keytab y, luego, haga clic en **OK (Aceptar)**. Durante la autenticación, el endpoint primero intenta establecer el SSO con el keytab. Si lo logra y el usuario que intenta acceder está en la **Allow List (Lista de permitidos)**, la autenticación es inmediata. De lo contrario, el proceso de autenticación se revierte a la autenticación manual (nombre de usuario/contraseña) con el **Type (Tipo)** de

© 2020 Palo Alto Networks, Inc.

autenticación especificado. No es necesario que el **Type (Tipo)** sea Kerberos. Para modificar este comportamiento de manera que los usuarios puedan autenticarse únicamente con Kerberos, configure **Use Default Authentication on Kerberos Authentication Failure (Utilizar autenticación por defecto si falla la autenticación Kerberos)** en **No** en una configuración de agente de portal de GlobalProtect.

6. En la pestaña **Advanced (Avanzada)**, haga clic en **Add (Añadir)** para añadir una **Allow List (Lista de permitidos)** y seleccione los usuarios y grupos de usuarios que pueden autenticarse con este perfil. La opción **all (todo)** permite que todos los usuarios se autentiquen con este perfil. Por defecto, la lista no tiene entradas, lo que significa que ningún usuario puede autenticarse.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.

Configuración de autenticación RADIUS o TACACS+

RADIUS es un protocolo y software de cliente/servidor que permite a los servidores de acceso remoto comunicarse con un servidor central para autenticar a los usuarios de acceso telefónico y autorizar su acceso al sistema o servicio solicitado. TACACS+ es un protocolo de autenticación bien establecido, común a las redes UNIX, que permite que un servidor de acceso remoto reenvíe la contraseña de inicio de sesión de un usuario a un servidor de autenticación para determinar si se puede permitir el acceso a un sistema determinado.

STEP 1 | Cree un perfil de servidor.

El perfil de servidor identifica el servicio de autenticación externo e indica al cortafuegos cómo conectarse con dicho servicio de autenticación y acceder a las credenciales de autenticación para sus usuarios.

Si desea realizar la Habilitación del envío de VSA a un servidor RADIUS, debe crear un perfil de servidor RADIUS.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** y seleccione el tipo de perfil (**RADIUS** o **TACACS+**).
2. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de servidor RADIUS o TACACS+.
3. Introduzca un **Profile Name (Nombre de perfil)**, como `GP-User-Auth`.
4. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.
5. Configure los siguientes **Server Settings (Ajustes de servidor)**.
   - **Timeout (sec) [Tiempo de espera (seg.)]**: el número de segundos antes de que caduque la solicitud de conexión del servidor debido a la falta de respuesta del servidor de autenticación.
   - **Authentication Protocol (Protocolo de Autenticación)**: el protocolo usado para la conexión con el servidor de autenticación. Las opciones incluyen **CHAP**, **PAP**, **PEAP-MSCHAPv2**, **PEAP with GTC (PEAP con GTC)** o **EAP-TTLS with PAP (EAP-TTLS con PAP)**.

     Si configura PEAP-MSCHAPv2 (Protocolo de autenticación extensible protegido-Protocolo de autenticación por desafío mutuo de Microsoft versión 2, Protected Extensible Authentication Protocol Microsoft Challenge Handshakie Authentication Protocol version 2, PEAP-MSCHAPv2) como el protocolo de autenticación, los usuarios remotos pueden cambiar sus contraseñas de RADIUS o Active Directory (AD) con la aplicación de GlobalPRotect cuando su contraseña caduque o un administrador de RADIUS o AD exija un cambio de contraseña en el siguiente inicio de sesión.

© 2020 Palo Alto Networks, Inc.

- (Solo RADIUS) **Retries (Reintentos)**: la cantidad de veces que el cortafuegos intenta conectarse al servidor de autenticación antes de abandonar la solicitud.
- (Solo TACACS+) **Use single connection for all authentication (Utilice una sola conexión para toda autenticación)**: la opción que permite que todas las solicitudes de autenticación TACACS+ se realicen en una única sesión TCP en lugar de sesiones separadas para cada solicitud.

6. Haga clic en **Add (Añadir)** en el área **Servers (Servidores)** y, luego, introduzca la siguiente información para conectarse al servidor de autenticación:
   - **Nombre**
   - Los servidores **RADIUS** o **TACACS+** en **Server (Servidor)** (dirección IP o FQDN del servidor)
   - **Secret (Secreto)** (el secreto compartido que permite al servicio de autenticación autenticar el cortafuegos)
   - **Puerto**
7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | (Opcional) Cree un perfil de autenticación.

El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios. En un portal o puerta de enlace, puede asignar uno o más perfiles de autenticación en uno o más perfiles de autenticación de cliente. Para obtener información sobre cómo un perfil de autenticación dentro de un perfil de autenticación de cliente admite la autenticación de usuario granular, consulte Configuración de una puerta de enlace de GlobalProtect y Configuración del acceso al portal de GlobalProtect.

Para permitir que los usuarios se conecten y cambien sus contraseñas caducadas sin intervención administrativa, considere usar la VPN de acceso remoto con inicio de sesión previo*.*

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y haga clic en **Add (Añadir)** para añadir un perfil nuevo.
2. Introduzca un **Name (Nombre)** para el perfil.
3. Seleccione el tipo de **Authentication (Autenticación)** en **Type (Tipo)** (**RADIUS** o **TACACS+**).
4. Seleccione el **Server Profile (Perfil del servidor)** de la autenticación RADIUS o TACACS+ que creó en el paso 1 del menú desplegable.
5. (Solo RADIUS) Habilite **Retrieve user group from RADIUS (Recuperar grupo de usuarios de RADIUS)** si desea incluir esta información en el perfil de autenticación.
6. Especifique el **User Domain (Dominio de usuario)** y el **Username Modifier (Modificador de nombre de usuario)**. El endpoint combina estos valores para modificar la cadena de dominio/nombre de usuario que introduce un usuario durante el inicio de sesión. El endpoint usa la cadena modificada para la autenticación y usa el valor de **User Domain (Dominio de usuario)** para la asignación de grupos de User-ID. La modificación de las entradas del usuario es útil cuando el servicio de autenticación requiere cadenas de dominio/nombre de usuario en un formato particular, pero usted no desea depender de los usuarios para introducir correctamente el dominio. Puede seleccionar una de las siguientes opciones:
   - Para enviar la información de usuario sin modificar, deje en blanco el **User Domain (Dominio de usuario)** (predeterminado) y defina el **Username Modifier (Modificador de nombre de usuario)** con la variable **%USERINPUT%** (predeterminado).
   - Para que un dominio preceda a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina el **Username Modifier (Modificador de nombre de usuario)** como **%USERDOMAIN%\%USERINPUT%**.
   - Para anexar un dominio a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina **Username Modifier (Modificador de nombre de usuario)** como **%USERINPUT%@ %USERDOMAIN%**.

© 2020 Palo Alto Networks, Inc.

Si Username Modifier (Modificador de nombre de usuario) incluye la variable %USERDOMAIN%, el valor de User Domain (Dominio de usuario) sustituye cualquier cadena de dominio que introduzcan los usuarios. Si el campo User Domain (Dominio de usuario) está en blanco, el dispositivo elimina toda cadena de dominio introducida por el usuario.

7. En la pestaña **Advanced (Avanzada)**, haga clic en **Add (Añadir)** para añadir una **Allow List (Lista de permitidos)** y seleccione los usuarios y grupos de usuarios que pueden autenticarse con este perfil. La opción **all (todo)** permite que todos los usuarios se autentiquen con este perfil. Por defecto, la lista no tiene entradas, lo que significa que ningún usuario puede autenticarse.
8. Haga clic en **OK (Aceptar)**.

STEP 3 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación de certificado de cliente

Con la autenticación del certificado de cliente opcional, el usuario presenta el certificado e cliente junto con una solicitud de conexión en el portal o puerta de enlace de GlobalProtect. El portal o la puerta de enlace pueden usar un certificado de cliente único o compartido para validar que el usuario o el endpoint pertenezcan a su organización.

Los métodos para la implementación de los certificados de cliente dependen de los requisitos de seguridad para su organización:

- Implementación de certificados de cliente compartidos para autenticación
- Implementación de certificados de equipo para autenticación
- Implementación de certificados de cliente específicos del usuario para autenticación

Implementación de certificados de cliente compartidos para autenticación

Para confirmar que un endpoint pertenece a su organización, usted puede usar el mismo certificado de cliente para todos los endpoints, o bien generar certificados separados para implementarlos con una configuración de agente en particular. Use este flujo de trabajo para emitir certificados de cliente autofirmados e impleméntelos desde el portal.

STEP 1 | Genere un certificado para implementar en varios endpoints de GlobalProtect.

1. Cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect.
2. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Generate (Generar)** para generar un nuevo certificado.
3. Configure el **Certificate Type (Tipo de certificado)** en **Local** (predeterminado).
4. Introduzca un **Certificate Name (Nombre de certificado)**. Este nombre no puede contener espacios.
5. Introduzca un **Common Name (Nombre común)** para identificar este certificado como un certificado de aplicación (por ejemplo, `GP_Windows_App`). Dado que este certificado se implementará en todas las aplicaciones conla misma configuración de agente, no es necesario identificar de forma exclusiva usuarios o endpoints específicos.
6. En el campo **Signed By (Firmado por)**, seleccione su CA raíz.
7. Seleccione un **OCSP Responder (Respondedor OCSP)** para verificar el estado de revocación de los certificados.
8. Haga clic en **OK (Aceptar)** para generar el certificado.

STEP 2 | Configure la autenticación en dos fases.

Configure los ajustes de autenticación en una configuración de agente de portal de GlobalProtect para permitir que el portal implemente de forma transparente el certificado de cliente, que es **Local** para el cortafuegos, en las aplicaciones que reciben la configuración.

Implementación de certificados de equipo para autenticación

Para confirmar que el endpoint pertenece a su organización, use su propia infraestructura de clave pública (public-key infrastructure, PKI) para emitir y distribuir certificados de equipo a cada endpoint (recomendado)

© 2020 Palo Alto Networks, Inc.

o genere un certificado de equipo autofirmado para exportar. Con los métodos de conexión de inicio de sesión previo, se requiere un certificado de equipo que debe instalarse en el endpoint para que los componentes de GlobalProtect otorguen el acceso.

Para confirmar que el endpoint pertenece a su organización, también debe configurar un perfil de autenticación para autenticar al usuario (consulte Autenticación en dos fases).

Utilice el siguiente flujo de trabajo para crear el certificado de cliente e implementarlo manualmente en un endpoint. Para obtener más información, consulte Acerca de la autenticación de usuarios de GlobalProtect. Para obtener un ejemplo de configuración, consulte VPN de acceso remoto (perfil del certificado).

STEP 1 | Emita certificados de cliente para aplicaciones y endpoints de GlobalProtect.

Esto permite que el portal y las puertas de enlace de GlobalProtect validen que el endpoint pertenece a su organización.

1. Cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect.
2. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Generate (Generar)**.
3. Introduzca un **Certificate Name (Nombre de certificado)**. El nombre de certificado no puede contener espacios.
4. Introduzca la dirección IP o FQDN que aparecerá en el certificado en el campo **Common Name (Nombre común)**.
5. Seleccione la CA raíz del menú desplegable **Signed By (Firmado por)**.
6. Seleccione un **OCSP Responder (Respondedor OCSP)** para verificar el estado de revocación de los certificados.
7. En **Cryptographic Settings (Configuración de criptografía)**, configure los ajustes del certificado, incluidos el algoritmo de cifrado en **Algorithm (Algoritmo)**, la longitud de las claves en **Number of Bits (Número de bits)**, el algoritmo de resumen (SHA1, SHA256, SHA384 o SHA512) en **Digest (Resumen)** y los días durante los que tiene validez en **Expiration (Vencimiento)**.

   Si el cortafuegos está en modo FIPS-CC y el algoritmo de generación de claves es RSA, las claves RSA deben ser de 2.048 o 3072 bits.
8. En el área **Certificate Attributes (Atributos del certificado)**, haga clic en **Add (Añadir)** y defina los atributos que identifican de manera única los endpoints que pertenecen a su organización. Tenga en cuenta que si añade un atributo de **Host Name (Nombre de host)** (que llena el campo SAN del certificado), debe coincidir con el valor que haya definido en el campo **Common Name (Nombre común)**.
9. Haga clic en **OK (Aceptar)** para generar el certificado.

STEP 2 | Instale certificados en el almacén de certificados personales de los endpoints.

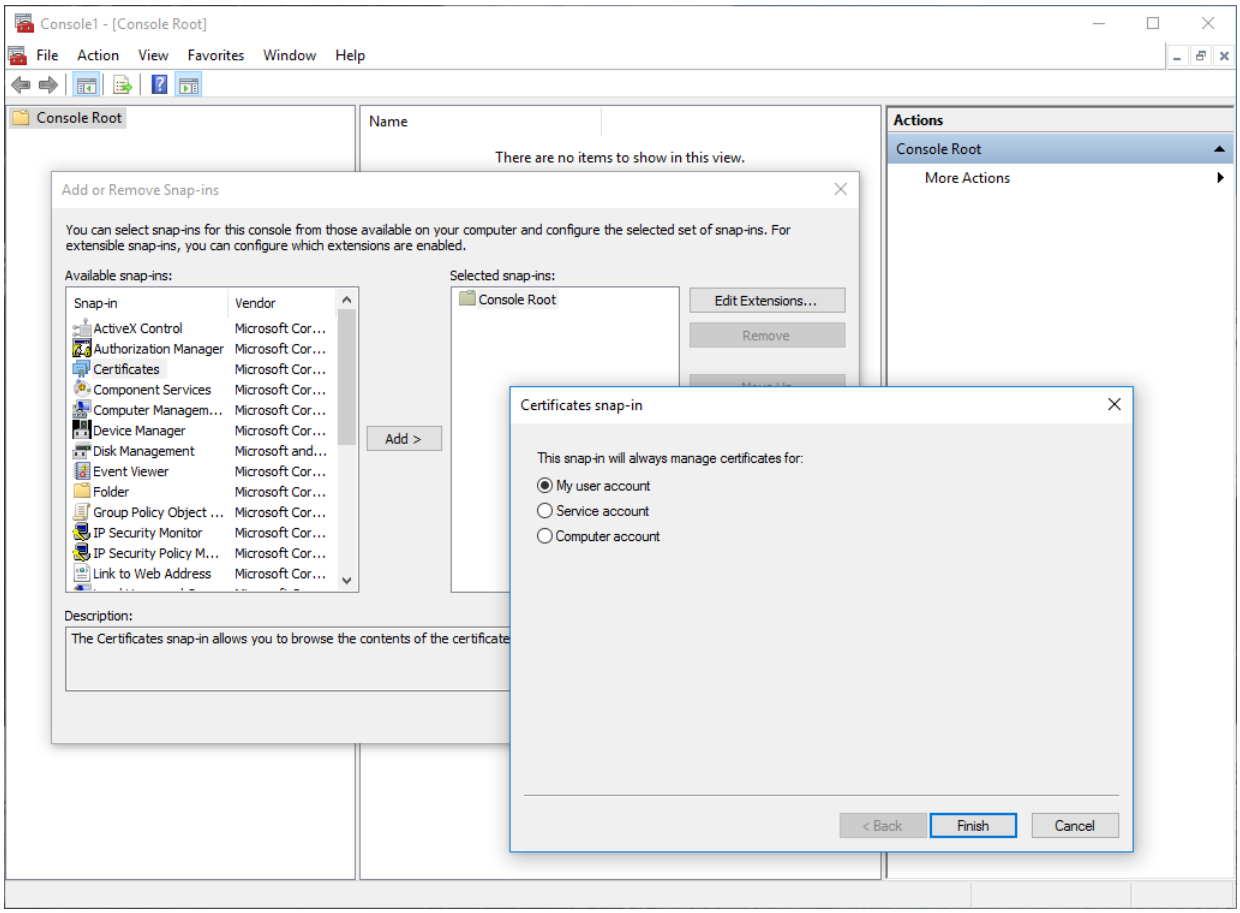
Si usa certificados de usuario o certificados de equipo exclusivos, cada certificado debe instalarse en el almacén de certificados personales del endpoint antes de la primera conexión al portal o la puerta de enlace. Los certificados de máquina se guardan en el almacén de certificados del ordenador local en Windows y en el llavero del sistema en macOS. Los certificados de usuario se guardan en el almacén de certificados del usuario actual en Windows y en el llavero del sistema en macOS.

Por ejemplo, para instalar un certificado en un sistema Windows con Microsoft Management Console:

1. Desde la línea de comandos, introduzca `mmc` para iniciar Microsoft Management Console.
2. Seleccione **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)**.
3. En la lista **Available snap-ins (Complementos disponibles)**, seleccione **Certificates (Certificados)**, y luego, haga clic en **Add (Añadir)** y seleccione uno de los siguientes complementos de certificados según el tipo de certificado que importe:

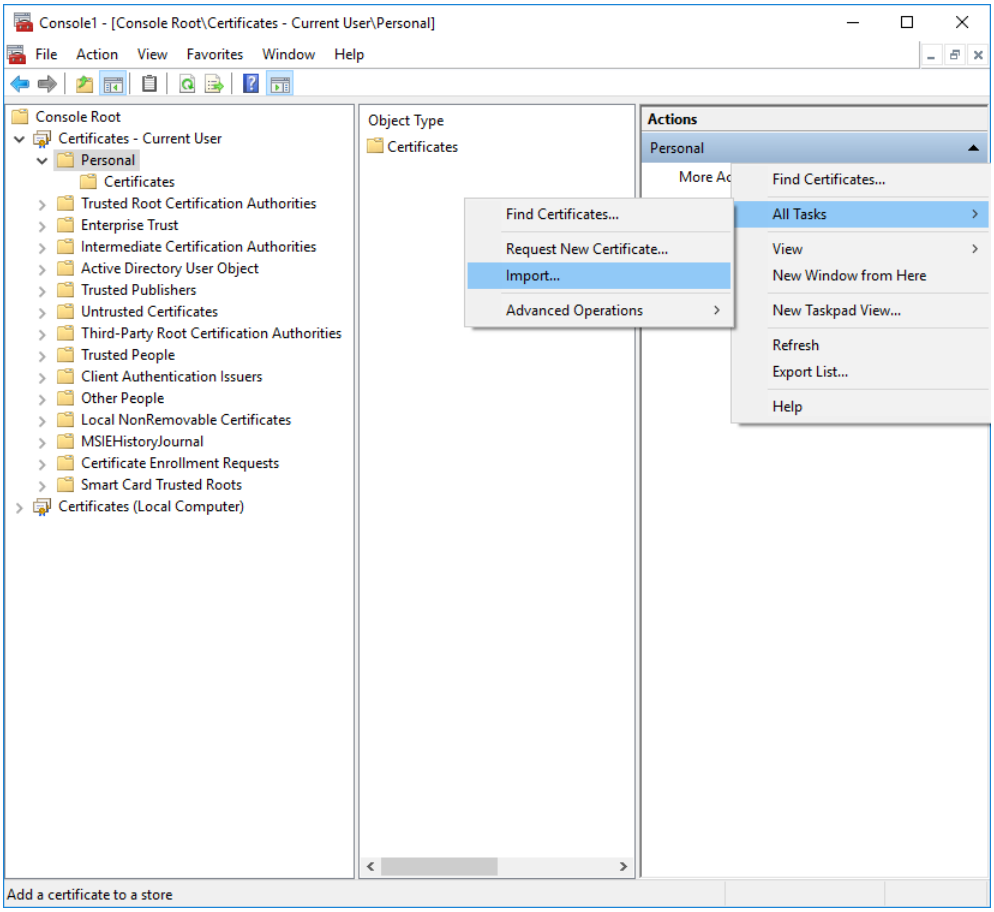
© 2020 Palo Alto Networks, Inc.

- **Computer account**: seleccione esta opción si importa un certificado de equipo.
- **My user account (Mi cuenta de usuario)**: seleccione esta opción si importa un certificado de usuario.



4. Desde **Console Root (Raíz de consola)**, expanda **Certificates (Certificados)** y luego seleccione **Personal**.
5. En la columna **Actions (Acciones)**, seleccione **Personal** > **More Actions (Más acciones)** > **All Tasks (Todas las tareas)** > **Import (Importar)** y siga los pasos del Asistente de importación de certificados para importar el archivo PKCS que recibió de la CA.

© 2020 Palo Alto Networks, Inc.

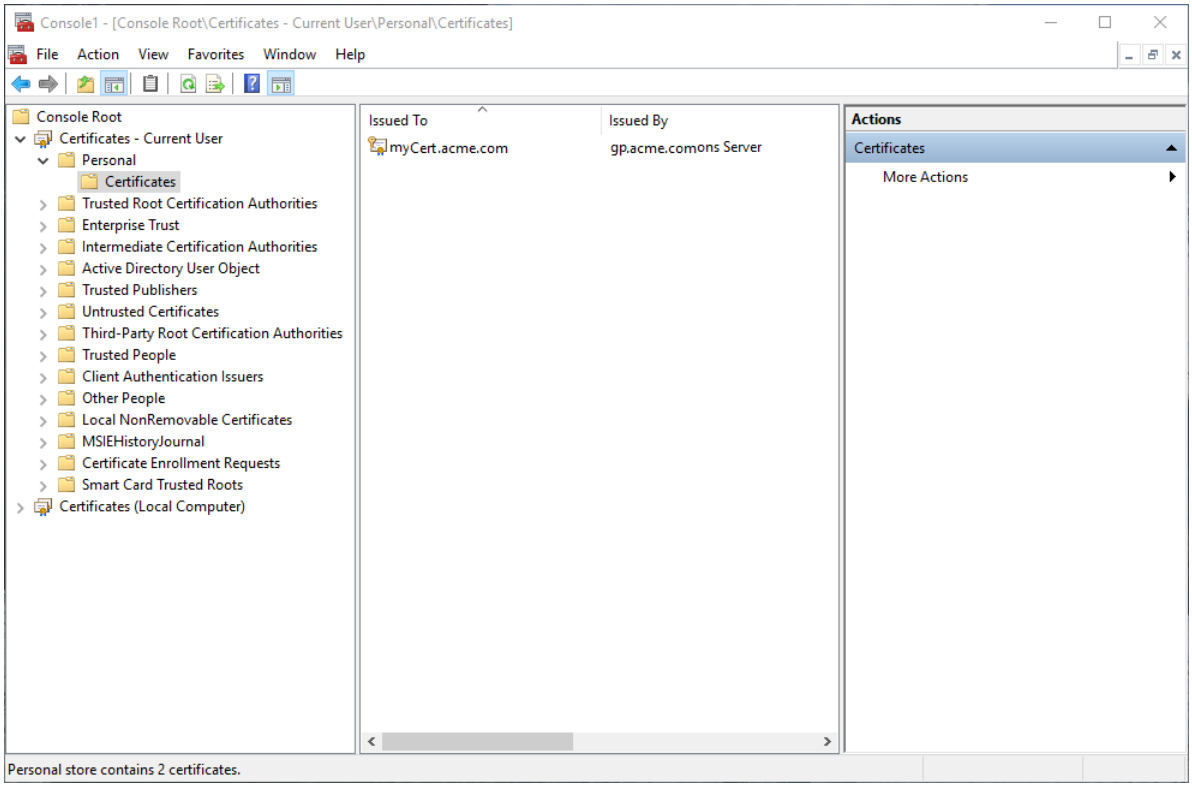


6. Haga clic en **Browse (Examinar)** y seleccione el archivo de certificado .p12 para importar (seleccione **Personal Information Exchange [Intercambio de información personal]** como el tipo de archivo a buscar) e introduzca la **Password (Contraseña)** que usó para cifrar la clave privada. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.

STEP 3 | Compruebe que se ha añadido el certificado al almacén de certificados personales.

Navegue al almacén de certificados personal desde **Console Root (Raíz de consola)** (**Certificates [Certificados]** > **Personal** > **Certificates [Certificados]**:

© 2020 Palo Alto Networks, Inc.



STEP 4 | Importe el certificado de CA raíz usado para emitir los certificados de clientes en el cortafuegos.

Este paso solo es necesario si los certificados de cliente fueron emitidos por una CA externa, como una CA pública o una CA de PKI de empresa. Si usa certificados autofirmados, el portal y las puertas de enlace ya confían en la CA raíz.

1. Descargue el certificado de CA raíz usado para emitir los certificados de clientes (formato Base64).
2. Importe el certificado de CA raíz desde la CA que generó los certificados de cliente en el cortafuegos:
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)**.
   2. Configure el **Certificate Type (Tipo de certificado)** en **Local** (predeterminado).
   3. Introduzca un **Certificate Name (Nombre de certificado)** que identifique al certificado como su certificado de CA de cliente.
   4. Haga clic en **Browse (Examinar)** y seleccione el **Certificate File (Archivo de certificado)** que descargó desde la CA.
   5. Configure **File Format (Formato de archivo)** en **Base64 Encoded Certificate (PEM) (Certificado codificado en Base64 [PEM])** y haga clic en **OK (Aceptar)**.
   6. En la pestaña **Device Certificates (Certificados del dispositivo)**, seleccione el certificado que acaba de importar para abrir la información del certificado.
   7. Seleccione **Trusted Root CA (CA raíz de confianza)** y, a continuación, haga clic en **OK (Aceptar)**.

STEP 5 | Cree un perfil de certificado de cliente.

1. Seleccione **Device (Dispositivo)** > **Certificates (Certificados)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y, luego, haga clic en **Add (Añadir)** para añadir un nuevo perfil de certificado.
2. Introduzca un **Name (Nombre)** de perfil.

© 2020 Palo Alto Networks, Inc.

3. Seleccione un valor de **Username Field (Campo de nombre de usuario)** para especificar qué campo en el certificado contendrá la información de identidad del usuario.

   Si planea configurar el portal o las puertas de enlace para autenticar a los usuarios con certificados únicamente, debe especificar el **Username Field (Campo de nombre de usuario)**. Esto habilita a GlobalProtect para que asocie un nombre de usuario con el certificado.

   Si planea configurar el portal o la puerta de enlace para la autenticación en dos fases, puede dejar el valor por defecto **None (Ninguno)** o bien, para añadir una capa adicional de seguridad, especificar un nombre de usuario. Si especifica un nombre de usuario, su servicio de autenticación externa verifica que el nombre de usuario en el certificado cliente coincida con el nombre de usuario que solicita la autenticación. Esto garantiza que el usuario sea aquel para el cual se emitió el certificado.

   Los usuarios no pueden cambiar el nombre de usuario que se incluye en el certificado.

4. En el área **CA Certificates (Certificados de CA)**, haga clic en **Add (Añadir)**. Seleccione el certificado de CA raíz de confianza que importó en el paso 4 desde la lista desplegable **CA Certificate (Certificado de CA)** y haga clic en **OK (Aceptar)**.

STEP 6 | Guarde la configuración.

Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Implementación de certificados de cliente específicos del usuario para autenticación

Para autenticar usuarios individuales, debe emitir un certificado de cliente exclusivo para cada usuario de GlobalProtect e implementarlo en los endpoints antes de habilitar GlobalProtect. Para automatizar la generación e implementación de certificados cliente específicos del usuario, puede configurar su portal de GlobalProtect para que funcione como un cliente de protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) en un servidor SCEP en la PKI de su empresa.

El funcionamiento de SCEP es dinámico, ya que la PKI de la empresa genera un certificado específico del usuario cuando el portal lo solicita y envía el certificado al portal. Luego, el portal implementa el certificado en la aplicación de forma transparente. Cuando un usuario solicita acceso, la aplicación puede presentar el certificado del cliente para autenticar con el portal o la puerta de enlace.

El portal o la puerta de enlace de GlobalProtect usan información de identificación sobre el endpoint y el usuario para evaluar si permite acceder al usuario. GlobalProtect bloquea el acceso si la ID de host está en una lista de bloqueo de dispositivos o si la sesión coincide con alguna opción de bloqueo especificada en un perfil de certificado. Si la autenticación falla debido a un certificado no válido del cliente basado en SCEP, la aplicación de GlobalProtect intenta autenticarse con el portal (sobre la base de la configuración en el perfil de autenticación) y recuperar el certificado. Si la aplicación no puede recuperar el certificado desde el portal, el endpoint no puede conectarse.

STEP 1 | Cree un perfil de SCEP.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SCEP** y, luego, haga clic en **Add (Añadir)** para añadir un perfil nuevo de SCEP.
2. Introduzca un nombre en **Name (Nombre)** para identificar el perfil de SCEP.
3. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.

© 2020 Palo Alto Networks, Inc.

STEP 2 | (Opcional) Para que la generación de certificados basada en SCEP sea más segura, configure un mecanismo de respuesta de comprobación de SCEP entre la PKI y el portal de cada solicitud de certificado.

Después de configurar este mecanismo, su operación es invisible y no es necesario introducir más datos.

Para cumplir con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) de los Estados Unidos, use una comprobación SCEP dinámica. Para ello, haga clic en **Dynamic (Dinámica) SCEP Challenge (Comprobación SCEP)** y especifique una **Server URL (URL de servidor)** que use HTTPS (consulte el paso 7).

Seleccione una de las siguientes opciones de **Desafío SCEP**:

- **None (Ninguna)**: (**valor por defecto**) el servidor SCEP no comprueba el portal antes de emitir un certificado.
- **Fixed (Fijo)**: ingrese la comprobación de inscripción **Password (Contraseña)** obtenida del servidor SCEP en la infraestructura de PKI.
- **Dynamic (Dinámico)**: Ingrese un **Username (Nombre de usuario)** y **Password (Contraseña)** de su elección (posiblemente las credenciales del administrador de PKI) y la **Server URL (URL de servidor)** de SCEP donde el cliente del portal envía estas credenciales. Estas sirven para realizar la autenticación en el servidor SCEP, que genera en segundo plano una contraseña de un solo uso (one-time password, OTP) para el portal tras cada solicitud de certificado; después de cada solicitud, la OTP nueva aparece en el campo actualizado `The enrollment challenge password is` (La contraseña de comprobación de la inscripción es). La PKI aprueba cada contraseña nueva de manera transparente en el portal, el cual luego utiliza la contraseña para su solicitud de certificado.

STEP 3 | Especifique los ajustes de la conexión entre el servidor SCEP y el portal para permitir que el portal solicite y reciba certificados de cliente.

Puede incluir información adicional sobre el endpoint o el usuario mediante la especificación de tokens en el nombre de **Subject (Asunto)** del certificado.

En el campo **Subject (Asunto)** de CSR para el servidor SCEP, el portal incluye el valor del token como **CN** y el ID de host como **SerialNumber (Número de serie)**. El ID del host varía por tipo de endpoint: GUID (Windows), dirección MAC de la interfaz (macOS), ID de Android (endpoints de Android), UDID (endpoints de iOS) o un nombre único que asigne GlobalProtect (Chrome).

1. En el área **Configuration (Configuración)**, ingrese la **Server URL (URL de servidor)** que el portal usa para conectarse al servidor SCEP en el PKI (por ejemplo, `http://10.200.101.1/certsrv/mscep/`).
2. Ingrese el **CA-IDENT Name (Nombre de CA-IDENT)** (hasta 255 caracteres de longitud) para identificar al servidor SCEP.
3. Escriba un nombre de **Subject (Asunto)** para los certificados generados por el servidor SCEP. El nombre de asunto debe ser un nombre distintivo con el formato <**`attribute`**>=<**`value`**> y debe incluir un atributo de nombre común (CN) (`CN=`<**`variable`**>). El CN admite las siguientes tokens dinámicos:
   - `$USERNAME`: utilice este token para permitir que el portal solicite certificados para un usuario específico. Para usar esta variable, también debe Habilitar la asignación de grupos. El nombre de usuario introducido por el usuario debe coincidir con el nombre en la tabla de asignación de grupos de usuarios.
   - `$EMAILADDRESS`: utilice este token para solicitar certificados asociados con una dirección de correo electrónico específica. Para usar esta variable, también debe habilitar la asignación de grupo y configurar **Mail Attributes (Atributos de correo)** en el área **Mail Domains (Dominios de correo)** del perfil del servidor. Si GlobalProtect no puede identificar una dirección de correo electrónico para el usuario, genera una ID único y rellena el CN con ese valor.

© 2020 Palo Alto Networks, Inc.

- `$HOSTID`: para solicitar certificados únicamente para el endpoint, especifique el token de ID del host. Cuando un usuario intenta iniciar sesión en el portal, el endpoint envía información de identificación que incluye su valor de ID de host.

Cuando el portal de GlobalProtect envíe los ajustes SCEP a la aplicación, la parte de CN del nombre de asunto se sustituirá por el valor real (nombre de usuario, ID de host o dirección de correo electrónico) del propietario del certificado (por ejemplo, **`O=acme,CN=johndoe`**).

4. Seleccione **Subject Alternative Name Type (Tipo de nombre de asunto alternativo)**:
   - **RFC 822 Name (Nombre RFC 822)**: introduzca el nombre del correo electrónico en el asunto o la extensión de nombre alternativo de asunto del certificado.
   - **DNS Name (Nombre de DNS)**: ingrese el nombre de DNS usado para evaluar los certificados.
   - **Uniform Resource Identifier (Identificador uniforme de recurso)**: ingrese el nombre del recurso desde el que la aplicación obtendrá el certificado.
   - **None (Ninguno)**: no especifique atributos para el certificado.

STEP 4 | (Opcional) Configure **Cryptographic Settings (Ajustes criptográficos)** para el certificado.

- Seleccione la **Number of Bits (Cantidad de bits)** (longitud de la clave) del certificado.

  Si el cortafuegos está en modo FIPS-CC y el algoritmo de generación de claves es RSA. Las claves RSA deben ser de 2.048 bits o más.
- En **Digest for CSR (Resumen de CSR)**, seleccione el algoritmo de resumen para la CSR: SHA1, SHA256, SHA384 o SHA512.

STEP 5 | (Opcional) Configure los usos permitidos del certificado, ya sea para firma o cifrado.

- Para usar este certificado para la firma, seleccione la casilla de verificación **Use as digital signature**. Esta opción permite que el endpoint use la clave privada en el certificado para validar una firma digital.
- Para usar este certificado para cifrado, seleccione la casilla de verificación **Use for key encipherment (Usar para cifrado de clave)**. Esta opción permite que la aplicación use la clave privada en el certificado para cifrar los datos intercambiados en la conexión HTTPS establecida con los certificados emitidos por el servidor SCEP.

STEP 6 | (Opcional) Para garantizar que el portal se conecte al servidor SCEP correcto, introduzca la huella digital de certificado CA en **CA Certificate Fingerprint (Huella de certificado de CA)**. Obtenga esta huella en el campo **Thumbprint (Huella)** de la interfaz del servidor SCEP.

1. Introduzca la URL para la IU administrativa del servidor SCEP (por ejemplo, **`http://<hostname or IP>/CertSrv/mscep_admin/`**).
2. Copie la huella e introdúzcala en el campo **CA Certificate Fingerprint (Huella de certificado de CA)**.

STEP 7 | Habilite la autenticación SSL mutua entre el servidor SCEP y el portal GlobalProtect. Esto es necesario para cumplir con los estándares federales de EE. UU. de procesamiento de la información (U.S. Federal Information Processing Standard, FIPS).

La operación FIPS-CC se indica en la página de inicio de sesión del cortafuegos y su barra de estado.

Seleccione el **CA Certificate (Certificado de CA)** raíz del servidor SCEP. De manera opcional, puede habilitar la autenticación SSL mutua entre el servidor SCEP y el portal de GlobalProtect seleccionado un **Client Certificate (Certificado de cliente)**.

STEP 8 | Guarde y confirme la configuración.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes.

© 2020 Palo Alto Networks, Inc.

2. Haga clic en **Commit (Confirmar)** para confirmar la configuración.

El portal intenta solicitar un certificado de CA con la configuración del perfil de SCEP y, luego, lo guarda en el cortafuegos que aloja el portal. Si se obtiene correctamente, el certificado de CA se muestra en **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.

STEP 9 | (Opcional) Si el portal no logra obtener el certificado después de guardar el perfil de SCEP, puede generar manualmente una solicitud de firma de certificado (certificate signing request, CSR) desde el portal.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Generate (Generar)** para generar un nuevo certificado.
2. Seleccione **SCEP** como el **Certificate Type (Tipo de certificado)**.
3. Introduzca un **Certificate Name (Nombre de certificado)**. Este nombre no puede contener espacios.
4. Seleccione el **SCEP Profile (Perfil SCEP)** para usar para enviar una CSR a la PKI de su empresa.
5. Haga clic en **OK** para enviar la solicitud y generar el certificado.

STEP 10 | Configure la autenticación en dos fases.

Asigne al perfil de SCEP una configuración de agente del portal de GlobalProtect para permitir que el portal solicite e implemente de forma trasparente los certificados de cliente en las aplicaciones que reciben la configuración.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación en dos fases

Si necesita una autenticación sólida para proteger activos confidenciales o cumplir con requisitos reglamentarios, como PCI, SOX o HIPAA, configure GlobalProtect para que use un servicio de autenticación que utilice el esquema de autenticación en dos fases. Un esquema de autenticación en dos fases requiere dos elementos: algo que conozca el usuario final (como un PIN o una contraseña) y algo que el usuario tenga (hardware o de token/OTP, tarjeta inteligente o certificado). También puede habilitar la autenticación en dos fases con una combinación de servicios de autenticación externa y perfiles de cliente y certificado.

Los siguientes temas brindan ejemplos sobre cómo configurar la autenticación en dos fases en GlobalProtect:

- Habilitación de la autenticación en dos fases con perfiles de autenticación y certificado
- Habilitación de la autenticación en dos fases mediante contraseñas de un solo uso (OTP)
- Habilitación de autenticación en dos fases mediante tarjetas inteligentes
- Habilitación de la autenticación de doble factor mediante una aplicación de token de software

Habilitación de la autenticación en dos fases con perfiles de autenticación y certificado

El siguiente flujo de trabajo describe cómo configurar GlobalProtect para solicitar que los usuarios se autentiquen tanto con un perfil de certificado como con un perfil de autenticación. El usuario debe autenticarse correctamente con ambos métodos para poder conectarse al portal/puerta de enlace. Para obtener más detalles sobre esta configuración, consulte el VPN de acceso remoto con la autenticación en dos fases.

STEP 1 | Cree un perfil de servidor de autenticación.

El perfil de servidor de autenticación determina de qué manera el cortafuegos se conecta con un servicio de autenticación externo y recupera las credenciales de autenticación para sus usuarios.

Si usa LDAP para conectarse a Active Directory (AD), debe crear un perfil de servidor LDAP diferente para cada dominio de AD.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** y un tipo de perfil (**LDAP**, **Kerberos**, **RADIUS** o **TACACS+**).
2. Seleccione **Add** para añadir un nuevo perfil.
3. Introduzca un **Profile Name (Nombre de perfil)** como `gp-user-auth`.
4. (Solo LDAP) Seleccione en **Type (Tipo)** el tipo de servidor LDAP (**active-directory [directorio activo]**, **e-directory [directorio electrónico]**, **sun** u **other [otro]**).
5. Haga clic en **Add (Añadir)** en el área de **Servers (Servidores)** o **Servers List (Lista de servidores)** (según el tipo de perfil de servidor) y, luego, introduzca la siguiente información para las conexiones al servicio de autenticación:
   - **Name (Nombre)** del servidor.
   - Dirección IP de FQDN del **Server (Servidor)**
   - **Puerto**
6. (Solo RADIUS, TACACS+ y LDAP) Especifique la siguiente configuración para habilitar la autenticación del cortafuegos en el servicio de autenticación:
   - RADIUS y TACACS+: introduzca el **Secret (Secreto)** compartido al añadir la entrada del servidor.
   - LDAP: introduzca el valor de **Bind DN (DN de enlace)** y **Password (Contraseña)**.

© 2020 Palo Alto Networks, Inc.

7. (Solo LDAP) Si desea que el endpoint use SSL o TLS para una conexión más segura con el servidor del directorio, habilite la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)** (está habilitada por defecto). El protocolo que usa el endpoint depende del **Port (Puerto)** del servidor en la **Server List (Lista de servidores)**:
   - 389 (por defecto): TLS (específicamente, el endpoint usa la operación StartTLS para actualizar la conexión de texto no cifrado inicial a TLS).
   - 636: SSL.
   - Cualquier otro puerto: El endpoint primero intenta usar TLS. Si el servidor de directorio no admite TLS, el endpoint utiliza SSL.
8. (LDAP únicamente) Para mayor seguridad, habilite la opción **Verify Server Certificate for SSL sessions (Verificar el certificado del servidor para las sesiones SSL)** de modo que el endpoint verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar esta verificación, debe seleccionar también la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)**. Para que la verificación se realice correctamente, una de las siguientes condiciones debe ser verdadera:
   - El certificado está en la lista de certificados de dispositivo: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Importe el certificado al endpoint, si fuera necesario.
   - El firmante del certificado está en la lista de autoridades de certificación confiables: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Default Trusted Certificate Authorities (Autoridades de certificados de confianza por defecto)**.
9. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Cree un perfil de autenticación que identifique el servicio para los usuarios de autenticación. Más tarde tendrá la opción de asignar el perfil en el portal y las puertas de enlace.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y haga clic en **Add (Añadir)** para añadir un perfil nuevo.
2. Introduzca un **Name (Nombre)** para el perfil.
3. Seleccione el tipo de **Authentication (Autenticación)** en **Type (Tipo)**.
4. Seleccione el **Server Profile (Perfil de servidor)** que creó en el paso 1.
5. (Solo LDAP) Introduzca **sAMAccountName** como el **Login Attribute (Atributo de inicio de sesión)**.
6. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 3 | Cree un perfil de certificado de cliente para que utilice el portal a fin de autenticar los certificados de cliente que provienen de los endpoints de usuarios.

Cuando configure la autenticación en dos fases para usar certificados de cliente, el servicio de autenticación externa utilizará el valor de nombre de usuario para autenticar al usuario, si se especifica, en el certificado del cliente. De este modo se garantiza que el usuario que se está registrando es en realidad el usuario para el que se emitió el certificado.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y, luego, haga clic en **Add (Añadir)** para añadir un perfil de certificado nuevo.
2. Introduzca un **Name (Nombre)** para el perfil.
3. Seleccione uno de los siguientes valores de **Username Field (Campo de nombre de usuario)**:
   - Si planea que el certificado de cliente autentique a usuarios individuales, seleccione el campo del certificado que identifique al usuario.
   - Si implementa un certificado de cliente desde el portal, seleccione **None (Ninguno)**.

© 2020 Palo Alto Networks, Inc.

- Si configura un perfil de certificado para usarlo con el método de conexión de inicio de sesión previo, seleccione **None (Ninguno)**.

4. Haga clic en **Add (Añadir)** para añadir los **CA Certificates (Certificados de CA)** que desea asignar al perfil y, luego, configure los siguientes ajustes:
   1. Seleccione el **CA certificate (Certificado de CA)**, ya sea un certificado de CA de raíz confiable o el certificado de CA de un servidor SCEP. Si fuera necesario, importe el certificado.
   2. (Opcional) Introduzca la **Default OCSP URL (URL de OCSP predeterminada)**.
   3. (Opcional) Seleccione un certificado para **OCSP Verify Certificate (Certificado de verificación de OCSP)**.
   4. (Opcional) En **Template Name (Nombre de plantilla)**, introduzca el nombre de la plantilla empleada para firmar el certificado.
5. (Opcional) Seleccione las siguientes opciones para especificar cuándo bloquear la sesión solicitada del usuario:
   1. el estado del certificado es desconocido.
   2. El componente de GlobalProtect no recupera el estado del certificado dentro de la cantidad de segundos que se indica en **Certificate Status Timeout (Tiempo de espera de estado de certificado)**.
   3. El atributo de número de serie en el asunto de un certificado de cliente no coincide con el ID de host que la aplicación de GlobalProtect informa para el endpoint.
   4. Los certificados se vencieron.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | (Opcional) Emita certificados de cliente para clientes y endpoints de GlobalProtect.

Para implementar de manera transparente los certificados de cliente, configure su portal para que distribuya un certificado de cliente compartido a los endpoints o configure el portal para que utilice SCEP para solicitar e implementar certificados de cliente únicos para cada usuario.

1. Utilice su PKI empresarial o CA pública para emitir un certificado de cliente para cada usuario de GlobalProtect.
2. Para los métodos de conexión de inicio de sesión previo, instale certificados en el almacén de certificados personales del endpoint.

STEP 5 | Guarde la configuración de GlobalProtect.

Haga clic en **Commit (Confirmar)**.

Habilitación de la autenticación en dos fases mediante contraseñas de un solo uso (OTP)

Utilice este flujo de trabajo para configurar la autenticación en dos fases con contraseñas de un solo uso (one-time passwords, OTP) en el portal y las puertas de enlace. Cuando un usuario solicita el acceso, el portal o la puerta de enlace indica al usuario que introduzca una OTP. El servicio de autenticación envía la OTP como token al dispositivo RSA del usuario.

La configuración de un esquema de autenticación en dos fases es similar a la configuración de otros tipos de autenticación. El esquema de autenticación en dos fases requiere que configure lo siguiente:

- Un perfil de servidor (generalmente para un servicio RADIUS para la autenticación en dos fases) asignado a un perfil de autenticación.
- Un perfil de autenticación de cliente que incluya el perfil de autenticación para el servicio que utilizan estos componentes.

© 2020 Palo Alto Networks, Inc.

Por defecto, la aplicación proporciona las mismas credenciales usadas para el inicio de sesión en el portal y la puerta de enlace. En el caso de la autenticación OTP, este comportamiento hace que la autenticación falle inicialmente en la puerta de enlace y, debido al retraso que esto ocasiona en la solicitud de inicio de sesión al usuario, la OTP del usuario puede caducar. Para evitar esto, usted debe configurar los portales y las puertas de enlace que solicitan la OTP en lugar de usar las mismas credenciales con una configuración basada en cada aplicación.

También puede reducir la frecuencia con la cual los usuarios deben ingresar las OTP al configurar una cancelación de autenticación. Esto permite que los portales y las puertas de enlace generen y acepten una cookie cifrada segura para autenticar al usuario durante un tiempo especificado. Los portales o puertas de enlace no exigen una nueva OTP hasta que la cookie caduque, con lo cual se reduce la cantidad de veces que los usuarios deben proporcionar una OTP.

STEP 1 | Después de haber configurado el servicio RADIUS back-end para generar tokens para las OTP y garantizar que los usuarios tengan todos los dispositivos necesarios (tal como un token de hardware), configure un servidor RADIUS para que interactúe con el cortafuegos.

Puede consultar instrucciones específicas en su servidor RADIUS. En la mayoría de los casos, necesitará configurar un agente de autenticación y una configuración de cliente en el servidor RADIUS para habilitar la comunicación entre el cortafuegos y el servidor RADIUS. También debe definir el secreto compartido que se debe utilizar para cifrar las sesiones entre el cortafuegos y el servidor RADIUS.

STEP 2 | En cada cortafuego que aloja las puertas de enlace o el portal, cree un perfil de servidor RADIUS. (Para una implementación pequeña, un cortafuegos puede alojar el portal y las puertas de enlace).

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **RADIUS**.
2. Seleccione **Add** para añadir un nuevo perfil.
3. Introduzca un **Profile Name (Nombre de perfil)** para este perfil de RADIUS.
4. En el área **Servers (Servidores)**, seleccione **Add (Añadir)** para añadir una instancia de RADIUS y, luego, introduzca lo siguiente:
   - Un nombre descriptivo en **Name (Nombre)** para identificar este servidor RADIUS.
   - La dirección IP del **RADIUS Server (Servidor RADIUS)**.
   - El **Secret (Secreto)** compartido para cifrar sesiones entre el cortafuegos y el servidor RADIUS.
   - El número de **Port (Puerto)** desde el que el servidor RADIUS detecta las solicitudes de autenticación (por defecto, 1812)
5. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Cree un perfil de autenticación.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y luego **Add (Añadir)** para añadir un nuevo perfil.
2. Introduzca un **Name (Nombre)** para el perfil. El nombre no puede contener espacios.
3. Seleccione **RADIUS** como el tipo de servicio de autenticación en **Type (Tipo)**.
4. Seleccione el **Server Profile (Perfil de servidor)** que ha creado para acceder a su servidor RADIUS.
5. Introduzca el nombre de **User Domain (Dominio de usuario)**. El cortafuegos utiliza este valor para hacer coincidir los usuarios de autenticación con las entradas de la Lista de permitidas y para la asignación de grupos de User-ID.
6. Seleccione un **Username Modifier (Modificador de nombre de usuario)** para modificar el formato de nombre de usuario/dominio que espera el servidor RADIUS.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Asigne el perfil de autenticación a un portal o puerta de enlace de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Usted puede establecer varias configuraciones de autenticación de cliente para el portal y las puertas de enlace. Para cada configuración de autenticación de cliente, usted puede especificar el perfil de autenticación que se aplicará a los endpoints de un SO específico.

Este paso describe cómo añadir el perfil de autenticación a la configuración de puerta de enlace o portal. Para obtener más información sobre cómo configurar estos componentes, consulte Portales de GlobalProtect y Puertas de enlace de GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** o **Gateways (Puertas de enlace)**.
2. Seleccione una configuración de puerta de enlace o portal existente o haga clic en **Add (Añadir)** para añadir una nueva. Si añade un nuevo portal o puerta de enlace, especifique el nombre, la ubicación y los parámetros de red.
3. En la pestaña **Authentication (Autenticación)**, seleccione un **SSL/TLS service Profile (Perfil de servicio SSL/TLS** o **Add** para añadir un nuevo perfil.
4. Haga clic en **Add (Añadir)** para añadir una nueva configuración de **Client Authentication (Autenticación de cliente)** y, luego, configure los siguientes ajustes:
   - Introduzca un nombre en **Name (Nombre)** para la configuración de autenticación del cliente.
   - Seleccione el **OS (SO)** del endpoint al cual se aplica esta configuración.
   - Seleccione el **Authentication Profile (Perfil de autenticación)** que creó en Creación de un perfil de autenticación.
   - (Opcional) Una **Username Label (Etiqueta de nombre de usuario)** personalizada.
   - (Opcional) Una **Password Label (Etiqueta de contraseña)** personalizada.
   - (Opcional) Un **Authentication Message (Mensaje de autenticación)** personalizado.
5. Haga clic en **OK (Aceptar)** para guardar la configuración.

STEP 5 | (Opcional) Configure el portal o las puertas de enlace para que soliciten un nombre de usuario y contraseña, o solo una contraseña, cada vez que el usuario inicie sesión. La autenticación en dos fases no admite la opción de guardar la contraseña con OTP, ya que el usuario debe introducir una contraseña dinámica cada vez que inicia sesión.

Este paso describe cómo configurar el ajuste de contraseña en una configuración de agente de portal. Para obtener detalles adicionales, consulte Personalización de la aplicación de GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y luego seleccione una configuración del portal existente.
2. En el diálogo GlobalProtect Portal Configuration (Configuración del portal de GlobalProtect), seleccione **Agent (Agente)**.
3. Seleccione una configuración de agente existente o haga clic en **Add (Añadir)** para añadir una nueva.
4. En la pestaña **Authentication (Autenticación)**, configure **Save User Credentials (Guardar credencales de usuario)** en **Save Username Only (Guardar solo el nombre de usuario)** o en **No**. Este ajuste permite que GlobalProtect solicite a los usuarios contraseñas dinámicas para cada componente que usted seleccione en el paso siguiente.
5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.

STEP 6 | Seleccione los componentes de GlobalProtect (portal y tipos de puertas de enlace) que solicitarán contraseñas dinámicas, tales como OTP.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y luego seleccione una configuración del portal existente.
2. En el diálogo GlobalProtect Portal Configuration (Configuración del portal de GlobalProtect), seleccione **Agent (Agente)**.
3. Seleccione una configuración de agente existente o haga clic en **Add (Añadir)** para añadir una nueva.
4. Seleccione la pestaña **Authentication (Autenticación)** y luego seleccione los **Components that Require Dynamic Passwords (Two-Factor Authentication) (Componentes que requieren contraseñas**

© 2020 Palo Alto Networks, Inc.

dinámicas [autenticación en dos fases]). Cuando se seleccionan, el portal y los tipos de puertas de enlace solicitan OTP.

No seleccione la opción Components that Require Dynamic Passwords (Two-Factor Authentication) (Componentes que requieren contraseñas dinámicas (autenticación de dos factores)) para los componentes que usan la autenticación SAML.

5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.

STEP 7 | Si el inicio de sesión único (single sign-on, SSO) está activado, desactívelo. Debido a que la configuración del agente especifica RADIUS como el servicio de autenticación, el SSO de Kerberos no es compatible.

Este paso describe cómo desactivar el SSO. Para obtener detalles adicionales, consulte Definición de las configuraciones del agente de GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y luego seleccione una configuración del portal existente.
2. En el diálogo GlobalProtect Portal Configuration (Configuración del portal de GlobalProtect), seleccione **Agent (Agente)**.
3. Seleccione una configuración de agente existente o haga clic en **Add (Añadir)** para añadir una nueva.
4. En la pestaña **App (Aplicación)**, configure **Use Single Sign-on (Windows Only) (Usar inicio de sesión único [Solo Windows])** en **No**.
5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.

STEP 8 | (Opcional) Para minimizar la cantidad de veces que un usuario debe proporcionar credenciales, configure una cancelación de autenticación.

Por defecto, el portal o las puertas de enlace autentican al usuario con un perfil de autenticación y un perfil de certificado opcional. Con la cancelación de autenticación, el portal o la puerta de enlace autentican al usuario con una cookie cifrada que se implementó en el endpoint. Mientras la cookie sea válida, el usuario puede iniciar sesión sin introducir credenciales habituales o una OTP. Para más información, consulte Autenticación de cookies en el portal o la puerta de enlace.

Si debe bloquear de inmediato el acceso a un endpoint cuya cookie todavía no caducó (por ejemplo, en caso de pérdida o robo del endpoint), puede bloquear el acceso del endpoint *añadiendo el dispositivo a una lista de bloqueo.*

Para obtener más información, consulte Portales de GlobalProtect y Puertas de enlace de GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** o **Gateways (Puertas de enlace)**.
2. Seleccione una configuración de puerta de enlace o portal existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. Dependiendo de si configura un portal o una puerta de enlace, seleccione una de las siguientes opciones:
   - **Configuración del portal de GlobalProtect**: en el cuadro de diálogo GlobalProtect Portal Configuration (Configuración del portal de GlobalProtect), seleccione **Agent (Agente)** > <*agent-config*> > **Authentication (Autenticación)**.
   - **Configuración de la puerta de enlace de GlobalProtect**: en el diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)** > <*client-setting*> > **Authentication Override (Cancelación de la autenticación)**.
4. Configure los siguientes ajustes **Authentication Override (Cancelación de autenticación)**.
   - **Name (Nombre)** de la cancelación de autenticación.

© 2020 Palo Alto Networks, Inc.

- **Generate cookie for authentication override (Generar cookie para la cancelación de autenticación)**: habilita el portal o la puerta de enlace para que generen cookies cifradas específicas del endpoint. Una vez que los usuarios se autentiquen correctamente, el portal o la puerta de enlace emitirán una cookie de autenticación para el endpoint.

  La cookie de autenticación incluye los siguientes campos:

  - `user (usuario)`: nombre de usuario que se utiliza para autenticar al usuario.
  - `domain (dominio)`: nombre de dominio del usuario.
  - `os (so)`: nombre de la aplicación que se utiliza en el dispositivo.
  - `hostID (ID de host)`: ID único asignado por GlobalProtect para identificar el host.
  - `gen time (fecha/hora de generación)`: fecha y hora en que se generó la cookie de autenticación.
  - `ip`: dirección IP del dispositivo que se utiliza para autenticarse correctamente en GlobalProtect y obtener la cookie.
- **Accept cookie for authentication override (Aceptar cookie para la anulación de autenticación)**: indica al portal o puerta de enlace que autentique al usuario mediante una cookie válida y cifrada. Cuando el endpoint presenta una cookie válida, el portal o la puerta de enlace verifican que la cookie fue cifrada por el portal o la puerta de enlace, descifra la cookie y luego autentica al usuario.

  La aplicación de GlobalProtect debe conocer el nombre del usuario que realiza la conexión para cotejar y recuperar las cookies de autenticación asociadas de su terminal. Después de recuperarlas, las envía al portal o a la puerta de enlace para proceder a la autenticación del usuario.

  (Solo Windows) Si establece la opción Use Single Sign-On (Usar inicio de sesión único) en Yes (Sí) (SSO habilitado) en la configuración del agente del portal (Network (Red) > GlobalProtect > Portals (Portales) > <portal-config> > Agent (Agente) > <agent-config> > App (Aplicación)), la aplicación de GlobalProtect utiliza el nombre de usuario de Windows para recuperar la cookie de autenticación local para el usuario. Si especifica No en Use Single Sign-On (Usar inicio de sesión único), deshabilita SSO, por lo que debe habilitar la opción Save User Credentials (Guardar credenciales de usuarios) en la aplicación de GlobalProtect para que esta recupere la cookie de autenticación del usuario. Configure la opción Save User Credentials (Guardar credenciales de usuarios) en Yes (Sí) para guardar tanto el nombre de usuario como la contraseña o bien seleccione Save Username Only (Guardar solo nombre de usuario) para guardar únicamente el primero.

  (Solo en macOS) Como los endpoints con macOS no admiten SSO, debe habilitar la opción Save User Credentials (Guardar credenciales de usuarios) en la aplicación de GlobalProtect para que esta recupere la cookie de autenticación del usuario. Configure la opción Save User Credentials (Guardar credenciales de usuarios) en Yes (Sí) para guardar tanto el nombre de usuario como la contraseña o bien seleccione Save Username Only (Guardar solo nombre de usuario) para guardar únicamente el primero.
- **Cookie Lifetime (Duración de la cookie)**: especifica las horas, días o semanas que la cookie es válida. El periodo de validez típico es de 24 horas para las puertas de enlace (que protegen información confidencial) o de 15 días para el portal. El intervalo de horas es de 1 a 72; para las semanas, de 1 a 52 y para los días, de 1 a 365. Después de que la cookie caduca en el portal o la puerta de enlace (según lo que ocurra primero), el portal o la puerta de enlace solicitan al usuario que se autentique y posteriormente cifran una nueva cookie para enviar al endpoint.

© 2020 Palo Alto Networks, Inc.

- **Certificate to Encrypt/Decrypt Cookie (Certificado para cifrar/descifrar la cookie)**: especifica el certificado que se debe usar para cifrar o descifrar la cookie. Usted debe usar el mismo certificado en el portal y las puertas de enlace.

  Se recomienda configurar el certificado RSA para que utilice el algoritmo de resumen más fuerte que su red admite.

  El portal y las puertas de enlace utilizan el esquema de relleno de cifrado RSA PKCS#1 V1.5 para generar la cookie (usando la clave pública del certificado) y descifrar la cookie (usando la clave privada del certificado).

5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.

STEP 9 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 10 | Verifique la configuración.

Desde un endpoint que ejecute la aplicación de GlobalProtect, trate de conectarse a una puerta de enlace o portal en el que haya habilitado la autenticación con OTP. Debería ver mensajes parecidos a estos:

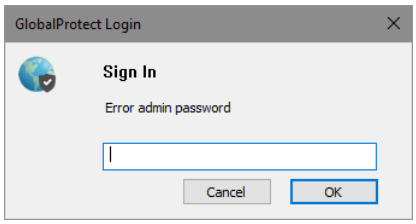


Figure 1: Mensaje emergente de OTP

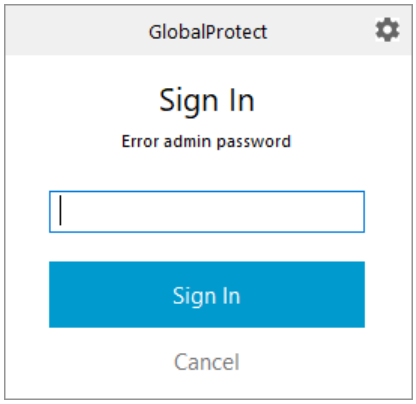


Figure 2: Mensaje de OTP en el panel de estado de GlobalProtect

Habilitación de autenticación en dos fases mediante tarjetas inteligentes

Si desea habilitar a sus usuarios finales para que se autentiquen con una tarjeta inteligente o una tarjeta de acceso común (common access card, CAC), debe importar el certificado de CA raíz que emitió los certificados contenidos en las CAC o tarjetas inteligentes en el portal y la puerta de enlace. Puede crear un perfil de certificado que incluya esa CA raíz y la aplique a sus configuraciones de portal o puerta de enlace para habilitar el uso de tarjetas inteligentes en el proceso de autenticación.

STEP 1 | Configure su infraestructura para tarjetas inteligentes

© 2020 Palo Alto Networks, Inc.

Este procedimiento da por hecho que ha facilitado tarjetas inteligentes y lectores de tarjetas inteligentes a sus usuarios finales.

Puede consultar instrucciones específicas en la documentación del software del proveedor de autenticación.

En la mayoría de los casos, la configuración de la infraestructura para tarjetas inteligentes implica la generación de certificados para los usuarios finales y los servidores participantes, que en este caso son el portal y las puertas de enlace de GlobalProtect.

STEP 2 | Importe el certificado de la CA raíz que emitió los certificados de cliente contenidos en las tarjetas inteligentes de los usuarios finales.

Asegúrese de que se puede acceder al certificado desde su sistema de gestión y siga estos pasos:

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Import (Importar)** para importar un certificado.
2. Introduzca un **Certificate Name (Nombre de certificado)**.
3. Introduzca la ruta y el nombre del **Certificate File (Archivo de certificado)** que recibió de la CA o seleccione **Browse (Examinar)** para buscar el archivo.
4. Seleccione **Base64 Encoded Certificate (PEM) (Certificado codificado en Base64 [PEM])** en la lista desplegable **File Format (Formato de archivo)** y haga clic en **OK (Aceptar)** para importar el certificado.

STEP 3 | Cree el perfil de certificado en cada portal/puerta de enlace en la que planee usar autenticación con tarjeta inteligente o CAC.

Consulte la ayuda en línea para obtener detalles de otros campos de perfil de certificado, como si debe usar CRL u OCSP.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**.
2. Seleccione un perfil de certificado existente o haga clic en **Add (Añadir)** para añadir uno nuevo.
3. Introduzca un **Name (Nombre)** para el perfil de certificados.
4. En el campo **Username (Nombre de usuario)**, del certificado que PAN-OS usa para comparar la dirección IP del ID de usuario, ya sea **Subject (Asunto)** para usar un nombre común, **Subject Alt (Asunto alternativo): Email (Correo electrónico)** para usar una dirección de correo electrónico o **Subject Alt (Asunto alternativo): Principal Name** para usar el nombre principal.
5. En el área **CA Certificates (Certificados de CA)**, haga clic en **Add (Añadir)** para añadir el certificado de CA raíz de confianza que importó en el paso anterior al perfil del certificado. Cuando se le indique, seleccione el **CA Certificate (Certificado de CA)** y haga clic en **OK (Aceptar)**.
6. Haga clic en **OK (Aceptar)** para guardar el perfil del certificado.

STEP 4 | Asigne el perfil de certificado a un portal o puerta de enlace. Este paso describe cómo añadir el perfil de certificado a la configuración de puerta de enlace o portal. Para obtener detalles sobre cómo configurar estos componentes, consulte Portales de GlobalProtect y Puertas de enlace de GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** o **Gateways (Puertas de enlace)**.
2. Seleccione una configuración de puerta de enlace o portal existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En el diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione **Authentication (Autenticación)**.
4. Seleccione el **Certificate Profile (Perfil de certificado)** que acaba de crear.

© 2020 Palo Alto Networks, Inc.

5. Haga clic en **OK (Aceptar)** para guardar la configuración.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 6 | Verifique la configuración.

Desde un endpoint que ejecute la aplicación de GlobalProtect, trate de conectarse a una puerta de enlace o portal en el que haya configurado la autenticación con tarjetas inteligentes. Cuando se le indique, inserte su tarjeta inteligente y compruebe que puede autenticarse correctamente en GlobalProtect.

Habilitación de la autenticación de doble factor mediante una aplicación de token de software

Si su empresa utiliza una aplicación de token de software (token flexible), como SecurID RSA, para implementar la autenticación de dos factores, los usuarios deben abrir primero su aplicación de token de software y especificar su PIN para obtener un código de acceso y, después, introducir el código de acceso en su aplicación de GlobalProtect en el campo **Password (Contraseña)**. Este proceso de dos pasos complica el proceso de inicio de sesión.

Para simplificar el proceso de inicio de sesión y mejorar la experiencia de los usuarios, GlobalProtect ofrece autenticación de token flexible sin interrupciones. El usuario especifica el PIN RSA en el campo **Password (Contraseña)** de GlobalProtect y GlobalProtect recupera el código de acceso RSA y continúa con la conexión sin que el usuario realice el paso adicional de abrir la aplicación RSA.

Esta característica es compatible con los tres modos RSA: Estilo PinPad (PIN integrado con código de token), estilo Fob (llave) (PIN seguido de código de token) y modo Pinless (sin PIN). Para los estilos PinPad y Fob, el usuario especifica el PIN en el campo **Password (Contraseña)** y GlobalProtect recupera el código de acceso. En el modo Pinless (sin PIN), el campo Password (Contraseña) está atenuado y los usuarios especifican su nombre de usuario.

Esta función es compatible con dispositivos Windows a partir de la aplicación de GlobalProtect ™ 5.1.

STEP 1 | Cambie las claves de registro en los dispositivos Windows del cliente para habilitar la autenticación de token flexible sin interrupciones.

Debe cambiar el Registro de Windows en los dispositivos Windows de los clientes para habilitar la autenticación de token flexible sin interrupciones. GlobalProtect recupera esta entrada de registro solo una vez, cuando se inicializa la aplicación de GlobalProtect.

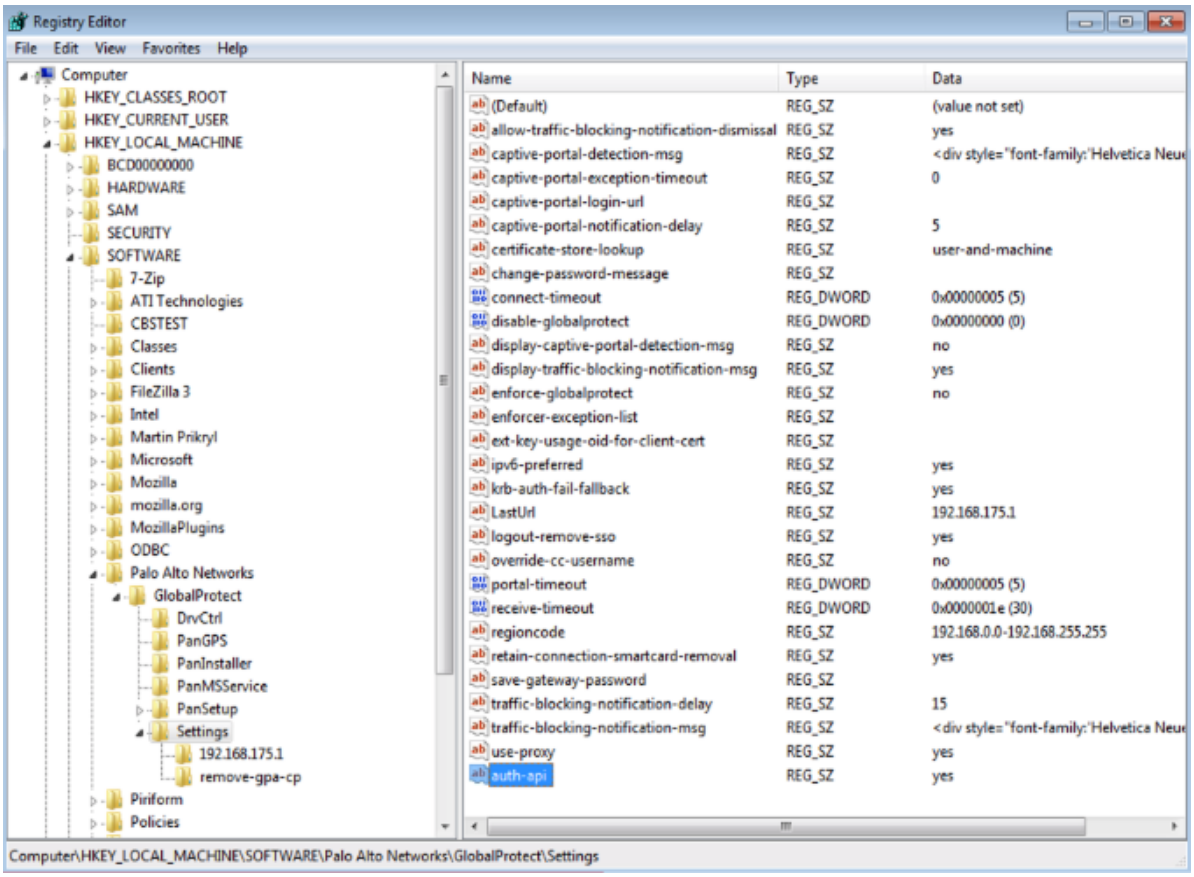
1. Abra el Editor de Registro de Windows y seleccione **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Palo Alto Networks** > **GlobalProtect** > **Settings (Configuración)**.
2. Cambie el valor **auth-api** a **yes**.

Con auth-api establecido en yes en la máquina de cliente, debe configurar el portal y las puertas de enlace con la autenticación basada en RSA. No se admite ningún otro perfil de autenticación porque GlobalProtect intentará recuperar el código de acceso.

Debido a que el portal y la puerta de enlace utilizan la autenticación RSA, le recomendamos que habilite la autenticación basada en cookies en las puertas de enlace. El token que se recupera para el portal puede seguir activo cuando GlobalProtect intenta obtener el código de acceso para la puerta de enlace, y la autenticación puede fallar porque el código de acceso ya se ha usado. Por lo tanto, le

© 2020 Palo Alto Networks, Inc.

sugerimos que genere una cookie de anulación de autenticación en el portal y acepte la cookie en la puerta de enlace.



STEP 2 | Configure el portal y la puerta de enlace con autenticación basada en RSA.

STEP 3 | Habilite la autenticación basada en cookies en el portal GlobalProtect.

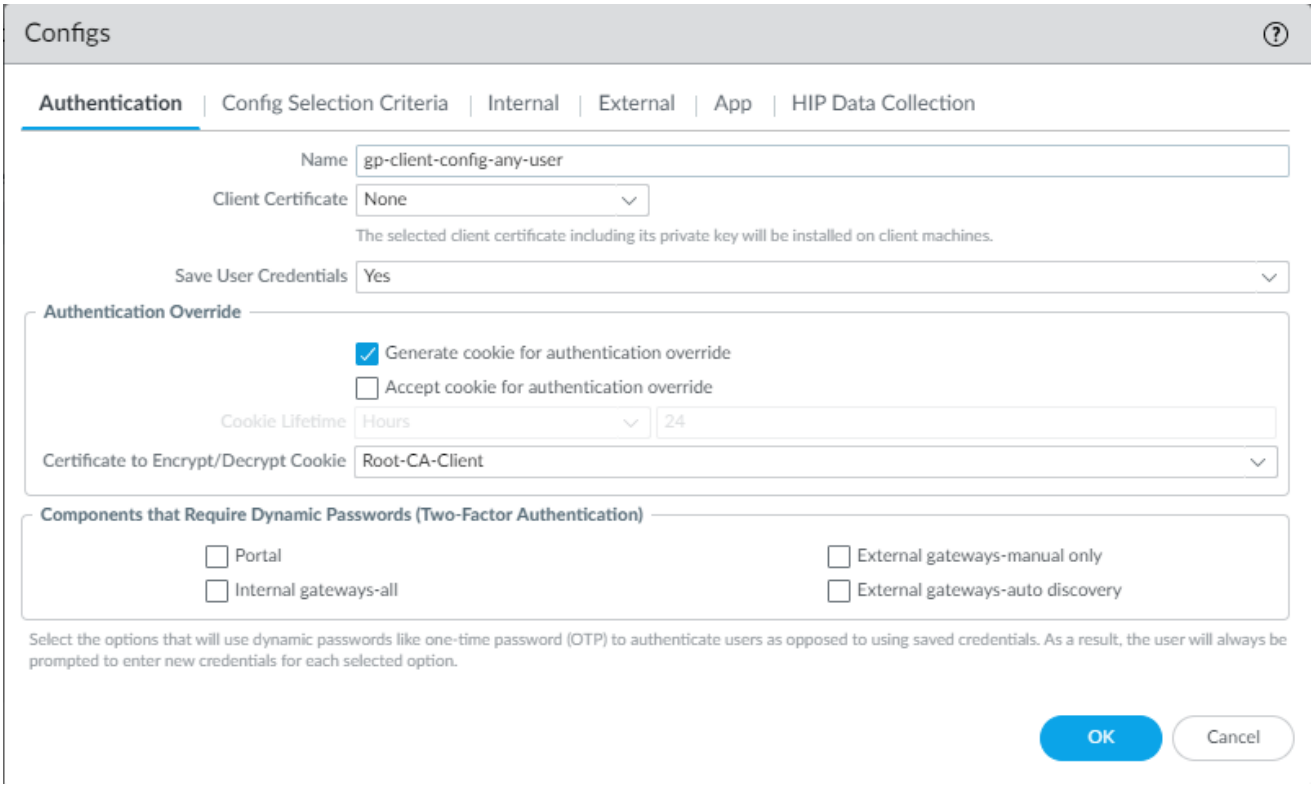
La especificación de GlobalProtect para anular una autenticación existente permite que GlobalProtect sobrescriba una contraseña existente con una contraseña recién creada.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>*; a continuación, seleccione la pestaña **Agent** (Agente).
2. **Añada** una configuración de agente o seleccione una existente.
3. Seleccione **Generate cookie for authentication override (Generar cookie para cancelación de autenticación)**.

   La cookie de autenticación incluye los siguientes campos:

   - `user (usuario)`: nombre de usuario que se utiliza para autenticar al usuario.
   - `domain (dominio)`: nombre de dominio del usuario.
   - `os (so)`: nombre de la aplicación que se utiliza en el dispositivo.
   - `hostID (ID de host)`: ID único asignado por GlobalProtect para identificar el host.
   - `gen time (fecha/hora de generación)`: fecha y hora en que se generó la cookie de autenticación.
   - `ip`: dirección IP del dispositivo que se utiliza para autenticarse correctamente en GlobalProtect y obtener la cookie.

© 2020 Palo Alto Networks, Inc.



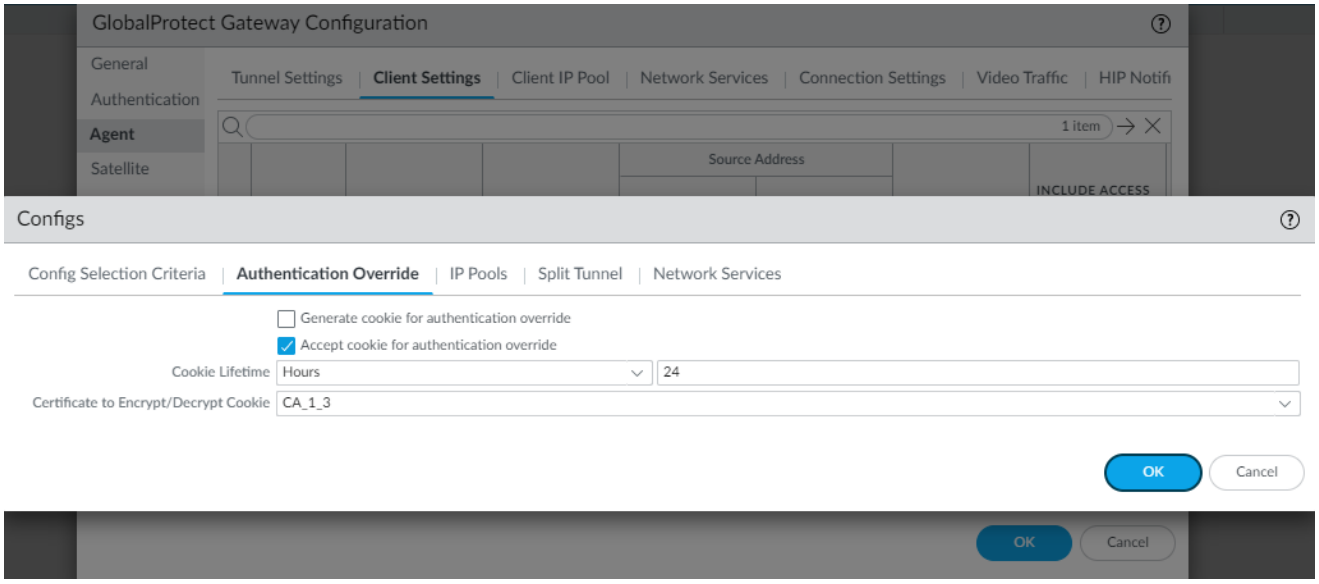
STEP 4 | Habilite la puerta de enlace de GlobalProtect para aceptar cookies para anulaciones de autenticación.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway>* y seleccione la pestaña **Agent (Agente)**.
2. Seleccione **Client Settings (Configuración de cliente)** y, a continuación, elija la configuración de cliente de GlobalProtect o añada una nueva.
3. Seleccione **Authentication Override (Anulación de autenticación)**; a continuación, elija **Accept cookie for authentication override (Aceptar cookie para anulación de autenticación)**.

   La cookie de autenticación incluye los siguientes campos:

   - `user (usuario)`: nombre de usuario que se utiliza para autenticar al usuario.
   - `domain (dominio)`: nombre de dominio del usuario.
   - `os (so)`: nombre de la aplicación que se utiliza en el dispositivo.
   - `hostID (ID de host)`: ID único asignado por GlobalProtect para identificar el host.
   - `gen time (fecha/hora de generación)`: fecha y hora en que se generó la cookie de autenticación.
   - `ip`: dirección IP del dispositivo que se utiliza para autenticarse correctamente en GlobalProtect y obtener la cookie.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>*; a continuación, seleccione la pestaña **Authentication** (Autenticación).

STEP 6 | **Añada** un nuevo perfil de autenticación de cliente o seleccione uno existente; luego, elija **Automatically retrieve passcode from SoftToken application (Recuperar automáticamente el código de acceso de la aplicación SoftToken)**.

© 2020 Palo Alto Networks, Inc.

Client Authentication

Name: Local

OS: Any

Authentication Profile: Local

☑ Automatically retrieve passcode from SoftToken application

GlobalProtect App Login Screen

Username Label: Username

Password Label: Password

Authentication Message: Enter login credentials

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate: No (User Credentials AND Client Certificate Required)

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

OK | Cancel

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación para endpoints strongSwan Ubuntu y CentOS

Para extender el acceso de GlobalProtect a los endpoints de strongSwan Ubuntu y CentOS, configure la autenticación para estos endpoints.

Para ver la versión de lanzamiento mínima de GlobalProtect que es compatible con strongSwan en Ubuntu Linux y CentOS, consulte ¿Qué versiones de sistema operativo son compatibles con GlobalProtect?

Para conectarse a la puerta de enlace de GlobalProtect, el usuario debe autenticarse correctamente. Los siguientes flujos de trabajo muestran ejemplos sobre cómo habilitar la autenticación en los endpoints de strongSwan. Para obtener información completa sobre strongSwan, consulte la wiki de strongSwan.

- Habilitación de la autenticación con un perfil de certificado
- Habilitación de la autenticación con un perfil de autenticación
- Habilitación de la autenticación con una autenticación en dos fases

Habilitación de la autenticación con un perfil de certificado

El siguiente flujo de trabajo muestra cómo habilitar la autenticación para clientes strongSwan con un perfil de certificado.

STEP 1 | Configure un túnel IPsec para que la puerta de enlace de GlobalProtect se comunique con un cliente strongSwan.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**.
2. Seleccione una puerta de enlace existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Authentication (Autenticación)** del diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione el **Certificate Profile (Perfil del certificado)** que desea usar para la autenticación.
4. Seleccione **Agent (Agente)** > **Tunnel Settings (Ajustes del túnel)** para habilitar **Tunnel Mode (Modo de túnel)** y especifique los siguientes ajustes para configurar el túnel:
   - Seleccione la casilla de verificación **Enable X-Auth Support (Habilitar compatibilidad con X-Auth)**.
   - Si ya configuró un **Group Name (Nombre de grupo)** y hay una **Group Password (Contraseña de grupo)** ya configurada, elimínelas.
   - Haga clic en **OK (Aceptar)** para guardar los ajustes.

STEP 2 | Verifique que los ajustes de la conexión predeterminada en la sección `conn %default` del archivo de configuración del túnel IPsec (`ipsec.conf`) estén correctamente definidos para el cliente strongSwan.

El archivo ipsec.conf generalmente se encuentra en la carpeta /etc.

Las configuraciones de este procedimiento se analizan y verifican para las siguientes versiones:

- *Ubuntu 14.0.4 con strongSwan 5.1.2 y CentOS 6.5 con strongSwan 5.1.3 para PAN-OS 6.1.*
- *Ubuntu 14.0.4 con strongSwan 5.2.1 para PAN-OS 7.0.*

© 2020 Palo Alto Networks, Inc.

Las configuraciones en este procedimiento se pueden usar para referencia si está usando una versión diferente de strongSwan. Consulte la wiki de strongSwan para obtener más información.

Modifique los siguientes ajustes en la sección `conn %default` del archivo `ipsec.conf` con estos ajustes recomendados.

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | Modifique el archivo de configuración IPsec del cliente strongSwan (**`ipsec.conf`**) y el archivo de contraseña IPsec (**`ipsec.secrets`**) para que usen los ajustes recomendados.

El archivo ipsec.secrets generalmente se encuentra en la carpeta /etc.

Use el nombre de usuario de cliente de strongSwan como el nombre común del certificado.

Modifique los siguientes elementos del archivo `ipsec.conf` con estos ajustes recomendados.

```
conn <connection name>
keyexchange=ikev1
authby=rsasig
ike=aes-sha1-modp1024,aes256
left=<strongSwan/Linux-client-IP-address>
leftcert=<client certificate with the strongSwan client username used as the
 certificate's common name>
leftsourceip=%config
leftauth2=xauth
right=<GlobalProtect-Gateway-IP-address>
rightid="CN=<Subject-name-of-gateway-certificate>"
rightsubnet=0.0.0.0/0
auto=add
```

Modifique los siguientes elementos del archivo `ipsec.conf` con estos ajustes recomendados.

```
:RSA
<private key file> "<passphrase if used>"
```

STEP 4 | Inicie los servicios IPsec de strongSwan y conéctese al túnel IPsec que desea que el cliente strongSwan use cuando se autentica en la puerta de enlace de GlobalProtect.

Use la variable `config <name>` para nombrar la configuración de túnel.

- Ubuntu:

```
ipsec start
ipsec up <name>
```

- CentOS:

© 2020 Palo Alto Networks, Inc.

```
strongSwan start
strongswan up <name>
```

STEP 5 | Verifique que el túnel esté configurado correctamente y que la conexión VPN se haya establecido en el cliente strongSwan y la puerta de enlace GlobalProtect.

1. Verifique la información de estado detallada sobre una conexión específica (al nombrar la conexión) o verifique la información de estado para todas las conexiones desde el cliente strongSwan:
   - Ubuntu:

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS:

     ```
     strongswan statusall [<connection name>]
     ```

2. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**. En la columna **Info (información)**, seleccione **Remote Users (Usuarios remotos)** de la puerta de enlace configurada para la conexión con el cliente strongSwan. El cliente de strongSwan debe aparecer en **Current Users (Usuarios actuales)**.

Habilitación de la autenticación con un perfil de autenticación

El siguiente flujo de trabajo muestra cómo habilitar la autenticación para clientes strongSwan con un perfil de autenticación. El perfil de autenticación especifica qué perfil de servidor debe utilizarse para autenticar clientes strongSwan.

STEP 1 | Configure el túnel IPsec que la puerta de enlace de GlobalProtect usará para comunicarse con un cliente strongSwan.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**.
2. Seleccione una puerta de enlace existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Authentication (Autenticación)** del diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione el **Authentication Profile (Perfil de autenticación)** que desea usar.
4. Seleccione **Agent (Agente)** > **Tunnel Settings (Ajustes del túnel)** para habilitar **Tunnel Mode (Modo de túnel)** y especifique los siguientes ajustes para configurar el túnel:
   - Seleccione la casilla de verificación **Enable X-Auth Support (Habilitar compatibilidad con X-Auth)**.
   - Ingrese un **Group Name (Nombre de grupo)** y **Group Password (Contraseña de grupo)** si todavía no están configurados.
   - Haga clic en **OK (Aceptar)** para guardar la configuración de estos túneles.

STEP 2 | Verifique que los ajustes de la conexión predeterminada en la sección **`conn %default`** del archivo de configuración del túnel IPsec (**`ipsec.conf`**) estén correctamente definidos para el cliente strongSwan.

El archivo ipsec.conf generalmente se encuentra en la carpeta /etc.

Las configuraciones de este procedimiento se analizan y verifican para las siguientes versiones:

- *Ubuntu 14.0.4 con strongSwan 5.1.2 y CentOS 6.5 con strongSwan 5.1.3 para PAN-OS 6.1.*

© 2020 Palo Alto Networks, Inc.

- *Ubuntu 14.0.4 con strongSwan 5.2.1 para PAN-OS 7.0.*

  Las configuraciones en este procedimiento se pueden usar para referencia si está usando una versión diferente de strongSwan. Consulte la wiki de strongSwan para obtener más información.

En la sección `conn %default` del archivo `ipsec.conf`, configure los siguientes ajustes recomendados.

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | Modifique el archivo de configuración IPsec del cliente strongSwan (**`ipsec.conf`**) y el archivo de contraseña IPsec (**`ipsec.secrets`**) para que usen los ajustes recomendados.

El archivo ipsec.secrets generalmente se encuentra en la carpeta /etc.

Use el nombre de usuario de cliente de strongSwan como el nombre común del certificado.

Configure los siguientes ajustes recomendados en el archivo ipsec.conf:

```
conn <connection name>
keyexchange=ikev1
ikelifetime=1440m
keylife=60m
aggressive=yes
ike=aes-sha1-modp1024,aes256
esp=aes-sha1
xauth=client
left=<strongSwan/Linux-client-IP-address>
leftid=@#<hex of Group Name configured in the GlobalProtect gateway>
leftsourceip=%modeconfig
leftauth=psk
rightauth=psk
leftauth2=xauth
right=<gateway-IP-address>
rightsubnet=0.0.0.0/0
xauth_identity=<LDAP username>
auto=add
```

Configure los siguientes ajustes recomendados en el archivo ipsec.secrets:

```
: PSK <Group Password configured in the gateway>
 <username> : XAUTH "<user password>"
```

STEP 4 | Inicie los servicios IPsec de strongSwan y conéctese al túnel IPsec que desea que el cliente strongSwan use cuando se autentica en la puerta de enlace de GlobalProtect.

- Ubuntu:

```
ipsec start
```


© 2020 Palo Alto Networks, Inc.

```
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | Verifique que el túnel esté configurado correctamente y que la conexión VPN se haya establecido en el cliente strongSwan y la puerta de enlace GlobalProtect.

1. Verifique la información de estado detallada sobre una conexión específica (al nombrar la conexión) o verifique la información de estado para todas las conexiones desde el cliente strongSwan:
   - Ubuntu:

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS:

     ```
     strongswan statusall [<connection name>]
     ```

2. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**. En la columna **Info (información)**, seleccione **Remote Users (Usuarios remotos)** de la puerta de enlace configurada para la conexión con el cliente strongSwan. El cliente de strongSwan debe aparecer en **Current Users (Usuarios actuales)**.

Habilitación de la autenticación con una autenticación en dos fases

Con la autenticación en dos fases, el cliente de strongSwan debe autenticarse correctamente al usar tanto un perfil de certificado como un perfil de autenticación para poder conectar con la puerta de enlace de GlobalProtect. El siguiente flujo de trabajo muestra cómo habilitar la autenticación para clientes strongSwan con un perfil de autenticación en dos fases.

STEP 1 | Configure el túnel IPsec que la puerta de enlace de GlobalProtect usará para comunicarse con un cliente strongSwan.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**.
2. Seleccione una puerta de enlace existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Authentication (Autenticación)** del diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione el **Certificate Profile (Perfil del certificado)** y **Authentication Profile (Perfil de autenticación)** que desea usar.
4. Seleccione **Agent (Agente)** > **Tunnel Settings (Ajustes del túnel)** para habilitar **Tunnel Mode (Modo de túnel)** y especifique los siguientes ajustes para configurar el túnel:
   - Seleccione la casilla de verificación **Enable X-Auth Support (Habilitar compatibilidad con X-Auth)**.
   - Si ya configuró un **Group Name (Nombre de grupo)** y hay una **Group Password (Contraseña de grupo)** ya configurada, elimínelas.
   - Haga clic en **OK (Aceptar)** para guardar la configuración de estos túneles.

STEP 2 | Verifique que los ajustes de la conexión predeterminada en la sección **`conn %default`** del archivo de configuración del túnel IPsec (**`ipsec.conf`**) estén correctamente definidos para el cliente strongSwan.

El archivo ipsec.conf generalmente se encuentra en la carpeta /etc.

© 2020 Palo Alto Networks, Inc.

Las configuraciones de este procedimiento se analizan y verifican para las siguientes versiones:

- *Ubuntu 14.0.4 con strongSwan 5.1.2 y CentOS 6.5 con strongSwan 5.1.3 para PAN-OS 6.1.*
- *Ubuntu 14.0.4 con strongSwan 5.2.1 para PAN-OS 7.0.*

Utilice las configuraciones de este procedimiento como referencia si está usando una versión diferente de strongSwan. Consulte la wiki de strongSwan para obtener más información.

Configure los siguientes ajustes recomendados en el archivo ipsec.conf:

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | Modifique el archivo de configuración IPsec del cliente strongSwan (**`ipsec.conf`**) y el archivo de contraseña IPsec (**`ipsec.secrets`**) para que usen los ajustes recomendados.

El archivo ipsec.secrets generalmente se encuentra en la carpeta /etc.

Use el nombre de usuario de cliente de strongSwan como el nombre común del certificado.

Configure los siguientes ajustes recomendados en el archivo ipsec.conf:

```
conn <connection name>
keyexchange=ikev1
authby=xauthrsasig
ike=aes-sha1-modp1024
esp=aes-sha1
xauth=client
left=<strongSwan/Linux-client-IP-address>
leftcert=<client-certificate-without-password>
leftsourceip=%config
right=<GlobalProtect-gateway-IP-address>
rightid=%anyCN=<Subject-name-of-gateway-cert>”
rightsubnet=0.0.0.0/0
leftauth2=xauth
xauth_identity=<LDAP username>
auto=add
```

Configure los siguientes ajustes recomendados en el archivo ipsec.secrets:

```
<username> :XAUTH “<user password>”
::RSA <private key file> “<passphrase if used>”
```

STEP 4 | Inicie los servicios IPsec de strongSwan y conéctese al túnel IPsec que desea que el cliente strongSwan use cuando se autentica en la puerta de enlace de GlobalProtect.

- Ubuntu:

© 2020 Palo Alto Networks, Inc.

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | Verifique que el túnel esté configurado correctamente y que la conexión VPN se haya establecido en el cliente strongSwan y la puerta de enlace GlobalProtect.

1. Verifique la información de estado detallada sobre una conexión específica (al nombrar la conexión) o verifique la información de estado para todas las conexiones desde el cliente strongSwan:
   - Ubuntu:

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS:

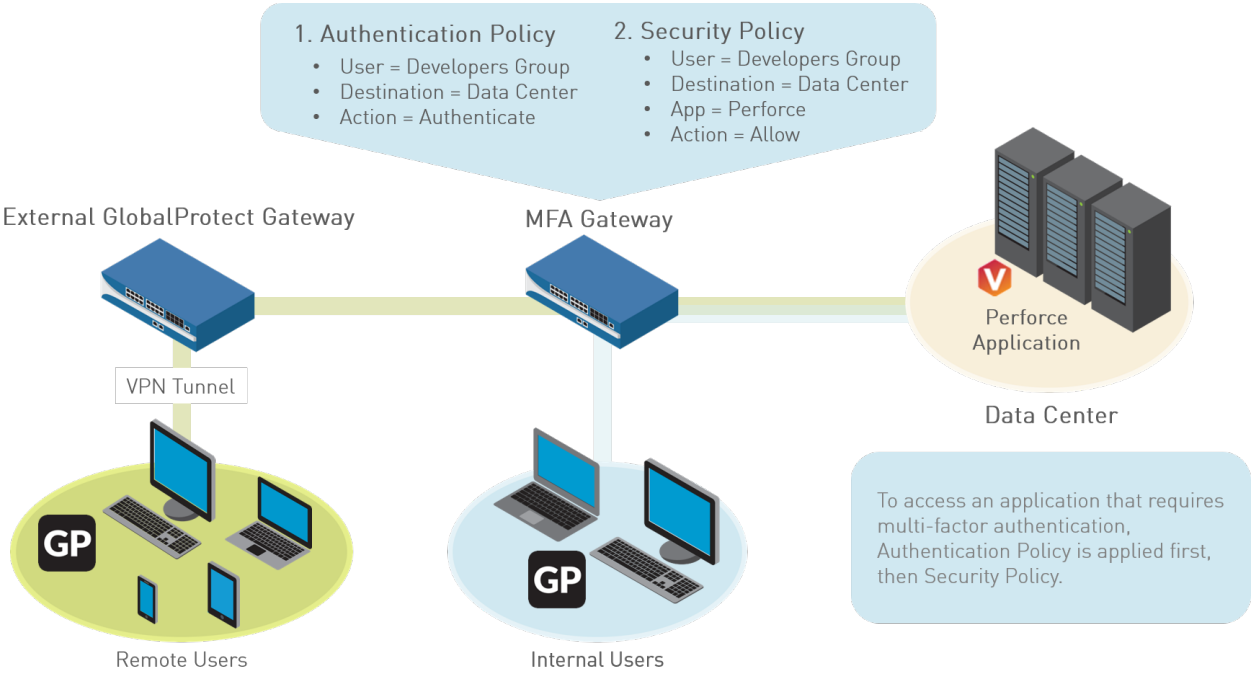
     ```
     strongswan statusall [<connection name>]
     ```

2. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**. En la columna **Info (información)**, seleccione **Remote Users (Usuarios remotos)** de la puerta de enlace configurada para la conexión con el cliente strongSwan. El cliente de strongSwan debe aparecer en **Current Users (Usuarios actuales)**.

© 2020 Palo Alto Networks, Inc.

Configuración de GlobalProtect para facilitar las notificaciones de autenticación multifactor

Para proteger aplicaciones clave y evitar que los atacantes utilicen credenciales robadas para realizar un movimiento lateral en su red, puede configurar la autenticación de factores múltiples basada en políticas (MFA) Esto garantiza que cada usuario responda a múltiples desafíos de autenticación de diferentes tipos (factores) antes de poder acceder a servicios y aplicaciones altamente confidenciales.



Si una sesión de usuario coincide con la política de autenticación, el tipo de aplicación o servicio determina la experiencia del usuario para las notificaciones sobre el desafío de autenticación:

- (Solo en endpoints de Windows o macOS) **Non-browser-based applications (Aplicaciones que no están basadas en navegador)**: para facilitar las notificaciones de MFA para las aplicaciones que no son HTTP (como Perforce) en endpoints de Windows o macOS, se requiere una aplicación de GlobalProtect. Cuando una sesión coincide con una regla de la política de autenticación, el cortafuegos envía una notificación UDP a la aplicación de GlobalProtect con un enlace URL incorporado a la página Authentication Portal (Portal de autenticación). Luego, la aplicación de GlobalProtect muestra este mensaje como una notificación emergente para el usuario.
- **Aplicaciones basadas en navegador**: las aplicaciones basadas en navegador no requieren que GlobalProtect muestre mensajes de notificación al usuario. Cuando el cortafuegos identifica una sesión como tráfico de navegación web (basado en app-ID), el cortafuegos presenta automáticamente al usuario la página del portal de autenticación (anteriormente llamada Página del portal cautivo) especificada en la regla de política de autenticación. Para más información, consulte Configuración de autenticación multifactor.

Para configurar GlobalProtect para que muestre notificaciones de MFA para aplicaciones no basadas en navegador, utilice el siguiente flujo de trabajo:

STEP 1 | Antes de configurar GlobalProtect, configure la autenticación multifactor en el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Si usa la autenticación en dos fases con GlobalProtect para autenticarse en la puerta de enlace o el portal, se requiere un perfil de servidor RADIUS. Si usa GlobalProtect para notificar al usuario sobre una coincidencia de política de autenticación (mensaje UDP), un perfil de servidor de Autenticación multifactor es suficiente.

Para usar autenticación multifactor para proteger recursos confidenciales, la solución más fácil es integrar el cortafuegos con un proveedor MFA que ya está establecido en su red. Cuando su estructura de MFA esté lista, puede comenzar a configurar los componentes de su política de autenticación. Para más información, consulte Configuración de autenticación multifactor.

- Habilite el Portal cautivo para registrar las marcas de tiempo de autenticación y actualizar las asignaciones de usuario.
- Cree perfiles de servidor que definan cómo se conectará el cortafuegos a los servicios que autentican a los usuarios.
- Asigne los perfiles del servidor a un perfil de autenticación que especifique los parámetros de autenticación.
- Configure una regla de política de seguridad que permita a los usuarios acceder a los recursos que requieren autenticación.

STEP 2 | (Solo puertas de enlace externas) Para que GlobalProtect admita la autenticación multifactor en puertas de enlace externas, debe Configurar una página de respuesta para la interfaz del túnel de ingreso en el cortafuegos:

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** > **MFA Login Page (Página de inicio de sesión de MFA)**.
2. Seleccione y a continuación use **Export (Exportar)** para exportar la plantilla **Predefined (Predefinido)** a una ubicación de su elección.
3. En su endpoint, use un editor HTML para personalizar la página de la respuesta descargada y guardarla con un nombre de archivo único.
4. Vuelva al diálogo **MFA Login Page (Página de inicio MFA)** en el cortafuegos, haga clic en **Import (Importar)** para importar su página personalizada y en **Browse (Examinar)** para elegir el **Import File (Archivo de importación)** y, luego, seleccione **Destination (Destino)** (sistema virtual o ubicación compartida). Haga clic en **OK (Aceptar)** y, luego, en **Close (Cerrar)**.

STEP 3 | (Solo puertas de enlace externas) Habilite las **Response Pages (Páginas de respuesta)** como un servicio permitido en el perfil de **Interface Mgmt (Gestión de interfaz**:

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)** y, luego, seleccione el perfil.
2. En la zona **Permitted Services (Servicios Permitidos)**, seleccione **Response Pages (Páginas de respuesta)** y haga clic **OK (Aceptar)**.

STEP 4 | (Solo puertas de enlace externas) Adjunte el perfil de **Interface Mgmt (Gestión de interfaz)** a una interfaz de túnel:

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y elija la interfaz de túnel en la que desea usar la página de respuesta.
2. Seleccione **Advanced (Avanzado)** y luego seleccione el perfil de **Interface Mgmt (Gestión de interfaz)** que configuró en el paso anterior como el **Management Profile (Perfil de gestión)**.

STEP 5 | (Solo para puertas de enlace externas) Seleccione **Enable User Identification (Habilitar identificación de usuario)** en la zona asociada con la interfaz de túnel (**Network (Red)** > **Zones (Zonas)** > **<tunnel-zone**).

© 2020 Palo Alto Networks, Inc.

STEP 6 | Configure los clientes de GlobalProtect para admitir notificaciones de autenticación multifactor para aplicaciones no basadas en navegador.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, seleccione una configuración de portal (o haga clic en **Add [Añadir]** para añadir una).
2. Seleccione **Agent (Agente)** y, luego, una configuración de agente existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **App (Aplicación)**, especifique lo siguiente:
   - Establezca **Enable Inbound Authentication Prompts from MFA Gateways (Habilitar solicitudes de autenticación entrantes desde las puertas de enlace de MFA)** en **Yes (Sí)**. Para admitir la MFA, la aplicación de GlobalProtect debe recibir y confirmar las solicitudes de autenticación por UDP que proceden de la puerta de enlace. Seleccione **Yes (Sí)** para permitir que la aplicación de GlobalProtect reciba y acepte la indicación. De manera predeterminada, este valor está configurado en **No**, lo que significa que GlobalProtect bloquea las solicitudes de autenticación por UDP de la puerta de enlace.
   - En el campo **Network Port for Inbound Authentication Prompts (UDP) (Puerto de red para solicitudes de autenticación entrantes [UDP])**, especifique el número de puerto que usa la aplicación de GlobalProtect para recibir las solicitudes de autenticación entrantes de las puertas de enlace de MFA. El puerto predeterminado es 4501. Para cambiar el puerto, especifique un número de 1 a 65535.
   - En el campo **Trusted MFA Gateways (Puertas de enlace de MFA de confianza)**, especifique la dirección y el número de puerto (obligatorio solo cuando no es el predeterminado, como 6082) de las puertas de enlace de la URL de redirección en las que debe confiar la aplicación de GlobalProtect para la MFA. Cuando la aplicación de GlobalProtect recibe una solicitud de autenticación por UDP con una URL de redirección destinada al puerto de red especificado, GlobalProtect solo muestra un mensaje de autenticación si dicha URL es de confianza.
   - Configure el **Default Message for Inbound Authentication Prompts (Mensaje predeterminado para mensajes de autenticación de entrada)**. Cuando los usuarios intentan acceder a un recurso que requiere autenticación adicional, GlobalProtect recibe un paquete UDP que contiene la solicitud de autenticación de entrada y muestra este mensaje. El paquete UDP también contiene la URL de la página del Portal de autenticación que especificó en Configuración de autenticación multifactor. GlobalProtect adjunta automáticamente la URL al mensaje. Por ejemplo, para mostrar la notificación que se muestra al comienzo de este tema, introduzca el siguiente mensaje:

     ```
     Ha intentado acceder a un recurso protegido que requiere autenticación
     adicional. Proceda a la autenticación en:
     ```
4. Guarde la configuración del agente (haga clic en **OK (Aceptar)** dos veces), y luego seleccione **Commit (Confirmar)** para confirmar sus cambios

© 2020 Palo Alto Networks, Inc.

Habilitación de envío de VSA a un servidor RADIUS

Cuando se comunica con los portales o puertas de enlace, los endpoints de GlobalProtect envían información que incluye la dirección IP, el sistema operativo (SO), el nombre de host, el dominio de usuario y la versión de la aplicación de GlobalProtect del endpoint. Usted puede habilitar el cortafuegos para que envíe esta información como atributos específicos del proveedor (Vendor-Specific Attributes, VSA) a un servidor RADIUS durante la autenticación (por defecto, el cortafuegos no envía los VSA). Los administradores de RADIUS luego pueden realizar tareas administrativas en función de dichos VSA. Por ejemplo, los administradores de RADIUS pueden usar el atributo de SO para definir una política que exija la autenticación de contraseña periódica para los usuarios de Microsoft Windows y la autenticación de contraseña de un solo uso (one-time password, OTP) para los usuarios de Google Android.

Los siguientes son requisitos previos para este procedimiento:

- Importe el diccionario RADIUS de Palo Alto Networks a su servidor RADIUS.
- Configure un perfil de servidor RADIUS y asígnelo a un perfil de autenticación. Consulte Configuración de autenticación externa para obtener más detalles.
- Asigne el perfil de autenticación a un portal o puerta de enlace de GlobalProtect. Consulte Configuración de acceso al portal de GlobalProtect o Configuración de una puerta de enlace de GlobalProtect para obtener más detalles.

STEP 1 | Inicie sesión en la CLI del cortafuegos.

STEP 2 | Introduzca el comando para cada VSA que desea enviar:

```
username@hostname> set authentication radius-vsa-on client-source-ip
username@hostname> set authentication radius-vsa-on client-os
username@hostname> set authentication radius-vsa-on client-hostname
username@hostname> set authentication radius-vsa-on user-domain
username@hostname> set authentication radius-vsa-on client-gp-version
```

Si más tarde desea que el cortafuegos deje de enviar VSA particulares, ejecute los mismos comandos, pero use la opción ***`radius-vsa-off`*** *en lugar de* ***`radius-vsa-on`****.*

© 2020 Palo Alto Networks, Inc.

Habilitación de la asignación de grupo

Dado que el agente o la aplicación que se ejecuta en los sistemas de sus usuarios finales requieren la autenticación correcta del usuario antes de tener acceso a GlobalProtect, se conoce la identidad de cada usuario de GlobalProtect. Sin embargo, para poder definir configuraciones de GlobalProtect o políticas de seguridad basadas en la pertenencia a grupos, el cortafuegos debe recuperar la lista de grupos y la lista de miembros correspondiente del servidor de directorios. Esto recibe el nombre de *asignación de grupos*.

Para habilitar esta función, debe crear un perfil de servidor LDAP que indique al cortafuegos cómo conectarse al servidor de directorios y autenticarlo, así como el modo de buscar en el directorio la información de usuarios y grupos. Cuando el cortafuegos se conecta al servidor LDAP y recupera las asignaciones de grupos, usted puede seleccionar grupos al definir las configuraciones de agente y las políticas de seguridad. El cortafuegos admite una variedad de servidores de directorio LDAP, incluidos Microsoft Active Directory (AD), Novell eDirectory y Sun ONE Directory Server.

Utilice el siguiente procedimiento para conectarse a su directorio LDAP y así permitir que el cortafuegos recupere información de asignación de usuario a grupo:

STEP 1 | Cree un perfil de servidor LDAP que especifique cómo conectarse a los servidores de directorio a los que debería conectarse el cortafuegos para obtener información de asignación de grupos.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **LDAP** y luego **Add (Añadir)**.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.
4. Para cada servidor LDAP (con un máximo de cuatro), haga clic en **Add** e introduzca un nombre en **Name** (para identificar el servidor), la dirección IP del servidor (campo **LDAP Server**) y un puerto de servidor en **Port** (por defecto es 389).
5. Seleccione el **Type (Tipo)** de servidor en el menú desplegable: **active-directory**, **e-directory**, **sun**, u **other (otro)**.
6. (LDAP únicamente) Si desea que el dispositivo use SSL o TLS para una conexión más segura con el servidor del directorio, seleccione la casilla de verificación **Require SSL/TLS secured connection (Exigir conexión segura con SSL/TLS)** (está seleccionada por defecto). El protocolo que usa el dispositivo depende del **Port (Puerto)** del servidor:
   - 389 (predeterminado): TLS (específicamente, el dispositivo usa la operación StartTLS, que actualiza la conexión de texto no cifrado inicial a TLS).
   - 636—SSL
   - Cualquier otro puerto: El dispositivo intenta primer usar TLS. Si el servidor de directorio no admite TLS, el dispositivo cambia a SSL.
7. Para mayor seguridad, seleccione la casilla de verificación **Verify Server Certificate for SSL sessions (Verificar certificado de servidor para las sesiones SSL)** (está desmarcada por defecto), para que el dispositivo verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar esta verificación, debe seleccionar también la casilla de verificación **Require SSL/TLS secured connection (Exigir conexión segura con SSL/TLS)**. Para que la verificación se realice correctamente, el certificado debe reunir una de las siguientes condiciones:
   - Está en la lista de certificados de dispositivo: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Importe el certificado al dispositivo, si fuera necesario:
   - El firmante del certificado está en la lista de autoridades de certificación confiables: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Default Trusted Certificate Authorities (Autoridades de certificados de confianza por defecto)**.
8. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Añada el perfil de servidor LDAP a la configuración de asignación de grupos de User-ID.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **Group Mapping Settings (Configuración de asignación de grupos)** y haga clic en **Add (Añadir)** para añadir la configuración de una nueva asignación de grupos.
2. Seleccione **Server Profile (Perfil de servidor)**.
3. En **Name (Nombre)**, introduzca un nombre para la configuración de asignación de grupos.
4. Seleccione el **Server Profile (Perfil de servidor)** que acaba de crear.
5. En **Update Interval (Intervalo entre actualizaciones)**, especifique los segundos que deben transcurrir para que el cortafuegos inicie una conexión al servidor de directorios LDAP a fin de obtener las actualizaciones realizadas en los grupos que se emplean en sus políticas; el intervalo va de 60 a 86 400 segundos.
6. El perfil de servidor debe tener marcada la opción **Enabled (Habilitado)** de la asignación de grupos.

STEP 3 | (Opcional) Permita que GlobalProtect recupere los números de serie del servidor de directorios.

Si GlobalProtect dispone del número de serie de los terminales, puede identificar el estado de los que se conectan, así como aplicar las políticas de seguridad basadas en perfiles de información de hosts (host information profile, HIP). En el caso de los terminales gestionados, puede enlazar su número de serie a la cuenta de su equipo en el servidor de directorios. Así, el cortafuegos puede recuperar previamente los números de serie de esos terminales gestionados cuando recupere la información sobre la asignación de grupos de dicho servidor.

1. En la configuración de la asignación de grupos, seleccione **Server Profile (Perfil de servidor)**.
2. Habilite la opción **Fetch list of managed devices (Obtener lista de dispositivos gestionados)**.

STEP 4 | (Opcional) Especifique los atributos que identifican a los usuarios y a los grupos de usuarios.

1. En la configuración de la asignación de grupos, seleccione **User and Group Attributes (Atributos de usuarios y grupos)**.
2. En el área User Attributes (Atributos de usuarios), especifique los valores de **Primary Username (Nombre de usuario principal)**, **E-Mail (Correo electrónico)** y **Alternate Username 1-3 (Nombre de usuario alternativo 1-3)** que permiten identificar a cada usuario.
3. En el área Group Attributes (Atributos de grupos), especifique los valores de **Group Name (Nombre de grupo)**, **Group Member (Miembro de grupo)** e **E-Mail (Correo electrónico)** que permiten identificar los grupos de usuarios.

STEP 5 | (Opcional) Limite los grupos que pueden seleccionarse en las reglas de políticas.

Por defecto, si no especifica grupos, todos los grupos están disponibles en reglas de políticas.

1. Añada grupos existentes del servicio de directorio:
   1. En la configuración de la asignación de grupos, seleccione **Group Include List (Lista de inclusión de grupos)**.
   2. En la lista Available Groups (Grupos disponibles), seleccione los grupos que deben aparecer en las reglas de las políticas y, a continuación, haga clic en el icono Add (Añadir ⊕) para moverlos a la lista Included Groups (Grupos incluidos).
2. Si desea basar reglas de políticas en atributos de usuario que no coincidan con grupos de usuario existentes, cree grupos personalizados que se basen en filtros de LDAP:
   1. En la configuración de la asignación de grupos, seleccione **Custom Group (Grupo personalizado)**.
   2. Haga clic en **Add (Añadir)** para añadir un grupo personalizado nuevo.
   3. Introduzca un nombre de usuario en **Name** que sea único en la configuración de asignación de grupo para el cortafuegos o sistema virtual actual. Si el **Name (Nombre)** tiene el mismo valor que el nombre distintivo (DN) de un dominio de grupo AD existente, el cortafuegos usa el grupo personalizado en todas las referencias a ese nombre (por ejemplo, en políticas y logs).

© 2020 Palo Alto Networks, Inc.

4. Especifique un **LDAP Filter (Filtro LDAP)** de hasta 2048 UTF-8 caracteres y luego haga clic en **OK (Aceptar)**. El cortafuegos no valida filtros LDAP.

   Para optimizar las búsquedas LDAP y minimizar el impacto de desempeño en el servidor del directorio LDAP, use atributos indexados y reduzca el alcance de la búsqueda para incluir objetos de usuario y grupo que necesita para la política o visibilidad. De manera alternativa, puede crear grupos personalizados sobre la base de filtros LDAP.

STEP 6 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Puertas de enlace de GlobalProtect

> Conceptos de puertas de enlace de GlobalProtect
> Tareas de requisito previo para la configuración de la puerta de enlace de GlobalProtect
> Configuración de una puerta de enlace de GlobalProtect
> Tráfico de división de túnel (Split Tunnel) en puertas de enlace de GlobalProtect

© 2020 Palo Alto Networks, Inc.

Descripción general de puertas de enlace de GlobalProtect

Debido a que la configuración del portal de GlobalProtect que se brinda en las aplicaciones incluye la lista de puertas de enlace a las que se puede conectar el endpoint, se recomienda que configure las puertas de enlace antes de configurar el portal.

Las Puertas de enlace de GlobalProtect se configuran para brindar dos funciones principales.

- Aplican la política de seguridad para las aplicaciones de GlobalProtect que conectan las puertas de enlace. También puede habilitar la recopilación HIP en la puerta de enlace para mejorar la granularidad de la política de seguridad. Para obtener más información sobre la habilitación de comprobaciones HIP, consulte Información de host.
- Brindan acceso a una red virtual privada (virtual private network, VPN) a la red corporativa interna. El acceso de VPN se proporciona mediante un túnel SSL o IPsec entre el endpoint y la interfaz del túnel en el cortafuegos que aloja la puerta de enlace.

Entonces podrá configurar las puertas de enlace de GlobalProtect en los cortafuegos de VM-Series implementados en la nube AWS. Mediante la implementación de un cortafuegos VM-Series en la nube AWS, puede implementar rápida y fácilmente las puertas de enlace de GlobalProtect en cualquier región sin el gasto ni la logística de TI que suelen ser necesarias para establecer esta infraestructura. Para obtener detalles, consulte Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS*.*

© 2020 Palo Alto Networks, Inc.

Conceptos de puertas de enlace de GlobalProtect

Estas secciones proporcionan información sobre la prioridad de conexión de la puerta de enlace en una configuración de puerta de enlace múltiple y compatibilidad con MIB para las puertas de enlace de GlobalProtect.

- Tipos de puertas de enlace
- Prioridad de la puerta de enlace en una configuración de varias puertas de enlace
- Soporte MIB de GlobalProtect

Tipos de puertas de enlace

Las puertas de enlace de GlobalProtect proporcionan la aplicación de la seguridad en el tráfico de las aplicaciones de GlobalProtect. Además, si la función del Perfil de información de host (Host Information Profile, HIP) está habilitada, la puerta de enlace genera un informe de HIP a partir de los datos del host sin procesar que envían los endpoints, que pueden usarse para la instauración de políticas.

Puede configurar una puerta de enlace de GlobalProtect en cualquier cortafuegos de última generación de Palo Alto Networks. Puede ejecutar tanto una puerta de enlace como un portal en el mismo cortafuegos, o puede tener varias puertas de enlace distribuidas en toda la empresa.

GlobalProtect es compatible con los siguientes tipos de puertas de enlace:

- **Interna**: una puerta de enlace interna es una interfaz en la red interna configurada como una puerta de enlace de GlobalProtect que permite aplicar políticas de seguridad para el acceso a recursos internos. Cuando se usa junto con User-ID o las comprobaciones HIP, una puerta de enlace interna permite ofrecer un método preciso y seguro para identificar y controlar el tráfico por usuario o estado del dispositivo. Las puertas de enlace internas son útiles en entornos confidenciales que requieren acceso autenticado a los recursos críticos. Puede configurar una puerta de enlace interna tanto en el modo de túnel como de no túnel. La aplicación de GlobalProtect se conecta a la puerta de enlace interna después de realizar la detección de host interno para determinar la ubicación del endpoint.
- **Puerta de enlace externa (descubrimiento automático)**: una puerta de enlace externa reside fuera de la red corporativa y proporciona seguridad y/o acceso a la red privada virtual (VPN) para los usuarios remotos. De manera predeterminada, la aplicación de GlobalProtect se conecta automáticamente a la puerta de enlace externa **Best Available (Mejor disponible)** en función de la prioridad que asigne a la puerta de enlace, la región de origen y el tiempo de respuesta (consulte Prioridad de la puerta de enlace en una configuración de varias puertas de enlace).
- **Puerta de enlace externa (manual)**: una puerta de enlace externa manual también reside fuera de la red corporativa y proporciona seguridad y/o acceso a la red privada virtual (VPN) para los usuarios remotos. La diferencia entre la puerta de enlace externa de descubrimiento automático y la puerta de enlace externa manual es que la aplicación de GlobalProtect solo se conecta a una puerta de enlace externa manual cuando el usuario inicia una conexión. También puede configurar diferentes requisitos de autenticación para puertas de enlace externas manuales. Para configurar una puerta de enlace manual, debe identificar la puerta de enlace como **Manual** cuando defina las configuraciones del agente de GlobalProtect.

Prioridad de la puerta de enlace en una configuración de varias puertas de enlace

Para habilitar el acceso seguro de su fuerza laboral itinerante, sin importar la ubicación, puede implementar estratégicamente cortafuegos adicionales de última generación de Palo Alto Networks y configurarlos como

© 2020 Palo Alto Networks, Inc.

puertas de enlace de GlobalProtect. Para determinar la puerta de enlace preferida a la cual se conectarán sus aplicaciones, añada las puertas de enlace a una configuración de agente de portal y asigne a cada puerta de enlace una prioridad de conexión. Consulte Definición de las configuraciones de agente de GlobalProtect.

Si una configuración de agente de portal de GlobalProtect contiene más de una puerta de enlace, la aplicación tratará de comunicarse con todas las puertas de enlace enumeradas en su configuración de agente. La aplicación utiliza la prioridad y el tiempo de respuesta para determinar a qué puerta de enlace se conectará. Con la aplicación de GlobalProtect 4.0.2 y versiones anteriores, la aplicación se conecta a una puerta de enlace de menor prioridad solo si el tiempo de respuesta para la puerta de enlace de mayor prioridad es mayor que el tiempo de respuesta promedio de todas las puertas de enlace.

Por ejemplo, considere los siguientes tiempos de respuesta para la gw1 y gw2:

Nombre	Prioridad	Tiempo de respuesta
gw1	La más alta	80 ms
gw2	high (alta)	25 ms

La aplicación determina que el tiempo de respuesta para la puerta de enlace con la prioridad más alta (el número más alto) es mayor que el tiempo de respuesta promedio de ambas puertas de enlace (52,5 ms) y, como resultado, se conecta a la gw2. En este ejemplo, la puerta de enlace no se conectó a la gw1 incluso a pesar de que tenía prioridad más alta, ya que un tiempo de respuesta de 80 ms era más alto que el promedio de ambas.

Ahora considere los siguientes tiempos de respuesta para la gw1, gw2 y una tercera puerta de enlace, gw3:

Nombre	Prioridad	Tiempo de respuesta
gw1	La más alta	30 ms
gw2	high (alta)	25 ms
gw3	Intermedia	50 ms

En este ejemplo, el tiempo de respuesta promedio para todas las puertas de enlace es de 35 ms. La aplicación entonces evaluaría qué puertas de enlace respondieron más rápido que el tiempo de respuesta promedio y vería que la gw1 y gw2 tuvieron tiempos de respuesta más rápidos. Luego, la aplicación se conectaría a la puerta de enlace que tuviera la prioridad más alta. En este ejemplo, la aplicación se conecta a la gw1 ya que la gw1 tiene la prioridad más alta de todas las puertas de enlace con tiempos de respuesta por debajo del promedio.

Además de la prioridad de la puerta de enlace, puede añadir una o más regiones seguras a una configuración de puerta de enlace externa. GlobalProtect reconoce la región de origen y solo permite que los usuarios se conecten a las puertas de enlace configuradas para esa región. Con respecto de la selección de puertas de enlace, primero se considera la región de origen y luego la prioridad de la puerta de enlace.

En la aplicación de GlobalProtect 4.0.3 y versiones posteriores, la aplicación de GlobalProtect da prioridad a las puertas de enlace con prioridad más alta, alta y media, por delante de las puertas de enlace a las que se asignó una prioridad baja o más baja; independientemente del tiempo de respuesta. Luego, la aplicación de GlobalProtect añade las puertas de enlace asignadas una prioridad baja o a la más baja, a la lista de puertas de enlace. Esto garantiza que la aplicación intente primero conectarse a las puertas de enlace que configure con una mayor prioridad.

© 2020 Palo Alto Networks, Inc.

Soporte MIB de GlobalProtect

Los endpoints de Palo Alto Networks admiten bases de información de gestión (management information bases, MIB) estándar y para empresas que le permiten supervisar el estado físico, estadísticas de uso, capturas y otra información útil del endpoint. La mayoría de las MIB usan grupos de objetos para describir las características del endpoint con el marco del Protocolo simple de administración de redes (Simple Network Management Protocol, SNMP). Debe cargar estas MIB en su gestor SNMP para supervisar los objetos (capturas y estadísticas de endpoint) que se definen en las MIB (para obtener los detalles, consulte Uso de un gestor SNMP para explorar MIB y objetos en la Guía del administrador de PAN-OS 8.1).

El PAN-COMMON-MIB, que se incluye con los MIB empresariales, utiliza el grupo de objetos panGlobalProtect. La siguiente tabla describe los objetos que conforman el grupo de objetos panGlobalProtect.

Object (Objeto)	Description (Descripción)
panGPGWUtilizationPct	Utilización (como porcentaje) de la puerta de enlace de GlobalProtect
panGPGWUtilizationMaxTunnels	Cantidad máxima de túneles permitidos
panGPGWUtilizationActiveTunnels	Cantidad de túneles activos

Utilice estos objetos SNMP para controlar la utilización de puertas de enlace de GlobalProtect y realizar cambios según fuera necesario. Por ejemplo, si la cantidad de túneles activos alcanza el 80 % o es mayor que la cantidad máxima de túneles permitidos, debe considerar añadir puertas de enlace adicionales.

© 2020 Palo Alto Networks, Inc.

Tareas de requisito previo para la configuración de la puerta de enlace de GlobalProtect

Antes de poder configurar la puerta de enlace de GlobalProtect, debe haber realizado las tareas siguientes:

- Cree las interfaces (y zonas) para el cortafuegos en el que planifique configurar cada puerta de enlace. Para las puertas de enlace que requieren conexiones de túnel, debe configurar tanto la interfaz física como la interfaz de túnel virtual. Consulte Creación de interfaces y zonas para GlobalProtect.
- Configure los certificados del servidor de la puerta de enlace y el perfil de servicio SSL/TLS necesarios para que la aplicación de GlobalProtect establezca una conexión SSL con la puerta de enlace. Consulte Habilitación de SSL entre componentes de GlobalProtect.
- Defina los perfiles de autenticación o los perfiles del certificado que se usarán para autenticar a los usuarios de GlobalProtect. Consulte Autenticación.

© 2020 Palo Alto Networks, Inc.

Configuración de una puerta de enlace de GlobalProtect

Una vez completadas estas tareas previas obligatorias, configure las puertas de enlace de GlobalProtect.

STEP 1 | Añada un gateway.

1. **Añada** una puerta de enlace nueva (**Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**).
2. En **Name (Nombre)**, introduzca el nombre de la puerta de enlace.

   El nombre de la puerta de enlace no puede contener espacios y debe ser exclusivo para cada sistema virtual. Se recomienda que incluya la ubicación u otra información descriptiva que ayude a los usuarios y a otros administradores a identificar la puerta de enlace.
3. (Opcional) En **Location (Ubicación)**, seleccione la ubicación del sistema virtual al que pertenece la puerta de enlace.

STEP 2 | Especifique la información de red que permita a los endpoints conectarse a la puerta de enlace.

Cree la interfaz de red de la puerta de enlace si aún no existe.

No vincule un perfil de gestión de interfaces que permita HTTP, HTTPS, Telnet o SSH en la interfaz que configure, ya que franquearía el acceso a la interfaz de gestión desde internet. Siga las sugerencias de Prácticas recomendadas para proteger el acceso administrativo *para proteger el acceso administrativo a los cortafuegos de modo que se eviten ataques efectivos.*

1. En **Interface (Interfaz)**, seleccione la interfaz que deben usar los terminales para comunicarse con la puerta de enlace.
2. Especifique el **IP Address Type (Tipo de dirección IP)** y la **IP Address (Dirección IP)** para el servicio web de la puerta de enlace:
   - En **IP Address Type (Tipo de dirección IP)**, seleccione **IPv4 Only (Solo IPv4)**, **IPv6 Only (Solo IPv6)** o **IPv4 and IPv6 (IPv4 e IPv6).** Utilice **IPv4 and IPv6 (IPv4 e IPv6)** si su red admite dos configuraciones de pila, donde IPv4 e IPv6 se ejecutan al mismo tiempo.
   - La dirección IP debe ser compatible con el tipo de dirección IP. Por ejemplo, `172.16.1.0` para las direcciones IPv4 o `21DA:D3:0::2F3b` para las direcciones IPv6. Para las configuraciones de pila doble, introduzca una dirección IPv4 e IPv6.

STEP 3 | Configure los ajustes de logs de descifrado.

Puede registrar los protocolos de enlace TLS/SSL correctos e incorrectos y reenviar los logs de descifrado a los recopiladores de logs, a otros dispositivos de almacenamiento y a administradores específicos.

- De forma predeterminada, el cortafuegos registra solo los protocolos de enlace TLS incorrectos. También es recomendable registrar los protocolos de enlace correctos para tener visibilidad de todo el tráfico descifrado que permitan los recursos disponibles (pero no descifre el tráfico privado o confidencial; siga las prácticas recomendadas de descifrado y descifre todo el tráfico que pueda).
- Si aún no lo ha hecho, cree un perfil de reenvío de logs para reenviar los logs de descifrado y especifíquelo en la configuración de la puerta de enlace.
- Si registra un protocolo de enlace TLS correcto además de un protocolo de enlace TLS incorrecto, configure una cuota de espacio de almacenamiento de log más grande para el log de descifrado (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Administración)** > **Logging and Reporting Settings (Configuración de creación de logs e informes)** > **Log Storage (Almacenamiento**

© 2020 Palo Alto Networks, Inc.

de logs)). La cuota predeterminada (asignación) es el uno por ciento de la capacidad de almacenamiento de logs del dispositivo para los logs de descifrado y el uno por ciento para el resumen general de descifrado. No hay una asignación predeterminada para los resúmenes de descifrado por hora, por día o por semana. La configuración de logs de descifrado proporciona más información sobre cómo asignar el espacio de log del cortafuegos a los logs de descifrado.

STEP 4 | Especifique de qué manera la puerta de enlace autenticará a los usuarios.

Si aún no existe ningún perfil de servicio de capa de sockets seguros (secure sockets layer, SSL) o seguridad de capa de transporte (transport layer security, TLS) para la puerta de enlace, realice el procedimiento Implementación de certificados de servidores en los componentes de GlobalProtect.

Si aún no existen perfiles de autenticación o perfiles de certificados, realice la tarea de configuración de la autenticación a fin de configurar esos perfiles para la puerta de enlace.

Configure cualquiera de los siguientes ajustes de **Authentication (Autenticación)** de la puerta de enlace (**Network (Red)** > **GlobalProtect** > **Gateways (Puerta de enlace)** > *<gateway-config>* > **Authentication (Autenticación)**):

- Para proteger la comunicación entre la puerta de enlace y la aplicación de GlobalProtect, seleccione **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)** para la puerta de enlace.

  La versión máx. de TLS en el perfil de servicio SSL/TLS es TLSv1.2. TLSv1.3 no es actualmente compatible con la aplicación de GlobalProtect y las conexiones VPN sin cliente.

  Para brindar la seguridad más estricta, en Min Version (Versión mínima) del perfil de servicio SSL/TLS, seleccione TLSv1.2.

- Para autenticar a los usuarios con una base de datos de usuario local o un servicio de autenticación externo, como LDAP, Kerberos, TACACS+, SAML o RADIUS (incluida OTP), haga clic en **Add (Añadir)** para añadir una configuración de **Client Authentication (Autenticación de cliente)** con los siguientes ajustes:
  - En **Name (Nombre)**, especifique un nombre que identifique la configuración de autenticación de los clientes.
  - Identifique el tipo de **OS (SO)** (sistema operativo) al que se aplica esta configuración. De manera predeterminada, la configuración se aplica a **Any (Cualquier)** sistema operativo.
  - Seleccione o añada un **Authentication Profile (Perfil de autenticación)** para autenticar endpoints que intentan acceder a la puerta de enlace.
  - En **Username Label (Etiqueta de nombre de usuario)**, introduzca una etiqueta personalizada para iniciar sesión en la puerta de enlace, por ejemplo, una **`Email Address (username@domain) (Dirección de correo electrónico [nombre-usuario@dominio])`**.
  - En **Password Label (Etiqueta de contraseña)**, introduzca una etiqueta de contraseña personalizada para el inicio de sesión de la puerta de enlace (por ejemplo, un **`código de acceso`** para la autenticación en dos fases basada en token).
  - Introduzca un **Authentication Message (Mensaje de autenticación)** para ayudar a los usuarios finales a comprender qué credenciales deben usar cuando inician sesión. El mensaje puede tener hasta 256 caracteres de longitud (el predeterminado es `Enter login credentials [Introduzca las credenciales de inicio de sesión]`).
  - Para definir si los usuarios se pueden autenticar en la puerta de enlace con credenciales o certificados de cliente, seleccione una de estas opciones:
    - Si los usuarios se deben autenticar en la puerta de enlace con ambos elementos, configure la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credenciales de usuario o certificados de cliente)** en **No (User Credentials AND Client Certificate Required) (No, exigir credenciales de usuario y certificados de cliente)**, que es el valor predeterminado.

© 2020 Palo Alto Networks, Inc.

- Para permitir que los usuarios se autentiquen en la puerta de enlace con cualquiera de estos elementos, configure la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credenciales de usuario o certificados de cliente)** en **Yes (User Credentials OR Client Certificate Required) (Sí, exigir credenciales de usuario o certificados de cliente)**.

  Si configura esta opción en **Yes (Sí)**, la puerta de enlace busca primero el certificado de cliente en el terminal. Si no hay ninguno o si no ha configurado ningún perfil de certificados en la configuración de autenticación de los clientes, el usuario del terminal se puede autenticar en la puerta de enlace con sus credenciales.

- Para autenticar a los usuarios basándose en un certificado de cliente o una tarjeta inteligente / CAC, seleccione el **Certificate Profile (Perfil del certificado)** correspondiente. Debe implementar previamente el certificado del cliente o implementar certificados de cliente específicos del usuario para la autenticación con el Protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP).
  - Si los usuarios se deben autenticar en la puerta de enlace con las credenciales y con los certificados de cliente, tiene que especificar tanto el perfil de certificados como el perfil de autenticación.
  - Si los usuarios se pueden autenticar en la puerta de enlace con sus credenciales o con los certificados de cliente y especifica el perfil de autenticación para autenticar a los usuarios, el perfil de certificados es opcional.
  - Si los usuarios se pueden autenticar en la puerta de enlace con sus credenciales o con los certificados de cliente, pero no selecciona ningún perfil de autenticación para autenticar a los usuarios, el perfil de certificados es obligatorio.
  - Si no configura ningún perfil de autenticación que coincida con un sistema operativo concreto, el perfil de certificados es obligatorio.

  Si los usuarios se pueden autenticar en la puerta de enlace con sus credenciales o con los certificados de cliente, no seleccione ningún perfil de certificados donde Username Field (Campo de nombre de usuario) se haya configurado en None (Ninguno).

- Para usar la autenticación con dos factores, seleccione tanto un perfil de autenticación como un perfil de certificados. El usuario se debe autenticar con ambos métodos para obtener acceso.

  (Solo en Chrome) Si configura la puerta de enlace para que use certificados de cliente y LDAP para la autenticación con dos factores, los Chromebooks que ejecutan Chrome OS 47 o versiones posteriores muestran demasiadas solicitudes para seleccionar el certificado de cliente. Para evitarlo, configure una política que especifique el certificado de cliente en la consola de administración de Google y, luego, impleméntela en los Chromebooks gestionados.

  1. *Inicie sesión en la consola de administración de Google y seleccione Device management (Administración de dispositivos) > Chrome management (Administración de Chrome) > User settings (Configuración de usuario).*
  2. *En la sección Client Certificates (Certificados de cliente), introduzca el patrón de URL siguiente en Automatically Select Client Certificate for These Sites (Seleccionar automáticamente el certificado de cliente de estos sitios):*

     ```
     {"pattern": "https://[*.]","filter":{}}
     ```
  3. *Haga clic en Save (Guardar). La consola de administración de Google implementa la política en todos los dispositivos en apenas unos minutos.*
  4. *Para evitar que los usuarios de GlobalProtect inicien sesión desde dispositivos en cuarentena a la puerta de enlace de GlobalProtect, seleccione Block login for quarantined devices (Bloquear inicio de sesión para dispositivos en cuarentena).*

© 2020 Palo Alto Networks, Inc.

STEP 5 | Habilite la tunelización y, luego, configure los parámetros de los túneles.

Es obligatorio especificar los parámetros de los túneles para las puertas de enlace externas, pero opcional para las internas.

Si desea forzar el uso del modo de túnel de red privada virtual (virtual private network, VPN) SSL, quite la marca de la opción **Enable IPSec (Habilitar IPSec)**. De manera predeterminada, solo se utiliza VPN SSL si el terminal no logra establecer el túnel de seguridad del protocolo de internet (internet protocol security, IPSec).

La autenticación ampliada solo se admite en los túneles de IPSec. Si marca Enable X-Auth Support (Permitir autenticación ampliada), no se usan los perfiles criptográficos de IPSec de GlobalProtect.

Para obtener más información sobre los algoritmos criptográficos admitidos, consulte Funciones criptográficas de la aplicación de GlobalProtect.

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Tunnel Settings (Configuración de túneles)**.
2. Habilite **Tunnel Mode (Modo de túnel)** para permitir el túnel dividido.
3. En **Tunnel Interface (Interfaz de túnel)**, seleccione la interfaz definida al crear la interfaz de red de la puerta de enlace.
4. (Opcional) En **Max User (Máximo de usuarios)**, especifique el número máximo de usuarios que puede acceder al mismo tiempo a la puerta de enlace para realizar la autenticación o para obtener actualizaciones de perfiles de información de hosts (host information profile, HIP) o de la aplicación de GlobalProtect. El rango de valores se muestra cuando el campo está vacío y varía según la plataforma.
5. Marque **Enable IPSec (Habilitar IPSec)** y, a continuación, seleccione un perfil en **GlobalProtect IPSec Crypto (Criptografía de IPSec de GlobalProtect)** para proteger los túneles de VPN entre la aplicación y la puerta de enlace de GlobalProtect. El perfil **default (predeterminado)** utiliza un cifrado AES-128-CBC y una autenticación sha1.

   IPSec no es compatible con los endpoints de Windows 10 UWP.

   Si desea crear un perfil nuevo, seleccione **New GlobalProtect IPSec Crypto (Nueva criptografía de IPSec de GlobalProtect)** en el menú desplegable **GlobalProtect IPSec Crypto (Criptografía de IPSec de GlobalProtect)** y configure los ajustes siguientes:

   1. En **Name (Nombre)**, especifique un nombre para identificar el perfil.
   2. Haga clic en **Add (Añadir)** para añadir en **Authentication (Autenticación)** y en **Encryption (Cifrado)** los algoritmos que los peers de VPN pueden usar para negociar las claves que protegen los datos en el túnel:
      - **Encryption (Cifrado)**: si no sabe qué algoritmos admiten los peers de VPN, añada varios del más seguro al menos seguro: **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**. Los peers negocian con el algoritmo más seguro para establecer el túnel.
      - **Authentication (Autenticación)**: seleccione el algoritmo de autenticación (**sha1**) para proporcionar protección de la integridad y autenticidad de los datos. Aunque es obligatorio indicar el algoritmo de autenticación en el perfil, solo se aplica al cifrado AES-CBC (**aes-128-cbc**). Si usa un algoritmo de cifrado AES-GCM (**aes-256-gcm** o **aes-128-gcm**), se ignora este ajuste porque estos cifrados brindan protección nativa de integridad de la carga útil de seguridad encapsulada (encapsulating security payload, ESP).
   3. Haga clic en **OK (Aceptar)** para guardar el perfil.
6. (Opcional) Haga clic en **Enable X-Auth Support (Habilitar compatibilidad con autenticación de X)** si un endpoint debe conectarse con la puerta de enlace mediante una VPN externa (por ejemplo, un

© 2020 Palo Alto Networks, Inc.

cliente VPNC que se ejecuta en Linux). Si habilita la autenticación de X, debe brindar el nombre del **Group (Grupo)** y la **Group Password (Contraseña del grupo)** (si el endpoint lo requiere). De forma predeterminada, no es necesario que el usuario vuelva a autenticarse si caduca la clave que establece el túnel IPSec. Para solicitar que los usuarios se vuelvan a autenticar, deshabilite la opción **Skip Auth on IKE Rekey (Saltar autenticación de clave de registro de IKE)**.

También debe quitar la marca de la opción Skip Auth on IKE Rekey (Omitir autenticación al cambiar clave de IKE) si desea permitir la autenticación ampliada en los terminales con strongSwan, ya que estos exigen una nueva autenticación durante las negociaciones de asociaciones de seguridad (security association, SA) del intercambio de claves por internet (internet key exchange, IKE). Además, tiene que añadir el ajuste ***`closeaction=restart`*** *a la sección* `conn %default` *del archivo de configuración de IPSec de strongSwan. Para obtener más información sobre la configuración de IPSec de StrongSwan, consulte* Configuración de la autenticación para endpoints strongSwan Ubuntu y CentOS*.*

Si bien el acceso a X-Auth es compatible con endpoints de iOS y Android, ofrece una funcionalidad limitada para GlobalProtect en estos endpoints. En su lugar, use la aplicación de GlobalProtect para simplificar el acceso a todas las funciones de seguridad que proporciona GlobalProtect en los terminales con iOS y Android. La aplicación de GlobalProtect para iOS está disponible en la App Store de Apple. La aplicación de GlobalProtect para Android está disponible en Google Play.

STEP 6 | (Solo en modo de túnel) Especifique los criterios de selección de las configuraciones de ajustes de los clientes.

La puerta de enlace se sirve de los criterios de selección para determinar qué configuración debe suministrar a las aplicaciones de GlobalProtect que se conectan. Si tiene varias configuraciones, colóquelas en el orden correcto. En cuanto la puerta de enlace encuentra una coincidencia basándose en los valores especificados en **Source User (Usuario de origen)**, **OS (Sistema operativo)** y **Source Address (Dirección de origen)**, proporciona la configuración asociada al usuario. Así, las configuraciones más específicas deberán preceder a las más generales. Consulte el paso 13 si desea obtener instrucciones para ordenar la lista de configuraciones que tienen a su disposición los clientes.

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Client Settings (Configuración de clientes)**.
2. Seleccione una configuración de ajustes de cliente existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. Configure los valores adecuados en **Config Selection Criteria (Criterios de selección de configuraciones)**:
   - Para implementar esta configuración en usuarios o grupos de usuarios concretos, haga clic en **Add (Añadir)** en **Source User (Usuario de origen)** y añádalos. Para implementar esta configuración solo en usuarios que tienen aplicaciones en modo de funcionamiento anterior al inicio de sesión, seleccione **pre-logon (anterior al inicio de sesión)** en el menú desplegable **Source User (Usuario de origen)**. Para implementarla en todos los usuarios, seleccione **any (cualquiera)**.

     Para implementar la configuración en grupos concretos, primero debe asignar usuarios a los grupos como se explica en Habilitación de la asignación de grupo*.*
   - Para implementar esta configuración según el sistema operativo del terminal, como Android o Chrome, haga clic en **Add (Añadir)** en **OS (Sistema operativo)**. Para implementarla en todos los sistemas operativos, seleccione **Any (Cualquiera)**.
   - Para implementar esta configuración según la ubicación del usuario, haga clic en **Add (Añadir)** en **Region (Región)** o **IP Address (Dirección IP)** y elija el origen (IPv4 o IPv6). Para implementarla en

© 2020 Palo Alto Networks, Inc.

todas las ubicaciones de usuarios, no especifique ningún valor en **Region (Región)** ni en **IP Address (Dirección IP)**.

4. Haga clic en **OK (Aceptar)** para guardar los criterios de selección de las configuraciones.

STEP 7 | (Solo en modo de túnel) Configure los ajustes de anulación de autenticación para permitir que la puerta de enlace genere y acepte cookies seguras y cifradas para la autenticación del usuario.

Esta capacidad le permite al usuario brindar credenciales de inicio de sesión solo una vez durante el período de tiempo especificado (por ejemplo, cada 24 horas).

De manera predeterminada, las puertas de enlace autentican a los usuarios con un perfil de autenticación y un perfil de certificado opcional. Cuando la cancelación de autenticación está habilitada, GlobalProtect almacena en caché el resultado del inicio de sesión correcto y utiliza la cookie para autenticar al usuario en lugar de pedirle las credenciales. Para más información, consulte Autenticación de cookies en el portal o la puerta de enlace. Si los certificados de cliente son obligatorios, el terminal también debe proporcionar un certificado válido para obtener acceso.

Si debe bloquear el acceso a terminales cuyas cookies no han vencido porque, por ejemplo, se han perdido o los han robado, añada los dispositivos a la lista de bloqueo.

1. En el cuadro de diálogo Configuración de la puerta de enlace de GlobalProtect, seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)**.
2. Seleccione una configuración de ajustes de cliente existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. Configure los siguientes ajustes **Authentication Override (Cancelación de autenticación)**.
   - **Name (Nombre)**: identifica a la configuración.
   - **Generate cookie for authentication override (Generar cookie para la anulación de la autenticación)**: permite que la puerta de enlace genere cookies cifradas y específicas del endpoint y emite cookies de autenticación al endpoint.

     La cookie de autenticación incluye los siguientes campos:

     - `user (usuario)`: nombre de usuario que se utiliza para autenticar al usuario.
     - `domain (dominio)`: nombre de dominio del usuario.
     - `os (so)`: nombre de la aplicación que se utiliza en el dispositivo.
     - `hostID (ID de host)`: ID único asignado por GlobalProtect para identificar el host.
     - `gen time (fecha/hora de generación)`: fecha y hora en que se generó la cookie de autenticación.
     - `ip`: dirección IP del dispositivo que se utiliza para autenticarse correctamente en GlobalProtect y obtener la cookie.
   - **Accept cookie for authentication override (Aceptar cookie para la anulación de autenticación)**: permite que la puerta de enlace autentique usuarios con una cookie válida y cifrada. Cuando la aplicación presenta una cookie válida, la puerta de enlace verifica que el portal o la puerta de enlace cifraron la cookie, descifra la cookie y, luego, autentica el usuario.

     La aplicación de GlobalProtect debe conocer el nombre del usuario que realiza la conexión para cotejar y recuperar las cookies de autenticación asociadas de su terminal. Después de recuperarlas, las envía al portal o a la puerta de enlace para proceder a la autenticación del usuario.

     (Solo Windows) Si establece la opción Use Single Sign-On (Usar inicio de sesión único) en Yes (Sí) (SSO habilitado) en la configuración del agente del portal (Network (Red) > GlobalProtect > Portals (Portales) > <portal-config> > Agent (Agente) > <agent-config> > App (Aplicación)), la aplicación de GlobalProtect utiliza el nombre de usuario de Windows para recuperar la cookie de autenticación

© 2020 Palo Alto Networks, Inc.

local para el usuario. Si especifica No en Use Single Sign-On (Usar inicio de sesión único), deshabilita SSO, por lo que debe habilitar la opción Save User Credentials (Guardar credenciales de usuarios) *en la aplicación de GlobalProtect para que esta recupere la cookie de autenticación del usuario. Configure la opción Save User Credentials (Guardar credenciales de usuarios) en Yes (Sí) para guardar tanto el nombre de usuario como la contraseña o bien seleccione Save Username Only (Guardar solo nombre de usuario) para guardar únicamente el primero.*

- **Cookie Lifetime (Duración de la cookie)**: especifica las horas, días o semanas durante las cuales la cookie es válida (el valor predeterminado es 24 horas). El intervalo de horas es de 1 a 72; de semanas, de 1 a 52; y de días, de 1 a 365. Cuando vence la cookie, el usuario debe volver a introducir las credenciales de inicio de sesión y, entonces, la puerta de enlace cifra una cookie nueva para enviarla a la aplicación. Este valor puede ser el mismo o diferente del de **Cookie Lifetime (Duración de la cookie)** que configuró para el portal.
- **Certificate to Encrypt/Decrypt Cookie (Certificado para cifrar/descifrar la cookie)**: seleccione el certificado de RSA para cifrar o descifrar la cookie. Debe usar el mismo certificado en el portal y la puerta de enlace.

  Se recomienda configurar el certificado RSA para que utilice el algoritmo de resumen más fuerte que su red admite.

  El portal y la puerta de enlace usan el esquema de relleno de cifrado de RSA PKCS #1 v. 1.5 para generar la cookie con la clave de certificado pública y para descifrarla con la clave de certificado privada.

STEP 8 | (Solo en modo de túnel, opcional) Configure los grupos de IP de clientes empleados para asignar direcciones IPv4 o IPv6 a los adaptadores de red virtual en los terminales que se conectan a la puerta de enlace.

Configure solo los grupos de IP de los clientes en Network (Red) > GlobalProtect > Gateways (Puertas de enlace) > <gateway-config> > GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect) > Agent (Agente) > Client Settings (Configuración de clientes) > <client-setting> > Configs (Configuraciones) > IP Pools (Grupos de IP) o bien de las puertas de enlace en Network (Red) > GlobalProtect > Gateways (Puertas de enlace) > <gateway-config> > GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect) > Agent (Agente) > Client IP Pool (Grupo de IP de clientes).

En el modo sin túnel, no hace falta especificar los ajustes de grupos de IP ni de división de túneles en las configuraciones de las puertas de enlace internas porque las aplicaciones usan los ajustes de red asignados al adaptador de red físico.

No es posible utilizar objetos de dirección al configurar grupos de direcciones IP de puerta de enlace

1. En el cuadro de diálogo Configuración de la puerta de enlace de GlobalProtect, seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)**.
2. Seleccione una configuración de ajustes de cliente existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. Configure cualquiera de los ajustes siguientes en **IP Pools (Grupos de IP)**:
   - Para especificar el grupo de direcciones IP del servidor de autenticación para los terminales que requieren direcciones IP estáticas, marque la opción **Retrieve Framed-IP-Address attribute**

© 2020 Palo Alto Networks, Inc.

from authentication server (Recuperar atributo de dirección IP entramada del servidor de autenticación) y, luego, haga clic en **Add (Añadir)** para añadir la subred o el intervalo de direcciones IP a **Authentication Server IP Pool (Grupo de IP de servidor de autenticación)**. Una vez establecido el túnel, se crea una interfaz en el ordenador del usuario remoto con la dirección de la subred o del intervalo de IP que coincide con el atributo de IP entramada del servidor de autenticación.

El grupo de direcciones IP del servidor de autenticación debe ser lo suficientemente grande para admitir todas las conexiones simultáneas. La asignación de la dirección IP es estática y se conserva incluso después de que el usuario se desconecta.

- Para especificar el **IP Pool (Grupo de IP)** usado para asignar direcciones IPv4 o IPv6 a los endpoints que se conectan con la puerta de enlace, **añada** el intervalo/subred de la dirección IP. Puede añadir subredes o intervalos de IPv4 o IPv6, o una combinación de ambos.

  Para garantizar el enrutamiento de retorno adecuado a la puerta de enlace, debe usar un rango diferente de direcciones IP de aquellas asignadas a grupos de IP existentes en la puerta de enlace (si corresponde) y a los endpoints que están físicamente conectados a su red LAN. Le recomendamos que use un esquema de direcciones IP privadas.

4. Haga clic en **OK (Aceptar)** para guardar la configuración del grupo de IP.

STEP 9 | (Solo en modo de túnel, opcional) Deshabilite la división de la tunelización para garantizar que todo el tráfico, incluido el de la subred local, atraviese el túnel VPN para someterlo a inspección y aplicarle las políticas.

STEP 10 | (Solo en modo de túnel, opcional) Configure los ajustes de división de túneles según la ruta de acceso.

STEP 11 | (Solo en modo de túnel, opcional) Configure los ajustes de división de túneles según el dominio de destino.

STEP 12 | (Solo en modo de túnel, opcional) Configure los ajustes de división de túneles según la aplicación.

STEP 13 | (Solo en modo de túnel, opcional) Configure los ajustes del sistema de nombres de dominio (domain name system, DNS) para una configuración de ajustes de los clientes.

Si configura al menos un servidor DNS o un sufijo de DNS en la configuración de ajustes para los clientes con Network (Red) > GlobalProtect > Gateways (Puertas de enlace) > <gateway-config> > Agent (Agente) > Client Settings (Configuración de clientes) > <client-settings-config> > Network Services (Servicios de red), la puerta de enlace envía a los endpoints la configuración de ambos elementos de DNS, aun cuando configure servidores DNS y sufijos de DNS globales (para toda la puerta de enlace).

Si no configura ningún servidor DNS ni ningún sufijo de DNS en la configuración de ajustes para los clientes, la puerta de enlace envía a los endpoints los servidores DNS y los sufijos de DNS globales, siempre que haya configurado Network (Red) > GlobalProtect > Gateways (Puertas de enlace) > <gateway-config> > Agent (Agente) > Network Services (Servicios de red).

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Client Settings (Configuración de clientes)**.
2. Seleccione una configuración de ajustes de cliente existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. Configure cualquiera de los ajustes siguientes en **Network Services (Servicios de red)**:

© 2020 Palo Alto Networks, Inc.

- En **DNS Server (Servidor DNS)**, especifique la dirección IP del servidor al que envía las consultas de DNS la aplicación de GlobalProtect que tiene esta configuración de clientes. Puede añadir hasta 10 servidores DNS separando las direcciones IP con coma.
- En **DNS Suffix (Sufijo de DNS)**, especifique el sufijo que deben utilizar los terminales de forma local cuando encuentren nombres de host incompletos que no pueden resolver.

STEP 14 | (Solo en modo de túnel) Organice las configuraciones de agente de puerta de enlace de modo que la configuración correcta se implemente en cada aplicación de GlobalProtect.

Cuando se conecta una aplicación, la puerta de enlace compara la información de origen del paquete con las configuraciones de agentes definidas en **Agent (Agente)** > **Client Settings (Configuración de clientes)**. Al igual que con la evaluación de reglas de seguridad, la puerta de enlace busca una coincidencia empezando por la parte superior de la lista. Cuando encuentra una coincidencia, brinda la configuración correspondiente a la aplicación.

- Para mover una configuración de puerta de enlace hacia arriba en la lista de configuraciones, selecciónela y haga clic en **Move Up (Subir)**.
- Para mover una configuración de puerta de enlace hacia abajo en la lista de configuraciones, selecciónela y haga clic en **Move Down (Bajar)**.

STEP 15 | (Solo en modo de túnel, opcional) Configure los grupos de direcciones IP globales empleados para asignar direcciones IPv4 o IPv6 a los adaptadores de red virtual en todos los endpoints que se conectan a la puerta de enlace.

Esta opción le permite simplificar la configuración mediante la definición de grupos de IP en el nivel de la puerta de enlace, en lugar de definir grupos de IP para cada configuración de cliente en la configuración de la puerta de enlace.

Configure solo los grupos de IP de las puertas de enlace en (Network (Red) > GlobalProtect > Gateways (Puertas de enlace) > <gateway-config> > Agent (Agente) > Client IP Pool (Grupo de IP de clientes) o bien de los clientes enNetwork (Red) > GlobalProtect > Gateways (Puertas de enlace) > <gateway-config> > Agent (Agente) > Client Settings (Configuración de clientes) > <client-setting> > IP Pools (Grupos de IP).

No es posible utilizar objetos de dirección al configurar grupos de direcciones IP de puerta de enlace

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Client IP Pool (Grupo de IP de clientes)**.
2. **Añada** el intervalo/subred de las direcciones IP usadas para asignar las direcciones IPv4 o IPv6 a todos los endpoints que se conectan a la puerta de enlace. Puede añadir subredes o intervalos de IPv4 o IPv6, o una combinación de ambos.

   Para garantizar el enrutamiento de retorno adecuado a la puerta de enlace, debe usar un rango diferente de direcciones IP de aquellas asignadas a grupos de IP existentes en la puerta de enlace (si corresponde) y a los endpoints que están físicamente conectados a su red LAN. Le recomendamos que use un esquema de direcciones IP privadas.

STEP 16 | (Solo en modo de túnel) Especifique los ajustes de configuración de red para los terminales.

Los ajustes de red no son necesarios para las configuraciones de puerta de enlace interna en el modo sin túnel, dado que la aplicación de GlobalProtect usa los ajustes de red asignados al adaptador de red físico.

© 2020 Palo Alto Networks, Inc.

En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Network Services (Servicios de red)** y, a continuación, configure cualquiera de los siguientes ajustes de configuración de red:

- Si el cortafuegos tiene configurada una interfaz como cliente DHCP, configure esa interfaz en **Inheritance Source (Origen de herencia)** para que se asignen sus mismos ajustes a la aplicación de GlobalProtect. También puede marcar la opción **Inherit DNS Suffixes (Heredar sufijos de DNS)** para heredar lo sufijos del origen de herencia.
- Asigne manualmente el servidor **Primary DNS (DNS principal)**, el servidor **Secondary DNS (DNS secundario)**, el servidor **Primary WINS (WINS principal)**, el servidor **Secondary WINS (WINS secundario)** y el **DNS Suffix (Sufijo DNS)**. Para introducir varios sufijos DNS (hasta 100), sepárelos con una coma.

El DNS Suffix (Sufijo DNS) no puede incluir caracteres que no sean ASCII.

STEP 17 | (Opcional) Modifique los ajustes de tiempo de espera por defecto para los endpoints.

En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Connection Settings (Configuración de conexión)** y, a continuación, configure los siguientes ajustes del área Timeout Configuration (Configuración de tiempo de espera):

- En **Login Lifetime (Duración de sesión)**, modifique la vigencia máxima de cada sesión en la puerta de enlace; el valor predeterminado es 30 días. Durante este período, el usuario permanece conectado siempre que la puerta de enlace reciba una comprobación HIP del endpoint dentro del período de **Inactivity Logout (Cierre de sesión por inactividad)**. Después de este período, la sesión de inicio de sesión finaliza automáticamente.
- En **Inactivity Logout (Cierre de sesión por inactividad)**, especifique cuánto tiempo debe pasar para que se cierre automáticamente cada sesión inactiva; el valor predeterminado es 3 horas. Se cierra la sesión de GlobalProtect de los usuarios si la puerta de enlace no recibe una comprobación HIP desde el endpoint durante el período de tiempo configurado.
- En **Disconnect on Idle (Desconectar por inactividad)**, especifique cuántos minutos deben transcurrir para que se cierre la sesión en GlobalProtect de los usuarios inactivos; el valor predeterminado es 180 minutos. Se cierra la sesión de GlobalProtect de los usuarios si la aplicación de GlobalProtect no envió tráfico a través del túnel VPN dentro del período de tiempo configurado. Este ajuste solo se aplica a las aplicaciones de GlobalProtect que emplean el método de conexión bajo demanda.

STEP 18 | (Opcional) Configure la restauración automática de los túneles de VPN SSL.

Si se pierde la conexión de GlobalProtect porque la red está inestable o porque cambia el estado del terminal, puede permitir o impedir que la aplicación de GlobalProtect restablezca automáticamente el túnel de VPN en puertas de enlace concretas. Para ello, configure la restauración automática de los túneles de VPN SSL.

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Connection Settings (Configuración de conexión)**.
2. En Authentication Cookie Usage Restrictions (Restricciones de uso de cookies de autenticación), configure una de estas opciones:
   - Para impedir que la aplicación de GlobalProtect restablezca automáticamente el túnel de VPN en esta puerta de enlace, marque **Disable Automatic Restoration of SSL VPN (Deshabilitar restauración automática de VPN SSL)**.
   - Para permitir que la aplicación de GlobalProtect restablezca automáticamente el túnel de VPN en esta puerta de enlace, quite la marca de **Disable Automatic Restoration of SSL VPN (Deshabilitar restauración automática de VPN SSL)**, que está marcada de forma predeterminada.

© 2020 Palo Alto Networks, Inc.

STEP 19 | (Opcional) Configure la aplicación de la dirección IP de origen en las cookies de autenticación.

Puede configurar el portal o la puerta de enlace de GlobalProtect para que acepte las cookies de los terminales solo cuando su dirección IP coincida con las direcciones IP de origen para las que se hayan emitido las cookies originalmente o bien con un intervalo concreto de direcciones IP de la red, el cual puede definir con una máscara de subred de enrutamiento entre dominios sin clases (classless inter-domain routing, CIDR), como /24 o /32. Por ejemplo, si se emite originalmente una cookie de autenticación para un terminal cuya dirección IP de origen pública es 201.109.11.10 y define en /24 la máscara de subred del intervalo de direcciones IP de la red, dicha cookie es válida después en los terminales cuyas direcciones IP de origen públicas se encuentran dentro del intervalo 201.109.11.0/24.

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Connection Settings (Configuración de conexión)**.
2. En la sección Authentication Cookie Usage Restrictions (Restricciones de uso de cookies de autenticación), marque **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) (Restringir uso de cookies de autenticación para la restauración automática de túneles de VPN o la sustitución de autenticación)** y, a continuación, configure una de estas condiciones:
   - Si selecciona **The original Source IP for which the authentication cookie was issued (A la IP de origen para la que se emite originalmente)**, la cookie de autenticación solo es válida si la dirección IP de origen pública del terminal que intenta usarla es idéntica a la del terminal para el que se ha emitido.
   - Si selecciona **The original Source IP network range (Al intervalo de IP de origen de red originales)**, la cookie de autenticación solo es válida si la dirección IP de origen pública del terminal que intenta usarla se encuentra dentro del intervalo indicado. En **Source IPv4 Netmask (Máscara de red IPv4 de origen)** o **Source IPv6 Netmask (Máscara de red IPv6 de origen)**, defina la máscara de subred del intervalo de direcciones IP de la red en las que tiene validez la cookie de autenticación, por ejemplo, `32` o `128`).

STEP 20 | (Solo en modo de túnel) Excluya el tráfico HTTP o HTTPS de transmisión de vídeo procedente del túnel VPN.

STEP 21 | (Opcional) Defina los mensajes de notificación que ven los usuarios finales cuando se aplica una regla de seguridad con un HIP.

Este paso solo se aplica si ha creado HIP y los ha añadido a las políticas de seguridad. Para obtener más información sobre cómo configurar la función HIP y cómo crear mensajes de notificación de HIP, consulte Información de host.

1. En el diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **HIP Notification (Notificación de HIP)**.
2. Seleccione una configuración de notificación HIP existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. Configure los siguientes ajustes:
   - Seleccione el objeto o el perfil **Host Information (Información del host)** al cual se aplica este mensaje.
   - Puede mostrar el mensaje cuando se encuentra una coincidencia con el HIP en la política o cuando no se encuentra. Seleccione **Match Message (Mensaje si hay coincidencia)** en el primer caso o **Not Match Message (Mensaje si no hay coincidencia)** en el segundo y, a continuación, marque **Enable (Habilitar)** para habilitar las notificaciones. Si lo desea, cree mensajes para ambos casos en función de los objetos cotejados y los objetivos de la política. Para **Match Message (Mensaje de coincidencia)**, también puede habilitar la opción **Include Mobile App List (Incluir en la lista de aplicaciones móviles)** para indicar las aplicaciones que pueden activar la coincidencia de HIP.
   - Seleccione si desea visualizar el mensaje como **System Tray Balloon** o como **Pop Up Message**.

© 2020 Palo Alto Networks, Inc.

- En **Template (Plantilla)**, introduzca el texto del mensaje con el formato adecuado y haga clic en **OK(Aceptar)**.
- Repita estos pasos para cada mensaje que quiera definir.

STEP 22 | Guarde la configuración de la puerta de enlace.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes.
2. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 23 | (Opcional) Configure la aplicación de GlobalProtect de modo que muestre la etiqueta que identifica la ubicación de esta puerta de enlace cuando se conectan los usuarios finales. Para ello, especifique la ubicación física del cortafuegos en el que ha configurado la puerta de enlace.

Si se produce un comportamiento inusual, como un rendimiento deficiente de la red, los usuarios finales pueden facilitar la ubicación a los profesionales del servicio de asistencia, que les resulta útil para solucionar el problema. Ese dato también permite determinar la proximidad a la puerta de enlace para evaluar si es preciso cambiar a otra puerta de enlace más cercana.

Si no especifica la ubicación de la puerta de enlace, la aplicación de GlobalProtect muestra este campo vacío.

- **En la interfaz de línea de comandos (command-line interface, CLI)**: utilice el siguiente comando de la CLI para especificar la ubicación física del cortafuegos en el que ha configurado la puerta de enlace:

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- **En la interfaz de programación de aplicaciones (application programming interface, API) con lenguaje de marcado extensible (extensible markup language, XML)**: utilice el siguiente comando de la API XML para especificar la ubicación física del cortafuegos en el que ha configurado la puerta de enlace:
  - **devices (dispositivos)**: nombre del cortafuegos en el que ha configurado la puerta de enlace.
  - **location (ubicación)**: ubicación del cortafuegos en el que ha configurado la puerta de enlace.

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```


© 2020 Palo Alto Networks, Inc.

Tráfico de división de túnel (Split Tunnel) en puertas de enlace de GlobalProtect

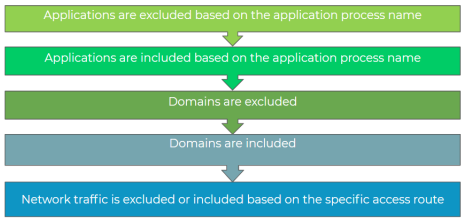
Puede configurar el tráfico de división de túnel en función de una ruta de acceso, dominio de destino, aplicación y aplicación de transmisión de vídeo HTTP / HTTPS.

Con una suscripción a GlobalProtect, puede forzar o aplicar reglas de división de túnel en los endpoints de Windows y macOS.

La capacidad de división de túnel le permite conservar el ancho de banda y enrutar el tráfico para:

- Cree un túnel en las aplicaciones de la nube pública y SaaS empresariales para lograr una visibilidad y un control integrales de las aplicaciones SaaS y evitar los riesgos asociados con Shadow IT en entornos donde no es posible tunelizar todo el tráfico.
- Envíe tráfico sensible a la latencia, como VoIP, fuera del túnel VPN. El resto del tráfico pasa a través de la VPN para la inspección y cumplimiento de políticas por parte de la puerta de enlace de GlobalProtect.
- Excluya el tráfico HTTP o HTTPS de transmisión de vídeo procedente del túnel VPN. Las aplicaciones de transmisión de vídeo, como YouTube y Netflix, consumen grandes cantidades de ancho de banda. Mediante la exclusión del tráfico de transmisión de vídeo de menor riesgo desde el túnel VPN, puede disminuir el consumo de banda ancha en la puerta de enlace.

Las reglas de división de túnel se aplican para los endopoints de Windows y macOS en el siguiente orden:



Consulte las siguientes secciones sobre cómo configurar el tráfico de división de túnel en las puertas de enlace:

- Configuración de división de túnel (Split Tunnel) basada en la ruta de acceso
- Configure de una división de túnel (Split Tunnel) basada en el dominio y la aplicación
- Exclusión de tráfico de vídeo del túnel VPN de GlobalProtect

Configuración de división de túnel (Split Tunnel) basada en la ruta de acceso

Si no se incluye o excluye rutas, todas las solicitudes se dirigirán a través del túnel VPN (sin división de túneles). Puede incluir o excluir el tráfico de subred IP de destino específico para que no se envíe a través del túnel VPN. Las rutas que envía a través del túnel VPN pueden definirse como las rutas que incluye en el túnel, como rutas que excluye del túnel o ambas. Por ejemplo, puede establecer la división de túneles para permitir a los usuarios remotos acceder a internet sin pasar por el túnel VPN. Las rutas más específicas tienen prioridad sobre las menos específicas.

Cuando defina el tráfico de división de túnel para incluir rutas de acceso, estas son las rutas que la puerta de enlace envía a los endpoints de los usuarios remotos para especificar qué tráfico pueden enviar a través del túnel VPN. Cuando defina el tráfico de división de túnel para excluir rutas de acceso, estas rutas se envían a través del adaptador físico en el endpoint en lugar de enviarse a través del túnel VPN de GlobalProtect

© 2020 Palo Alto Networks, Inc.

a través del adaptador virtual (el túnel). Al excluir el tráfico de división de túnel por las rutas de acceso, puede enviar tráfico sensible a la latencia o que consuma una gran cantidad ancho de banda fuera del túnel VPN. Por otra parte, el resto del tráfico se enruta a través de la VPN para la inspección y el cumplimiento de políticas por parte de la puerta de enlace de GlobalProtect.

Las rutas locales tienen prioridad sobre las rutas enviadas desde la puerta de la enlace. Si habilita la división de túneles, los usuarios pueden acceder directamente a los proxies y a los recursos locales, como las impresoras locales, sin enviar tráfico de la subred local por el túnel VPN. Si deshabilita la división de la tunelización, todo el tráfico debe atravesar el túnel de VPN para someterlo a inspección y aplicarle las políticas siempre que los usuarios están conectados a GlobalProtect. Según marque o no la opción de acceso directo a la red local, el tráfico IPv4 e IPv6 muestra estos comportamientos:

Table 1: Comportamiento del tráfico IPv4

Tráfico IPv4 a subred local	Opción No direct access to local network (Sin acceso directo a la red local) habilitada		Opción No direct access to local network (Sin acceso directo a la red local) deshabilitada	
	Antes de establecer el túnel	Después de establecer el túnel	Antes de establecer el túnel	Después de establecer el túnel
Nuevo tráfico entrante	Se permite el tráfico en la subred local a través del adaptador físico.	(Solo en Windows 10) Cuando deshabilita el túnel dividido según el dominio de destino y la aplicación, el tráfico se envía a través del túnel VPN. Si habilita el túnel dividido según el dominio de destino y la aplicación, se permite el tráfico en la subred local a través del adaptador físico. (Solo en macOS) Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.

© 2020 Palo Alto Networks, Inc.

Tráfico IPv4 a subred local	Opción No direct access to local network (Sin acceso directo a la red local) habilitada		Opción No direct access to local network (Sin acceso directo a la red local) deshabilitada	
Nuevo tráfico saliente	Se permite el tráfico en la subred local a través del adaptador físico.	El tráfico se envía a través del túnel de VPN.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.
Tráfico existente	Se permite el tráfico en la subred local a través del adaptador físico.	Se finaliza el tráfico.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.

Table 2: Comportamiento del tráfico IPv6

Tráfico IPv6 a subred local	Opción No direct access to local network (Sin acceso directo a la red local) habilitada		Opción No direct access to local network (Sin acceso directo a la red local) deshabilitada	
	Antes de establecer el túnel	Después de establecer el túnel	Antes de establecer el túnel	Después de establecer el túnel
Nuevo tráfico entrante	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.
Nuevo tráfico saliente	Se permite el tráfico en la subred local a través del adaptador físico.	El tráfico se envía a través del túnel de VPN.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.
Tráfico existente	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.	Se permite el tráfico en la subred local a través del adaptador físico.

Utilice los siguientes pasos para configurar la división de túnel basada en rutas de acceso.

STEP 1 | Antes de comenzar:

1. Configure una puerta de enlace de GlobalProtect.
2. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* para modificar una puerta de enlace existente o añadir una nueva.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Habilite una división de túnel.

1. En el cuadro de diálogo **GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect)**, seleccione **Agent (Agente)** > **Tunnel Settings (Configuración de túneles)** para habilitar **Tunnel Mode (Modo de túnel)**.
2. Configure los parámetros del túnel para la aplicación de GlobalProtect.

STEP 3 | (Solo en modo de túnel) Deshabilite la división de túneles para garantizar que todo el tráfico, incluido el de la subred local, atraviese el túnel VPN para someterlo a inspección y aplicarle las políticas.

1. En el cuadro de diálogo **GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect)**, seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)** > *<client-setting-config>* para seleccionar una configuración de ajustes del cliente existente y añadir una nueva.
2. Seleccione **Split Tunnel (Dividir túnel)** > **Access Route (Ruta de acceso)** y, a continuación, marque la opción **No direct access to local network (Sin acceso directo a la red local)**.

   Si habilita esta opción, se deshabilita el tráfico de la división de túneles y los usuarios no pueden enviar tráfico directamente a los proxies ni a los recursos locales mientras están conectados a GlobalProtect.

STEP 4 | (Solo en modo de túnel) Configure los ajustes de división de túneles según la ruta de acceso.

Los ajustes de división de túneles se asignan al adaptador de red virtual en el endpoint cuando la aplicación de GlobalProtect establece un túnel con la puerta de enlace.

No especifique la misma ruta como ruta de acceso de inclusión y de exclusión, ya que eso genera un error de configuración.

Puede enrutar cierto tráfico para incluirlo o excluirlo del túnel especificando las subredes de destino o el objeto de dirección (de tipo **IP Netmask (Máscara de red IP)**).

1. En el cuadro de diálogo **GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect)**, seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)** > *<client-setting-config>* para seleccionar una configuración de ajustes del cliente existente y añadir una nueva.
2. Configure uno de los siguientes ajustes de túnel dividido basado en la ruta de acceso en **Split Tunnel (Túnel dividido)** (**Split Tunnel [Túnel dividido]** > **Access Route [Ruta de acceso]**):
   - (Opcional) En el área **Includes (Inclusiones)**, **añada** las subredes de destino o el objeto de dirección (del tipo **IP Netmask (Máscara de red IP)**) para dirigir solo determinado tráfico destinado para su red LAN a GlobalProtect. Puede incluir subredes IPv6 o IPv4.

     En PAN-OS 8.0.2 y versiones posteriores, se pueden usar hasta 100 rutas de acceso para incluir el tráfico en una configuración de puerta de enlace de división de túnel. Se debe combinar con la aplicación de GlobalProtect 4.1.x o una versión posterior para poder usar hasta 1000 rutas de acceso.
   - (Opcional) En el área **Excludes (Exclusiones)**, **añada** las subredes de destino o el objeto de dirección (del tipo **IP Netmask (Máscara de red IP)**) que desea que la aplicación excluya. Las rutas excluidas deben ser más específicas que las rutas incluidas para evitar excluir más tráfico del que se pretende. Puede excluir subredes IPv6 o IPv4. El cortafuegos admite hasta 100 rutas de acceso de exclusión en una configuración de puerta de enlace de división de túnel. Se debe combinar con la aplicación de GlobalProtect 4.1.x o una versión posterior para poder usar hasta 200 rutas de acceso de exclusión.

     No puede excluir rutas de acceso para endpoints que utilizan Android en Chromebooks. Solo las rutas IPv4 son compatibles con Chromebooks.
3. Haga clic en **OK (Aceptar)** para guardar la configuración del túnel dividido.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Guarde la configuración de la puerta de enlace.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes.
2. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Configure de una división de túnel (Split Tunnel) basada en el dominio y la aplicación

Cuando configure una división de túnel para incluir todo el tráfico (IPv4 e IPv6) basado en el dominio de destino y el puerto (opcional) o la aplicación, todo el tráfico que va a ese dominio o aplicación específico se enviará a través del túnel VPN para la inspección y la aplicación de políticas. Por ejemplo, puede permitir que todo el tráfico de Salesforce atraviese el túnel VPN con el dominio de destino ***Salesforce.com**. Al incluir todo el tráfico de Salesforce en el túnel VPN, puede proporcionar acceso seguro a todo el dominio y subdominios de Salesforce. Puede configurar la división de túneles sin especificar ninguna subred de direcciones IP de destino. De ese modo, extiende dicha función a los dominios y aplicaciones con direcciones IP públicas dinámicas, como las de SaaS y las de nubes públicas.

Cuando configure una división de túnel para excluir el tráfico (IPv4 e IPv6) en función del dominio y el puerto de destino (opcional) o la aplicación, todo el tráfico para esa aplicación o dominio específico se enviará directamente al adaptador físico en el endpoint sin inspección. Por ejemplo, puede excluir todo el tráfico de Skype desde el túnel VPN mediante el nombre de proceso de la aplicación **C:\Program Files (x86)\Skype\Phone\Skype**.

Esta función solo se admite en endpoints con Windows 7 Service Pack 2 y versiones posteriores y en macOS 10.10 y versiones posteriores.

Utilice los siguientes pasos para configurar una división de túnel para incluir o excluir el tráfico en función del dominio de destino o el nombre del proceso de la aplicación.

STEP 1 | Antes de comenzar:

1. Configure una puerta de enlace de GlobalProtect.
2. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* para modificar una puerta de enlace existente o añadir una nueva.

STEP 2 | Habilite una división de túnel.

1. En el cuadro de diálogo **GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect)**, seleccione **Agent (Agente)** > **Tunnel Settings (Configuración de túneles)** para habilitar **Tunnel Mode (Modo de túnel)**.
2. Configure los parámetros del túnel para la aplicación de GlobalProtect.

STEP 3 | (Solo en modo de túnel) Configure los ajustes de división de túneles según el dominio de destino. Estos ajustes se asignan al adaptador de red virtual en el endpoint cuando la aplicación de GlobalProtect establece un túnel con la puerta de enlace.

(Requiere la aplicación de GlobalProtect™ 5.2.)

Puede aplicar tráfico DNS además del tráfico de red si ya ha especificado **Both Network Traffic and DNS (Tráfico de red y DNS)** como **Split-Tunnel Option (Opción de túnel dividido)** en el área **App Configurations (Configuraciones de aplicaciones)** de su portal de GlobalProtect.

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)** > *<client-setting-config>* para seleccionar una configuración de ajustes del cliente existente o añadir una nueva.

© 2020 Palo Alto Networks, Inc.

2. (Opcional) **Añada** las aplicaciones de nube pública o SaaS que desee enrutar a GlobalProtect a través de la conexión VPN mediante el dominio de destino y puerto (**Split Tunnel (División de túneles)** > **Domain and Application (Dominio y aplicación)** > **Include Domain (Incluir dominio)**). Puede añadir hasta 200 entradas a la lista. Por ejemplo, añada **`*.gmail.com`** para permitir que todo el tráfico de Gmail atraviese el túnel VPN.
3. (Opcional) Haga clic en **Add (Añadir)** para añadir aplicaciones de nube pública o SaaS que desea excluir del túnel VPN mediante el dominio de destino y puerto (**Split Tunnel [Túnel dividido]** > **Domain and Application [Dominio y aplicación]** > **Exclude Domain [Excluir dominio]**). Puede añadir hasta 200 entradas a la lista. Por ejemplo, añada **`*.target.com`** para excluir todo el tráfico de destino del túnel VPN.
4. Haga clic en **OK (Aceptar)** para guardar la configuración del túnel dividido.

STEP 4 | (Solo en modo de túnel) Configure la configuración de la división de túnel en función de la aplicación.

El tráfico de Safari no se puede añadir a la regla de división de túnel basada en aplicaciones en los endpoints de macOS.

Puede usar variables de entorno para configurar una división de túnel basada en la aplicación en los endpoints de Windows y macOS.

1. En el cuadro de diálogo GlobalProtect Gateway Configuration (Configuración de la puerta de enlace de GlobalProtect), seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)** > *<client-setting-config>* para seleccionar una configuración de ajustes del cliente existente o añadir una nueva.
2. (Opcional) Haga clic en **Add (Añadir)** para añadir aplicaciones de nube pública o SaaS que desea enrutar a GlobalProtect a través de la conexión VPN mediante el nombre de proceso de la aplicación (**Split Tunnel [Túnel dividido]** > **Domain and Application [Dominio y aplicación]** > **Include Client Application Process Name [Incluir nombre de proceso de la aplicación del cliente]**). Puede añadir hasta 200 entradas a la lista. Por ejemplo, añada **`/Applications/RingCentral for Mac.app/Contents/MacOS/Softphone`** para permitir que todo el tráfico basado en RingCentral pase a través del túnel VPN en los endpoints de macOS.
3. (Opcional) Haga clic en **Add (Añadir)** para añadir aplicaciones de nube pública o SaaS que desea excluir del túnel VPN mediante el nombre de proceso de la aplicación (**Split Tunnel [Túnel dividido]** > **Domain and Application [Dominio y aplicación]** > **Exclude Client Application Process Name [Excluir nombre de proceso de la aplicación del cliente]**). Puede añadir hasta 200 entradas a la lista. Por ejemplo, añada **`/Applications/Microsoft Lync.app/Contents/MacOS/Microsoft Lync`** para excluir todo el tráfico de aplicación de Microsoft Lync del túnel VPN.
4. Haga clic en **OK (Aceptar)** para guardar la configuración del túnel dividido.

STEP 5 | Guarde la configuración de la puerta de enlace.

1. Haga clic en **OK (Aceptar)** para guardar la configuración de la puerta de enlace.
2. **Commit (Confirmar)** los cambios.

Exclusión de tráfico de vídeo del túnel VPN de GlobalProtect

Puede configurar la división del túnel para excluir el tráfico de transmisión de vídeo HTTP/HTTPS en un dominio específico para que no se envíe a través del túnel VPN. Esto permite que el tráfico de vídeo vaya directamente desde las interfaces físicas en el endpoint. La funcionalidad App-ID en el cortafuegos identifica la transmisión de vídeo antes de que el tráfico pueda dividirse con el túnel. Mediante la exclusión del tráfico de transmisión de vídeo de menor riesgo (como YouTube y Netflix) desde el túnel VPN, puede disminuir el consumo de banda ancha en la puerta de enlace.

Todos los tipos de tráfico de vídeo se redirigen a las siguientes aplicaciones de transmisión de vídeo:

© 2020 Palo Alto Networks, Inc.

- YouTube
- Dailymotion
- Netflix

Si excluye cualquier otra aplicación de transmisión de vídeo del túnel de VPN, solo se redirigen a esas aplicaciones los siguientes tipos de tráfico de vídeo:

- MP4
- WebM
- MPEG

Utilice los siguientes pasos para configurar una división de túnel para excluir el tráfico de transmisión de vídeo del túnel VPN.

STEP 1 | Antes de comenzar:

1. Siga estos requisitos previos:
   - Esta función solo se admite en endpoints con Windows 7 Service Pack 2 y versiones posteriores y en macOS 10.10 y versiones posteriores.
   - Debe asegurarse de que los grupos de IP utilizados para asignar direcciones IP a los adaptadores de red virtual en estos puntos finales no incluyan ninguna dirección IPv6. Si el adaptador físico en un endpoint de Windows o macOS admite solo direcciones IPv4, el usuario del endpoint no puede acceder a las aplicaciones de transmisión de vídeos que usted excluye del túnel VPN cuando configura que la puerta de enlace de GlobalProtect asigne direcciones IPv6 a los adaptadores de red virtual en los endpoints que se conectan con la puerta de enlace.
   - Si excluye el tráfico de transmisión de vídeo del túnel VPN, no incluya aplicaciones de navegador web, como Firefox o Chrome, en el túnel VPN. Esto garantiza que no exista lógica en conflicto en la configuración de túnel dividido y que sus usuarios puedan transmitir vídeos de los navegadores web.
   - Para excluir el tráfico de la aplicación Sling TV del túnel VPN, configure la división de túnel basada en una aplicación.
2. Configure una puerta de enlace de GlobalProtect.
3. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* para modificar una puerta de enlace existente o añadir una nueva.

STEP 2 | Habilite una división de túnel.

1. En el cuadro de diálogo **GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect)**, seleccione **Agent (Agente)** > **Tunnel Settings (Configuración de túneles)** para habilitar **Tunnel Mode (Modo de túnel)**.
2. Configure los parámetros del túnel para la aplicación de GlobalProtect.

STEP 3 | (Solo en modo de túnel) Excluya el tráfico HTTP o HTTPS de transmisión de vídeo procedente del túnel de VPN.

1. En el cuadro de diálogo **GlobalProtect Gateway Configuration (Configuración de puerta de enlace de GlobalProtect)**, seleccione **Agent (Agente)** > **Video Traffic (Tráfico de vídeo)**.
2. Habilite la opción **Exclude video applications from the tunnel (Excluir aplicaciones de vídeo del túnel)**.

   Si habilita esta opción, pero no excluye del túnel VPN determinadas aplicaciones de transmisión de vídeo, se excluye todo el tráfico de transmisión de vídeo.
3. (Opcional) Haga clic en **Browse (Explorar)** para buscar la lista de **Applications (Aplicaciones)** y ver todas las aplicaciones de transmisión de vídeos que puede excluir del túnel VPN. Haga clic en el icono

© 2020 Palo Alto Networks, Inc.

de añadir ( ) en las aplicaciones que desee excluir. Por ejemplo, haga clic en el icono de añadir de **directv** para excluir el tráfico de transmisión de vídeos de DIRECTV del túnel VPN.

4. **Añada** las aplicaciones de transmisión de vídeo que desee excluir del túnel VPN mediante el menú desplegable **Applications (Aplicaciones)**, que es una versión abreviada de la lista **Applications (Aplicaciones)**. Puede añadir hasta 200 entradas de aplicaciones de vídeo a la lista. Por ejemplo, seleccione **youtube-streaming (Transmisión de YouTube)** para excluir del túnel de VPN todo el tráfico de transmisión de vídeo basado en YouTube.

STEP 4 | Guarde la configuración de la puerta de enlace.

1. Haga clic en **OK (Aceptar)** para guardar la configuración de la puerta de enlace.
2. **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Portales de GlobalProtect

- Descripción general del portal de GlobalProtect
- Tareas de requisito previo para la configuración del portal de GlobalProtect
- Configuración del acceso al portal de GlobalProtect
- Definición de las configuraciones de agente de GlobalProtect
- Personalización de la aplicación de GlobalProtect
- Personalización de las páginas de inicio de sesión, bienvenida y ayuda del portal de GlobalProtect
- VPN sin cliente de GlobalProtect

© 2020 Palo Alto Networks, Inc.

Descripción general del portal de GlobalProtect

El portal de GlobalProtect proporciona las funciones de gestión para su infraestructura de GlobalProtect. Cada endpoint que participa en la red de GlobalProtect recibe información de configuración desde el portal, incluida la información sobre las puertas de enlace disponibles y los certificados de cliente que pueden ser necesarios para conectarse a las puertas de enlace. Además, el portal controla el comportamiento y la distribución del software de la aplicación de GlobalProtect para los endpoints con macOS y Windows.

El portal no distribuye la aplicación de GlobalProtect para su uso en endpoints móviles. Para obtener la aplicación de GlobalProtect para endpoints móviles, los usuarios finales deben descargarla desde la tienda del dispositivo: App Store para iOS, Google Play para Android, Chrome Web Store para Chromebooks o Microsoft Store para Windows 10 UWP. Sin embargo, las configuraciones de agente que se implementan en los usuarios de aplicaciones móviles controlan las puertas de enlace a las cuales los endpoints móviles tienen acceso. Para obtener más detalles sobre las versiones compatibles, consulte ¿Qué versiones de sistema operativo son compatibles con GlobalProtect?

Además de distribuir el software de la aplicación de GlobalProtect, puede configurar el portal GlobalProtect para proporcionar acceso remoto seguro a aplicaciones web empresariales comunes que utilizan tecnologías HTML, HTML5 y JavaScript. Los usuarios tienen la ventaja de contar con el acceso seguro de los navegadores web con SSL sin instalar el software de la aplicación de GlobalProtect. Esto resulta útil cuando necesita permitir el acceso de un socio o contratista a las aplicaciones y habilitar de manera segura activos no gestionados, incluidos los endpoints personales. Consulte VPN sin cliente de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Tareas de requisito previo para la configuración del portal de GlobalProtect

Antes de poder configurar el portal de GlobalProtect, debe haber realizado las tareas siguientes:

- Cree las interfaces (y zonas) para el cortafuegos donde planifique configurar el portal. Consulte Creación de interfaces y zonas para GlobalProtect.
- Configurar el certificado del servidor del portal, el certificado del servidor de la puerta de enlace, los perfiles de servicio SSL/TLS y, opcionalmente, cualquier certificado de cliente que se vaya a implementar a los usuarios finales para habilitar las conexiones SSL/TLS para los servicios de GlobalProtect™. Consulte Habilitación de SSL entre componentes de GlobalProtect.
- Definir los perfiles de autenticación y los perfiles del certificado opcionales que el portal puede usar para la autenticación de usuarios de GlobalProtect. Consulte Autenticación.
- Configuración de una puerta de enlace de GlobalProtect y entender Prioridad de la puerta de enlace en una configuración de varias puertas de enlace.

© 2020 Palo Alto Networks, Inc.

Configuración del acceso al portal de GlobalProtect

Tras completar las Tareas de requisitos previos para la configuración del portal de GlobalProtect, configure el portal de GlobalProtect del siguiente modo:

STEP 1 | Añada el portal.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, haga clic en **Add (Añadir)** para añadir un portal.
2. Introduzca un **Name (Nombre)** para el portal.

   El nombre de la puerta de enlace no puede contener espacios y debe ser exclusivo para cada sistema virtual.
3. (Opcional) Seleccione el sistema virtual al que pertenece este portal en el campo **Location**.

STEP 2 | Especifique los ajustes de red que permitan a la aplicación comunicarse con el portal.

Si no creó la interfaz de red para el portal, consulte Creación de interfaces y zonas para GlobalProtect. Si aún no ha creado un perfil de servicio SSL/TLS para el portal, consulte Implementación de certificados de servidores en los componentes de GlobalProtect.

No vincule un perfil de gestión de interfaces que permita HTTP, HTTPS, Telnet o SSH en las interfaces donde haya configurado un portal o una puerta de enlace de GlobalProtect, ya que franquearía el acceso a la interfaz de gestión desde internet. Siga las recomendaciones de las Prácticas recomendadas para proteger el acceso administrativo *para garantizar la seguridad del acceso administrativo a sus cortafuegos, de forma que evitará ataques efectivos.*

1. Seleccione **General**.
2. En el área **Network Settings (Configuración de red)**, seleccione una interfaz.
3. Especifique el **IP Address Type (Tipo de dirección IP)** y la **IP address (Dirección IP)** para el servicio web del portal:
   - El tipo de dirección IP puede ser **IPv4 Only (Solo IPv4)**, **IPv6 Only (Solo IPv6)** o **IPv4 and IPv6 (IPv4 e IPv6).** Utilice **IPv4 and IPv6 (IPv4 e IPv6)** si su red admite dos configuraciones de pila, donde IPv4 e IPv6 se ejecutan al mismo tiempo.
   - La dirección IP debe ser compatible con el tipo de dirección IP. Por ejemplo, `172.16.1.0` para las direcciones IPv4 o `21DA:D3:0::2F3b` para las direcciones IPv6. Para las configuraciones de pila doble, introduzca una dirección IPv4 e IPv6.
4. Seleccione un **SSL/TLS Service Profile**.

STEP 3 | Seleccione **General** y configure los ajustes del registro de descifrado.

Puede registrar los protocolos de enlace TLS/SSL correctos e incorrectos y reenviar los logs de descifrado a los recopiladores de logs, a otros dispositivos de almacenamiento y a administradores específicos.

- De forma predeterminada, el cortafuegos registra solo los protocolos de enlace TLS incorrectos. También es recomendable registrar los protocolos de enlace correctos para tener visibilidad de todo el tráfico descifrado que permitan los recursos disponibles (pero no descifre el tráfico privado o confidencial; siga las prácticas recomendadas de descifrado y descifre todo el tráfico que pueda).
- Si aún no lo ha hecho, cree un perfil de reenvío de logs para reenviar los logs de descifrado y especifíquelo en la configuración de la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

- Si registra un protocolo de enlace TLS correcto además de un protocolo de enlace TLS incorrecto, configure una cuota de espacio de almacenamiento de log más grande para el log de descifrado (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Administración)** > **Logging and Reporting Settings (Configuración de creación de logs e informes)** > **Log Storage (Almacenamiento de logs)**). La cuota predeterminada (asignación) es el uno por ciento de la capacidad de almacenamiento de logs del dispositivo para los logs de descifrado y el uno por ciento para el resumen general de descifrado. No hay una asignación predeterminada para los resúmenes de descifrado por hora, por día o por semana. La configuración de logs de descifrado proporciona más información sobre cómo asignar el espacio de log del cortafuegos a los logs de descifrado.

STEP 4 | Seleccione las páginas de ayuda e inicio de sesión personalizadas o deshabilite estas páginas por completo. Consulte Personalización de las páginas de inicio de sesión, bienvenida y ayuda del portal de GlobalProtect para obtener más detalles sobre la creación de las páginas de ayuda e inicio de sesión personalizadas.

1. Seleccione **General**.
2. En el área Appearance (Diseño), configure cualquiera de los siguientes ajustes:
   - Para configurar la **Portal Login Page (Página de inicio de sesión del portal)** para el acceso del usuario al portal, seleccione la página de inicio de sesión **factory-default (predeterminada de fábrica)**, luego seleccione **Import (Importar)** para importar una página de inicio de sesión personalizada o **Disable (Desactivar)** para desactivar el acceso a la página de inicio de sesión.
   - Para configurar la **App Help Page (Página de ayuda de la aplicación)** de modo que brinde asistencia a los usuarios sobre la aplicación de GlobalProtect, seleccione la página de ayuda **factory-default (predeterminada de fábrica)**, luego haga clic en **Import (Importar)** para importar una página de ayuda personalizada o seleccione **None (Ninguna)** para eliminar la opción **Help (Ayuda)** del menú de **Settings (Configuración)** del panel de estado de GlobalProtect.

STEP 5 | Especifique de qué manera el portal autentica a los usuarios.

1. Seleccione **Authentication (Autenticación)**.
2. Configure cualquiera de los siguientes ajustes de autenticación en el portal:

   Si aún no ha creado un certificado de servidor para el portal y ha emitido certificados de puerta de enlace, consulte la Implementación de certificados de servidores en los componentes de GlobalProtect*.*

   - Para garantizar la comunicación entre el portal y la aplicación de GlobalProtect, seleccione el **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)** que configuró para el portal.
   - Para autenticar a los usuarios mediante una base de datos de usuario local o un servicio de autenticación externo, como LDAP, Kerberos, TACACS+, SAML o RADIUS (incluido OTP), defina las configuraciones de autenticación del cliente de GlobalProtect**.**
   - Para autenticar a los usuarios basándose en un certificado de cliente o una tarjeta inteligente / CAC, seleccione el **Certificate Profile (Perfil del certificado)** correspondiente. Debe implementar previamente el certificado del cliente o implementar certificados de cliente específicos del usuario para la autenticación con el Protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP).
     - Si los usuarios se deben autenticar en el portal con las credenciales y con los certificados de cliente, tiene que especificar tanto el perfil de certificados como el perfil de autenticación.
     - Si los usuarios se pueden autenticar en el portal con sus credenciales o con los certificados de cliente y selecciona un perfil de autenticación para autenticar a los usuarios, el perfil de certificados es opcional.
     - Si los usuarios se pueden autenticar en el portal con sus credenciales o con los certificados de cliente, pero no selecciona ningún perfil de autenticación para autenticar a los usuarios, el perfil de certificados es obligatorio.

© 2020 Palo Alto Networks, Inc.

- Si no configura ningún perfil de autenticación que coincida con un sistema operativo concreto, el perfil de certificados es obligatorio.

Si los usuarios se pueden autenticar en el portal con sus credenciales o con los certificados de cliente, seleccione un perfil de certificados donde Username Field (Campo de nombre de usuario) se haya configurado en Subject (Asunto) o Subject Alt (Asunto alternativo).

STEP 6 | Defina los datos que recopila la aplicación de GlobalProtect de los terminales conectados después de que los usuarios se autentiquen en el portal.

La aplicación de GlobalProtect envía estos datos al portal para compararlos con los criterios de selección definidos para cada configuración de agente del portal. El portal se basa en esos criterios para suministrar la configuración adecuada a las aplicaciones de GlobalProtect que se conectan.

1. Seleccione **Portal Data Collection (Recopilación de datos de portal)**.
2. Configure cualquiera de los siguientes ajustes de recopilación de datos:
   - En **Certificate Profile (Perfil de certificados)**, seleccione el perfil que identifica los certificados de equipo de los terminales conectados que debe recopilar la aplicación de GlobalProtect.
   - Para que la aplicación de GlobalProtect recopile información de hosts personalizada de los terminales conectados, defina los siguientes datos del registro o la lista de propiedades en el área Custom Checks (Comprobaciones personalizadas):
     - Para recopilar datos del registro de los terminales con Windows, seleccione **Windows** y, a continuación, haga clic en **Add (Añadir)** para añadir los valores oportunos en **Registry Key (Clave de registro)** y **Registry Value (Valor de registro)**.
     - Para recopilar datos de la lista de propiedades de los endpoints macOS, seleccione **Mac** y, a continuación, haga clic en **Add (Añadir)** para añadir la clave en **Plist (Lista de propiedades)** y el valor correspondiente en **Key (Clave)**.

STEP 7 | Guarde la configuración del portal.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes.
2. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

© 2020 Palo Alto Networks, Inc.

Definición de las configuraciones de autenticación de cliente de GlobalProtect

Cada configuración de autenticación de cliente de GlobalProtect especifica los ajustes que permiten al usuario autenticarse con el portal de GlobalProtect. Usted puede personalizar los ajustes para cada SO o puede configurar los ajustes para que se apliquen en todos los endpoints. Por ejemplo, puede configurar los usuarios de Android para que utilicen la autenticación RADIUS y los usuarios de Windows para que utilicen la autenticación LDAP. También puede personalizar la autenticación del cliente para los usuarios que acceden al portal desde un navegador web (para descargar la aplicación de GlobalProtect) o para el acceso VPN de IPsec (X-Auth) externo a las puertas de enlace de GlobalProtect.

STEP 1 | Configuración del acceso al portal de GlobalProtect.

STEP 2 | Especifique de qué manera el portal autentica a los usuarios.

Puede configurar el portal de GlobalProtect para que autentique a los usuarios mediante una base de datos de usuario local o un servicio de autenticación externo, como LDAP, Kerberos, TACACS+, SAML o RADIUS (incluido OTP). Si todavía no configuró los perfiles de autenticación o certificado, consulte Autenticación para obtener instrucciones.

En el diálogo GlobalProtect Portal Configuration (Configuración del portal de GlobalProtect) (**Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>*), seleccione **Authentication (Autenticación)** y **añada** una nueva configuración de **Client Authentication (Autenticación de cliente)** con los siguientes ajustes:

- Introduzca un nombre en **Name (Nombre)** para identificar la configuración de autenticación del cliente.
- Especifique los endpoints en los cuales desea implementar esta configuración. Para aplicar esta configuración a todos los terminales, acepte el valor predeterminado **Any (Cualquiera)** en **OS (Sistema operativo)**. Para aplicar esta configuración a los terminales que ejecutan un sistema operativo concreto, selecciónelo en **OS (Sistema operativo)**, por ejemplo, **Android**. También puede aplicarla a los terminales que se conectan al portal de Clientless VPN desde un navegador web.
- Para permitir que los usuarios se autentiquen en el portal o la puerta de enlace con sus credenciales, seleccione o añada un perfil en **Authentication Profile (Perfil de autenticación)**.
  - Si los usuarios se deben autenticar en el portal o la puerta de enlace con las credenciales y con los certificados de cliente, tiene que especificar tanto el perfil de autenticación como el perfil de certificados.
  - Si los usuarios se pueden autenticar en el portal o la puerta de enlace con sus credenciales o con los certificados de cliente y selecciona un perfil de certificados para autenticar a los usuarios, el perfil de autenticación es opcional.
  - Si los usuarios se pueden autenticar en el portal o la puerta de enlace con sus credenciales o con los certificados de cliente, pero no selecciona ningún perfil de certificados para autenticar a los usuarios o bien define **Certificate Profile (Perfil de certificados)** en **None (Ninguno)**, el perfil de autenticación5 es obligatorio.
- (Opcional) Ingrese una etiqueta de nombre de usuario personalizada en **Username Label (Etiqueta de nombre de usuario)** para el inicio de sesión del portal de GlobalProtect (por ejemplo, una **dirección de correo electrónico (nombredeusuario@dominio**).
- (Opcional) Ingrese una etiqueta de contraseña personalizada en **Password Label (Etiqueta de contraseña)** para el inicio de sesión del portal de GlobalProtect (por ejemplo, un **código de acceso** para la autenticación de dos factores basada en tokens).

© 2020 Palo Alto Networks, Inc.

- (Opcional) Introduzca un **Authentication Message (Mensaje de autenticación)** para ayudar a los usuarios finales a comprender qué credenciales deben usar cuando inician sesión. El mensaje puede tener hasta 256 caracteres de longitud (el predeterminado es `Enter login credentials [Introduzca las credenciales de inicio de sesión]`).
- Para definir si los usuarios se pueden autenticar en el portal con credenciales o certificados de cliente, seleccione una de estas opciones:
  - Si los usuarios se deben autenticar en el portal con ambos elementos, configure la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credenciales de usuario o certificados de cliente)** en **No (User Credentials AND Client Certificate Required) (No, exigir credenciales de usuario y certificados de cliente)**, que es el valor predeterminado.
  - Para permitir que los usuarios se autentiquen en el portal con cualquiera de estos elementos, configure la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credenciales de usuario o certificados de cliente)** en **Yes (User Credentials OR Client Certificate Required) (Sí, exigir credenciales de usuario o certificados de cliente)**.

    Si configura esta opción en **Yes (Sí)**, el portal de GlobalProtect busca primero el certificado de cliente en el terminal. Si no hay ninguno o si no ha configurado ningún perfil de certificados en la configuración de autenticación de los clientes, el usuario final se debe autenticar en el portal con sus credenciales.

STEP 3 | Ordene las configuraciones de autenticación del cliente con las configuraciones de sistema operativo específico en la parte superior de la lista y las configuraciones que se aplican a **Any (Cualquier)** sistema operativo en la parte inferior de la lista (**Network [Red]** > **GlobalProtect** > **Portals [Portales]** > **<portal-config>** > **Authentication [Autenticación]**). Como con la evaluación de reglas de seguridad, el portal busca una coincidencia empezando por la parte superior de la lista. Cuando encuentra una coincidencia, brinda la configuración correspondiente a la aplicación.

- Para subir una configuración de cliente en la lista de configuraciones, selecciónela y haga clic en **Move Up (Mover hacia arriba)**.
- Para bajar una configuración de cliente en la lista de configuraciones, selecciónela y haga clic en **Move Down**.

STEP 4 | (Opcional) Para habilitar la autenticación en dos fases usacon un perfil de autenticación y un perfil de certificado, configure ambos en esta configuración de portal.

El portal debe autenticar al endpoint con ambos métodos para que el usuario pueda obtener el acceso.

(Solo en Chrome) Si configura el portal para que use certificados de cliente y LDAP para la autenticación con dos factores, los Chromebooks que ejecutan Chrome OS 47 o versiones posteriores muestran demasiadas solicitudes para seleccionar el certificado de cliente. Para evitarlo, configure una política que especifique el certificado de cliente en la consola de administración de Google y, luego, impleméntela en los Chromebooks gestionados:

1. *Inicie sesión en la consola de administración de Google y seleccione Device management (Administración de dispositivos) > Chrome management (Administración de Chrome) > User settings (Configuración de usuario).*
2. *En la sección Client Certificates (Certificados de cliente), introduzca el patrón de URL siguiente en Automatically Select Client Certificate for These Sites (Seleccionar automáticamente el certificado de cliente de estos sitios):*

   `{"pattern": "https://[*.]","filter":{}}`

© 2020 Palo Alto Networks, Inc.

3. *Haga clic en Save (Guardar). La consola de administración de Google implementa la política en todos los dispositivos en apenas unos minutos.*

En el diálogo GlobalProtect Portal Configuration (Configuración del portal de GlobalProtect) (**Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>*), seleccione **Authentication (Autenticación)** para seleccionar el **Certificate Profile (Perfil de certificado)** para autenticar usuarios en función de un certificado de cliente o tarjeta inteligente.

El campo de nombre común (common name, CN) y, si corresponde, de nombre alternativo del asunto (Subject Alternative Name, SAN) del certificado deben coincidir exactamente con la dirección IP o FQDN de la interfaz donde configure el portal. De lo contrario, las conexiones HTTPS al portal fallarán.

STEP 5 | Guarde la configuración del portal.

1. Haga clic en **OK (Aceptar)** para guardar la configuración.
2. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Definición de las configuraciones de agente de GlobalProtect

Cuando un usuario de GlobalProtect se conecta al portal de GlobalProtect y es autenticado por este, el portal envía la configuración de agente a la aplicación en función de la configuración que haya definido. Si tiene roles diferentes para los usuarios o grupos que necesitan configuraciones específicas, puede crear una configuración de agente separada para cada tipo de usuario o grupo de usuario. El portal utiliza el SO del endpoint y el nombre de usuario o nombre de grupo para determinar la configuración de agente que se debe implementar. Al igual que con otras evaluaciones de reglas de seguridad, el portal comienza a buscar una coincidencia en la parte superior de la lista. Cuando encuentra una coincidencia, el portal envía la configuración a la aplicación.

La configuración puede incluir lo siguiente:

- Una lista de las puertas de enlace a las cuales el endpoint puede conectarse.
- Entre las puertas de enlace externas, cualquier puerta de enlace que el usuario pueda seleccionar manualmente para la sesión.
- El certificado de CA raíz requerido para habilitar la aplicación a fin de establecer una conexión SSL con las puertas de enlace de GlobalProtect.
- El certificado de CA raíz para el descifrado proxy de reenvío SSL.
- El certificado de cliente que el endpoint debería presentar a la puerta de enlace al conectarse. Esta configuración es necesaria solo si se requiere la autenticación mutua entre la aplicación y el portal o la puerta de enlace.
- La cookie cifrada segura que el endpoint debería presentar al portal o la puerta de enlace al conectarse. La cookie se incluye solo si usted habilita el portal para que genere una.
- La configuración que usa el endpoint para determinar si está conectado a la red local o a una red externa.
- La configuración del comportamiento de la aplicación, tal como lo que los usuarios finales pueden ver en su pantalla, si pueden guardar la contraseña de GlobalProtect y si se les solicitará a los usuarios actualizar el software.

Si el portal está inactivo o es inaccesible, la aplicación usará la versión en caché de su configuración de agente desde su última conexión de portal realizada correctamente para obtener los ajustes, incluida con qué puertas de enlace se podrá conectar la aplicación, qué certificados de CA raíz se usarán para establecer una comunicación segura con las puertas de enlace y qué método de conexión emplear.

© 2020 Palo Alto Networks, Inc.

Utilice el siguiente procedimiento para crear una configuración de agente.

STEP 1 | Añada uno o más certificados de CA raíz de confianza a la configuración de agente de portal para permitir que la aplicación de GlobalProtect verifique la identidad del portal y las puertas de enlace.

El portal implementa el certificado en un archivo de certificado que solo lo lee GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione la configuración del portal en la cual está añadiendo la configuración del agente y, luego, seleccione la pestaña **Agent (Agente)**.
3. En el campo **Trusted Root CA (CA raíz de confianza)**, haga clic en **Add (Añadir)** y seleccione el certificado de CA que se usó para emitir los certificados de servidor de la puerta de enlace o el portal.

   La interfaz web presenta una lista de certificados de CA que se importan al cortafuegos que sirve como portal de GlobalProtect. La interfaz web también excluye certificados de entidad final, a veces conocido como el primer certificados en la cola de certificados, de la lista de certificados que puede seleccionar. También puede **Import (Importar)** un nuevo certificado de CA.

   Utilice las siguientes recomendaciones al crear y agregar certificados:

   - *Utilice el mismo emisor de certificados para emitir certificados para todas sus puertas de enlace.*
   - *Agregue la cadena de certificados completa (CA raíz de confianza y certificados CA intermedios) a la configuración del agente del portal.*
4. (Opcional) Implemente certificados de CA adicionales para fines distintos de los de GlobalProtect (por ejemplo, descifrado de proxy de reenvío SSL).

   Esta opción le permite usar el portal para implementar certificados en el endpoint y el agente para instalarlos en el almacén local de certificados raíz. Esto puede ser útil si no tiene otro método para distribuir estos certificados de servidor o si prefiere usar el portal para la distribución de certificados.

   Para el descifrado de proxy de reenvío SSL, especifique el certificado de reenvío fiable que el cortafuegos utiliza (únicamente en endpoints de Windows y macOS) para finalizar la conexión HTTPS, inspeccionar el tráfico para comprobar el cumplimiento de las políticas y volver a establecer la conexión HTTPS para reenviar el tráfico cifrado.

   1. Añada el certificado como se describe en el paso anterior.
   2. Habilite la opción **Install in Local Root Certificate Store (Instalar en el almacén local de certificados raíz)**.

      El portal envía automáticamente el certificado cuando el usuario inicia sesión en el portal y lo instala en el almacén local del endpoint, con lo cual se elimina la necesidad de que instale el certificado manualmente.

STEP 2 | Añada una configuración de agente.

La configuración de agente especifica los ajustes de configuración de GlobalProtect se implementarán en las aplicaciones que se conecten. Debe definir al menos una configuración de agente.

1. Acceda a la configuración del portal con **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* y **añada** una configuración de agente nueva.
2. Introduzca un nombre en **Name** para identificar la configuración. Si pretende crear múltiples configuraciones, asegúrese de que el nombre que defina para cada una sea suficientemente descriptivo para distinguirlas.

STEP 3 | (Opcional) Configure los ajustes para especificar de qué manera los usuarios con esta configuración se autentican con el portal.

© 2020 Palo Alto Networks, Inc.

Si la puerta de enlace autentica endpoints usando un certificado de cliente, usted debe seleccionar la fuente que distribuye el certificado.

Configure cualquiera de los ajustes siguientes en **Authentication (Autenticación)**:

- Para habilitar a los usuarios para que se autentiquen con el portal usando certificados de clientes, seleccione la fuente **Client Certificate** (**SCEP**, **Local** o **None**) que distribuye el certificado y su clave privada a un endpoint. Si utiliza una CA interna para distribuir certificados a los endpoints, seleccione **None (Ninguno)** (predeterminado). Para habilitar el portal a fin de que genere y envíe un certificado de equipo a la aplicación para su almacenamiento en el almacén de certificados local y utilizar el certificado para la autenticación del portal y la puerta de enlace, seleccione **SCEP** y el perfil SCEP asociado. Estos certificados son específicos del dispositivo y solo pueden usarse en el endpoint para el cual se emitió. Para usar el mismo certificado para todos los endpoints, seleccione un certificado que sea **Local** para el portal. Con la opción **None (Ninguno)**, el portal no envía un certificado al endpoint, sino que usted puede usar otras maneras para obtener un certificado para el endpoint.
- Especifique si se guardarán las credenciales del usuario con la opción **Save User Credentials**. Seleccione **Yes (Sí)** para guardar el nombre de usuario y la contraseña (predeterminado), **Save Username Only (Guardar solo nombre de usuario)** para guardar solo el nombre de usuario, **Only with User Fingerprint (Solo con huellas del usuario)** para guardar la biometría del usuario (huellas) o, en extremos de iOS X solo, las credenciales de Face ID, o **No** para no guardar nunca las credenciales.

  Cuando configura Save User Credentials (Guardar credenciales de usuario) en No, y si el portal y la puerta de enlace están configurados para utilizar los mismos métodos de autenticación, la aplicación de GlobalProtect puede autenticarse en la puerta de enlace de forma transparente mediante las credenciales proporcionadas por el usuario para autenticarse en el portal. No se requiere que el usuario vuelva a especificar sus credenciales para autenticarse en la puerta de enlace.

  Si usted configura el portal o las puertas de enlace para solicitar una contraseña dinámica, tal como una contraseña de un solo uso (one-time password, OTP), el usuario debe introducir una nueva contraseña en cada inicio de sesión. En este caso, la aplicación de GlobalProtect ignora la selección para guardar el nombre de usuario y la contraseña, si se especifica, y guarda solo el nombre de usuario. Para obtener más información, consulte Habilitación de la autenticación en dos fases mediante contraseñas de un solo uso (OTP).

  Si selecciona las opciones **Save User Credentials (Guardar credenciales de usuario) Only with User Fingerprint (Solo con huellas del usuario)**, GlobalProtect puede aprovechar las capacidades del sistema operativo de la aplicación para validar al usuario antes de permitir la autenticación con GlobalProtect. Los usuarios finales deben proporcionar una huella que coincida con una plantilla de huella fiable en el endpoint para usar una contraseña guardada para la autenticación en el portal y las puertas de enlace de GlobalProtect. En iOS X, GlobalProtect también admite el reconocimiento facial con Face ID. GlobalProtect no almacena la plantilla facial o la huella que se utilizan para la autenticación, pero se basa en las capacidades de escaneo del sistema operativo para determinar la validez de una coincidencia de escaneo.

STEP 4 | Si el endpoint de GlobalProtect no requiere conexiones de túnel cuando está en la red interna, configure la detección del host interno.

1. Seleccione **Internal (Interna)**.
2. Habilite **Internal Host Detection (Detección de hosts internos)** con el valor **IPv4** o el valor **IPv6**.
3. Introduzca la **IP Address (Dirección IP)** de un host al que solo se tenga acceso desde la red interna. La dirección IP especificada debe ser compatible con el tipo elegido, **IPv4** o **IPv6**. Por ejemplo, 172.16.1.0 para IPv4 o 21DA:D3:0:2F3b para IPv6).
4. Introduzca el **Hostname (Nombre de host)** de DNS que corresponda a la dirección IP que ingresa. Los endpoints que intentan conectarse a GlobalProtect intentan realizar una búsqueda DNS inversa en la

© 2020 Palo Alto Networks, Inc.

dirección especificada. Si la búsqueda falla, el endpoint determina que está en la red externa y luego inicia una conexión de túnel hacia una puerta de enlace en su lista de puertas de enlace externas.

STEP 5 | Configure el acceso a un sistema de gestión de endpoints móviles de terceros.

Este paso es necesario si los endpoints móviles que utilizan esta configuración serán gestionados por un sistema de gestión de endpoints móviles de terceros. Todos los endpoints se conectarán inicialmente al portal y, si el sistema de gestión de endpoints móviles de terceros está configurado en la configuración de agente del portal correspondiente, el endpoint se redirigirá a ella para su inscripción.

1. Introduzca la dirección IP o FQDN de la interfaz de registro del endpoint asociada con el sistema de gestión de endpoints móviles. El valor que introduzca aquí deberá coincidir exactamente con el valor del certificado del servidor asociado a la interfaz de registro de endpoints. Puede indicar una dirección IPv6 o IPv4.
2. Especifique el **Enrollment Port (Puerto de inscripción)** en el cual el sistema de gestión de endpoints móviles detecta las solicitudes de inscripción. Este valor debe coincidir con el valor definido en el sistema de gestión de endpoints móviles (por defecto, 443).

STEP 6 | Especifique los criterios de selección de la configuración de agente del portal.

El portal se sirve de los criterios de selección especificados para determinar qué configuración debe suministrar a las aplicaciones de GlobalProtect que se conectan. Por lo tanto, si tiene múltiples configuraciones, debe asegurarse de ordenarlas correctamente. Tan pronto como el portal encuentre una coincidencia, brinda la configuración. Así, las configuraciones más específicas deberán preceder a las más generales. Consulte el paso 12 para obtener instrucciones sobre cómo ordenar la lista de configuraciones de agente.

Seleccione **Config Selection Criteria (Criterios de selección de configuraciones)** y, a continuación, configure cualquiera de las siguientes opciones:

- Para especificar el usuario, el grupo de usuarios o el sistema operativo a los que se aplica esta configuración, seleccione **User/User Group (Usuario o grupo de usuarios)** y, a continuación, configure cualquiera de las siguientes opciones:
  - Para suministrar esta configuración a las aplicaciones que ejecutan un sistema operativo concreto, haga clic en **Add (Añadir)** y seleccione el sistema al que se aplica está configuración en **OS (Sistema operativo)**: **Android**, **Chrome**, **iOS**, **Linux**, **Mac**, **Windows** o **WindowsUWP (Windows [UWP])**. Defina **OS (Sistema operativo)** en **Any (Cualquiera)** para implementar la configuración en todos los sistemas operativos.
  - Para restringir esta configuración a un usuario o un grupo concretos, haga clic en **Add (Añadir)** y, después, selecciónelo en **User/User Group (Usuario o grupo de usuarios)**. Repita este paso para cada usuario/grupo que desee añadir. Para restringir la configuración a los usuarios que aún no iniciaron sesión en sus endpoints, seleccione **pre-logon (Inicio de sesión previo)** desde el menú desplegable **User/User Group (Usuario/grupo de usuarios)**. Para implementar la configuración en todos los usuarios con independencia del estado de inicio de sesión (antes y después de hacerlo), seleccione **any (cualquiera)** en el menú desplegable **User/User Group (Usuario o grupo de usuarios)**.

    Para poder restringir la configuración a grupos específicos, debe asignar los usuarios a grupos, como se describe en Habilitación de la asignación de grupo.
- Para suministrar esta configuración a las aplicaciones en función de atributos concretos de los dispositivos, seleccione **Device Checks (Comprobaciones en dispositivos)** y, a continuación, configure cualquiera de las siguientes opciones:
  - Para suministrar esta configuración en función de la presencia del número de serie del terminal en Active Directory o Azure AD, seleccione una opción en el menú desplegable **Machine account exists with device serial number (Cuenta de equipo con número de serie de dispositivo)**. Si define esta opción en **Yes (Sí)**, la configuración de agente solo se aplica a los terminales en los que

© 2020 Palo Alto Networks, Inc.

exista un número de serie, es decir, los terminales gestionados. Si define esta opción en **No**, la configuración de agente solo se aplica a los terminales en los que no exista un número de serie, es decir, los terminales no gestionados. Si define esta opción en **None (Ninguna)**, no se tiene en cuenta la presencia del número de serie para suministrar la configuración.

- Para suministrar esta configuración en función del certificado de equipo del terminal, seleccione en **Certificate Profile (Perfil de certificados)** el perfil que se debe cotejar con el certificado de equipo instalado en el terminal.

- Para suministrar esta configuración a las aplicaciones en función de los datos personalizados de los hosts, seleccione **Custom Checks (Comprobaciones personalizadas)**. Marque **Custom Checks (Comprobaciones personalizadas)** para habilitarlas y, a continuación, defina cualquiera de los siguientes datos en el registro o en la lista de propiedades:
  - Para verificar si los terminales con Windows disponen de una clave de registro concreta, siga estos pasos:
    1. Seleccione **Custom Checks (Comprobaciones personalizadas)** > **Registry Key (Clave de registro)** y haga clic en **Add (Añadir)** para añadir una clave de registro nueva.
    2. Cuando se le indique, introduzca en **Registry Key (Clave de registro)** la clave que se debe cotejar.
    3. (Opcional) Para suministrar esta configuración solo en el caso de que el terminal carezca de la clave de registro o del valor de clave especificados, marque **Key does not exist or match specified value data (La clave no existe o no coincide con los datos de valor especificados)**.
    4. (Opcional) Para suministrar esta configuración en función de valores concretos del registro, haga clic en **Add (Añadir)** para añadir los valores oportunos en **Registry Value (Valor de registro)** y **Value Data (Datos de valor)**. Para suministrar esta configuración solo a los terminales que no tengan los valores especificados en **Registry Value (Valor de registro)** o **Value Data (Datos de valor)**, marque **Negate (Negar)**.
  - Para verificar si los terminales con macOS disponen de una entrada concreta en la lista de propiedades, siga estos pasos:
    1. Seleccione **Custom Checks (Comprobaciones personalizadas)** > **Plist (Lista de propiedades)** y haga clic en **Add (Añadir)** para añadir una lista nueva.
    2. Cuando se le indique, introduzca el nombre en **Plist (Lista de propiedades)**.
    3. (Opcional) Para suministrar esta configuración solo en el caso de que el terminal carezca de la lista de propiedades especificada, marque **Plist does not exist (No existe la lista de propiedades)**.
    4. (Opcional) Para suministrar esta configuración en función de pares de clave y valor concretos de la lista de propiedades, haga clic en **Add (Añadir)** y, a continuación, introduzca los datos oportunos en **Key (Clave)** y **Value (Valor)**. Para buscar coincidencias solo de terminales que no tengan la clave o el valor especificados, marque **Negate (Negar)**.

STEP 7 | Especifique las puertas de enlace externas a las que se podrán conectar los usuarios con esta configuración.

Considere las siguientes recomendaciones cuando configure las puertas de enlace:

- *Si añade puertas de enlace tanto internas como externas a la misma configuración, asegúrese de habilitar Internal Host Detection (Detección de host interno) (paso 4).*
- *Para obtener más información sobre cómo la aplicación de GlobalProtect determina la puerta de enlace a la cual debe conectarse, consulte* Prioridad de la puerta de enlace en una configuración de varias puertas de enlace*.*

1. Seleccione **External (Externa)**.
2. Haga clic en **Add (Añadir)** para añadir en **External Gateways (Puertas de enlace externas)** las puertas a las que se pueden conectar los usuarios.

© 2020 Palo Alto Networks, Inc.

3. Introduzca un **Name (Nombre)** descriptivo para la puerta de enlace. El nombre que introduzca debe coincidir con el nombre que definió cuando configuró la puerta de enlace y debe ser lo suficientemente descriptivo para que los usuarios conozcan la ubicación de la puerta de enlace a la que están conectados.
4. Introduzca el FQDN o la dirección IP de la interfaz donde está configurada la puerta de enlace en el campo **Address (Dirección)**. Puede configurar una dirección IPv4 o IPv6. La dirección que especifique debe coincidir exactamente con el nombre común (common name, CN) en el certificado del servidor de la puerta de enlace.
5. **Add (Añadir)** una o más **Source Regions (Regiones fuente)** para la puerta de enlace, o seleccione **Any (Cualquiera)** para hacer que la puerta de enlace esté disponible para todas las regiones. Cuando los usuarios se conectan, GlobalProtect reconoce la región y solo permite que los usuarios se conecten a las puertas de enlace configuradas para esa región. Para la selección de puertas de enlace, primero se considera la región de origen y luego la prioridad de la puerta de enlace.
6. Configure la **Priority (Prioridad)** de la puerta de enlace al clic en el campo y seleccionar uno de los siguientes valores:
   - Si solo tiene una puerta de enlace externa, puede dejar este valor fijado en **Highest (Más alto)** (valor por defecto).
   - Si tiene varias puertas de enlace externas, puede modificar los valores de prioridad (desde **Highest [Más alto]** hasta **Lowest [Más bajo]**) para indicar la preferencia para este grupo de usuarios específico al que se aplica la configuración. Por ejemplo, si prefiere que el grupo de usuarios se conecte a una puerta de enlace local, debería configurar la prioridad con un valor más alto que el de las puertas de enlace geográficamente distantes. El valor de prioridad se usa entonces para valorar el algoritmo de selección de la puerta de enlace del agente.
   - Si no quiere que las aplicaciones establezcan automáticamente conexiones con la puerta de enlace, seleccione **Manual only (Manual únicamente)**. Esta configuración es útil en entornos de prueba.
7. Seleccione la casilla de verificación **Manual** para permitir que los usuarios puedan cambiar manualmente a la puerta de enlace.

STEP 8 | Especifique las puertas de enlace internas a las que se podrán conectar los usuarios con esta configuración.

Asegúrese de no usar a petición como método de conexión si su configuración incluye puertas de enlace internas.

1. Seleccione **Internal (Interna)**.
2. Haga clic en **Add (Añadir)** para añadir en **Internal Gateways (Puertas de enlace internas)** las puertas a las que se pueden conectar los usuarios.
3. Introduzca un **Name (Nombre)** descriptivo para la puerta de enlace. El nombre que introduzca debe coincidir con el nombre que definió al configurar la puerta de enlace y debe ser lo suficientemente descriptivo para que los usuarios conozcan la ubicación de la puerta de enlace a la que están conectados.
4. Introduzca el FQDN o la dirección IP de la interfaz donde está configurada la puerta de enlace en el campo **Address (Dirección)**. Puede configurar una dirección IPv4 o IPv6. La dirección que especifique debe coincidir exactamente con el nombre común (common name, CN) en el certificado del servidor de la puerta de enlace.
5. (Opcional) Puede **Add (Añadir)** una o más **Source Addresses (Direcciones de origen)** a la configuración de la puerta de enlace. La dirección de origen puede ser una dirección predefinida, un rango o una subred de IP. GlobalProtect admite las direcciones IPv6 e IPv4. Cuando los usuarios se conectan, GlobalProtect reconoce la dirección de origen del endpoint y solo permite que los usuarios se conecten a las puertas de enlace configuradas para esa dirección.
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

© 2020 Palo Alto Networks, Inc.

7. (Opcional) Puede **Add (Añadir)** un **DHCP Option 43 Code (Código de opción 43 de DHCP)** a la configuración de la puerta de enlace. Puede incluir uno o más códigos de opciones alternativas asociados con la información específica del proveedor (Opción 43) que el servidor DHCP, debido a su configuración, puede ofrecer al cliente. Por ejemplo, puede tener un código de subopción 100 que está asociado a una dirección IP de 192.168.3.1.

   Cuando un usuario se conecta, el portal de GlobalProtect envía la lista de códigos de opción en la configuración del portal a la aplicación de GlobalProtect y el agente selecciona las puertas de enlace indicadas por estas opciones.

   Cuando se configuran tanto la dirección de origen como las opciones de DHCP, la lista de puertas de enlace disponibles presentadas al endpoint se basa en la combinación (unión) de las dos configuraciones.

   Las opciones DHCP son compatibles con endpoints de Windows y macOS únicamente. Las opciones DHCP no se pueden usar para seleccionar puertas de enlace que usan direccionamiento IPv6.

8. (Opcional) Seleccione **Internal Host Detection (Detección de host interno)** para permitir que la aplicación de GlobalProtect determine si está dentro de la red empresarial. Cuando el usuario intenta iniciar sesión, la aplicación realiza una búsqueda de DNS inversa del **Hostname (Nombre de host)** interno en la **IP Address (Dirección IP)** especificada.

   El host sirve como un punto de referencia que se puede alcanzar si el endpoint está dentro de la red empresarial. Si la aplicación encuentra el host, el endpoint está dentro de la red y la aplicación se conecta a una puerta de enlace interna; si la aplicación no encuentra el host interno, el endpoint está afuera de la red y la aplicación se conecta a una de las puertas de enlace externas.

   Puede configurar el direccionamiento **IPv4** o **IPv6** para **Internal Host Detection (Detección de host interno)**. La dirección IP que especifique debe ser compatible con el tipo de dirección IP. Por ejemplo, 172.16.1.0 para IPv4 o 21DA:D3:0:2F3b para IPv6).

STEP 9 | Personalice el comportamiento de la aplicación de GlobalProtect para los usuarios con esta configuración.

Modifique la configuración de la aplicación como desee. Para obtener detalles adicionales sobre cada opción, consulte Personalización de la aplicación de GlobalProtect.

STEP 10 | (Opcional) Defina los datos personalizados del perfil de información de hosts (host information profile, HIP) que la aplicación debe recopilar o excluir de la recopilación.

Siga este paso solo si pretende usar la función HIP, si desea obtener información que no se puede recopilar mediante los objetos estándar de HIP o si hay información de HIP que no le interesa recopilar. Consulte la Información de host para obtener información detallada acerca del uso de la función HIP.

Para obtener más información sobre la recopilación de datos personalizados de HIP, consulte Recopilación de datos de procesos y aplicaciones de endpoints.

1. Seleccione **HIP Data Collection (Recopilación de datos de HIP)**.
2. Marque **Collect HIP Data (Recopilar datos de HIP)** para que la aplicación de GlobalProtect pueda recopilar información.
3. En **Max Wait Time (sec) (Tiempo máximo de espera [s])**, especifique durante cuánto tiempo busca datos de HIP la aplicación antes de enviar los disponibles; el intervalo es de 10 a 60 segundos y el valor predeterminado, 20 segundos.
4. En **Certificate Profile (Perfil de certificados)**, seleccione el perfil que emplea el portal de GlobalProtect para cotejar el certificado de equipo que envía la aplicación de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

5. Seleccione **Exclude Categories** para excluir categorías específicas o proveedores, aplicaciones o versiones dentro de una categoría. Para obtener más detalles, consulte Configuración de la aplicación de políticas basadas en HIP.
6. Seleccione **Custom Checks (Comprobaciones personalizadas)** para definir los datos personalizados que desea recopilar de los hosts que ejecutan esta configuración de agente.

STEP 11 | Guarde la configuración del agente.

Haga clic en **OK** para guardar la configuración de agente.

STEP 12 | Organice las configuraciones de agente de modo que la configuración correcta se implemente en cada aplicación.

Cuando una aplicación se conecta, el portal compara la información de origen en el paquete con las configuraciones de agente que definió. Como con la evaluación de reglas de seguridad, el portal busca una coincidencia empezando por la parte superior de la lista. Cuando encuentra una coincidencia, brinda la configuración correspondiente a la aplicación.

- Para subir una configuración de agente en la lista de configuraciones, selecciónela y haga clic en **Move Up**.
- Para bajar una configuración de agente en la lista de configuraciones, selecciónela y haga clic en **Move Down (Mover hacia abajo)**.

STEP 13 | Guarde la configuración del portal.

1. Haga clic en **ACEPTAR** para guardar la configuración de portal.
2. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Personalización de la aplicación de GlobalProtect

La configuración del agente del portal le permite personalizar cómo sus usuarios finales interactúan con las aplicaciones de GlobalProtect instaladas en sus endpoints. Puede personalizar la visualización y el comportamiento de la aplicación, así como definir diferentes ajustes para las distintas configuraciones del agente de GlobalProtect que cree. Por ejemplo, puede especificar lo siguiente:

- A qué menús y vistas pueden acceder los usuarios.
- Si los usuarios pueden desinstalar o deshabilitar la aplicación (solo el método de conexión de inicio de sesión del usuario).
- Si desea mostrar una página de bienvenida cuando el inicio de sesión se realice correctamente. También puede configurar si el usuario puede omitir o no la página de bienvenida, y puede personalizar las páginas de inicio de sesión, ayuda y bienvenida del portal de GlobalProtect para explicar cómo usar GlobalProtect dentro de su entorno.
- Si la aplicación de GlobalProtect se actualiza automáticamente o solicita a los usuarios que lo hagan de forma manual.
- Si se solicita a los usuarios la autenticación multifactor para acceder a los recursos de redes confidenciales.

También puede definir la configuración de la aplicación en el registro de Windows, el instalador de Windows (Msiexec) y la plist global de macOS. Los ajustes que se definen en la interfaz web (la configuración de agente del portal) tienen prioridad sobre los ajustes definidos en el registro de Windows, Msiexec o la plist de macOS. Para obtener más detalles, consulte Implementación de la configuración de aplicación de forma trasparente.

Los ajustes adicionales disponibles solo a través del registro de Windows o el instalador de Windows (Msiexec) le permiten lo siguiente:

© 2020 Palo Alto Networks, Inc.

- Especificar si la aplicación solicita al usuario final las credenciales cuando el SSO de Windows falla.
- Especificar la dirección IP del portal por defecto (o nombre de host).
- Habilitar GlobalProtect para iniciar una conexión antes de que el usuario inicie sesión en el endpoint.
- Implementar secuencias de comando que se ejecuten antes o después de que GlobalProtect establezca una conexión o después de que se desconecte.
- Configure la aplicación de GlobalProtect para que ajuste las credenciales de terceros en los endpoints de Windows, lo que habilita el SSO cuando se usa un proveedor de credenciales de terceros.

Para obtener más información, consulte Ajustes personalizables de la aplicación.

STEP 1 | Seleccione la configuración de agente que desea personalizar.

También puede configurar la mayoría de los ajustes de la aplicación en el registro de Windows, el instalador de Windows (Msiexec) y la plist de macOS. Sin embargo, los ajustes que se definen en la interfaz web tienen prioridad sobre los ajustes definidos en el registro de Windows, Msiexec o la plist de macOS. Consulte Implementación de la configuración de la aplicación de forma trasparente *para obtener más detalles.*

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione el portal en el que desea añadir la configuración de agente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Agent (Agente)**, seleccione la configuración del agente que desea modificar o haga clic en **Add (Añadir)** para añadir una nueva.
4. Seleccione la pestaña **App (Aplicación)**.

   El área App Configurations (Configuraciones de la aplicación) muestra los ajustes de la aplicación con los valores predeterminados que puede personalizar para cada configuración de agente. Cuando cambia el comportamiento predeterminado, el color del texto cambia de gris al color predeterminado.

STEP 2 | Especifique el **Connect Method (Método de conexión)** que la aplicación usa para su conexión con GlobalProtect.

Utilice el método de conexión Pre-logon (Always On) [Inicio de sesión previo [siempre activado]), Pre-logon then On-demand [Inicio de sesión previo (luego bajo demanda)] o User-log on (Always On) [Inicio de sesión de usuario (Siempre activado)] para acceder a la red usando una puerta de enlace interna.

En el área App Configurations (Configuraciones de la aplicación), seleccione una de las siguientes opciones de **Connect Method (Método de conexión)**:

- **User-logon (Always On) (Inicio de sesión de usuario [Siempre activo])**: La aplicación de GlobalProtect se conecta automáticamente al portal en cuanto el usuario inicia sesión en el endpoint (o dominio). Cuando se usa en conjunto con el SSO (solo en los endpoints de Windows), el inicio de sesión de GlobalProtect es transparente para el usuario final.

  En los endpoints de iOS, esta configuración evita que las aplicaciones de contraseña de un solo uso (OTP) funcionen porque GlobalProtect obliga a todo el tráfico a atravesar el túnel.
- **Pre-logon (Always On) (Inicio de sesión previo [Siempre activado])**: La aplicación de GlobalProtect autentica al usuario y establece un túnel CPN con la puerta de enlace de GlobalProtect antes de que el usuario inicie sesión en el endpoint. Esta opción requiere que utilice una solución de PKI externa para implementar previamente un certificado de equipo en cada endpoint que reciba esta configuración. Consulte VPN de acceso remoto con inicio de sesión anterior para obtener más detalles sobre el inicio de sesión previo.

© 2020 Palo Alto Networks, Inc.

- **On-demand (Manual user initiated connection) (A demanda [Conexión manual iniciada por el usuario])**: Los usuarios deben iniciar la aplicación manualmente para conectarse a GlobalProtect. Use este método de conexión solo para puertas de enlace externas.
- **Pre-logon then On-demand (Inicio de sesión previo y luego a demanda)**: Similar al método de conexión **Pre-logon (Always On) (Inicio de sesión previo [Siempre activado])**, este método (que requiere la versión de lanzamiento de contenido 590-3397 o posterior) permite que la aplicación de GlobalProtect autentique al usuario y establezca un túnel de VPN a la puerta de enlace de GlobalProtect antes de que el usuario inicie sesión en el endpoint. A diferencia del método de conexión de inicio de sesión previo, una vez que el usuario inicia sesión en el endpoint, los usuarios deben iniciar manualmente la aplicación para conectarse con GlobalProtect si la conexión finaliza por algún motivo. La ventaja de esta opción es que puede permitir a los usuarios especificar una nueva contraseña una vez que la suya caduque o cuando la olvidan, pero igualmente requiere que los usuarios inicien manualmente la conexión después de iniciar sesión.

STEP 3 | Especificar si se deben aplicar las conexiones de GlobalProtect para el acceso a la red.

(Solo en Windows 10) Cuando se habilita **Enforce GlobalProtect Connection for Network Access (Habilitar conexión de GlobalProtect para acceso de red)** se omiten los siguientes tipos de aplicaciones y se bloquean todas las demás conexiones salientes (no entrantes):

- Procesos del agente de GlobalProtect (**PanGPA.exe**), del servicio GlobalProtect (**PanGPS.exe**) y del servicio de subsistema de la autoridad de seguridad local (**lsass.exe**)
- Protocolos DHCP, DNS, NetBIOS (sistema básico de entrada/salida de red) y resolución de nombres de multidifusión local de enlace (LLMNR, Link-Local Multicast Name Resolution)
- Tráfico de interfaz de bucle

(Solo en macOS) Cuando se habilita **Enforce GlobalProtect Connection for Network Access (Habilitar conexión de GlobalProtect para acceso de red)** se omiten los siguientes tipos de aplicaciones y se bloquean todas las demás conexiones entrantes y salientes:

- Aplicación de GlobalProtect y el servicio GlobalProtect (PanGPS)
- Protocolos DNS y DHCP
- Tráfico de interfaz de bucle
- Procesos `ocspd`, `syspolicyd`, `ntpd`, `apsd` y `trustd`

Para aplicar GlobalProtect para el acceso de red, le recomendamos que habilite esta función únicamente para usuarios que se conecten en los modos User-logon o Pre-logon. Los usuarios que se conectan en el modo On-demand (Por demanda) posiblemente no puedan establecer una conexión dentro de los periodos de gracia permitidos.

En el área App Configurations, configure cualquiera de las siguientes opciones:

- Para forzar todo el tráfico de red para que atraviese un túnel de GlobalProtect, configure **Enforce GlobalProtect Connection for Network Access (Aplicar la conexión GlobalProtect para el acceso de red)** en **Yes (Sí)**. De manera predeterminada, GlobalProtect no es obligatorio para tener acceso a la red; por lo tanto, los usuarios pueden acceder a internet aunque GlobalProtect esté deshabilitado o desconectado. Para proporcionar instrucciones a los usuarios antes de que se bloquee el tráfico, configure GlobalProtect con la opción **Displays Traffic Blocking Notification Message (Muestra el mensaje de notificación de bloqueo de tráfico)** y, de manera opcional, especifique cuándo se debe mostrar el mensaje (**Traffic Blocking Notification Delay [Demora de notificación de bloqueo de tráfico]**).

Cuando está habilitada la opción Enforce GlobalProtect Connection for Network Access (Aplicar la conexión de GlobalProtect para el acceso de red), es posible que deba considerar permitir a los usuarios deshabilitar la aplicación de GlobalProtect con un código de acceso. La función Enforce GlobalProtect Connection for Network

© 2020 Palo Alto Networks, Inc.

Access (Aplicar la conexión de GlobalProtect para el acceso de red) mejora la seguridad de red exigiendo una conexión de GlobalProtect para el acceso de red. En raras ocasiones, los endpoints pueden no conectarse a la VPN y requerir el inicio de sesión administrativo remoto para solucionar problemas. Si deshabilita la aplicación de GlobalProtect (para Windows o macOS) con el código de acceso brindado por el administrador durante la sesión de solución de problemas, puede permitirles a los administradores conectarse a su endpoint de manera remota.

- Configure exclusiones para direcciones IP locales específicas o segmentos de red para acceso a la red especificando esas direcciones IP para **Allow traffic to specified hosts/networks when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established (Permitir tráfico a hosts/redes especificadas cuando Enforce GlobalProtect Connection for Network Access está habilitado y GlobalProtect Connection no está establecido)**. Especifique hasta diez direcciones IP o segmentos de red para los que desee permitir el acceso cuando aplique GlobalProtect para el acceso a la red y GlobalProtect no pueda establecer una conexión.

  Esta opción requiere la versión de contenido 8196-5685 o una posterior.

  Al configurar las exclusiones, puede mejorar la experiencia del usuario si le permite acceder a recursos locales cuando GlobalProtect esté desconectado. Por ejemplo, cuando GlobalProtect no está conectado, GlobalProtect puede permitir el acceso a direcciones locales de enlace. Esto provoca que el usuario pueda acceder a un segmento de red local o dominio de difusión.
- (Windows 10 y macOS que ejecutan macOS Catalina 10.15.4 o posterior únicamente; requiere la aplicación de GlobalProtect ™ 5.2.) Configure exclusiones para nombres de dominio específicos y completos para los que desee permitir el acceso cuando aplique conexiones de GlobalProtect para acceso a la red especificando estos nombres de dominio completamente calificados para **permitir el tráfico al FQDN especificado cuando la opción Enforce GlobalProtect Connection (Aplicar conexión de GlobalProtect) para el acceso a la red está habilitada y la conexión GlobalProtect no está establecida**.

  Especifique hasta veinte nombres de dominio totalmente calificados para los que desea permitir el acceso cuando aplique conexiones de GlobalProtect para el acceso a la red y GlobalProtect no pueda establecer una conexión.

  Los nombres de dominio completos que proporciona se utilizan solo cuando **Enforce GlobalProtect Connection for Network Access (Aplicar conexión de GlobalProtect para el acceso de red)** está configurado en **Yes (Sí)**. Utilice comas para separar varios nombres de dominio completos (por ejemplo, google.com y gmail.com). Utilice el carácter comodín (*) para los nombres de dominio (por ejemplo, *.gmail.com). La longitud máxima es de 1024 caracteres.

  Esta opción requiere la versión de contenido 8284-6139 o una posterior.

  Al configurar las exclusiones FQDN, puede mejorar la experiencia del usuario si le permite acceder a recursos específicos cuando GlobalProtect esté desconectado. Por ejemplo, el endpoint puede comunicarse con un proveedor de identidad alojado en la nube (IdP, Identity Provider) con fines de autenticación o con un servidor de gestión de dispositivos remoto incluso cuando la función Enforce GlobalProtect (Aplicar GlobalProtect) para acceso a la red está habilitada.
- Si los usuarios deben iniciar sesión en un portal cautivo para acceder a internet, especifique cuántos segundos tienen como máximo para hacerlo en **Captive Portal Exception Timeout (sec) (Tiempo de espera para excepción de portal cautivo [s])**; el intervalo es de 0 a 3600 y el valor predeterminado, 0 segundos. Si no inician sesión antes de que transcurra este tiempo, se agota el tiempo de espera de la página de inicio de sesión en el portal cautivo y se impide el uso de la red a los usuarios.

  Para que la aplicación de GlobalProtect muestre una notificación cuando detecte un portal cautivo, configure **Display Captive Portal Detection Message (Mostrar mensaje de detección de portal**

© 2020 Palo Alto Networks, Inc.

cautivo) en **Yes (Sí)**. En el campo **Captive Portal Notification Delay (sec) (Demora de notificación de portal cautivo [s])**, introduzca los segundos que tarda la aplicación de GlobalProtect en mostrar este mensaje; el intervalo es de 1 a 120 y el valor predeterminado, 5 segundos. GlobalProtect inicia este temporizador después de detectar el portal cautivo, pero antes de poder acceder a internet. Si desea ofrecer más instrucciones, configure **Captive Portal Detection Message (Mensaje de detección de portal cautivo)**.

Para iniciar automáticamente su navegador web predeterminado después de la detección del portal cautivo para que los usuarios puedan iniciar sesión sin problemas en él, en el campo **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection (Iniciar automáticamente la página web en el navegador predeterminado tras la detección del portal cautivo)**, especifique el nombre de dominio completo (FQDN) o la dirección IP del sitio web que desee utilizar para el intento de conexión inicial que activa el tráfico web cuando se inicia el navegador web predeterminado (la longitud máxima es de 256 caracteres). El portal cautivo intercepta este intento de conexión del sitio web y redirige el navegador web predeterminado a la página de inicio de sesión del portal cautivo. Si este campo está vacío (predeterminado), GlobalProtect no inicia el navegador web predeterminado automáticamente al detectar el portal cautivo.

Estas opciones necesitan la versión de contenido 607-3486 o una versión posterior. La opción Captive Portal Notification Delay (Demora de notificación de portal cautivo) necesita la versión de contenido 8118-5277 o una versión posterior. La opción Automatically Launch Webpage in Default Browser Upon Captive Portal Detection (Iniciar automáticamente la página web en el navegador predeterminado tras la detección del portal cautivo) requiere la versión de lanzamiento de contenido publicada el 8 de julio de 2019 o posterior.

STEP 4 | Especifique ajustes adicionales de conexión de GlobalProtect.

Cuando el inicio de sesión único (single sign-on, SSO) está habilitado (opción predeterminada), la aplicación de GlobalProtect usa las credenciales de inicio de sesión de Windows del usuario para autenticarse automáticamente y conectarse al portal y puerta de enlace de GlobalProtect. Esto también permite que la aplicación de GlobalProtect ajuste las credenciales de terceros para garantizar que los usuarios de Windows puedan autenticarse y conectarse incluso con un proveedor de credenciales de terceros.

En el área App Configurations, configure cualquiera de las siguientes opciones:

- (Solo Windows y macOS; para que macOS sea compatible es necesaria la versión de contenido 8196-5685 o superior) Establezca **Use Single Sign-On (Windows) (Usar inicio de sesión único (Windows))** o **Use Single Sign-On (macOS) (Usar inicio de sesión único (macOS))** en **No** para deshabilitar el inicio de sesión único.

  Si configura la autenticación de usuarios mediante el lenguaje de marcado para confirmaciones de seguridad (security assertion markup language, SAML) en la puerta de enlace de GlobalProtect y, además, genera y acepta cookies para sustituir la autenticación, debe definir la opción Use Single Sign-On (Usar inicio de sesión único) en No en estos casos: el nombre de usuario de Windows es diferente del nombre de usuario de SAML (por ejemplo, el primero es "usuario" y el segundo, "usuario123") o el nombre de usuario contiene un nombre de dominio completo (fully qualified domain name, FDQN) (por ejemplo, el nombre de usuario de Windows es "usuario" y el de SAML, "usuario@ejemplo.es").
- (Versión de publicación de contenido 8284-6139 o posterior; requiere la aplicación de GlobalProtect 5.2) Establezca **Use Default Browser for SAML Authentication (Usar navegador predeterminado para la autenticación SAML)** en **Yes (Sí)** para habilitar la aplicación de GlobalProtect para abrir el

© 2020 Palo Alto Networks, Inc.

navegador del sistema predeterminado para la autenticación SAML. El valor predeterminado es **No**. La aplicación abrirá un navegador integrado.

Si ha configurado el portal de GlobalProtect para autenticar los usuarios a través de la autenticación de lenguaje de marcado de aserción de seguridad (SAML, Security Assertion Markup Language), los usuarios finales pueden conectarse a la aplicación u otras aplicaciones habilitadas para SAML sin tener que volver a especificar sus credenciales para una experiencia de inicio de sesión único sin problemas (SSO, Single Sign-On). Puede habilitar la aplicación de GlobalProtect para que los usuarios finales puedan aprovechar el mismo inicio de sesión para GlobalProtect y usar su navegador del sistema predeterminado para la autenticación SAML como Chrome, Firefox o Safari.

- Si marca **Automatically Use SSL When IPSec Is Unreliable (Usar SSL automáticamente si IPSec es inestable)**, especifique el número de horas durante las que debe hacerlo la aplicación de GlobalProtect; el intervalo va de 0 a 168 horas. Si configura esta opción, la aplicación de GlobalProtect no intenta establecer ningún túnel de IPSec durante el período especificada. Este temporizador se pone en marcha cada vez que se queda inactivo un túnel de IPSec por haberse agotado el tiempo de espera de su conexión permanente.

  Si acepta el valor predeterminado de `0`, la aplicación no recurre a un túnel de SSL si puede establecer un túnel de IPSec. Solo recurre al primero si no logra establecer el túnel de IPSec.

  Esta opción necesita la versión de contenido publicada el 8 de julio de 2019 o posterior.

- Elija las opciones de conexión SSL para la aplicación de GlobalProtect. Puede optar por aplicar solo conexiones SSL, no permitir conexiones SSL o permitir que el usuario elija SSL o IPSec (predeterminado) dependiendo de la ubicación geográfica y el rendimiento de la red para proporcionar la mejor experiencia de usuario.

  En el área de Configuración de la aplicación, elija las opciones **Connect with SSL Only (Conectar solo con SSL)** que desee permitir.

  Esta opción necesita la versión de contenido 8207-5750 o una versión posterior.

  - **Yes (Sí)**: solicite que todos los clientes de GlobalProtect se conecten únicamente con SSL.
  - **No**: conéctese con el protocolo configurado en la puerta de enlace para la conexión VPN. Si la configuración de la puerta de enlace ha habilitado IPSec, utilizará IPSec para la conexión VPN. Si la puerta de enlace tiene SSL configurado, utilizará SSL para la conexión VPN.
  - **User can Change (El usuario puede cambiar)**: permita que el usuario cambie si quiere usar SSL o seguir utilizando IPSec en la aplicación de GlobalProtect.

    En la aplicación, el usuario puede seleccionar **Settings (Configuración)** > **General** para habilitar **Connect with SSL Only (Conectar solo con SSL)** y **Settings (Configuración)** > **Connection (Conexión)** para comprobar que el **protocolo** sea **SSL**.

- (Versión de publicación de contenido 8346-6423 o posterior; requiere la aplicación de GlobalProtect 5.2.4) Especifique el valor **GlobalProtect Connection MTU (bytes) [MTU de conexión de GlobalProtect (bytes)]** que utiliza la aplicación para conexiones de puerta de enlace. Puede especificar el intervalo de MTU de 1000 a 1420 bytes en lugar del valor predeterminado de MTU de 1400 bytes. El valor predeterminado es de 1400 horas.

  (Solo en Windows UWP) Después de configurar manualmente el valor **GlobalProtect Connection MTU (bytes) [MTU de conexión de GlobalProtect (bytes)]** mediante el comando `netsh`, el cliente de GlobalProtect no podrá establecer el valor **GlobalProtect Connection MTU (bytes) [MTU de conexión de GlobalProtect (bytes)]** en la configuración del portal superior al valor configurado manualmente.

© 2020 Palo Alto Networks, Inc.

Si el valor de MTU es inferior a 1280 bytes e IPv6 está habilitado, el adaptador de GlobalProtect cambiará automáticamente el valor a 1280 bytes según el requisito mínimo de MTU admitido para IPv6.

Puede optimizar la experiencia de conexión para los usuarios finales que se conectan a través de redes que requieren valores de unidad de transmisión máxima (MTU, Maximum Transmission Unit) inferiores al estándar de 1500 bytes configurando el valor de MTU que utiliza la aplicación de GlobalProtect para conectarse a la puerta de enlace. Al reducir el tamaño de la MTU, puede eliminar los problemas de rendimiento y conectividad que se producen debido a la fragmentación cuando las conexiones del túnel VPN pasan por múltiples proveedores de servicios de Internet (ISP, Internet Service Providers) y rutas de red con una MTU inferior a 1500 bytes. Por ejemplo, puede ajustar el valor de MTU para un grupo específico de usuarios de una región a un valor de MTU más bajo mediante una configuración de portal diferente con un requisito de valor de MTU más bajo. El valor de MTU que configuró para un portal específico se aplica a todas las conexiones de túnel de puerta de enlace enumeradas para ese portal para los protocolos de túnel IPSec y SSL.

- Ingrese la **Maximum Internal Gateway Connection Attempts (Cantidad máxima de intentos de conexión con la puerta de enlace interna)** para especificar la cantidad de veces que la aplicación de GlobalProtect puede reintentar la conexión con una puerta de enlace interna una vez que el primer intento falle (el rango es de 0 a 100; se recomienda 4 o 5; el valor predeterminado de 0 indica que la aplicación de GlobalProtect no reintenta la conexión). Si aumenta este valor, puede permitir que la aplicación se conecte a una puerta de enlace interna que está temporalmente desactivada o que no se puede alcanzar, pero se vuelve a activar antes de agotar la cantidad de reintentos especificada. Aumentar el valor también garantiza que la puerta de enlace interna recibe la información de host y usuario más actualizada.
- Ingrese el **GlobalProtect App Config Refresh Interval (Intervalo de actualización para la configuración de la aplicación de GlobalProtect)** para especificar la cantidad de horas que el portal de GlobalProtect espera antes de iniciar la siguiente actualización de la configuración de un cliente (el rango es de 1 a 168; el valor predeterminado es 24).
- (Solo para Windows) De acuerdo con sus requisitos de seguridad, especifique si desea **Retain Connection on Smart Card Removal (Conservar conexión si se extrae la tarjeta inteligente)**. De manera predeterminada, esta opción está configurada en **Yes (Sí)**, lo que significa que GlobalProtect conserva el túnel cuando un usuario extrae una tarjeta inteligente que contiene un certificado de cliente. Para finalizar el túnel, configure esta opción en **No**.

  Esta función requiere una versión de contenido 590-3397 o posterior.

- Configure una **Automatic Restoration of VPN Connection Timeout (Restauración automática del tiempo de espera de la conexión VPN)** para especificar la acción que realiza GlobalProtect cuando se desconecta el túnel. Configure esta opción en **Yes (Sí)** para permitir que GlobalProtect intente restablecer la conexión una vez que se desconecte el túnel. Configure esta opción en **No** para evitar que GlobalProtect intente volver a conectarse una vez que se desconecte el túnel. Configure **Wait Time Between VPN Connection Restore Attempts (Tiempo de espera entre intentos de restaurar la conexión VPN)** para ajustar la cantidad de tiempo (en segundos) que GlobalProtect espera entre los intentos de restaurar la conexión (el rango es de 1 a 60 segundos; el valor predeterminado es 5).

  Con el método de conexión "siempre activada", si un usuario cambia de una red externa a una interna antes de que caduque el valor del tiempo de espera, GlobalProtect no lleva a cabo una detección de red. Como resultado, GlobalProtect restaura la conexión a la última puerta de enlace externa conocida. Para activar la detección del host interno, el usuario debe seleccionar Refresh Connection (Actualizar conexión) desde el menú de configuración en el panel de estado de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Configure los menús y las vistas de IU que están disponibles para los usuarios que tienen esta configuración de agente.

En el área App Configurations, configure cualquiera de las siguientes opciones:

- Si desea que los usuarios vean solo la información de estado básica dentro de la aplicación, configure **Enable Advanced View (habilitar vista avanzada)** en **No**. Cuando deshabilite esta opción, los usuarios podrán ver la información de las siguientes pestañas:
  - **General**: muestra el nombre de usuario y los portales asociados a la cuenta de GlobalProtect.
  - **Notification (Notificación)**: muestra cualquier notificación de GlobalProtect.

  El valor predeterminado es **Yes (Sí)**. Cuando habilite esta opción, los usuarios podrán ver las siguientes pestañas adicionales:
  - **Connection (Conexión)**: muestra las puertas de enlace configuradas para la aplicación de GlobalProtect e información sobre cada puerta de enlace.
  - **Host Profile (Perfil de host)**: muestra los datos de endpoint que GlobalProtect utiliza para supervisar y aplicar políticas de seguridad mediante HIP.
  - **Troubleshooting (Solución de problemas)**: muestra información sobre la configuración de red, la configuración de ruta, las conexiones activas y los logs. También puede recopilar logs generados por GlobalProtect y establecer el nivel de log.
- Si desea ocultar el icono de la bandeja del sistema de GlobalProtect en los endpoints, configure **Display GlobalProtect Icon (Mostrar icono de GlobalProtect)** en **No**. Cuando el icono está oculto, los usuarios no pueden realizar tareas como cambiar contraseñas guardadas, volver a detectar la red, volver a enviar información de host, ver información de solución de problemas o iniciar conexiones a demanda. Sin embargo, los mensajes de notificaciones HIP, intentos de inicio de sesión y diálogos de certificados aún se muestran según sea necesario.
- Para evitar que los usuarios lleven a cabo la detección de red, configure **Enable Rediscover Network Option (Habilitar opción para volver a detectar la red)** en **No**. Cuando deshabilita esta opción, la opción **Refresh Connection (Actualizar conexión)** está en gris en el menú de ajustes del panel de estado de GlobalProtect.
- Para evitar que los usuarios reenvíen manualmente los datos HIP a la puerta de enlace, configure **Enable Resubmit Host Profile Option (Habilitar la opción de volver a enviar el perfil de host)** en **No**. Esta opción está habilitada de manera predeterminada y es útil en casos en los que la política de seguridad basada en HIP evita que los usuarios accedan a los recursos, ya que permite que el usuario solucione el problema de cumplimiento en el ordenador antes de volver a enviar los datos de HIP.
- (Solo para Windows) para permitir que GlobalProtect muestre notificaciones en la bandeja del sistema, configure **Show System Tray Notifications (Mostrar notificaciones de la bandeja del sistema)** en **Yes (Sí)**.
- Para crear un mensaje personalizado que se muestre a los usuarios cuando las contraseñas estén por vencer, ingrese uno en **Custom Password Expiration Message (LDAP Authentication Only) (Mensaje personalizado de vencimiento de contraseña [Solo para la autenticación LDAP])**. La longitud máxima del mensaje es de 200 caracteres.
- Para crear un mensaje personalizado que especifique las políticas o requisitos de contraseña cuando los usuarios cambian su contraseña de Active Directory (AD), ingrese uno en **Change Password Message (Mensaje de cambio de contraseña)**. La longitud máxima del mensaje es de 255 caracteres.

STEP 6 | Defina qué usuarios finales con esta configuración pueden hacerlo en su aplicación.

- Configure **Allow User to Change Portal Address (Permitir al usuario modificar la dirección del portal)** en **No** para deshabilitar el campo **Portal** en el panel de estado de la aplicación de GlobalProtect. Como el usuario no puede especificar el portal al que se debe conectar, debe suministrar su dirección predeterminada en el registro de Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` con la clave `Portal`) o en la lista de propiedades de macOS (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist` [Librería/Preferencias/

© 2020 Palo Alto Networks, Inc.

`com.paloaltonetworks.GlobalProtect.settings.plist]` con la clave `Portal` en el diccionario `PanSetup`). Para obtener más información, consulte Implementación de la configuración de la aplicación de forma trasparente.

- Para evitar que los usuarios descarten la página de bienvenida, configure **Allow User to Dismiss Welcome Page** en **No**. Cuando esta opción está configurada en **Yes (Sí)**, el usuario puede omitir la página de bienvenida y evitar que GlobalProtect muestre la página después de los inicios de sesión subsiguientes.

STEP 7 | Especifique si los usuarios pueden deshabilitar la aplicación de GlobalProtect.

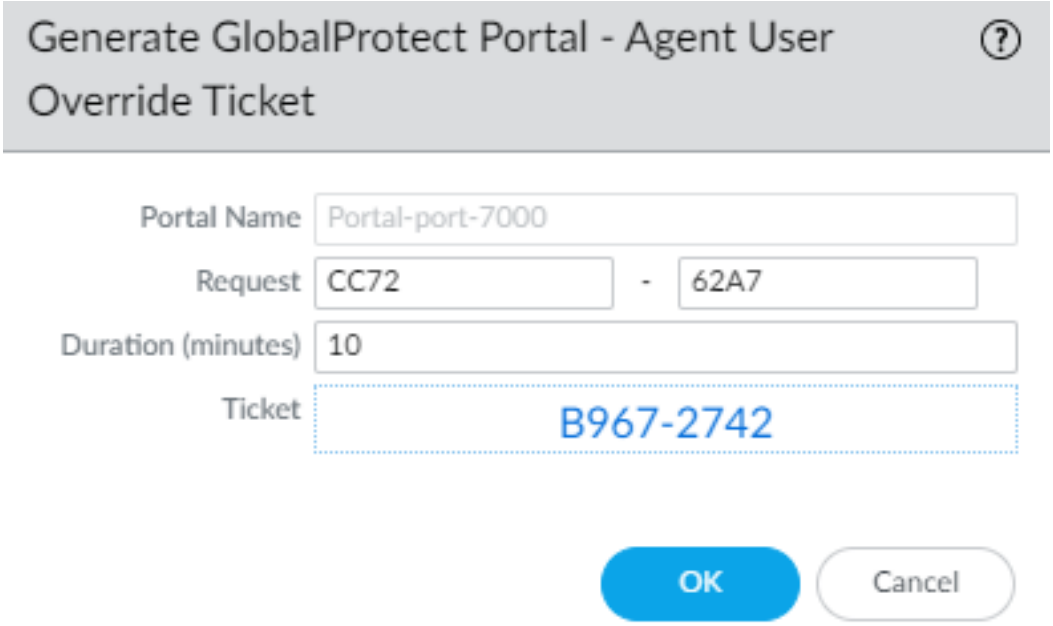
La opción **Allow User to Disable GlobalProtect (Permitir al usuario deshabilitar GlobalProtect)** se aplica a las configuraciones de agente con el **Connect Method (Método de conexión) User-Logon (Always On) (Inicio de sesión del usuario [Siempre activado])**. En el modo de inicio de sesión del usuario, la aplicación se conecta automáticamente tan pronto como el usuario inicia sesión en el endpoint. Este modo a veces se denomina como "siempre activado", es por eso que el usuario debe anular este comportamiento para deshabilitar la aplicación de GlobalProtect.

De manera predeterminada, esta opción está configurada en **Allow (Permitir)**, lo que permite que los usuarios deshabiliten GlobalProtect sin brindar un comentario, código de acceso o número de vale.

Si el icono de bandeja del sistema de GlobalProtect no está visible, los usuarios no pueden deshabilitar la aplicación de GlobalProtect. Consulte el paso 5 para obtener más información.

- Para evitar que los usuarios con el método de conexión de inicio de sesión del usuario desactiven GlobalProtect, configure **Allow User to Disable GlobalProtect (Permitir al usuario desactivar la aplicación de GlobalProtect)** en **Disallow (No permitir)**.
- Para permitir que los usuarios deshabiliten GlobalProtect solo si brindan un código de acceso, configure **Allow User to Disable GlobalProtect App (Permitir al usuario deshabilitar la aplicación de GlobalProtect)** en **Allow with Passcode (Permitir con código de acceso)**. Luego, en el área Disable GlobalProtect App (Desactivar aplicación de GlobalProtect), introduzca (y confirme) el **Passcode (Código de acceso)** que los usuarios finales deben suministrar.
- Para permitir que los usuarios deshabiliten GlobalProtect solo si brindan un vale, configure **Allow User to Disable GlobalProtect (Permitir al usuario deshabilitar GlobalProtect)** en **Allow with Ticket (Permitir con vale)**. Con esta opción, la acción de deshabilitar hace que la aplicación genere un número de solicitud, que el usuario final debe comunicar al administrador. Entonces el administrador hace clic en la página **Generate Ticket (Genera ticket)** en la página **Network (Red)** > **GlobalProtect** > **Portals (Portales)** e introduce el número de solicitud desde el usuario final para general el vale. El administrador proporciona el vale al usuario final, quien lo ingresa en el diálogo Disable GlobalProtect (Deshabilitar GlobalProtect) para desactivar la aplicación.

© 2020 Palo Alto Networks, Inc.



- Para limitar la cantidad de veces que los usuarios pueden deshabilitar la aplicación de GlobalProtect, especifique el valor en **Max Times User Can Disable (Cantidad máxima de veces que el usuario puede deshabilitar)** en el área Disable GlobalProtect App (Deshabilitar la aplicación de GlobalProtect). Un valor de 0 (predeterminado) indica que los usuarios no están limitados en la cantidad de veces que pueden deshabilitar la aplicación.

  Este ajuste se aplica solo con las opciones Allow (Permitir), Allow with Comment (Permitir con comentario) y Allow with Passcode (Permitir con código de acceso).

  Si los usuarios ya deshabilitaron la aplicación de GlobalProtect la cantidad máxima de veces y deben continuar teniendo la capacidad de deshabilitar la aplicación:

  - Puede aumentar el valor de **Max Times User Can Disable (Cantidad máxima de veces que el usuario puede deshabilitar)** en la configuración de agente del portal de GlobalProtect (**Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **App (Aplicación)**). El usuario debe seleccionar **Refresh Connection (Actualizar conexión)** en el menú de ajustes del panel de estado de GlobalProtect o establecer una nueva conexión de GlobalProtect para que se aplique el valor nuevo.
  - Los usuarios deberán volver a instalar la aplicación para reiniciar el contador.
- Para restringir la duración en que la aplicación puede deshabilitarse, ingrese un valor en **Disable Timeout (min) (Deshabilitar tiempo de espera [minutos])** en el área Disable GlobalProtect App (Deshabilitar aplicación de GlobalProtect). Un valor de 0 (predeterminado) indica que no hay una restricción de tiempo en la que el usuario puede mantener deshabilitada la aplicación.

  Este ajuste se aplica solo con las opciones Allow (Permitir), Allow with Comment (Permitir con comentario) y Allow with Passcode (Permitir con código de acceso).

STEP 8 | Especifique si los usuarios pueden desinstalar la aplicación de GlobalProtect.

Use la opción **Allow User to Uninstall GlobalProtect App (Permitir al usuario desinstalar la aplicación de GlobalProtect)** para permitir a los usuarios desinstalar la aplicación de GlobalProtect, evitar que desinstalen dicha aplicación o permitir que la desinstalen si especifican una contraseña creada por usted.

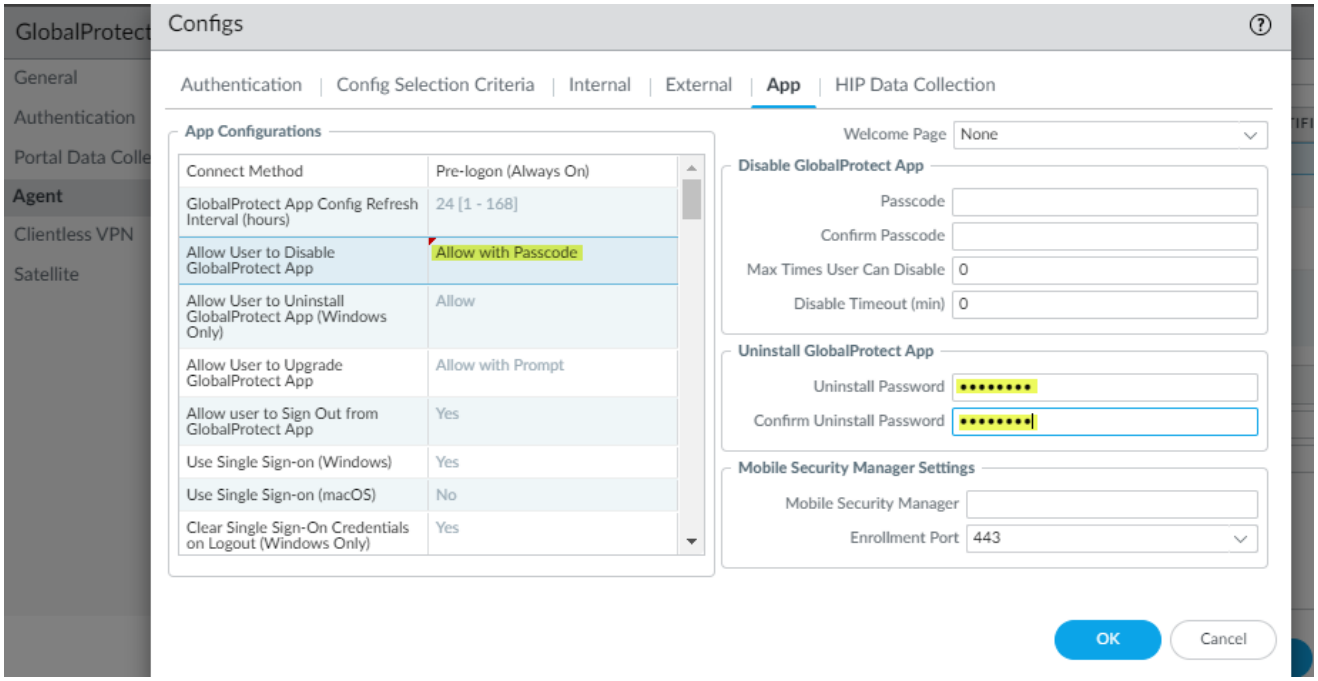
© 2020 Palo Alto Networks, Inc.

Esta configuración se envía al registro del dispositivo de endpoint cuando se conecta al portal por primera vez, y se guarda para cada portal al que se conecta.

Esta opción necesita la versión de contenido 8207-5750 o una versión posterior.

- Para permitir que los usuarios desinstalen la aplicación GlobalProtect sin restricciones, seleccione **Allow (Permitir)**.
- Para evitar que los usuarios desinstalen la aplicación de GlobalProtect, seleccione **Disallow (No permitir)**.

  Si establece **Disallow (No permitir)** en el registro de Windows, el valor para ese portal se establece en 1 en `Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\ 'Uninstall = 1'`.
- Para permitir que los usuarios desinstalen la aplicación de GlobalProtect con una contraseña, seleccione **Allow with Passcode (Permitir con código de acceso)**; después, en la sección Uninstall GlobalProtect App (Desinstalar aplicación de GlobalProtect), especifique una **contraseña de desinstalación** y **confírmela**.



STEP 9 | Especifique si los usuarios pueden cerrar sesión en la aplicación de GlobalProtect.

En el área App Configurations (Configuraciones de la aplicación), establezca **Allow user to Sign Out from GlobalProtect App (Permitir al usuario cerrar sesión en la aplicación de GlobalProtect)** en **No** para evitar que los usuarios cierren sesión en la aplicación de GlobalProtect; establezca **Allow user to Sign Out from GlobalProtect App (Permitir que el usuario cierre sesión en la aplicación de GlobalProtect)** en **Yes (Sí)** para permitir que los usuarios cierren sesión.

Esta opción requiere la versión de contenido 8196-5685 o una posterior.

STEP 10 | Configure los ajustes de certificado y el comportamiento de los usuarios que reciben esta configuración.

© 2020 Palo Alto Networks, Inc.

En el área App Configurations, configure cualquiera de las siguientes opciones:

- **Client Certificate Store Lookup (Búsqueda de almacenes de certificados de cliente)**: seleccione qué almacén debe usar la aplicación para buscar certificados de clientes. Los certificados de **User (Usuario)** se guardan en el almacén de certificados del usuario actual en Windows y en el llavero personal en macOS. Los certificados de **Machine (Equipo)** se guardan en el almacén de certificados del ordenador local en Windows y en el llavero del sistema en macOS. De manera predeterminada, la aplicación busca certificados de **User and machine (Usuario y equipo)** en ambos lugares.
- **SCEP Certificate Renewal Period (days)**: con SCEP, el portal puede solicitar un nuevo certificado de cliente antes de que el certificado caduque. Este periodo antes de que el certificado caduque es el *periodo de renovación del certificado SCEP* opcional. Durante una cantidad configurable de días antes de que el certificado del cliente caduque, el portal puede solicitar un nuevo certificado del servidor SCEP en la PKI de la empresa (el intervalo es 0-30; el valor por defecto es 7). Un valor de 0 significa que el portal no renueva automáticamente el certificado de cliente cuando actualiza la configuración de cliente.

  Para que la aplicación de GlobalProtect obtenga el certificado nuevo durante el período de renovación, el usuario debe iniciar sesión en la aplicación. Por ejemplo, si un certificado de cliente posee un periodo de validez de 90 días, el periodo de renovación del certificado es de 7 días y el usuario inicia sesión durante los 7 días finales del periodo de validez del certificado, el portal adquiere un nuevo certificado y lo implementa con una configuración de agente nueva. Para obtener más información, consulte Implementación de certificados de cliente específicos del usuario para autenticación.
- **Extended Key Usage OID for Client Certificate (OID de uso de clave extendida para el certificado de cliente)** (solo para endpoints de Windows y macOS): use esta opción solo si habilitó la autenticación de cliente, espera varios certificados de cliente en el endpoint e identificó un objetivo secundario mediante el cual puede filtrar los certificados de cliente. Esta opción le permite especificar un objetivo secundario para un certificado de cliente utilizando el identificador de objeto (OID) asociado. Por ejemplo, para mostrar solo certificados de clientes que también sean para la autenticación de servidor, ingrese el OID 1.3.6.1.5.5.7.3.1. Cuando la aplicación de GlobalProtect encuentra solo un certificado de cliente que coincide con el objetivo secundario, GlobalProtect automáticamente lo selecciona y realiza la autenticación con ese certificado. De lo contrario, GlobalProtect solicita al usuario que seleccione el certificado del cliente de la lista de certificados de clientes filtrados que coincida con los criterios. Para obtener más información, incluida una lista de objetivos comunes de certificados y OID, consulte la Guía de funciones nuevas de PAN-OS 7.1.
- Si no desea que la aplicación establezca una conexión con el portal cuando el certificado del portal no es válido, configure **Allow User to Continue with Invalid Portal Server Certificate (Permitir al usuario continuar con certificado de servidor del portal no válido)** en **No**. Tenga en cuenta que el portal brinda solo la configuración del agente, no el acceso de red. Por lo tanto, la seguridad del portal es menos crítica que la seguridad de la puerta de enlace. Sin embargo, si implementó un certificado de servidor de confianza para el portal, deshabilitar esta opción puede ayudarlo a evitar los ataques por desconocidos (man-in-the-middle, MTM).

STEP 11 | Especifique si los usuarios reciben avisos de inicio de sesión cuando se requiere autenticación multifactor para acceder a los recursos de red confidenciales.

Para las conexiones de puerta de enlace, los recursos de red confidenciales (como aplicaciones financieras o de desarrollo de software) pueden requerir más autenticación. Puede configurar GlobalProtect para mostrar las notificaciones de autenticación multifactor que se requieren para acceder a estos recursos.

En el área App Configurations, configure cualquiera de las siguientes opciones:

- Establezca **Enable Inbound Authentication Prompts from MFA Gateways (Habilitar solicitudes de autenticación entrantes desde las puertas de enlace de MFA)** en **Yes (Sí)**. Para admitir la autenticación multifactor (multi-factor authentication, MFA), la aplicación de GlobalProtect

© 2020 Palo Alto Networks, Inc.

debe recibir y aceptar las solicitudes UDP entrantes de la puerta de enlace. Seleccione **Yes (Sí)** para permitir que las aplicaciones de GlobalProtect reciban y acepten la indicación. De manera predeterminada, el valor está configurado en **No**, lo que significa que GlobalProtect bloqueará las solicitudes UDP de la puerta de enlace.

- Especifique el **Network Port for Inbound Authentication Prompts (UDP) (Puerto de red para las solicitudes de autenticación entrantes [UDP])** que la aplicación de GlobalProtect usa para recibir las solicitudes de autenticación entrantes de las puertas de enlace de MFA. El puerto predeterminado es 4501. Para cambiar el puerto, especifique un número de 1 a 65535.
- Especifique las **Trusted MFA Gateways (Puertas de enlace de MFA de confianza)** en las que la aplicación de GlobalProtect puede confiar para realizar la autenticación multifactor. Cuando una aplicación de GlobalProtect recibe un mensaje UDP en el puerto de red especificado, GlobalProtect muestra un mensaje de autenticación solo si la indicación de UDP proviene de una puerta de enlace de confianza.
- Configure **Inbound Authentication Message (Mensaje de autenticación entrante)**, por ejemplo, `You have attempted to access a protected resource that requires additional authentication (Intentó acceder a un recurso protegido que requiere autenticación adicional). Proceda a la autenticación en:`. Cuando los usuarios intentan acceder a un recurso que requiere autenticación adicional, GlobalProtect recibe y muestra un mensaje de autenticación entrante. GlobalProtect automáticamente adjunta la URL de la página del portal de autenticación que especifica cuando configura la autenticación multifactor al mensaje de autenticación entrante.

STEP 12 | (Solo en Windows) Configure los ajustes de los endpoints de Windows que reciben estos parámetros.

- **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only) [Resolver todos los FQDN utilizando servidores DNS asignados por el túnel (solo Windows)]**: configure las preferencias de resolución DNS para el túnel de GlobalProtect. Seleccione **No** para permitir que los endpoints de Windows envíen consultas DNS al servidor DNS configurado en el adaptador físico si el servidor DNS configurado en la puerta de enlace no resuelve la consulta inicial. Esta opción conserva el comportamiento nativo de Windows para consultar todos los servidores DNS en todos los adaptadores recursivamente, pero puede dar lugar a largos tiempos de espera para resolver algunas consultas DNS. Seleccione **Yes (Sí)** (predeterminado) para permitir que los endpoints de Windows resuelvan todas las consultas DNS con los servidores DNS que configure en la puerta de enlace, en lugar de permitir que el endpoint envíe algunas consultas DNS a los servidores DNS configurados en el adaptador físico.

  Esta función no admite DNS en TCP.

  Esta función requiere la versión de lanzamiento de contenido 731 o posterior y la aplicación de GlobalProtect 4.0.3 y versiones posteriores.
- **Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Enviar informe de HIP de inmediato si cambia el estado del Centro de seguridad de Windows [WSC])**: seleccione **No** para evitar que la aplicación de GlobalProtect envíe datos HIP cuando cambia el estado del Centro de seguridad de Windows (Windows Security Center, WSC). Seleccione **Yes (Sí)** (valor por defecto) para enviar inmediatamente datos HIP cuando cambia el estado de WSC.
- **Clear Single Sign-On Credentials on Logout (Borrar credenciales de inicio de sesión único al cerrar sesión)**: seleccione **No** para conservar credenciales de inicio de sesión único cuando el usuario cierra sesión. Seleccione **Yes (Sí)** (predeterminado) para borrarlas y forzar a los usuarios a ingresar las credenciales en el siguiente inicio de sesión.
- **Use Default Authentication on Kerberos Authentication Failure**: seleccione **No** para usar solo la autenticación de Kerberos. Seleccione **Yes (Sí)** (predeterminado) para volver a intentar usando el método de autenticación predeterminado una vez que la autenticación de Kerberos falle.

© 2020 Palo Alto Networks, Inc.

STEP 13 | (Solo en Windows) Configure la aplicación de GlobalProtect para los endpoints de Windows en **Detect Proxy for Each Connection (Detectar proxy en cada conexión)**.

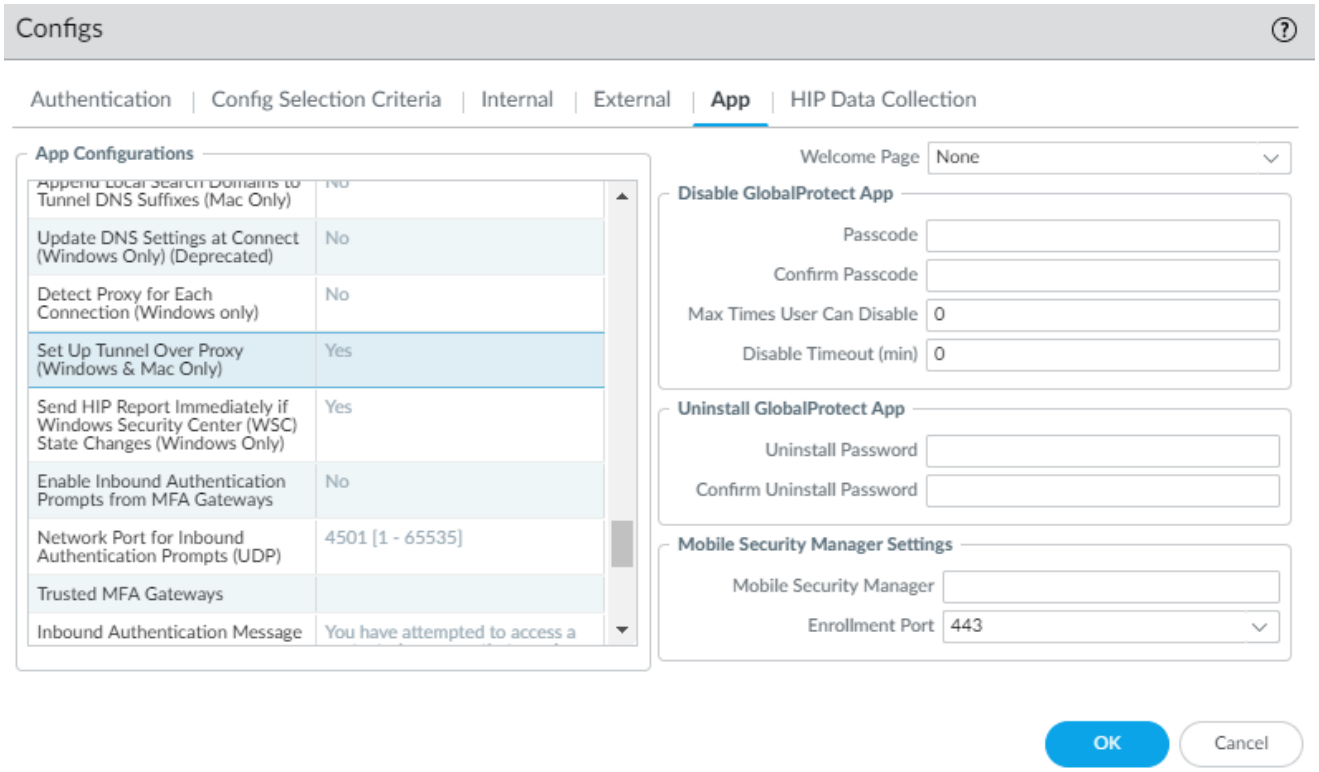
Para obtener más información sobre el comportamiento del tráfico de red basado en el uso de los proxies, consulte la sección relativa a las conexiones de túneles por proxies.

- Seleccione **No** para detectar automáticamente el proxy de la conexión del portal y usarlo para conexiones posteriores.
- Seleccione **Yes (Sí)** (predeterminado) para autodetectar el servidor proxy en cada conexión.

STEP 14 | (Solo en Windows y macOS) Especifique si GlobalProtect debe utilizar los proxies o eludirlos.

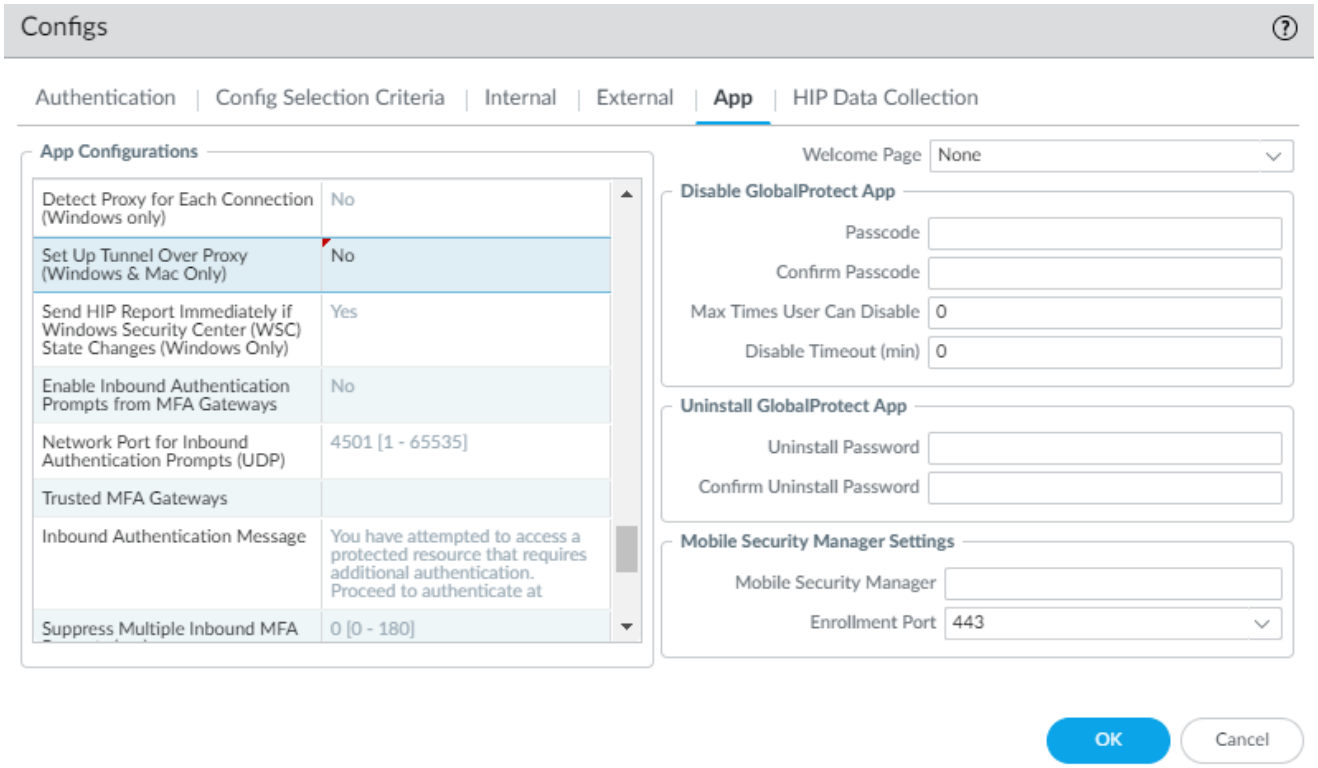
Este ajuste permite configurar el comportamiento del tráfico de red basándose en el uso de los proxies de GlobalProtect. Para obtener más información, consulte la sección relativa a las conexiones de túneles por proxies.

- Para exigir que GlobalProtect utilice los proxies, defina la opción **Set Up Tunnel Over Proxy (Windows & Mac only) (Configurar túnel por proxy [solo en Windows y Mac])** en **Yes (Sí)**.



- Para exigir que GlobalProtect eluda los proxies, defina la opción **Set Up Tunnel Over Proxy (Windows & Mac only) (Configurar túnel por proxy [solo en Windows y Mac])** en **No**.

© 2020 Palo Alto Networks, Inc.



STEP 15 | Si sus endpoints experimentan latencia o lentitud con frecuencia al conectarse al portal o las puertas de enlace de GlobalProtect, considere el ajuste de los valores de tiempo de espera del portal y TCP.

Para darles más tiempo a sus endpoints para que se conecten o reciban datos del portal o puerta de enlace, aumente los valores de tiempo de espera según sea necesario. Tenga en cuenta que si aumenta los valores, se pueden generar tiempos de espera más prolongados si la aplicación de GlobalProtect no puede establecer la conexión. Por el contrario, si reduce los valores, es posible que se impida que la aplicación de GlobalProtect establezca una conexión cuando el portal o la puerta de enlace no responde antes de que finalice el tiempo de espera.

En el área App Configurations (Configuraciones de la aplicación), configure algunas de las siguientes opciones de tiempo de espera:

- **Portal Connection Timeout (sec) (Tiempo de espera de conexión con el portal [segundos])**: la cantidad de segundos (de 1 a 600) antes de que se agote el tiempo de espera de la solicitud de conexión al portal debido a que este no responde. Cuando su cortafuegos ejecuta versiones de contenido de aplicaciones y amenazas anteriores a 777-4484, el valor predeterminado es 30. A partir de la versión de contenido 777-4484, el valor predeterminado es 5.
- **TCP Connection Timeout (sec) (Tiempo de espera de conexión TCP [segundos])**: la cantidad de segundos (de 1 a 600) antes de que se agote el tiempo de espera de la solicitud de conexión TCP debido a que no hay respuesta en un extremo de la conexión. Cuando su cortafuegos ejecuta versiones de contenido de aplicaciones y amenazas anteriores a 777-4484, el valor predeterminado es 60. A partir de la versión de contenido 777-4484, el valor predeterminado es 5.
- **TCP Receive Timeout (sec)**: la cantidad de segundos antes de que una conexión TCP se agote debido a la falta de cierta respuesta parcial de una solicitud TCP (el intervalo es 1-600; el valor por defecto es 30).

STEP 16 | (Windows 10 y macOS con macOS Catalina 10.15.4 o posterior; requiere la aplicación de GlobalProtect™ 5.2) Especifique si desea habilitar el DNS dividido para permitir que los usuarios

© 2020 Palo Alto Networks, Inc.

dirijan sus consultas de DNS para aplicaciones y recursos a través del túnel VPN o fuera del túnel VPN además del tráfico de red. Para ello, especifique **Split-Tunnel Option (Opción de túnel dividido)**.

Seleccione **Network Traffic Only (Solo tráfico de red)** para incluir y excluir reglas que se aplican solo al tráfico de aplicaciones de red y no al tráfico de DNS. Todo el tráfico DNS pasa por el túnel VPN independientemente del túnel dividido según el dominio de destino que especificó para las inclusiones y exclusiones. Cuando selecciona **Both Network Traffic and DNS (Tráfico de red y DNS)**, el túnel dividido basado en el dominio de destino que especificó para las inclusiones y exclusiones se aplica al tráfico de DNS y al tráfico de aplicaciones de red asociado para ese dominio.

Con Split DNS (DNS dividido), puede configurar qué dominios resuelven los servidores DNS asignados por VPN y qué dominios pueden resolver los servidores DNS locales.

Esta opción requiere la versión de contenido 8284-6139 o una posterior.

STEP 17 | Especifique si se permitirán conexiones de escritorio remotas en los túneles VPN existentes al especificar el tiempo de espera del switch del usuario para renombrar el túnel en **User Switch Tunnel Rename Timeout**. Cuando un usuario nuevo se conecta a un equipo de Windows usando el protocolo de escritorio remoto (Remote Desktop Protocol, RDP), la puerta de enlace reasigna el túnel VPN al nuevo usuario. Entonces la puerta de enlace puede aplicar las políticas de seguridad en el nuevo usuario.

El permitir las conexiones de escritorio remotas en los túneles VPN puede ser útil en situaciones en las que un administrador de TI necesita acceder a un sistema de usuario final remoto usando RDP.

De manera predeterminada, el valor de **User Switch Tunnel Rename Timeout (Tiempo de espera para cambio de nombre del túnel de cambio del usuario)** es 0, lo que significa que la puerta de enlace de GlobalProtect finaliza la conexión si un usuario nuevo se autentica mediante el túnel VPN. Para modificar este comportamiento, configure un valor de 1 a 600 segundos. Si el nuevo usuario no inicia sesión en la puerta de enlace antes de que se agote el tiempo de espera, la puerta de enlace de GlobalProtect finaliza el túnel de VPN asignado al primer usuario.

El cambio del valor de User Switch Tunnel Rename Timeout (Tiempo de espera para cambio de nombre del túnel del switch del usuario) solo afecta al túnel RDP y no cambia el nombre de un túnel anterior al inicio de sesión cuando se configura.

STEP 18 | Para permitir que GlobalProtect conserve el túnel VPN existente después de que los usuarios cierren sesión en su endpoint, especifique un valor **Preserve Tunnel on User Logoff Timeout (Conservar túnel cuando el usuario se desconecte)** (el intervalo es de 0 a 600 segundos; el valor predeterminado es 0 segundos). Si acepta el valor predeterminado de `0`, GlobalProtect no conserva el túnel después del cierre de sesión del usuario.

Esta opción necesita la versión de contenido publicada el 8 de julio de 2019 o posterior.

Tenga en cuenta los siguientes comportamientos de conexión de GlobalProtect cuando configure GlobalProtect para conservar el túnel VPN:

- Si el mismo usuario cierra sesión y luego vuelve a iniciar sesión en un endpoint dentro del periodo de espera especificado en el modo Always On (Siempre activado) u On-Demand (Bajo demanda), GlobalProtect permanecerá conectado sin solicitar ninguna interacción del usuario (incluida la autenticación del portal y la puerta de enlace). Si el usuario no vuelve a iniciar sesión dentro del periodo de espera especificado, el túnel se desconecta y debe restablecer la conexión de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

- Si un usuario cierra la sesión de un endpoint y, a continuación, un usuario diferente inicia sesión en el mismo endpoint en el modo Always On (Siempre activado) u On-Demand (Bajo demanda), el túnel existente cambia de nombre para el nuevo usuario solo si el nuevo usuario se autentica con éxito en GlobalProtect dentro del especificado periodo de espera. Si el nuevo usuario no inicia sesión y se autentica correctamente dentro del periodo de espera especificado, el túnel existente se desconecta y se debe establecer una nueva conexión a GlobalProtect. Si el nuevo usuario está en modo Always On (Siempre activado), GlobalProtect intenta establecer una nueva conexión automáticamente. Si el nuevo usuario está en modo On-Demand (Bajo demanda), debe establecer una nueva conexión a GlobalProtect manualmente.

STEP 19 | Especifique cómo se actualizará la aplicación de GlobalProtect.

Si desea controlar cuándo los usuarios pueden actualizar, puede personalizar la actualización de la aplicación por configuración. Por ejemplo, si desea probar una versión en un pequeño grupo de usuarios antes de implementarla en toda su base de usuarios, puede crear una configuración que se aplique a los usuarios de su grupo de TI solamente; de esta manera, les permitirá actualizar y probar la aplicación y se deshabilitarán las actualizaciones en todas las demás configuraciones de usuario o grupo. Una vez que haya examinado detenidamente la versión nueva, puede modificar las configuraciones de agente para el resto de sus usuarios a fin de permitir la actualización.

De manera predeterminada, la opción **Allow User to Upgrade GlobalProtect App (Permitir al usuario actualizar la aplicación de GlobalProtect)** está configurada en **Allow with Prompt (Permitir con solicitud)**, lo que significa que se solicita a los usuarios finales que actualicen cuando se activa una versión nueva de la aplicación en el cortafuegos. Para modificar este comportamiento, seleccione una de las siguientes opciones:

- **Allow Transparently (Permitir de forma transparente)**: las actualizaciones se producen automáticamente sin la interacción del usuario. Las actualizaciones pueden ocurrir cuando el usuario esté trabajando de manera remota o conectado dentro de la red corporativa.
- **Internal (Interna)**: las actualizaciones se producen automáticamente sin la interacción del usuario, siempre que este esté conectado dentro de la red corporativa. Se recomienda esta configuración para evitar actualizaciones lentas en situaciones de poco ancho de banda. Cuando un usuario se conecta desde afuera de la red corporativa, la actualización se pospone y se vuelve a activar cuando el usuario se conecta dentro de la red corporativa. Debe configurar puertas de enlace internas y detección de host interno para usar esta opción.
- **Disallow (No permitir)**: esta opción evita las actualizaciones de la aplicación.
- **Allow Manually (Permitir manualmente)**: los usuarios finales inician las actualizaciones de la aplicación. En este caso, el usuario debe seleccionar **Check Version (Comprobar versión)** en el menú de configuración del panel de estado de GlobalProtect para determinar si existe una versión nueva disponible de la aplicación y, luego, actualizarla si lo desea. Tenga en cuenta que esta opción no funciona si la aplicación de GlobalProtect está oculta del usuario. Consulte el paso 5 para obtener detalles sobre la configuración de **Display GlobalProtect Icon (Mostrar icono de GlobalProtect)**.

Las actualizaciones para Allow Transparently (Permitir de manera transparente) y Internal (Interno) solo tienen lugar si la versión del software de GlobalProtect en el portal es más reciente que la versión del software de GlobalProtect en el endpoint. Por ejemplo, un agente de GlobalProtect 3.1.3 que se conecta a un portal de GlobalProtect 3.1.1 no se actualiza.

STEP 20 | Añada un **Change Password Message (Mensaje de cambio de contraseña)** para especificar las políticas o requisitos de contraseña que sus usuarios deben cumplir cuando cambian las contraseñas (por ejemplo, debe contener al menos un número y una letra en mayúscula).

© 2020 Palo Alto Networks, Inc.

STEP 21 | Especifique si desea que la aplicación de GlobalProtect envíe logs de criterios de selección de puerta de enlace al cortafuegos especificando la opción **Log Gateway Selection Criteria (Criterios de selección de puerta de enlace de log)**.

Seleccione **Yes (Sí)** para permitir que la aplicación de GlobalProtect envíe los logs mejorados para los criterios de selección de la puerta de enlace al cortafuegos. El valor predeterminado es **No**. La aplicación no envía los logs mejorados al cortafuegos.

Para ayudarlo a identificar detalles de por qué la aplicación de GlobalProtect eligió conectarse a una puerta de enlace específica, la aplicación de GlobalProtect recopila e informa información para identificar los criterios de selección de la puerta de enlace y la latencia entre la puerta de enlace y el endpoint. La información sobre los criterios de selección de la puerta de enlace puede ayudarlo a identificar la prioridad y el tiempo de respuesta de la puerta de enlace seleccionada, la lista de intentos de conexión de la puerta de enlace y las estadísticas sobre la latencia de la red antes y después del túnel. Los campos de logs mejorados para los criterios de selección de la puerta de enlace se han añadido a los logs de GlobalProtect en **Monitor (Supervisar)** > **Logs** > **GlobalProtect**.

STEP 22 | Especifique si desea mostrar una página de bienvenida cuando el inicio de sesión se realice correctamente.

Una página de bienvenida puede ser útil para dirigir a los usuarios a los recursos internos a los que solo pueden acceder cuando están conectados a GlobalProtect, como su Intranet u otros servidores internos.

De manera predeterminada, la única indicación de que la aplicación se conectó correctamente es un mensaje de globo que muestra la barra del menú o la bandeja del sistema.

Para mostrar una página de bienvenida después de un inicio de sesión correcto, seleccione **factory-default (predeterminado de fábrica)** en el menú desplegable **Welcome Page (Página de bienvenida)**. GlobalProtect muestra la página de bienvenida en la aplicación de GlobalProtect. También puede seleccionar una página de bienvenida personalizada que brinde información específica a sus usuarios o para un grupo de usuarios concreto (según la configuración de portal que se implemente). Para obtener detalles sobre la creación de páginas personalizadas, consulte Personalización de las páginas de inicio de sesión, bienvenida y ayuda del portal de GlobalProtect.

STEP 23 | (Solo en Windows) En **Display Status Panel at Startup (Mostrar panel de estado al inicio)**, especifique si la aplicación de GlobalProtect debe abrir este panel.

- Para suprimir el panel de estado cuando los usuarios establecen la conexión de GlobalProtect por primera vez, seleccione **No**.
- Para mostrar el panel de estado automáticamente cuando los usuarios establecen la conexión de GlobalProtect por primera vez, seleccione **Yes (Sí)**. Con esta opción, los usuarios deben hacer clic fuera del panel de estado para cerrarlo manualmente.

STEP 24 | Guarde la configuración del agente.

1. Si ya terminó de realizar la personalización de sus configuraciones de agente, haga clic en **OK (Aceptar)** para guardar su configuración de agente. De lo contrario, vuelva a Definición de la configuración del agente de GlobalProtect para completarla.
2. Haga clic en **OK (Aceptar)** para guardar la configuración del portal.
3. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Personalización de las páginas de inicio de sesión, bienvenida y ayuda del portal de GlobalProtect

GlobalProtect proporciona páginas de inicio de sesión, bienvenida y ayuda predeterminadas. Sin embargo, puede crear sus propias páginas de personalización con su marca corporativa, políticas de uso aceptable y enlaces a sus recursos internos.

© 2020 Palo Alto Networks, Inc.

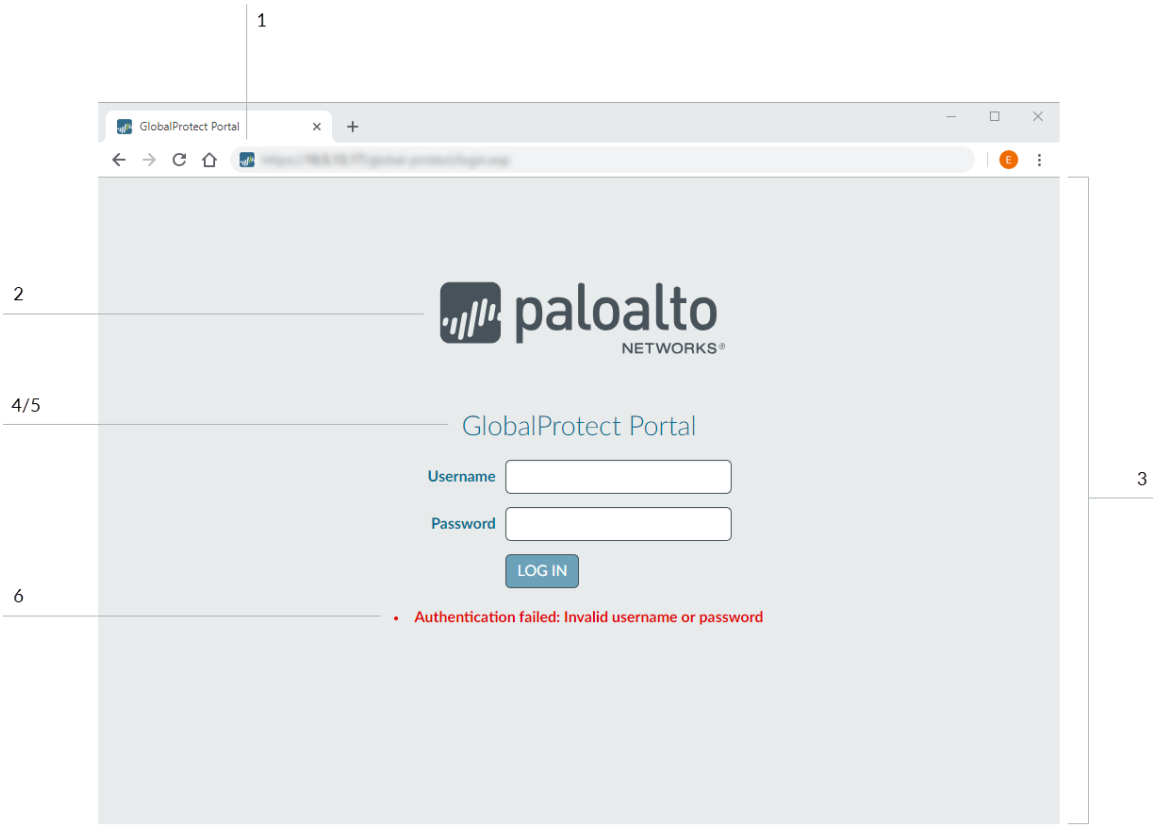
Como alternativa, puede deshabilitar el acceso del navegador a la página de inicio de sesión del portal para evitar los intentos no autorizados de autenticación en el portal de GlobalProtect (configure la opción Portal Login Page (Página de inicio de sesión del portal) > Disable (Deshabilitar) de Network (Red) > GlobalProtect > Portals (Portales) > <portal_config > General). Con la página de inicio de sesión del portal desactivada, puede usar una herramienta de distribución de software, como System Center Configuration Manager (SCCM) de Microsoft, para permitir que sus usuarios descarguen e instalen la aplicación de GlobalProtect.

STEP 1 | Exporte la página predeterminada de inicio de sesión, inicio, bienvenida o ayuda del portal.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el enlace para la página correspondiente del portal de GlobalProtect, como **GlobalProtect Portal Login Page (Página de inicio de sesión del portal de GlobalProtect)**.
3. Seleccione la página predefinida en **Default (Predeterminada)** y haga clic en **Export (Exportar)**.

STEP 2 | Edite la página exportada.

1. Use el editor de texto de HTML que prefiera para abrir y editar la página.
2. Para editar la página de inicio de sesión o de inicio, configure cualquiera de las siguientes variables:
   - **Página de inicio de sesión en el portal de GlobalProtect**:

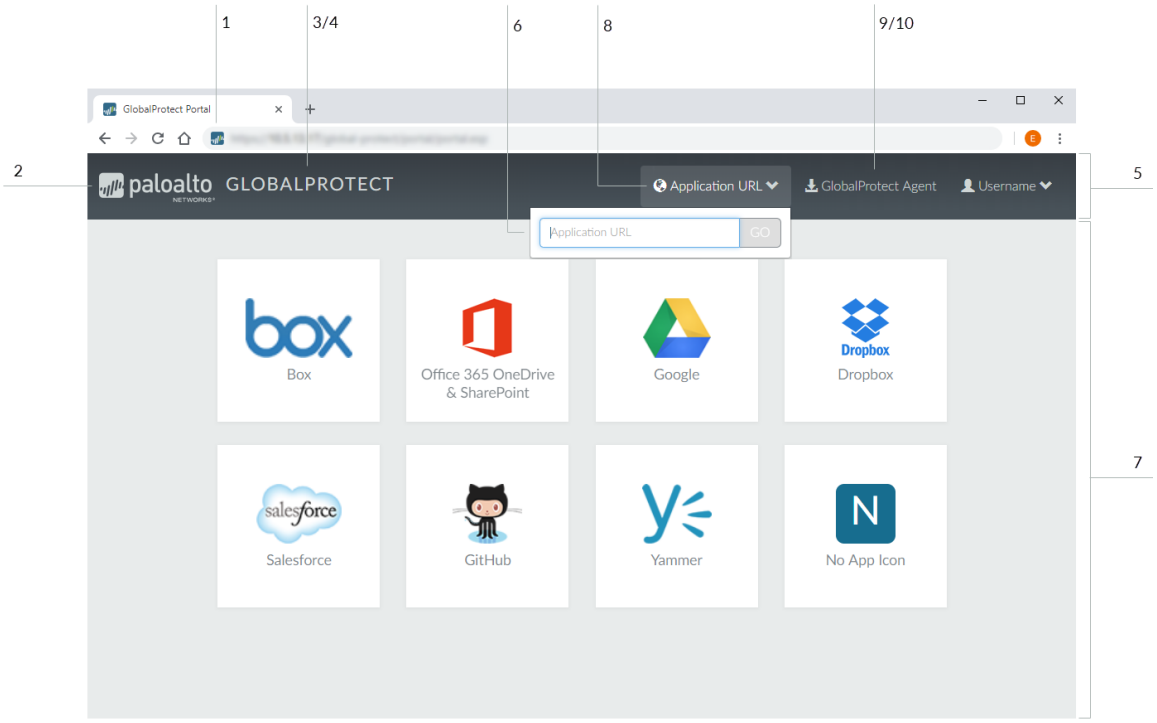


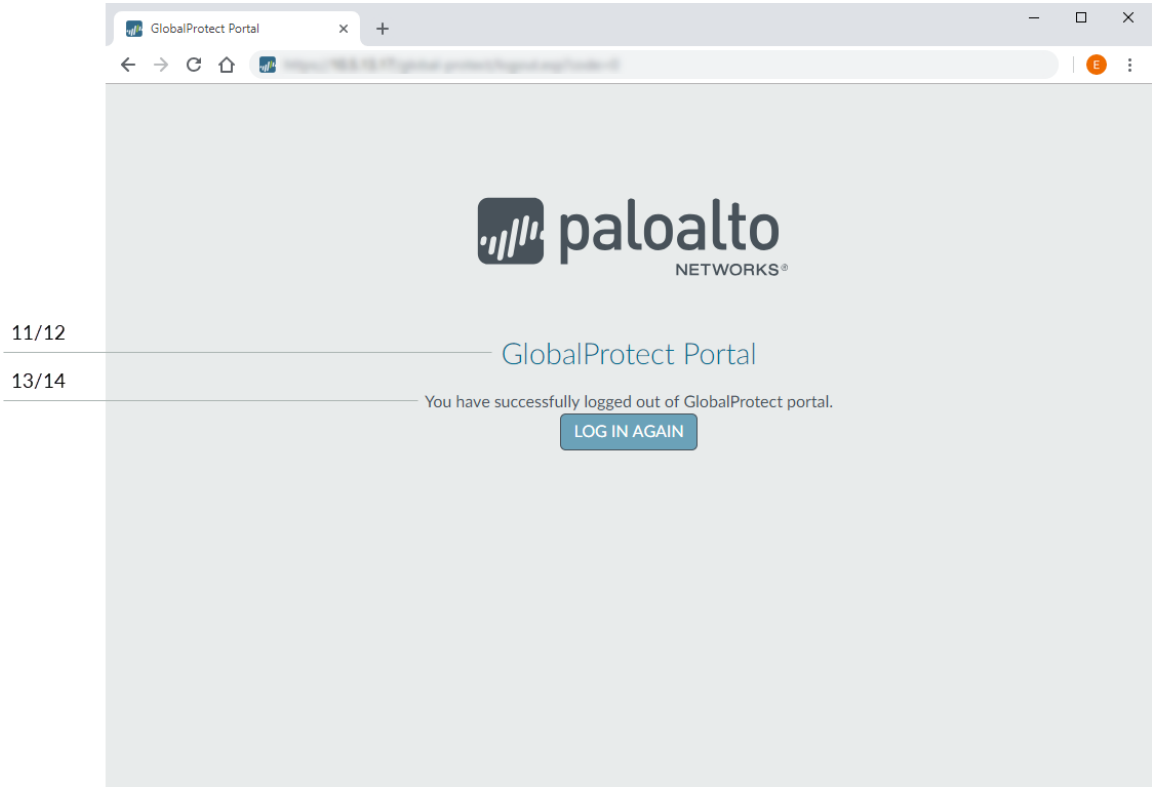
© 2020 Palo Alto Networks, Inc.

Número de etiqueta	Variable	Description (Descripción)	Ejemplo
1	`favicon`	URL del icono mostrado en la barra de direcciones del navegador web.	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	`logo`	URL del logotipo de la empresa.	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	`bg_color`	Color de fondo de la página de inicio de sesión.	`var bg_color = '#D3D3D3';`
4	`gp_portal_name`	Texto mostrado debajo del logotipo de la empresa.	`var gp_portal_name = 'GlobalProtect Portal';`
5	`gp_portal_name_color`	Color del texto mostrado debajo del logotipo de la empresa.	`var gp_portal_name_color = '#000000';`
6	`error_text_color`	Color del texto de los mensajes de error de inicio de sesión.	`var error_text_color = '#196390';`

- **Página de inicio del portal de GlobalProtect**:

© 2020 Palo Alto Networks, Inc.





© 2020 Palo Alto Networks, Inc.

Número de etiqueta	Variable	Description (Descripción)	Ejemplo
1	`favicon`	URL del icono mostrado en la barra de direcciones del navegador web.	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	`logo`	URL del logotipo de la empresa.	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	`navbar_text`	Texto de la barra de navegación.	`var navbar_text = 'GlobalProtect';`
4	`navbar_text_color`	Color del texto de la barra de navegación.	`var navbar_text_color = '#D3D3D3';`
5	`navbar_bg_color`	Color de fondo de la barra de navegación.	`var navbar_bg_color = '#A9A9A9';`
6	`dropdown_bg_color`	Color de fondo del menú desplegable.	`var dropdown_bg_color = '#FFFFFF';`
7	`bg_color`	Color de fondo de la página de inicio.	`var bg_color = '#D3D3D3';`
8	`label_custom_app_url`	Etiqueta de las URL de las aplicaciones personalizadas o internas.	`var label_custom_app_url = 'Application URL';`
9	`display_globalprotect_agent`	Opción para mostrar u ocultar el botón de descarga de aplicaciones de GlobalProtect: introduzca **1** para mostrarlo o **0** para ocultarlo.	`var display_globalprotect_agent = 1;`

© 2020 Palo Alto Networks, Inc.

Número de etiqueta	Variable	Description (Descripción)	Ejemplo
10	`label_globalprotect_agent`	Etiqueta del botón de descarga de aplicaciones de GlobalProtect.	`var label_globalprotect_agent = 'GlobalProtect Agent';`
11	`gp_portal_name`	Texto mostrado debajo del logotipo de la empresa en la página de cierre de sesión en el portal.	`var gp_portal_name = 'GlobalProtect Portal';`
12	`gp_portal_name_color`	Color del texto mostrado debajo del logotipo de la empresa en la página de cierre de sesión en el portal.	`var gp_portal_name_color = '#000000';`
13	`logout_text_array`	Mensajes mostrados en la página de cierre de sesión en el portal tras el cierre. *Solo puede modificar los mensajes existentes, pero no puede eliminar estos ni añadir nuevos.*	`var logout_text_array = ["You have successfully logged out of GlobalProtect portal.", "GlobalProtect Gateway is not licensed. Contact system administrator.", "User not authenticated to GlobalProtect portal.", "System error, contact system administrator.", "System error, failed to delete user session. Contact system administrator.", "Can not create user session. Max-capacity reached. Contact system administrator."];`
14	`logout_text_color`	Color del texto de los mensajes mostrados en la página de cierre de sesión en el portal tras el cierre.	`var logout_text_color = '#000000';`

© 2020 Palo Alto Networks, Inc.

3. Guarde la imagen editada con un nuevo nombre de archivo. Asegúrese de que la página conserva su codificación UTF-8.

STEP 3 | Importe las nuevas páginas.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el enlace para la página correspondiente del portal de GlobalProtect.
3. Haga clic en **Import (Importar)** para importar la nueva página del portal. Introduzca la ruta y el nombre de archivo en el campo **Import File (Importar archivo)** o **Browse (Examinar)** para encontrar y seleccionar el archivo.
4. (Opcional) Seleccione el sistema virtual en el que se usará esta página en la lista desplegable **Destination (Destino)** o seleccione **Shared (Compartido)** (valor por defecto) para que esté disponible para todos los sistemas virtuales.
5. Haga clic en **OK (Aceptar)** para importar el archivo.

STEP 4 | Configure el portal para utilizar las nuevas páginas.

- **Portal Login Page (Página de inicio de sesión en portal)**, **Portal Landing Page (Página de destino de portal)** y **App Help Page (Página de ayuda de aplicaciones)**:
  1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
  2. Seleccione el portal al que desea añadir la página de inicio de sesión, de destino (inicio) o de ayuda para las aplicaciones.
  3. En el área Appearance (Apariencia) de la pestaña **General**, seleccione la página nueva en la lista desplegable relevante.
- **Custom Welcome Page (Página de bienvenida personalizada)**:
  1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
  2. Seleccione el portal al que desea añadir la página de bienvenida.
  3. En la pestaña **Agent**, seleccione la configuración de agente a la cual desea añadir la página de bienvenida.
  4. En la pestaña **App (Aplicación)**, seleccione la página nueva en el menú desplegable **Welcome Page (Página de bienvenida)**.
  5. Haga clic en **OK** para guardar la configuración de agente.

STEP 5 | Guarde la configuración del portal.

Haga clic en **OK (Aceptar)** para guardar la configuración del portal y, a continuación, haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 6 | Compruebe si se muestra la nueva página.

- **Pruebe la página de inicio de sesión**: abra un navegador web y vaya a la URL de su portal (no añada el número de puerto :4443 al final de la URL o será redirigido a la interfaz web para el cortafuegos). Por ejemplo, introduzca `https://myportal` en lugar de `https://myportal:4443`. Aparecerá la nueva página de inicio de sesión del portal.
- **Pruebe la página de inicio**: abra un navegador web y vaya a la URL del portal; no añada el número de puerto :4443 al final de la URL o se redirige a la interfaz web del cortafuegos. Por ejemplo, introduzca `https://myportal` en lugar de `https://myportal:4443`. Introduzca sus credenciales en **Username (Nombre de usuario)** y en **Password (Contraseña)** y, luego, haga clic en **LOG IN (INICIAR SESIÓN)** para entrar en el portal. Aparece la nueva página de inicio del portal.
- **Pruebe la página de ayuda**: haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la aplicación de GlobalProtect. Cuando el panel de estado se abra, haga clic en el icono de configuración ( ) para abrir el menú de configuración. Seleccione **Help (Ayuda)** para ver la página de ayuda nueva.

© 2020 Palo Alto Networks, Inc.

- **Pruebe la página de bienvenida**: haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la aplicación de GlobalProtect. Cuando el panel de estado se abra, haga clic en el icono de configuración (⚙) para abrir el menú de configuración. Seleccione **Welcome Page (Página de bienvenida)** para ver la página de bienvenida nueva.

© 2020 Palo Alto Networks, Inc.

Aplicaciones de GlobalProtect

- Descarga de la aplicación de GlobalProtect
- Implementación del software de la aplicación de GlobalProtect
- Definición de las configuraciones de agente de GlobalProtect
- Personalización de la aplicación de GlobalProtect
- Implementación de la configuración del agente de forma transparente

© 2020 Palo Alto Networks, Inc.

Implementación de la aplicación de GlobalProtect para usuarios finales

Para poder conectarse a GlobalProtect™, un endpoint debe ejecutar la aplicación de GlobalProtect. El método de implementación del software depende del tipo de endpoint de la siguiente forma:

Zero Trust	Opciones de implementación
Endpoints de macOS y Windows	Existen varias opciones que puede usar para distribuir e instalar el software en los endpoints de macOS y Windows: • **Directamente desde el portal**: descargue el software de la aplicación en el cortafuegos que aloja el portal y actívelo para que los usuarios finales puedan instalar las actualizaciones cuando se conecten al portal. Esta opción proporciona una flexibilidad que le permitirá controlar el modo y el momento en el que los usuarios finales recibirán actualizaciones basadas en la configuración del agente que definió para cada usuario, grupo o sistema operativo. Sin embargo, si dispone de un gran número de aplicaciones que necesitan actualizaciones, puede que aumente la carga de su portal. Consulte Alojamiento de actualizaciones de la aplicación en el portal para obtener instrucciones. • **Desde un servidor web**: si tiene un gran número de endpoints que necesiten actualizar la aplicación de forma simultánea, considere alojar las actualizaciones de la aplicación en un servidor web para reducir la carga del cortafuegos. Consulte Alojamiento de actualizaciones de la aplicación en un servidor web para obtener instrucciones. • **De forma transparente desde la línea de comandos**: para los endpoints de Windows, puede implementar la configuración de la aplicación automáticamente en el instalador de Windows (Msiexec). Sin embargo, para actualizar a una versión de la aplicación posterior utilizando MSIEXEC, primero debe desinstalar la aplicación existente. Además, Msiexec permite la implementación de la configuración de la aplicación directamente en los endpoints mediante el ajuste de los valores en el registro de Windows. De manera similar, también puede implementar la configuración de la aplicación a los endpoints de macOS ajustando la configuración en la plist de macOS. Consulte Implementación de la configuración de la aplicación de forma transparente. • **Con reglas de políticas de grupo**: en entornos Active Directory, la aplicación de GlobalProtect también se puede distribuir a usuarios finales mediante una política de grupo de Active Directory. Las políticas de grupo AD permiten la modificación automatizada del software y la configuración de endpoints de Windows. Consulte el artículo en http://support.microsoft.com/kb/816102 para obtener más información sobre cómo utilizar la política de grupo para distribuir automáticamente programas en endpoints o usuarios. • **Desde un sistema de gestión de endpoint móvil**: si utiliza un sistema de gestión móvil, como un MDM o EMM, para gestionar sus endpoints móviles, puede usar el sistema para implementar y configurar la aplicación de GlobalProtect. Consulte Gestión de endpoints móviles.

© 2020 Palo Alto Networks, Inc.

Zero Trust	Opciones de implementación
Teléfono Windows 10 y Windows 10 UWP	• **Desde un sistema de gestión de endpoint móvil**: si utiliza un sistema de gestión móvil, como un MDM o EMM, que admita endpoints de Windows 10, puede usar el sistema para implementar y configurar la aplicación de GlobalProtect. Consulte Gestión de endpoints móviles. • **Desde Microft Store**: el usuario final también puede descargar e instalar la aplicación de GlobalProtect directamente desde Microsoft Store. Para obtener instrucciones sobre cómo descargar y probar la instalación de la aplicación de GlobalProtect, consulte Descarga e instalación de la aplicación móvil de GlobalProtect.
Endpoints iOS y Android	• **Desde un sistema de gestión de endpoint móvil**: si utiliza un sistema de gestión móvil, como un MDM o EMM, puede usar el sistema para implementar y configurar la aplicación de GlobalProtect. Consulte Gestión de endpoints móviles. • **Desde una tienda de aplicaciones**: el usuario final puede descargar e instalar la aplicación de GlobalProtect directamente desde la App Store de Apple (endpoints iOS) o desde Google Play (endpoints Android). Para obtener instrucciones sobre cómo descargar y probar la instalación de la aplicación de GlobalProtect, consulte Descarga e instalación de la aplicación móvil de GlobalProtect.
Chromebooks	• **Desde la consola de administración de Google**: la consola de gestión de Google le posibilita gestionar los ajustes y aplicaciones de Chromebook desde una ubicación central basada en la Web. Para implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google, consulte Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google. *La aplicación de GlobalProtect para Android solo se admite en algunos Chromebooks. En los Chromebooks que no admiten aplicaciones para Android, debe seguir ejecutando la aplicación de GlobalProtect para Chrome, que no es compatible a partir de la aplicación de GlobalProtect 5.0 y posterior.* • **Desde AirWatch**: puede implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados que están inscritos con AirWatch. Después de implementar la aplicación, configure e implemente un perfil VPN para configurar la aplicación de GlobalProtect para los usuarios finales de forma automática. Para implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados con AirWatch, consulte Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con AirWatch.
Linux	Luego de descargar la aplicación de GlobalProtect para Linux desde el sitio de soporte, puede distribuir e instalar la aplicación: • **Con las herramientas de distribución de aplicación de Linux**: la distribución de aplicaciones de Linux generalmente se gestiona con herramientas externas (como Chef y Puppet) o mediante un repositorio local para el sistema operativo Linux (por ejemplo, repositorios Ubuntu y repositorios RHEL). Consulte la documentación del sistema operativo Linux para obtener más información.

© 2020 Palo Alto Networks, Inc.

Zero Trust	Opciones de implementación
	• **Instalación manual**: si pone a disposición el software de sus usuarios finales, pueden instalarlo manualmente con las herramientas de Linux como **`apt`** o **`dpkg`**. Para obtener instrucciones sobre cómo instalar la aplicación de GlobalProtect para Linux, consulte la Guía de usuario de la aplicación de GlobalProtect.

Como método alternativo a la implementación de la aplicación de GlobalProtect, puede configurar el portal de GlobalProtect para proporcionar acceso remoto seguro a aplicaciones web empresariales comunes que utilizan tecnologías HTML, HTML5 y Javascript. Los usuarios tienen la ventaja de contar con el acceso seguro de los navegadores web con SSL sin instalar el software de la aplicación de GlobalProtect. Consulte VPN sin cliente de GlobalProtect.

Descarga de la aplicación de GlobalProtect

Los usuarios finales se deben poner en contacto con el administrador de TI para obtener el último software de GlobalProtect admitido.

Antes de suministrar la aplicación de GlobalProtect a los usuarios finales, debe cargar su nuevo paquete de instalación en el cortafuegos que aloja el portal y, luego, activar el software para permitir su descarga a las aplicaciones que se conectan al portal. Este método de implementación es válido con todas las versiones de la aplicación que no están destinadas a dispositivos móviles. Si desea descargar la versión móvil de la aplicación de GlobalProtect, visite la tienda de aplicaciones para dichos dispositivos; para obtener más información, consulte Descarga e instalación de la aplicación móvil de GlobalProtect.

Para descargar la última aplicación directamente del cortafuegos, este debe tener una ruta de servicio que le permita acceder al servidor de actualizaciones de Palo Alto Networks (consulte Implementación de la aplicación de GlobalProtect para usuarios finales). Si el cortafuegos no tiene acceso a internet, use un ordenador conectado a internet para descargar el paquete de software de la página de actualizaciones de software del sitio del servicio de asistencia de Palo Alto Networks. Luego, cárguelo manualmente en el cortafuegos.

Para descargar manualmente el paquete de software de la aplicación:

STEP 1 | Inicie sesión en el portal de atención al cliente de Palo Alto Networks (https://support.paloaltonetworks.com/).

Debe tener una cuenta válida de Palo Alto Networks para iniciar sesión y descargar software de la página de actualizaciones de software. Si no puede iniciar sesión y necesita asistencia, ingrese en https://www.paloaltonetworks.com/support/tabs/overview.html.

STEP 2 | Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.

STEP 3 | Seleccione la versión de la aplicación de GlobalProtect oportuna según el sistema operativo.

STEP 4 | Lea las notas de la versión y, a continuación, haga clic en el enlace para realizar la descarga.

STEP 5 | Implementación de la aplicación de GlobalProtect para usuarios finales.

Consulte la Matriz de compatibilidad de Palo Alto Networks para conocer los sistemas operativos en los que puede instalar cada versión de la aplicación de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Alojamiento de actualizaciones de la aplicación en el portal

La manera más sencilla de implementar el software de la aplicación de GlobalProtect es descargar el paquete de instalación de la nueva aplicación en el cortafuegos que aloja su portal y, a continuación, activar el software para descargar las aplicaciones que se conectan al portal. Para hacerlo de forma automática, el cortafuegos debe tener una ruta de servicio que le permita acceder a Actualizar servidor de Palo Alto Networks. Si el cortafuegos no tiene acceso a internet, consulte Descarga de la aplicación de GlobalProtect y use un ordenador conectado a internet para descargar el paquete de software de la página de actualizaciones de software del sitio del servicio de asistencia de Palo Alto Networks. Luego, cárguelo manualmente en el cortafuegos.

Usted define el modo en que las actualizaciones del software de la aplicación se implementan en las configuraciones de agente del portal: si se producen automáticamente cuando la aplicación se conecta al portal, si se indica al usuario que actualice la aplicación o si el usuario final puede comprobar y descargar de forma manual una nueva versión de la aplicación. Para obtener detalles sobre la configuración de un agente, consulte Definición de las configuraciones del agente de GlobalProtect.

STEP 1 | En el cortafuegos que aloja el portal de GlobalProtect, busque nuevas imágenes de software de la aplicación.

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)** para ver la lista de imágenes de software de la aplicación disponibles.

- Si el cortafuegos tiene acceso a Update Server (Servidor de actualización), haga clic en **Check Now (Comprobar ahora)** para comprobar si hay actualizaciones recientes. Si el valor de la columna **Action (Acción)** es **Download (Descargar)**, indica que hay una versión nueva de la aplicación disponible.
- Si el cortafuegos no tiene acceso a Update Server (Servidor de actualización), debe descargar la imagen de software desde el sitio de asistencia de actualizaciones de software de Palo Alto Networks, como se describe en el paso 2.

STEP 2 | Descargue la imagen de software de la aplicación.

- Si el cortafuegos tiene acceso a Update Server (Servidor de actualización), localice la versión de la aplicación que desea y haga clic en **Download (Descargar)**. Cuando se complete la descarga del agente, el valor en la columna **Action (Acción)** cambia a **Activate (Activar)**.
- Si el cortafuegos no tiene acceso al servidor de actualizaciones, siga el procedimiento Descarga de la aplicación de GlobalProtect. Luego de descargar la imagen de software, vuelva a la página **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect) del cortafuegos** para cargarla mediante la opción **Upload (Cargar)**.

STEP 3 | Active la imagen de software de la aplicación para que los usuarios finales puedan descargarla desde el portal.

Solo se puede activar una imagen del software de la aplicación a la vez. Si activa una nueva versión, pero tiene algunas aplicaciones que requieren una versión previamente activada, debe activar la versión requerida de nuevo para habilitar la descarga.

- Si la imagen de software se descargó automáticamente desde Update Server (Servidor de actualización), haga clic en **Activate (Activar)**.
- Si cargó manualmente la imagen de software en el cortafuegos, haga clic en **Activate From File (Activar desde archivo)** y, a continuación, seleccione el **GlobalProtect Client File (Archivo de cliente de GlobalProtect)** que cargó desde el menú desplegable. Haga clic en **OK (Aceptar)** para activar la imagen seleccionada. Puede que tenga que actualizar la página para que la versión muestre **Currently Activated (Activado actualmente)**.

© 2020 Palo Alto Networks, Inc.

Alojamiento de actualizaciones de la aplicación en un servidor web

Si un gran número de endpoints debe instalar o actualizar el software de la aplicación de GlobalProtect, considere alojar las imágenes del software de la aplicación de GlobalProtect en un servidor web externo. Así se reducirá la carga en el cortafuegos cuando los usuarios se conecten y descarguen la aplicación.

STEP 1 | Descargue y active la versión de la aplicación de GlobalProtect que pretende alojar en el servidor web para el cortafuegos.

Siga los pasos para descargar y activar el software de la aplicación en el cortafuegos, tal y como se describe en Alojamiento de actualizaciones de la aplicación en el portal.

STEP 2 | Descargue la imagen de la aplicación de GlobalProtect que quiere alojar en su servidor web.

Descargue la misma imagen que activó en el portal.

En un navegador web, realice el procedimiento Descarga de la aplicación de GlobalProtect.

STEP 3 | Publique los archivos de imagen de software en su servidor web.

STEP 4 | Redirija a los usuarios finales al servidor web.

En el cortafuegos que aloja el portal, introduzca los siguientes comandos de la CLI en el modo operativo:

```
> set global-protect redirect on
> set global-protect redirect location <path>
```

donde <*path*> es la ruta en la URL a la carpeta donde se aloja la imagen (por ejemplo, **`https://acme/GP`**).

STEP 5 | Compruebe la redirección.

1. En un navegador web, vaya a la siguiente URL:

   ```
   https://<portal address or name>
   ```

   Por ejemplo, **`https://gp.acme.com`**.
2. En la página de inicio de sesión del portal, introduzca su nombre de usuario en **Name (Nombre)** y la contraseña en **Password (Contraseña)** y, a continuación, haga clic en **Login (Iniciar sesión)**. Tras iniciar sesión correctamente, el portal debería redirigirlo a la descarga.

Comprobación de la instalación de la aplicación

Utilice el siguiente procedimiento para probar la instalación de la aplicación de GlobalProtect.

STEP 1 | Cree una configuración de agente para comprobar la instalación de la aplicación.

Cuando instale inicialmente el software de la aplicación de GlobalProtect en el endpoint, el usuario final debe haber iniciado la sesión en el sistema con una cuenta con privilegios administrativos. Las siguientes actualizaciones de software de la aplicación no necesitan privilegios administrativos.

© 2020 Palo Alto Networks, Inc.

Se recomienda crear una configuración de agente limitada a un grupo reducido de usuarios como, por ejemplo, administradores del departamento de TI responsables de la administración del cortafuegos:

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione una configuración de portal existente que desee modificar o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Agent (Agente)**, seleccione una configuración existente o haga clic en **Add (Añadir)** para añadir una que se implemente en usuarios/grupo de prueba.
4. En la pestaña **User/User Group (Usuario/grupo de usuarios)**, haga clic en **Add (Añadir)** para añadir el **User/User Group (Usuario/grupo de usuarios)** que probará la aplicación.
5. En la pestaña **App (Aplicación)**, configure **Allow User to Upgrade GlobalProtect App (Permitir al usuario actualizar la aplicación de GlobalProtect)** en **Allow with Prompt (Permitir con solicitud)**. Haga clic en **OK (Aceptar)** para guardar la configuración.
6. (Opcional) En la pestaña **Agent (Agente)**, seleccione la configuración de agente que acaba de crear o modificar y haga clic en **Move up (Mover hacia arriba)** para que quede más arriba de la lista que cualquier configuración más genérica que haya creado.

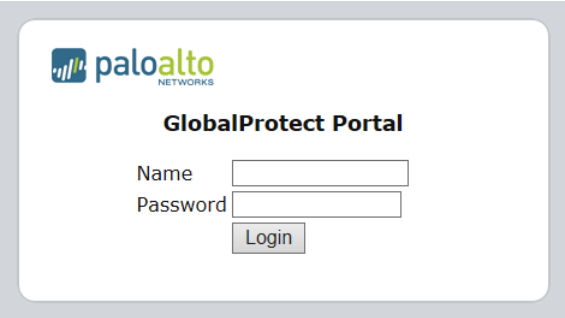
   Cuando una aplicación de GlobalProtect se conecta, el portal compara la información de origen en el paquete con las configuraciones de agente que definió. Como con la evaluación de la regla de seguridad, el portal busca una coincidencia empezando por la parte superior de la lista. Cuando encuentra una coincidencia, brinda la configuración correspondiente a la aplicación.
7. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 2 | Inicie sesión en el portal de GlobalProtect.

1. Inicie su navegador web y vaya a la siguiente URL:

```
https://<portal address or name>
```

   Por ejemplo, `https://gp.acme.com`.
2. En la página de inicio de sesión del portal, introduzca su nombre de usuario en **Name (Nombre)** y la contraseña en **Password (Contraseña)** y, a continuación, haga clic en **Login (Iniciar sesión)**.

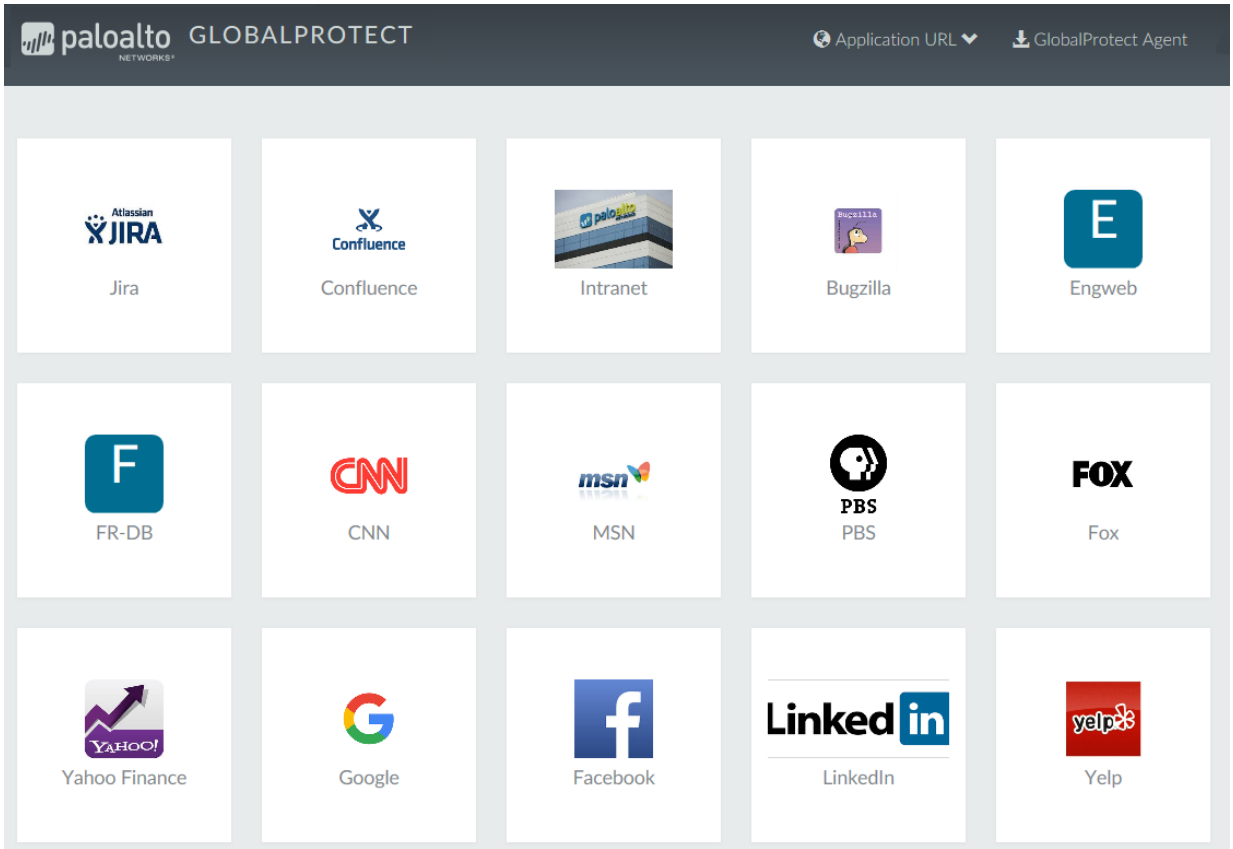


STEP 3 | Vaya a la página de descarga de la aplicación.

En la mayoría de los casos, la página de descarga de la aplicación aparece inmediatamente después de que inicia sesión en el portal. Use esta página para descargar el paquete de software de la aplicación más reciente.

© 2020 Palo Alto Networks, Inc.

Si ha habilitado el acceso VPN sin cliente de GlobalProtect, se abre una página de aplicaciones (en lugar de la página de descarga del agente) cuando inicia sesión en el portal. Seleccione **GlobalProtect Agent (Agente de GlobalProtect)** para abrir la página de descarga.



STEP 4 | Descargue la aplicación.

1. Para comenzar la descarga, haga clic en el enlace que corresponde al sistema operativo que ejecuta su ordenador.

© 2020 Palo Alto Networks, Inc.

2. Abra el archivo de instalación del software.
3. Cuando se le solicite ejecutar o guardar el software, haga clic en **Run (Ejecutar)**.
4. Cuando se le solicite, haga clic en **Run (Ejecutar)** para iniciar el Asistente de configuración de GlobalProtect.

Cuando instale inicialmente el software de la aplicación de GlobalProtect en el endpoint, el usuario final debe haber iniciado la sesión en el sistema con una cuenta con privilegios administrativos. Las siguientes actualizaciones de software de la aplicación no necesitan privilegios administrativos.

STEP 5 | Complete la configuración de la aplicación de GlobalProtect.

1. En el Asistente de configuración de GlobalProtect, haga clic en **Next (Siguiente)**.
2. Haga clic en **Next (Siguiente)** para aceptar la carpeta de instalación por defecto (`C:\Program Files\Palo Alto Networks\GlobalProtect`) o seleccione **Browse (Examinar)** para elegir una nueva ubicación y, luego, haga clic en **Next (Siguiente)** dos veces.
3. Luego de completar la instalación, haga clic en **Close (Cerrar)** para cerrar el asistente.

STEP 6 | Inicie sesión en GlobalProtect.

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. Introduzca la dirección FQDN o dirección IP del portal y luego haga clic en **Connect (Conectar)**.
3. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, seleccione la puerta de enlace desde el menú desplegable **Gateway (Puerta de enlace)** (solo para puertas de enlace externas).

Esta opción solo está disponible si habilita la selección de puertas de enlace manuales.

© 2020 Palo Alto Networks, Inc.

4. (Opcional) Dependiendo del modo de conexión, haga clic en **Connect (Conectarse)** para iniciar la conexión.
5. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y haga clic en **Sign In (Iniciar sesión)**.

Si la autenticación se realiza correctamente, usted está conectado a su red corporativa y el panel de estado muestra el estado **Connected (Conectado)** o **Connected - Internal (Conectado: interno)**. Si configuró una página de bienvenida, esta se muestra luego de que inicia sesión correctamente.

Descarga e instalación de la aplicación móvil de GlobalProtect

La aplicación de GlobalProtect proporciona una forma sencilla de extender las políticas de seguridad de la empresa a los endpoints móviles. Al igual que con otros endpoints remotos que ejecutan la aplicación de GlobalProtect, la aplicación móvil brinda acceso seguro a su red corporativa por un túnel VPN SSL o IPsec. La aplicación se conecta automáticamente a la puerta de enlace que está más cerca de la ubicación actual del usuario final. Además, el tráfico desde y hacia el endpoint está automáticamente sujeto al cumplimiento de la misma política de seguridad que otros hosts en su red corporativa. La aplicación móvil también recopila información sobre la configuración del host y puede usarla para mejorar el cumplimiento de la política de seguridad basada en HIP.

Existen dos métodos principales para instalar la aplicación de GlobalProtect: Puede implementar la aplicación desde su sistema MDM de terceros y enviar de forma transparente la aplicación a sus endpoints gestionados; o bien, puede instalar la aplicación directamente desde la tienda oficial de su endpoint:

- Endpoints de iOS: App Store
- Endpoints de Android y Chromebooks: Google Play

  A partir de la aplicación de GlobalProtect 5.0, la aplicación de GlobalProtect para Chrome OS no es compatible; utilice la aplicación de GlobalProtect para Android en su lugar.
- Teléfono Windows 10 y endpoints Windows 10 UWP: Microsoft Store

Este flujo de trabajo describe cómo instalar la aplicación de GlobalProtect directamente en el endpoint móvil. Para obtener instrucciones sobre cómo implementar la aplicación GlobalProtect desde AirWatch, consulte Implementación de la aplicación móvil de GlobalProtect con AirWatch.

STEP 1 | Cree una configuración de agente para comprobar la instalación de la aplicación.

Se recomienda crear una configuración de agente limitada a un grupo reducido de usuarios como, por ejemplo, administradores del departamento de TI responsables de la administración del cortafuegos:

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione una configuración de portal existente para modificar o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Agent (Agente)**, seleccione una configuración existente o haga clic en **Add (Añadir)** para añadir una nueva configuración que se implementará en usuarios/grupo de prueba.
4. En la pestaña **User/User Group (Usuario/grupo de usuarios)**, haga clic en **Add (Añadir)** para añadir el **User/User Group (Usuario/grupo de usuarios)** que probará la aplicación.
5. Seleccione el **OS (Sistema operativo)** para la aplicación que está probando (**iOS**, **Android** o **WindowsUWP**).
6. (Opcional) Seleccione la configuración de agente que acaba de crear/modificar y haga clic en **Move up (Mover hacia arriba)** para que quede más arriba de la lista que cualquier configuración más genérica que haya creado.
7. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

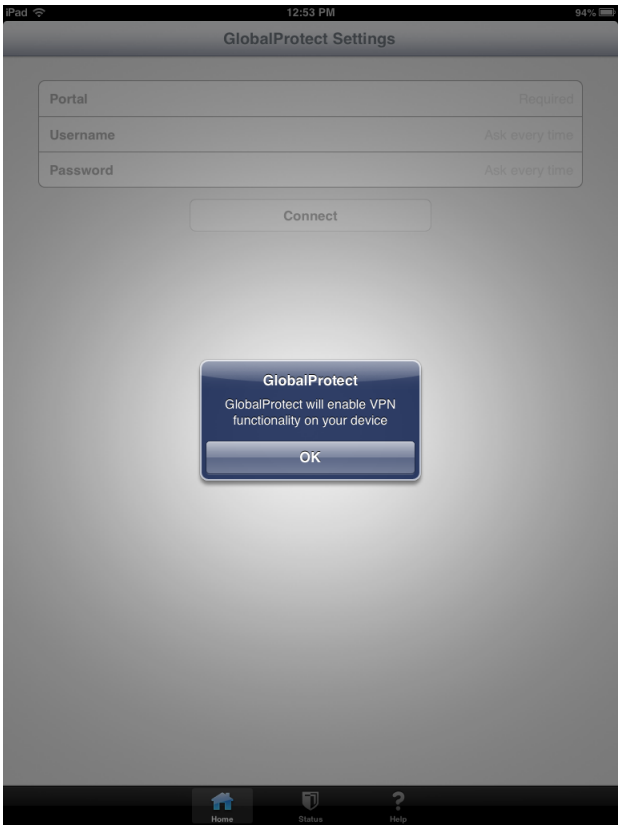
STEP 2 | Desde el endpoint, siga las indicaciones para descargar e instalar la aplicación.

© 2020 Palo Alto Networks, Inc.

- En endpoints Android, busque la aplicación en Google Play.
- En endpoints iOS, busque la aplicación en App Store.
- En endpoints de Windows 10 UWP, busque la aplicación en Microsoft Store.

STEP 3 | Inicie la aplicación.

Cuando se haya instalado correctamente, el icono de la aplicación de GlobalProtect aparecerá en la pantalla de inicio del endpoint. Para iniciar la aplicación, pulse el icono. Cuando aparezca el mensaje para habilitar la funcionalidad VPN de GlobalProtect, pulse **OK**.



STEP 4 | Conecte con el portal.

1. Cuando se le solicite, introduzca el nombre o dirección del **Portal**, el **Username (Nombre de usuario)** y la **Password (Contraseña)**. El nombre del portal debe ser un FQDN y no debe incluir https:// al principio.

© 2020 Palo Alto Networks, Inc.

2. Pulse **Connect (Conectar)** y compruebe que la aplicación establezca correctamente una conexión a GlobalProtect.

   Si el sistema de gestión de endpoints móviles externo está configurado, la aplicación le pedirá que se inscriba.

© 2020 Palo Alto Networks, Inc.

Implementación de la configuración de la aplicación de forma trasparente

Como alternativa a la implementación de los ajustes de la aplicación desde la configuración del portal, puede definirlos directamente desde el registro de Windows, archivo plist global de macOS o, solo en endpoints de Windows, con el instalador de Windows (Msiexec). La ventaja es que permite la implementación de la configuración de la aplicación de GlobalProtect en los endpoints antes de su primera conexión al portal de GlobalProtect.

Los ajustes definidos en la configuración del portal de GlobalProtect siempre tienen prioridad sobre los ajustes definidos en el registro de Windows o la plist de macOS. Si define ajustes en el registro o la plist, pero la configuración del portal especifica otros ajustes, los ajustes que recibe la aplicación del portal cancelarán los ajustes definidos en el endpoint. Esta cancelación también incluirá ajustes relacionados con el inicio de sesión, como la conexión a demanda, la utilización del inicio de sesión único (single sign-on, SSO) y la conexión de la aplicación en caso de que el certificado del portal no sea válido. Por lo tanto, debe evitar ajustes que estén en conflicto. Además, la configuración del portal se almacena en la caché del endpoint. Esta configuración en caché se utilizará si la aplicación de GlobalProtect o el endpoint se reinician.

En las siguientes secciones, se describen los ajustes personalizables de la aplicación que están disponibles y cómo implementar esos ajustes de forma transparente en los endpoints de Windows y macOS:

- Ajustes personalizables de la aplicación
- Implementación de los ajustes de la aplicación para los endpoints de Windows
- Implementación de los ajustes de la aplicación para los endpoints de macOS

Además de usar el registro de Windows y la plist de macOS para implementar los ajustes de la aplicación de GlobalProtect, puede activar la aplicación de GlobalProtect para recopilar la información específica del registro de Windows y la plist de macOS de los endpoints, incluidos los datos sobre las aplicaciones instaladas en los endpoints, los procesos que se ejecutan en los endpoints y los atributos o propiedades de esas aplicaciones y procesos. A continuación, puede supervisar los datos y añadirlos a una regla de seguridad como criterios de coincidencia. El tráfico del endpoint que coincida con ciertos ajustes de registro que haya definido puede ponerse en vigor de acuerdo con la regla de seguridad. Además, puede configurar comprobaciones personalizadas para recopilar datos de procesos y aplicaciones de endpoints*.*

Ajustes personalizables de la aplicación

Además de implementar previamente la dirección del portal, también puede definir los ajustes de la aplicación. Para implementar los ajustes de la aplicación en los endpoints de Windows, usted define claves en el registro de Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`). Para implementar los ajustes de la aplicación en los endpoints de macOS, usted define entradas en el diccionario `PanSetup` de la plist de macOS (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`). Únicamente en los endpoints de Windows, también puede usar el instalador de Windows para implementar ajustes de la aplicación desde Msiexec.

Los siguientes temas describen cada ajuste personalizable de la aplicación. Los ajustes definidos en la configuración de agente del portal de GlobalProtect tienen prioridad sobre los ajustes definidos en el registro de Windows o la plist de macOS.

Algunos ajustes no tienen una configuración de portal correspondiente en la interfaz web y deben configurarse con el registro de Windows o Msiexec. Estas configuraciones

© 2020 Palo Alto Networks, Inc.

adicionales incluyen: `can-prompt-user-credential`, `wrap-cp-guid` y `filter-non-gpcp`.

- Opciones de visualización de la aplicación
- Opciones de comportamiento del usuario
- Opciones de comportamiento de la aplicación
- Opciones de implementación de secuencias de comandos

Opciones de visualización de la aplicación

La siguiente tabla detalla las opciones que puede configurar en el registro de Windows y la plist de macOS para personalizar la visualización de la aplicación de GlobalProtect.

Table 3: Tabla: Ajustes personalizables de la aplicación

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Enable Advanced View (Habilitar vista avanzada)	`enable-advanced-view yes | no`	`ENABLEADVANCEDVIEW="yes | no"`	`yes`
Display GlobalProtect Icon (Mostrar icono GlobalProtect)	`show-agent-icon yes | no`	`SHOWAGENTICON="yes|no"`	`yes`
Enable Rediscover Network Option (Habilitar la opción de redescubrir red)	`rediscover-network yes | no`	`REDISCOVERNETWORK="yes | no"`	`yes`
Enable Resubmit Host Profile Option (Habilitar la opción Reenviar perfil de host)	`resubmit-host-info yes | no`	`RESUBMITHOSTINFO="yes | no"`	`yes`
Show System Tray Notifications (Mostrar notificaciones en la bandeja del sistema)	`show-system-tray-notifications yes | no`	`SHOWSYSTEMTRAYNOTIFICATIONS="yes | no"`	`yes`

Opciones de comportamiento del usuario

La siguiente tabla detalla las opciones que puede configurar en el registro de Windows y la plist de macOS para personalizar cómo interactúa el usuario con la aplicación de GlobalProtect.

Table 4: Tabla: Opciones personalizables de comportamiento del usuario

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Allow User to Change Portal	`can-change-portal yes | no`	`CANCHANGEPORTAL="yes | no"`	`yes`

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Address (Permitir al usuario cambiar la dirección del portal)			
Allow User to Dismiss Welcome Page (Permitir al usuario descartar la página de bienvenida)	`enable-hide-welcome-page yes | no`	`ENABLEHIDEWELCOMEPAGE= ”yes | no”`	`yes`
Allow User to Continue with Invalid Portal Server Certificate (Permitir al usuario continuar con certificado no válido de portal)	`can-continue-if-portal-cert-invalid yes | no`	`CANCONTINUEIFPORTALCERT INVALID= ”yes | no”`	`yes`
Allow User to Disable GlobalProtect App (Permitir al usuario desactivar la aplicación de GlobalProtect)	`disable-allowed yes | no`	`DISABLEALLOWED="yes | no"`	`no`
Save User Credentials (Guardar credenciales de usuario) Especifique un 0 para que GlobalProtect no guarde las credenciales, 1 para guardar el nombre de usuario y la contraseña, o 2 para guardar solo el nombre de usuario.	`save-user-credentials 0 | 1 | 2`	`SAVEUSERCREDENTIALS 0 | 1 | 2`	n/c
Not in portal (No en el portal) La opción **Allow user to save password**	`can-save-password yes | no`	`CANSAVEPASSWORD=”yes | no”`	`yes`

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
(Permitir al usuario guardar la contraseña) es obsoleta en la interfaz web de PAN-OS 7.1 y versiones posteriores pero se puede configurar desde el registro de Windows o la plist de macOS. Todo valor especificado en el campo **Save User Credentials (Guardar credenciales del usuario)** sobrescribe el valor que se especifique aquí.			
Solo Windows/No en portal Con este ajuste, el proveedor de credenciales de GlobalProtect puede mostrar el botón **Start GlobalProtect Connection (Iniciar conexión de GlobalProtect)**, que permite a los usuarios iniciar manualmente la conexión anterior al inicio de sesión de GlobalProtect.	**`ShowPrelogonButton yes | no`**	n/c	**`no`**

Opciones de comportamiento de la aplicación

La siguiente tabla detalla las opciones que puede configurar en el registro de Windows y la plist de macOS para personalizar el comportamiento de la aplicación de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Table 5: Tabla: Opciones personalizables de comportamiento de la aplicación

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Connect Method (Método de conexión)	`connect-method on-demand | pre-logon | user-logon`	`CONNECTMETHOD="on-demand | pre-logon | user-logon"`	`user-logon`
GlobalProtect App Config Refresh Interval (hours) (Intervalo de actualización de configuración para la aplicación de GlobalProtect [horas])	`refresh-config-interval <hours>`	`REFRESHCONFIGINTERVAL= "<hours>"`	`24`
Actualizar la configuración de DNS al conectar (solo Windows)	`flushdns yes | no`	`FLUSHDNS="yes | no"`	`no`
Enviar informe HIP inmediatamente si cambia el estado del centro de seguridad de Windows (WSC) (solo Windows)	`wscautodetect yes | no`	`WSCAUTODETECT="yes | no"`	`no`
Detect Proxy for Each Connection (Windows Only) (Detectar proxy para cada conexión [solo Windows])	`ProxyMultipleAuto Detection yes | no`	`ProxyMultipleAuto Detection="yes | no"`	`no`
Clear Single Sign-On Credentials on Logout (Windows Only) (Borrar credenciales de inicio de sesión único al desconectar [solo Windows])	`LogoutRemoveSSO yes | no`	`LogoutRemoveSSO="yes | no"`	`yes`
Use Default Authentication on Kerberos	`krb-auth-fail-fallback yes | no`	`KRBAUTHFAILFALLBACK= "yes | no"`	`no`

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Authentication Failure (Windows Only) (Utilizar autenticación por defecto si falla la autenticación Kerberos [solo Windows])			
Uso del navegador predeterminado para la autenticación SAML	(macOS plist) `default-browser yes | no`	`DEFAULTBROWSER= "yes | no"`	`no`
Custom Password Expiration Message (LDAP Authentication Only) (Mensaje personalizado de caducidad de contraseña [solo autenticación LDAP])	`PasswordExpiryMessage <message>`	`PasswordExpiryMessage "<message>"`	
Portal Connection Timeout (sec) (Tiempo de espera de la conexión al portal [s])	`PortalTimeout <portaltimeout>`	`PORTALTIMEOUT= "<portaltimeout>"`	`5`
TCP Connection Timeout (sec) (Tiempo de espera de la conexión TCP [s])	`ConnectTimeout <connecttimeout>`	`CONNECTTIMEOUT= "<connecttimeout>"`	`5`
TCP Receive Timeout (sec) (Tiempo de espera de la recepción TCP [s])	`ReceiveTimeout <receivetimeout>`	`RECEIVETIMEOUT= "<receivetimeout>"`	`30`
Client Certificate Store Lookup (Búsqueda del almacén de certificados de cliente)	`certificate-store-lookup user | machine | user and machine | invalid`	`CERTIFICATESTORELOOKUP= "user | machine | user and machine | invalid"`	`Usuario y equipo`

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
SCEP Certificate Renewal Period (days) (Periodo de renovación del certificado SCEP [días])	`scep-certificate-renewal-period <renewalPeriod>`	n/c	**7**
Maximum Internal Gateway Connection Attempts (Máximos intentos de conexión al gateway interno)	`max-internal-gateway-connection-attempts <maxValue>`	`MIGCA="<maxValue>"`	**0**
Extended Key Usage OID for Client Certificate (OID de uso de clave extendida para certificado de cliente)	`ext-key-usage-oid-for-client-cert <oidValue>`	`EXTCERTOID=”<oidValue>”`	n/c
User Switch Tunnel Rename Timeout (sec) (Tiempo de espera del switch del usuario para cambiar nombre del túnel [s])	`user-switch-tunnel-rename-timeout <renameTimeout>`	n/c	**0**
Use Single Sign-On (Usar inicio de sesión único) **(Solo en Windows)**	`use-sso yes | no`	`USESSO="yes | no"`	**yes**
Not in portal (No en el portal) Este ajuste especifica la dirección IP del portal por defecto (o nombre de host).	`portal <IPaddress>`	`PORTAL="<IPaddress>"`	n/c
Not in portal (No en el portal)	`prelogon 1`	`PRELOGON="1"`	**1**

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Este ajuste habilita a GlobalProtect para iniciar un túnel VPN antes de que un usuario inicie sesión en el dispositivo y se conecte al portal de GlobalProtect.			
Solo Windows/ No en portal Este ajuste se utiliza junto con el inicio de sesión único (single sign-on, SSO) e indica si se deben pedir o no al usuario las credenciales en caso de que falle el SSO.	`can-prompt-user-credential yes | no`	`CANPROMPTUSERCREDENTIAL= "yes | no"`	`yes`
Solo Windows/ No en portal Este ajuste filtra el mosaico del proveedor de credenciales externas de la página de inicio de sesión de Windows para que solo se muestre el mosaico nativo de Windows.*	`wrap-cp-guid {third party credential provider guid}`	`WRAPCPGUID="{guid_value]" FILTERNONGPCP="yes | no"`	`no`
Solo Windows/ No en portal Este ajuste es una opción adicional para el ajuste wrap-cp-guid y permite que el mosaico del proveedor de credenciales externas se	`filter-non-gpcp no`	n/c	n/c

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
muestre en la página de inicio de sesión de Windows, además del mosaico de inicio de sesión de Windows nativo.*			
Solo Windows/ No en portal Este ajuste le permite asignar direcciones IP estáticas a los endpoints de Windows.	**reserved-ipv4 <reserved-ipv4>** **reserved-ipv6 <reserved-ipv6>**	**RESERVEDIPV4="<reserved-ipv4>"** **RESERVEDIPV6="<reserved-ipv6>"**	n/c

Para obtener los pasos detallados para habilitar estos ajustes con el registro de Windows o el instalador de Windows (Msiexec), consulte Ajuste de SSO para proveedores de credenciales externas en endpoints de Windows*.*

Opciones de implementación de secuencias de comandos

La tabla siguiente muestra opciones que permiten que GlobalProtect inicie secuencias de comandos antes y después de establecer una conexión y antes de la desconexión. Debido a que estas opciones no están disponibles en el portal, debe definir los valores para la clave relevante, ya sea conexión VPN previa, conexión VPN posterior o desconexión VPN previa, del registro de Windows o la plist de macOS. Para obtener los pasos detallados para implementar las secuencias de comando, consulte Implementación de secuencias de comandos con el registro de Windows, Implementación de secuencias de comandos con Msiexec o Implementación de secuencias de comandos con la plist de macOS.

Tabla: Opciones de implementación de secuencias de comandos personalizables

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
Ejecute la secuencia de comandos que se especifica en el ajuste de comandos (incluidos los parámetros que pasaron a la secuencia de comandos). *Se admiten las variables ambientales.* *Especifique la ruta*	**command <parameter1> <parameter2> [...]** Ejemplo de Windows: **command %userprofile %\vpn_script.bat c: test_user** Ejemplo de macOS: **command $HOME/ vpn_script.sh / Users/test_user test_user**	**PREVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **POSTVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **PREVPNDISCONNECTCOMMAND= "<parameter1> <parameter2> [...]"**	**n/c**

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
completa en los comandos.			

(Opcional) Especifique los privilegios en virtud de los cuales los comandos se pueden ejecutar (el valor por defecto es usuario: si usted no especifica el contexto, el comando se ejecuta como el usuario activo actual).	`context admin | user`	`PREVPNCONNECTCONTEXT= "admin | user"`
		`POSTVPNCONNECTCONTEXT= "admin | user"`
		`PREVPNDISCONNECTCONTEXT= "admin | user"`
			`user`

(Opcional) Especifique la cantidad de segundos que la aplicación de GlobalProtect debe esperar para que el comando se ejecute (el intervalo es de 0 a 120). Si el comando no se completa antes de que se agote el tiempo, la aplicación puede establecer una conexión o desconectarse. Un valor de 0 (el valor por defecto) significa que la aplicación no espera para ejecutar el comando.
No es compatible para post-vpn-connect.
	`timeout <value>`
	Ejemplo:
	`timeout 60`
		`PREVPNCONNECTTIMEOUT= "<value>"`
		`POSTVPNCONNECTTIMEOUT= "<value>"`
		`PREVPNDISCONNECTTIMEOUT= "<value>"`
			`0`

(Opcional) Especifique la ruta completa de un archivo utilizado en un comando. La aplicación de GlobalProtect verifica la integridad del archivo cotejándolo con el valor especificado en la clave de suma de comprobación.
Se admiten las
	`file <path_file>`	`PREVPNCONNECTFILE= "<path_file>"`
		`POSTVPNCONNECTFILE= "<path_file>"`
		`PREVPNDISCONNECTFILE= "<path_file>"`
			`n/c`

© 2020 Palo Alto Networks, Inc.

Configuración del agente de portal	Registro de Windows/plist de macOS	Parámetro msiexec	predetermi
variables ambientales.			
(Opcional) Especifique la suma de comprobación sha256 del archivo al que se hace referencia en la clave file. Si se especifica la suma de comprobación, la aplicación de GlobalProtect solo ejecuta los comandos si la suma de comprobación generada por la aplicación de GlobalProtect coincide con el valor de suma de comprobación especificado aquí.	**checksum <value>**	**PREVPNCONNECTCHECKSUM= "<value>"** **POSTVPNCONNECTCHECKSUM= "<value>"** **PREVPNDISCONNECTCHECKSUM ="<value>"**	**n/c**
(Opcional) Especifique un mensaje de error para informar al usuario si el comando no puede ejecutarse o si sale con un código de retorno distinto de cero. *El mensaje debe ser 1024 o menos caracteres ANSI.*	**error-msg <message>** Ejemplo: **error-msg Failed executing pre-vpn-connect action!**	**PREVPNCONNECTERRORMSG= "<message>"** **POSTVPNCONNECTERRORMSG= "<message>"** **PREVPNDISCONNECTERRORMSG ="<message>"**	**n/c**

Implementación de los ajustes de la aplicación para los endpoints de Windows

Use el registro de Windows o el instalador de Windows (Msiexec) para implementar de forma transparente la aplicación y los ajustes de GlobalProtect en los endpoints de Windows.

- Implementación de los ajustes del agente en el registro de Windows
- Implementación de la configuración del agente desde Msiexec
- Implementación de secuencias de comandos con el registro de Windows
- Implementación de secuencias de comandos con Msiexec
- Implementación de la configuración de Connect Before Logon (Conectar antes de iniciar sesión) en el Registro de Windows
- Ajuste de SSO para proveedores de credenciales externas en endpoints de Windows
- Habilitación del ajuste de SSO para credenciales externas con el registro de Windows
- Habilitación del ajuste de SSO para credenciales externas con Windows Installer

© 2020 Palo Alto Networks, Inc.

Implementación de los ajustes de la aplicación en el registro de Windows

Puede habilitar la implementación de la configuración de la aplicación de GlobalProtect en los endpoints de Windows antes de su primera conexión al portal de GlobalProtect usando el registro de Windows. Use las opciones que se describen en la siguiente tabla para utilizar el registro de Windows a fin de personalizar los ajustes de la aplicación de los endpoints de Windows.

Además de usar el registro de Windows para implementar los ajustes de la aplicación de GlobalProtect, puede activar la aplicación de GlobalProtect para recopilar información específica del registro de Windows desde los endpoints de Windows. A continuación, puede supervisar los datos y añadirlos a una regla de seguridad como criterios de coincidencia. El tráfico del endpoint que coincida con ciertos ajustes de registro que haya definido puede ponerse en vigor de acuerdo con la regla de seguridad. Además, puede configurar comprobaciones personalizadas para recopilar datos de procesos y aplicaciones de endpoints.

STEP 1 | Encuentre los ajustes de personalización de la aplicación de GlobalProtect que se encuentran en el registro de Windows.

Abra el registro de Windows (introduzca **`regedit`** en el símbolo del sistema) y vaya a:

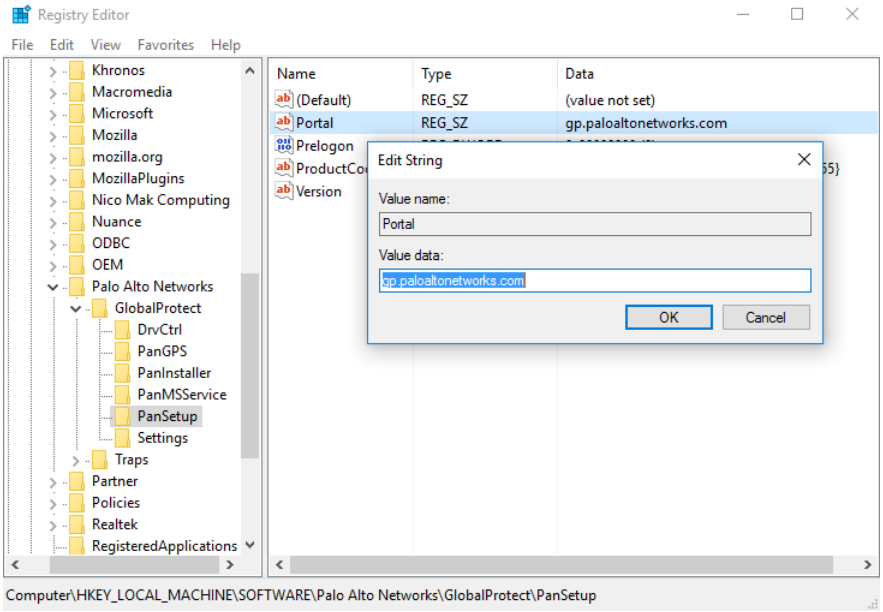
```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\
```

STEP 2 | Defina el nombre del portal.

Si no desea que el usuario final introduzca manualmente la dirección del portal ni siquiera en la primera conexión, puede implementar previamente la dirección del portal mediante el registro de Windows.

1. En el registro de Windows, vaya a:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup
   ```
2. Haga clic con el botón derecho en **Portal**y luego seleccione **Modify (Modificar)**.
3. Introduzca el nombre del portal en el campo **Value data (Datos del valor)** y, luego, haga clic en **OK (Aceptar)**.



© 2020 Palo Alto Networks, Inc.

STEP 3 | Implemente diferentes ajustes al endpoint de Windows, incluido el método de conexión para la aplicación de GlobalProtect y el inicio de sesión único (single sign-on, SSO).

Consulte Ajustes personalizables de la aplicación si desea obtener una lista completa de los comandos y valores que puede configurar con el registro de Windows.

Tiene la opción de implementar la configuración de conexión antes de iniciar sesión en los intendentes de Windows antes de permitir que los usuarios finales inicien sesión en la VPN antes de iniciar sesión en el endpoint.

STEP 4 | Permita que la aplicación de GlobalProtect ajuste las credenciales de terceros en los endpoints de Windows, lo que habilita el SSO cuando se usa un proveedor de credenciales de terceros.

Habilitación del ajuste de SSO para credenciales externas con el registro de Windows.

Implementación de los ajustes de la aplicación desde Msiexec

En los endpoints de Windows, tiene la opción de implementar automáticamente la aplicación de GlobalProtect y los ajustes de la aplicación del instalador de Windows (Msiexec) con la siguiente sintaxis:

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec es un programa ejecutable que instala o configura un producto desde la línea de comandos. En los endpoints que ejecutan Microsoft Windows XP o un sistema operativo posterior, la longitud máxima de la cadena que puede usar en el símbolo del sistema es 8191 caracteres.

Ejemplo de Msiexec	Description (Descripción)
`msiexec.exe /i GlobalProtect.msi /quiet PORTAL="portal.acme.com"`	Instale GlobalProtect en modo silencioso (sin interacción del usuario) y configure la dirección del portal.
`msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID="no"`	Instale GlobalProtect con la opción de impedir que los usuarios se conecten al portal si el certificado no es válido.

Para obtener una lista completa de ajustes y los valores predeterminados correspondientes, consulte Ajustes personalizables de la aplicación.

También puede habilitar el ajuste de SSO para credenciales externas con el instalador de Windows*.*

Implementación de secuencias de comandos con el registro de Windows

Puede habilitar la implementación de secuencias de comandos personalizadas en endpoints de Windows con el registro de Windows.

Puede configurar la aplicación de GlobalProtect para que inicie y ejecute una secuencia de comandos para cualquiera de los siguientes eventos: antes y después de establecer el túnel, y antes de desconectar el túnel. Para ejecutar la secuencia de comando en un evento particular, haga referencia a la secuencia de comandos por lotes desde una entrada de registro de comando para ese evento.

© 2020 Palo Alto Networks, Inc.

Según los ajustes de configuración, la aplicación de GlobalProtect puede ejecutar una secuencia de comandos antes y después de que la aplicación establezca una conexión con la puerta de enlace, y antes de que la aplicación se desconecte. Use el siguiente flujo de trabajo para utilizar el registro de Windows a fin de personalizar los ajustes de la aplicación de los endpoints de Windows.

Los ajustes de registro que le permiten implementar secuencias de comandos son compatibles en los endpoints que ejecutan la aplicación 2.3 de GlobalProtect y versiones posteriores.

STEP 1 | Abra el registro de Windows y busque los ajustes de personalización de la aplicación de GlobalProtect.

Abra el registro de Windows (introduzca **`regedit`** en el símbolo del sistema) y vaya hasta las siguientes ubicaciones de la clave, según cuándo desee ejecutar las secuencias de comandos (conexión previa/posterior o desconexión previa):

`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-connect`

`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\post-vpn-connect`

`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-disconnect`

Si la clave no existe en la clave Settings (Configuración), créela. Para ello, haga clic con el botón derecho del ratón en Settings (Configuración) y seleccione New (Nueva) > Key (Clave).

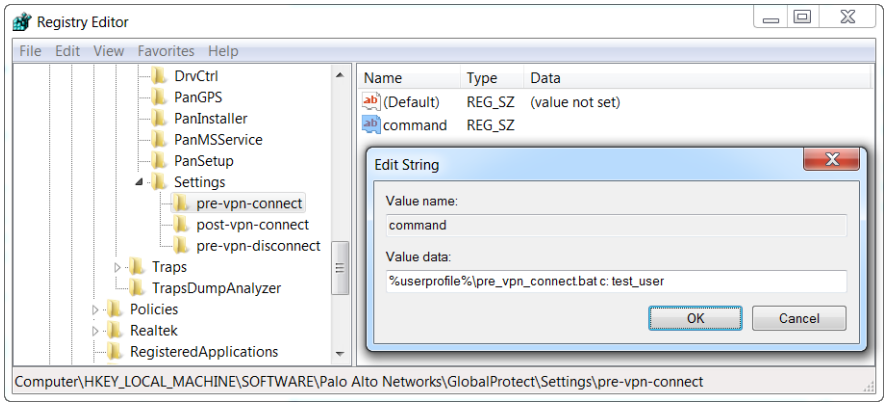
STEP 2 | Habilite la aplicación de GlobalProtect para que ejecute secuencias de comandos mediante la creación de un nuevo valor de cadena denominado **`command`**.

El archivo por lotes especificado aquí debe contener secuencias de comandos específicas (incluidos los parámetros que pasaron a la secuencia de comando) que desea ejecutar en el dispositivo.

1. Si la cadena `command` aún no existe, créela. Para ello, haga clic con el botón derecho del ratón en la clave `pre-vpn-connect`, `post-vpn-connect` o `pre-vpn-disconnect`, seleccione **New (Nuevo)** > **String Value (Valor de cadena)** y asígnele el nombre **`command`**).
2. Haga clic con el botón derecho en `command`y luego seleccione **Modify (Modificar)**.
3. Introduzca los comandos o secuencia de comandos que la aplicación de GlobalProtect debe ejecutar. Por ejemplo:

```
%userprofile%\pre_vpn_connect.bat c:test_user
```


© 2020 Palo Alto Networks, Inc.



STEP 3 | (Opcional) Añada entradas de registro adicional según fuera necesario para cada comando.

Cree o modifique secuencias de comandos de registro y sus correspondientes valores, incluidos context, timeout, file, checksum o error-msg. Para obtener más información, consulte Configuración de aplicación personalizable.

Implementación de secuencias de comandos con Msiexec

En los endpoints de Windows, puede usar el instalador de Windows (Msiexec) para implementar la aplicación de GlobalProtect, la configuración de la aplicación y las secuencias de comandos que la aplicación ejecutará automáticamente (consulte Ajustes personalizables de la aplicación. Para hacerlo, utilice la siguiente sintaxis:

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec es un programa ejecutable que instala o configura un producto desde una línea de comandos. En los sistemas que ejecutan Microsoft Windows XP o versiones posteriores, la longitud máxima de la cadena que puede usar en el símbolo del sistema es 8191 caracteres.

Esta limitación se aplica a la línea de comandos, las variables de entorno individuales (tales como la variable USERPROFILE) que son heredadas por otros procesos, y todas las expansiones de variable de entorno. Si ejecuta archivos por lotes desde la línea de comandos, este límite también se aplica al procesamiento de archivos por lotes.

Por ejemplo, para implementar secuencias de comando que se ejecutan en eventos de conexión o desconexión específicos, puede usar una sintaxis similar a los siguientes ejemplos:

Ejemplo: Use Msiexec para implementar secuencias de comandos que se ejecutan antes de un evento de conexión

Para obtener una secuencia de comandos que pueda copiar y pegar, ingrese aquí.

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c: test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
```


© 2020 Palo Alto Networks, Inc.

```
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
```

Para obtener una lista completa de ajustes y los valores predeterminados correspondientes, consulte Ajustes personalizables de la aplicación.

Ejemplo: Use Msiexec para implementar secuencias de comandos que se ejecutan en eventos de conexión previa, conexión posterior y desconexión previa

Para obtener una secuencia de comandos que pueda copiar y pegar, ingrese aquí.

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c: test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
POSTVPNCONNECTCOMMAND="c:\users\test_user\post_vpn_connect.bat c: test_user"
POSTVPNCONNECTCONTEXT="admin"
POSTVPNCONNECTFILE="%userprofile%\post_vpn_connect.bat"
POSTVPNCONNECTCHECKSUM="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf598"
POSTVPNCONNECTERRORMSG="Failed executing post-vpn-connect action."
PREVPNDISCONNECTCOMMAND="%userprofile%\pre_vpn_disconnect.bat c: test_user"
PREVPNDISCONNECTCONTEXT="admin"
PREVPNDISCONNECTTIMEOUT="0"
PREVPNDISCONNECTFILE="C:\Users\test_user\pre_vpn_disconnect.bat"
PREVPNDISCONNECTCHECKSUM="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0
118647ccf597"
PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-disconnect action."
```

Para obtener una lista completa de ajustes y los valores predeterminados correspondientes, consulte Ajustes personalizables de la aplicación.

Implementación de la configuración de Connect Before Logon (Conectar antes de iniciar sesión) en el Registro de Windows

Puede implementar la configuración de Connect Before Logon (Conectar antes de iniciar sesión) en los endpoints de Windows 10 antes de permitir que los usuarios finales inicien sesión en la VPN antes de iniciar sesión en el endpoint mediante el Registro de Windows. GlobalProtect recupera las claves de registro solo una vez, cuando se inicializa la aplicación de GlobalProtect.

Los métodos de conexión previa al inicio de sesión y de inicio de sesión previo y bajo demanda no son compatibles simultáneamente con Connect Before Logon (Conectar antes de iniciar sesión).

STEP 1 | Configure las claves de registro en los endpoints de Windows del usuario final.

Debe cambiar el Registro de Windows en los endpoints de Windows de los usuarios finales para poder habilitar Connect Before Logon (Conectar antes de iniciar sesión). Puede añadir automáticamente las claves de registro o agregar las claves manualmente.

© 2020 Palo Alto Networks, Inc.

- Para añadir automáticamente las claves de registro para `PanPlapProvider` y `PanPlapProvider.dll` en **PanGPS.exe** (`C:\Archivos de programa\Palo Alto Networks\GlobalProtect`), use el comando `-registerplap` para ejecutarlo como administrador mediante la siguiente sintaxis:

```
PanGPS.exe -registerplap
```

- Para anular automáticamente el registro de las claves para `PanPlapProvider` y `PanPlapProvider.dll` en **PanGPS.exe** (`C:\Archivos de programa\Palo Alto Networks\GlobalProtect`), use el comando `-unregisterplap` para ejecutarlo como administrador usando la siguiente sintaxis:

```
PanGPS.exe -unregisterplap
```

Para añadir manualmente las claves de registro, abra el Editor de Registro de Windows y especifique **regedit** en el símbolo del sistema.

Debe crear la carpeta `CLSID`.

1. En el Registro de Windows, vaya a `HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}`.

   Añada el valor `PanPlapProvider` en el formato **`@=PanPlapProvider`**.
2. En el Registro de Windows, vaya a `HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}\InprocServer32@="PanPlapProvider.dll"`.

   Verifique que el valor **ThreadingModel** esté establecido en **Apartment (Apartamento)**. Es el valor predeterminado.
3. En el Registro de Windows, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{20A29589-E76A-488B-A520-63582302A285}@="PanPlapProvider"`.

   Añada el valor `PanPlapProvider` en el formato **`@=PanPlapProvider`**.

STEP 2 | (Opcional) Configure direcciones o nombres de portal adicionales para mostrar.

Si está configurado, Connect Before Logon (Conectar antes de iniciar sesión) utilizará la dirección del portal predeterminada o el nombre en el Registro de Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` con la clave `Portal`).

Puede configurar direcciones de portal adicionales o nombres que desee mostrar en el menú desplegable Portal. Para ello, cambie las claves de registro en los endpoints de Windows del usuario final. Puede añadir hasta cinco direcciones o nombres de portal. Debe cambiar el Registro de Windows en los endpoints de Windows de los usuarios finales para poder definir las direcciones o los nombres del portal.

Abra el Editor de registro de Windows (introduzca **regedit** en el símbolo del sistema).

1. En el Registro de Windows, cree la carpeta `CBL` en `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. En el Registro de Windows, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Seleccione **Edit (Editar)** > **New (Nuevo)** > **String Value (Valor de cadena)** para crear una entrada de registro para cada portal que desee añadir.

© 2020 Palo Alto Networks, Inc.

Debes especificar cada entrada como *Portal1*, *Portal2*, *Portal3*, *Portal4* y *Portal5*. Las entradas no pueden contener espacios.

4. Haga clic con el botón derecho en el valor de registro *portal* y, a continuación, seleccione **Modify (Modificar)**.
5. Especifique la dirección IP o el nombre del portal de GlobalProtect en el campo **Value Data (Datos de valor)** y, a continuación, haga clic en **OK (Aceptar)**.
6. Repita los pasos 3 y 4 para cada portal que desee añadir.

STEP 3 | (Opcional) Visualice los nombres o direcciones de portal predefinidos.

Debe cambiar el Registro de Windows en los endpoints de Windows de los usuarios finales para poder ver las direcciones o los nombres del portal.

Abra el Editor de registro de Windows (introduzca **regedit** en el símbolo del sistema).

1. En el Registro de Windows, cree la carpeta `CBL` en `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. En el Registro de Windows, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Seleccione **Edit (Editar)** > **New (Nuevo)** > **String Value (Valor de cadena)** para crear una entrada de registro para *AlwaysShowPortal*.
4. Introduzca el valor como *yes (sí)* en el campo **Value Data (Datos de valor)** y, a continuación, haga clic en **OK (Aceptar)**.

De forma predeterminada, Connect Before Logon (Conectar antes de iniciar sesión) no muestra la dirección o el nombre del portal si solo se define un portal.

STEP 4 | (Opcional) Permita que los usuarios finales se autentiquen mediante una tarjeta inteligente.

Debe cambiar el Registro de Windows en los endpoints de Windows de los usuarios finales para poder habilitar la autenticación de la tarjeta inteligente.

Abra el Editor de registro de Windows (introduzca **regedit** en el símbolo del sistema).

1. En el Registro de Windows, cree la carpeta `CBL` en `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. En el Registro de Windows, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Seleccione **Edit (Editar)** > **New (Nuevo)** > **String Value (Valor de cadena)** para crear una entrada de registro para *UseSmartCard*.
4. Introduzca el valor como *yes (sí)* en el campo **Value Data (Datos de valor)** y, a continuación, haga clic en **OK (Aceptar)**.

STEP 5 | Reinicie el endpoint.

Debe reiniciar el endpoint para que las claves de registro de PLAP y Connect Before Logon (Conectar antes de iniciar sesión) surtan efecto.

STEP 6 | Verifique la configuración.

Una vez que configure los ajustes en el Registro de Windows y comience a usar Connect Before Logon (Conectar antes de iniciar sesión) con la aplicación de GlobalProtect™ 5.2, elija el método de autenticación:

- Connect Before Logon Using Smart Card Authentication (Conectarse antes de iniciar sesión mediante autenticación con tarjeta inteligente)

© 2020 Palo Alto Networks, Inc.

- Connect Before Logon Using SAML Authentication (Conectarse antes de iniciar sesión mediante autenticación SAML)
- Connect Before Logon Using Username/Password-Based Authentication (Conectarse antes de iniciar sesión mediante autenticación basada en nombre de usuario/contraseña)

Ajuste de SSO para proveedores de credenciales externas en endpoints de Windows

En los endpoints de Windows 7, la aplicación de GlobalProtect utiliza el marco de proveedor de credenciales de Microsoft para admitir un inicio de sesión único (single sign-on, SSO). Con el SSO, el proveedor de credenciales de GlobalProtect encapsula al proveedor de credenciales nativo de Windows, que habilita a GlobalProtect para usar las credenciales de inicio de sesión de Windows para autenticarse automáticamente y conectarse al portal y la puerta de enlace de GlobalProtect. Además, el SSO permite que los usuarios de Windows 10 actualicen su contraseña de Active Directory (AD) con el proveedor de credenciales de GlobalProtect cuando su contraseña vence o un administrador requiere un cambio de contraseña en el siguiente inicio de sesión.

Cuando otro proveedor de credenciales externo también existe en el endpoint, el proveedor de credenciales de GlobalProtect no puede reunir las credenciales de inicio de sesión de Windows del usuario. Como resultado, GlobalProtect no se conecta al portal y a la puerta de enlace de manera automática. Si el SSO falla, usted puede identificar al proveedor de credenciales externo y configurar la aplicación de GlobalProtect para que encapsule dichas credenciales de terceros, lo que permite a los usuarios autenticarse correctamente en Windows, GlobalProtect y el proveedor de credenciales externo usando solo sus credenciales de inicio de sesión de Windows.

Opcionalmente, puede configurar Windows para que muestre mosaicos de inicio de sesión separados: uno para cada proveedor de credenciales y otro para el inicio de sesión de Windows nativo. Esto es útil cuando un proveedor de credenciales externo añade una funcionalidad adicional que no se aplica a GlobalProtect.

Si desea eliminar el proveedor de credenciales de GlobalProtect del terminal con Windows, ejecute el comando ***`GlobalProtectPanGPS.exe -u`*** *en el símbolo del sistema.*

Use el registro de Windows o el instalador de Windows (`Msiexec`) para permitir que GlobalProtect ajuste las credenciales externas:

- Habilitación del ajuste de SSO para credenciales externas con el registro de Windows
- Habilitación del ajuste de SSO para credenciales externas con Windows Installer

El ajuste de SSO de GlobalProtect para proveedores de credenciales (credential providers, CP) externos depende de la configuración del CP externo. En algunos casos, el ajuste de SSO de GlobalProtect podría no funcionar correctamente si la implementación del CP externo no permite que GlobalProtect ajuste de manera correcta su CP.

Habilitación del ajuste de SSO para credenciales externas con el registro de Windows

Use las siguientes pasos en el registro de Windows para permitir que el SSO se ajuste a credenciales de terceros en los endpoints de Windows 7.

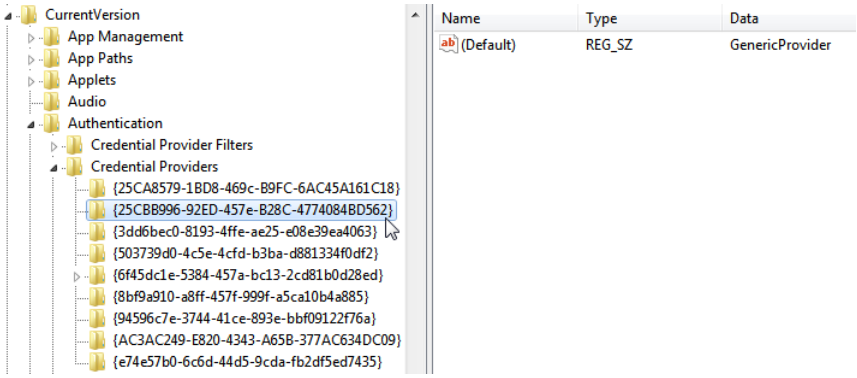
STEP 1 | Abra el registro de Windows y localice el identificador único global (globally unique identifier, GUID) para un proveedor de terceros que desee ajustar.

1. Desde el símbolo del sistema, ingrese **`regedit`** para abrir el editor de registro de Windows.
2. Vaya a la siguiente ubicación del registro de Windows para ver la lista de los proveedores de credenciales actualmente instalados:

© 2020 Palo Alto Networks, Inc.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion
\Authentication\Credential Providers.
```

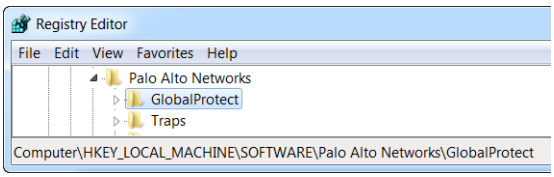
3. Copie la clave de GUID para el proveedor de credenciales que desea ajustar (incluidas las llaves `{` y `}` en cualquier extremo del GUID):



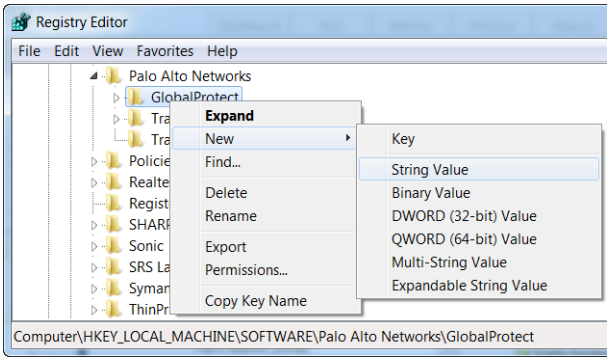
STEP 2 | Habilite el SSO para proveedores de credenciales externas al añadir el ajuste **`wrap-cp-guid`** al registro de GlobalProtect.

1. Vaya a la siguiente ubicación del registro de Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\ GlobalProtect:
```



2. Haga clic derecho en la carpeta **GlobalProtect**, y luego seleccione **New (Nuevo)** > **String Value (Valor de cadena)** para añadir un nuevo valor:



3. Configure los siguientes campos de **String Value (Valor de cadena)**:
   - **Name (Nombre)**: **`wrap-cp-guid`**
   - **Value data (Datos de valor)**: {**`<third-party credential provider GUID>`**}

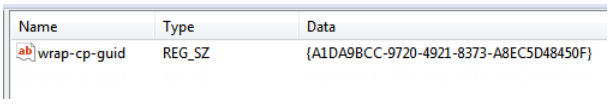
   En el campo Value data (Datos de valor), el valor de GUID que haya introducido debe estar rodeado de llaves de apertura y cierre: `{` y `}`.

   A continuación, se incluye un ejemplo de la apariencia que tendría una GUID de proveedor de credenciales externas en el campo **Value data (Datos de valor)**:

© 2020 Palo Alto Networks, Inc.

```
{A1DA9BCC-9720-4921-8373-A8EC5D48450F}
```

En la nueva entrada de **String Value (Valor de cadena)**, se muestran `wrap-cp-guid` como valor de **Name (Nombre)** y el GUID como valor de **Value Data (Datos de valor)**.



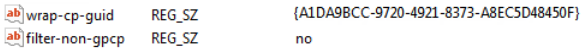
Name	Type	Data
wrap-cp-guid	REG_SZ	{A1DA9BCC-9720-4921-8373-A8EC5D48450F}

STEP 3 | Siguientes pasos:

- Con esta configuración, el mosaico de inicio de sesión nativo de Windows se muestra a los usuarios en la pantalla de inicio de sesión. Cuando los usuarios hacen clic en el mosaico e inician sesión en el sistema con sus credenciales de Windows, ese inicio único autentica a los usuarios en Windows, GlobalProtect y el proveedor de credenciales de terceros.
- (Opcional) Si desea mostrar varios mosaicos en la pantalla de inicio de sesión (por ejemplo, el mosaico de Windows nativo y el mosaico del proveedor de credenciales de terceros), continúe con el paso 4.
- (Opcional) Si desea asignar un proveedor de credenciales predeterminado para los usuarios, continúe con el paso 5.
- (Opcional) Si desea ocultar el mosaico de un proveedor de credenciales de terceros de la pantalla de inicio de sesión, continúe con el paso 6.

STEP 4 | (Opcional) Permita que el mosaico del proveedor de credenciales externas se muestre a los usuarios en el inicio de sesión.

Añada un segundo **String Value (Valor de cadena)** con el **Name (Nombre)** **`filter-non-gpcp`** e introduzca **`no`** en los **Value data (Datos de valor)** de la cadena:



wrap-cp-guid	REG_SZ	{A1DA9BCC-9720-4921-8373-A8EC5D48450F}
filter-non-gpcp	REG_SZ	no

Después de añadir este valor de cadena a la configuración de GlobalProtect, se presentan dos opciones de inicio sesión a los usuarios en la pantalla de inicio de sesión de Windows: el mosaico de Windows nativo y el mosaico del proveedor de credenciales externo.

STEP 5 | Asigne un proveedor de credenciales predeterminado para el inicio de sesión del usuario.

1. Abra el registro de Windows para localizar el identificador único global (globally unique identifier, GUID) para un proveedor de credenciales externo que desee asignar como el proveedor de credenciales predeterminado.
   1. Desde el símbolo del sistema, ingrese `regedit` para abrir el editor de registro de Windows.
   2. Vaya a la siguiente ubicación del registro de Windows para ver la lista de los proveedores de credenciales actualmente instalados:

      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
   3. Copie la clave de GUID completa para el proveedor de credenciales (incluidas las llaves `{` y `}` en cualquier extremo del GUID):
2. Abra el editor de políticas de grupos locales para habilitar y asignar un proveedor de credenciales predeterminado.
   1. Desde el símbolo del sistema, ingrese `gpedit.msc` para abrir el editor de políticas de grupos locales.
   2. Seleccione **Computer Configuration (Configuración del ordenador)** > **Administrative Templates (Plantillas administrativas)** > **System (Sistema)** > **Logon (Inicio de sesión)**.

© 2020 Palo Alto Networks, Inc.

3. En **Setting (Configuración)**, haga doble clic en **Assign a default credential provider (Asignar un proveedor de credenciales predeterminado)** para abrir la ventana **Assign a default credential provider (Asignar un proveedor de credenciales predeterminado)**.
4. Configure la política en **Enabled (Habilitada)**.
5. En **Assign the following credential provider as the default credential provider (Asignar el siguiente proveedor de credenciales como el proveedor de credenciales predeterminado)**, ingrese el GUID del proveedor de credenciales (que copió del registro de Windows).
6. Haga clic en **Apply (Aplicar)** y, luego, en **OK (Aceptar)** para guardar los cambios.

STEP 6 | (Opcional) Oculte el mosaico del proveedor de credenciales externo de la pantalla de inicio de sesión de Windows.

1. Abra el registro de Windows para localizar el identificador único global (globally unique identifier, GUID) para un proveedor de credenciales externo que desee ocultar.
   1. Desde el símbolo del sistema, ingrese `regedit` para abrir el editor de registro de Windows.
   2. Vaya a la siguiente ubicación del registro de Windows para ver la lista de los proveedores de credenciales actualmente instalados:

      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
   3. Copie la clave de GUID para el proveedor de credenciales que desea ocultar (incluidas las llaves `{` y `}` en cualquier extremo del GUID).
2. Abra el editor de políticas de grupos locales para ocultar el proveedor de credenciales externo.
   1. Desde el símbolo del sistema, ingrese `gpedit.msc` para abrir el editor de políticas de grupos locales.
   2. Seleccione **Computer Configuration (Configuración del ordenador)** > **Administrative Templates (Plantillas administrativas)** > **System (Sistema)** > **Logon (Inicio de sesión)**.
   3. En **Setting (Configuración)**, haga doble clic en **Exclude credential providers (Excluir proveedores de credenciales)** para abrir la ventana **Exclude credential providers (Excluir proveedores de credenciales)**.
   4. Configure la política en **Enabled (Habilitada)**.
   5. En **Exclude the following credential providers (Excluir los siguientes proveedores de credenciales)**, ingrese el GUID del proveedor de credenciales que desea ocultar (que copió del registro de Windows).

      Para ocultar varios proveedores de credenciales, separe cada GUID con una coma.
   6. Haga clic en **Apply (Aplicar)** y, luego, en **OK (Aceptar)** para guardar los cambios.

STEP 7 | Finalice los cambios.

Una vez que terminó de realizar cambios, reinicie el sistema para aplicar los cambios.

Habilitación del ajuste de SSO para credenciales externas con Windows Installer

Use las siguientes opciones en el instalador de Windows (Msiexec) para permitir que el SSO ajuste los proveedores de credenciales externos en los endpoints de Windows 7.

- Ajuste las credenciales externas y muestre el mosaico nativo a los usuarios en el inicio de sesión. Los usuarios pueden hacer clic en el mosaico para iniciar sesión en el endpoint con sus credenciales nativas de Windows. Con ese inicio de sesión único, los usuarios pueden autenticar en Windows, GlobalProtect y el proveedor de credenciales externas.

© 2020 Palo Alto Networks, Inc.

Utilice la siguiente sintaxis desde Windows Installer (Msiexec):

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}"
 FILTERNONGPCP="yes"
```

En la sintaxis anterior, el parámetro **FILTERNONGPCP** simplifica la autenticación para el usuario al filrar la opción para iniciar sesión en el sistema con las credenciales externas.

- Si desea que los usuarios tengan la opción de iniciar sesión con las credenciales de terceros, use la siguiente sintaxis del instalador de Windows (Msiexec):

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}"
FILTERNONGPCP="no"
```

En la sintaxis anterior, el parámetro **FILTERNONGPCP** se ha definido como **"no"**, lo cual filtra el mosaico de inicio de sesión del proveedor de credenciales externo para que solo aparezca el mosaico nativo. En este caso, se muestran a los usuarios tanto el mosaico nativo de Windows como el del proveedor de credenciales externas cuando inician sesión en el endpoint de Windows.

Implementación de los ajustes de la aplicación para los endpoints de macOS

Use el archivo de plist (lista de propiedades) global de macOS para configurar los ajustes de personalización de la aplicación de GlobalProtect o para implementar secuencias de comandos en endpoints de macOS.

- Implementación de la configuración de la aplicación en la plist de macOS
- Implementación de secuencias de comandos con la plist de macOS

Implementación de la configuración de la aplicación en la plist de macOS

Puede definir los ajustes de personalización de la aplicación de GlobalProtect en el archivo plist (lista de propiedades) global de macOS. Esto permite la implementación de la configuración de la aplicación de GlobalProtect en los endpoints de macOS antes de su primera conexión al portal de GlobalProtect.

En los endpoints de macOS, los archivos plist se encuentran en `/Library/Preferences` o en `~/Library/Preferences`. El símbolo de tilde (~) indica que la ubicación está en la carpeta de inicio del usuario actual. La aplicación de GlobalProtect de un endpoint de macOS comprueba en primer lugar los ajustes de plist de GlobalProtect. Si la plist no existe en esa ubicación, la aplicación de GlobalProtect busca los ajustes de plist en `~/Library/Preferences`.

Además de usar la plist de macOS para implementar los ajustes de la aplicación de GlobalProtect, debe activar la aplicación de GlobalProtect para recopilar información específica de la plist de macOS de los endpoints. A continuación, puede supervisar los datos y añadirlos a una regla de seguridad como criterios de coincidencia. El tráfico del endpoint que coincida con ciertos ajustes de registro que haya definido puede ponerse en vigor de acuerdo con la regla de seguridad. Además, puede configurar comprobaciones personalizadas para recopilar datos de procesos y aplicaciones de endpoints*.*

STEP 1 | Abra el archivo plist de GlobalProtect y busque los ajustes de personalización de la aplicación de GlobalProtect.

Use Xcode o un editor de plist alternativo para abrir el archivo de plist:

© 2020 Palo Alto Networks, Inc.

`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`

Luego vaya a:

`/Palo Alto Networks/GlobalProtect/Settings`

Si el diccionario `Settings` no existe, créelo. Añada cada clave al diccionario `Settings (Configuración)` como una cadena.

STEP 2 | Defina el nombre del portal.

Si no desea que el usuario final introduzca manualmente la dirección del portal ni siquiera en la primera conexión, puede implementar previamente la dirección del portal mediante la plist. En el diccionario `PanSetup`, configure una entrada para `Portal`.

STEP 3 | Implemente diferentes ajustes al endpoint de macOS, incluido el método de conexión para la aplicación de GlobalProtect.

Consulte Ajustes personalizables de la aplicación si desea obtener una lista completa de las claves y valores que puede configurar usando el archivo plist de macOS.

Implementación de secuencias de comandos con la plist de macOS

Cuando un usuario se conecta a la puerta de enlace de GlobalProtect por primera vez, la aplicación de GlobalProtect descarga el archivo de configuración y amacena los ajustes de la aplicación en un archivo de propiedades macOS (plist) de GlobalProtect. Además de realizar cambios en los ajustes de la aplicación, puede utilizar la plist para implementar secuencias de comandos en algunos o todos los siguientes eventos: antes y después de establecer el túnel, y antes de desconectar el túnel. Use el siguiente flujo de trabajo para usar la plist a fin de implementar secuencias de comando en endpoints de macOS.

Los ajustes de plist de macOS que le permiten implementar secuencias de comandos son compatibles en los endpoints que ejecutan la aplicación 2.3 de GlobalProtect y versiones posteriores.

STEP 1 | (Endpoints que ejecutan el SO Mac X 10.9 o un SO posterior) Renueve la caché de configuración. Esto evita que el SO utilice las preferencias de caché después de realizar cambios en el archivo plist.

Para borrar la caché de preferencias por defecto, ejecute el comando **`killall cfprefsd`** desde un terminal macOS.

STEP 2 | Abra el archivo plist de GlobalProtect y encuentre o cree el diccionario GlobalProtect asociado con el evento de conexión o desconexión. El diccionario con el cual añadirá los ajustes determina cuándo la aplicación de GlobalProtect ejecuta las secuencias de comando.

Use Xcode o un editor de plist alternativo para abrir el archivo plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) y vaya a una de las siguientes ubicaciones del diccionario:

- `/PaloAlto Networks/GlobalProtect/Settings/pre-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/post-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/pre-vpn-disconnect`

Si el diccionario `Settings` no existe, créelo. Luego, en `Settings (Configuración)`, cree un nuevo diccionario para el evento o los eventos en los cuales desea ejecutar secuencias de comandos.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Habilite la aplicación de GlobalProtect para que ejecute secuencias de comandos al crear una nueva **`String`** denominada **`command`**.

El valor especificado aquí debe hacer referencia a la secuencia de comandos de shell (y los parámetros que deben pasar a la secuencia de comandos) que desea ejecutar en sus endpoints.

Si la cadena `command` aún no existe, añádala al diccionario y especifique la secuencia de comandos y los parámetros en el campo **Value (Valor)**. Por ejemplo:

```
$HOME\pre_vpn_connect.sh
/Users/username username
```

Se admiten las variables ambientales.

Como práctica recomendada, especifique la ruta completa en los comandos.

STEP 4 | (Opcional) Añada ajustes adicionales relacionados con el comando, incluidos los privilegios de administrador, un valor de tiempo de espera para la secuencia de comandos, un valor de suma de comprobación para el archivo por lotes y un mensaje de error para mostrar si el comando no se ejecuta correctamente.

Cree o modifique secuencias de comandos adicionales en la plist (`context`, `timeout`, `file`, `checksum` o `error-msg`) e introduzca sus valores correspondientes. Para obtener más información, consulte Configuración de aplicación personalizable.

STEP 5 | Guarde los cambios al archivo plist.

Guarde el archivo plist.

VPN sin cliente de GlobalProtect

La VPN sin cliente de GlobalProtect proporciona acceso remoto seguro a aplicaciones web empresariales comunes. Los usuarios tienen la ventaja de contar con el acceso seguro de los navegadores web con SSL sin instalar el software de GlobalProtect. Esto resulta útil cuando necesita permitir el acceso de un socio o contratista a las aplicaciones y habilitar de manera segura activos no gestionados, incluidos los endpoints personales. Puede configurar la página de inicio del portal de GlobalProtect para proporcionar acceso a aplicaciones web basadas en usuarios y grupos de usuarios, y también permitir el inicio de sesión único en aplicaciones habilitadas para SAML. Los siguientes temas proporcionan información sobre cómo configurar y solucionar problemas de VPN sin cliente.

- Descripción general de VPN sin cliente
- Tecnologías compatibles
- Configuración de VPN sin cliente
- Solución de problemas de VPN sin cliente

© 2020 Palo Alto Networks, Inc.

Descripción general de VPN sin cliente

Cuando configura la VPN sin cliente de GlobalProtect, los usuarios remotos pueden iniciar sesión en el portal de GlobalProtect con un navegador web e iniciar las aplicaciones web que publica para los usuarios. Según los usuarios o grupos de usuarios, puede permitir que accedan a un conjunto de aplicaciones disponibles o permitirles acceder a aplicaciones corporativas adicionales a través de una URL de la aplicación personalizada.

Luego de iniciar sesión en el portal, los usuarios ven una página de aplicaciones publicadas con la lista de aplicaciones web que pueden ejecutar. Puede usar la página de inicio de aplicaciones predeterminadas en el portal de GlobalProtect o crear una página de inicio personalizada para su empresa.

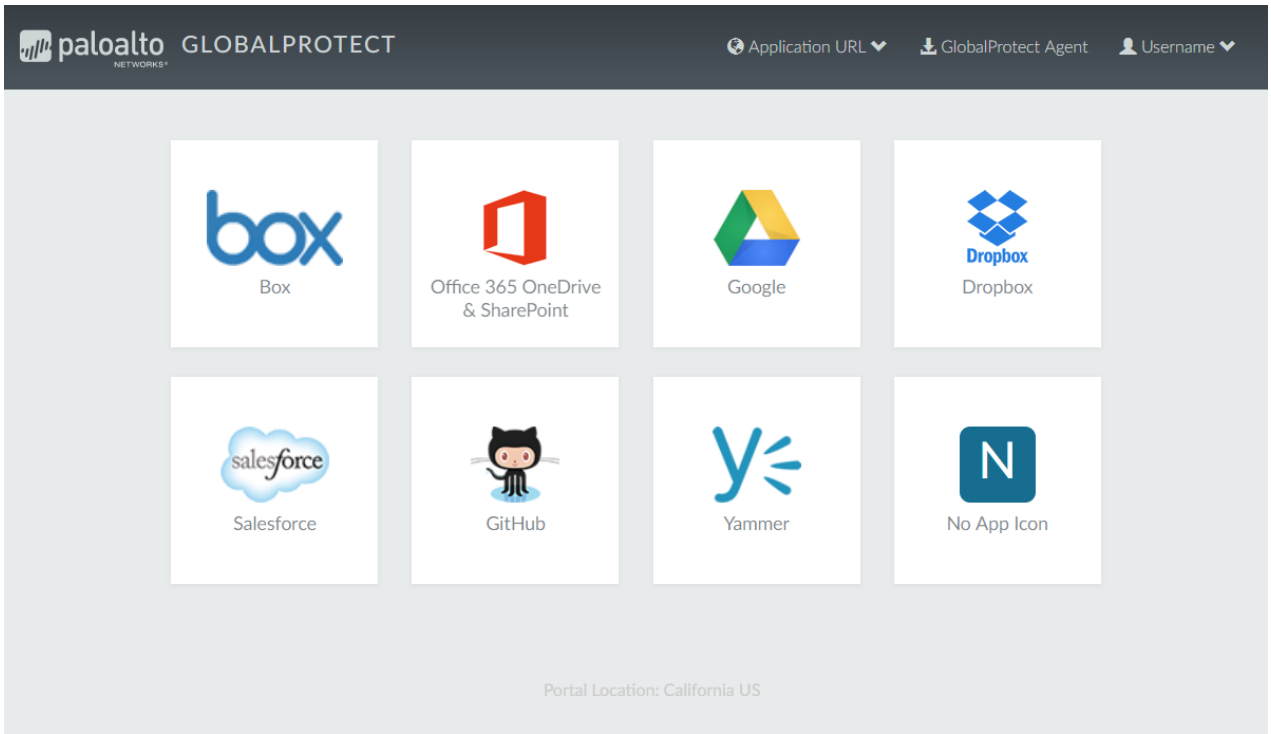


Figure 3: Página de inicio de aplicaciones para VPN sin cliente

Debido a que esta página reemplaza la página de destino predeterminada del portal, incluye un enlace a la página de descarga de la aplicación de GlobalProtect. Si la opción está configurada, los usuarios también pueden seleccionar la **Application URL (URL de la aplicación)** e introducir las URL para iniciar más aplicaciones web corporativas no publicadas.

Cuando configura una sola aplicación web (y deshabilita el acceso a las aplicaciones no publicadas), en lugar de llevar al usuario a la página de aplicaciones publicadas, la aplicación se iniciará automáticamente tan pronto como el usuario inicie sesión Si no configura la VPN sin cliente de GlobalProtect, los usuarios verán la página de descarga del software de la aplicación cuando inicien sesión en el portal.

Cuando configura la VPN sin cliente de GlobalProtect, necesita políticas de seguridad para permitir el tráfico de endpoints de GlobalProtect a la zona de seguridad asociada con el portal de GlobalProtect que aloja la página de inicio de las aplicaciones publicadas y políticas de seguridad para permitir el tráfico basado en usuarios desde la zona del portal de GlobalProtect a la zona de seguridad, donde se alojan los servidores de aplicaciones publicados. Las políticas de seguridad que usted defina controlan qué usuarios tienen permiso para usar cada aplicación publicada.

© 2020 Palo Alto Networks, Inc.

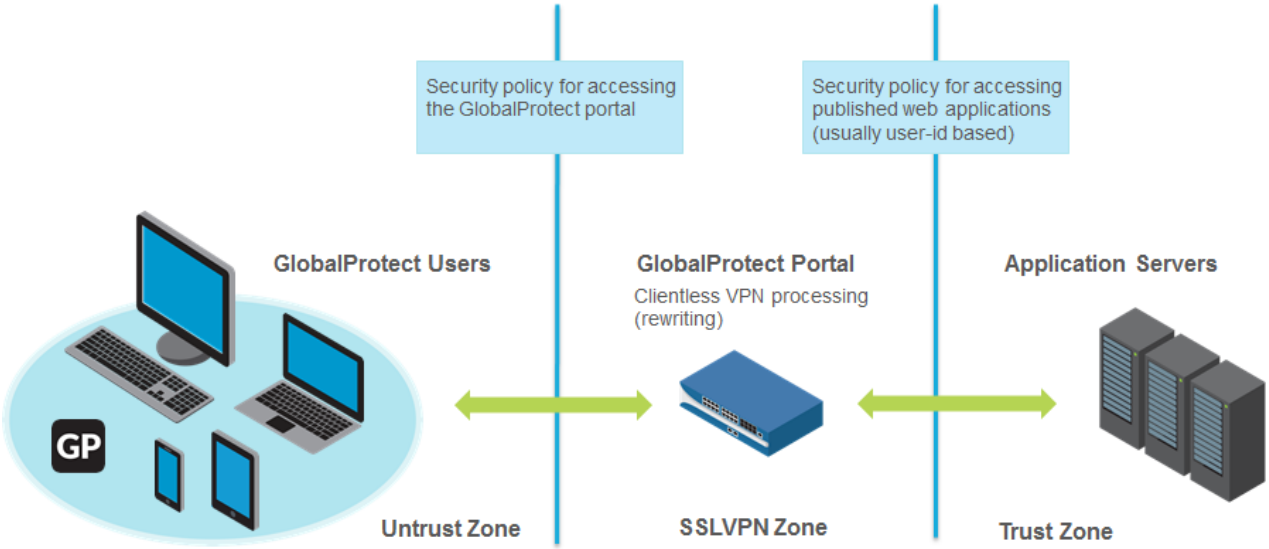


Figure 4: Zonas y política de seguridad para VPN sin cliente

© 2020 Palo Alto Networks, Inc.

Tecnologías compatibles

Puede configurar el portal GlobalProtect para proporcionar acceso remoto seguro a aplicaciones web empresariales comunes. Para obtener resultados óptimos, compruebe las aplicaciones de Clientless VPN de forma exhaustiva en un entorno controlado antes de implementarlas o ponerlas a disposición de numerosos usuarios.

No se admiten las siguientes tecnologías de aplicaciones web:

- *Aplicaciones no web como SSH, FTP, SMTP, protocolo de escritorio remoto (RDP, Remote Desktop Protocol), etc.*
- *HTTP 2.0*
- *Codificaciones que no son UTF-8*
- *Implementación de IPv6*
- *Varias transacciones en HTTP como autenticación NT LAN Manager (NTLM)*
- *Javascript ES6*
- *Los archivos no se reescriben, excepto HTML, Javascript y CSS (por ejemplo, Flash, Java Applet, Microsoft Silverlight, PDF, XML, etc.)*
- *Otras tecnologías (por ejemplo, Microsoft Silverlight o XML/XSLT)*
- *Cualquier codificación de contenido (por ejemplo, `Accept-Encoding: gzip, defalte, br`)*

Tecnología	Versión compatible

Tecnologías de aplicaciones web	• HTML
	• HTML5
	• HTML5-Web-Sockets
	• Javascript ES5 o anterior
	• RDP, VNC o SSH
	  • Los entornos de infraestructura de escritorio virtual (Virtual Desktop Infrastructure, VDI) y máquina virtual (Virtual Machine, VM), como Citrix XenApp y XenDesktop o VMWare Horizon y Vcenter, admiten el acceso nativo a través de HTML5. Puede usar RDP, VNC o SSH con estas máquinas a través de VPN sin cliente sin necesidad de un software intermedio externo adicional.
	  • En entornos que no incluyen soporte nativo para HTML5 u otra tecnología de aplicación web compatible con VPN sin cliente, puede usar proveedores externos, como HOBLink o Thinfinity, para el RDP a través de VPN sin cliente.
	• Adobe Flash: con Clientless VPN, los navegadores pueden mostrar contenido que utiliza Adobe Flash, documentos de Microsoft Word o documentos PDF de Adobe. No obstante, como Clientless VPN no puede reescribir las URL ni los enlaces HTML en ninguno de ellos, es posible que el contenido no se muestre correctamente.

Sistemas operativos	• Windows • macOS • iOS • Android • Chrome

© 2020 Palo Alto Networks, Inc.

Tecnología	Versión compatible
	• Linux
Navegadores compatibles	• Chrome • Perímetro • Internet Explorer • Safari • Firefox

© 2020 Palo Alto Networks, Inc.

Configuración de VPN sin cliente

Para configurar la VPN sin cliente de GlobalProtect:

STEP 1 | Antes de comenzar:

- Instale una suscripción de GlobalProtect en el cortafuegos que aloja la VPN sin cliente desde el portal de GlobalProtect. Consulte Licencias y suscripciones activas.
- Instale la última actualización dinámica de VPN sin cliente de GlobalProtect (consulte Instalación de las actualizaciones de contenido y software) y establezca una programación para instalar nuevas actualizaciones de contenido dinámico. Como práctica recomendada, se recomienda instalar siempre las últimas actualizaciones de contenido para la VPN sin cliente de GlobalProtect.

GlobalProtect Clientless VPN	Last checked: 2016/11/09 17:03:03 PST			Schedule: Every hour (Download and Install)		
58-11	panup-all-gp-58-11.candidate	GlobalProtectCli...	Full	75 KB	2016/11/07 18:57:21 PST	✔
58-10	panup-all-gp-58-10.candidate	GlobalProtectCli...	Full	74 KB	2016/10/25 17:51:17 PDT	✔ previously

- Se recomienda configurar un FQDN por separado para el portal de GlobalProtect que aloja la VPN sin cliente. No use el mismo FQDN que la interfaz web PAN-OS.
- Aloje el portal de GlobalProtect en el puerto SSL estándar (puerto TCP 443). Los puertos no estándar no son compatibles.

STEP 2 | Configure las aplicaciones que están disponibles con la VPN sin cliente de GlobalProtect. El portal de GlobalProtect muestra estas aplicaciones en la página de inicio que los usuarios ven cuando inician sesión (la página de inicio de las aplicaciones).

1. Seleccione **Network (Red)** > **GlobalProtect** > **Clientless Apps (Aplicaciones sin cliente)** y haga clic en **Add (Añadir)** para añadir una o más aplicaciones. Para cada aplicación, especifique la siguiente información:
   - **Name (Nombre)**: un nombre descriptivo para la aplicación (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
   - **Location (Ubicación)** (en el caso de un cortafuegos que esté en modo de Sistema virtual múltiple: el sistema virtual (vsys) en el que la VPN sin cliente está disponible. Si el cortafuegos no está en el modo de varios sistemas virtuales, no aparece el campo **Location (Ubicación)**.
   - **Application Home URL (URL de inicio de la aplicación)**: La URL en la que se encuentra la aplicación web (hasta 4,095 caracteres).
   - **Application Description (Descripción de la aplicación)** (Opcional): una descripción breve de la aplicación (hasta 255 caracteres).
   - **Application Icon (Icono de la aplicación)** (Opcional): un icono para identificar la aplicación en la página de la aplicación publicada. Puede examinar el contenido del disco para cargar el icono.
2. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Cree grupos para administrar conjuntos de aplicaciones web.

Los grupos de aplicaciones sin cliente son útiles si desea gestionar varias colecciones de aplicaciones y proporcionar acceso en función de grupos de usuarios. Por ejemplo, las aplicaciones financieras para el equipo de G&A o aplicaciones de desarrollador para el equipo de ingeniería.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Clientless App Groups (Grupos de aplicaciones sin cliente)**. Haga clic en **Add (Añadir)** para añadir un grupo nuevo de Clientless VPN y especifique los valores siguientes:

© 2020 Palo Alto Networks, Inc.

- **Name (Nombre)**: un nombre descriptivo para el grupo de aplicaciones (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
- **Location (Ubicación)** (en el caso de un cortafuegos que esté en modo de Sistema virtual múltiple: el sistema virtual (vsys) en el que el grupo de aplicaciones de VPN sin cliente está disponible. Si el cortafuegos no está en el modo de varios sistemas virtuales, no aparece el campo **Location (Ubicación)**.

2. En la sección **Applications (Aplicaciones)**, haga clic en **Add (Añadir)** para añadir aplicaciones al grupo. Puede seleccionar de la lista de aplicaciones de VPN sin cliente existentes o definir una **New Clientless App (Nueva aplicación sin cliente)**.
3. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure el portal de GlobalProtect para proporcionar el servicio VPN sin cliente.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portal (Portal)** y seleccione una configuración de portal existente o haga clic en **Add (Añadir)** para añadir una nueva. Consulte Configuración del acceso al portal de GlobalProtect.
2. En la pestaña **Authentication (Autenticación)**, puede:
   - (Opcional) Crear una nueva autenticación de cliente específica para la VPN sin cliente. En este caso, seleccione **Browser (Navegador)** como el **OS (SO)** para la **Client Authentication (Autenticación de cliente)**.
   - Utilice una autenticación de cliente existente.
3. En **Clientless (Sin cliente)** > **General**, seleccione **Clientless VPN (VPN sin cliente)** para habilitar el servicio del portal y configurar lo siguiente:
   - En **Hostname (Nombre de host)**, especifique la dirección IP o el FQDN del portal de GlobalProtect que aloja la página de destino de las aplicaciones. Este nombre de host se utiliza para reescribir las URL de las aplicaciones. (Para obtener más información sobre la reescritura de URL, consulte el paso 8).

     Si utiliza Network Address Translation (NAT) para proporcionar acceso al portal GlobalProtect, la dirección IP o FQDN que introduzca debe coincidir (o resolverse) con la dirección IP NAT del portal GlobalProtect (la dirección IP pública). Debido a que los usuarios no pueden acceder al portal de GlobalProtect en un puerto personalizado, el puerto previo a la NAT también debe ser el puerto TCP 443.

   - Especifique una **Security Zone (Zona de seguridad)**. Esta zona se utiliza como zona de origen para el tráfico entre el cortafuegos y las aplicaciones. Las reglas de seguridad definidas desde esta zona para la zona de aplicaciones condicionan las aplicaciones a las que pueden acceder los usuarios.
   - Seleccione un servidor **DNS Proxy (Proxy de DNS)** o configure una **New DNS Proxy (Proxy DNS nuevo)** GlobalProtect utilizará este proxy para resolver los nombres de aplicaciones. Consulte, Objeto proxy DNS.
   - **Login Lifetime (Duración de sesión)**: especifique el número máximo de horas o minutos durante los que es válida la sesión de Clientless VPN. El periodo de tiempo de una sesión normal es 3 horas. El intervalo de horas es de 1 a 24 y el de minutos, de 60 a 1440. Después de que la sesión caduque, los usuarios deben volver a autenticarse e iniciar una nueva sesión VPN sin cliente.
   - **Inactivity Timeout (Tiempo de espera de inactividad)**: especifique el número máximo de horas o minutos durante los que puede permanecer inactiva la sesión de Clientless VPN. El tiempo de inactividad típico es de 30 minutos. El intervalo de horas es de 1 a 24 y el de minutos, de 5 a 1440. Si no se produce ninguna actividad durante el período especificado, los usuarios deben volver a autenticarse e iniciar otra sesión de Clientless VPN.
   - **Max User (Máximo de usuarios)**: especifique el número máximo de usuarios que puede tener una sesión abierta en el portal a la vez. Si no se especifica ningún valor, se supone la capacidad del endpoint. Si la capacidad del endpoint no es conocida, se presupone una capacidad de

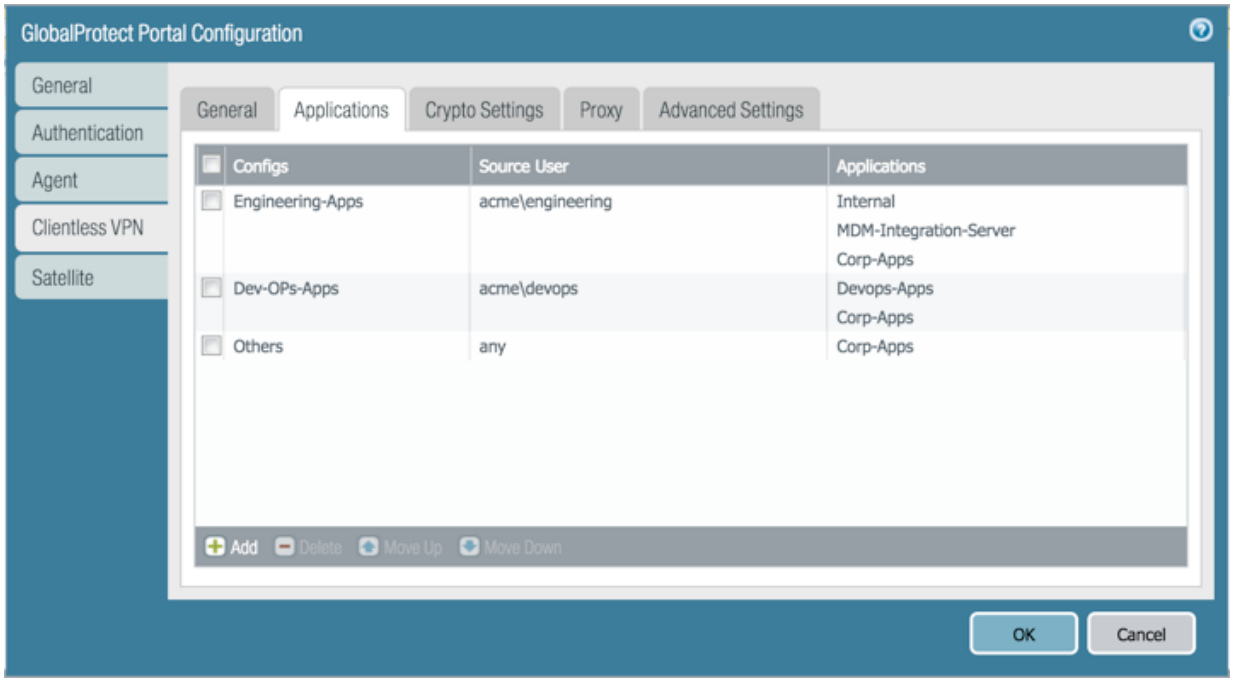
© 2020 Palo Alto Networks, Inc.

50 usuarios. Cuando se alcanza el número máximo de usuarios, los usuarios VPN sin cliente adicionales no pueden iniciar sesión en el portal.

STEP 5 | Asigna usuarios y grupos de usuarios a las aplicaciones.

Esta asignación controla qué aplicaciones pueden iniciar los usuarios o los grupos de usuarios desde una sesión VPN sin cliente de GlobalProtect.

El portal de GlobalProtect usa la configuración de usuario/grupo de usuarios que usted especifica para determinar qué configuración se distribuirá a los usuarios de VPN sin cliente de GlobalProtect que se conecten. Si tiene varias configuraciones, colóquelas en el orden correcto y asígnelas a todas las aplicaciones pertinentes. El portal empieza por el principio de la lista cuando busca coincidencias. En cuanto encuentra una coincidencia, proporciona la configuración asociada al usuario de GlobalProtect Clientless VPN.



La publicación de una aplicación a un usuario/grupo de usuarios o el permiso para iniciar aplicaciones no publicadas no implica que puedan acceder a esas aplicaciones. Las políticas de seguridad permiten controlar el acceso a las aplicaciones tanto si están publicadas como si no.

Debe configurar la asignación de grupo (Device (Dispositivo) > User Identification (Identificación de usuario) > Group Mapping Settings (Configuración de asignación de grupo)) antes de poder seleccionar los grupos.

1. En la pestaña **Applications (Aplicaciones)**, haga clic en **Add (Añadir)** para añadir **Applications to User Mapping (Aplicaciones a la asignación de usuarios)** para buscar coincidencias de usuarios con aplicaciones publicadas.
   - **Name (Nombre)**: introduzca un nombre para asignación (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
   - **Display application URL address bar (Mostrar la barra de direcciones URL de aplicaciones)**: seleccione esta opción para mostrar una barra de direcciones URL de aplicaciones desde la que los usuarios pueden iniciar aplicaciones que no están publicadas en la página de inicio de aplicaciones. Si habilita esta opción, los usuarios pueden seleccionar un valor en **Application URL (URL de aplicación)**.

© 2020 Palo Alto Networks, Inc.

2. Especificar los **Source Users (Usuarios de origen)**. Puede añadir usuarios individuales o grupos de usuarios con **Add (Añadir)**, a los cuales se aplique la configuración de aplicación actual. Estos usuarios tienen permiso para iniciar las aplicaciones configuradas con una VPN sin cliente de GlobalProtect. Además de los usuarios y grupos, puede usar el menú desplegable para especificar cuando esta configuración se aplique a los usuarios o grupos:
   - **any (cualquiera)**: la configuración de la aplicación se aplica a todos los usuarios (no es necesario **Add (Añadir)** usuarios o grupos de usuarios).
   - **select (seleccionar)**: la configuración de la aplicación se aplica solo a usuarios y grupos de usuarios que usted añade a esta lista con **Add (Añadir)**.
3. **Add (Añadir)** aplicaciones individuales o grupos de aplicaciones a la asignación. Los **Source Users (Usuarios de origen)** que incluyó en la configuración pueden utilizar la VPN sin cliente de GlobalProtect para unirse a las aplicaciones que añade.

STEP 6 | Especifique la configuración de seguridad para una sesión VPN sin cliente.

1. En la pestaña **Crypto Settings (Ajustes criptográficos)**, especifique los algoritmos de autenticación y cifrado para las sesiones SSL entre el cortafuegos y las aplicaciones publicadas.
   - **Protocol Versions (Versiones del protocolo)**: seleccione las versiones TLS / SSL mínimas y máximas requeridas. Cuanto mayor sea la versión TLS, más segura será la conexión. Las opciones incluyen **SSLv3**, **TLSv1.0**, **TLSv1.1**, o **TLSv1.2**.

     La versión máxima de TLS compatible con VPN sin cliente es TLSv1.2. TLSv1.3 no es compatible actualmente con conexiones VPN sin cliente.
   - **Key Exchange Algorithms (Algoritmos de intercambio de claves)**: seleccione los tipos de algoritmos soportados para el intercambio de claves. Las opciones son: **RSA**, Diffie-Hellman (**DHE**), o Curva Elíptica Efímera Diffie-Hellman (**ECDHE**).
   - **Encryption Algorithms (Algoritmos de cifrado)**: seleccione los algoritmos de cifrado soportados. Se recomienda **AES128** o un cifrado más seguro.
   - **Authentication Algorithms (Algoritmos de autenticación)**: seleccione los algoritmos de autenticación soportados. Las opciones son: **MD5**, **SHA1**, **SHA256** y **SHA384**. Se recomienda **SHA256** o superior.
2. Seleccione la acción a tomar cuando se produzcan los siguientes problemas con un certificado de servidor presentado por una aplicación:
   - **Block sessions with expired certificate (Bloquear sesiones con certificado caducado)**: si el certificado del servidor ha caducado, bloquee el acceso a la aplicación.
   - **Block sessions with untrusted issuers (Bloquear sesiones con emisores no fiables)**: si el certificado de servidor se emite desde una autoridad con certificado no fiable, bloquee el acceso a la aplicación.
   - **Block sessions with unknown certificate status (Bloquear sesiones con estado de certificado desconocido)**: si el servicio OCSP o CRL devuelve el estado de revocación de certificado `desconocido`, bloquear el acceso a la aplicación.
   - **Block sessions on certificate status check timeout (Bloquear sesiones en el tiempo de espera de comprobación de estado del certificado)**: si la comprobación del estado del certificado se agota antes de recibir una respuesta de cualquier servicio de estado del certificado, bloquee el acceso a la aplicación.

STEP 7 | (Opcional) Especifique una o más configuraciones de servidor proxy para acceder a las aplicaciones.

Solo se admite la autenticación básica del proxy (nombre de usuario y contraseña).

© 2020 Palo Alto Networks, Inc.

Si los usuarios necesitan llegar a las aplicaciones a través de un servidor proxy, especifique un **Proxy Server (Servidor proxy)**. Puede añadir múltiples configuraciones de servidor proxy, una para cada conjunto de dominios.

- **Name (Nombre)**: una etiqueta (de hasta 31 caracteres) para identificar la configuración del servidor proxy. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
- **Domains (Dominios)**: agrega los dominios servidos por el servidor proxy. Puede usar un carácter comodín (*) al comienzo del nombre de dominio para indicar varios dominios.
- **Use Proxy (Usar proxy)**: seleccione asignar un servidor proxy para proporcionar acceso a los dominios.
- **Server (Servidor)**: especifique la dirección IP o el nombre de host del servidor proxy.
- **Port (Puerto)**: especifica un puerto para la comunicación con el servidor proxy.
- **User (Usuario)** y **Password (Contraseña)**: especifica el **User (Usuario)** y **Password (Contraseña)** necesarios para iniciar sesión en el servidor proxy. Especifica la contraseña nuevamente para verificación.

STEP 8 | (Opcional) especifique cualquier tratamiento especial para los dominios de aplicaciones.

La VPN sin cliente actúa como un proxy inverso y modifica las páginas web devueltas por las aplicaciones web publicadas. Reescribe todas las URL y presenta una página reescrita a los usuarios remotos. Cuando estos acceden a cualquiera de esas URL, las solicitudes pasan por el portal de GlobalProtect.

En algunos casos, la aplicación puede tener páginas a las que no es necesario acceder a través del portal (por ejemplo, la aplicación puede incluir un símbolo bursátil de yahoo.finance.com). Puede excluir estas páginas.

En la pestaña **Advanced Settings (Configuración avanzada)**, haga clic en **Add (Añadir)** para añadir nombres de dominio, nombres de host o direcciones IP a **Rewrite Exclude Domain List (Lista de dominios de exclusión de reescritura)**. Estos dominios se excluyen de las reglas de reescritura y no se pueden volver a escribir.

No se pueden especificar rutas en los nombres de host ni los nombres de dominio. El carácter comodín (*) de los nombres de host y de dominio solo puede aparecer al principio, por ejemplo, *.comerciovirtual.es.

STEP 9 | Guarde la configuración del portal.

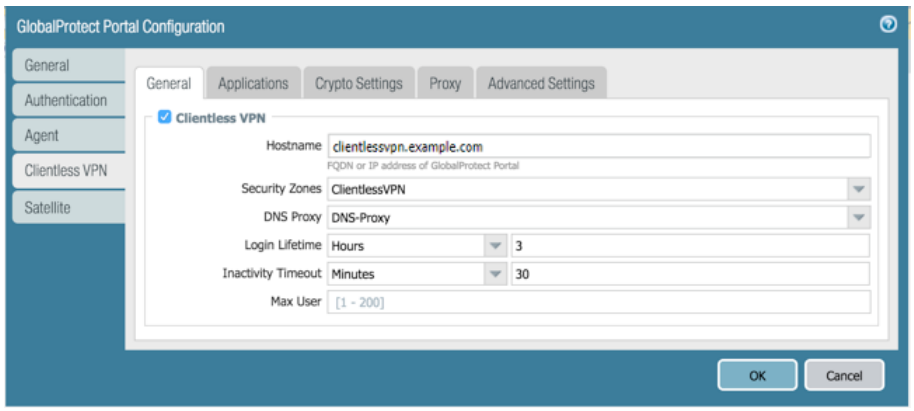
1. Haga clic en **OK** dos veces.
2. **Commit (Confirmar)** los cambios.

STEP 10 | Configure una Regla de política de seguridad para permitir a los usuarios acceder a las aplicaciones publicadas.

Necesita políticas de seguridad para lo siguiente:

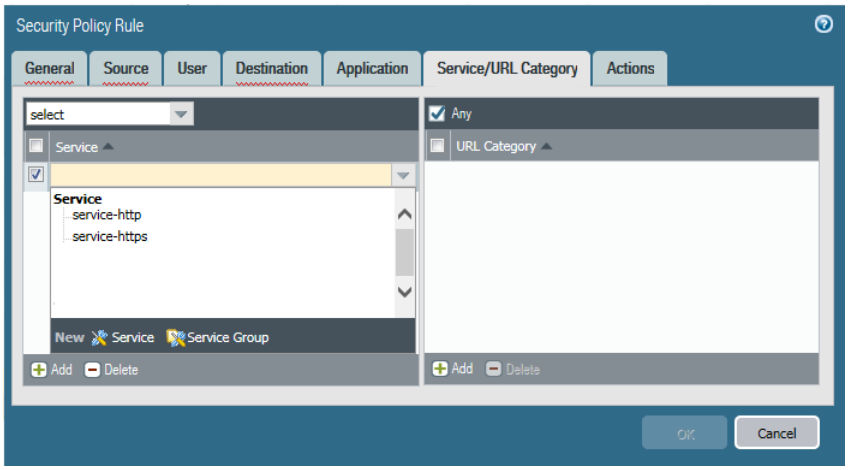
- Facilitar el acceso desde internet al portal de GlobalProtect que aloja Clientless VPN. Este es el tráfico que proviene de la zona de Internet o no fiable a la zona donde aloja el portal de VPN sin cliente.
- Permitir el acceso a internet de los usuarios de Clientless VPN. Este es el tráfico de la zona de VPN sin cliente a la zona de Internet o Untrust.

© 2020 Palo Alto Networks, Inc.



- Permitir que los usuarios de VPN sin cliente accedan a los recursos corporativos. Este es el tráfico de la zona de VPN sin cliente a la zona Corp o Trust. Las políticas de seguridad que usted defina controlan qué usuarios tienen permiso para usar cada aplicación publicada. En la zona de seguridad donde se alojan los servidores de aplicaciones publicadas, marque **Enable User Identification (Habilitar identificación de usuarios)**.

  El campo **Service/URL (Servicio/URL)** de **Security Policy Rule (Regla de política de seguridad)** está definido en **application-default (valor predeterminado para la aplicación)** de forma predeterminada. La VPN sin cliente no funcionará para sitios HTTPS con esta configuración predeterminada. Cambie **Service/URL (Servicio/URL)** para incluir ambos **service-http** y **service-https**.



- Cuando configura un servidor proxy para acceder a las aplicaciones de VPN sin cliente, asegúrese de incluir la dirección IP y el puerto del proxy en la definición de la política de seguridad. Cuando se accede a las aplicaciones a través de un servidor proxy, solo se aplican las políticas de seguridad definidas para la dirección IP y el puerto del proxy.

STEP 11 | (Opcional) Configure la página de destino del portal de Clientless VPN de modo que muestre la ubicación del portal a la que se conectan los usuarios de Clientless VPN. Para ello, especifique la ubicación física del cortafuegos en el que ha configurado el portal.

Si se produce un comportamiento inusual, como un rendimiento deficiente de la red, los usuarios de Clientless VPN pueden facilitar la ubicación a los profesionales del servicio de asistencia, que les resulta útil para solucionar el problema. Ese dato también permite determinar la proximidad al portal para evaluar si es preciso cambiar a otro portal más cercano.

Si no especifica la ubicación del portal, la página de destino del portal de Clientless VPN muestra este campo vacío.

© 2020 Palo Alto Networks, Inc.

- **En la interfaz de línea de comandos (command-line interface, CLI)**: utilice el siguiente comando de la CLI para especificar la ubicación física del cortafuegos en el que ha configurado el portal:

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- **En la interfaz de programación de aplicaciones (application programming interface, API) con lenguaje de marcado extensible (extensible markup language, XML)**: utilice el siguiente comando de la API XML para especificar la ubicación física del cortafuegos en el que ha configurado el portal:
  - **devices (dispositivos)**: nombre del cortafuegos en el que ha configurado el portal.
  - **location (ubicación)**: ubicación del cortafuegos en el que ha configurado el portal.

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

La dirección IP de origen del tráfico de Clientless VPN (tal como se detecta en la aplicación) es la dirección IP de la interfaz de salida por la cual accede el portal a la aplicación o la dirección IP traducida cuando se usa la NAT de origen.

© 2020 Palo Alto Networks, Inc.

Solución de problemas de VPN sin cliente

Debido a que esta característica implica la reescritura dinámica de aplicaciones HTML, es posible que el contenido HTML de algunas aplicaciones no se vuelva a escribir correctamente y se rompa la aplicación. Si se producen problemas, use los comandos en la siguiente tabla para poder identificar la causa probable:

Table 6: Tabla: Reescribir las estadísticas del motor

Acción	Comando
Comandos de la CLI	
Enumere la versión del contenido dinámico de VPN sin cliente que se está utilizando También puede ver la versión de la actualización dinámica desde **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas) > GlobalProtect Clientless VPN (VPN sin cliente de GlobalProtect)**.	**show system setting ssl-decrypt memory** proxy uses shared allocator SSL certificate cache: Current Entries: 1 Allocated 1, Freed 0 Current CRE (61-62) : 3456 KB (Actual 3343 KB) Last CRE (60-47) : 3328 KB (Actual 3283 KB) En este ejemplo, la actualización dinámica actual es la versión 61-62, y la última actualización dinámica instalada es la versión 60-47.
Listar usuarios activos (actuales) de VPN sin cliente	**show global-protect-portal current-user portal GPClientlessPortal filter-user all-users** GlobalProtect Portal : GPClientlessPortal Vsys-Id : 1 User : paloaltonetworks.com\johndoe Session-id : 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0 Client-IP : 5.5.5.5 Inactivity Timeout : 1800 Seconds before inactivity timeout : 1750 Login Lifetime : 10800 Seconds before login lifetime : 10748 Total number of user sessions: 1
Mostrar resultados de resolución DNS Esto puede ser útil para determinar si hay	**show system setting ssl-decrypt dns-cache** Total DNS cache entries: 89

© 2020 Palo Alto Networks, Inc.

Acción	Comando

problemas de DNS. Si hay un problema de DNS, observará consultas en un FQDN que no se pudo resolver en el resultado de la CLI.	`Site  IP  Expire(secs)`
	`  Interface`
	`bugzilla.panw.local  10.0.2.15  querying`
	`  0`
	`www.google.com  216.58.216.4  Expired`
	`  0`
	`stats.g.doubleclick.net  74.125.199.154  Expired`
	`  0`

Mostrar todas las sesiones de usuario de VPN sin cliente y las cookies almacenadas	**`show`**
	`system setting ssl-decrypt gp-cookie-cache`
	
	`User: johndoe, Session-id:`
	`  1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0,`
	`Client-ip: 199.167.55.50`

Mostrar las estadísticas de reescritura
 	
Esto es útil para identificar el estado del motor de reescritura de la VPN sin cliente.
 	
Consulte Solución de problemas de VPN sin cliente para obtener información sobre las estadísticas de reescritura y su significado o propósito.
	`show system setting ssl-decrypt rewrite-stats`
	
	`Rewrite Statistics`
	`  initiate_connection  : 11938`
	`  setup_connection  : 11909`
	`  session_notify_mismatch  : 1`
	`  reuse_connection  : 37`
	`  file_end  : 4719`
	`  packet  : 174257`
	`  packet_mismatch_session  : 1`
	`  peer_queue_update_rcvd  : 167305`
	`  peer_queue_update_sent  : 167305`
	`  peer_queue_update_rcvd_failure: 66`
	`  setup_connection_r  : 11910`
	`  packet_mismatch_session_r  : 22`
	`  pkt_no_dest  : 23`
	`  cookie_suspend  : 2826`
	`  cookie_resume  : 2826`
	`  decompress  : 26`
	`  decompress_freed  : 26`
	`  dns_resolve_timeout  : 27`
	`  stop_openend_response  : 43`
	`  received_fin_for_pending_req  : 26`
	`Destination Statistics`
	`  To mp  : 4015`
	`  To site  : 12018`
	`  To dp  : 17276`
	`Return Codes Statistics`
	`  ABORT  : 18`
	`  RESET  : 30`
	`  PROTOCOL_UNSUPPORTED  : 7`
	`  DEST_UNKNOWN  : 10`
	`  CODE_DONE  : 52656`
	`  DATA_GONE  : 120359`
	`  SWITCH_PARSER  : 48`
	`  INSERT_PARSER  : 591`
	`  SUSPEND  : 2826`
	`  Total Rewrite Bytes  : 611111955`
	`  Total Rewrite Useconds  : 6902825`

© 2020 Palo Alto Networks, Inc.

Acción	Comando
	`Total Rewrite Calls : 176545`
Comandos de depuración	
Habilite los logs de depuración en el cortafuegos que el portal de VPN sin cliente	**`debug dataplane packet-diag set log feature ssl all`** **`debug dataplane packet-diag set log feature misc all`** **`debug dataplane packet-diag set log feature proxy all`** **`debug dataplane packet-diag set log feature flow basic`** **`debug dataplane packet-diag set log on`**
Habilitar la captura de paquetes en el cortafuegos que ejecuta el portal de Clientless VPN	**`debug dataplane packet-diag set capture username <portal-username>`** **`debug dataplane packet-diag set capture stage clientless-vpn-client file <clientless-vpn-client-file>`** **`debug dataplane packet-diag set capture stage clientless-vpn-server file <clientless-vpn-server-file>`** **`debug dataplane packet-diag set capture stage firewall file <firewall-file>`** **`debug dataplane packet-diag set capture stage receive file <receive-file>`** **`debug dataplane packet-diag set capture stage transmit file <transmit-file>`** **`debug dataplane packet-diag set capture on`** *Si ejecuta los comandos de captura de paquetes, después de que los usuarios inicien sesión en el portal de Clientless VPN, aparece una página de autorización para informarles de que los paquetes capturados durante su sesión contendrán datos de texto sin cifrar. Si los usuarios confirman su autorización, acceden a la página de destino de las aplicaciones, donde se empiezan a capturar paquetes. Si no lo autorizan, se cierra la sesión en el portal de Clientless VPN. Para continuar con una sesión normal, sin captura de paquetes, se deben poner en contacto con un administrador.* *Si ejecuta los comandos de captura de paquetes en las sesiones que ya están en curso, se cierra automáticamente la sesión en el portal de Clientless VPN de esos usuarios, que deben iniciar sesión de nuevo para aceptar o declinar la captura.*

Mostrar archivos de captura de paquetes	**`debug dataplane packet-diag show setting`**
	`---------- Packet diagnosis setting: ----------`
	`Packet filter`
	`Enabled: no`
	`Match pre-parsed packet: no`
	`---------- Logging`
	`Enabled: no`

© 2020 Palo Alto Networks, Inc.

Acción	Comando

	`Log-throttle: no`
	`Sync-log-by-ticks: yes`
	`Features:`
	`Counters:`
	`----------`
	`Packet capture`
	`Enabled: yes`
	`Snaplen: 0`
	`Username: test1`
	`Stage clientless-vpn-client: file client.pcap`
	`  Captured: packets - 3558  bytes - 11366322`
	`  Maximum: packets - 0  bytes - 0`
	`Stage clientless-vpn-server: file server.pcap`
	`  Captured: packets - 1779  bytes - 5651923`
	`  Maximum: packets - 0  bytes - 0`
	`----------`

Exportar archivos de captura de paquetes a servidores del protocolo de copia segura (secure copy protocol, SCP)	**`scp export filter-pcap`**
	`+ remote-port SSH port number on remote host`
	`+ source-ip Set source address to specified interface address`
	`* from  from`
	`* to  Destination (username@host:path)`
	
	`scp export filter-pcap from` ***`<source-file>`*** `to <scp-server> Destination (username@host:path)`

Table 7: Tabla: Reescribir las estadísticas del motor

Estadística	Description (Descripción)
initiate_connection_failure	El inicio de la conexión no logró respaldar el host
setup_connection_failure	Error de configuración de conexión
setup_connection_duplicate	Existe una sesión peer duplicada
session_notify_mismatch	Sesión prácticamente no válida
packet_mismatch_session	Error al encontrar la sesión correcta para el paquete entrante
peer_queue_update_rcvd_failure	La sesión no se validó cuando el peer recibió la actualización del paquete
peer_queue_update_sent_failure	Error al enviar actualizaciones de paquetes a los peers o no pudo enviar al peer las actualizaciones de longitud de cola del paquete
exceed_pkt_queue_limit	Demasiados paquetes en cola
proxy_connection_failure	Fallo de conexión proxy

© 2020 Palo Alto Networks, Inc.

Estadística	Description (Descripción)
setup_connection_r	Instalación de la sesión de peer en el servidor de aplicaciones. Este valor debe coincidir con los valores de **`initiate_connection`** y **`setup_connection`**.
setup_connection_duplicate_r	Ya existen sesiones duplicadas en el proxy
setup_connection_failure_r	Error al configurar la sesión de peer
session_notify_mismatch_r	No se encontró la sesión de peer
packet_mismatch_session_r	No se encontró la sesión de peer al intentar obtener el paquete
exceed_pkt_queue_limit_r	Demasiados paquetes retenidos
unknown_dest	Error al encontrar el host de destino
pkt_no_dest	No existe destino para este paquete
cookie_suspend	Sesión suspendida para recuperar cookies
cookie_resume	Recibió respuesta de MP con las cookies actualizadas. Este valor generalmente coincide con el valor de cookie_suspend.
descompress_failure	Error al descomprimir
memory_alloc_failure	Error al asignar memoria
wait_for_dns_resolve	Sesión suspendida para resolver solicitudes DNS
dns_resolve_reschedule	Consulta de DNS reprogramada por falta de respuesta (vuelva a intentar antes del tiempo de espera)
dns_resolve_timeout	Tiempo de espera de consulta de DNS.
setup_site_conn_failure	Error al configurar la conexión al sitio web (proxy, DNS)
site_dns_invalid	Error de resolución DNS
multiple_multipart	Tipo de contenido multiparte procesado
site_from_referer	Recibió el host de back-end del sitio de referencia. Esto puede indicar enlaces de reescritura fallidos de flash u otro contenido que la VPN sin cliente no reescribe.
received_fin_for_pending_req	Recibió FIN del servidor para la solicitud pendiente del cliente
unmatched_http_state	Contenido HTTP inesperado. Esto puede indicar un problema al analizar los encabezados o el cuerpo http.

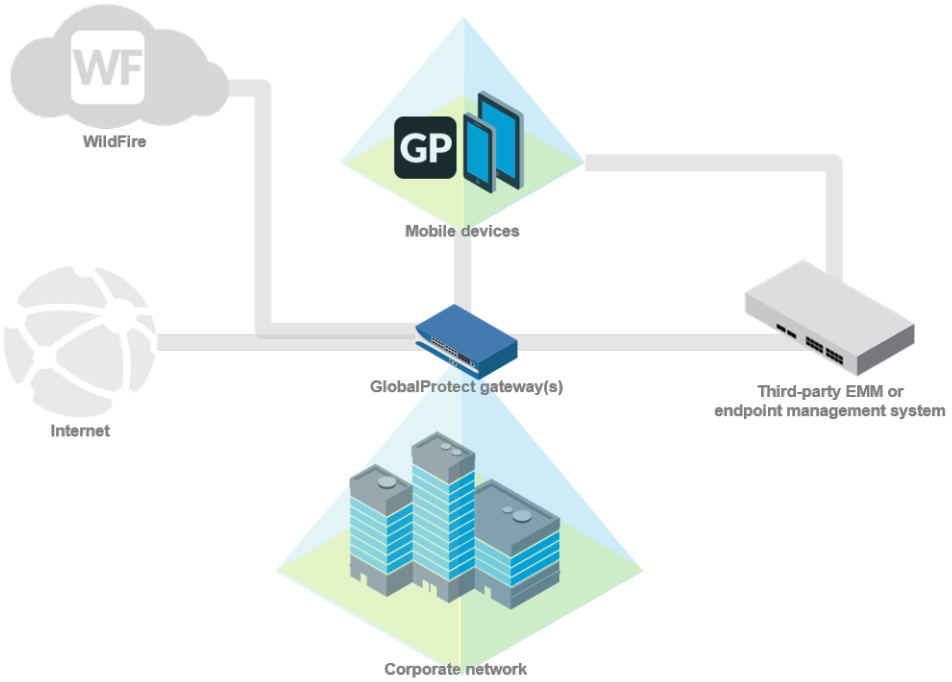
Gestión de dispositivos móviles

> Descripción general de la gestión de dispositivos móviles
> Configuración de la integración de MDM con GlobalProtect

© 2020 Palo Alto Networks, Inc.

Descripción general de la gestión de dispositivos móviles

Los endpoints móviles son cada vez más potentes, por lo que los usuarios finales confían cada vez más en ellos para realizar sus tareas comerciales. Sin embargo, usan los mismos terminales con los que acceden a la red empresarial para conectarse a internet sin protección contra amenazas y vulnerabilidades.



Si dispone de un sistema de gestión de dispositivos móviles (mobile device management, MDM) o un sistema de gestión de la movilidad empresarial (enterprise mobility management, EMM), le resulta más fácil administrar los terminales móviles, ya que puede implementar automáticamente la configuración empresarial para las cuentas y la red privada virtual (virtual private network, VPN) en los terminales que cumplen los requisitos. También puede usar su sistema de gestión de dispositivos móviles para solucionar los fallos de seguridad al interactuar con un endpoint que está en peligro. De este modo se logra proteger tanto la información de la empresa con la información personal del usuario final. Por ejemplo, si un usuario final pierde un endpoint, usted puede bloquear remotamente el endpoint desde el sistema de gestión de dispositivos móviles o incluso limpiar el endpoint (ya sea por completo o de manera selectiva).

Además de las funciones de gestión de dispositivos remotos y el aprovisionamiento de cuentas que puede brindar un sistema de gestión de dispositivos móviles, cuando se integra con su infraestructura VPN existente de GlobalProtect™, puede usar la información del host que el endpoint registra para aplicar políticas de seguridad para el acceso a las aplicaciones mediante la puerta de enlace de GlobalProtect. También puede usar las herramientas de control que están integradas al cortafuegos de última generación de Palo Alto para controlar el tráfico de los endpoints móviles.

Integración de GlobalProtect con sistemas de MDM o de EMM

Para integrar la implementación de GlobalProtect con sistemas de MDM o de EMM, siga uno de estos métodos:

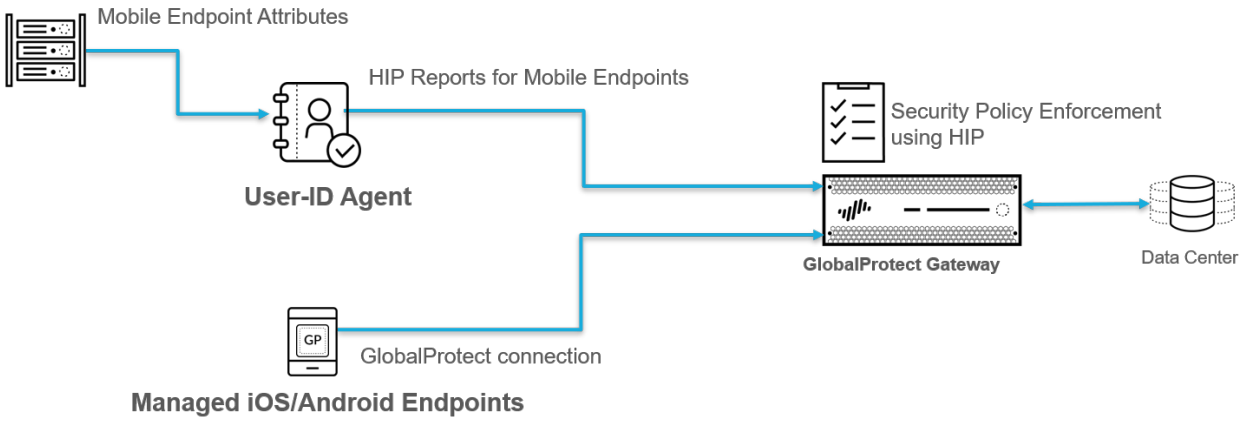
© 2020 Palo Alto Networks, Inc.

Integración de cortafuegos con sistemas de MDM o de EMM (solo en AirWatch)

Configure el agente de User-ID para Windows de modo que se comunique con el servidor de MDM de AirWatch a fin de recopilar información sobre los hosts de los terminales conectados. El agente de User-ID envía esa información a la puerta de enlace de GlobalProtect como parte del informe sobre perfiles de información de hosts (host information profile, HIP) que permite aplicar las políticas basadas en HIP.

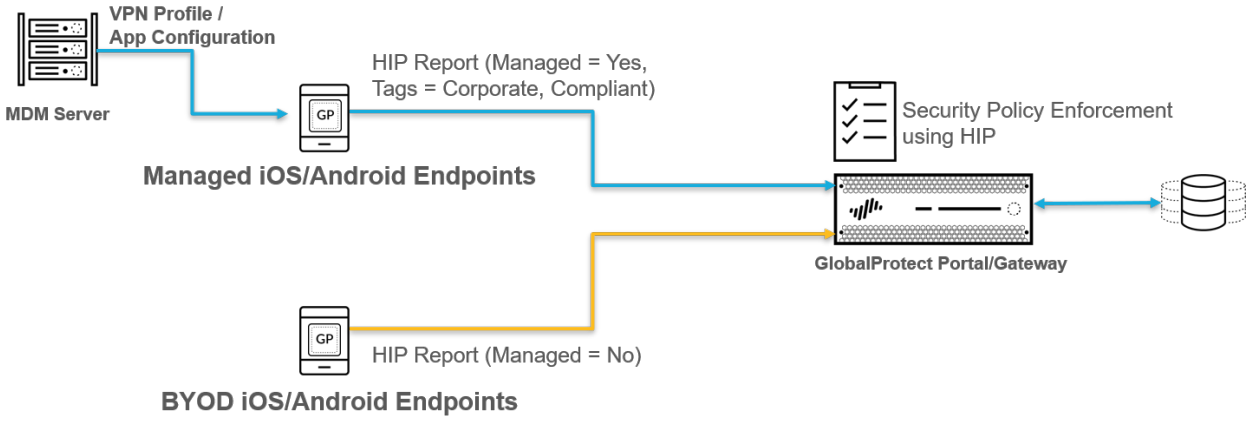
La integración de los cortafuegos se admite en PAN-OS 8.0 y en las versiones posteriores.

La integración de los cortafuegos solo se admite con VMware AirWatch.



Integración de aplicaciones de GlobalProtect con sistemas de MDM o de EMM

Desde la versión 5.0, la aplicación de GlobalProtect para terminales con iOS y Android puede obtener de los sistemas de MDM los atributos y las etiquetas de datos de los proveedores. En el caso de los terminales con iOS, los sistemas de MDM envían dichos atributos a la aplicación de GlobalProtect como parte del perfil de VPN y, en el caso de los terminales con Android, como parte de la configuración de restricciones de aplicaciones. Entonces, la aplicación de GlobalProtect envía los atributos y las etiquetas a la puerta de enlace de GlobalProtect como parte del informe de HIP que permite aplicar las políticas basadas en HIP.



Se admite la integración de aplicaciones de GlobalProtect con VMware AirWatch, MobileIron y Microsoft Intune. No obstante, este método de integración también es válido con cualquier

© 2020 Palo Alto Networks, Inc.

sistema de MDM o de EMM que admita atributos de datos de proveedores en el perfil de VPN.

En la tabla siguiente se describen los atributos de datos de proveedores admitidos:

Atributo de MDM	Atributo de informes de HIP	Categoría de informes de HIP	Description (Descripción)
`mobile_id`	**ID de host**	**General**	Identificador único de dispositivo (unique device identifier, UDID) del terminal.
`managed`	**Gestionado**	**General**	Valor que indica si se trata de un terminal gestionado: **Yes (Sí)** significa que lo es y **No**, que no lo es.
`compliance`	**Tag (Etiqueta)**	**Dispositivo móvil**	Estado que indica si el terminal acata las políticas de cumplimiento de MDM definidas, por ejemplo, **Compliant (Conforme)**. Este valor se anexa al atributo **Tag (Etiqueta)** del informe de HIP.
`ownership`	**Tag (Etiqueta)**	**Dispositivo móvil**	Categoría de propiedad del terminal, por ejemplo, **Employee Owned (Propiedad del empleado)**. Este valor se anexa al atributo **Tag (Etiqueta)** del informe de HIP.
`tag`	**Tag (Etiqueta)**	**Dispositivo móvil**	Etiquetas que se deben cotejar con otros atributos basados en MDM.

© 2020 Palo Alto Networks, Inc.

Configuración de la integración de MDM con GlobalProtect

Para configurar la integración de la gestión de dispositivos móviles (mobile device management, MDM) con GlobalProtect, realice este flujo de trabajo:

STEP 1 | Configuración de la infraestructura de GlobalProtect.

1. Creación de interfaces y zonas para GlobalProtect.
2. Habilitación de SSL entre componentes de GlobalProtect.
3. Configuración de la autenticación de usuario en GlobalProtect Consulte Acerca de la autenticación de usuarios de GlobalProtect.
4. Habilitación de la asignación de grupo.
5. Configuración de una puerta de enlace de GlobalProtect.
6. Active las licencias para cada cortafuegos que ejecuta una puerta de enlace que admite la aplicación de GlobalProtect en los endpoints móviles.
7. Configuración del acceso al portal de GlobalProtect.

STEP 2 | Configure el sistema de gestión de dispositivos móviles y decida si admitirá solo endpoints corporativos o tanto endpoints personales como corporativos.

Consulte las instrucciones de su sistema de gestión de dispositivos móviles (mobile device management, MDM) o sistema de gestión de movilidad empresarial (enterprise mobility management, EMM).

STEP 3 | Obtenga la aplicación de GlobalProtect para los endpoints móviles.

- App store: Descarga e instalación de la aplicación móvil de GlobalProtect
- Sistemas de gestión de dispositivos móviles compatibles: Implementación de la aplicación móvil de GlobalProtect
- Otro sistema de gestión de dispositivos móviles de terceros: consulte las instrucciones de su proveedor sobre cómo implementar aplicaciones en endpoints gestionados.

STEP 4 | Configure la integración de MDM.

Configure la integración de MDM con uno de los métodos siguientes:

- Integración del cortafuegos con un sistema de MDM o de EMM:
  - Configurar el agente de User-ID de Windows para recopilar información de host
- Integración de la aplicación de GlobalProtect con un sistema de MDM o de EMM:
  - Gestión de la aplicación de GlobalProtect con proveedores de MDM aptos
  - Gestión de la aplicación de GlobalProtect con MDM externo

STEP 5 | Configure las políticas dirigidas a los endpoints móviles usando información de host.

Configuración de la aplicación de políticas basadas en HIP para endpoints gestionados

Gestión de la aplicación de GlobalProtect con proveedores de MDM aptos

Consulte las siguientes secciones para obtener información sobre cómo implementar, configurar y gestionar la aplicación de GlobalProtect para terminales móviles con sistemas de MDM externos aptos:

© 2020 Palo Alto Networks, Inc.

- Proveedores de MDM aptos
- Implementación de la aplicación móvil de GlobalProtect
- Configuraciones de VPN siempre activada
- Configuraciones VPN de acceso remoto iniciada por el usuario
- Configuraciones VPN por aplicación
- Habilitación de la integración de análisis de aplicaciones con WildFire
- Supresión de notificaciones en la aplicación de GlobalProtect para endpoints de macOS

Si no utiliza ningún sistema de MDM externo apto, realice el procedimiento Gestión de la aplicación de GlobalProtect con MDM externo.

Proveedores de MDM aptos

En la tabla siguiente se enumeran los proveedores de gestión de dispositivos móviles (mobile device management, MDM) aptos a los que puede recurrir para configurar, implementar y gestionar la aplicación de GlobalProtect por sistema operativo. A: indica que el sistema operativo no es compatible.

Si desea usar otro proveedor, consulte Gestión de la aplicación de GlobalProtect con MDM externo

Proveedor de MDM compatible	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
AirWatch	✓ (VPN por aplicación únicamente)	✓	—	—	✓	—	—
Microsoft Intune	✓ (Solo Always On (Siempre activado), Acceso remoto (Remote Access) y Per-App VPN (VPN por aplicación))	✓	—	—	✓ (VPN siempre activada y por aplicación únicamente)	—	—
MobileIron	✓ (VPN siempre activada únicamente)	✓	—	—	—	—	—

© 2020 Palo Alto Networks, Inc.

Proveedor de MDM compatible	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Consola de gestión de Google	✓ (Compatibilidad con aplicaciones con Android en Chromebooks; solo para implementar aplicaciones)	–	✓ (Implementación de aplicaciones únicamente)	–	–	–	–

Puede usar la consola de gestión de Google únicamente para implementar la aplicación de GlobalProtect; no puede usar la consola para establecer configuraciones de VPN. Debe establecer la configuración de VPN en el portal de GlobalProtect antes de poder implementar la aplicación con la consola de gestión de Google.

Implementación de la aplicación móvil de GlobalProtect

La aplicación de GlobalProtect proporciona una forma sencilla de extender las políticas de seguridad de la empresa a los endpoints móviles. Al igual que con otros endpoints remotos que ejecutan la aplicación de GlobalProtect, la aplicación móvil brinda acceso seguro a su red corporativa por un túnel VPN SSL o IPsec. La aplicación se conectará a la puerta de enlace más cercana a la ubicación actual del usuario final. Además, el tráfico desde y hacia el endpoint móvil está automáticamente sujeto al cumplimiento de la misma política de seguridad que otros endpoints en su red corporativa. La aplicación también recopila información sobre la configuración del host y puede usarla para mejorar el cumplimiento de la política de seguridad basada en HIP.

Existen dos métodos principales para instalar la aplicación de GlobalProtect: Instale la aplicación directamente desde la tienda de aplicaciones para su endpoint (consulte Descarga e instalación de la aplicación móvil de GlobalProtect) o bien, implemente la aplicación desde un sistema de gestión de dispositivos móviles (como AirWatch) y envíe de forma transparente la aplicación a sus endpoints gestionados.

- Implementación de la aplicación móvil de GlobalProtect con AirWatch
- Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con AirWatch
- Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune
- Implementación de la aplicación móvil de GlobalProtect con MobileIron
- Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google

Implementación de la aplicación móvil de GlobalProtect con AirWatch

Puede implementar la aplicación de GlobalProtect en los endpoints gestionados que se inscribieron con AirWatch. Los endpoints que ejecutan iOS o Android deben descargar el agente de AirWatch para inscribirse con el MDM de AirWatch. Los endpoints de Windows 10 no requieren el agente de AirWatch, pero requieren que usted configure la inscripción en el endpoint. Después de implementar la aplicación,

© 2020 Palo Alto Networks, Inc.

configure e implemente un perfil VPN para configurar la aplicación de GlobalProtect para los usuarios finales de forma automática.

Si desea ejecutar la aplicación de GlobalProtect para Android en Chromebooks gestionados, realice el procedimiento Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con AirWatch.

STEP 1 | Antes de comenzar, asegúrese de que los endpoints en los cuales desea implementar la aplicación de GlobalProtect estén inscritos con AirWatch:

- **Android e iOS**: descargue el agente de AirWatch y siga los mensajes para inscribirse.
- **Teléfono Windows y Windows 10 UWP**: configure el endpoint Windows 10 UWP para inscribirse con AirWatch (desde el endpoint, seleccione **Settings (Ajustes)** > **Accounts (Cuentas)** > **Work access (Acceder a Work)** > **Connect (Conectar)**).

STEP 2 | Desde AirWatch, seleccione **APPS & BOOKS (Aplicaciones y libros)** > **Public (Público)** > **Add Application (Añadir aplicación)**.

STEP 3 | Seleccione el grupo de la organización mediante el cual se gestionará esta aplicación.

STEP 4 | Seleccione la **Platform (Plataforma)** (**Apple iOS**, **Android** o **Windows Phone**).

STEP 5 | Busque la aplicación de GlobalProtect en la tienda de aplicaciones del endpoint o introduzca una de las siguientes URL de la página de aplicaciones de GlobalProtect:

- **iOS Apple**: https://itunes.apple.com/us/app/globalprotect/id592489989?mt=8&uo=4
- **Android**: https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect
- **Windows Phone**: https://www.microsoft.com/en-us/p/globalprotect/9nblggh6bzl3

STEP 6 | Haga clic en **Next (Siguiente)**. Si buscó la aplicación en la tienda de aplicaciones del endpoint, también debe hacer clic en **Select (Seleccionar)** para elegir la aplicación de una lista de resultados de búsqueda.

Si buscó la aplicación de GlobalProtect para Android y no ve la aplicación en la lista, comuníquese con su administrador de Android for Work para añadir GlobalProtect a la lista de aplicaciones aprobadas de la empresa o use la URL de la aplicación en Google Play Store.

STEP 7 | En la pestaña **Assignment (Asignación)**, seleccione los **Assigned Smart Groups (Smart Groups asignados)** que tendrán acceso a esta aplicación.

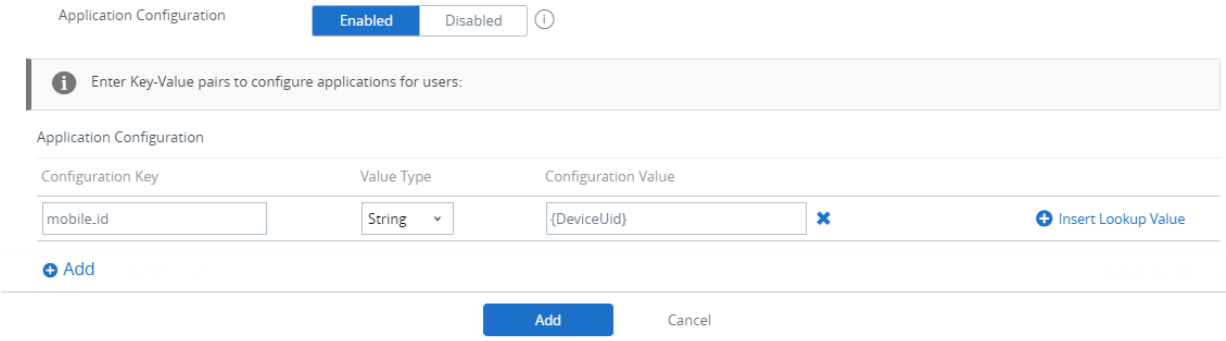
STEP 8 | Seleccione el **App Delivery Method (Méodo de envío de la aplicación)**. Este puede ser **Auto (Automático)** que envía la aplicación automáticamente al dispositivo u **On Demand (A demanda)**.

STEP 9 | (Solo en la aplicación de GlobalProtect para Android) Seleccione **Enable (Habilitar)** para permitir que la opción Application Configuration (Configuración de la aplicación) utilice el UDID para identificar el endpoint.

Añada el siguiente par de clave-valor:

- Clave de configuración: **`mobile_id`**
- Tipo de valor: **`String`**
- Valor de configuración: **`{DeviceUid}`**

© 2020 Palo Alto Networks, Inc.



STEP 10 | Seleccione **Save & Publish (Guardar y publicar)** para enviar el catálogo de aplicaciones a los endpoints de los Smart Groups que asignó en la sección **Assignment (Asignación)**.

Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con AirWatch

Desde la versión 5.0, puede implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados que están inscritos con AirWatch. Después de implementar la aplicación, configure e implemente un perfil VPN para configurar la aplicación de GlobalProtect para los usuarios finales de forma automática.

La aplicación de GlobalProtect para Android solo se admite en algunos Chromebooks. En los Chromebooks que no admiten aplicaciones para Android, debe seguir ejecutando la aplicación de GlobalProtect para Chrome, que no es compatible a partir de la aplicación de GlobalProtect 5.0 y posterior.

pero no puede implementar esta junto con la aplicación para Android en el mismo Chromebook.

Siga estos pasos para implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados con AirWatch:

STEP 1 | Configure la consola de administración de Google.

La consola de administración de Google permite gestionar los servicios de Google que tienen a su disposición los usuarios de su organización. AirWatch emplea la consola de administración de Google para realizar la integración con Chromebooks.

1. Inicie sesión como administrador en la consola de administración de Google.
2. En la consola, seleccione **Security (Seguridad)** > **Advanced Settings (Configuración avanzada)** > **Manage API client access (Administrar el acceso de cliente API)**.
3. En el campo **Client Name (Nombre del cliente)**, introduzca el ID de cliente proporcionado por AirWatch.
4. En el campo **One or More API Scopes (Uno o más ámbitos API)**, introduzca los ámbitos de API de Google de los siguientes en los que desea controlar acceso a las aplicaciones:

   Separe los ámbitos de API con coma.

   - https://www.googleapis.com/auth/chromedevicemanagementapi
   - https://www.googleapis.com/auth/admin.directory.user

© 2020 Palo Alto Networks, Inc.

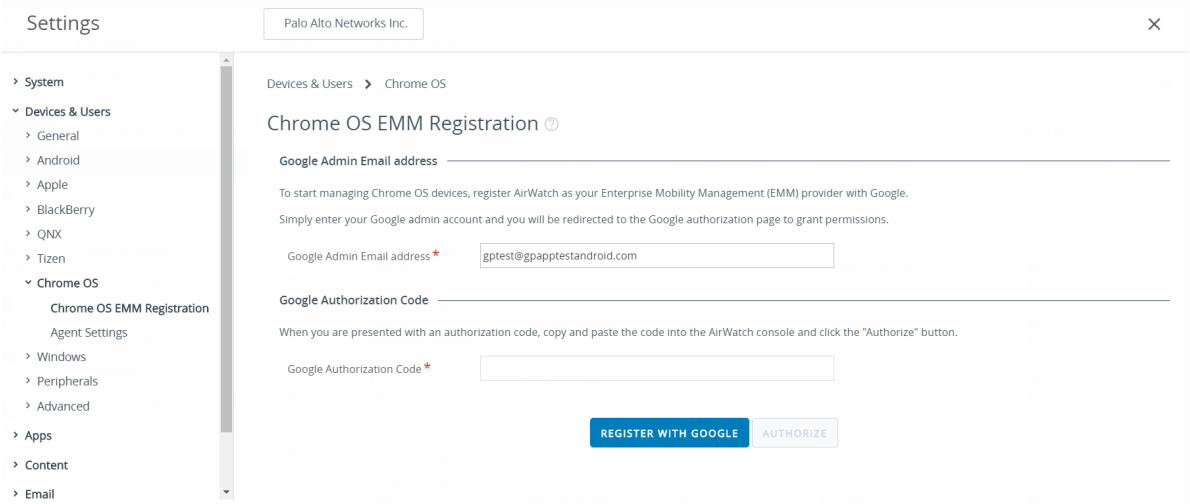
- https://www.googleapis.com/auth/admin.directory.device.chromeos

5. Haga clic en **Authorize (Autorizar)**.
6. Habilite **Chrome Management - Partner Access (Administración de Chrome - Acceso de partners)** en las políticas de dispositivos, a las que se accede con **Device Management (Administración de dispositivos)** > **Device Settings (Configuración del dispositivo)** > **Chrome Management (Administración de Chrome)** > **Device Settings (Configuración del dispositivo)**, y en las políticas de usuarios, a las que se accede con **Device Management (Administración de dispositivos)** > **Device Settings (Configuración del dispositivo)** > **Chrome Management (Administración de Chrome)** > **User Settings (Configuración de usuario)**.

STEP 2 | Registre AirWatch como proveedor de gestión de la movilidad empresarial (enterprise mobility management, EMM) para Google.

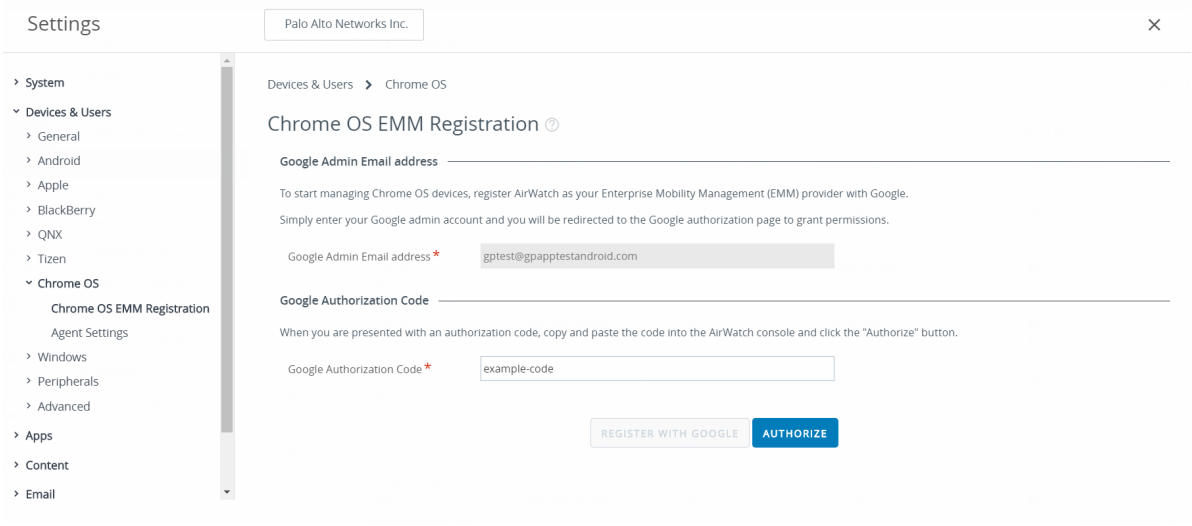
Para gestionar los Chromebooks con AirWatch, debe registrar AirWatch con la consola de administración de Google.

1. Inicie sesión en la consola de AirWatch.
2. Seleccione **Devices (Dispositivos)** > **Devices Settings (Configuración de dispositivos)** > **Devices & Users (Dispositivos y usuarios)** > **Chrome OS** > **Chrome OS EMM Registration (Registro de EMM en Chrome OS)**.
3. En **Google Admin Email address (Dirección de correo de administración de Google)**, introduzca el correo electrónico con el que accede a la consola de administración de Google.
4. Hag clic en **REGISTER WITH GOOGLE (REGISTRAR EN GOOGLE)**. Se le redirige a la página de autorización de Google, en la que obtiene un código de autorización de Google.



5. En **Google Authorization Code (Código de autorización de Google)**, introduzca el código obtenido en la página de autorización de Google.
6. Haga clic en **AUTHORIZE (AUTORIZAR)** para terminar el registro.

© 2020 Palo Alto Networks, Inc.



STEP 3 | Inscriba los Chromebooks en AirWatch.

Para gestionar los Chromebooks con AirWatch, primero debe inscribir los Chromebooks en AirWatch y sincronizarlos.

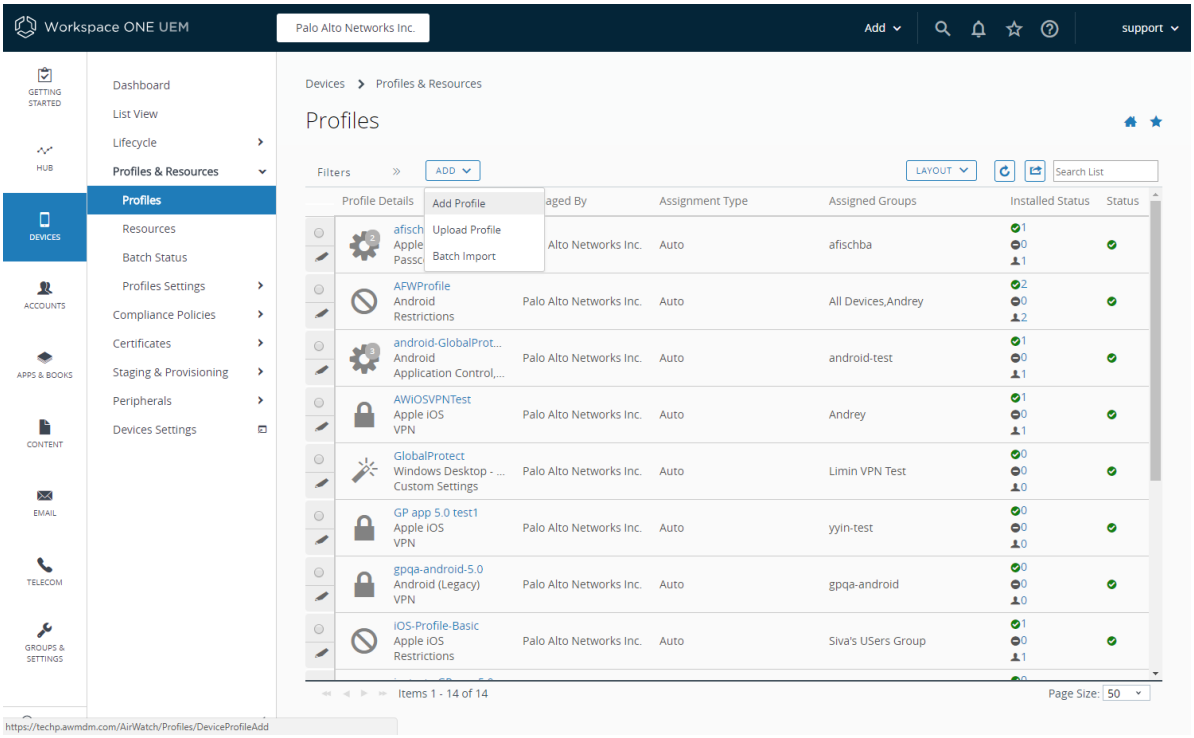
1. En su Chromebook, pulse **CTRL+ALT+E** para abrir la pantalla de inscripción de la empresa.
2. Introduzca el nombre de usuario y la contraseña de la carta de bienvenida a la administración de Google o bien las credenciales de usuario de G Suite.
3. Haga clic en **Enroll device (Inscribir dispositivo)**. Una vez inscrito el Chromebook, recibe un mensaje de confirmación.
4. Inicie sesión en la consola de AirWatch.
5. Seleccione **Devices (Dispositivos)** > **Devices Settings (Configuración de dispositivos) > Devices & Users (Dispositivos y usuarios)** > **Chrome OS** > .
6. Haga clic en **Device Sync (Sincronización de dispositivos)** para sincronizar todos los Chromebooks inscritos en AirWatch.

STEP 4 | Añada la aplicación de GlobalProtect para Android a un perfil de Chrome OS de AirWatch.

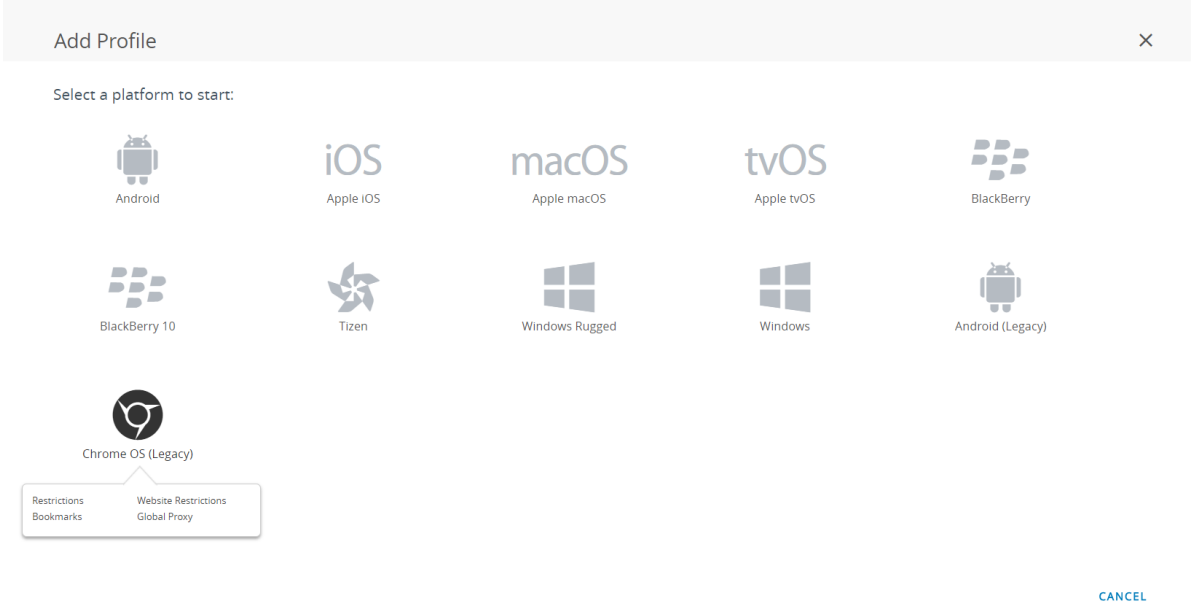
El perfil **Application Control (Control de aplicaciones)** permite añadir aplicaciones de Google Play y Chrome Web Store.

1. Inicie sesión en la consola de AirWatch.
2. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y haga clic en **ADD (Añadir)** para añadir un perfil de Chrome OS nuevo.

© 2020 Palo Alto Networks, Inc.

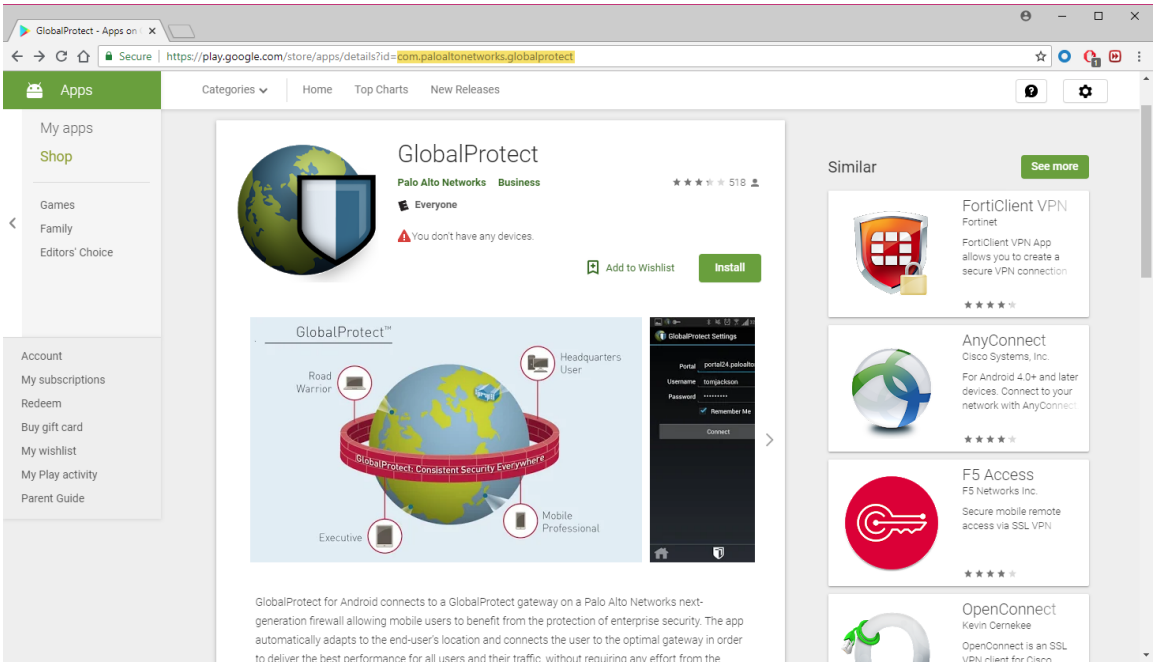


3. Seleccione **Chrome OS (Legacy) (Chrome OS [Heredado])** en la lista de plataformas.



4. Configure los ajustes de **General**.
5. Configure los ajustes de **Application Control (Control de aplicaciones)**.
   1. En **App ID (ID de aplicación)**, introduzca el ID de GlobalProtect que aparece en la URL de Google Play (com.paloaltonetworks.globalprotect).

© 2020 Palo Alto Networks, Inc.



2. Introduzca el nombre de la aplicación en **Name (Nombre)**.
3. Si lo desea, marque **Pin App to Shelf (Anclar aplicación a estantería)**. Introduzca **Y (Sí)** para anchar la aplicación a la estantería de aplicaciones del Chromebook.
4. Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune

Puede implementar la aplicación de GlobalProtect en endpoints gestionados inscriptos con Microsoft Intune o en usuarios cuyos endpoints no estén inscriptos con Microsoft Intune (iOS únicamente). Después de implementar la aplicación, configure e implemente un perfil VPN en endpoints gestionados para configurar la aplicación de GlobalProtect para el usuario final de forma automática.

STEP 1 | Inscriba endpoints con Microsoft Intune.

Para implementar la aplicación de GlobalProtect en sus endpoints, asegúrese de que los endpoints están inscriptos con Microsoft Intune.

STEP 2 | Añada la aplicación de GlobalProtect a Microsoft Intune.

Antes de poder asignar la aplicación de GlobalProtect a cualquier usuario o endpoint, debe añadir la aplicación a Microsoft Intune.

STEP 3 | Establezca el tipo de asignación de la aplicación de GlobalProtect.

Puede determinar quién puede acceder a la aplicación de GlobalProtect al asignar la aplicación a usuarios o endpoints. Antes de asignar la aplicación, debe establecer el tipo de asignación para la aplicación. El tipo de asignación pone a disposición, requiere o desinstala la aplicación.

STEP 4 | Asigne la aplicación de GlobalProtect a usuarios o endpoints específicos.

Después de establecer el tipo de asignación para la aplicación de GlobalProtect, puede asignar la aplicación a usuarios o endpoints específicos.

(iOS únicamente) Puede asignar la aplicación de GlobalProtect a usuarios cuyos endpoints no se inscribieron con Microsoft Intune.

© 2020 Palo Alto Networks, Inc.

Implementación de la aplicación móvil de GlobalProtect con MobileIron

Puede implementar la aplicación de GlobalProtect en los endpoints gestionados que se inscribieron con MobileIron. Después de implementar la aplicación, configure e implemente un perfil VPN para configurar la aplicación de GlobalProtect para el usuario final de forma automática.

STEP 1 | Añada usuarios a MobileIron.

Antes de que los usuarios registren sus endpoints en MobileIron, debe crear una entrada de usuario para cada usuario.

STEP 2 | (Opcional) Asigne usuarios a grupos de usuarios.

Para implementar la aplicación de GlobalProtect en función de la pertenencia a un grupo, en lugar de usuarios individuales, puede asignar usuarios a diferentes grupos de usuarios.

STEP 3 | Invite a usuarios a registrar sus endpoints con MobileIron.

Después de añadir usuarios a MobileIron, puede invitarlos a registrar sus endpoints.

STEP 4 | Añada la aplicación de GlobalProtect al catálogo de aplicaciones de MobileIron.

El catálogo de aplicaciones detalla las aplicaciones móviles disponibles para sus usuarios. Puede buscar y añadir la aplicación de GlobalProtect desde una tienda pública (como la tienda de aplicaciones de Apple) o cargar la aplicación directamente a MobileIron como una aplicación local. Debe configurar los ajustes de distribución de aplicaciones para indicar cómo se instalará y configurará la aplicación de GlobalProtect en los endpoints registrados.

Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google

La consola de gestión de Google le posibilita gestionar los ajustes y aplicaciones de Chromebook desde una ubicación central basada en la Web. Puede implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados y configurar los ajustes asociados de redes privadas virtuales (virtual private network, VPN) con la consola.

Para configurar la aplicación para el usuario automáticamente, puede usar opcionalmente la Consola de administración de Google Chromebook para configurar e implementar configuraciones en dispositivos gestionados con Chrome OS. Puede usar la Consola del administrador de Google para gestionar la configuración y las aplicaciones de Chromebook.

Siga estas recomendaciones para implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados:

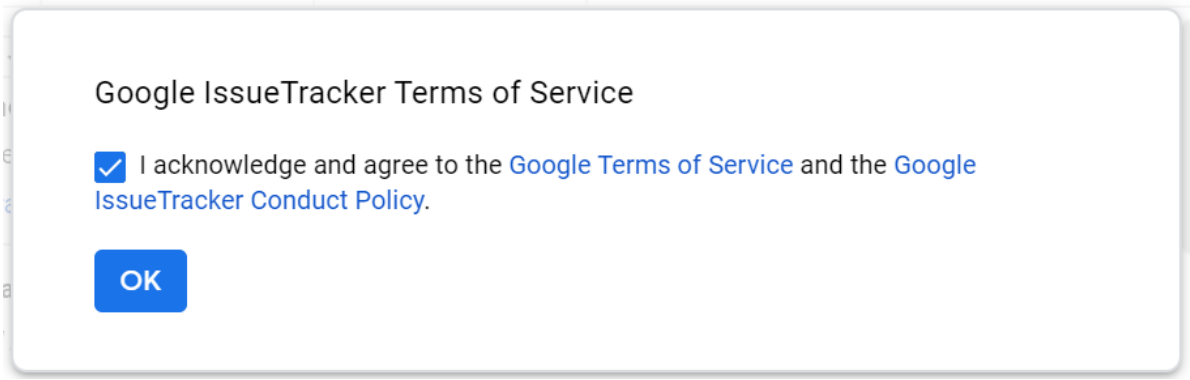
- *No puede enviar un certificado único de autenticación al dispositivo con la Consola del administrador de Google.*
- *Desde su Chromebook, pulse CTRL+ALT+T para abrir la línea de comando del terminal. Use el comando* `route` *para ver las rutas que están instaladas en el dispositivo. Puede determinar si se incluyen las rutas de acceso para la división de túnel.*
- *Debido a que las aplicaciones a menudo usan diferentes formatos de archivo, puede usar OpenSSL para convertir los certificados del formato PKCS # 12 al formato Base64. Utilice el comando* `openssl base64 -A -in` *<certificate-in-p12-format>* `-out` *<cert.txt>.*

Siga estos pasos para implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google:

© 2020 Palo Alto Networks, Inc.

STEP 1 | Antes de comenzar:

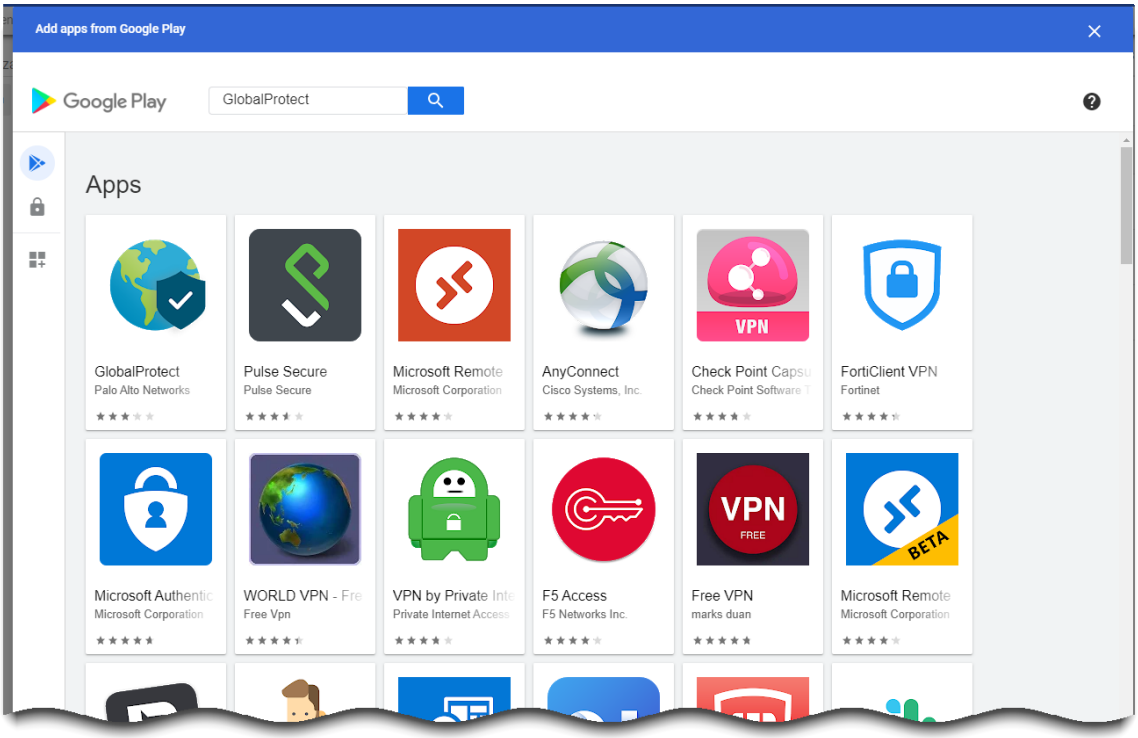
- Configure las puertas de enlace de GlobalProtect para que admitan la aplicación de GlobalProtect para Android en Chromebooks gestionados. Consulte Configuración de una puerta de enlace de GlobalProtect.
- Configure el portal y personalice la aplicación de GlobalProtect para Android en Chromebooks gestionados. Debe configurar una o más puertas de enlace a las que se pueda conectar la aplicación de GlobalProtect. Consulte Configuración del acceso al portal de GlobalProtect. Consulte la Matriz de compatibilidad de Palo Alto Networks para obtener una lista de las funciones compatibles con Android en Chrome OS.
- (Recomendado) Habilite el SSO de SAML para la aplicación de GlobalProtect para Android en Chromebooks para realizar una autenticación perfecta. Le recomendamos que configure el SSO de SAML para permitir que los usuarios se conecten automáticamente después de iniciar sesión en Chromebook sin tener que volver a especificar sus credenciales en la aplicación de GlobalProtect. Esto garantiza que los usuarios tengan acceso a una seguridad ininterrumpida. Consulte Configuración de autenticación SAML.
- Cuando los usuarios se conecten a GlobalProtect por primera vez en Android en Chromebooks gestionados, debe aparecer el siguiente mensaje de notificación de la VPN de supresión antes de configurar el túnel:



STEP 2 | Apruebe la aplicación de GlobalProtect para los usuarios de los Chromebooks.

1. Inicie sesión como administrador en la consola de administración de Google.
2. En la consola de administración, seleccione **Devices (Dispositivos)** > **Chrome management (Administración de Chrome)** para ver y modificar los ajustes de gestión de Chrome.
3. Seleccione **Apps & extensions (Aplicaciones y extensiones)**.
4. En el área Apps and extensions (Aplicaciones y extensiones), haga clic en el enlace de la **página de configuración de la aplicación**.
5. Haga clic en el botón + para añadir GlobalProtect a la lista de aplicaciones para Android aprobadas de la Google Playstore.
6. Cuando se inicie Google Play Store, busque `GlobalProtect` y haga clic en el icono de esta aplicación.

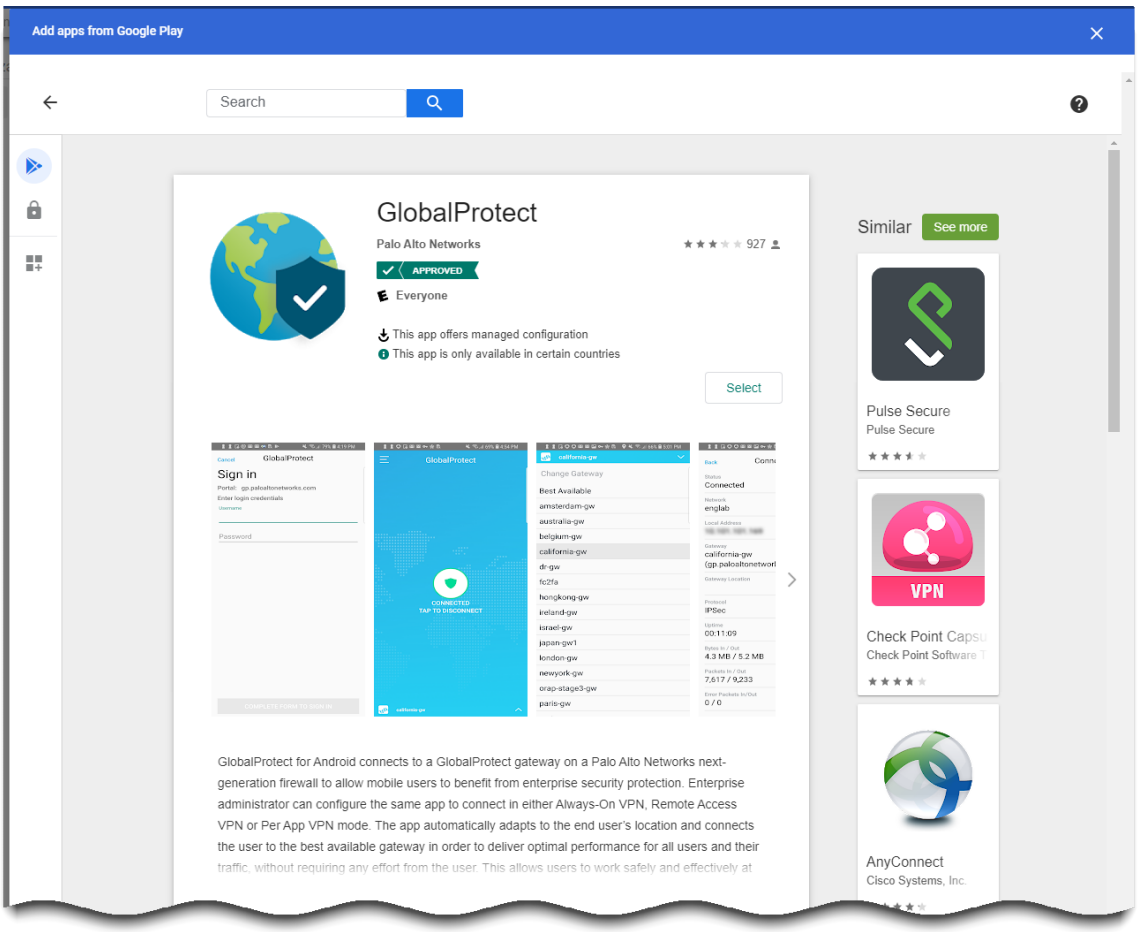
© 2020 Palo Alto Networks, Inc.



7. Haga clic en **Select (Seleccionar)** para añadir la aplicación de GlobalProtect.

   Aparecerá un mensaje si la aplicación de GlobalProtect se añade correctamente como resultado.

© 2020 Palo Alto Networks, Inc.



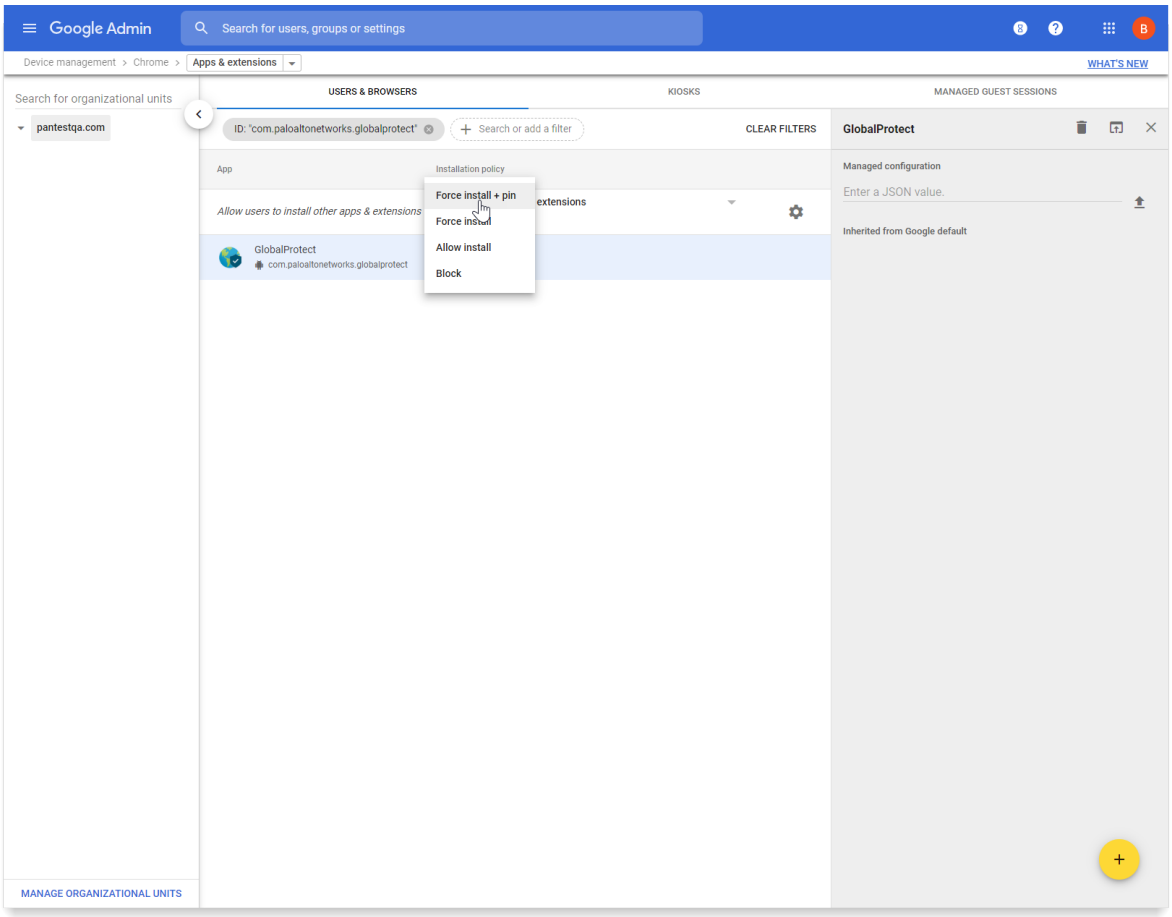
STEP 3 | Determine cómo se instala la aplicación de GlobalProtect en los Chromebooks.

Después de aprobar la aplicación de GlobalProtect, debe especificar cómo se instala en los Chromebooks. Para impedir que los usuarios la desinstalen y eludan su uso, fuerce su instalación automática en cuanto inicien sesión en sus Chromebooks.

1. En la configuración de administración de la extensión de la aplicación (**Device Management (Administración de dispositivos)** > **Chrome** > **App & Extensions (Aplicaciones y extensiones)**), seleccione **GlobalProtect** en la lista Apps (Aplicaciones).
2. Seleccione su unidad organizativa de la lista en el lado izquierdo de la página.
3. Seleccione una de las siguientes opciones:
   - (Recomendado) **Force install + pin (Forzar instalación + anclar)**: habilite y ancle la aplicación de GlobalProtect instalada a la fuerza en la barra de tareas. Si seleccionó esta opción, los usuarios no tendrán la opción de cerrar sesión en la aplicación.
   - **Force install (Forzar instalación)**: utilice esta opción si desea asegurarse de que la aplicación de GlobalProtect se instala automáticamente en cada Chromebook cuando los usuarios inician sesión en sus Chromebooks. Para evitar que los usuarios desinstalen la aplicación de GlobalProtect y eviten los requisitos de seguridad y cumplimiento, utilice la opción **Force install (Forzar instalación)**. Si seleccionó esta opción, los usuarios no tendrán la opción de cerrar sesión en la aplicación.
   - **Allow install (Permitir instalación)**: instale esta aplicación manualmente desde Google Playstore. Esta opción también permite a los usuarios desinstalar la aplicación de GlobalProtect de sus Chromebooks.

© 2020 Palo Alto Networks, Inc.

- **Block (Bloquear)**: impide que los usuarios instalen esta aplicación.



4. Haga clic en **SAVE (GUARDAR)** para guardar los cambios.

STEP 4 | Aplique una configuración gestionada a la aplicación de GlobalProtect.

Si ha habilitado la instalación forzosa de la aplicación de GlobalProtect, puede aplicarle un archivo de configuración gestionada que contiene valores para sus ajustes configurables.

1. En App Management setting (Configuración de administración de la aplicación) (**Device Management (Administración de dispositivos)** > **Chrome management (Administración de Chrome)** > **App & Extensions (Aplicaciones y extensiones)**), seleccione **GlobalProtect** en la lista Apps (Aplicaciones).
2. Seleccione su unidad organizativa de la lista en el lado izquierdo de la página.
3. Haga clic en el icono **Upload from file (Cargar desde archivo)** en el lateral derecho de la página para seleccionar y cargar su archivo de configuración gestionado. También puede especificar el nombre del valor clave en formato JSON, como se muestra en la siguiente configuración de ejemplo.

```
{
 "portal": "acme.portal.com",
 "username": "user123"
}
```

En la siguiente tabla se muestra un ejemplo de la configuración en el archivo de configuración gestionado. Para las configuraciones que son relevantes para su empresa, póngase en contacto con su administrador de TI.

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)	Tipo de valor	Ejemplo
portal	Dirección IP o nombre de dominio completo (fully qualified domain name, FQDN) del portal.	Cadena	**acme.portal.com**
nombre de usuario	Nombre de usuario para la autenticación en el portal.	Cadena	**user123**
Contraseña	Contraseña para la autenticación en el portal.	Cadena	**password123**
client_certificate	Certificado de cliente para la autenticación en el portal.	Secuencia de comandos (en Base64)	**DAFDSaweEWQ23wDSAFD**...
client_certificate _passphrase (frase_contraseña_certificado_cliente)	Frase de contraseña del certificado de cliente para la autenticación en el portal.	Cadena	**PA$$W0RD$123**
app_list	Lista de aplicaciones permitidas o prohibidas para controlar qué tráfico de aplicaciones puede atravesar el túnel VPN en una configuración de VPN por aplicación.	Cadena	**allow list| block list: com.google.calendar; com.android.email; com.android.chrome**
connect_method	Método de conexión a la VPN.	Cadena	**user-logon | on-demand**
mobile_id	Identificador único empleado para identificar los terminales móviles, tal como se ha configurado en un sistema externo de gestión de dispositivos móviles (mobile device management, MDM).	Cadena	**5188a8193be43f42d332 dde5cb2c941e**
remove_vpn_config _via_restriction (eliminar_configuración_VPN_mediante_restricción)	Marca para eliminar la configuración de VPN.	Expresión booleana	**true | false**
allow_vpn_bypass	Indicador para permitir que el tráfico de la	Expresión booleana	**true | false**

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)	Tipo de valor	Ejemplo
	aplicación evite el túnel VPN.		
cert_alias	Nombre único utilizado para identificar el certificado del cliente durante la autenticación del portal o la puerta de enlace.	Cadena	**`Company User client ( Cliente de usuario de la empresa)`**
managed	Indicador para marcar si el dispositivo está inscrito en un servidor MDM.	Expresión booleana	**`true | false`**
ownership	Categoría de propiedad del dispositivo, por ejemplo, **Employee Owned (Propiedad del empleado)**.	Cadena	**`byod`**
compliance	Estado de cumplimiento que indica si el dispositivo cumple con las políticas de cumplimiento que ha definido.	Cadena	**`yes`**
tag	Etiquetas que permiten identificar dispositivos. Cada etiqueta debe estar separada por una coma.	Cadena	**`GuestAccount,SatelliteOffice`**

4. Haga clic en **SAVE (GUARDAR)** para guardar los cambios.

STEP 5 | Aplique políticas en la aplicación de GlobalProtect para Android en Chromebooks gestionados.

- Cree objetos HIP mediante la **información de host** específica para Android en Chromebooks gestionados. A continuación, úselo como condiciones de coincidencia en cualquier perfil de información de host (Host Information Profile, HIP).
- Aplique la política de seguridad correspondiente con un perfil HIP como condición de coincidencia en una regla de políticas. Por defecto, la aplicación recopila categorías de datos de información para ayudarlo a identificar el estado de seguridad del host.

Configuraciones de VPN siempre activada

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. La aplicación de GlobalProtect se conecta al portal de GlobalProtect (tras el inicio de sesión del usuario) para enviar información de usuario y del host y recuperar la configuración del agente. Después de que la aplicación recibe la configuración del agente del portal, se conecta automáticamente y establece un túnel VPN a la puerta de enlace de GlobalProtect que se especificó en la configuración del agente.

© 2020 Palo Alto Networks, Inc.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN siempre activada con sistemas de gestión de dispositivos móviles compatibles:

- Establecimiento de una configuración de VPN siempre activada con AirWatch
- Establecimiento de una configuración de VPN siempre activada con Microsoft Intune
- Establecimiento de una configuración de VPN siempre activada con MobileIron
- Establecimiento de una configuración de VPN siempre activada con la consola de gestión de Google

Establecimiento de una configuración de VPN siempre activada con AirWatch

AirWatch es una plataforma de gestión de movilidad empresarial que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por AirWatch y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración siempre activada con AirWatch:

- Establecimiento de una configuración de VPN siempre activada para endpoints iOS con AirWatch
- Establecimiento de una configuración de VPN siempre activada para endpoints de Windows 10 UWP con AirWatch

Establecimiento de una configuración de VPN siempre activada para endpoints iOS con AirWatch

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN.

Use los siguientes pasos para establecer una configuración de VPN siempre activada para endpoints iOS con AirWatch:

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

La aplicación de GlobalProtect para iOS también está disponible en la App Store de Apple en China.

STEP 2 | Desde la consola de AirWatch, modifique un perfil iOS Apple existente o añada uno nuevo.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **iOS** de la lista de plataformas.

© 2020 Palo Alto Networks, Inc.

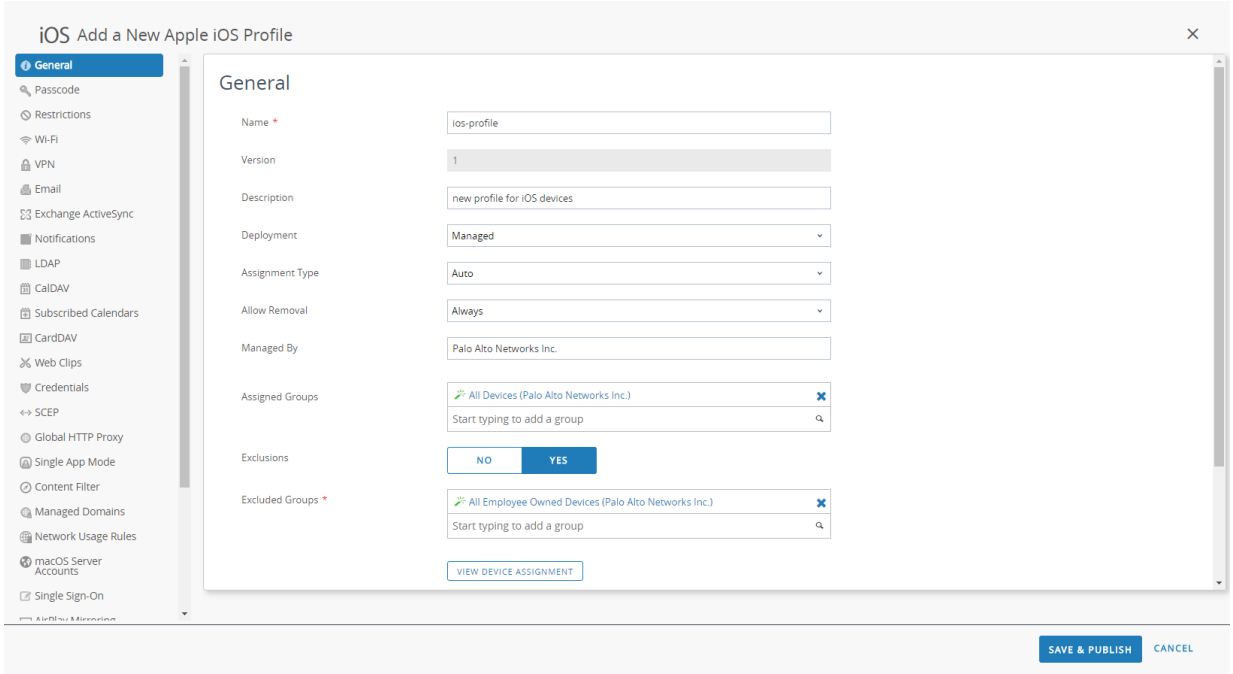
STEP 3 | Configure los ajustes en **General**:

1. Introduzca un **Name (Nombre)** para el perfil.
2. (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.
3. (Opcional) Seleccione el método **Deployment (Implementación)**, que determina si se eliminará el perfil automáticamente luego de la cancelación de la inscripción, ya sea **Managed (Administrada)** (se elimina el perfil) o **Manual** (el perfil permanece instalado hasta que el usuario final lo elimina).
4. (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
5. (Opcional) Seleccione si desea habilitar la opción **Allow Removal (Permitir eliminación)** del perfil para el usuario final. Seleccione **Always (Siempre)** para permitir que el usuario final elimine manualmente el perfil en cualquier momento, **Never (Nunca)** para evitar que lo elimine o **With Authorization (Con autorización)** para permitir que pueda eliminarlo con la autorización del administrador. Si se elige la opción **With Authorization (Con autorización)**, se añade una contraseña obligatoria.
6. (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
7. (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
8. (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.
9. (Opcional) Si habilita la opción de **Install only on devices inside selected areas (Instalar únicamente en dispositivos dentro de las áreas seleccionadas)**, el perfil puede instalarse únicamente en endpoints

© 2020 Palo Alto Networks, Inc.

en la geocerca o regiones de iBeacon especificados. Cuando se le indique, añada la geocerca o regiones de iBeacon en el campo **Assigned Geofence Areas (Áreas de geocerca asignadas)**.

10. (Opcional) Si selecciona la opción **Enable Scheduling and install only during selected time periods (Habilitar los plazos e instalar únicamente durante los períodos de tiempo seleccionados)**, puede aplicar un plazo (**Devices [Dispositivos]** > **Profiles & Resources [Perfiles y recursos]** > **Profiles Settings [Ajustes de perfil]** > **Time Schedules [Plazos]**) para la instalación del perfil, que limita los períodos de tiempo durante los cuales se puede instalar el perfil en los endpoints. Cuando se le indique, introduzca el nombre del plazo en el campo **Assigned Schedules (Plazos asignados)**.
11. (Opcional) Seleccione la **Removal Date (Fecha de eliminación)** en la cual desea que se elimine el perfil de todos los endpoints.

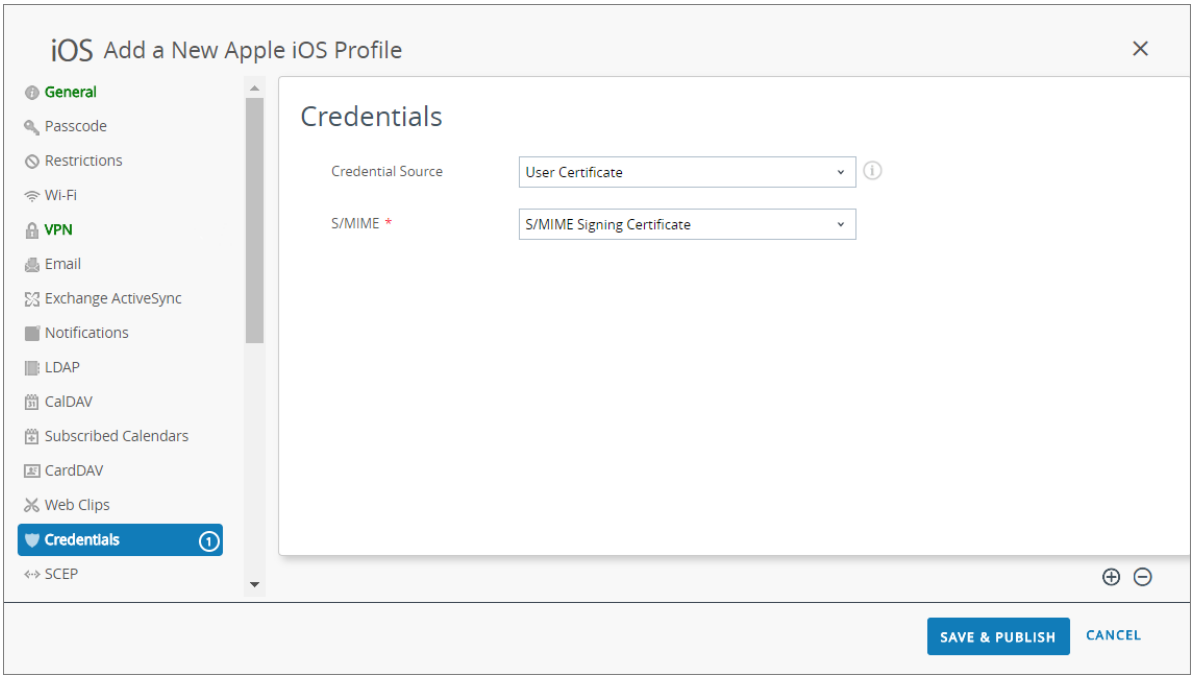


STEP 4 | (Opcional) Si su implementación de GlobalProtect requiere autenticación del certificado de cliente, configure los ajustes de las **Credentials (Credenciales)**:

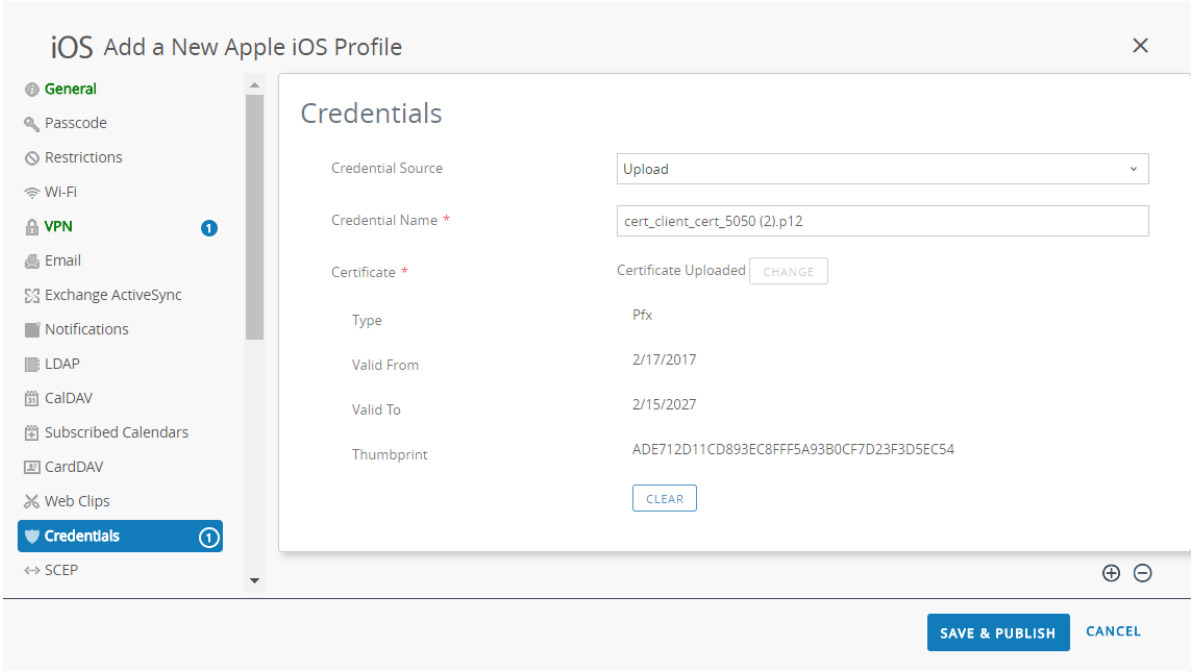
A partir de iOS 12, si desea usar certificados de cliente para la autenticación de cliente de GlobalProtect, debe implementar los certificados de cliente como parte del perfil de VPN que se envía desde el servidor de MDM. Si implementa certificados de cliente desde el servidor de MDM con otro método, la aplicación de GlobalProtect no puede usar los certificados.

- Para extraer certificados de cliente de usuarios de AirWatch:
  1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
  2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).

© 2020 Palo Alto Networks, Inc.



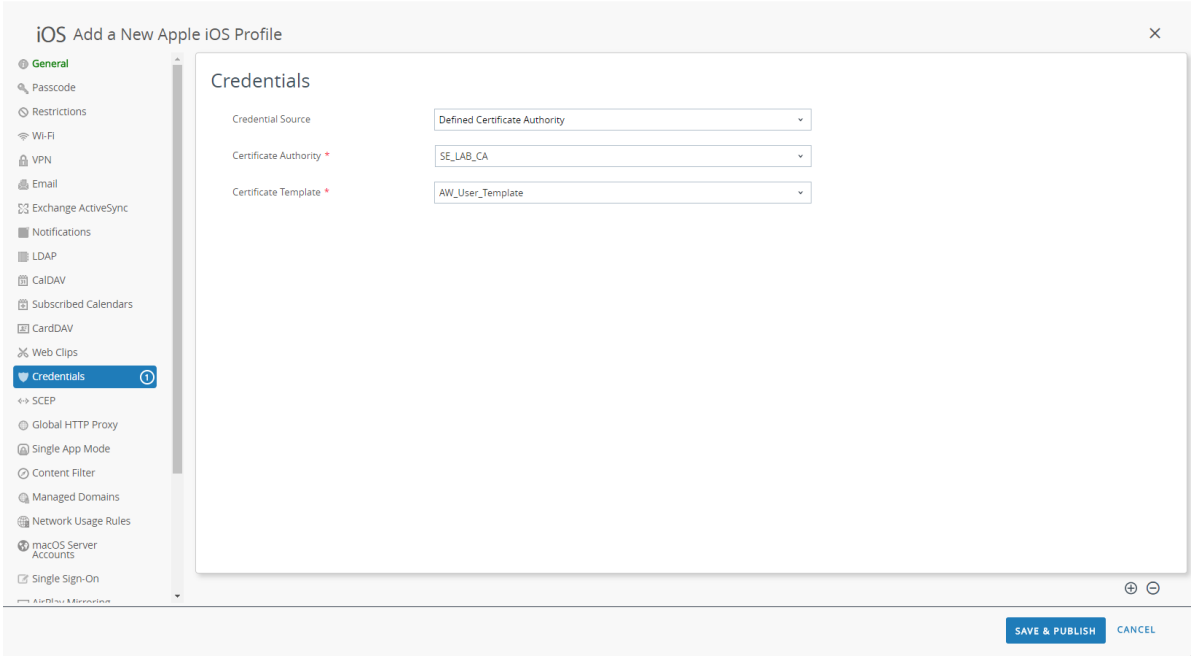
- Para cargar un certificado de cliente manualmente:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
  2. Introduzca el **Credential Name (Nombre de credencial)**.
  3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
  4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.



- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.

© 2020 Palo Alto Networks, Inc.

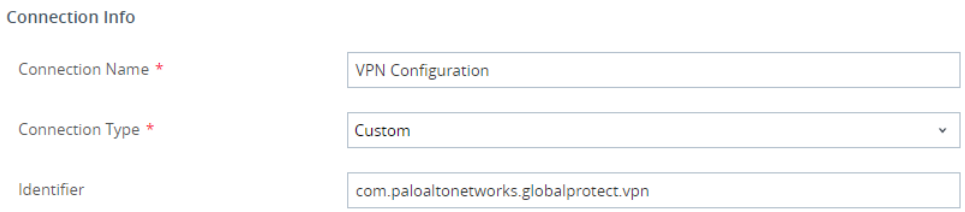
3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.



STEP 5 | Configure los ajustes de **VPN**.

1. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
2. Seleccione el **Connection Type (Tipo de conexión)** de la red:
   - Para la aplicación GlobalProtect 4.1.x y versiones anteriores, seleccione **Palo Alto Networks GlobalProtect**.
   - Para la aplicación GlobalProtect 5.0 y versiones posteriores, seleccione **Custom (Personalizado)**.
3. (Opcional) Si en **Connection Type (Tipo de conexión)**, selecciona **Custom (Personalizado)**, introduzca el ID de paquete (**com.paloaltonetworks.globalprotect.vpn**) en el campo **Identifier (Identificador)** para identificar la aplicación de GlobalProtect.

   *Si descargó la aplicación de GlobalProtect directamente de la App Store de Apple en China, especifique el ID del paquete (**com.paloaltonetworks.globalprotect.vpncn**) en el campo Identifier (Identificador)*



4. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
5. (Opcional) Introduzca el nombre de usuario de la **Account (Cuenta)** de VPN o haga clic en el botón añadir (**+**) para ver los valores de búsqueda compatibles que puede introducir.
6. (Opcional) En el campo **Disconnect on idle (Desconectar por inactividad)**, especifique la cantidad de tiempo (en segundos) después de la cual se cierra la sesión de los endpoints de la aplicación de GlobalProtect después de que la aplicación deja de enrutar tráfico a través del túnel de VPN.

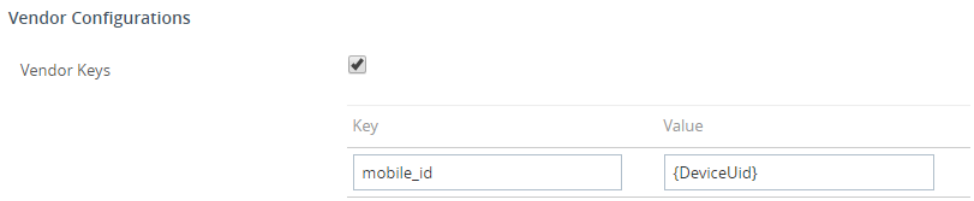
© 2020 Palo Alto Networks, Inc.

7. En el área Authentication (Autenticación), seleccione un método de **Authentication (Autenticación)** de usuario: **Password (Contraseña)**, **Certificate (Certificado)**, **Password + Certificate (Contraseña y certificado)**.
8. Cuando se le indique, introduzca una contraseña en **Password (Contraseña)** o seleccione el **Identity Certificate (Certificado de identidad)** que GlobalProtect usará para autenticar usuarios. El **Identity Certificate (Certificado de identidad)** es el mismo certificado que configuró en los ajustes de **Credentials (Credenciales)**.
9. Seleccione las opciones **Enable VPN On Demand (Habilitar VPN bajo demanda)** y **Use new on demand keys (Usar nuevas claves bajo demanda)**.
10. Configure una regla bajo demanda con **Acción: Conectar**.
11. (Opcional) Seleccione el tipo de **Proxy** y configure los ajustes relevantes.

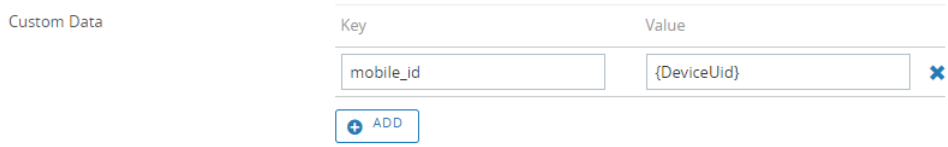
STEP 6 | (Opcional) (a partir de GlobalProtect 5.0) Si su implementación de GlobalProtect requiere HIP integration with MDM (Integración de HIP con MDM), especifique el atributo de identificador de dispositivo único (unique device identifier, UDID).

GlobalProtect admite la integración con MDM para obtener atributos de dispositivos móviles desde el servidor MDM, que se usarán en la aplicación de la política basada en HIP. Para que la integración con MDM funcione, la aplicación de GlobalProtect debe presentar el UDID del endpoint en la puerta de enlace de GlobalProtect. El atributo UDID permite a la aplicación de GlobalProtect recuperar y usar información de UDID en implementaciones basadas en MDM. Si elimina el atributo de UDID del perfil, ya no podrá usar la integración con MDM. La aplicación de GlobalProtect genera un nuevo UDID, pero no se puede usar para la integración.

- Si usa el **Connection Type (Tipo de conexión)** de la red **Palo Alto Networks GlobalProtect**, vaya a los ajustes de **VPN** y habilite las **Vendor Keys (Claves de proveedor)** en el área Vendor Configurations (configuraciones de proveedor). En **Key (Clave)**, seleccione **`mobile_id`** y en **Value (Valor)**, seleccione **`{DeviceUid}`**.



- Si usa el **Connection Type (Tipo de conexión)** de la red **Custom (Personalizada)**, vaya a los ajustes de **VPN** y haga clic en **ADD (Añadir)** para añadir los **Custom Data (Datos personalizados)** en el área Connection Info (Información de conexión). En **Key (Clave)**, seleccione **`mobile_id`** y en **Value (Valor)**, seleccione **`{DeviceUid}`**.



STEP 7 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

Establecimiento de una configuración de VPN siempre activada para endpoints de Windows 10 UWP con AirWatch

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN. Para requisitos de seguridad aún más

© 2020 Palo Alto Networks, Inc.

estrictos, puede habilitar el bloqueo de VPN que fuerza a que la conexión segura siempre esté activada y conectada, y deshabilita el acceso de red cuando la aplicación no está conectada. Esta configuración es similar a la opción **Enforce GlobalProtect for Network Access (Aplicar GlobalProtect para el acceso de red)** que configuraría normalmente en el portal de GlobalProtect.

Debido a que AirWatch aún no incluye a GlobalProtect como un proveedor oficial de conexión para los endpoints de Windows, usted debe seleccionar un proveedor de VPN alternativo, editar los ajustes para la aplicación de GlobalProtect e importar la configuración nuevamente en el perfil VPN según se describe en el siguiente flujo de trabajo.

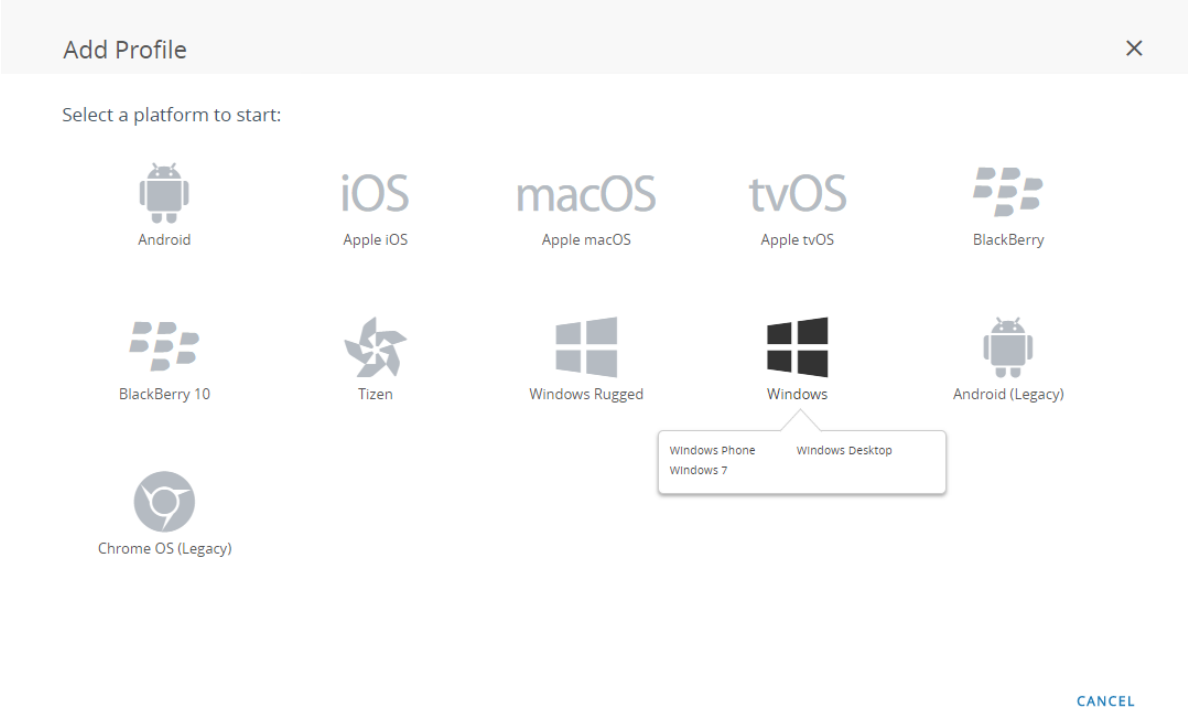
Use los siguientes pasos para establecer una configuración de VPN siempre activada para endpoints de Windows 10 UWP con AirWatch:

STEP 1 | Descargue la aplicación de GlobalProtect para Windows 10 UWP:

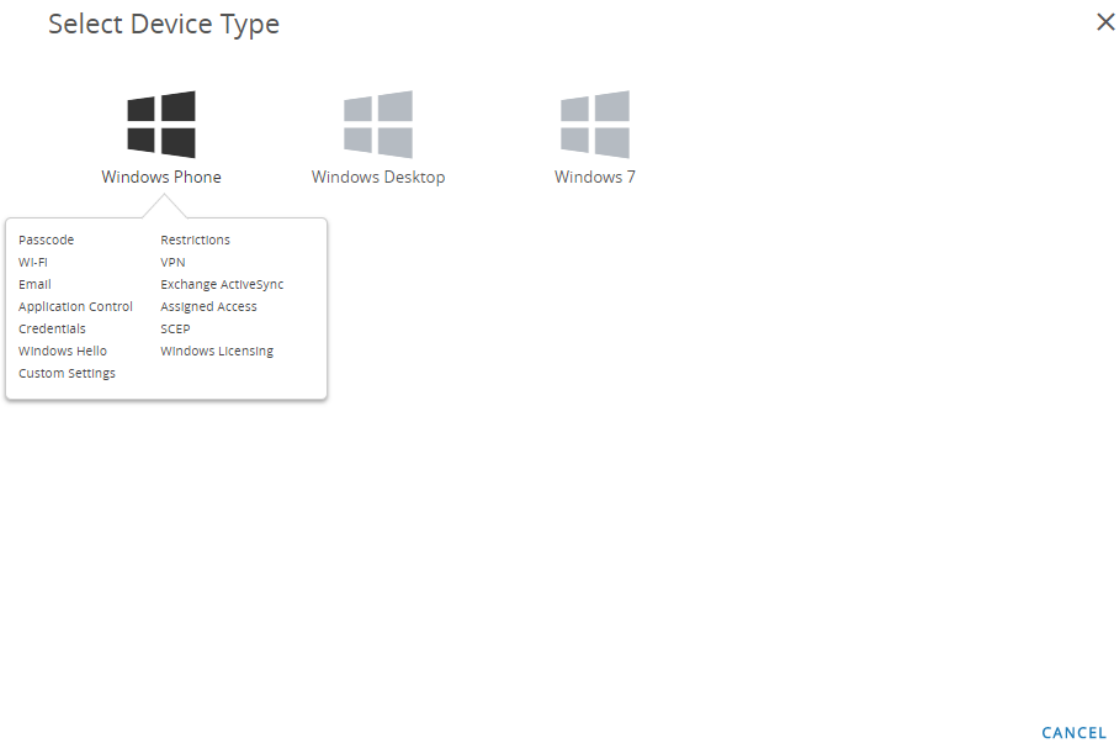
- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde Microsoft Store.

STEP 2 | En la consola de AirWatch, modifique un perfil de Windows 10 UWP existente o añada uno nuevo.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **Windows** como la plataforma y **Windows Phone** como el tipo de dispositivo.



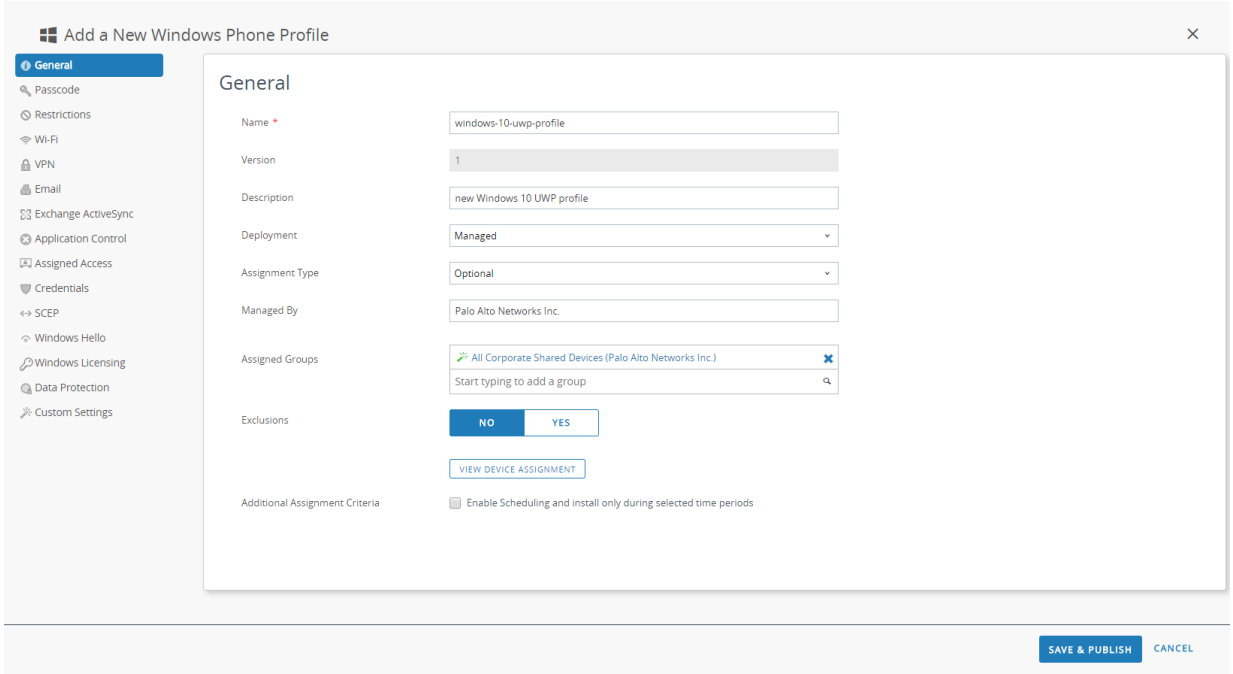
© 2020 Palo Alto Networks, Inc.



STEP 3 | Configure los ajustes en **General**:

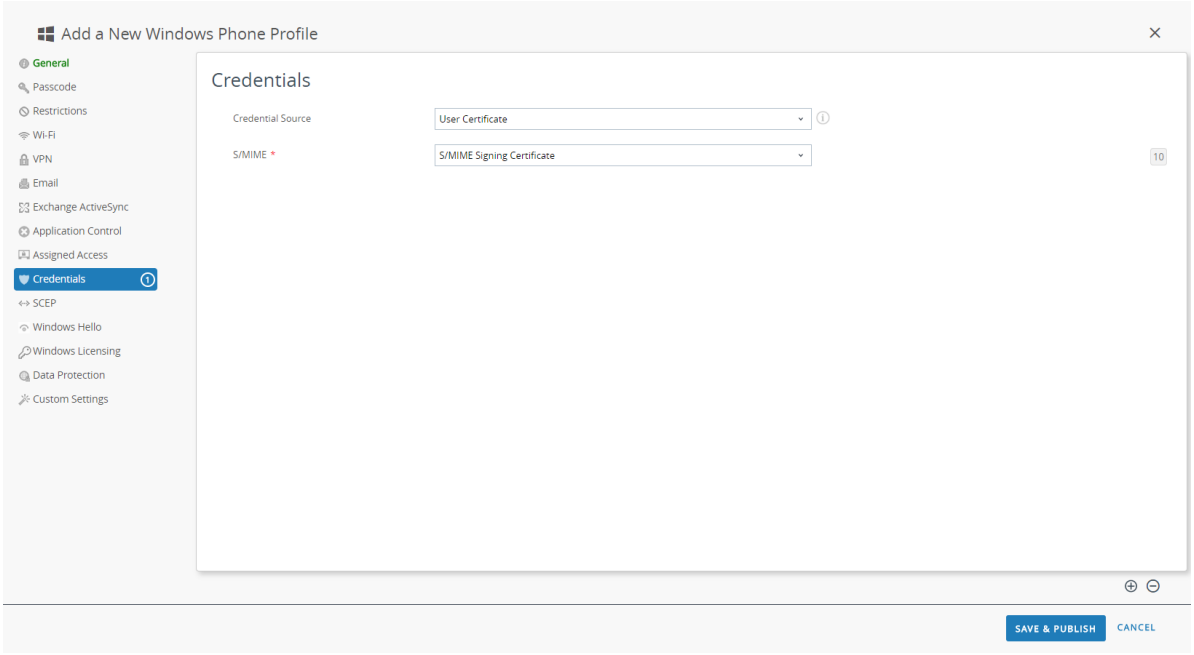
1. Introduzca un **Name (Nombre)** para el perfil.
2. (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.
3. (Opcional) En el método de **Deployment (Implementación)**, seleccione **Managed (Gestionado)** para permitir que el perfil se elimine automáticamente luego de la cancelación de la inscripción
4. (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
5. (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
6. (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
7. (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.
8. (Opcional) Si selecciona la opción **Enable Scheduling and install only during selected time periods (Habilitar los plazos e instalar únicamente durante los períodos de tiempo seleccionados)**, puede aplicar un plazo (**Devices [Dispositivos]** > **Profiles & Resources [Perfiles y recursos]** > **Profiles Settings [Ajustes de perfil]** > **Time Schedules [Plazos]**) para la instalación del perfil, que limita los períodos de tiempo durante los cuales se puede instalar el perfil en los endpoints. Cuando se le indique, introduzca el nombre del plazo en el campo **Assigned Schedules (Plazos asignados)**.

© 2020 Palo Alto Networks, Inc.



STEP 4 | (Opcional) Si su implementación de GlobalProtect requiere autenticación del certificado de cliente, configure los ajustes de las **Credentials (Credenciales)**:

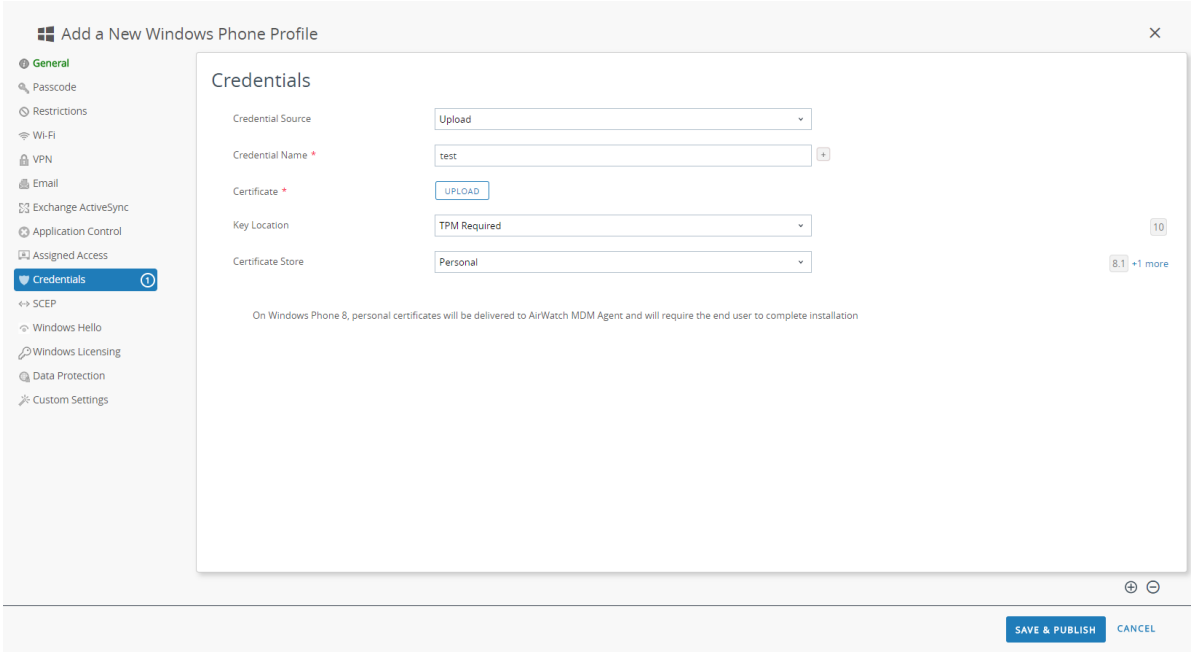
- Para extraer certificados de cliente de usuarios de AirWatch:
  1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
  2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).



- Para cargar un certificado de cliente manualmente:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
  2. Introduzca el **Credential Name (Nombre de credencial)**.

© 2020 Palo Alto Networks, Inc.

3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.
5. Seleccione la **Key Location (Ubicación de clave)** donde desea almacenar la clave privada del certificado:
   - **TPM Required (TPM requerida)**: almacene la clave privada en un módulo de plataforma fiable. Si un módulo de plataforma fiable no está disponible en el endpoint, no se puede instalar la clave privada.
   - **TPM If Present (TPM si está presente)**: almacene la clave privada en un módulo de plataforma fiable si hay uno disponible en el endpoint. Si un módulo de plataforma fiable no está disponible en el endpoint, la clave privada se almacena en el software del endpoint.
   - **Software**: almacene la clave privada en el software del endpoint.
   - **Passport**: guarde la clave privada en Microsoft Passport. Para usar esta opción, se debe instalar AirWatch Protection Agent en el endpoint.
6. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.

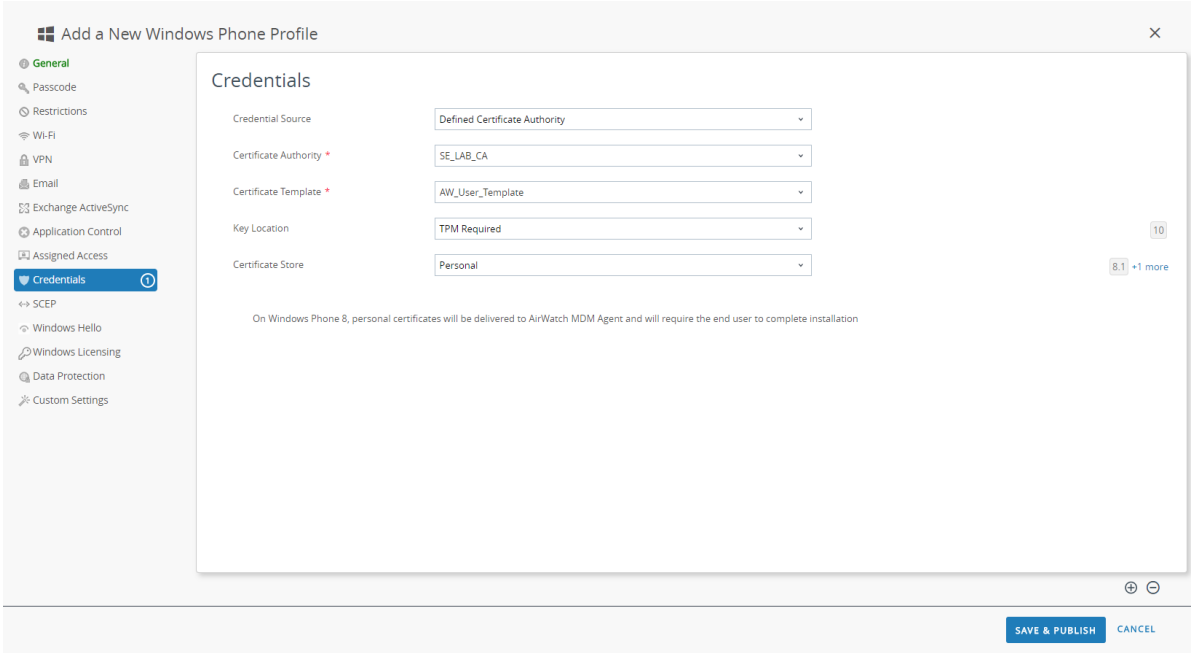


- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.
  3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.
  4. Seleccione la **Key Location (Ubicación de clave)** donde desea almacenar la clave privada del certificado:
     - **TPM Required (TPM requerida)**: almacene la clave privada en un módulo de plataforma fiable. Si un módulo de plataforma fiable no está disponible en el endpoint, no se puede instalar la clave privada.
     - **TPM If Present (TPM si está presente)**: almacene la clave privada en un módulo de plataforma fiable si hay uno disponible en el endpoint. Si un módulo de plataforma fiable no está disponible en el endpoint, la clave privada se almacena en el software del endpoint.
     - **Software**: almacene la clave privada en el software del endpoint.

© 2020 Palo Alto Networks, Inc.

- **Passport**: guarde la clave privada en Microsoft Passport. Para usar esta opción, se debe instalar AirWatch Protection Agent en el endpoint.

5. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.



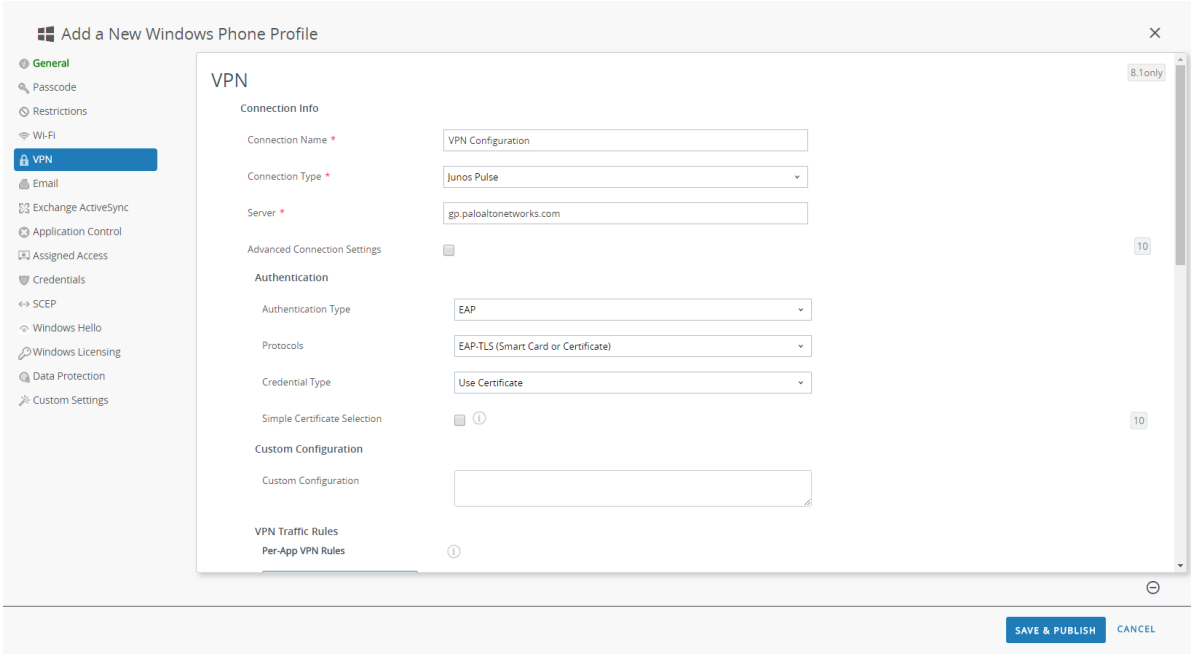
STEP 5 | Configure los ajustes de **VPN**.

1. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
2. Seleccione un proveedor de **Connection Type (Tipo de conexión)** alternativo (no seleccione **IKEv2**, **L2TP**, **PPTP** o **Automatic [Automático]**, ya que estos no tienen los ajustes del proveedor asociado necesarios para el perfil de VPN de GlobalProtect).

   Debe seleccionar un proveedor alternativo debido a que AirWatch aún no incluye a GlobalProtect como proveedor oficial de conexión para los endpoints de Windows.

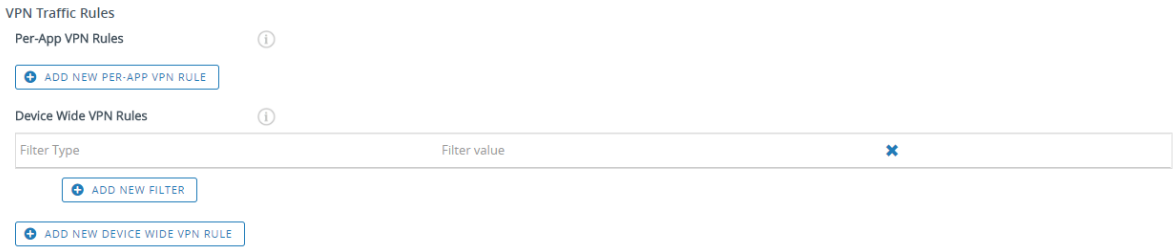
3. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
4. En el área Authentication (Autenticación), seleccione un **Authentication Type (Tipo de autenticación)** para especificar el método de autenticación de los usuarios finales.

© 2020 Palo Alto Networks, Inc.



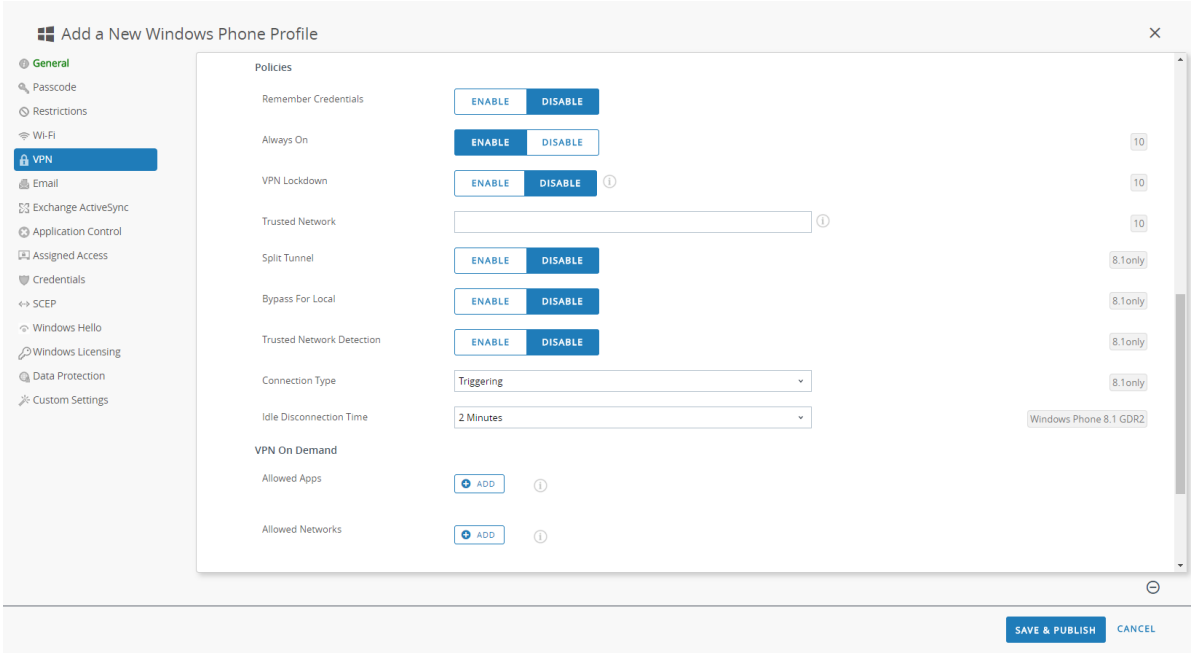
5. (Opcional) Para permitir que GlobalProtect guarde las credenciales de usuario, seleccione **ENABLE (HABILITAR)** para habilitar la opción **Remember Credentials (Recordar credenciales)** en el área Policies (Políticas).
6. (Opcional) En el área VPN Traffic Rules (Reglas de tráfico de VPN), seleccione **ADD NEW DEVICE WIDE VPN RULE (AÑADIR NUEVA REGLA DE VPN PARA DISPOSITIVOS)** para enviar a través del túnel de VPN el tráfico que coincida con una ruta específica. Estas reglas no están vinculadas por aplicación, pero se evalúan en todo el endpoint. Si el tráfico coincide con los criterios de coincidencia especificados, se dirige a través del túnel de VPN.

   Añada criterios de coincidencia haciendo clic en **ADD NEW FILTER (AÑADIR NUEVO FILTRO** e introduciendo un **Filter Type (Tipo de filtro)** y el **Filter Value (Valor de filtro)** correspondiente.



7. Para mantener siempre la conexión de GlobalProtect, habilite cualquiera de las siguientes opciones en el área Policies (Políticas):
   - Seleccione **ENABLE (HABILITAR)** en **Always On (Siempre activada)** para forzar la conexión segura de modo que esté siempre activada.
   - Seleccione **ENABLE (HABILITAR) VPN Lockdown (Bloqueo de VPN)** para forzar la conexión segura de modo que esté siempre activada y conectada, y deshabilitar el acceso cuando la aplicación no esté conectada. La opción **VPN Lockdown (Bloqueo de VPN)** en AirWatch es similar a la opción **Enforce GlobalProtect for Network Access (Aplicar GlobalProtect para el acceso de red)** que configuraría en el portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.



8. (Opcional) Especifique direcciones de red fiables en **Trusted Network (Red fiable)** si desea que GlobalProtect se conecte únicamente cuando detecte una conexión de red fiable.

STEP 6 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

STEP 7 | Para seleccionar GlobalProtect como proveedor de tipo de conexión, edite el perfil de VPN en XML.

Para minimizar las ediciones adicionales en el XML sin procesar, revise los ajustes de su perfil VPN antes de exportar la configuración. Si necesita cambiar un ajuste después de exportar el perfil VPN, puede realizar los cambios en el XML sin procesar o puede actualizar el ajuste en el perfil VPN y realizar este paso nuevamente.

1. En **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**, seleccione el botón de opción junto al nuevo perfil que añadió en los pasos previos y seleccione **</>XML** en la parte superior de la tabla. AirWatch abre la vista XML del perfil.
2. Exporte el perfil y luego ábralo en un editor de texto de su elección.
3. Edite los siguientes ajustes para GlobalProtect:

- En el elemento LocIURI que especifica PluginPackageFamilyName, cambie el elemento por:

```
<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/
PluginPackageFamilyName</LocURI>
```

- En el elemento Data que sigue, cambie el valor por:

```
<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>
```

1. Guarde sus cambios en el perfil exportado.
2. Vuelva a AirWatch y seleccione **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**.
3. Cree y asigne un nombre a un perfil nuevo (seleccione **ADD [Añadir]** > **Add Profile [Añadir perfil]** > **Windows** > **Windows Phone**).
4. Seleccione **Custom Settings (Ajustes personalizados)** > **Configure (Configurar)** y luego copie y pegue la configuración modificada.
5. Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

© 2020 Palo Alto Networks, Inc.

STEP 8 | Limpie el perfil original al seleccionarlo en **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**, y luego, **More Actions (Más acciones)** > **Deactivate (Desactivar)**. AirWatch traslada el perfil a la lista Inactive.

STEP 9 | Compruebe la configuración.

Establecimiento de una configuración de VPN siempre activada con Microsoft Intune

Microsoft Intune es una plataforma de gestión de movilidad empresarial basada en la nube que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por Microsoft Intune y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración siempre activada con Microsoft Intune:

- Establecimiento de una configuración de VPN siempre activada para endpoints iOS con Microsoft Intune
- Establecimiento de una configuración de VPN siempre activada para endpoints de Windows 10 UWP con Microsoft Intune

Establecimiento de una configuración de VPN siempre activada para endpoints iOS con Microsoft Intune

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN.

Use los siguientes pasos para establecer una configuración de VPN siempre activada para endpoints iOS con Microsoft Intune:

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

STEP 2 | (Opcional) Si su implementación requiere autenticación basada en certificados, configure un perfil de certificado.

STEP 3 | Cree un nuevo perfil de VPN para iOS.

- En **Platform (Plataforma)**, seleccione **iOS**.

STEP 4 | Establezca los ajustes de VPN siempre activada para endpoints iOS.

- En **Connection type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect**.

Establecimiento de una configuración de VPN siempre activada para endpoints de Windows 10 UWP con Microsoft Intune

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN.

Use los siguientes pasos para establecer una configuración de VPN siempre activada para endpoints de Windows 10 UWP con Microsoft Intune:

STEP 1 | Descargue la aplicación de GlobalProtect para Windows 10 UWP:

- Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune.

© 2020 Palo Alto Networks, Inc.

- Descargue la aplicación de GlobalProtect directamente desde Microsoft Store.

STEP 2 | (Opcional) Si su implementación requiere autenticación basada en certificados, configure un perfil de certificado.

STEP 3 | Cree un nuevo perfil de VPN para Windows 10 UWP.

- En **Platform (Plataforma)**, seleccione **Windows 10 and later (Windows 10 y posterior)**.

STEP 4 | Establezca los ajustes de VPN siempre activada para endpoints de Windows 10 UWP.

- En **Connection type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect**.
- Habilite la VPN **Always On (Siempre activada)**.

Establecimiento de una configuración de VPN siempre activada con MobileIron

MobileIron es una plataforma de gestión de movilidad empresarial que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por MobileIron y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración siempre activada con MobileIron:

- Establecimiento de una configuración de VPN siempre activada para endpoints iOS con MobileIron
- Establecimiento de una configuración de VPN siempre activada para endpoints Android con MobileIron

Establecimiento de una configuración de VPN siempre activada para endpoints iOS con MobileIron

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN.

Use los siguientes pasos para establecer una configuración de VPN siempre activada para endpoints iOS con MobileIron:

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implementación de la aplicación móvil de GlobalProtect con MobileIron.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

STEP 2 | (Opcional) Si su implementación requiere autenticación basada en certificados, añada una configuración de certificado y configure los ajustes del certificado.

STEP 3 | Añada una configuración de VPN siempre activada.

- En el tipo de configuración, seleccione **Always On VPN (VPN siempre activada)**.

STEP 4 | Establezca los ajustes de VPN siempre activada para iOS.

Establecimiento de una configuración de VPN siempre activada para endpoints Android con MobileIron

En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN.

Use los siguientes pasos para establecer una configuración de VPN siempre activada para endpoints Android con MobileIron:

© 2020 Palo Alto Networks, Inc.

STEP 1 | Descargue la aplicación de GlobalProtect para Android.

- Implementación de la aplicación móvil de GlobalProtect con MobileIron.
- Descargue la aplicación de GlobalProtect directamente desde Google Play.

STEP 2 | (Opcional) Si su implementación requiere autenticación basada en certificados, añada una configuración de certificado y configure los ajustes del certificado.

STEP 3 | Añada una configuración de VPN siempre activada.

- En el tipo de configuración, seleccione **Always On VPN (VPN siempre activada)**.

STEP 4 | Establezca los ajustes de VPN siempre activada para Android.

Establecimiento de una configuración de VPN siempre activada con la consola de gestión de Google

La consola de gestión de Google es una plataforma de gestión de movilidad empresarial basada en la nube que le permite gestionar Chromebooks desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los Chromebooks gestionados por la consola de gestión de Google y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Establecimiento de una configuración de VPN siempre activada para Chromebooks con la consola de gestión de Google

Chromebooks admite redes privadas virtuales (virtual private network, VPN) siempre activas gracias a la ampliación de la compatibilidad de la aplicación de GlobalProtect para Android. En una configuración de VPN siempre activada, la conexión segura de GlobalProtect está siempre activada. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect siempre se enruta a través del túnel VPN. Al permitir que los usuarios finales ejecuten la aplicación de GlobalProtect para Android en sus Chromebooks, tiene la certeza de que siempre están conectados a GlobalProtect y disfrutan de seguridad activa en todo momento.

- *La aplicación de GlobalProtect para Android solo se admite en algunos Chromebooks.*
- *En los Chromebooks que no admiten aplicaciones para Android, debe seguir usando la aplicación de GlobalProtect para Chrome, pero no puede utilizar la VPN siempre activa.*
- *Si instala la aplicación de GlobalProtect para Android en un Chromebook para aprovechar la función de VPN siempre activa, desinstale, en su caso, la aplicación de GlobalProtect para Chrome.*

Use los siguientes pasos para establecer una configuración de VPN siempre activada para Chromebooks con la consola de gestión de Google.

Los siguientes pasos son únicamente aplicables para implementar la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google. En la actualidad, AirWatch no admite configuraciones de VPN siempre activa cuando se instala en la aplicación de GlobalProtect para Android en Chromebooks gestionados.

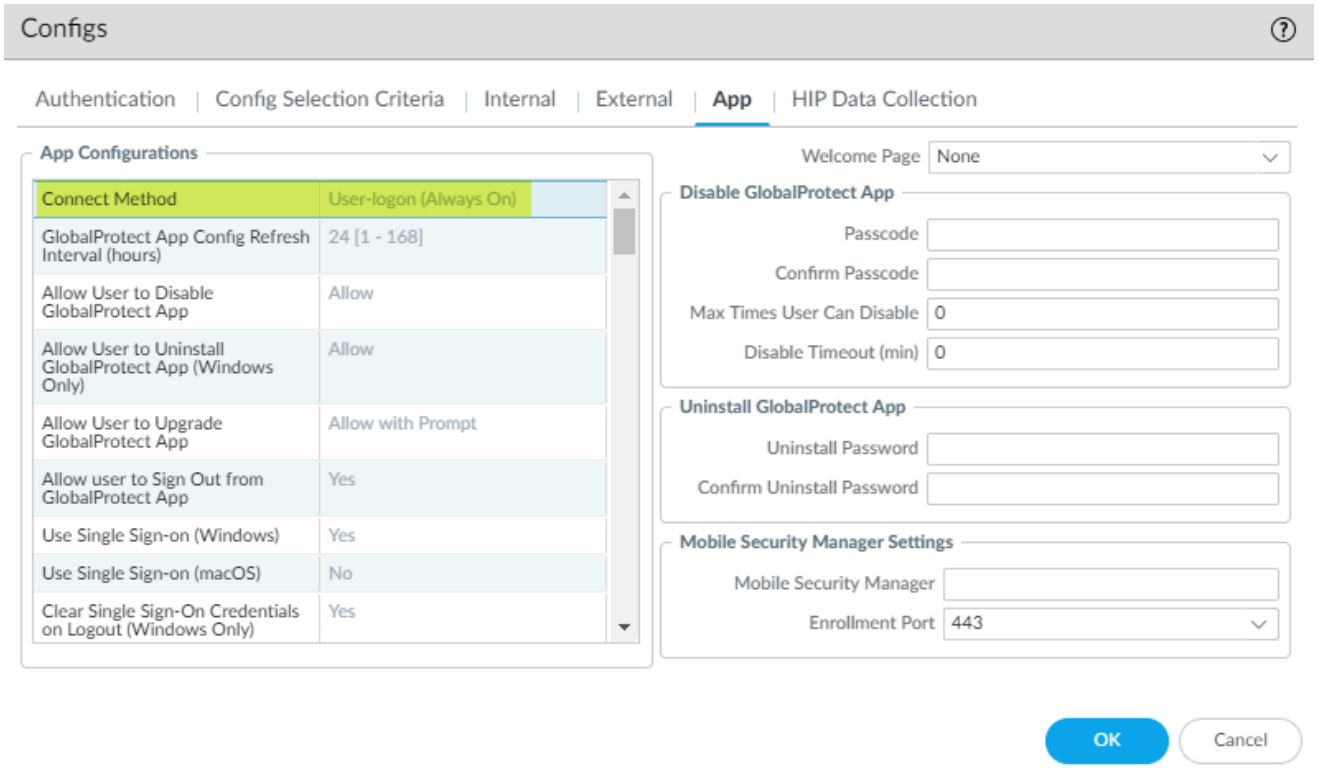
STEP 1 | En el cortafuegos de Palo Alto Networks, realice el procedimiento Configuración del acceso al portal de GlobalProtect.

STEP 2 | Definición de las configuraciones de agente de GlobalProtect.

STEP 3 | Personalización de la aplicación de GlobalProtect.

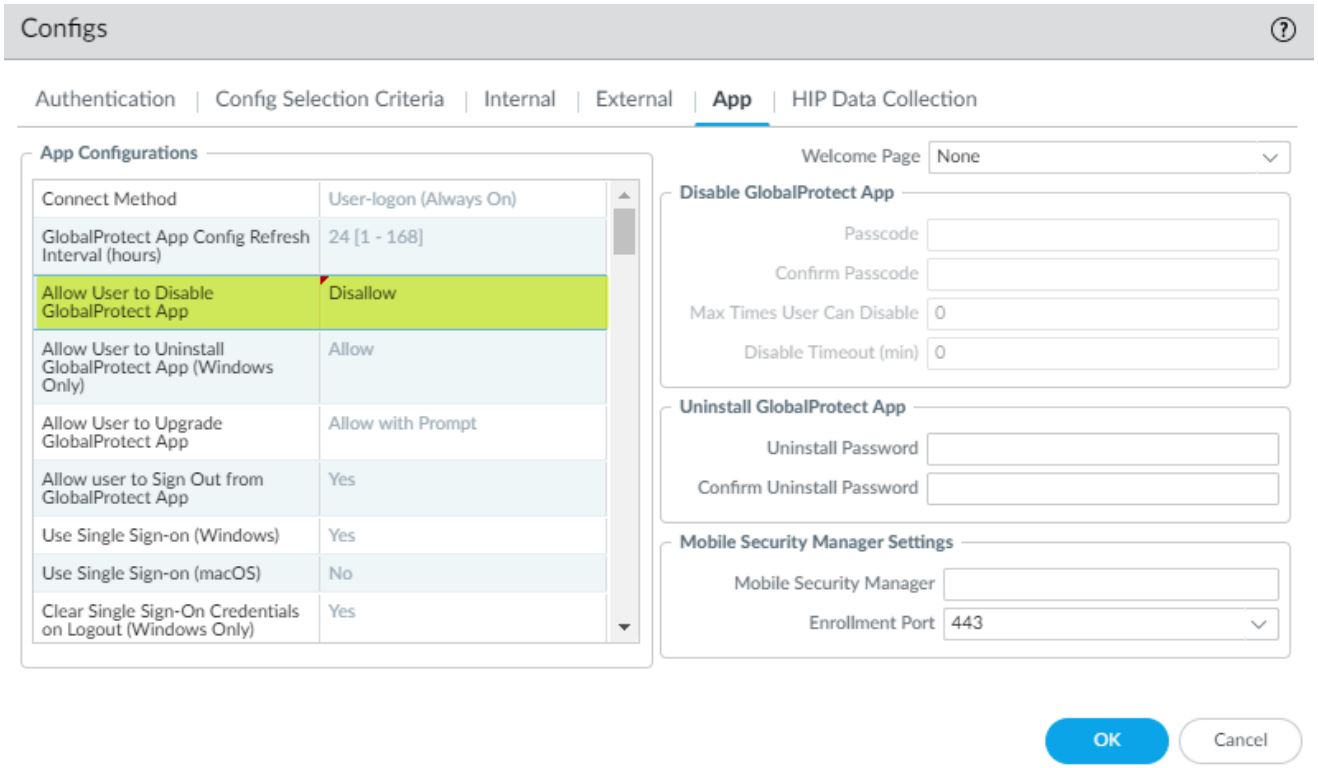
© 2020 Palo Alto Networks, Inc.

- Para configurar la conexión de GlobalProtect de modo que siempre esté activa, defina **Connect Method (Método de conexión)** en **User-logon (Always On) (Inicio de sesión de usuario [siempre activo])**.



- Para impedir que los usuarios deshabiliten la aplicación de GlobalProtect, defina la opción **Allow User to Disable GlobalProtect App (Permitir al usuario deshabilitar la aplicación de GlobalProtect)** en **Disallow (No permitir)**.

© 2020 Palo Alto Networks, Inc.



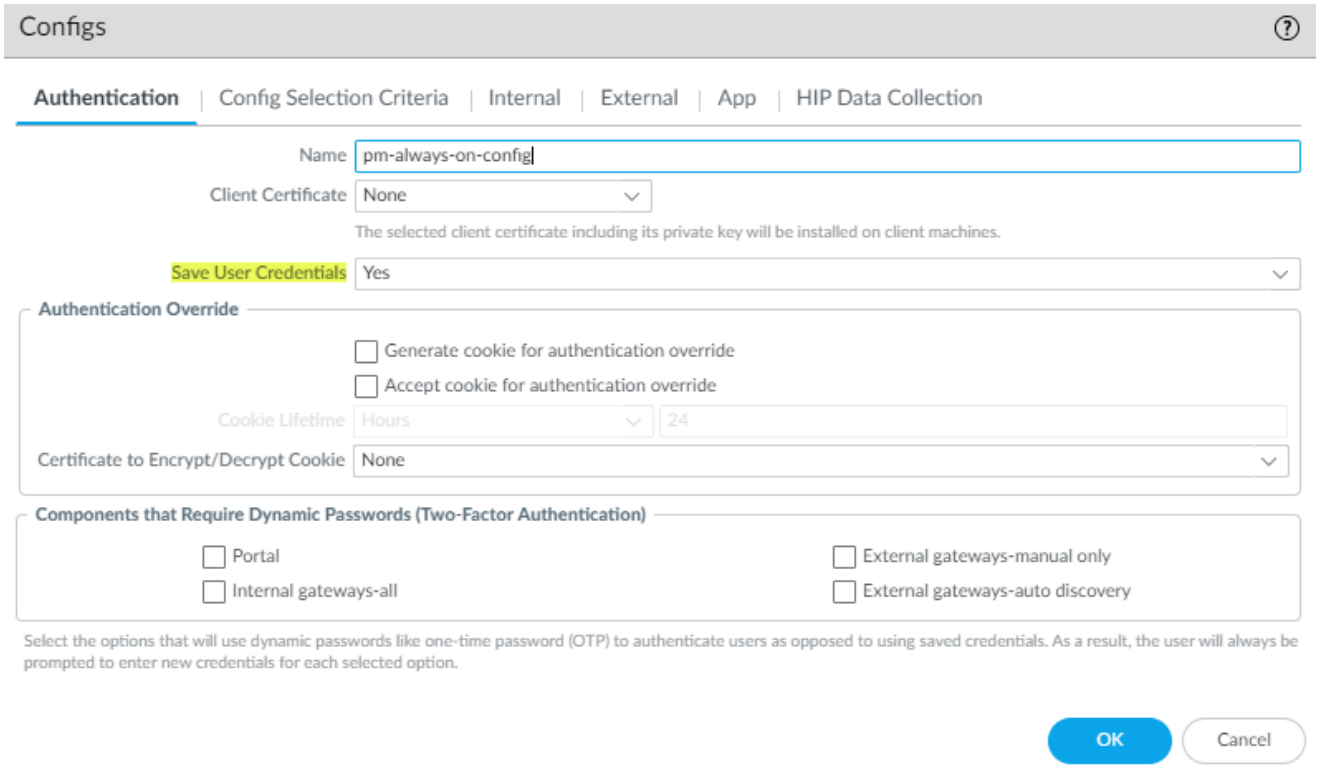
STEP 4 | Habilite la autenticación transparente en GlobalProtect.

Para impedir que los usuarios omitan las solicitudes de autenticación de GlobalProtect y, por lo tanto, se desconecten de GlobalProtect, configure una de las siguientes opciones de autenticación transparente:

- Permita que los usuarios se autentiquen en GlobalProtect de forma transparente mediante la autenticación con certificados de cliente.
- Habilite el inicio de sesión transparente permitiendo que la aplicación de GlobalProtect guarde tanto el nombre de usuario como la contraseña.

  1. Acceda a la configuración de agente del portal con **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* y seleccione **Authentication (Autenticación)**.
  2. Configure la opción **Save User Credentials (Guardar credenciales de usuarios)** en **Yes (Sí)**.

© 2020 Palo Alto Networks, Inc.



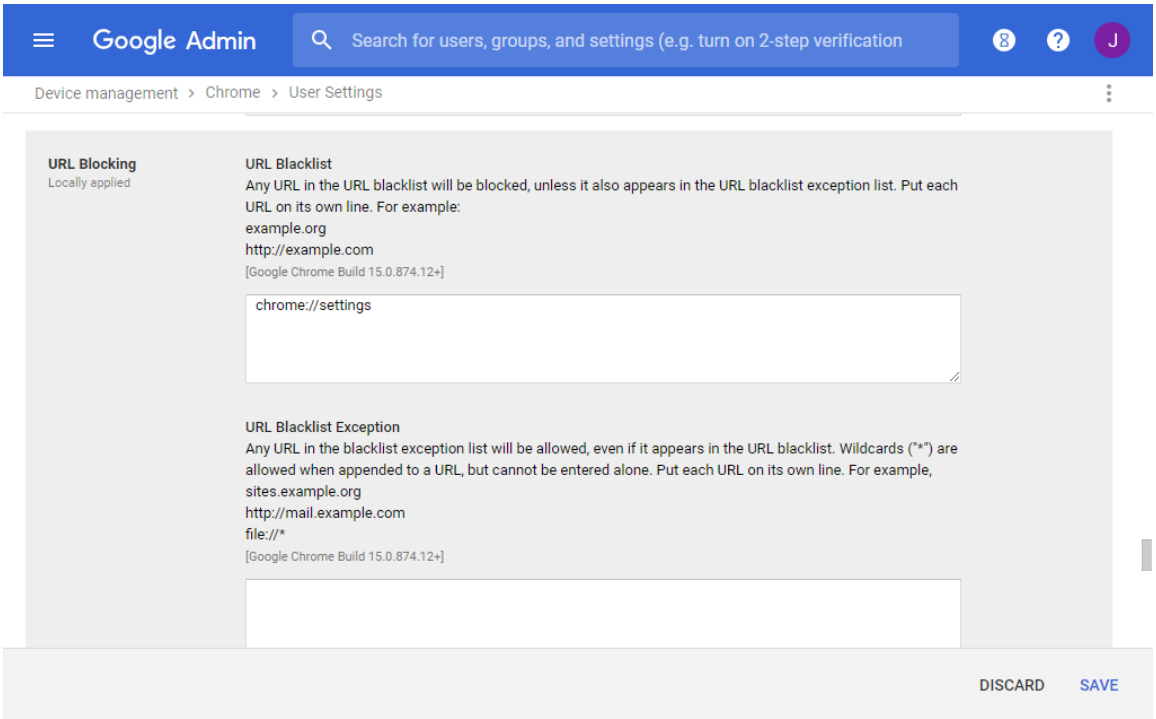
3. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración de agente del portal.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar los cambios en el cortafuegos.

STEP 6 | Impida que los usuarios de Chromebooks eludan GlobalProtect usando la configuración de VPN de Chrome OS.

1. Inicie sesión como administrador en la consola de administración de Google.
2. Implementación de la aplicación de GlobalProtect para Android en Chromebooks gestionados con la consola de administración de Google en todos los Chromebooks gestionados.
3. Incluya la configuración de Chrome (`chrome://settings`) en la lista de elementos no permitidos para que los usuarios no puedan modificar ningún ajuste de VPN:
   1. Seleccione **Device Management (Administración de dispositivos)** > **Chrome management (Administración de Chrome)** > **User Settings (Configuración de usuario)**.
   2. En el área Content (Contenido) > URL Blocking (Bloqueo de URL), introduzca `chrome://settings` en el cuadro de texto **URL Blacklist (Lista negra de URL)**.

© 2020 Palo Alto Networks, Inc.



4. Haga clic en **SAVE (GUARDAR)** para guardar los cambios.

Configuraciones VPN de acceso remoto iniciada por el usuario

En una configuración de VPN de acceso remoto (a demanda), los usuarios deben iniciar manualmente la aplicación de GlobalProtect para establecer la conexión segura de GlobalProtect. La aplicación de GlobalProtect se conecta al portal de GlobalProtect (tras el inicio de sesión del usuario) para enviar información de usuario y del host y recuperar la configuración del agente. Una vez la aplicación reciba la configuración del agente del portal, se conecta y establece un túnel VPN a la puerta de enlace de GlobalProtect que se especificó en la configuración del agente.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN de acceso remoto iniciada por el usuario con sistemas de gestión de dispositivos móviles compatibles:

- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario con AirWatch
- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario con Microsoft Intune
- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario con MobileIron

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario con AirWatch

AirWatch es una plataforma de gestión de movilidad empresarial que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los dispositivos móviles gestionados por AirWatch y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN de acceso remoto iniciada por el usuario con AirWatch:

- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con AirWatch

© 2020 Palo Alto Networks, Inc.

- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints de Windows 10 UWP con AirWatch

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con AirWatch

En una configuración de VPN de acceso remoto (a demanda), los usuarios deben iniciar manualmente la aplicación para establecer la conexión segura de GlobalProtect. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect se enruta a través del túnel VPN únicamente después de que los usuarios inician y establecen la conexión.

Use los siguientes pasos para establecer una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con AirWatch:

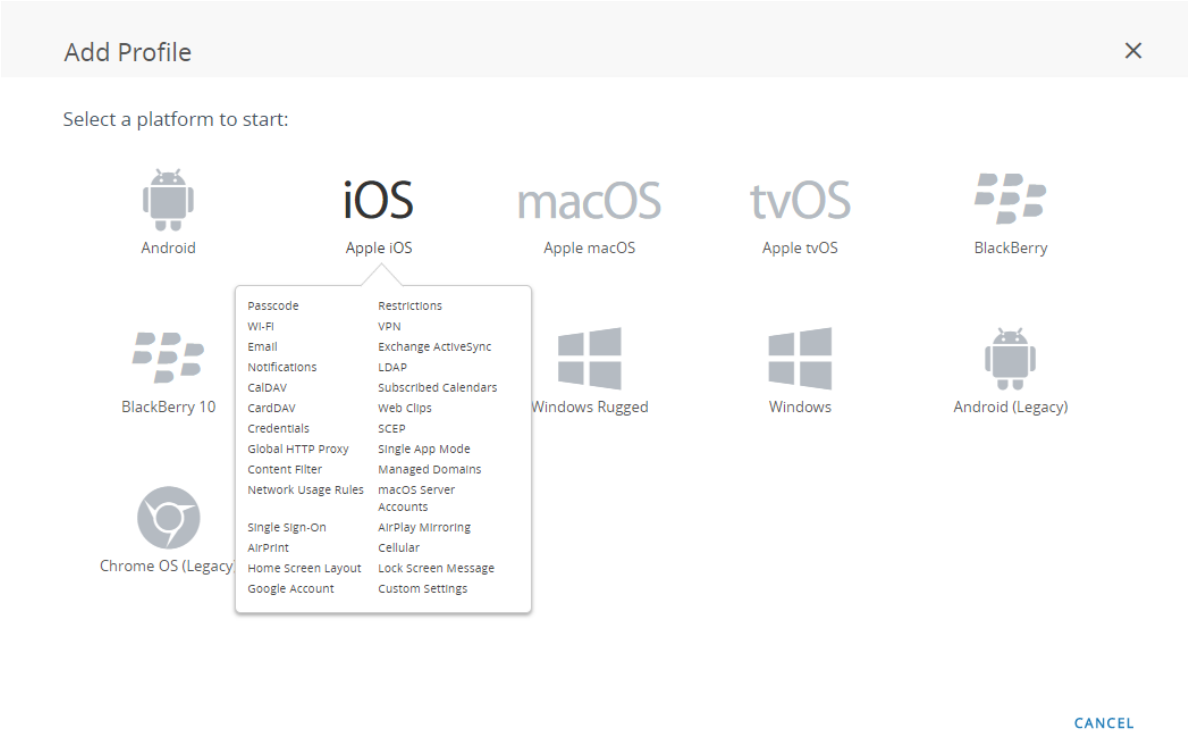
STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

La aplicación de GlobalProtect para iOS también está disponible en la App Store de Apple en China.

STEP 2 | Desde la consola de AirWatch, modifique un perfil iOS Apple existente o añada uno nuevo.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **iOS** de la lista de plataformas.



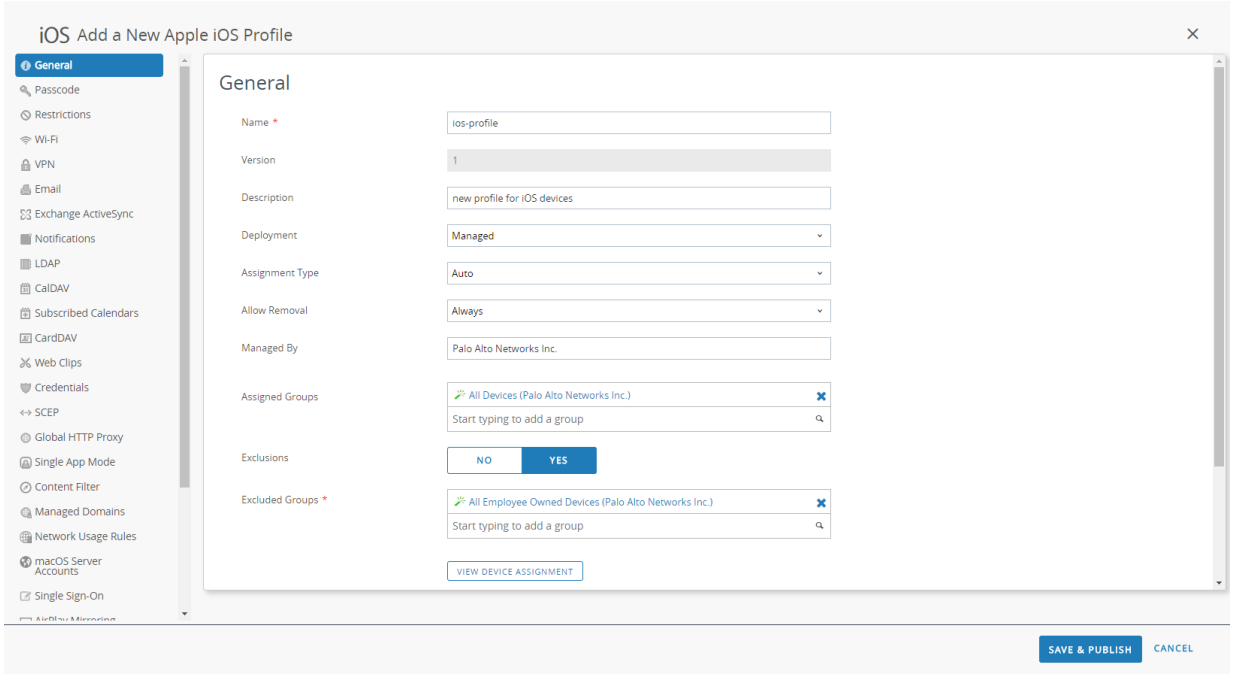
STEP 3 | Configure los ajustes en **General**:

1. Introduzca un **Name (Nombre)** para el perfil.
2. (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Seleccione el método **Deployment (Implementación)**, que determina si se eliminará el perfil automáticamente luego de la cancelación de la inscripción, ya sea **Managed (Administrada)** (se elimina el perfil) o **Manual** (el perfil permanece instalado hasta que el usuario final lo elimina).
4. (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
5. (Opcional) Seleccione si desea habilitar la opción **Allow Removal (Permitir eliminación)** del perfil para el usuario final. Seleccione **Always (Siempre)** para permitir que el usuario final elimine manualmente el perfil en cualquier momento, **Never (Nunca)** para evitar que lo elimine o **With Authorization (Con autorización)** para permitir que pueda eliminarlo con la autorización del administrador. Si se elige la opción **With Authorization (Con autorización)**, se añade una contraseña obligatoria.
6. (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
7. (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
8. (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.
9. (Opcional) Si habilita la opción de **Install only on devices inside selected areas (Instalar únicamente en dispositivos dentro de las áreas seleccionadas)**, el perfil puede instalarse únicamente en endpoints en la geocerca o regiones de iBeacon especificados. Cuando se le indique, añada la geocerca o regiones de iBeacon en el campo **Assigned Geofence Areas (Áreas de geocerca asignadas)**.
10. (Opcional) Si selecciona la opción **Enable Scheduling and install only during selected time periods (Habilitar los plazos e instalar únicamente durante los períodos de tiempo seleccionados)**, puede aplicar un plazo (**Devices [Dispositivos]** > **Profiles & Resources [Perfiles y recursos]** > **Profiles Settings [Ajustes de perfil]** > **Time Schedules [Plazos]**) para la instalación del perfil, que limita los períodos de tiempo durante los cuales se puede instalar el perfil en los endpoints. Cuando se le indique, introduzca el nombre del plazo en el campo **Assigned Schedules (Plazos asignados)**.
11. (Opcional) Seleccione la **Removal Date (Fecha de eliminación)** en la cual desea que se elimine el perfil de todos los endpoints.

© 2020 Palo Alto Networks, Inc.



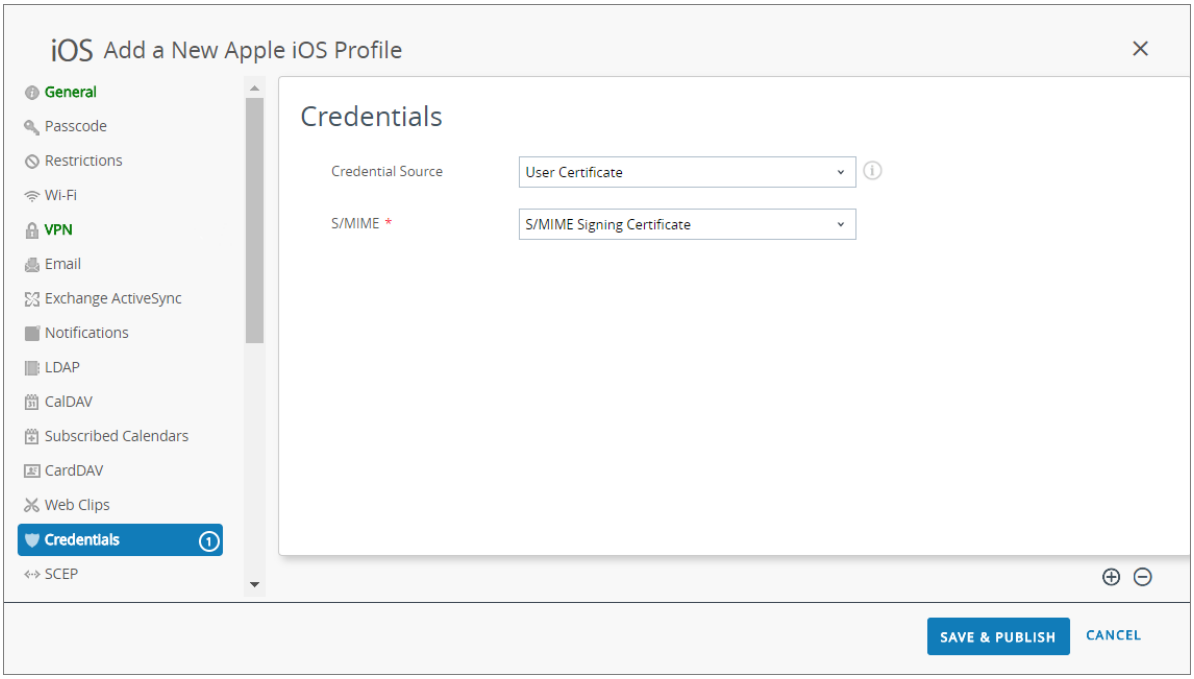
STEP 4 | Configure los ajustes de **Credentials (Credenciales)**:

Todas las configuraciones de VPN de acceso remoto para endpoints iOS requieren autenticación basada en certificado.

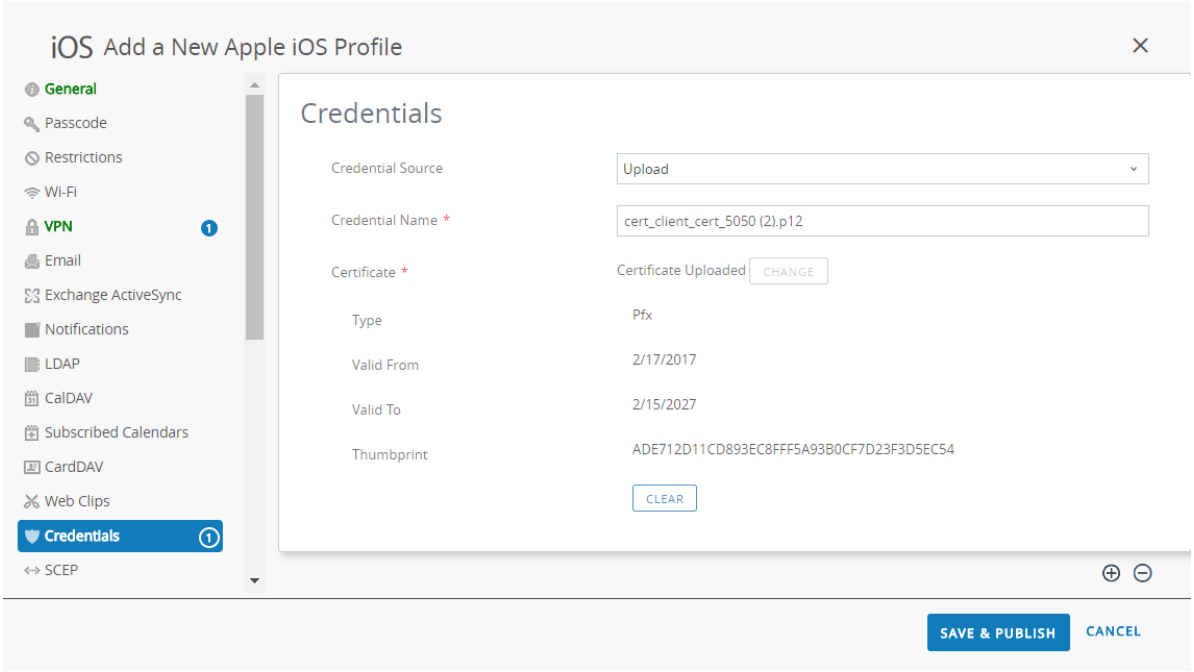
A partir de iOS 12, si desea usar certificados de cliente para la autenticación de cliente de GlobalProtect, debe implementar los certificados de cliente como parte del perfil de VPN que se envía desde el servidor de MDM. Si implementa certificados de cliente desde el servidor de MDM con otro método, la aplicación de GlobalProtect no puede usar los certificados.

- Para extraer certificados de cliente de usuarios de AirWatch:
  1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
  2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).

© 2020 Palo Alto Networks, Inc.



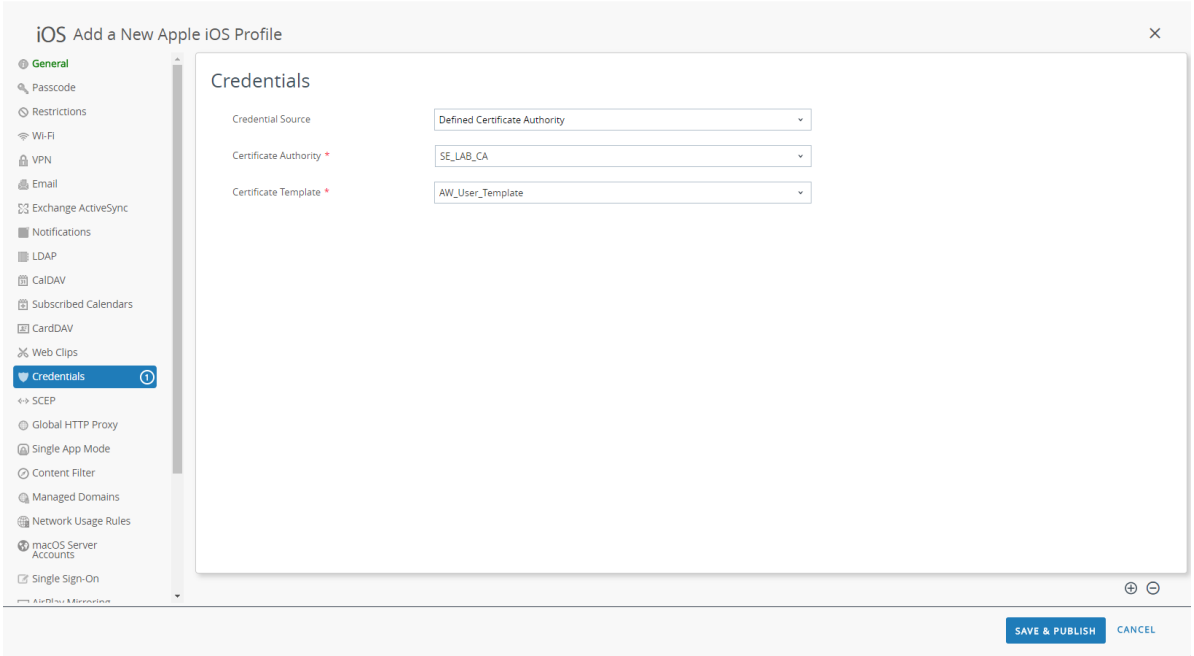
- Para cargar un certificado de cliente manualmente:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
  2. Introduzca el **Credential Name (Nombre de credencial)**.
  3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
  4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.



- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.

© 2020 Palo Alto Networks, Inc.

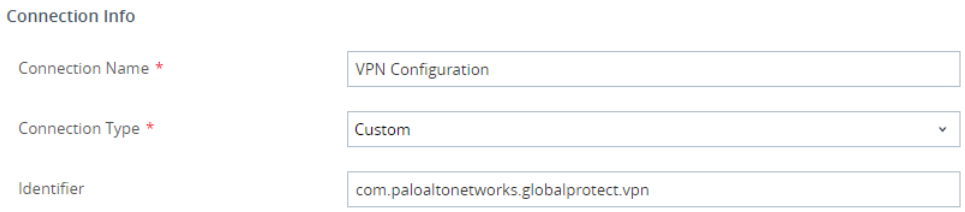
3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.



STEP 5 | Configure los ajustes de **VPN**.

1. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
2. Seleccione el **Connection Type (Tipo de conexión)** de la red:
   - Para la aplicación GlobalProtect 4.1.x y versiones anteriores, seleccione **Palo Alto Networks GlobalProtect**.
   - Para la aplicación GlobalProtect 5.0 y versiones posteriores, seleccione **Custom (Personalizado)**.
3. (Opcional) Si en **Connection Type (Tipo de conexión)**, selecciona **Custom (Personalizado)**, introduzca el ID de paquete (**com.paloaltonetworks.globalprotect.vpn**) en el campo **Identifier (Identificador)** para identificar la aplicación de GlobalProtect.

   *Si descargó la aplicación de GlobalProtect directamente de la App Store de Apple en China, especifique el ID del paquete (**com.paloaltonetworks.globalprotect.vpncn**) en el campo Identifier (Identificador)*



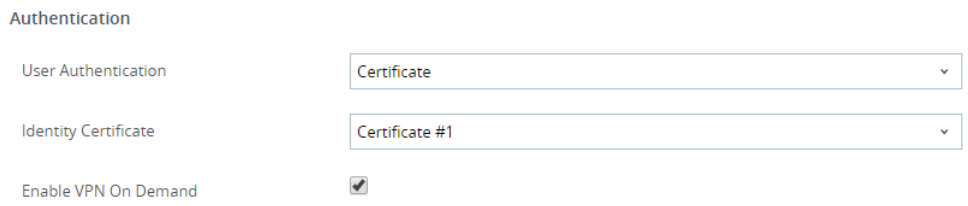
4. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
5. (Opcional) Introduzca el nombre de usuario de la **Account (Cuenta)** de VPN o haga clic en el botón añadir (**+**) para ver los valores de búsqueda compatibles que puede introducir.
6. (Opcional) En el campo **Disconnect on idle (Desconectar por inactividad)**, especifique la cantidad de tiempo (en segundos) después de la cual se cierra la sesión de los endpoints de la aplicación de GlobalProtect después de que la aplicación deja de enrutar tráfico a través del túnel de VPN.

© 2020 Palo Alto Networks, Inc.

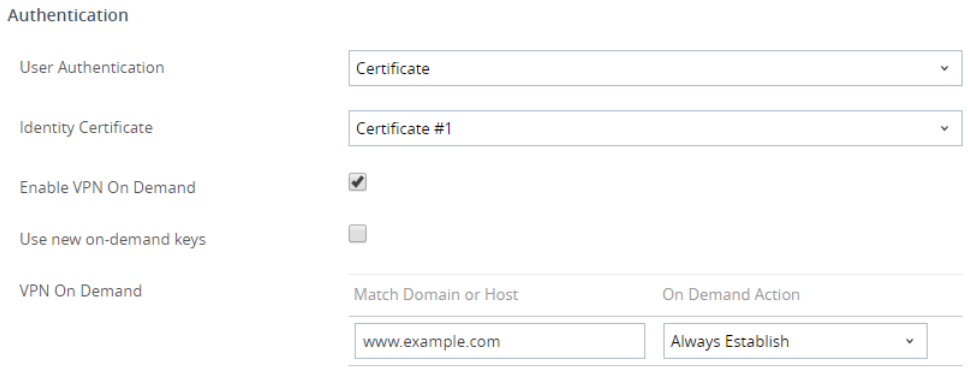
7. En el área Authentication (Autenticación), seleccione **Certificate (Certificado)** como método de **Authentication (Autenticación)**.

   Todas las configuraciones de VPN de acceso remoto para endpoints iOS requieren autenticación basada en certificado.

8. Cuando se le indique, seleccione el **Identity Certificate (Certificado de identidad)** que GlobalProtect usará para autenticar usuarios. El **Identity Certificate (Certificado de identidad)** es el mismo certificado que configuró en los ajustes de **Credentials (Credenciales)**.
9. Asegúrese de que la opción **Enable VPN On Demand (Habilitar VPN a demanda)** esté habilitada (ajuste predeterminado).

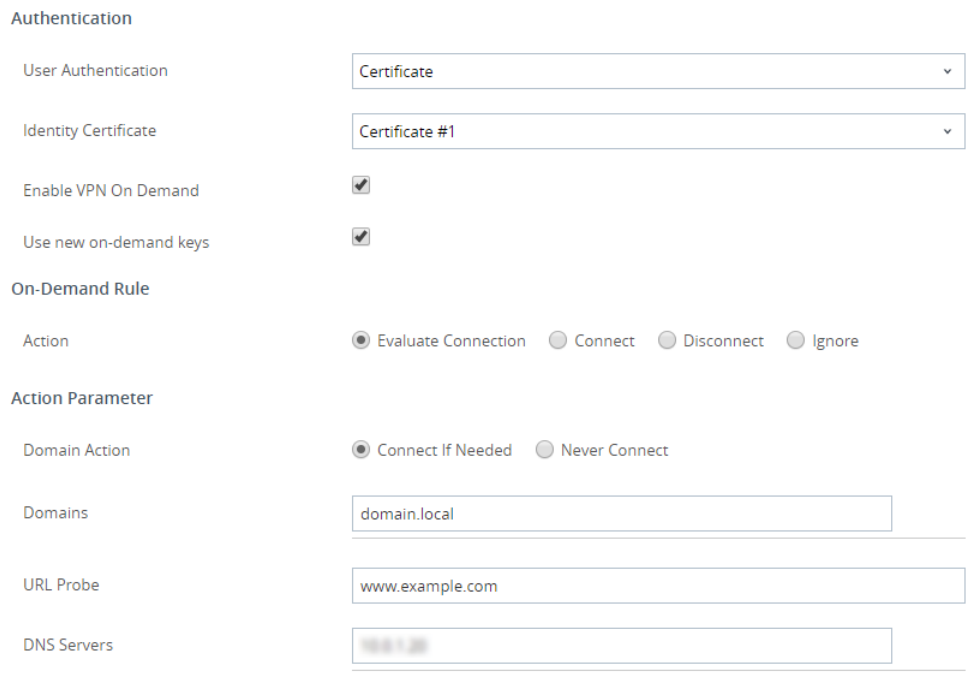


10. (Opcional) Configure las reglas de conexión de **VPN On-Demand (VPN a demanda)** heredadas:
    - **Match Domain or Host (Dominio o host para la coincidencia)**: introduzca el dominio o nombre de host que activa la conexión a GlobalProtect cuando acceden los usuarios.
    - **On Demand Action (Acción a demanda)**: en **On Demand Action (Acción a demanda)**, seleccione **Establish if Needed (Establecer si fuera necesario)** o **Always Establish (Establecer siempre)** para establecer la conexión a GlobalProtect únicamente si los usuarios no pueden conectarse directamente a un dominio o nombre de host especificado. En **On Demand Action (Acción a demanda)**, seleccione **Never Establish (Nunca establecer)** para evitar que se establezca la conexión a GlobalProtect cuando los usuarios acceden al dominio o nombre de host especificado. Si ya se estableció la conexión, se puede continuar con.

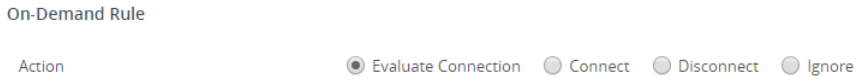


11. (Opcional) Establezca más reglas de conexión granular a demanda habilitando la opción **Use new on-demand keys (Usar nuevas claves a demanda)** para la aplicación de GlobalProtect. Puede añadir varias reglas haciendo clic en **ADD RULE (AÑADIR REGLA)**.

© 2020 Palo Alto Networks, Inc.



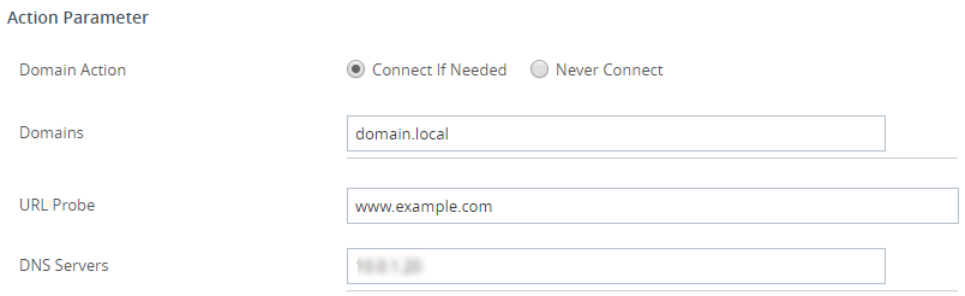
- En el área On-Demand Rule (Regla a demanda), seleccione una **Action (Acción)** que se aplicará a la conexión a GlobalProtect en función de los criterios que defina:
  - **Evaluate Connection (Evaluar conexión)**: establece automáticamente la conexión a GlobalProtect en función de los ajustes de red y conexión. Esta evaluación se produce cada vez que un usuario intenta conectarse a un dominio.
  - **Connect (Conectar)**: establece automáticamente la conexión a GlobalProtect.
  - **Disconnect (Desconectar)**: deshabilita GlobalProtect automáticamente y evita que GlobalProtect vuelva a conectarse.
  - **Ignore (Ignorar)**: deja la conexión existente de GlobalProtect como está y evita que GlobalProtect se vuelva a conectar si se desconecta.



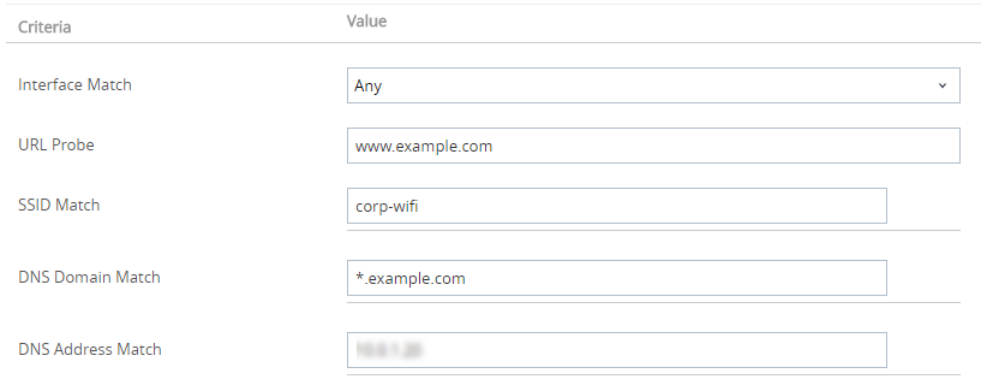
- (Opcional) Si establece la **Action (Acción)** para su regla de conexión a demanda en **Evaluate Connection (Evaluar conexión)**, también debe configurar un parámetro de acción para especificar si GlobalProtect puede intentar volver a conectarse si falla la resolución del nombre de dominio durante la evaluación de la conexión (por ejemplo, si el servidor DNS no responde debido a un tiempo de espera). Puede añadir varios parámetros haciendo clic en **ADD ACTION PARAMETERS (AÑADIR PARÁMETROS DE ACCIÓN)**.
  - En **Domain Action (Acción de dominio)**, seleccione **Connect if Needed (Conectar si fuera necesario)** para permitir que GlobalProtect se vuelva a conectar o en **Never Connect (Nunca conectar)** para evitar que GlobalProtect se vuelva a conectar.
  - Introduzca los **Domains (Dominios)** a los que se aplica este **Action Parameter (Parámetro de acción)**.
  - (Opcional) Si en **Domain Action (Acción de dominio)**, selecciona **Connect if Needed (Conectar si fuera necesario)**, introduzca la URL HTTP o HTTPS que desea sondear en el campo **URL Probe (Sondeo de URL)**. Si el nombre de host de la URL no se puede resolver, no es posible conectarse al servidor o el servidor no responde con un código de estado HTTP 200, se establece la conexión a GlobalProtect.

© 2020 Palo Alto Networks, Inc.

- (Opcional) Si en **Domain Action (Acción de dominio)**, selecciona **Connect if Needed (Conectar si fuera necesario)**, introduzca las direcciones IP de los **DNS Servers (Servidores DNS)** (internos o externos de confianza) que se usan para resolver los **Domains (Dominios)** especificados. Si no es posible conectarse a los servidores DNS, se establece la conexión a GlobalProtect.



- Configure los siguientes criterios de coincidencia para su regla de conexión a demanda. Si un endpoint coincide con todos los criterios especificados, la regla de conexión a demanda se aplica a ese endpoint.
  - **Interface Match (Coincidencia de interfaz)**: especifique el tipo de conexión que coincidirá con el adaptador de red del endpoint: **Any (Cualquiera)**, **Ethernet**, **Wi-Fi**, **Cellular (Celular)**.
  - **URL Probe (Sondeo de URL)**: introduzca la URL HTTP o HTTPS para buscar coincidencias. Si la coincidencia es adecuada, se devuelve un código de estado HTTP 200.
  - **SSID Match (Coincidencia de SSID)**: introduzca la SSID de red para buscar coincidencias. Puede añadir varios SSID de red haciendo clic en el botón añadir (**+**). Para obtener una coincidencia, debe coincidir, al menos, un SSI de red del endpoint especificado.
  - **DNS Domain Match (Coincidencia de dominio DNS)**: introduzca el dominio DNS para buscar coincidencias. También puede buscar coincidencias con un comodín (como `*.example.com`) para incluir todos los subdominios.
  - **DNS Address Match (Coincidencia de dirección DNS)**: introduzca la dirección IP del servidor DNS para buscar coincidencias. Puede añadir varias direcciones IP de servidores DNS haciendo clic en el botón añadir (**+**). Además, puede buscar coincidencias con un comodín (como `17.*`) que incluye todos los servidores DNS sin direcciones IP. Para obtener una coincidencia adecuada, todas las direcciones IP del servidor DNS en el endpoint deben coincidir con las direcciones IP del servidor DNS especificado.



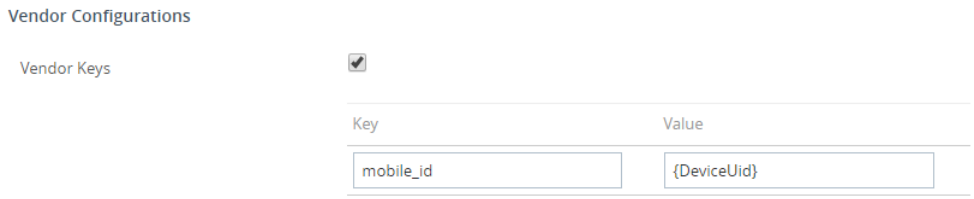
12.(Opcional) Seleccione el tipo de **Proxy** y configure los ajustes relevantes.

STEP 6 | (Opcional) (a partir de GlobalProtect 5.0) Si su implementación de GlobalProtect requiere HIP integration with MDM (Integración de HIP con MDM), especifique el atributo de identificador de dispositivo único (unique device identifier, UDID).

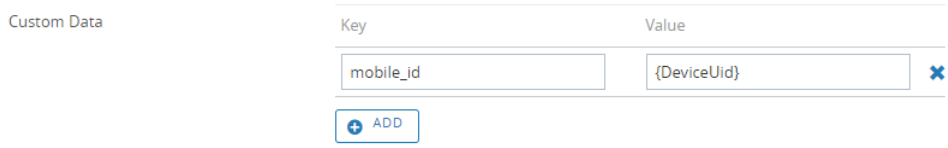
© 2020 Palo Alto Networks, Inc.

GlobalProtect admite la integración con MDM para obtener atributos de dispositivos móviles desde el servidor MDM, que se usarán en la aplicación de la política basada en HIP. Para que la integración con MDM funcione, la aplicación de GlobalProtect debe presentar el UDID del endpoint en la puerta de enlace de GlobalProtect. El atributo UDID permite a la aplicación de GlobalProtect recuperar y usar información de UDID en implementaciones basadas en MDM. Si elimina el atributo de UDID del perfil, ya no podrá usar la integración con MDM. La aplicación de GlobalProtect genera un nuevo UDID, pero no se puede usar para la integración.

- Si usa el **Connection Type (Tipo de conexión)** de la red **Palo Alto Networks GlobalProtect**, vaya a los ajustes de **VPN** y habilite las **Vendor Keys (Claves de proveedor)** en el área Vendor Configuration (Configuración de proveedor). En **Key (Clave)**, seleccione **`mobile_id`** y en **Value (Valor)**, seleccione **`{DeviceUid}`**.



- Si usa el **Connection Type (Tipo de conexión)** de la red **Custom (Personalizada)**, vaya a los ajustes de **VPN** y haga clic en **ADD (Añadir)** para añadir los **Custom Data (Datos personalizados)** en el área Connection Info (Información de conexión). En **Key (Clave)**, seleccione **`mobile_id`** y en **Value (Valor)**, seleccione **`{DeviceUid}`**.



STEP 7 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints de Windows 10 UWP con AirWatch

En una configuración de VPN de acceso remoto (a demanda), los usuarios deben iniciar manualmente la aplicación para establecer la conexión segura de GlobalProtect. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect se enruta a través del túnel VPN únicamente después de que los usuarios inician y establecen la conexión.

Debido a que AirWatch aún no incluye a GlobalProtect como un proveedor oficial de conexión para los endpoints de Windows, usted debe seleccionar un proveedor de VPN alternativo, editar los ajustes para la aplicación de GlobalProtect e importar la configuración nuevamente en el perfil VPN según se describe en el siguiente flujo de trabajo.

Use los siguientes pasos para establecer una configuración de VPN de acceso remoto iniciada por el usuario para endpoints de Windows 10 UWP con AirWatch:

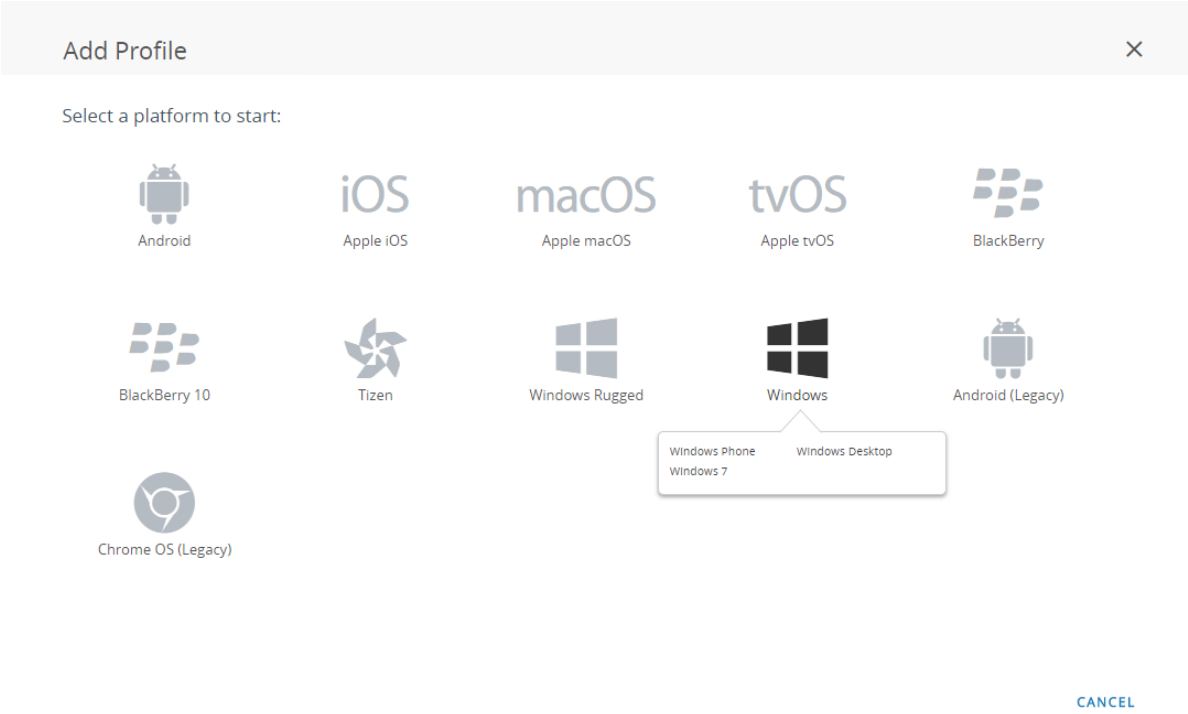
STEP 1 | Descargue la aplicación de GlobalProtect para Windows 10 UWP:

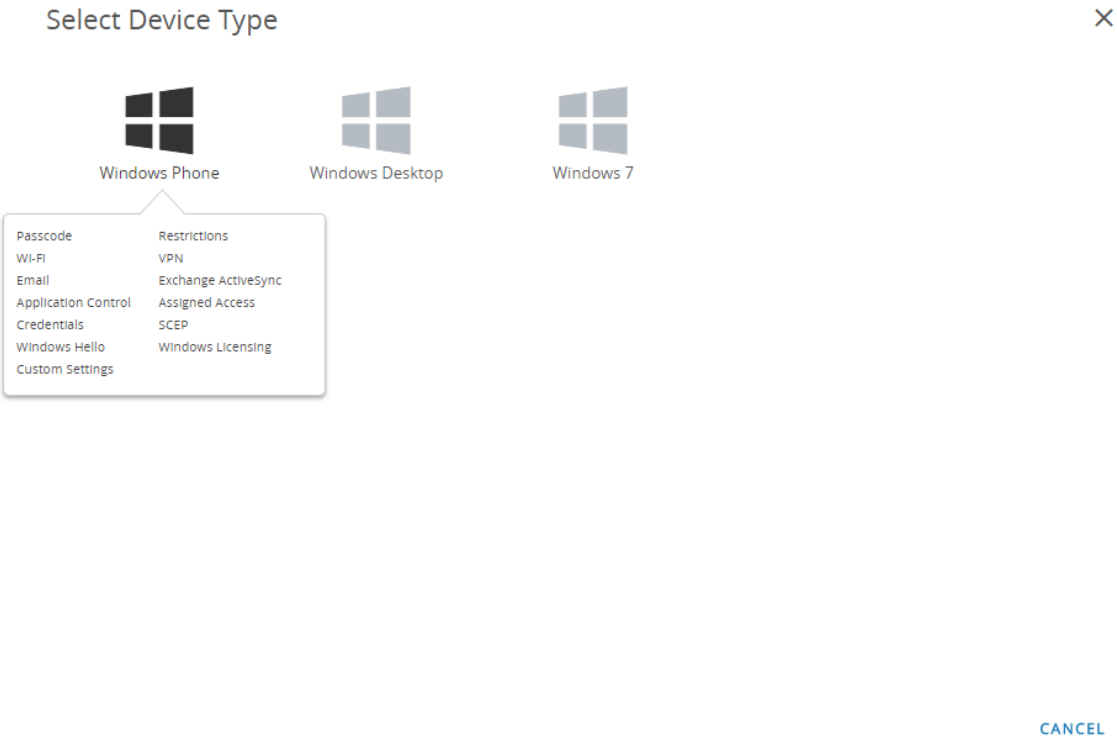
- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde Microsoft Store.

© 2020 Palo Alto Networks, Inc.

STEP 2 | En la consola de AirWatch, modifique un perfil de Windows 10 UWP existente o añada uno nuevo.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **Windows** como la plataforma y **Windows Phone** como el tipo de dispositivo.

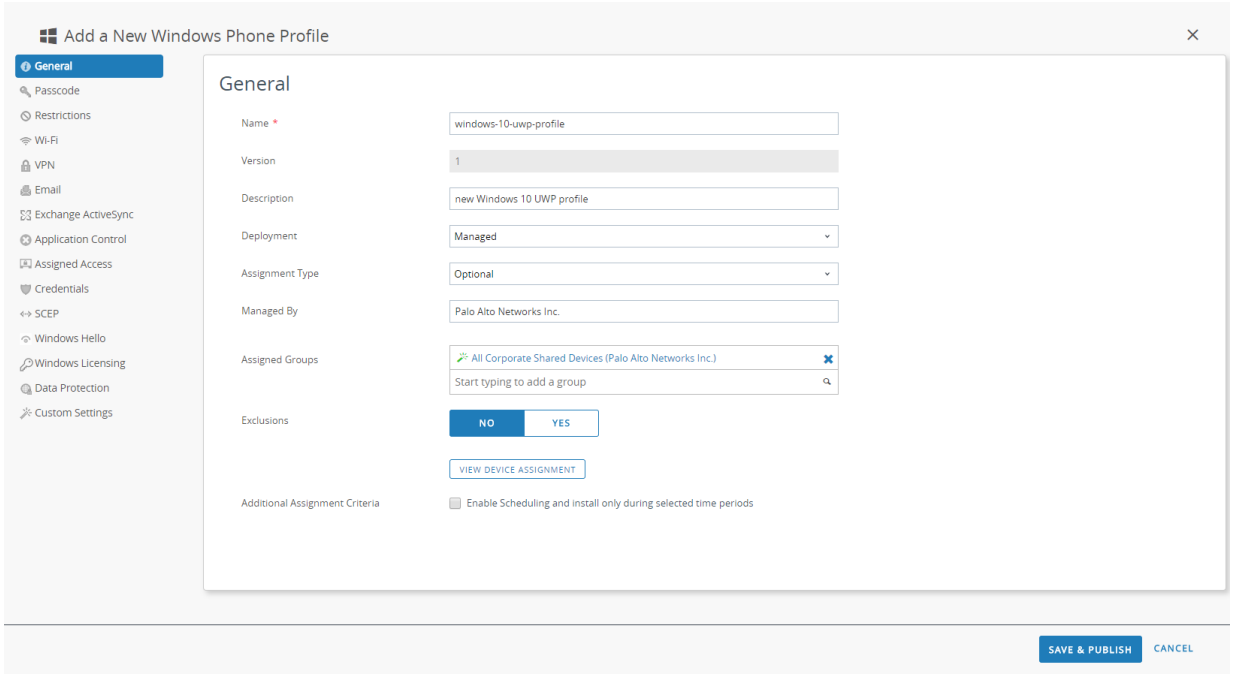




© 2020 Palo Alto Networks, Inc.

STEP 3 | Configure los ajustes en **General**:

1. Introduzca un **Name (Nombre)** para el perfil.
2. (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.
3. (Opcional) En el método de **Deployment (Implementación)**, seleccione **Managed (Gestionado)** para permitir que el perfil se elimine automáticamente luego de la cancelación de la inscripción
4. (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
5. (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
6. (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
7. (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.
8. (Opcional) Si selecciona la opción **Enable Scheduling and install only during selected time periods (Habilitar los plazos e instalar únicamente durante los períodos de tiempo seleccionados)**, puede aplicar un plazo (**Devices [Dispositivos]** > **Profiles & Resources [Perfiles y recursos]** > **Profiles Settings [Ajustes de perfil]** > **Time Schedules [Plazos]**) para la instalación del perfil, que limita los períodos de tiempo durante los cuales se puede instalar el perfil en los endpoints. Cuando se le indique, introduzca el nombre del plazo en el campo **Assigned Schedules (Plazos asignados)**.

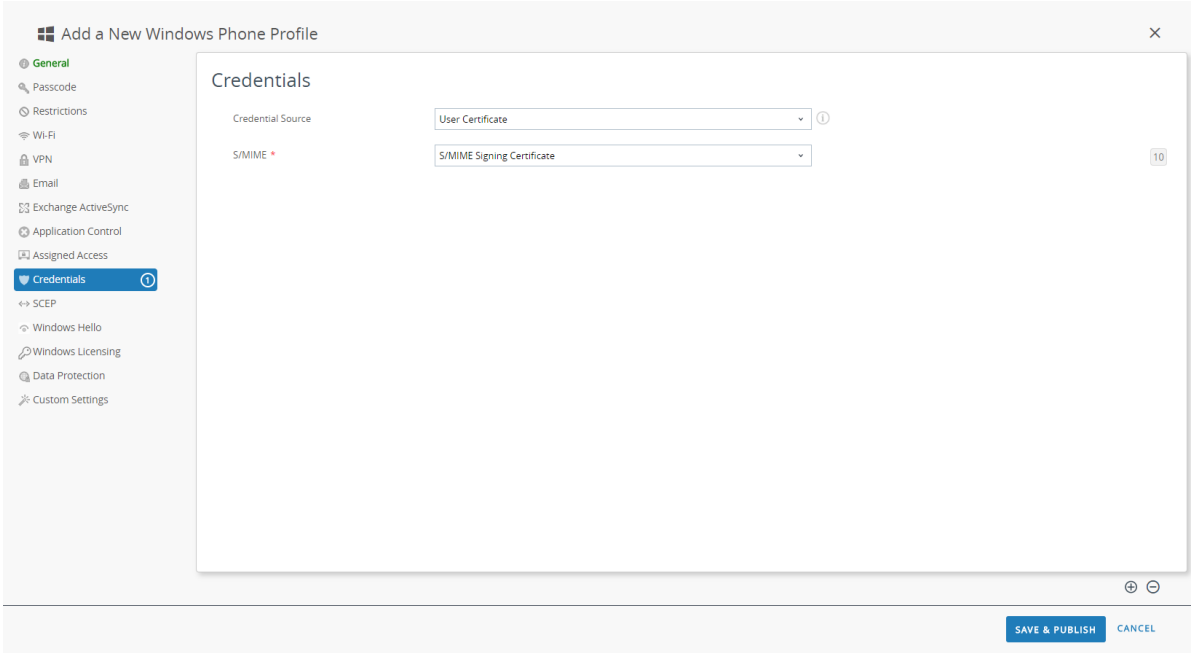


STEP 4 | (Opcional) Si su implementación de GlobalProtect requiere autenticación del certificado de cliente, configure los ajustes de las **Credentials (Credenciales)**:

- Para extraer certificados de cliente de usuarios de AirWatch:

© 2020 Palo Alto Networks, Inc.

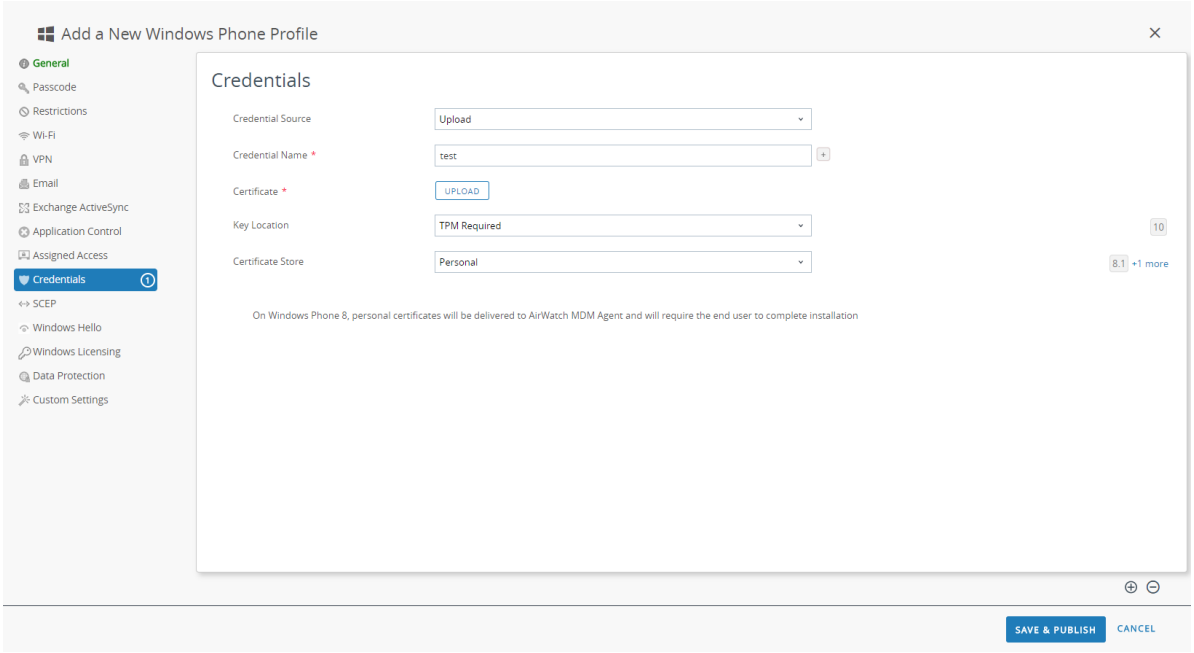
1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).



- Para cargar un certificado de cliente manualmente:

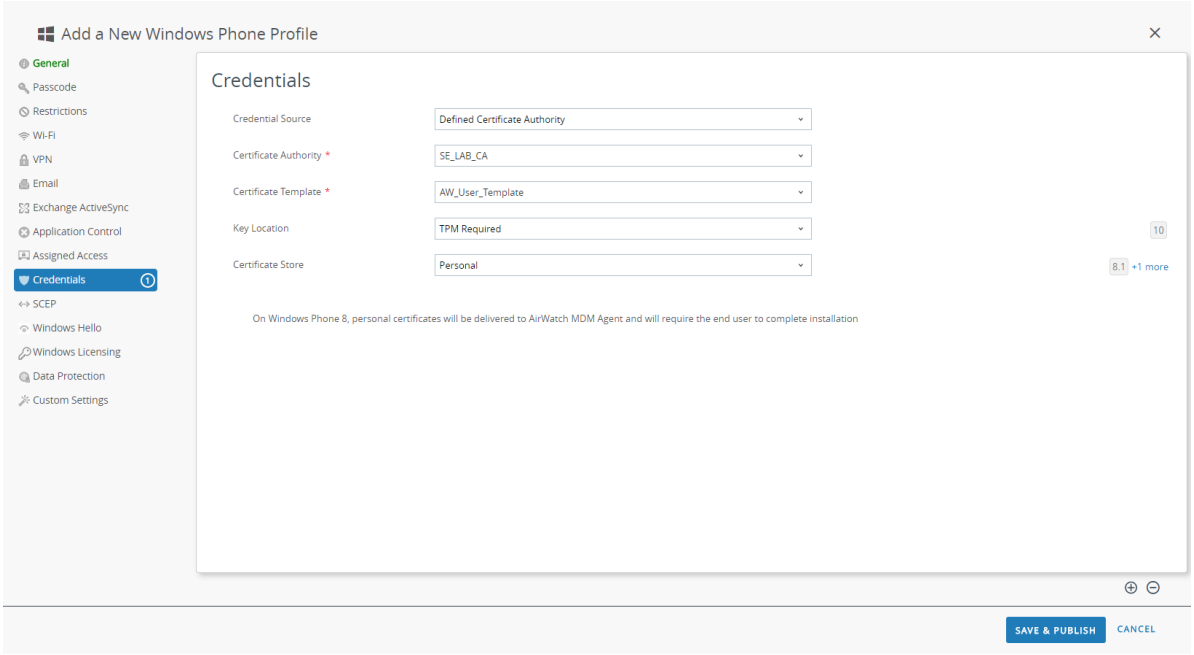
1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
2. Introduzca el **Credential Name (Nombre de credencial)**.
3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.
5. Seleccione la **Key Location (Ubicación de clave)** donde desea almacenar la clave privada del certificado:
   - **TPM Required (TPM requerida)**: almacene la clave privada en un módulo de plataforma fiable. Si un módulo de plataforma fiable no está disponible en el endpoint, no se puede instalar la clave privada.
   - **TPM If Present (TPM si está presente)**: almacene la clave privada en un módulo de plataforma fiable si hay uno disponible en el endpoint. Si un módulo de plataforma fiable no está disponible en el endpoint, la clave privada se almacena en el software del endpoint.
   - **Software**: almacene la clave privada en el software del endpoint.
   - **Passport**: guarde la clave privada en Microsoft Passport. Para usar esta opción, se debe instalar AirWatch Protection Agent en el endpoint.
6. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.

© 2020 Palo Alto Networks, Inc.



- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.
  3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.
  4. Seleccione la **Key Location (Ubicación de clave)** donde desea almacenar la clave privada del certificado:
     - **TPM Required (TPM requerida)**: almacene la clave privada en un módulo de plataforma fiable. Si un módulo de plataforma fiable no está disponible en el endpoint, no se puede instalar la clave privada.
     - **TPM If Present (TPM si está presente)**: almacene la clave privada en un módulo de plataforma fiable si hay uno disponible en el endpoint. Si un módulo de plataforma fiable no está disponible en el endpoint, la clave privada se almacena en el software del endpoint.
     - **Software**: almacene la clave privada en el software del endpoint.
     - **Passport**: guarde la clave privada en Microsoft Passport. Para usar esta opción, se debe instalar AirWatch Protection Agent en el endpoint.
  5. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.

© 2020 Palo Alto Networks, Inc.

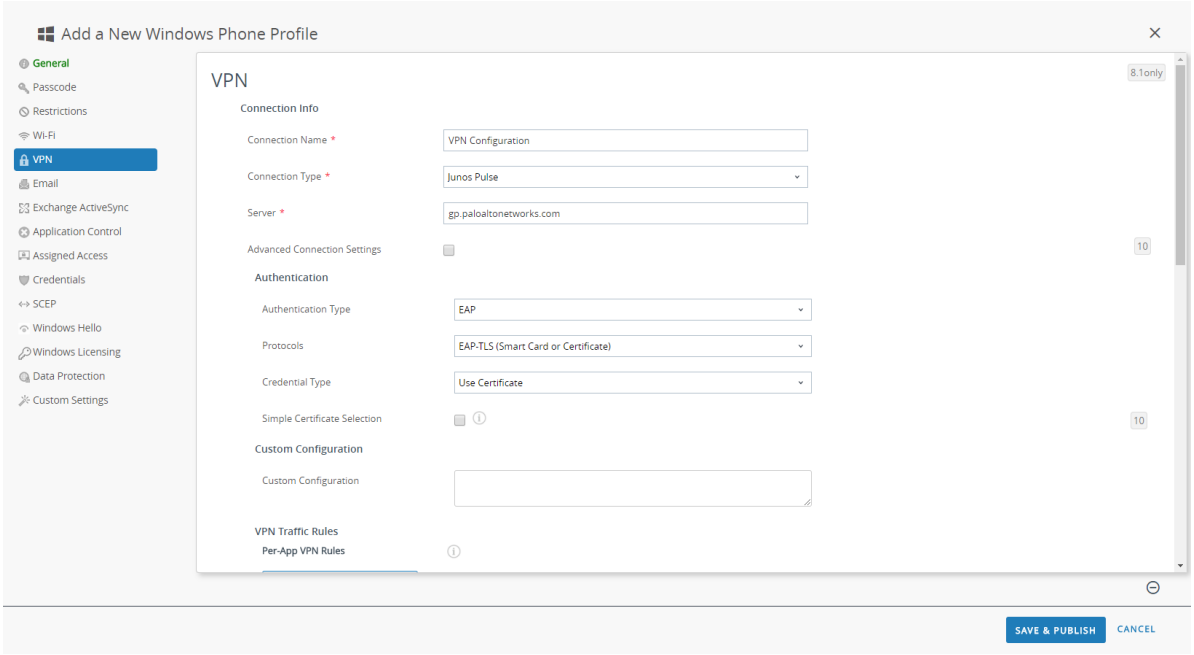


STEP 5 | Configure los ajustes de **VPN**.

1. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
2. Seleccione un proveedor de **Connection Type (Tipo de conexión)** alternativo (no seleccione **IKEv2**, **L2TP**, **PPTP** o **Automatic [Automático]**, ya que estos no tienen los ajustes del proveedor asociado necesarios para el perfil de VPN de GlobalProtect).

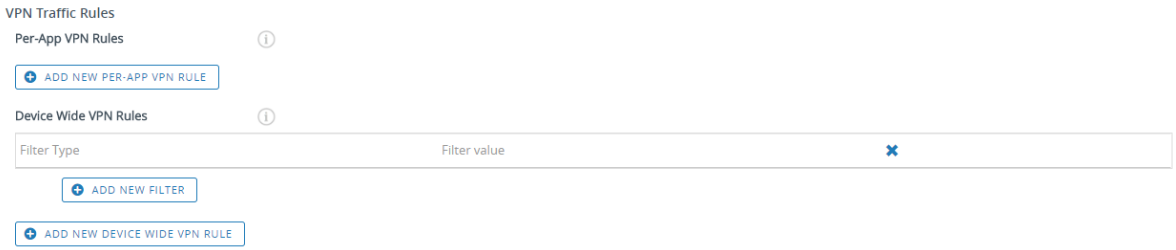
   Debe seleccionar un proveedor alternativo debido a que AirWatch aún no incluye a GlobalProtect como proveedor oficial de conexión para los endpoints de Windows.
3. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
4. En el área Authentication (Autenticación), seleccione un **Authentication Type (Tipo de autenticación)** para especificar el método de autenticación de los usuarios finales.

© 2020 Palo Alto Networks, Inc.



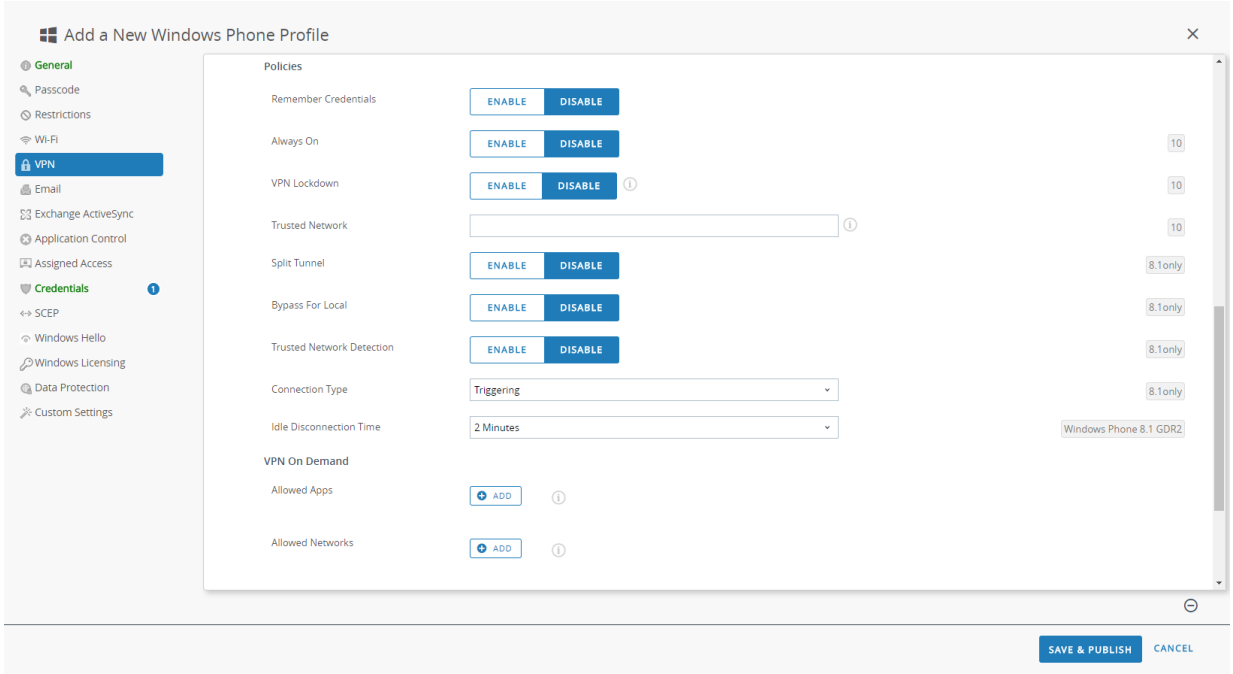
5. (Opcional) Para permitir que GlobalProtect guarde las credenciales de usuario, seleccione **ENABLE (HABILITAR)** para habilitar la opción **Remember Credentials (Recordar credenciales)** en el área Policies (Políticas).
6. (Opcional) En el área VPN Traffic Rules (Reglas de tráfico de VPN), seleccione **ADD NEW DEVICE WIDE VPN RULE (AÑADIR NUEVA REGLA DE VPN PARA DISPOSITIVOS)** para enviar a través del túnel de VPN el tráfico que coincida con una ruta específica. Estas reglas no están vinculadas por aplicación, pero se evalúan en todo el endpoint. Si el tráfico coincide con los criterios de coincidencia especificados, se dirige a través del túnel de VPN.

   Añada los criterios de coincidencia haciendo clic en **ADD NEW FILTER (Añadir nuevo filtro)**. Cuando se le indique, introduzca un **Filter Type (Tipo de filtro)** y el **Filter Value (Valor de filtro)** correspondiente.



7. Para garantizar que este perfil use el método de conexión a demanda, configure los siguientes ajustes en el área Policies (Políticas):
   - Seleccione **DISABLE (DESHABILITAR)** para **Always On (Siempre activada)**. Si este campo está **ENABLED (HABILITADO)**, la conexión segura siempre está activada.
   - Seleccione **DISABLE (DESHABILITAR)** para **VPN Lockdown (Bloqueo de VPN)**. Si se selecciona la opción **ENABLED (HABILITADO)** para este campo, la conexión segura siempre está activada y conectada, y el acceso a la red está deshabilitado cuando la aplicación no está conectada. La opción **VPN Lockdown (Bloqueo de VPN)** en AirWatch es similar a la opción **Enforce GlobalProtect for Network Access (Aplicar GlobalProtect para el acceso de red)** que configuraría en el portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.



STEP 6 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

STEP 7 | Para seleccionar GlobalProtect como proveedor de tipo de conexión, edite el perfil de VPN en XML.

Para minimizar las ediciones adicionales en el XML sin procesar, revise los ajustes de su perfil VPN antes de exportar la configuración. Si necesita cambiar un ajuste después de exportar el perfil VPN, puede realizar los cambios en el XML sin procesar o puede actualizar el ajuste en el perfil VPN y realizar este paso nuevamente.

1. En **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**, seleccione el botón de opción junto al nuevo perfil que añadió en los pasos previos y seleccione **</>XML** en la parte superior de la tabla. AirWatch abre la vista XML del perfil.
2. Exporte el perfil y luego ábralo en un editor de texto de su elección.
3. Edite los siguientes ajustes para GlobalProtect:

- En el elemento LocIURI que especifica PluginPackageFamilyName, cambie el elemento por:

  ```
  <LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/
  PluginPackageFamilyName</LocURI>
  ```
- En el elemento Data que sigue, cambie el valor por:

  ```
  <Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>
  ```

1. Guarde sus cambios en el perfil exportado.
2. Vuelva a AirWatch y seleccione **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**.
3. Cree (seleccione **Add (Añadir)** > **Add Profile (Añadir perfil)** > **Windows** > **Windows Phone**) y asigne un nombre a un perfil nuevo.
4. Seleccione **Custom Settings (Ajustes personalizados)** > **Configure (Configurar)** y luego copie y pegue la configuración modificada.
5. Haga clic en **Save & Publish** para guardar y publicar los cambios.

© 2020 Palo Alto Networks, Inc.

STEP 8 | Limpie el perfil original al seleccionarlo en **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**, y luego, **More Actions (Más acciones)** > **Deactivate (Desactivar)**. AirWatch traslada el perfil a la lista Inactive.

STEP 9 | Compruebe la configuración.

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario con Microsoft Intune

Microsoft Intune es una plataforma de gestión de movilidad empresarial basada en la nube que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por Microsoft Intune y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN de acceso remoto iniciada por el usuario con Microsoft Intune:

- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con Microsoft Intune

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con Microsoft Intune

En una configuración de VPN de acceso remoto (a demanda), los usuarios deben iniciar manualmente la aplicación para establecer la conexión segura de GlobalProtect. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect se enruta a través del túnel VPN únicamente después de que los usuarios inician y establecen la conexión.

Use los siguientes pasos para establecer una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con Microsoft Intune:

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

STEP 2 | (Opcional) Si su implementación requiere autenticación basada en certificados, configure un perfil de certificado.

STEP 3 | Cree un nuevo perfil de VPN para iOS.

- En **Platform (Plataforma)**, seleccione **iOS**.

STEP 4 | Configure los ajustes de VPN (acceso remoto) a demanda para endpoints iOS.

- En **Connection type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect**.
- En el área Ajustes de VPN automáticos, habilite **On-demand VPN (VPN a demanda)** para configurar las reglas condicionales que controlan en qué momento se inicia la conexión de VPN.

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario con MobileIron

MobileIron es una plataforma de gestión de movilidad empresarial que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por MobileIron y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

© 2020 Palo Alto Networks, Inc.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN de acceso remoto iniciada por el usuario con MobileIron:

- Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con MobileIron

Establecimiento de una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con MobileIron

En una configuración de VPN de acceso remoto (a demanda), los usuarios deben iniciar manualmente la aplicación para establecer la conexión segura de GlobalProtect. El tráfico que coincide con filtros específicos (como el puerto y la dirección IP) configurados en la puerta de enlace de GlobalProtect se enruta a través del túnel VPN únicamente después de que los usuarios inician y establecen la conexión.

Use los siguientes pasos para establecer una configuración de VPN de acceso remoto iniciada por el usuario para endpoints iOS con MobileIron:

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implementación de la aplicación móvil de GlobalProtect con MobileIron.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

STEP 2 | Añada la configuración de un certificado y configure los ajustes del certificado.

Todas las configuraciones de VPN a demanda requieren autenticación basada en certificado.

STEP 3 | Añada una configuración de VPN (acceso remoto) a demanda.

- En el tipo de configuración, seleccione **VPN On Demand (VPN a demanda)**.

STEP 4 | Configure ajustes de VPN a demanda para iOS.

- En **Connection Type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect** y configure los ajustes asociados.

Configuraciones VPN por aplicación

En una configuración VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enviar tráfico a través del túnel VPN de GlobalProtect. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN de GlobalProtect.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración VPN por aplicación usando sistemas de gestión de dispositivos móviles compatibles:

- Establecimiento de una configuración de VPN por aplicación con AirWatch
- Establecimiento de una configuración de VPN por aplicación con Microsoft Intune
- Establecimiento de una configuración de VPN por aplicación con MobileIron

Establecimiento de una configuración de VPN por aplicación con AirWatch

AirWatch es una plataforma de gestión de movilidad empresarial que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los dispositivos móviles gestionados por AirWatch y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN por aplicación con AirWatch:

- Establecimiento de una configuración de VPN por aplicación para endpoints iOS con AirWatch

© 2020 Palo Alto Networks, Inc.

- Establecimiento de una configuración de VPN por aplicación para endpoints Android con AirWatch
- Establecimiento de una configuración de VPN por aplicación para endpoints de Windows 10 UWP con AirWatch

Establecimiento de una configuración de VPN por aplicación para endpoints iOS con AirWatch

Puede habilitar el acceso a los recursos internos de sus endpoints móviles gestionados mediante la configuración del acceso VPN de GlobalProtect con AirWatch. En una configuración de VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enrutar tráfico a través del túnel VPN. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN.

Use los siguientes pasos para establecer una configuración de VPN por aplicación para endpoints iOS con AirWatch:

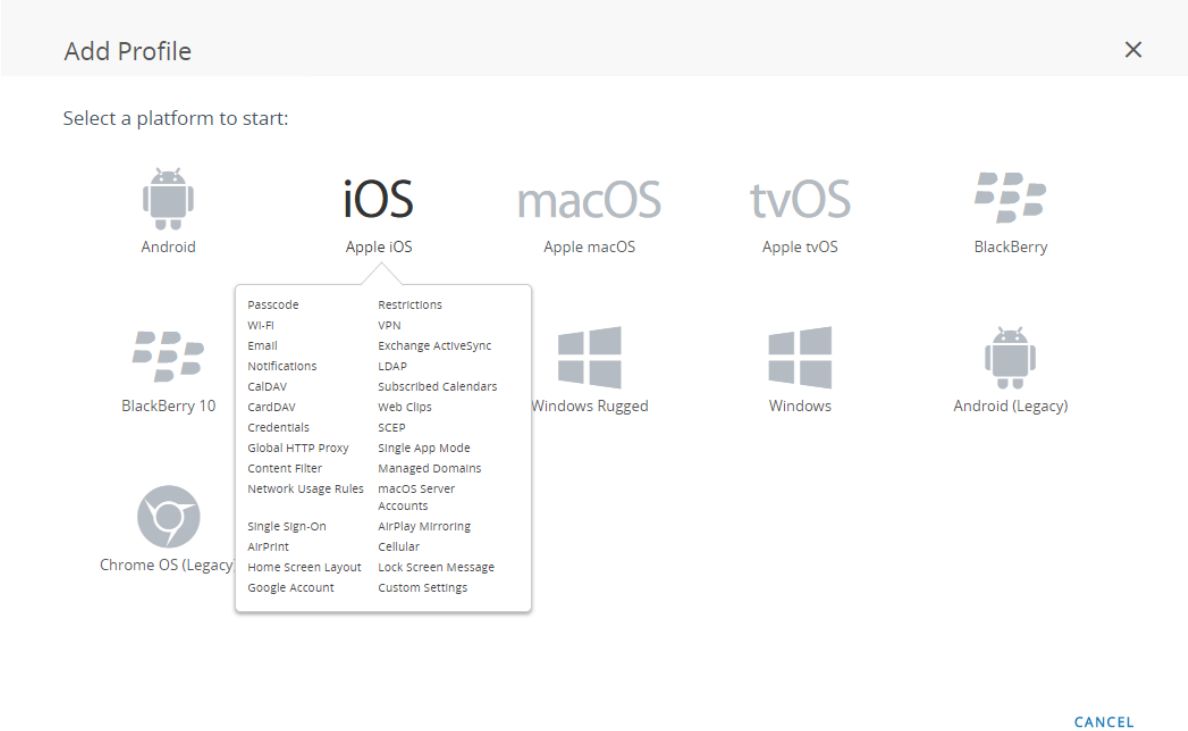
STEP 1 | Descargue la aplicación de GlobalProtect para iOS:

- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

La aplicación de GlobalProtect para iOS también está disponible en la App Store de Apple en China.

STEP 2 | Desde la consola de AirWatch, modifique un perfil iOS Apple existente o añada uno nuevo.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **iOS** de la lista de plataformas.

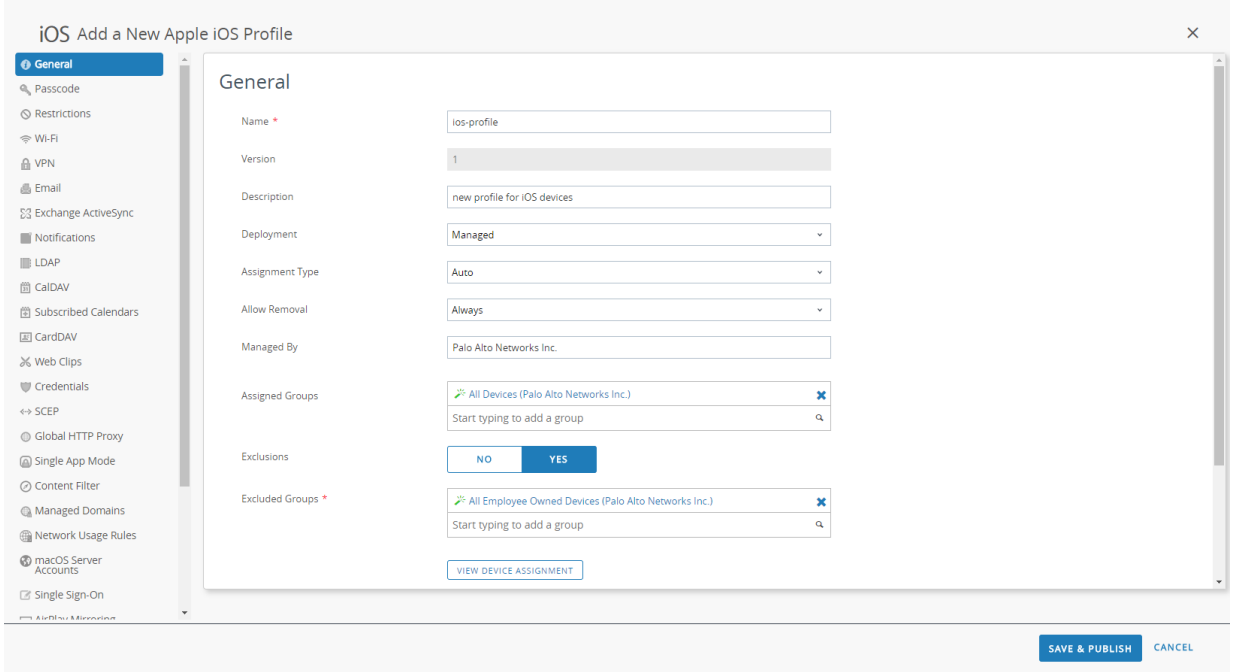


STEP 3 | Configure los ajustes en **General**:

1. Introduzca un **Name (Nombre)** para el perfil.
2. (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Seleccione el método **Deployment (Implementación)**, que determina si se eliminará el perfil automáticamente luego de la cancelación de la inscripción, ya sea **Managed (Administrada)** (se elimina el perfil) o **Manual** (el perfil permanece instalado hasta que el usuario final lo elimina).
4. (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
5. (Opcional) Seleccione si desea habilitar la opción **Allow Removal (Permitir eliminación)** del perfil para el usuario final. Seleccione **Always (Siempre)** para permitir que el usuario final elimine manualmente el perfil en cualquier momento, **Never (Nunca)** para evitar que lo elimine o **With Authorization (Con autorización)** para permitir que pueda eliminarlo con la autorización del administrador. Si se elige la opción **With Authorization (Con autorización)**, se añade una contraseña obligatoria.
6. (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
7. (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
8. (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.



STEP 4 | Configure los ajustes de **Credentials (Credenciales)**:

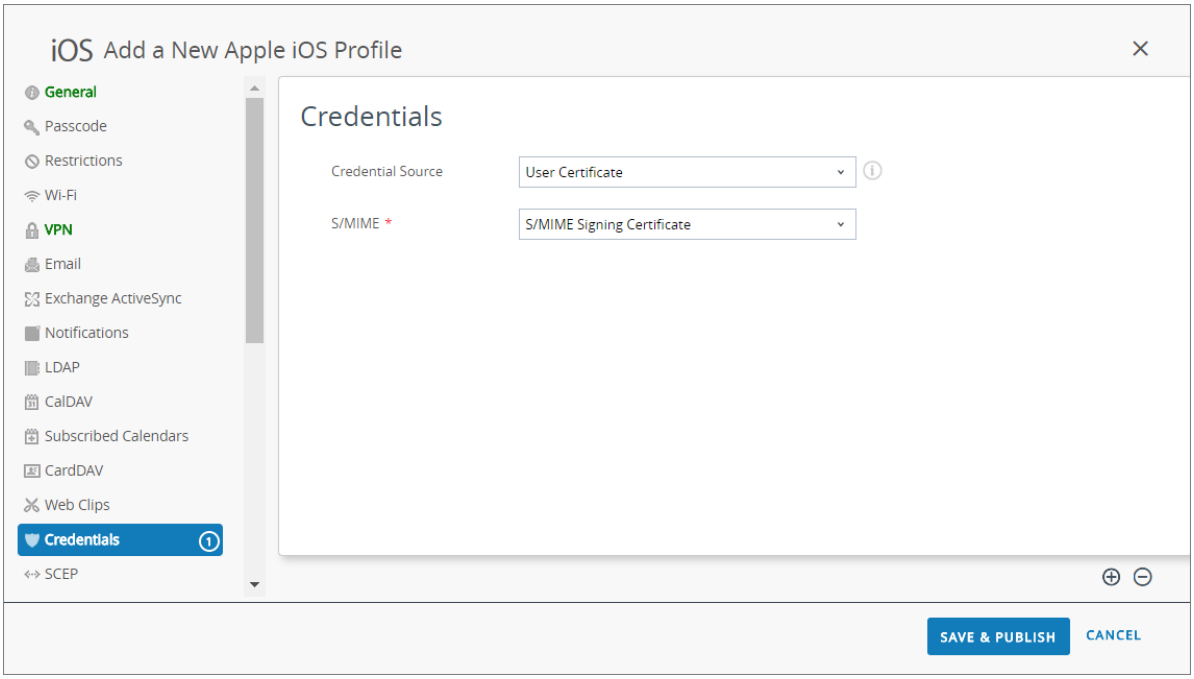
Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

A partir de iOS 12, si desea usar certificados de cliente para la autenticación de cliente de GlobalProtect, debe implementar los certificados de cliente como parte del perfil de VPN que se envía desde el servidor de MDM. Si implementa certificados de cliente

© 2020 Palo Alto Networks, Inc.

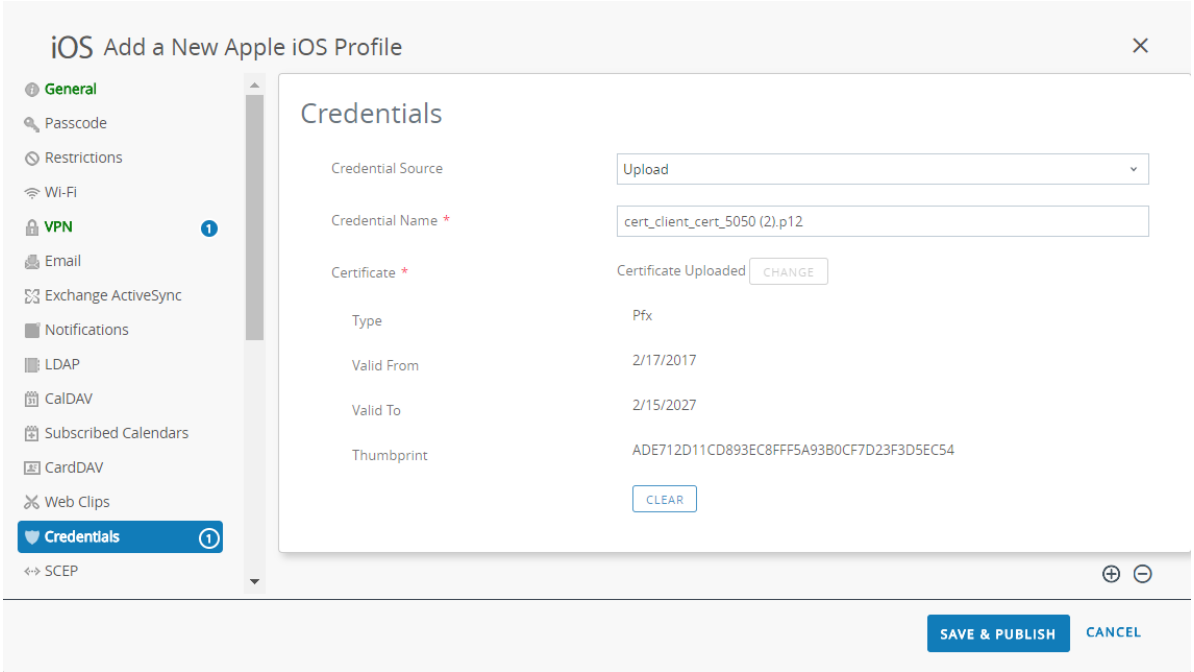
desde el servidor de MDM con otro método, la aplicación de GlobalProtect no puede usar los certificados.

- Para extraer certificados de cliente de usuarios de AirWatch:
  1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
  2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).

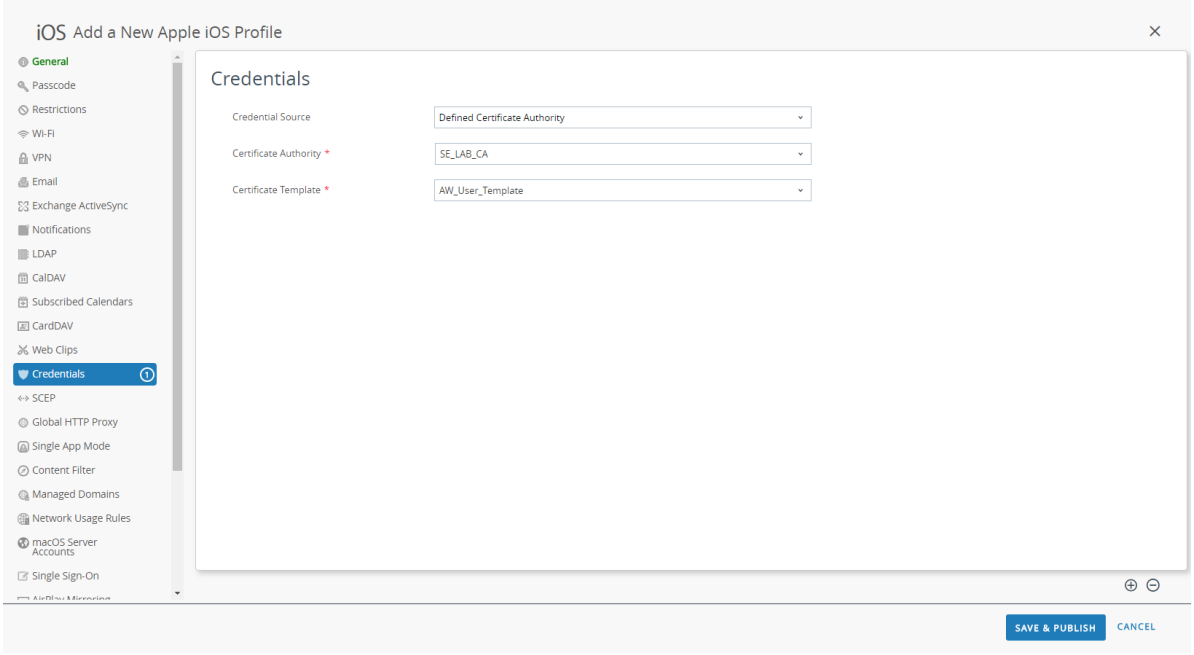


- Para cargar un certificado de cliente manualmente:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
  2. Introduzca el **Credential Name (Nombre de credencial)**.
  3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
  4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.

© 2020 Palo Alto Networks, Inc.



- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.
  3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.



STEP 5 | Configure los ajustes de **VPN**.

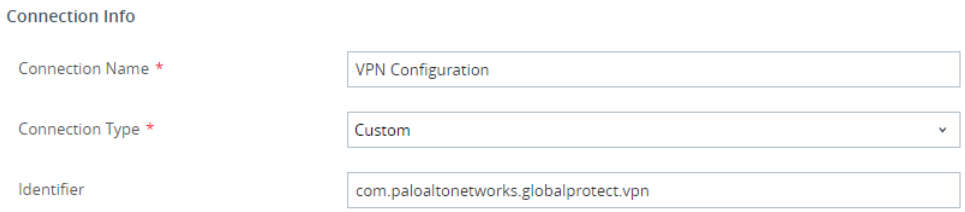
1. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
2. Seleccione el **Connection Type (Tipo de conexión)** de la red:

© 2020 Palo Alto Networks, Inc.

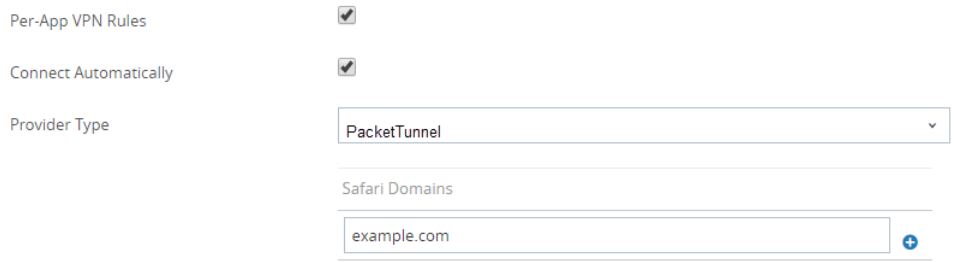
- Para la aplicación GlobalProtect 4.1.x y versiones anteriores, seleccione **Palo Alto Networks GlobalProtect**.
- Para la aplicación GlobalProtect 5.0 y versiones posteriores, seleccione **Custom (Personalizado)**.

3. (Opcional) Si en **Connection Type (Tipo de conexión)**, selecciona **Custom (Personalizado)**, introduzca el ID de paquete (**com.paloaltonetworks.globalprotect.vpn**) en el campo **Identifier (Identificador)** para identificar la aplicación de GlobalProtect.

   *Si descargó la aplicación de GlobalProtect directamente de la App Store de Apple en China, especifique el ID del paquete (**com.paloaltonetworks.globalprotect.vpncn**) en el campo Identifier (Identificador)*



4. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
5. (Opcional) Introduzca el nombre de usuario de la **Account (Cuenta)** de VPN o haga clic en el botón añadir (**+**) para ver los valores de búsqueda compatibles que puede introducir.
6. (Opcional) En el campo **Disconnect on idle (Desconectar por inactividad)**, especifique la cantidad de tiempo (en segundos) después de la cual se cierra la sesión de los endpoints de la aplicación de GlobalProtect después de que la aplicación deja de enrutar tráfico a través del túnel de VPN.
7. Habilite **Per App VPN Rules (Reglas de VPN por aplicación)** para enrutar todo el tráfico de aplicaciones gestionadas a través del túnel de VPN de GlobalProtect.
   - Habilite la opción **Connect Automatically (Conectar automáticamente)** de GlobalProtect para que se conecte automáticamente a los **Safari Domains (Dominios Safari)** especificados. Puede añadir varios **Safari Domains (Dominios Safari)** al clic en el botón añadir (**+**).
   - Seleccione el **Provider Type (Tipo de proveedor)** para indicar cómo se enviará el tráfico a través del túnel, ya sea en el nivel de la aplicación o en el de la IP. Utilice PacketTunnel.

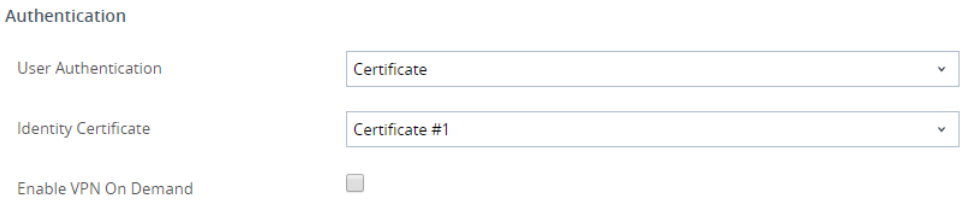


8. En el área Authentication (Autenticación), seleccione **Certificate (Certificado)** como método de **Authentication (Autenticación)**.

   Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

9. Cuando se le indique, seleccione el **Identity Certificate (Certificado de identidad)** que GlobalProtect usará para autenticar usuarios. El **Identity Certificate (Certificado de identidad)** es el mismo certificado que configuró en los ajustes de **Credentials (Credenciales)**.

© 2020 Palo Alto Networks, Inc.

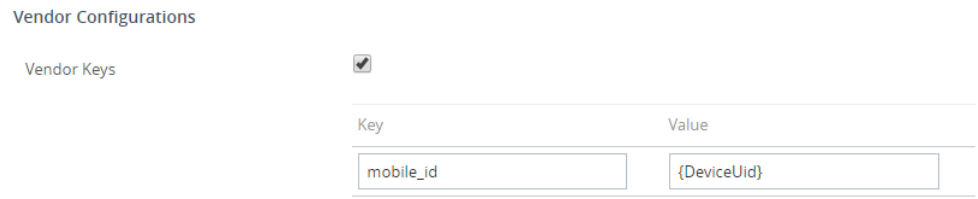


10.(Opcional) Seleccione el tipo de **Proxy** y configure los ajustes relevantes.

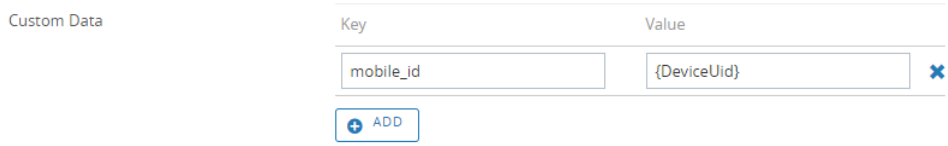
STEP 6 | (Opcional) (a partir de GlobalProtect 5.0) Si su implementación de GlobalProtect requiere HIP integration with MDM (Integración de HIP con MDM), especifique el atributo de identificador de dispositivo único (unique device identifier, UDID).

GlobalProtect admite la integración con MDM para obtener atributos de dispositivos móviles desde el servidor MDM, que se usarán en la aplicación de la política basada en HIP. Para que la integración con MDM funcione, la aplicación de GlobalProtect debe presentar el UDID del endpoint en la puerta de enlace de GlobalProtect. El atributo UDID permite a la aplicación de GlobalProtect recuperar y usar información de UDID en implementaciones basadas en MDM. Si elimina el atributo de UDID del perfil, ya no podrá usar la integración con MDM. La aplicación de GlobalProtect genera un nuevo UDID, pero no se puede usar para la integración.

- Si usa el **Connection Type (Tipo de conexión)** de la red **Palo Alto Networks GlobalProtect**, vaya a los ajustes de **VPN** y habilite las **Vendor Keys (Claves de proveedor)** en el área Vendor Configuration (Configuración de proveedor). En **Key (Clave)**, seleccione **`mobile_id`** y en **Value (Valor)**, seleccione **`{DeviceUid}`**.



- Si usa el **Connection Type (Tipo de conexión)** de la red **Custom (Personalizada)**, vaya a los ajustes de **VPN** y haga clic en **ADD (Añadir)** para añadir los **Custom Data (Datos personalizados)** en el área Connection Info (Información de conexión). En **Key (Clave)**, seleccione **`mobile_id`** y en **Value (Valor)**, seleccione **`{DeviceUid}`**.



STEP 7 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

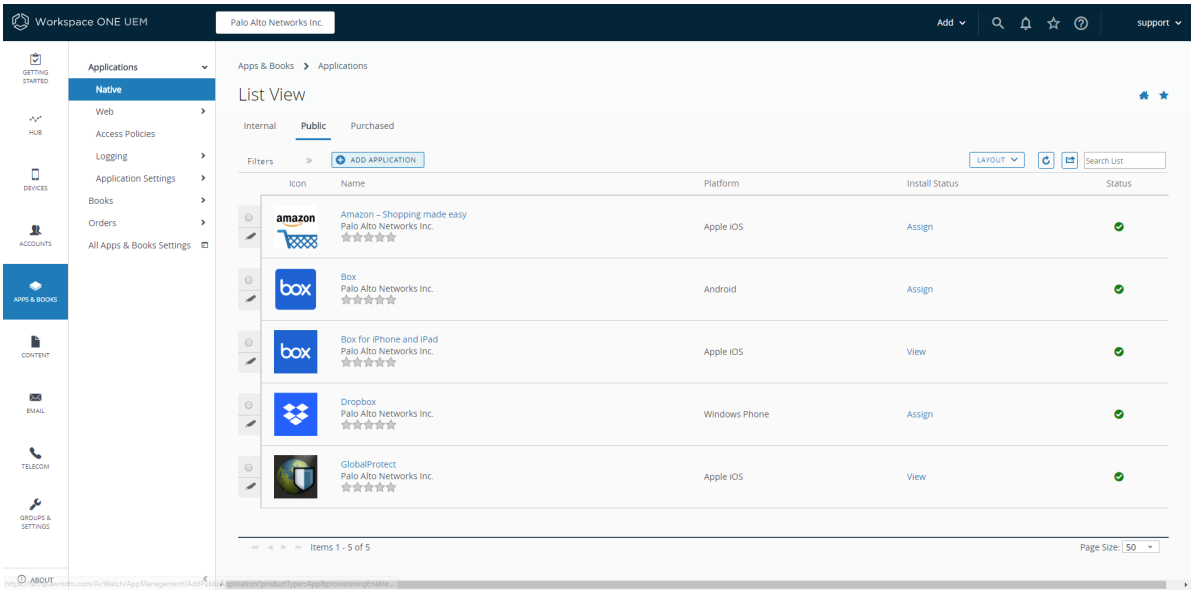
STEP 8 | Configure los ajustes de VPN por aplicación para una nueva aplicación gestionada o modifique los ajustes de una existente.

Después de configurar los ajustes para la aplicación y habilitar la VPN por aplicación, puede publicar la aplicación a un grupo de usuarios y habilitar la aplicación para que envíe tráfico a través del túnel VPN de GlobalProtect.

1. Seleccione **APPS & BOOKS (Aplicaciones y libros)** > **Applications (Aplicaciones)** > **Native (Nativo)** > **Public (Público)**.

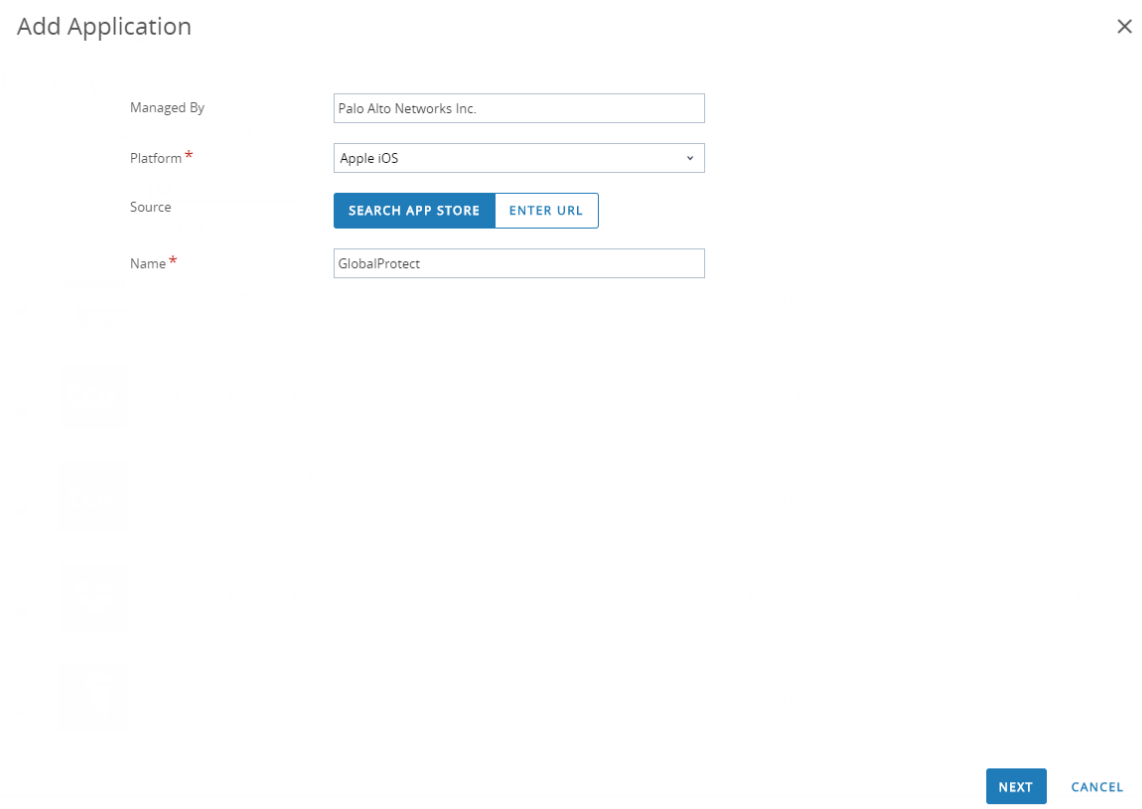
© 2020 Palo Alto Networks, Inc.

2. Para añadir una nueva aplicación, seleccione **Add Application (Añadir aplicación)**. Para modificar los ajustes de una aplicación existente, busque la aplicación en la lista de aplicaciones públicas (vista de lista) y seleccione el icono de edición ( ) en el menú de acciones junto a la fila.



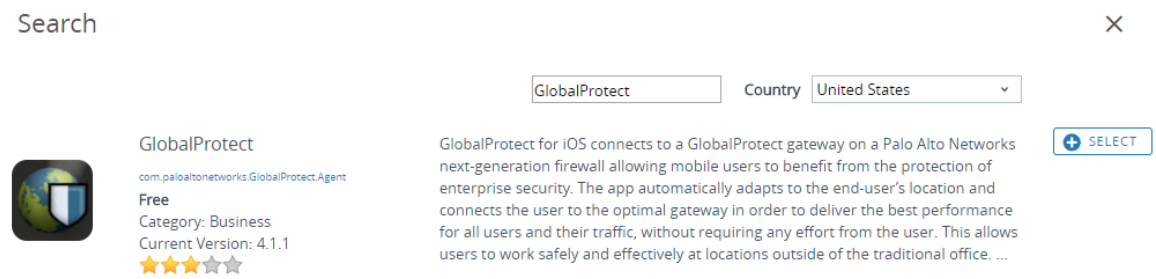
3. En el campo **Managed By (Gestionado por)**, seleccione el grupo organizaciones que gestionará esta aplicación.
4. En **Platform (Plataforma)**, seleccione **Apple iOS**.
5. Seleccione el **Source (Origen)** preferido para la ubicación de la aplicación:
   - **SEARCH APP STORE (Buscar en tienda de aplicaciones)**: introduzca el **Name (Nombre)** de la aplicación.
   - **ENTER URL (Introducir URL)**: introduzca la URL de la tienda de aplicaciones para la aplicación (por ejemplo, para añadir la aplicación Box, introduzca https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8&uo=4).

© 2020 Palo Alto Networks, Inc.



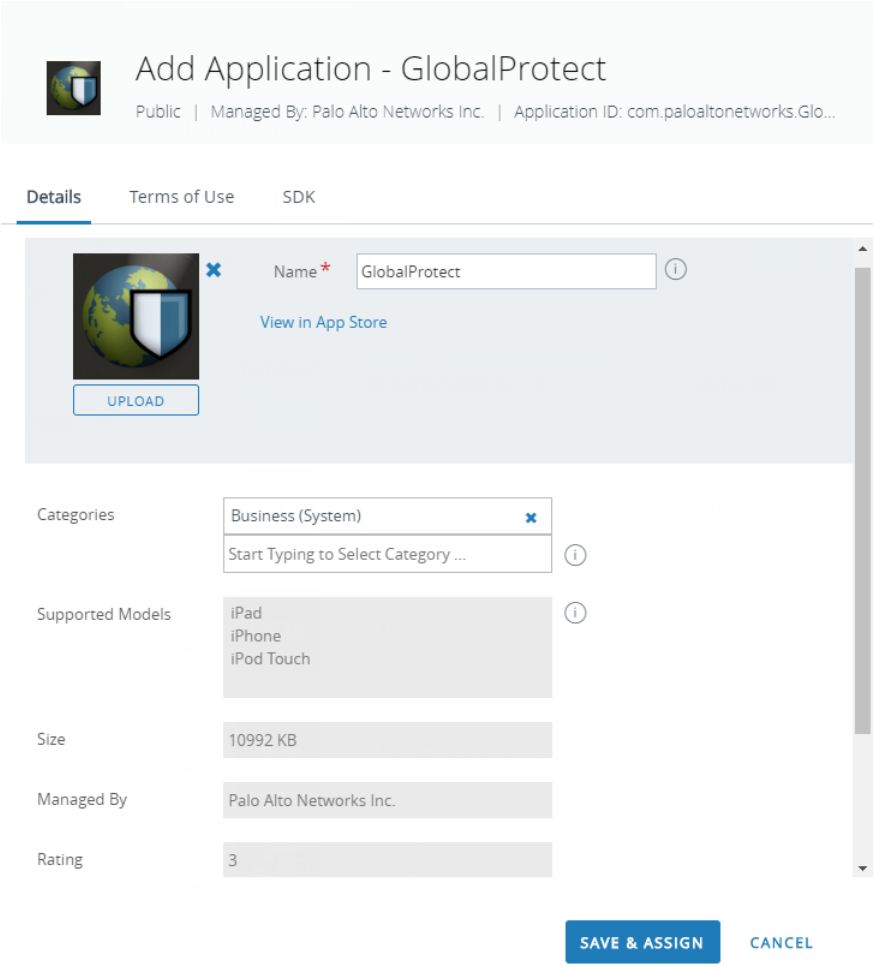
6. Haga clic en **NEXT (Siguiente)**.

   Si elige buscar la aplicación en la tienda de aplicaciones, debe hacer clic en **SELECT (SELECCIONAR)** para seleccionar la aplicación de la lista de resultados de búsqueda.



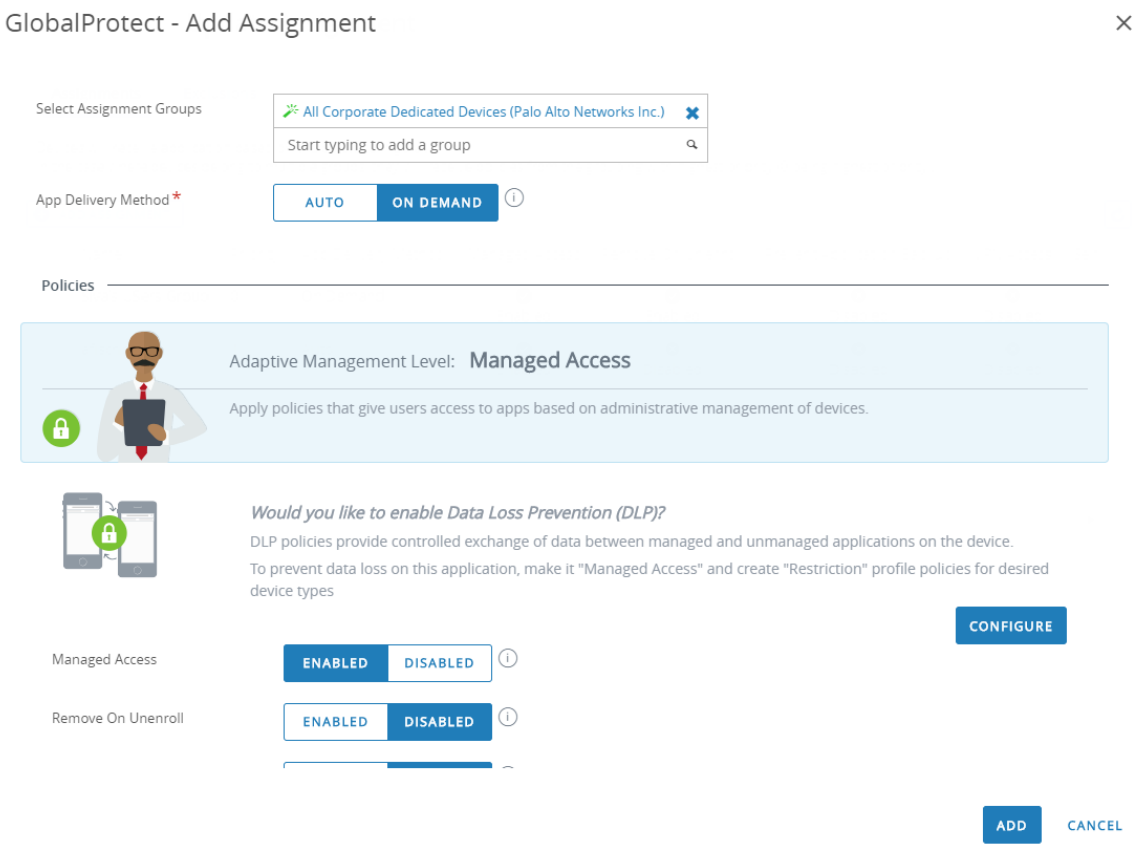
7. En el diálogo Add Application (Añadir aplicación), garantice que el **Name (Nombre)** de la aplicación sea correcto. Este es el nombre que aparecerá en el catálogo de aplicaciones de AirWatch.
8. (Opcional) Asigne la aplicación a **Categories (Categorías)** predefinidas o personalizadas para garantizar la facilidad del acceso en el catálogo de aplicaciones de AirWatch.

© 2020 Palo Alto Networks, Inc.



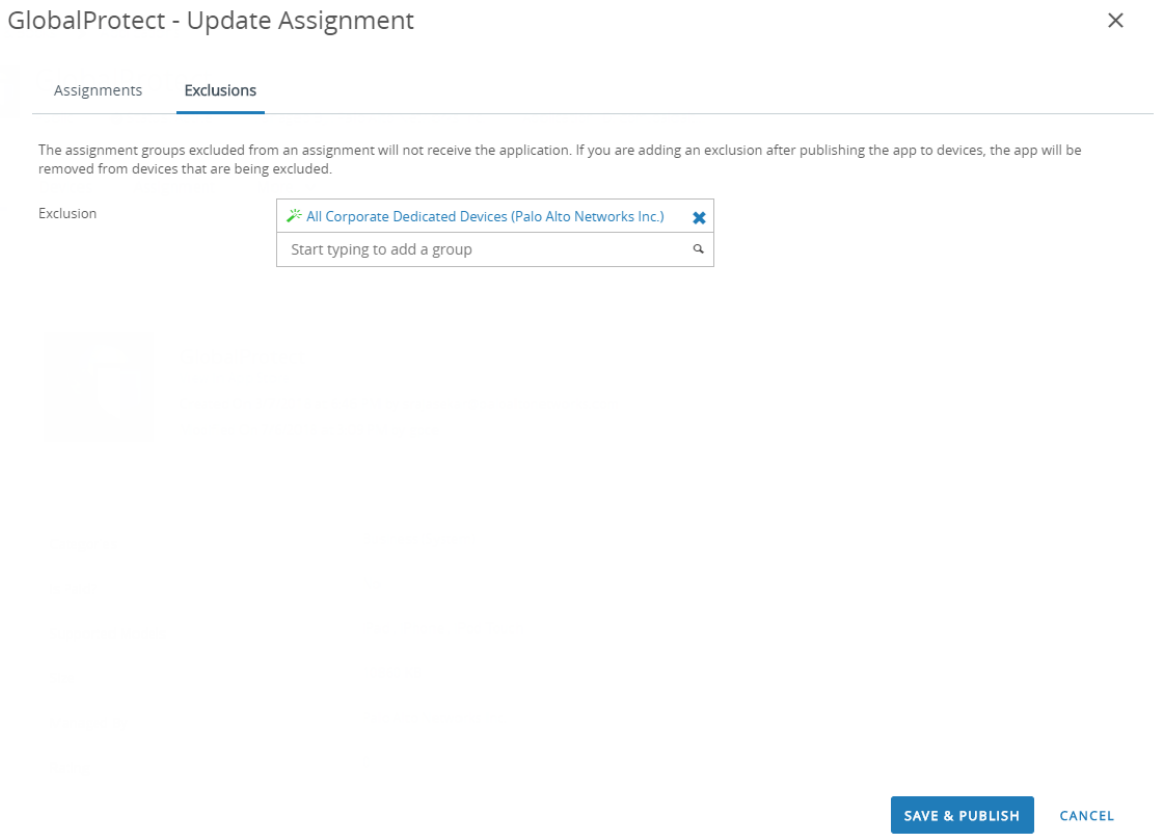
9. Haga clic en **SAVE & ASSIGN (GUARDAR Y ASIGNAR)** para guardar y asignar la aplicación nueva.
10. Seleccione la aplicación recientemente añadida de la lista de aplicaciones públicas (Vista de lista).
11. En **Applications (Aplicaciones)** > **Details View (Vista de detalles)**, haga clic en **ASSIGN (ASIGNAR)** en la esquina superior derecha de la pantalla.
12. Seleccione **Assignments (Asignaciones)** y haga clic en **ADD ASSIGNMENT (AÑADIR ASIGNACIÓN)** para añadir los Smart Groups que podrán acceder a esta aplicación.
    1. En el campo **Select Assignment Groups (Seleccionar grupos de asignación)**, seleccione los Smart Groups a los que desea brindar acceso a esta aplicación.
    2. Seleccione el **App Delivery Method (Método de envío de la aplicación)**. Si selecciona **AUTO (AUTOMÁTICO)**, la aplicación se implementa automáticamente en los Smart Groups especificados. Si selecciona **ON DEMAND (A demanda)**, la aplicación debe implementarse manualmente.
    3. En **Managed Access (Acceso gestionado)**, seleccione **ENABLED (HABILITADO)**. Esta opción le brinda a los usuarios acceso a la aplicación en función de las políticas de gestión que aplica.
    4. Configure los ajustes restantes según sea necesario.
    5. Haga clic en **ADD (Añadir)** para añadir una nueva asignación.

© 2020 Palo Alto Networks, Inc.



13.(Opcional) Para evitar que determinados Smart Groups accedan a la aplicación, seleccione **Exclusions (Exclusiones)** y seleccione los Smart Groups que desea excluir del campo **Exclusion (Exclusión)**.

© 2020 Palo Alto Networks, Inc.



14. Seleccione **SAVE & PUBLISH (Guardar y publicar)** para guardar y publicar la configuración a los Smart Groups asignados.

Establecimiento de una configuración de VPN por aplicación para endpoints Android con AirWatch

Puede habilitar el acceso a los recursos internos de sus endpoints móviles gestionados mediante la configuración del acceso VPN de GlobalProtect con AirWatch. En una configuración VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enviar tráfico a través del túnel VPN de GlobalProtect. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN de GlobalProtect.

Use los siguientes pasos para establecer una configuración de VPN por aplicación para endpoints Android con AirWatch:

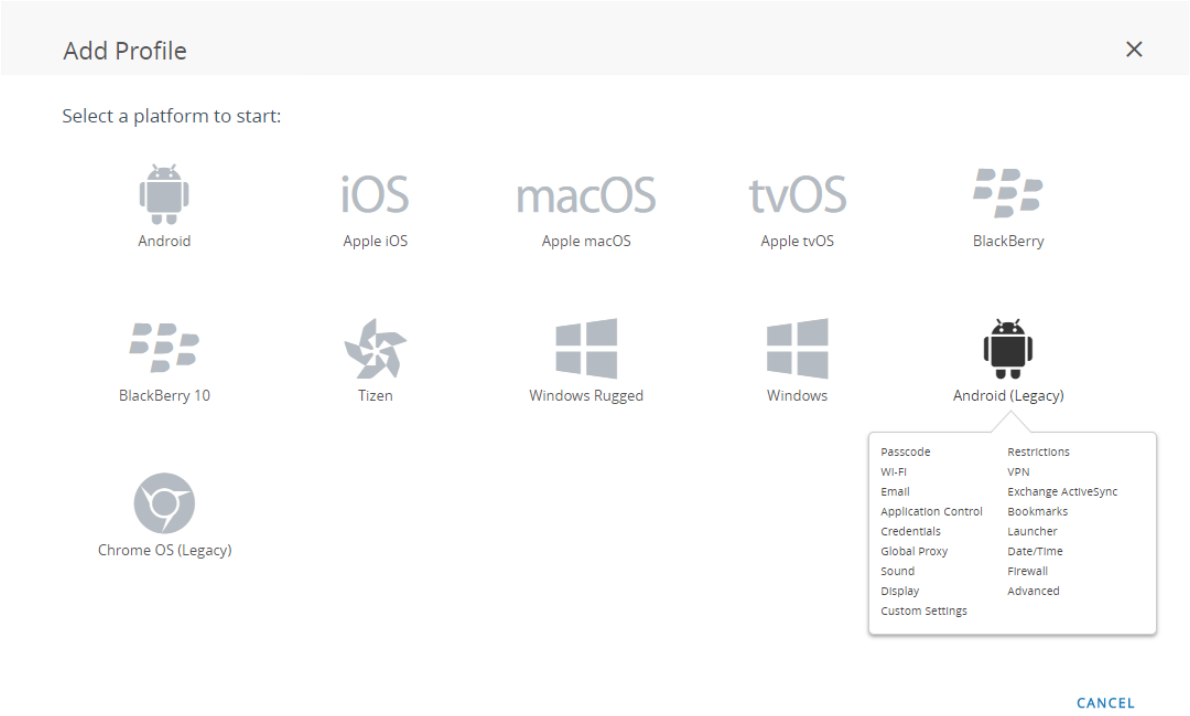
STEP 1 | Descargue la aplicación de GlobalProtect para Android:

- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde Google Play.

STEP 2 | Desde la consola de AirWatch, modifique un perfil Android existente o añada uno nuevo.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **Android (Legacy) (Android [Heredado])** de la lista de plataformas.

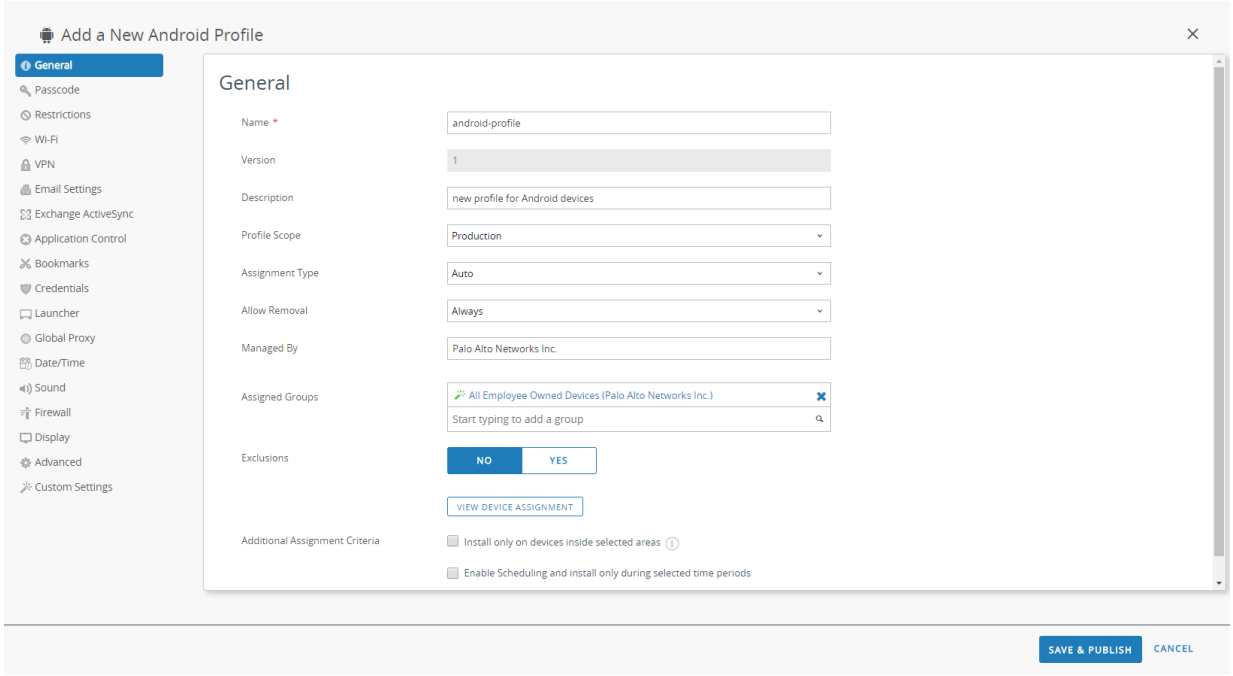
© 2020 Palo Alto Networks, Inc.



STEP 3 | Configure los ajustes en **General**:

1. Introduzca un **Name (Nombre)** para el perfil.
2. (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.
3. (Opcional) Seleccione el **Profile Scope (Alcance del perfil)**, ya sea **Production (Producción)**, **Staging (Almacenamiento provisional)** o **Both (Ambos)**.
4. (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
5. (Opcional) Seleccione si desea habilitar la opción **Allow Removal (Permitir eliminación)** del perfil para el usuario final. Seleccione **Always (Siempre)** para permitir que el usuario final elimine manualmente el perfil en cualquier momento, **Never (Nunca)** para evitar que lo elimine o **With Authorization (Con autorización)** para permitir que pueda eliminarlo con la autorización del administrador. Si se elige la opción **With Authorization (Con autorización)**, se añade una contraseña obligatoria.
6. (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
7. (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
8. (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.

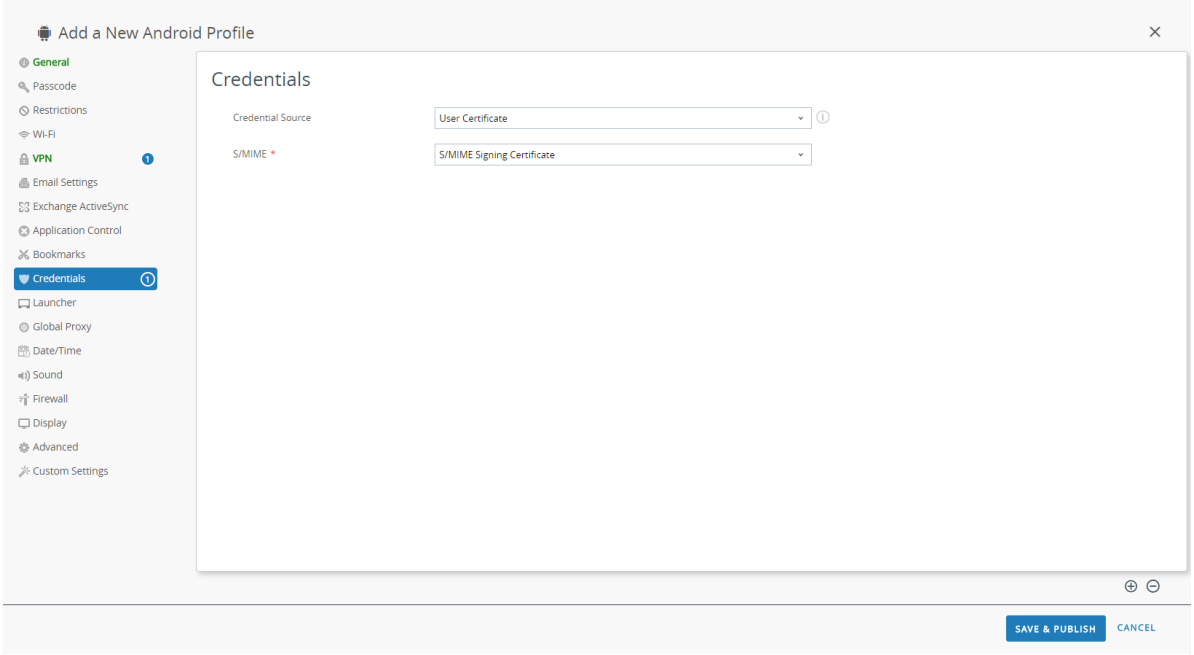
© 2020 Palo Alto Networks, Inc.



STEP 4 | Configure los ajustes de **Credentials (Credenciales)**:

Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

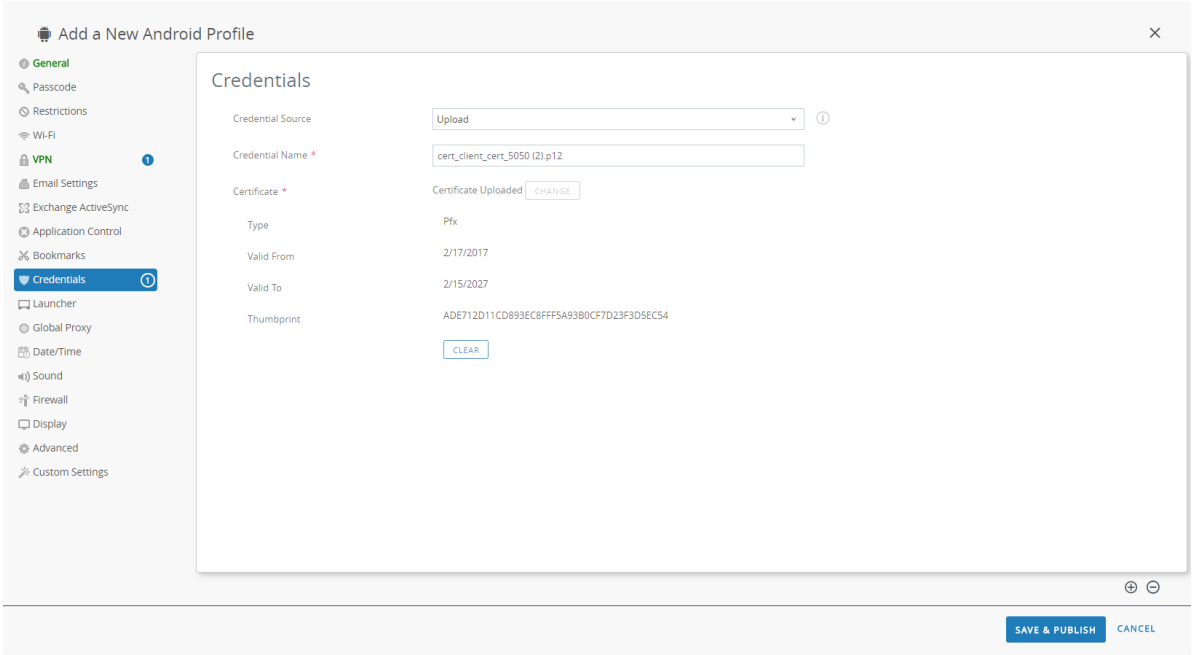
- Para extraer certificados de cliente de usuarios de AirWatch:
  1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
  2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).



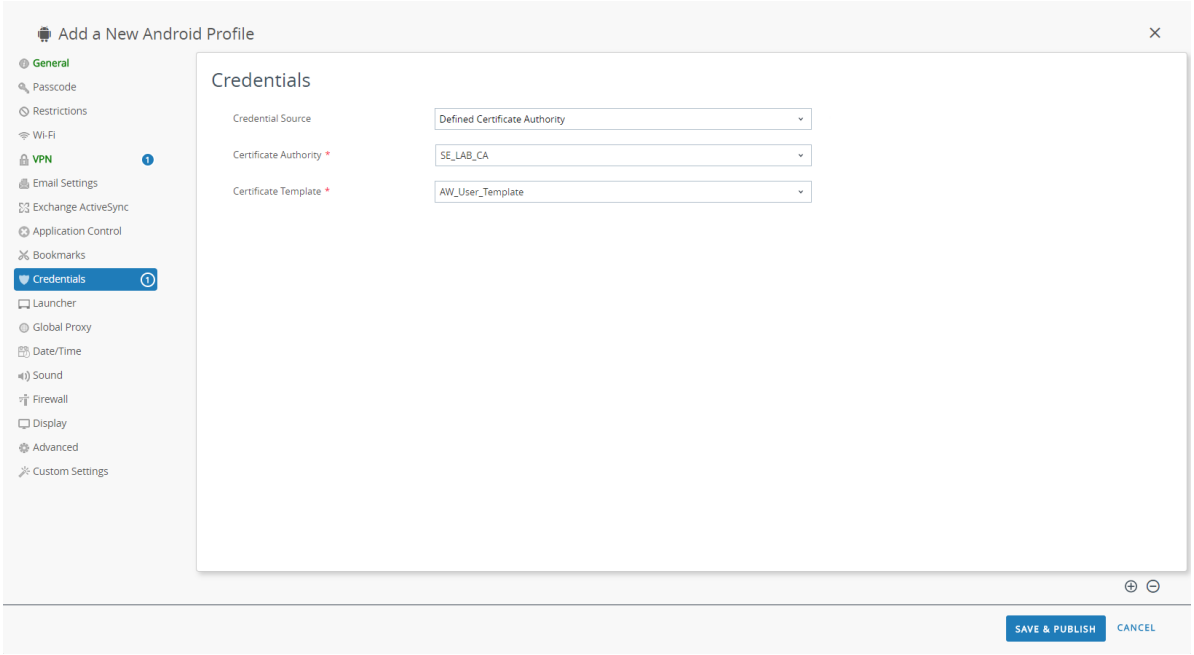
- Para cargar un certificado de cliente manualmente:

© 2020 Palo Alto Networks, Inc.

1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
2. Introduzca el **Credential Name (Nombre de credencial)**.
3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.



- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.
  3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.



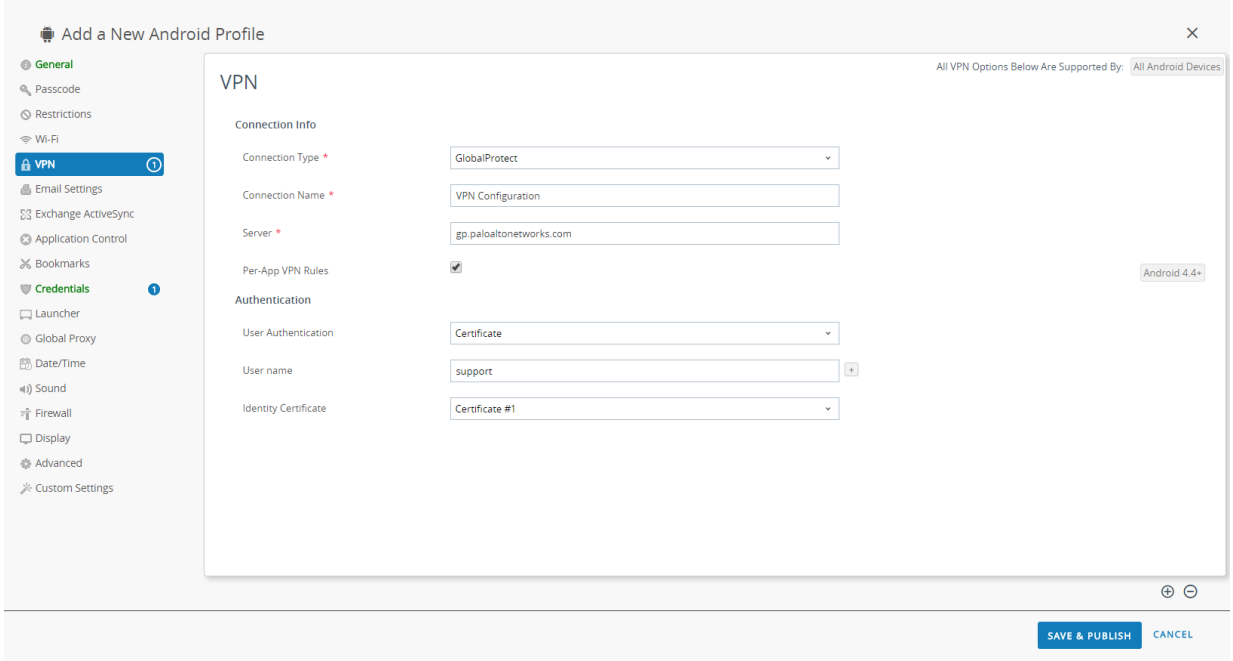
© 2020 Palo Alto Networks, Inc.

STEP 5 | Configure los ajustes de **VPN**.

1. En **Connection type (Tipo de conexión)** de la red, seleccione **GlobalProtect**.
2. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
3. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
4. Habilite **Per-App VPN Rules (Reglas de VPN por aplicación)** para enrutar todo el tráfico de aplicaciones gestionadas a través del túnel de VPN de GlobalProtect.
5. En el área Authentication (Autenticación), seleccione **Certificate (Certificado)** como método de **Authentication (Autenticación)**.

   Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

6. Introduzca el **User name (Nombre de usuario)** de la cuenta VPN o haga clic en el botón añadir (**+**) para ver los valores de búsqueda compatibles que puede introducir.
7. Cuando se le indique, seleccione el **Identity Certificate (Certificado de identidad)** que GlobalProtect usará para autenticar usuarios. El **Identity Certificate (Certificado de identidad)** es el mismo certificado que configuró en los ajustes de **Credentials (Credenciales)**.



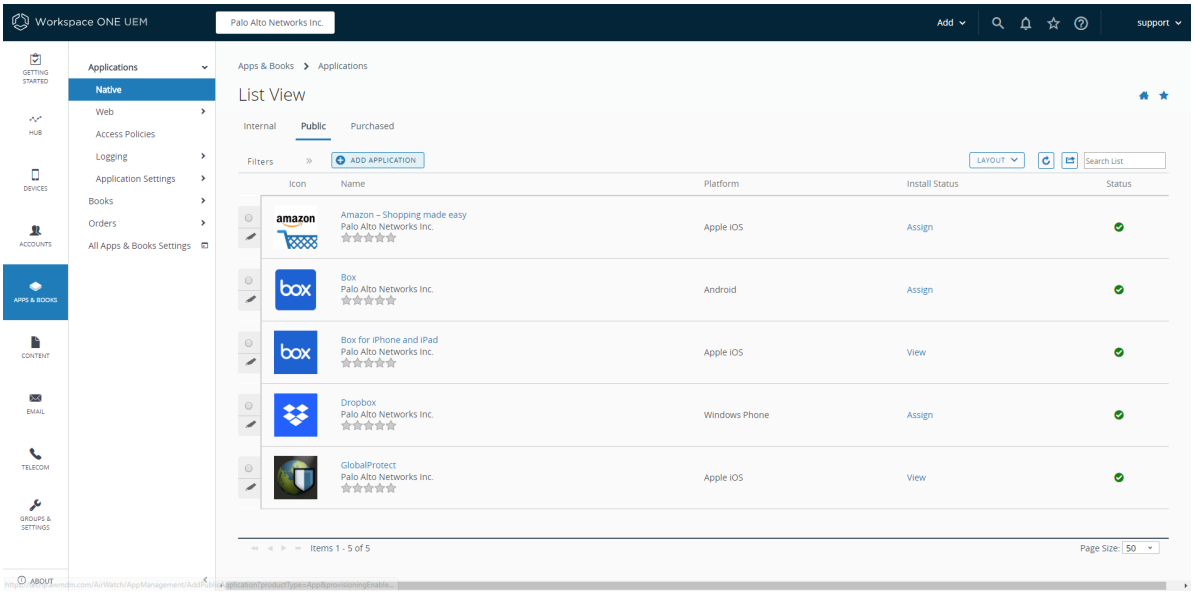
STEP 6 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

STEP 7 | Configure los ajustes de VPN por aplicación para una nueva aplicación gestionada o modifique los ajustes de una existente.

Después de configurar los ajustes para la aplicación y habilitar la VPN por aplicación, puede publicar la aplicación a un grupo de usuarios y habilitar la aplicación para que envíe tráfico a través del túnel VPN de GlobalProtect.

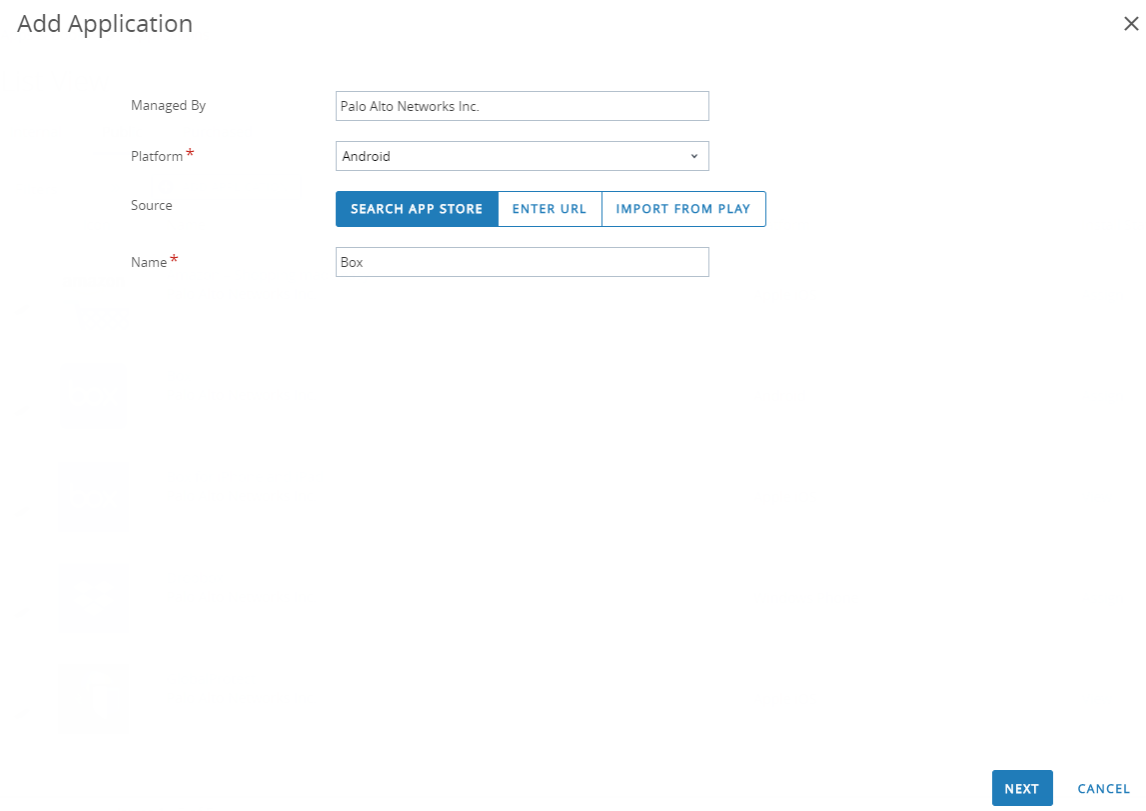
1. Seleccione **APPS & BOOKS (Aplicaciones y libros)** > **Applications (Aplicaciones)** > **Native (Nativo)** > **Public (Público)**.
2. Para añadir una nueva aplicación, seleccione **Add Application (Añadir aplicación)**. Para modificar los ajustes de una aplicación existente, busque la aplicación en la lista de aplicaciones públicas (vista de lista) y seleccione el icono de edición (✎) en el menú de acciones junto a la fila.

© 2020 Palo Alto Networks, Inc.



3. En el campo **Managed By (Gestionado por)**, seleccione el grupo organizaciones que gestionará esta aplicación.
4. En **Platform (Plataforma)**, seleccione **Android**.
5. Seleccione el **Source (Origen)** preferido para la ubicación de la aplicación:
   - **SEARCH APP STORE (Buscar en tienda de aplicaciones)**: introduzca el **Name (Nombre)** de la aplicación.
   - **ENTER URL (Introducir URL)**: introduzca la URL de Google Play para la aplicación (por ejemplo, para buscar la aplicación Box por URL, introduzca https://play.google.com/store/apps/details?id=com.box.android).
   - **IMPORT FROM PLAY (IMPORTAR DESDE PLAY)**: importa una aplicación aprobada con la empresa desde Google Play.

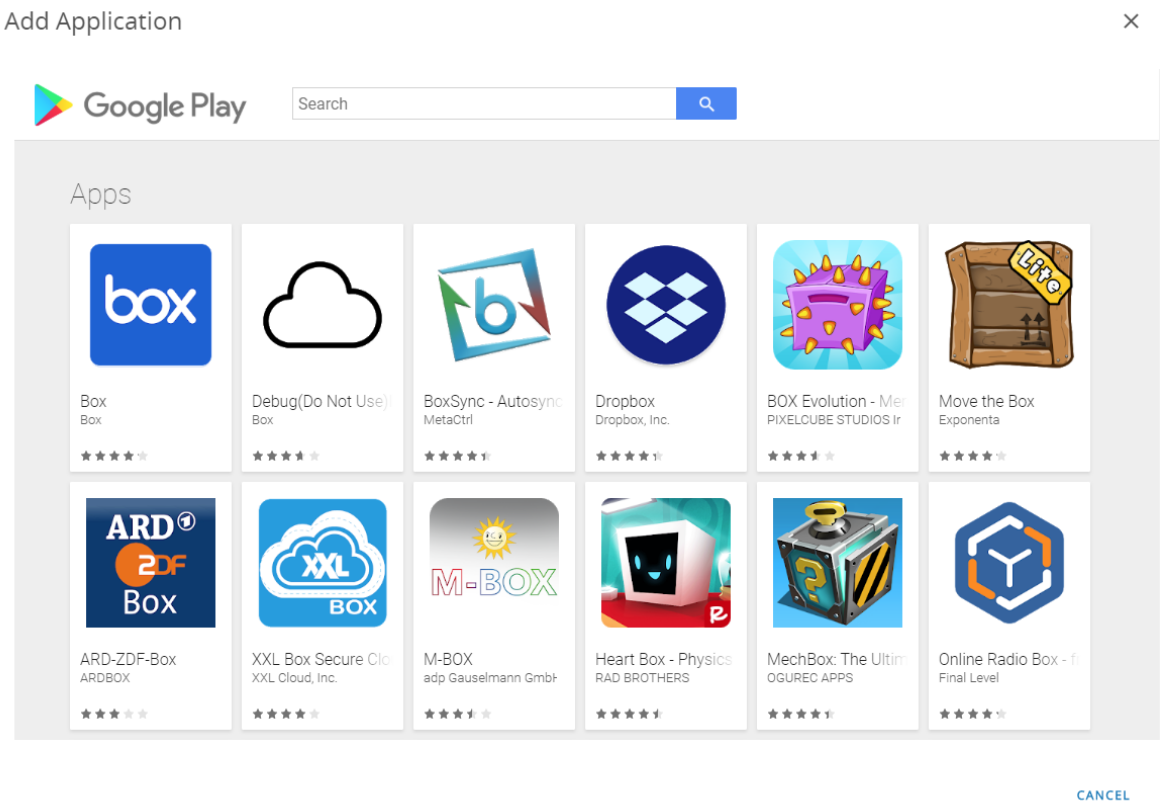
© 2020 Palo Alto Networks, Inc.

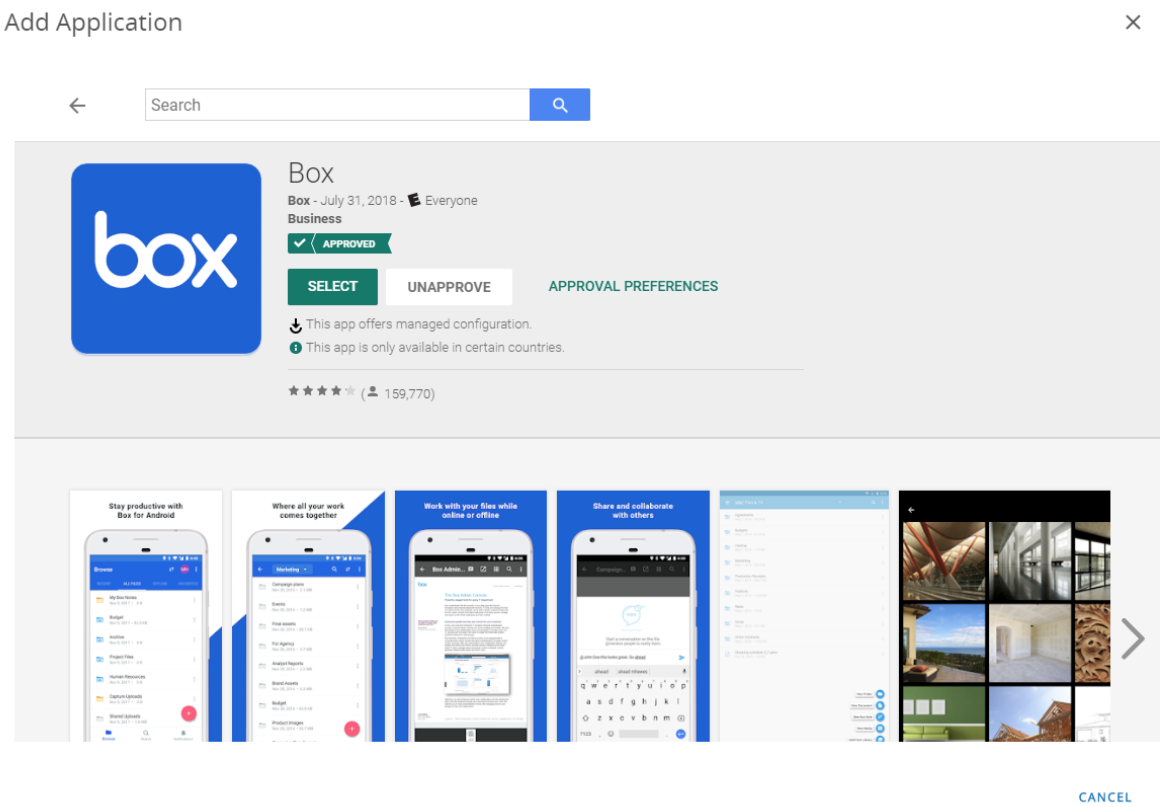


6. Haga clic en **NEXT (Siguiente)**.

   Si elige buscar Google Play, haga clic en el icono de aplicación de la lista de resultados de búsqueda. Si su empresa aún no ha aprobado la aplicación, debe hacer clic en **APPROVE (APROBAR)** para aprobar la aplicación. Después de que se apruebe la aplicación, haga clic en **SELECT (SELECCIONAR)** para seleccionar la aplicación.

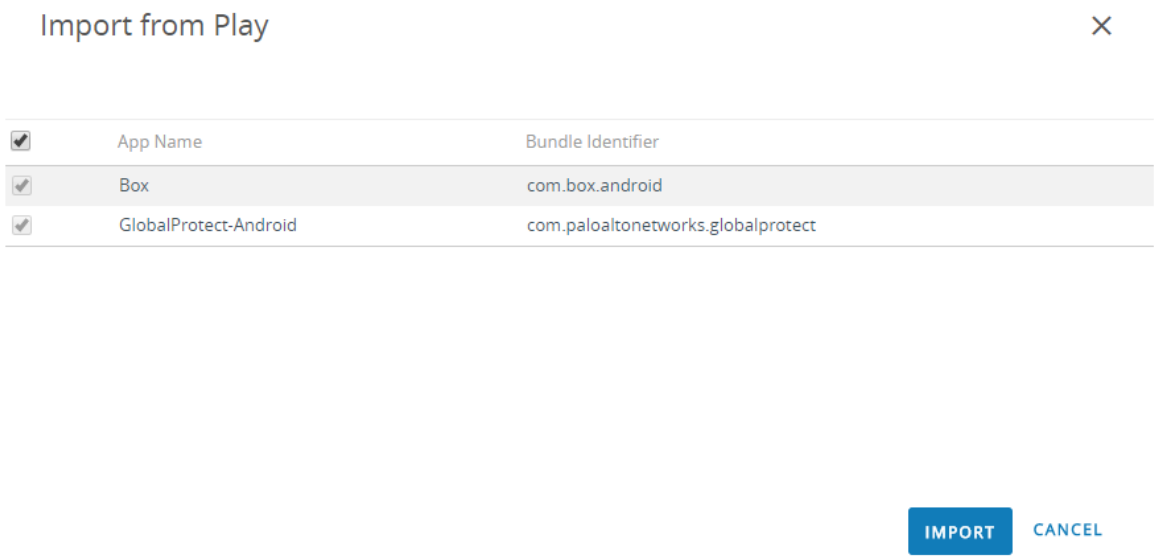
© 2020 Palo Alto Networks, Inc.





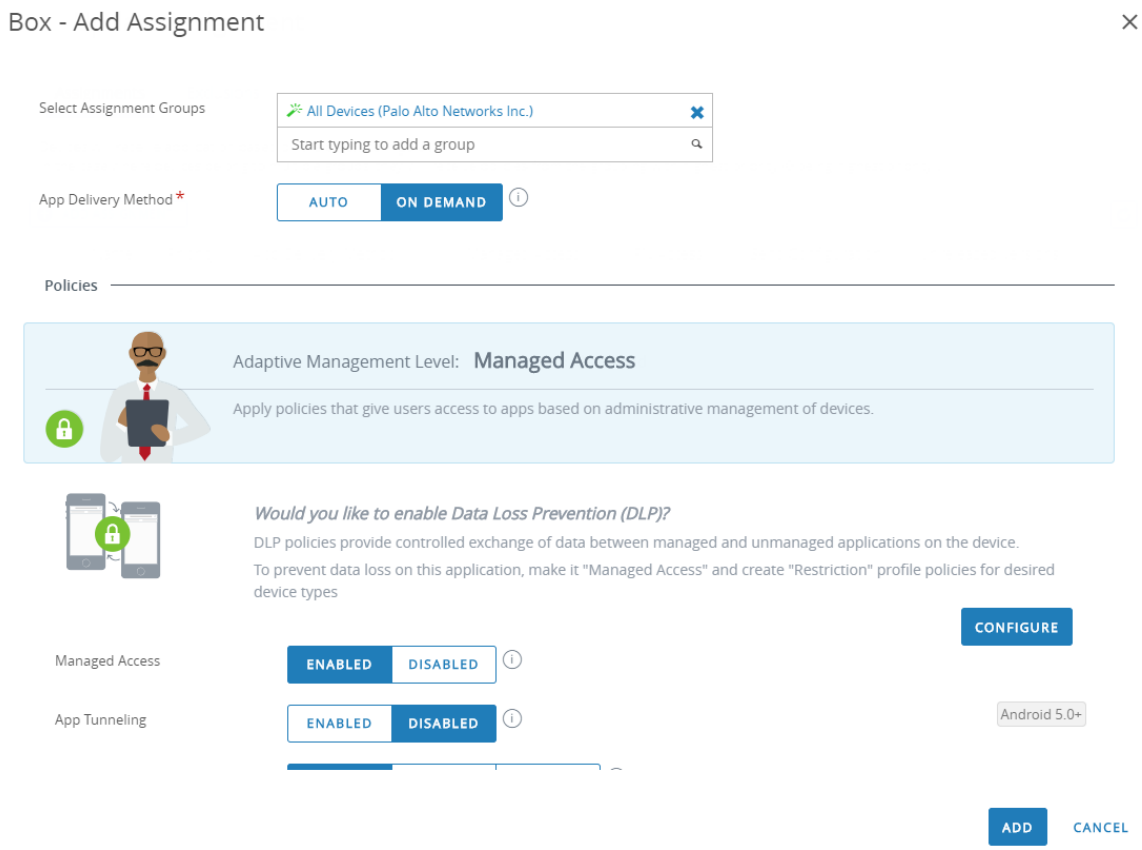
© 2020 Palo Alto Networks, Inc.

Si decidió importar la aplicación desde Google Play, seleccione la aplicación de la lista de aplicaciones de empresa aprobadas y haga clic en **IMPORT (IMPORTAR)**. Si no ve la aplicación en la lista, comuníquese con su administrador de Android for Work para aprobar la aplicación.



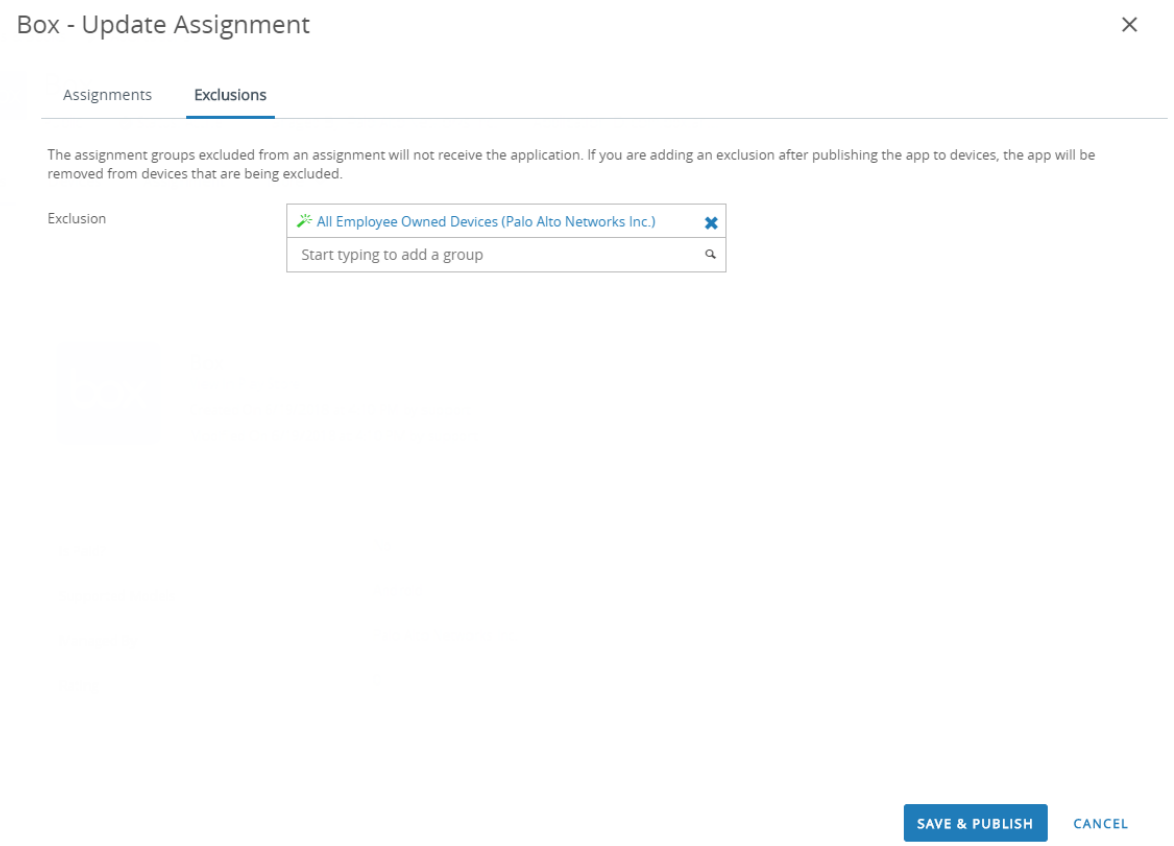
7. Seleccione la aplicación recientemente añadida de la lista de aplicaciones públicas (Vista de lista).
8. En **Applications (Aplicaciones)** > **Details View (Vista de detalles)**, haga clic en **ASSIGN (ASIGNAR)** en la esquina superior derecha de la pantalla.
9. Seleccione **Assignments (Asignaciones)** y haga clic en **ADD ASSIGNMENT (AÑADIR ASIGNACIÓN)** para añadir los Smart Groups que podrán acceder a esta aplicación.
   1. En el campo **Select Assignment Groups (Seleccionar grupos de asignación)**, seleccione los Smart Groups a los que desea brindar acceso a esta aplicación.
   2. Seleccione el **App Delivery Method (Método de envío de la aplicación)**. Si selecciona **AUTO (AUTOMÁTICO)**, la aplicación se implementa automáticamente en los Smart Groups especificados. Si selecciona **ON DEMAND (A demanda)**, la aplicación debe implementarse manualmente.
   3. En **Managed Access (Acceso gestionado)**, seleccione **ENABLED (HABILITADO)**. Esta opción le brinda a los usuarios acceso a la aplicación en función de las políticas de gestión que aplica.
   4. Configure los ajustes restantes según sea necesario.
   5. Haga clic en **ADD (Añadir)** para añadir una nueva asignación.

© 2020 Palo Alto Networks, Inc.



10.(Opcional) Para evitar que determinados Smart Groups accedan a la aplicación, seleccione **Exclusions (Exclusiones)** y seleccione los Smart Groups que desea excluir del campo **Exclusion (Exclusión)**.

© 2020 Palo Alto Networks, Inc.



11. Seleccione **SAVE & PUBLISH (Guardar y publicar)** para guardar y publicar la configuración a los Smart Groups asignados.

Establecimiento de una configuración de VPN por aplicación para endpoints de Windows 10 UWP con AirWatch

Puede habilitar el acceso a los recursos internos de sus endpoints móviles gestionados mediante la configuración del acceso VPN de GlobalProtect con AirWatch. En una configuración VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enviar tráfico a través del túnel VPN de GlobalProtect. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN de GlobalProtect.

Debido a que AirWatch aún no incluye a GlobalProtect como un proveedor oficial de conexión para los endpoints de Windows, usted debe seleccionar un proveedor de VPN alternativo, editar los ajustes para la aplicación de GlobalProtect e importar la configuración nuevamente en el perfil VPN según se describe en el siguiente flujo de trabajo.

Use los siguientes pasos para establecer una configuración de VPN por aplicación para endpoints de Windows 10 UWP usando AirWatch:

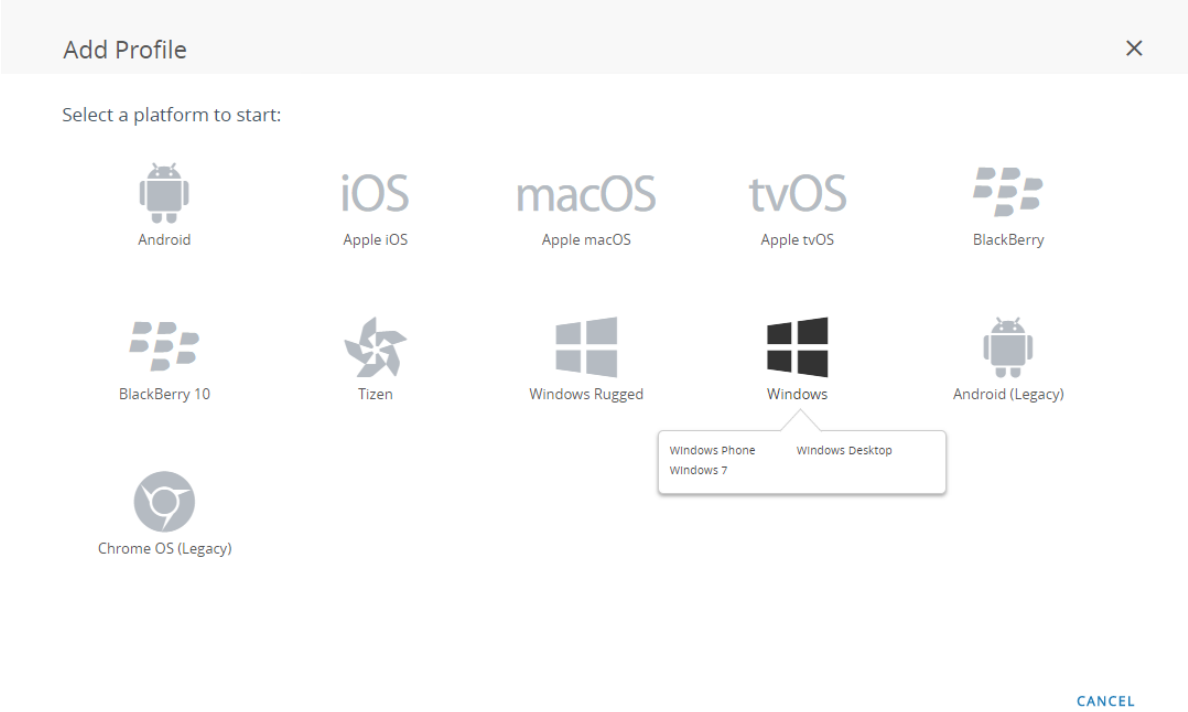
STEP 1 | Descargue la aplicación de GlobalProtect para Windows 10 UWP:

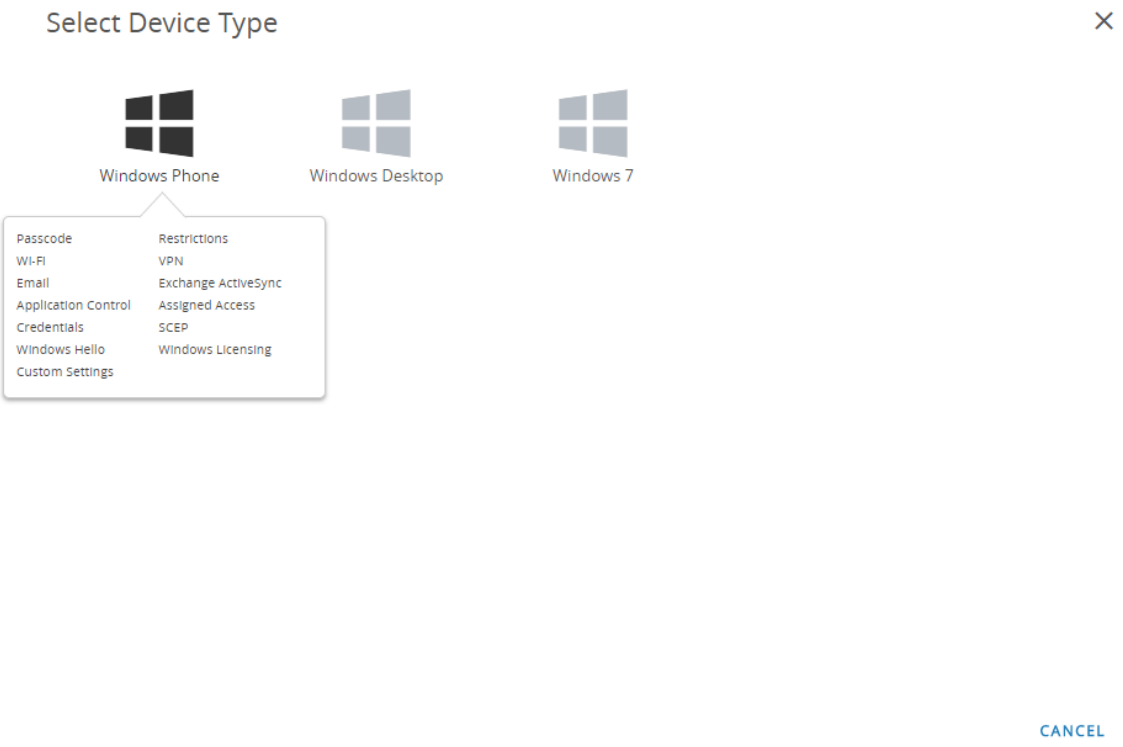
- Implemente la aplicación móvil de GlobalProtect con AirWatch.
- Descargue la aplicación de GlobalProtect directamente desde Microsoft Store.

STEP 2 | En la consola de AirWatch, modifique un perfil de Windows 10 UWP existente o añada uno nuevo.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y luego haga clic en **ADD (Añadir)** para añadir un nuevo perfil.
2. Seleccione **Windows** como la plataforma y **Windows Phone** como el tipo de dispositivo.

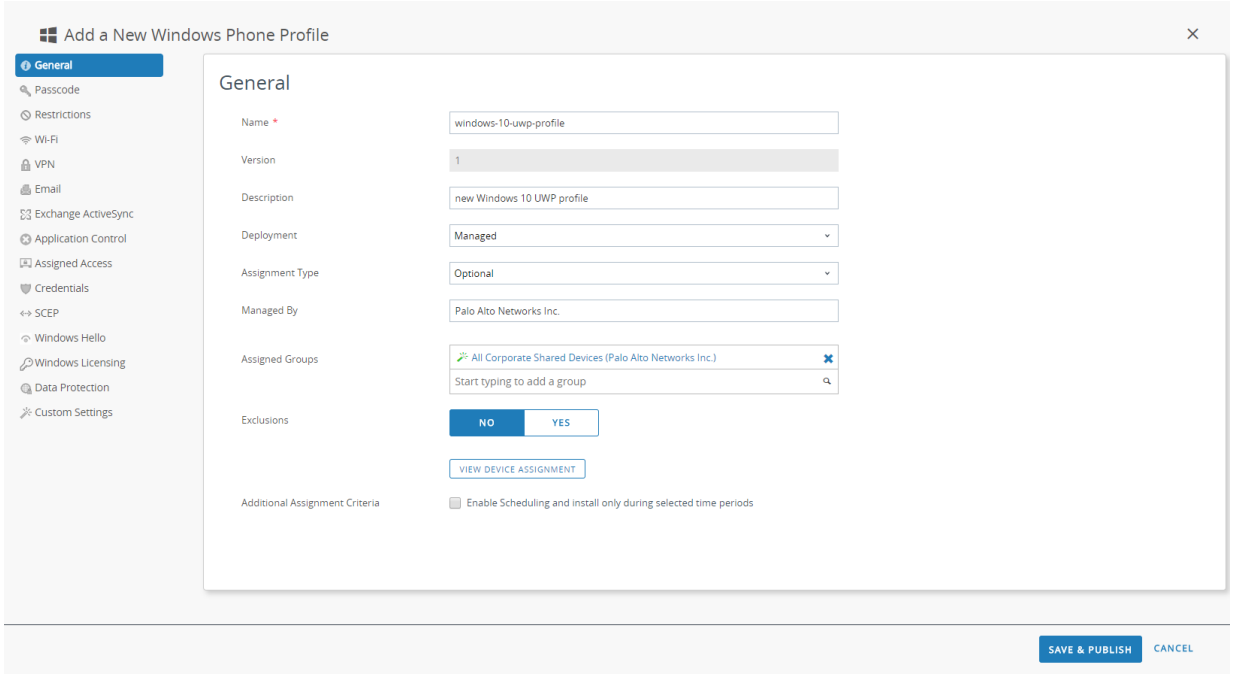




STEP 3 | Configure los ajustes en **General**:

© 2020 Palo Alto Networks, Inc.

- Introduzca un **Name (Nombre)** para el perfil.
- (Opcional) Introduzca una **Description (Descripción)** breve del perfil que indica su propósito.
- (Opcional) En el método de **Deployment (Implementación)**, seleccione **Managed (Gestionado)** para permitir que el perfil se elimine automáticamente luego de la cancelación de la inscripción
- (Opcional) Seleccione un **Assignment Type (Tipo de asignación)** para determinar de qué manera el perfil se implementa en los endpoints. Seleccione **Auto (Automático)** para implementar el perfil en todos los endpoints de forma automática, **Optional (Opcional)** para permitir al usuario final instalar el perfil desde el Portal de autoservicio (SSP) o implementar manualmente el perfil en endpoints individuales o **Compliance (Conformidad)** para implementar el perfil cuando un usuario final infringe una política de cumplimiento aplicable al endpoint.
- (Opcional) En el campo **Managed By (Gestionado por)**, introduzca el grupo de la organización con acceso administrativo al perfil.
- (Opcional) En el campo **Assigned Groups (Grupos asignados)**, añada los Smart Groups a los que desea que se añada el perfil. Este campo incluye la opción de crear un nuevo Smart Group que puede configurarse con especificaciones de sistema operativo mínimo, modelos de dispositivo, categorías de titularidad, grupos de la organización y más.
- (Opcional) Indique si desea incluir **Exclusions (Exclusiones)** para la asignación de este perfil. Si selecciona **Yes (Sí)**, se muestra el campo **Excluded Groups (Grupos excluidos)**, lo que le permite seleccionar esos Smart Groups que desea excluir de la asignación de este perfil.

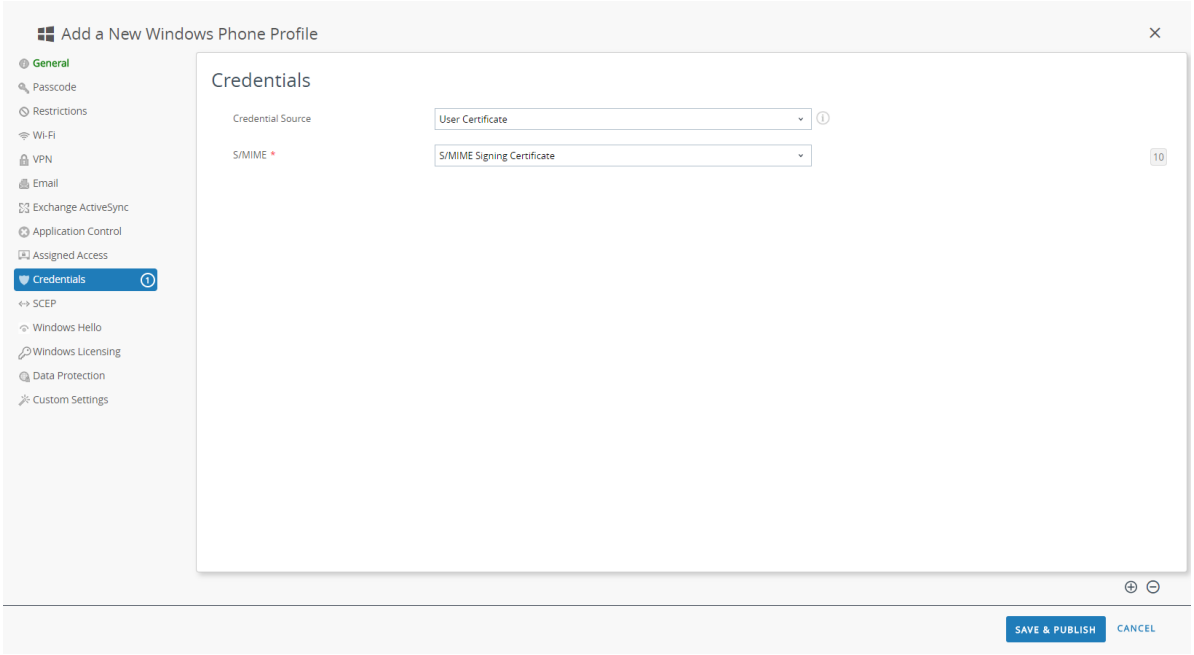


STEP 4 | Configure los ajustes de **Credentials (Credenciales)**:

Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

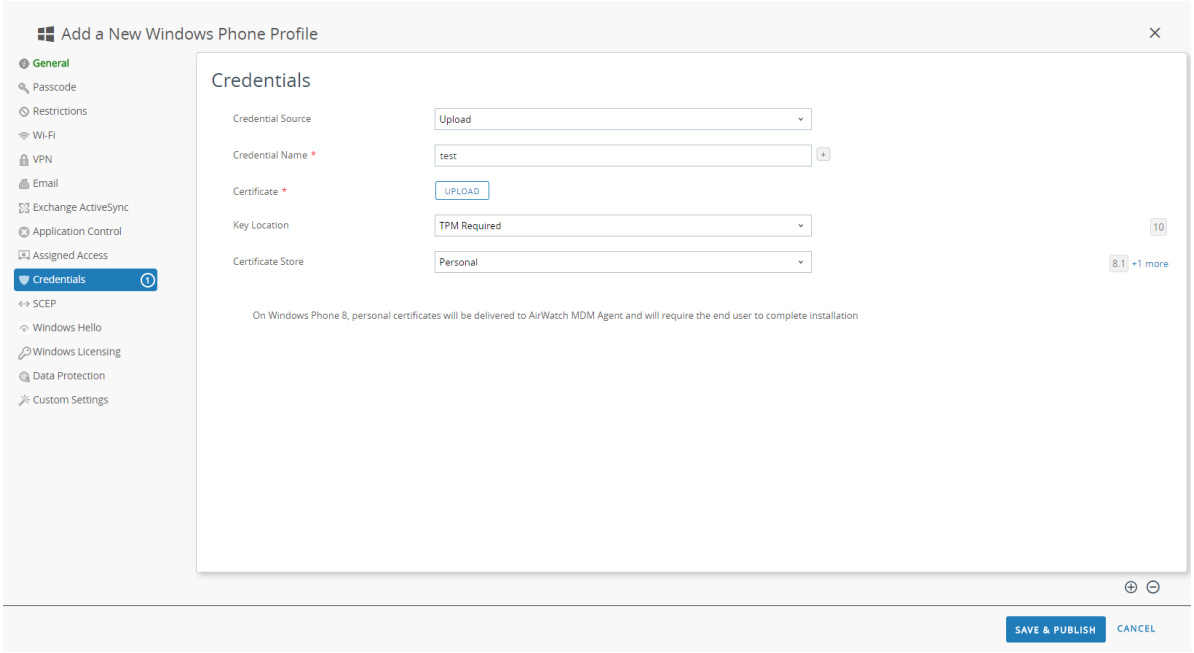
- Para extraer certificados de cliente de usuarios de AirWatch:
  1. En **Credential Source (Origen de la credencial)**, seleccione **User Certificate (Certificado de usuario)**.
  2. Seleccione el **S/MIME Signing Certificate (Certificado de firma S/MIME)** (predeterminado).

© 2020 Palo Alto Networks, Inc.



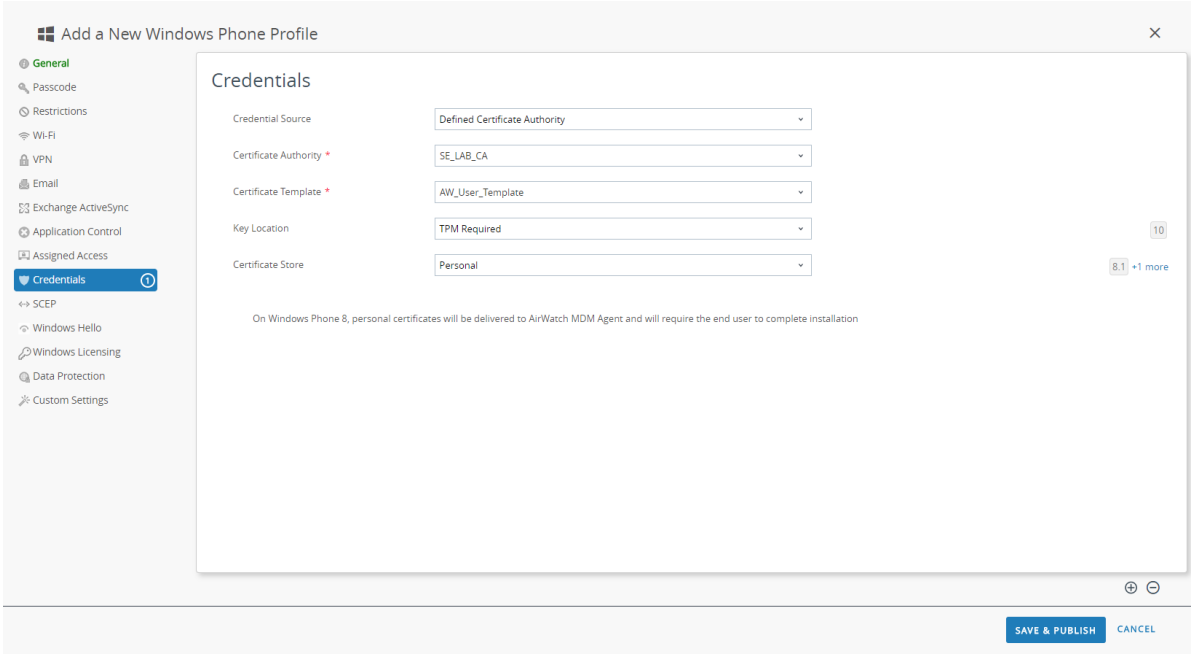
- Para cargar un certificado de cliente manualmente:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Upload (Carga)**.
  2. Introduzca el **Credential Name (Nombre de credencial)**.
  3. Haga clic en **UPLOAD (CARGA)** para buscar y seleccionar el certificado que desea cargar.
  4. Después de seleccionar un certificado, haga clic en **SAVE (GUARDAR)**.
  5. Seleccione la **Key Location (Ubicación de clave)** donde desea almacenar la clave privada del certificado:
     - **TPM Required (TPM requerida)**: almacene la clave privada en un módulo de plataforma fiable. Si un módulo de plataforma fiable no está disponible en el endpoint, no se puede instalar la clave privada.
     - **TPM If Present (TPM si está presente)**: almacene la clave privada en un módulo de plataforma fiable si hay uno disponible en el endpoint. Si un módulo de plataforma fiable no está disponible en el endpoint, la clave privada se almacena en el software del endpoint.
     - **Software**: almacene la clave privada en el software del endpoint.
     - **Passport**: guarde la clave privada en Microsoft Passport. Para usar esta opción, se debe instalar AirWatch Protection Agent en el endpoint.
  6. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.

© 2020 Palo Alto Networks, Inc.



- Para usar una autoridad de certificación predefinida y una plantilla:
  1. En **Credential Source (Origen de la credencial)**, seleccione **Defined Certificate Authority (Autoridad definida de certificación)**.
  2. Seleccione la **Certificate Authority (Autoridad de certificación)** de la cual desea obtener los certificados.
  3. Seleccione la **Certificate Template (Plantilla de certificado)** para la autoridad de certificación.
  4. Seleccione la **Key Location (Ubicación de clave)** donde desea almacenar la clave privada del certificado:
     - **TPM Required (TPM requerida)**: almacene la clave privada en un módulo de plataforma fiable. Si un módulo de plataforma fiable no está disponible en el endpoint, no se puede instalar la clave privada.
     - **TPM If Present (TPM si está presente)**: almacene la clave privada en un módulo de plataforma fiable si hay uno disponible en el endpoint. Si un módulo de plataforma fiable no está disponible en el endpoint, la clave privada se almacena en el software del endpoint.
     - **Software**: almacene la clave privada en el software del endpoint.
     - **Passport**: guarde la clave privada en Microsoft Passport. Para usar esta opción, se debe instalar AirWatch Protection Agent en el endpoint.
  5. En **Certificate store (Almacén de certificados)**, seleccione **Personal**.

© 2020 Palo Alto Networks, Inc.



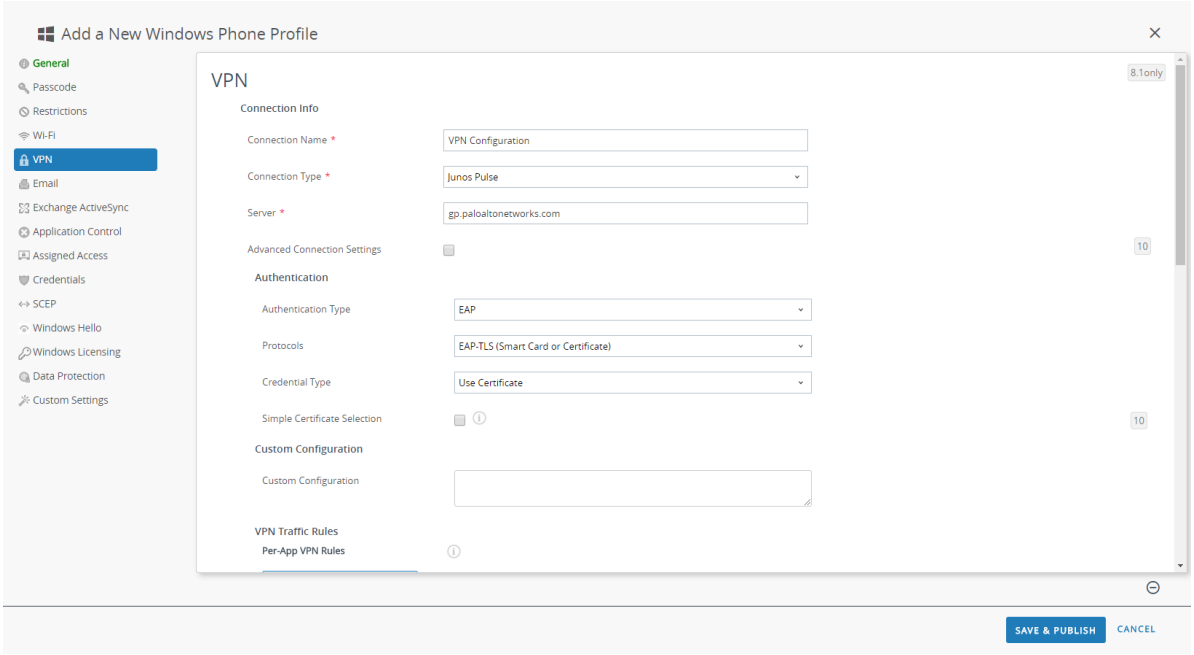
STEP 5 | Configure los ajustes de **VPN**.

1. Introduzca el **Connection Name (Nombre de la conexión)** que muestra el endpoint.
2. Seleccione un proveedor de **Connection Type (Tipo de conexión)** alternativo (no seleccione **IKEv2**, **L2TP**, **PPTP** o **Automatic [Automático]**, ya que estos no tienen los ajustes del proveedor asociado necesarios para el perfil de VPN de GlobalProtect).

   Debe seleccionar un proveedor alternativo debido a que AirWatch aún no incluye a GlobalProtect como proveedor oficial de conexión para los endpoints de Windows.
3. En el campo **Server (Servidor)**, introduzca el nombre de host o la dirección IP del portal de GlobalProtect al cual se conectarán los usuarios.
4. En el área Authentication (Autenticación), seleccione un **Authentication Type (Tipo de autenticación)** basado en certificado para especificar el método de autenticación de los usuarios finales.

   Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

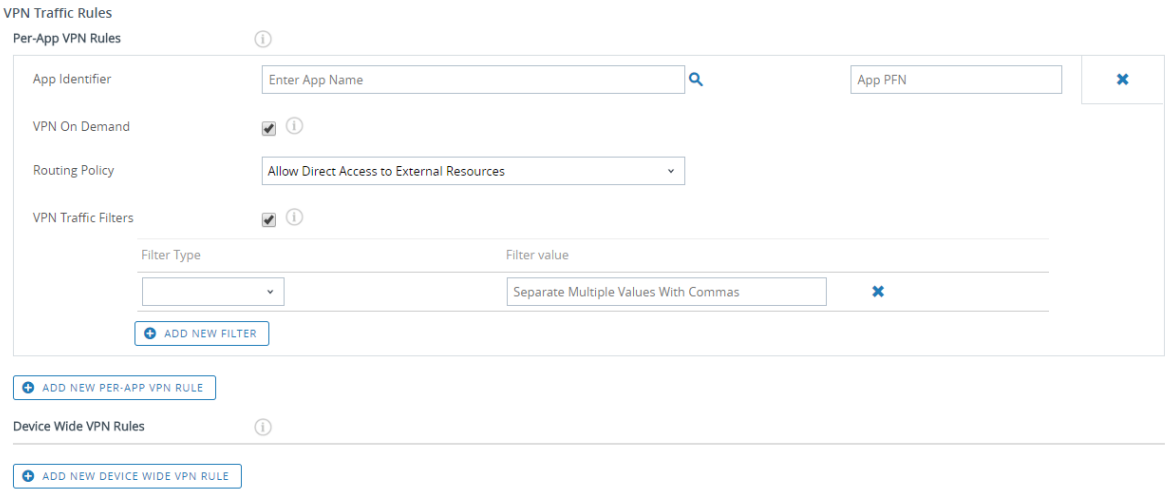
© 2020 Palo Alto Networks, Inc.



5. (Opcional) Para permitir que GlobalProtect guarde las credenciales de usuario, seleccione **ENABLE (HABILITAR)** para habilitar la opción **Remember Credentials (Recordar credenciales)** en el área Policies (Políticas).
6. En el área VPN Traffic Rules (Reglas de tráfico de VPN), haga clic en **ADD NEW PER-APP VPN RULE (Añadir nueva regla de VPN por aplicación)** para especificar las reglas de aplicaciones heredadas específicas (generalmente, archivos .exe) o aplicaciones modernas (generalmente, se descargan de la tienda de Microsoft):
   1. (Opcional) Habilitar **VPN On Demand (VPN a demanda)** para permitir que la conexión de GlobalProtect se establezca automáticamente cuando se inicia la aplicación.
   2. Seleccione una **Routing Policy (Política de enrutamiento)** para especificar si desea enviar el tráfico de la aplicación a través del túnel de VPN.
   3. (Opcional) Configure **VPN Traffic Filters (Filtros de tráfico de VPN)** específicos para enrutar el tráfico de la aplicación a través del túnel de VPN solo si coincide con los criterios de coincidencia específicos que define, como la dirección IP y el puerto.

      Añada los criterios de coincidencia haciendo clic en **ADD NEW FILTER (Añadir nuevo filtro)**. Cuando se le indique, introduzca un **Filter Name (Nombre de filtro)** y el **Filter Value (Valor de filtro)** correspondiente.

© 2020 Palo Alto Networks, Inc.

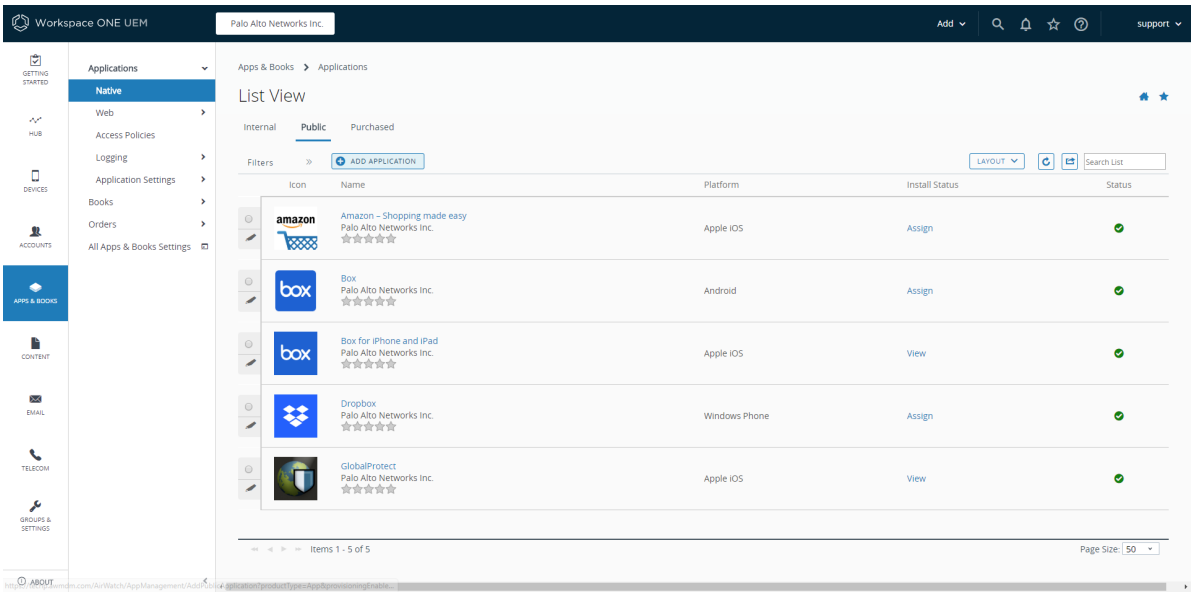


STEP 6 | Haga clic en **Save & Publish (Guardar y publicar)** para guardar y publicar los cambios.

STEP 7 | Configure los ajustes de VPN por aplicación para una nueva aplicación gestionada o modifique los ajustes de una existente.

Después de configurar los ajustes para la aplicación y habilitar la VPN por aplicación, puede publicar la aplicación a un grupo de usuarios y habilitar la aplicación para que envíe tráfico a través del túnel VPN de GlobalProtect.

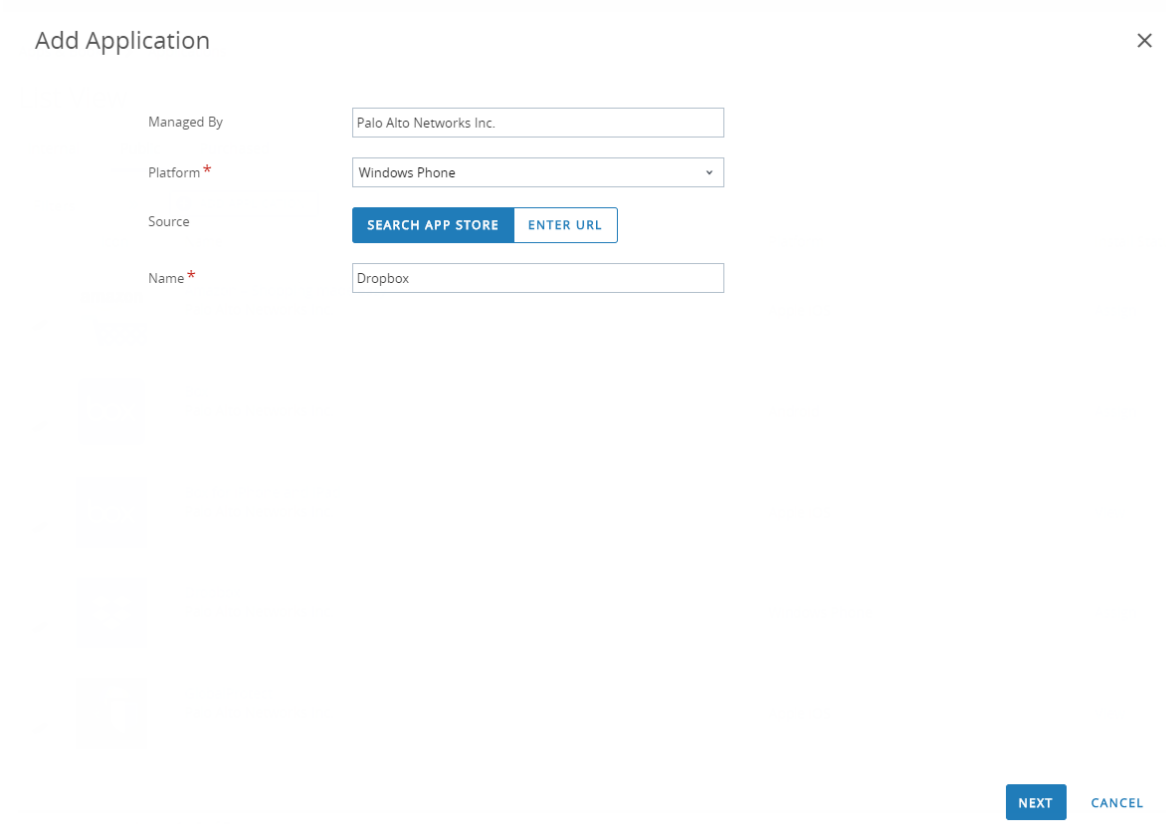
1. Seleccione **APPS & BOOKS (Aplicaciones y libros)** > **Applications (Aplicaciones)** > **Native (Nativo)** > **Public (Público)**.
2. Para añadir una nueva aplicación, seleccione **Add Application (Añadir aplicación)**. Para modificar los ajustes de una aplicación existente, busque la aplicación en la lista de aplicaciones públicas y seleccione el icono de edición ( ) en el menú de acciones junto a la fila.



3. En el campo **Managed By (Gestionado por)**, seleccione el grupo organizaciones que gestionará esta aplicación.
4. En **Platform (Plataforma)**, seleccione **Windows Phone**.
5. Seleccione el **Source (Origen)** preferido para la ubicación de la aplicación:

© 2020 Palo Alto Networks, Inc.

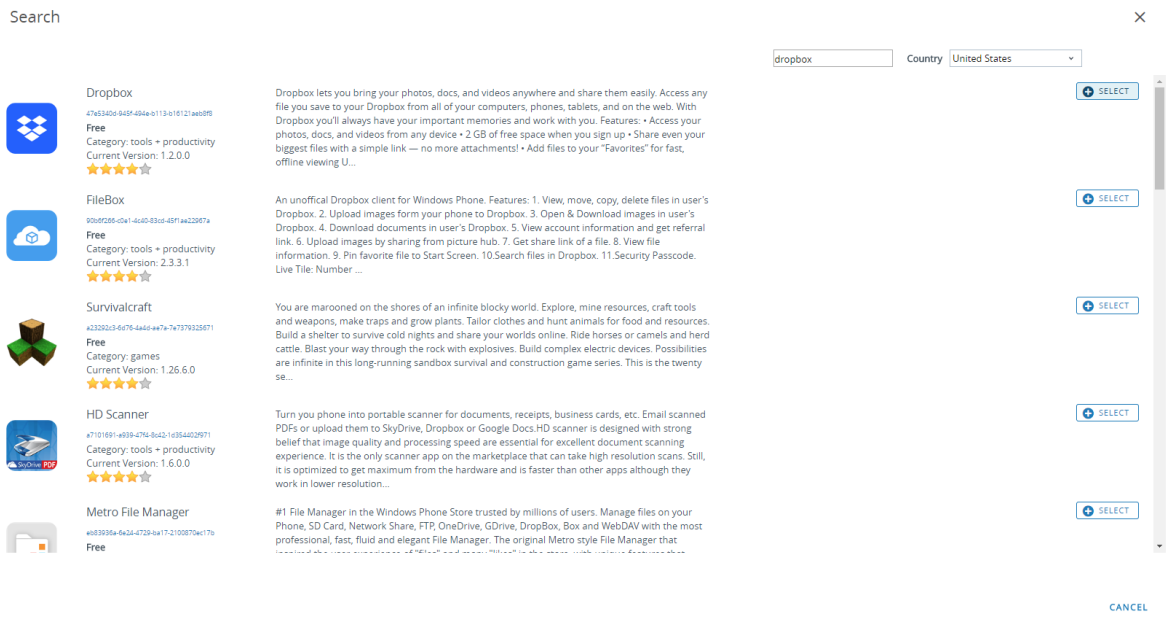
- **SEARCH APP STORE (Buscar en tienda de aplicaciones)**: introduzca el **Name (Nombre)** de la aplicación.
- **ENTER URL (Introducir URL)**: introduzca la URL de la tienda de Microsoft para la aplicación (por ejemplo, para buscar la aplicación móvil de Dropbox por URL, introduzca https://www.microsoft.com/en-us/p/dropbox-mobile/9wzdncrfj0pk).



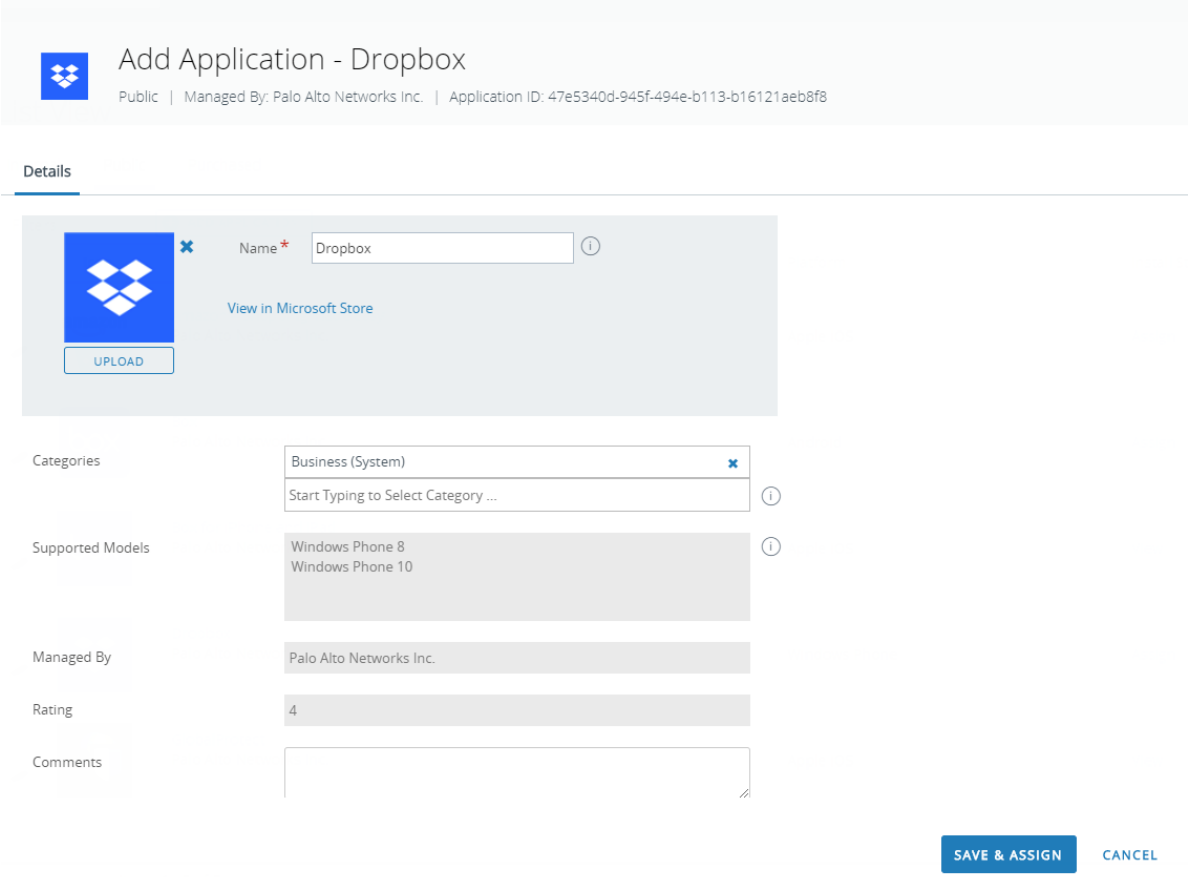
6. Haga clic en **NEXT (Siguiente)**.

   Si elige buscar la aplicación en la tienda de Microsoft, debe hacer clic en **SELECT (SELECCIONAR)** para seleccionar la aplicación de la lista de resultados de búsqueda.

© 2020 Palo Alto Networks, Inc.



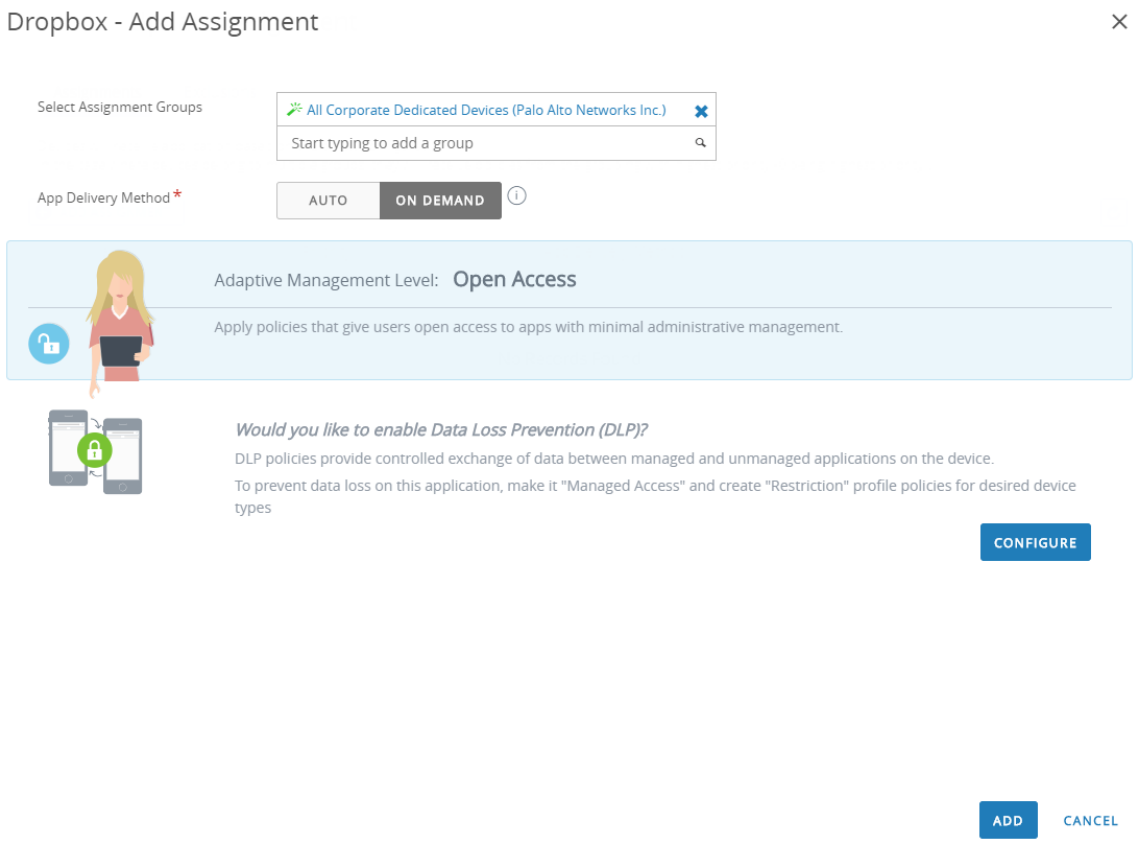
7. En el diálogo Add Application (Añadir aplicación), garantice que el **Name (Nombre)** de la aplicación sea correcto. Este es el nombre que aparecerá en el catálogo de aplicaciones de AirWatch.
8. (Opcional) Asigne la aplicación a **Categories (Categorías)** predefinidas o personalizadas para garantizar la facilidad del acceso en el catálogo de aplicaciones de AirWatch.



9. Haga clic en **SAVE & ASSIGN (GUARDAR Y ASIGNAR)** para guardar y asignar la aplicación nueva.

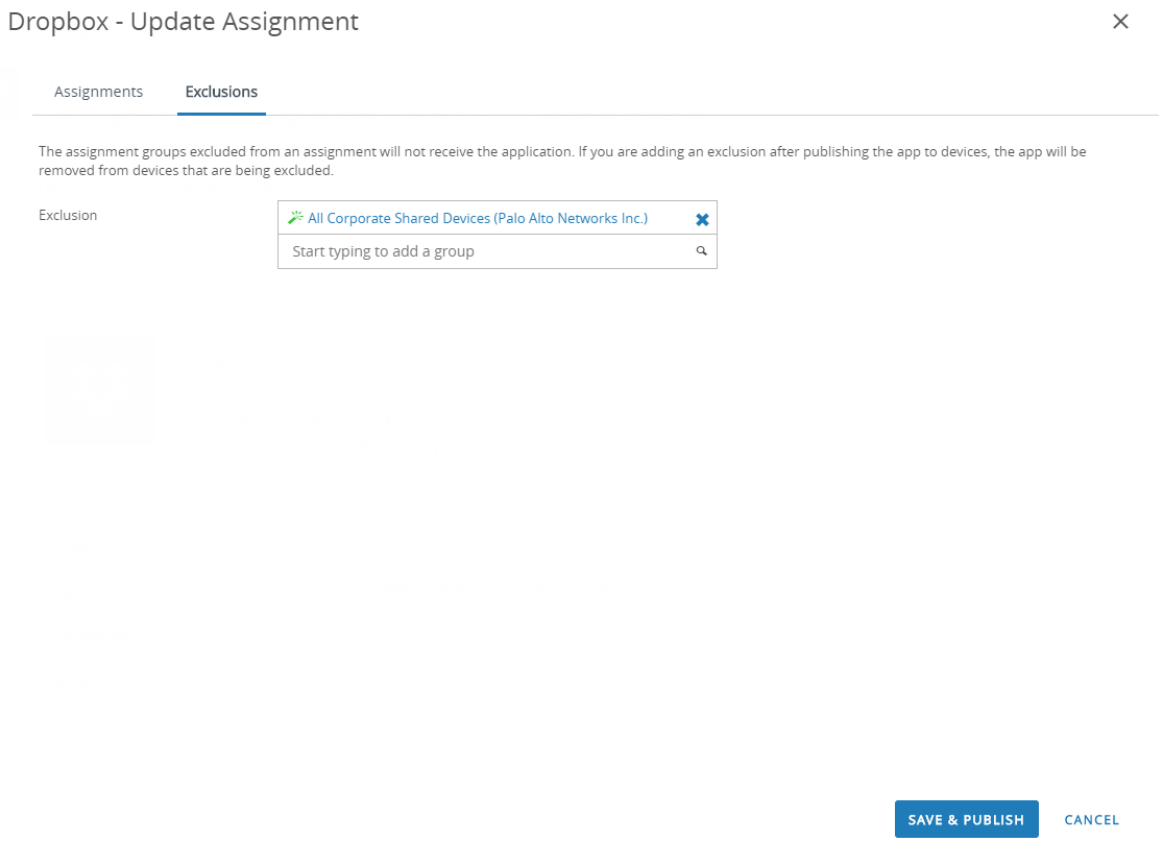
© 2020 Palo Alto Networks, Inc.

10. En el diálogo Update Assignment (Actualizar asignación), seleccione **Assignments (Asignaciones)** y haga clic en **ADD ASSIGNMENT (Añadir asignación)** para añadir los Smart Groups que podrán acceder a esta aplicación.
    1. En el campo **Select Assignment Groups (Seleccionar grupos de asignación)**, seleccione los Smart Groups a los que desea brindar acceso a esta aplicación.
    2. Seleccione el **App Delivery Method (Método de envío de la aplicación)**. Si selecciona **AUTO (AUTOMÁTICO)**, la aplicación se implementa automáticamente en los Smart Groups especificados. Si selecciona **ON DEMAND (A demanda)**, la aplicación debe implementarse manualmente.
    3. Haga clic en **ADD (Añadir)** para añadir una nueva asignación.



11. (Opcional) Para evitar que determinados Smart Groups accedan a la aplicación, seleccione **Exclusions (Exclusiones)** y seleccione los Smart Groups que desea excluir del campo **Exclusion (Exclusión)**.

© 2020 Palo Alto Networks, Inc.



12. Seleccione **SAVE & PUBLISH (Guardar y publicar)** para guardar y publicar la configuración a los Smart Groups asignados.

STEP 8 | Para seleccionar GlobalProtect como proveedor de tipo de conexión, edite el perfil de VPN en XML.

Para minimizar las ediciones adicionales en el XML sin procesar, revise los ajustes de su perfil VPN antes de exportar la configuración. Si necesita cambiar un ajuste después de exportar el perfil VPN, puede realizar los cambios en el XML sin procesar o puede actualizar el ajuste en el perfil VPN y realizar este paso nuevamente.

1. En **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**, seleccione el botón de opción junto al nuevo perfil que añadió en los pasos previos y seleccione **</>XML** en la parte superior de la tabla. AirWatch abre la vista XML del perfil.
2. Exporte el perfil y luego ábralo en un editor de texto de su elección.
3. Edite los siguientes ajustes para GlobalProtect:

- En el elemento LocIURI que especifica PluginPackageFamilyName, cambie el elemento por:

```
<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/
PluginPackageFamilyName</LocURI>
```

- En el elemento Data que sigue, cambie el valor por:

```
<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>
```

1. Guarde sus cambios en el perfil exportado.
2. Vuelva a AirWatch y seleccione **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**.

© 2020 Palo Alto Networks, Inc.

3. Cree (seleccione **Add (Añadir)** > **Add Profile (Añadir perfil)** > **Windows** > **Windows Phone**) y asigne un nombre a un perfil nuevo.
4. Seleccione **Custom Settings (Ajustes personalizados)** > **Configure (Configurar)** y luego copie y pegue la configuración modificada.
5. Haga clic en **Save & Publish** para guardar y publicar los cambios.

STEP 9 | Limpie el perfil original al seleccionarlo en **Devices (Dispositivos)** > **Profiles (Perfiles)** > **List View (Vista de lista)**, y luego, **More Actions (Más acciones)** > **Deactivate (Desactivar)**. AirWatch traslada el perfil a la lista Inactive.

STEP 10 | Compruebe la configuración.

Establecimiento de una configuración de VPN por aplicación con Microsoft Intune

Microsoft Intune es una plataforma de gestión de movilidad empresarial basada en la nube que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por Microsoft Intune y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN por aplicación con Microsoft Intune:

- Establecimiento de una configuración de VPN por aplicación para endpoints iOS con Microsoft Intune
- Establecimiento de una configuración de VPN por aplicación para endpoints de Windows 10 UWP con Microsoft Intune

Establecimiento de una configuración de VPN por aplicación para endpoints iOS con Microsoft Intune

Puede habilitar el acceso a los recursos internos de sus endpoints móviles gestionados mediante la configuración del acceso VPN de GlobalProtect con Microsoft Intune. En una configuración de VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enrutar tráfico a través del túnel VPN. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN.

Use los siguientes pasos para establecer una configuración de VPN por aplicación para endpoints iOS con Microsoft Intune:

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

STEP 2 | Añada aplicaciones a Microsoft Intune.

Antes de poder asignar, supervisar, configurar o proteger aplicaciones, debe añadirlas a Microsoft Intune.

- En **App type (Tipo de aplicación)**, seleccione **iOS**.
- Añada las aplicaciones de la tienda de iOS a Microsoft Intune.

STEP 3 | Configure los ajustes de VPN por aplicación para iOS.

- Cuando cree un perfil de VPN por aplicación, en **Platform (Plataforma)**, seleccione **iOS** y en **Connection type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect**.
- Cuando asocie una aplicación al perfil de VPN, seleccione su perfil de VPN por aplicación del menú desplegable **VPNS**.

© 2020 Palo Alto Networks, Inc.

Establecimiento de una configuración de VPN por aplicación para endpoints de Windows 10 UWP con Microsoft Intune

Puede habilitar el acceso a los recursos internos de sus endpoints móviles gestionados mediante la configuración del acceso VPN de GlobalProtect con Microsoft Intune. En una configuración de VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enrutar tráfico a través del túnel VPN. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN.

Use los siguientes pasos para establecer una configuración de VPN por aplicación para endpoints de Windows 10 UWP con Microsoft Intune:

STEP 1 | Descargue la aplicación de GlobalProtect para Windows 10 UWP:

- Implementación de la aplicación móvil de GlobalProtect con Microsoft Intune.
- Descargue la aplicación de GlobalProtect directamente desde Microsoft Store.

STEP 2 | Configuración de un perfil de certificado.

Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

STEP 3 | Cree un nuevo perfil de VPN para Windows 10 UWP.

- En **Platform (Plataforma)**, seleccione **Windows 10 and later (Windows 10 y posterior)**.

STEP 4 | Establezca los ajustes de VPN por aplicación para endpoints de Windows 10 UWP.

- En **Connection type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect**.
- En el área Apps and Traffic rules (Reglas de aplicaciones y tráfico), en la opción **Associate WIP or apps with this VPN (Asociar WIP o aplicaciones a esta VPN)**, seleccione **Associate apps with this connection (Asociar aplicaciones a esta conexión)**. Haga clic en **Enable (Habilitar)** para habilitar la opción **Restrict VPN connection to these apps (Restringir conexión de VPN a estas aplicaciones)** y en **Add (Añadir)** para añadir las aplicaciones asociadas que desea usar en la conexión de VPN.

Establecimiento de una configuración de VPN por aplicación con MobileIron

MobileIron es una plataforma de gestión de movilidad empresarial que le permite gestionar endpoints móviles desde una consola central. La aplicación de GlobalProtect proporciona una conexión segura entre los endpoints móviles gestionados por MobileIron y el cortafuegos al nivel de dispositivo o de la aplicación. Al usar GlobalProtect como conexión segura, se le permite la inspección sistemática del tráfico y la aplicación de la política de seguridad de red para la prevención de amenazas en los endpoints móviles.

Consulte las siguientes secciones para acceder a información sobre cómo establecer una configuración de VPN por aplicación usando MobileIron:

- Establecimiento de una configuración de VPN por aplicación para endpoints iOS con MobileIron

Establecimiento de una configuración de VPN por aplicación para endpoints iOS con MobileIron

Puede habilitar el acceso a los recursos internos de sus endpoints móviles gestionados mediante la configuración del acceso VPN de GlobalProtect con MobileIron. En una configuración de VPN por aplicación, puede especificar qué aplicaciones gestionadas pueden enrutar tráfico a través del túnel VPN. Las aplicaciones no gestionadas se siguen conectando directamente a internet en lugar de hacerlo a través del túnel de VPN.

Use los siguientes pasos para establecer una configuración de VPN por aplicación para endpoints iOSP con MobileIron:

© 2020 Palo Alto Networks, Inc.

STEP 1 | Descargue la aplicación de GlobalProtect para iOS.

- Implementación de la aplicación móvil de GlobalProtect con MobileIron.
- Descargue la aplicación de GlobalProtect directamente desde App Store.

STEP 2 | Añada la configuración de un certificado y configure los ajustes del certificado.

Todas las configuraciones de VPN por aplicación requieren autenticación basada en certificado.

STEP 3 | Añada una configuración de VPN por aplicación.

- En el tipo de configuración, seleccione **Per-app VPN (VPN por aplicación)**.

STEP 4 | Configure los ajustes de VPN por aplicación para iOS.

- En **Connection Type (Tipo de conexión)**, seleccione **Palo Alto Networks GlobalProtect** y configure los ajustes asociados.

Habilitación de la integración de análisis de aplicaciones con WildFire

Si habilita el análisis de aplicaciones en AirWatch, puede aprovechar la inteligencia de WildFire® contra amenazas a las aplicaciones para detectar malware en los terminales con Android. Si está habilitado, el agente de AirWatch envía la lista de aplicaciones que están instaladas en el endpoint Android a AirWatch. Esto ocurre durante la inscripción y posteriormente en el registro de cualquier endpoint. Luego, AirWatch consulta de manera regular WildFire para obtener veredictos y tomar medidas de cumplimiento en el endpoint sobre la base del veredicto.

STEP 1 | Antes de comenzar, obtenga una clave de API de WildFire. Si aún no tiene una clave de API, comuníquese con el departamento de soporte técnico.

STEP 2 | En AirWatch, seleccione**Groups & Settings (Grupos y ajustes)** > **All Settings (Todos los ajustes)** > **Apps (Aplicaciones)** > **App Scan (Análisis de aplicaciones)** > **Third Party Integration (Integración de terceros)**.

STEP 3 | Seleccione **Current Setting (Ajuste actual): Override**.

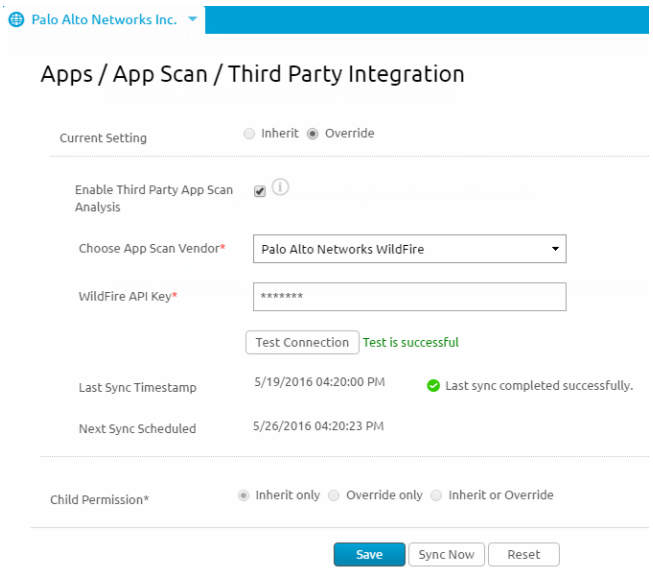
STEP 4 | Seleccione **Enable Third Party App Scan Analysis** para habilitar la comunicación entre AirWatch y WildFire.

STEP 5 | Seleccione **Palo Alto Networks WildFire** en el menú desplegable **Choose App Scan Vendor (Seleccionar proveedor de análisis de aplicaciones)**.

STEP 6 | Introduzca su clave de API de WildFire.

STEP 7 | Haga clic en Test Connection para garantizar que AirWatch pueda comunicarse con WildFire. Si el resultado de la prueba no es correcto, verifique la conectividad a internet, introduzca la clave de API de nuevo y vuelva a intentarlo.

© 2020 Palo Alto Networks, Inc.



STEP 8 | Haga clic en **Save (Guardar)** para guardar sus cambios. AirWatch programa una tarea de sincronización para comunicarse con WildFire a fin de obtener los veredictos más recientes para hashes de aplicación y ejecuta la tarea en intervalos periódicos. Haga clic en **Sync Now** para iniciar una sincronización manual con WildFire.

Supresión de notificaciones en la aplicación de GlobalProtect para endpoints de macOS

La aplicación GlobalProtect en macOS admite dos tipos de extensiones: kernel (dispositivo macOS que utiliza macOS Catalina 10.15.3 o anterior) y sistema (dispositivo macOS que utiliza macOS Catalina 10.15.4 o posterior y la aplicación de GlobalProtect 5.1.4 o posterior). Si ha configurado una división de túnel en la puerta de enlace de GlobalProtect o impone las conexiones de GlobalProtect para el acceso a la red (consulte Personalización de la aplicación GlobalProtect). Aparecerá un mensaje de notificación en la aplicación de GlobalProtect. El mensaje solicita a los usuarios que habiliten la extensión del kernel o la extensión del sistema en macOS que no se pudo cargar cuando accedan a la aplicación de GlobalProtect con esas características habilitadas.

Para permitir que los usuarios de la aplicación de GlobalProtect carguen automáticamente la extensión del kernel o la extensión del sistema sin recibir una notificación, puede usar el sistema de gestión de dispositivos móviles (Mobile Device Management System, MDM) compatible para crear una política para esa extensión, como Airwatch.

Consulte las siguientes secciones para obtener información sobre cómo eliminar las notificaciones en la aplicación de GlobalProtect para endopoints de macOS:

- Habilitación de las extensiones de kernel en la aplicación de GlobalProtect para endpoints de macOS
- Habilitación de las extensiones del sistema en la aplicación de GlobalProtect para endpoints de macOS

Habilitación de las extensiones de kernel en la aplicación de GlobalProtect para endpoints de macOS

A partir de macOS 10.13, Apple introdujo un cambio de software que requiere que los usuarios aprueben las extensiones del kernel para poder usarlas.

Aunque los usuarios pueden habilitar manualmente la extensión del kernel en macOS (**System Preferences (Preferencias del sistema)** > **Security & Privacy (Seguridad y privacidad)** y **Allow (Permitir)** extensión

© 2020 Palo Alto Networks, Inc.

del kernel), puede usar cualquier proveedor de MDM cualificado para crear una política y aprobar automáticamente la extensión del kernel. La nota técnica de Apple TN2450 describe el proceso.

El siguiente flujo de trabajo se ha probado con Airwatch.

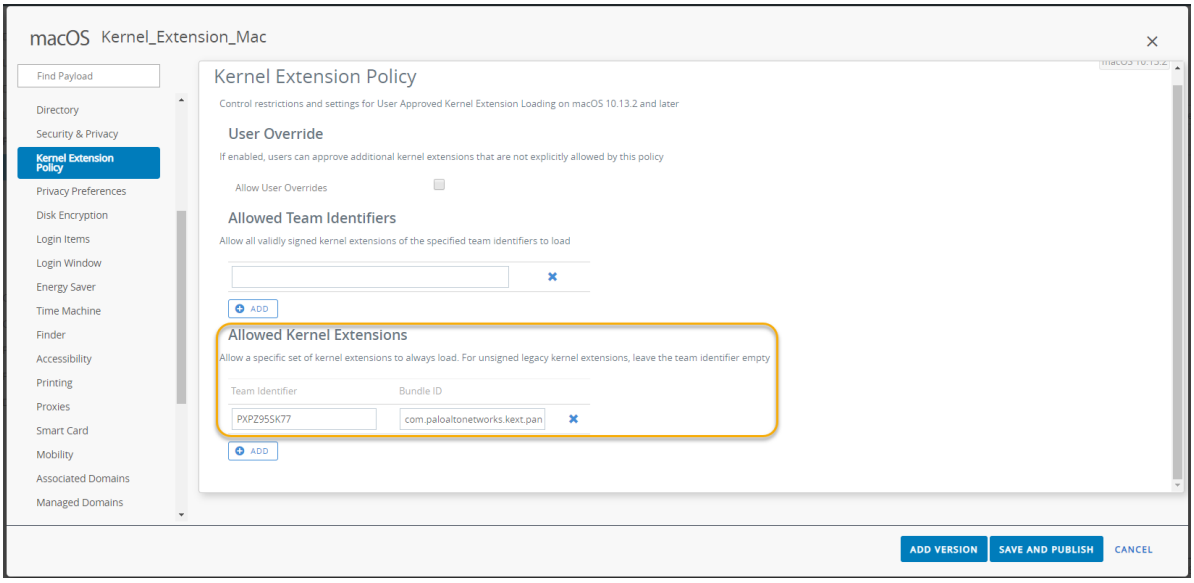
STEP 1 | Cree una política de extensión del kernel.

1. Inicie sesión en AirWatch como administrador.
2. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y, a continuación, seleccione **Add (Añadir)** > **Add Profile (Añadir perfil)** en el menú desplegable.
3. En el área **Add Profile (Añadir perfil)**, haga clic en **Apple macOS** y, a continuación, haga clic en el icono **Device Profile (Perfil del dispositivo)**.
4. En el área **General**, especifique el nombre del perfil.

   También puede seleccionar un perfil de extensión del kernel existente (**Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)**) en la lista.

STEP 2 | Añada una extensión de kernel y distribuya la política relevante a los dispositivos macOS.

1. Seleccione **Kernel Extension Policy (Política de extensión del kernel)**.
2. Especifique el **identificador de equipo** utilizado por la aplicación de GlobalProtect (**PXPZ95SK77**).
3. Introduzca el **ID del paquete** (**com.paloaltonetworks.kext.pangpd**).



4. Haga clic en **Save and Publish (Guardar y publicar)** para guardar los cambios.

Habilitación de las extensiones del sistema en la aplicación de GlobalProtect para endpoints de macOS

A partir de macOS 10.15.4, Apple ha limitado la compatibilidad de las extensiones del kernel. La aplicación de GlobalProtect utilizará extensiones del sistema en lugar de extensiones del kernel. Los usuarios deben aprobar las extensiones del sistema para poder usarlas.

Además de habilitar las extensiones del sistema, puede activar las extensiones de red en la aplicación de GlobalProtect para suprimir los mensajes emergentes de Network Extensions Configuration (Configuración de extensiones de red) que se utilizan para las funciones Split Tunnel (Dividir túnel) y Enforce GlobalProtect Connections for Network Access (Aplicar conexiones de GlobalProtect para el acceso de red). Puede utilizar el sistema de gestión de dispositivos móviles (MDM, Mobile Device Management System), como Jamf Pro, para cargar automáticamente las extensiones de red sin recibir mensajes emergentes. Consulte

© 2020 Palo Alto Networks, Inc.

el artículo de la base de conocimientos en https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8 para obtener información sobre cómo habilitar las extensiones de red y del sistema con Jamf Pro.

Siga los pasos que aparecen a continuación para configurar un perfil y aprobar automáticamente la extensión del sistema mediante AirWatch. Aunque esta configuración se ha probado con AirWatch, puede utilizar cualquier proveedor de cualificado para crear e implementar este perfil.

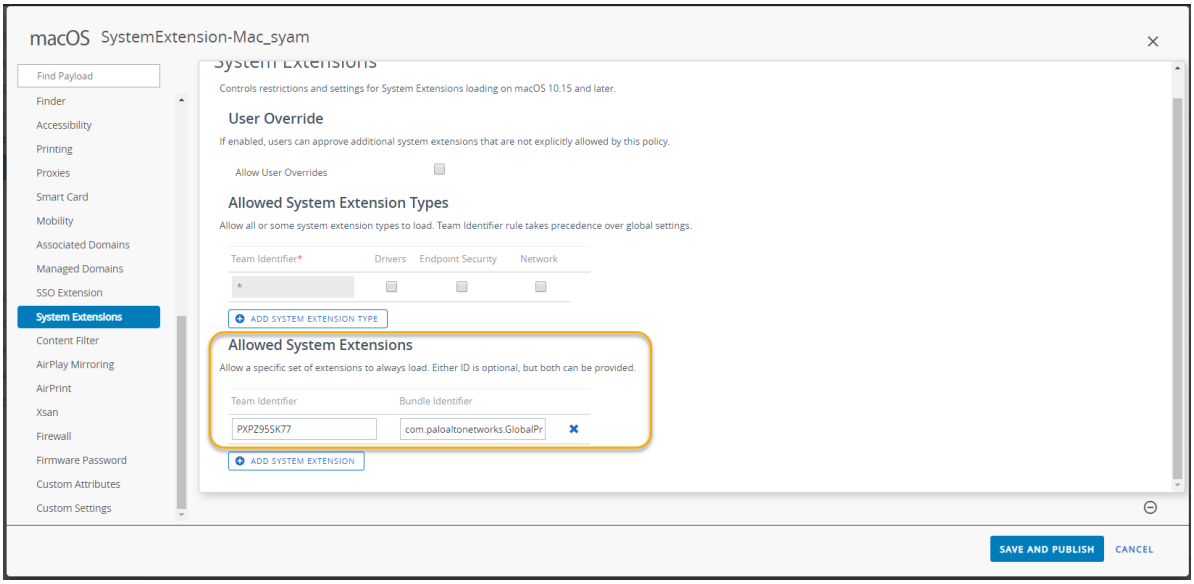
STEP 1 | Cree un perfil de extensión del sistema.

1. Inicie sesión en AirWatch como administrador.
2. Seleccione **Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)** y, a continuación, seleccione **Add (Añadir)** > **Add Profile (Añadir perfil)** en el menú desplegable.
3. En el área **Add Profile (Añadir perfil)**, haga clic en **Apple macOS** y, a continuación, haga clic en el icono **Device Profile (Perfil del dispositivo)**.
4. En el área **General**, especifique el nombre del perfil.

   También puede seleccionar un perfil de extensión del sistema existente (**Devices (Dispositivos)** > **Profiles & Resources (Perfiles y recursos)** > **Profiles (Perfiles)**) en la lista.

STEP 2 | Añada una extensión del sistema.

1. Seleccione **System Extensions (Extensiones del sistema)**.
2. Especifique el **identificador de equipo** utilizado por la aplicación de GlobalProtect (**PXPZ95SK77**).
3. Especifique el **identificador del paquete** (**com.paloaltonetworks.GlobalProtect.client.extension**).



4. Haga clic en **Save and Publish (Guardar y publicar)** para guardar los cambios.

Gestión de la aplicación de GlobalProtect con MDM externo

Para implementar y gestionar la aplicación de GlobalProtect, puede usar otros sistemas de gestión de dispositivos móviles (mobile device management, MDM) si no recurre a los proveedores aptos:

- Configuración de la aplicación de GlobalProtect para iOS
  - Ejemplo: Configuración de VPN a nivel de dispositivo de la aplicación GlobalProtect para iOS
  - Ejemplo: Configuración de VPN a nivel de aplicación de la aplicación GlobalProtect iOS
- Configuración de la aplicación de GlobalProtect para Android

© 2020 Palo Alto Networks, Inc.

- Ejemplo: Establecer la configuración de VPN
- Ejemplo: Eliminar la configuración de VPN

Configuración de la aplicación de GlobalProtect para iOS

Mientras que un sistema de MDM de terceros le permite enviar el ajuste de configuración que permite el acceso a sus recursos corporativos y proporciona un mecanismo para aplicar las restricciones del endpoint, no asegura la conexión entre endpoint móvil y los servicios a los que se conecta. Para permitir que la aplicación establezca conexiones seguras, debe habilitar la compatibilidad con VPN en el endpoint.

La siguiente tabla describe los ajustes típicos que puede configurar con el sistema de MDM de terceros:

setting	Description (Descripción)	Valor
Tipo de conexión	Tipo de conexión habilitada por la política.	**`Custom SSL`**
Identificador	Identificador para la VPN SSL personalizada en formato DNS inverso.	**`com.paloaltonetworks.globalprotect.vpn`**
Servidor	Nombre de host o dirección IP del portal de GlobalProtect.	**`<hostname or IP address>`** Por ejemplo: **`gp.paloaltonetworks.com`**
Cuenta	Cuenta de usuario para la autenticación de la conexión.	**`<username>`**
Autenticación de usuario	Tipo de autenticación para la conexión.	**`Certificate | Password`**
Credencial	(Autenticación de usuario con certificado únicamente) Credencial para autenticar la conexión.	**`<credential>`** Por ejemplo: **`clientcredial.p12`**
Habilitar VPN bajo demanda	(Opcional) El dominio y el nombre de host que establecen la conexión y la acción a demanda: • Siempre establecer conexión • Nunca establecer conexión • Establecer una conexión si fuera necesario	**`<domain and hostname and the on-demand action>`** Por ejemplo: `gp.acme.com; Never establish`

Ejemplo: Configuración de VPN a nivel de dispositivo de la aplicación GlobalProtect para iOS

El siguiente ejemplo muestra la configuración XML que contiene una carga útil VPN que puede usar para verificar la configuración de VPN a nivel de dispositivo de la aplicación de GlobalProtect para iOS.

```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
```


© 2020 Palo Alto Networks, Inc.

```
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample Device Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011d</string>
<key>UserDefinedName</key>
<string>Sample Device Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>OnDemandRules</key>
<array>
<dict>
<key>Action</key>
<string>Connect</string>
</dict>
</array>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
```


© 2020 Palo Alto Networks, Inc.

```
<string>Sample Device Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```


Ejemplo: Configuración de VPN a nivel de aplicación de la aplicación GlobalProtect iOS

El siguiente ejemplo muestra la configuración XML que contiene una carga útil VPN que puede usar para verificar la configuración de VPN a nivel de la aplicación de la aplicación de GlobalProtect para iOS.


```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample App Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed.applayer</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>VPNUUID</key>
<string>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIExldmVsIFZQTg==</
string>
<key>SafariDomains</key>
<array>
<string>*.paloaltonetworks.com</string>
</array>
<key>PayloadUUID</key>
<string>54370008-205f-7c59-0000-01a1</string>
<key>UserDefinedName</key>
<string>Sample App Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
```


© 2020 Palo Alto Networks, Inc.

```
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>OnDemandMatchAppEnabled</key>
<integer>1</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>OnlyAppLevel</key>
<integer>1</integer>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Sample App Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```


Configuración de la aplicación de GlobalProtect para Android

Puede implementar y configurar la aplicación de GlobalProtect en los endpoints de Android For Work de cualquier sistema de administración de dispositivos móviles (mobile device management, MDM) de terceros que admita limitaciones de datos de la aplicación de Android For Work.

En los endpoints de Android, el tráfico se enruta a través del túnel VPN de acuerdo con las rutas de acceso configuradas en la puerta de enlace de GlobalProtect. Desde su MDM de terceros que gestiona los endpoints de Android for Work, puede refinar aún más el tráfico que se enruta a través del túnel VPN.

© 2020 Palo Alto Networks, Inc.

En un entorno en el que el endpoint es propiedad de la empresa, el titular del endpoint gestiona todo el endpoint, incluidas todas las aplicaciones instaladas en ese endpoint. Por defecto, todas las aplicaciones instaladas pueden enviar tráfico a través del túnel VPN de acuerdo con las rutas de acceso definidas en la puerta de enlace.

En un entorno uso de dispositivos personales en el trabajo (bring-your-own-device, BYOD), el endpoint no es propiedad de la empresa y utiliza un perfil de trabajo para separar las aplicaciones comerciales de las personales. Por defecto, solo las aplicaciones gestionadas en el perfil de trabajo pueden enviar tráfico a través del túnel VPN de acuerdo con las rutas de acceso definidas en la puerta de enlace. Las aplicaciones del lado personal del endpoint no pueden enviar tráfico a través del túnel VPN establecido por la aplicación de GlobalProtect gestionada que se instaló en el perfil de trabajo.

Para enrutar tráfico desde un conjunto aún menor de aplicaciones, usted puede habilitar la VPN por aplicación de manera que GlobalProtect solo enrute tráfico desde aplicaciones gestionadas específicas. Para la VPN por aplicación, puede permitir o no permitir aplicaciones gestionadas específicas en una lista de permitidos o no permitidos para que el tráfico se enrute o no a través del túnel VPN.

Como parte de la configuración de VPN, también puede especificar de qué manera el usuario se conecta a la VPN. Cuando configura el método de conexión como **user-logon (Inicio de sesión del usuario)**, la aplicación de GlobalProtect establece una conexión automáticamente. Cuando configura el método de conexión como **on-demand (A demanda)**, los usuarios deben iniciar una conexión manualmente.

El método de conexión de VPN definido en el MDM tiene prioridad con respecto al método de conexión definido en la configuración del portal de GlobalProtect.

Cuando se elimina la configuración de VPN, se restablece automáticamente la aplicación de GlobalProtect con sus ajustes de configuración originales.

Para configurar la aplicación de GlobalProtect para Android, configure las siguientes restricciones de aplicación de Android.

Clave	Tipo de valor	Description (Descripción)	Ejemplo
portal	Cadena	Dirección IP o nombre de dominio completo (fully qualified domain name, FQDN) del portal.	`10.1.8.190`
nombre de usuario	Cadena	Nombre del usuario.	`john`
Contraseña	Cadena	Contraseña del usuario.	`Passwd!234`
mobile_id	Cadena	El ID móvil como se configuró en el servicio de MDM de terceros para identificar de manera única a un dispositivo móvil. GlobalProtect usa este ID móvil para recuperar la información del dispositivo.	`5188a8193be43f42d332dde5cb2c941e`
certificado	Secuencia de comandos (en Base64)	El certificado (cert) del cliente utilizado para autenticar al agente y al portal.	`DAFDSaweEWQ23wDSAFD….`

© 2020 Palo Alto Networks, Inc.

Clave	Tipo de valor	Description (Descripción)	Ejemplo
client_certificate_passphrase	Cadena	La clave asociada con el cliente del certificado.	**PA$$W0RD$123**
app_list	Cadena	La configuración para la VPN por aplicación. Comience la cadena con la lista de permitidos o la lista de no permitidos, y continúe con los nombres de las aplicaciones separados por punto y coma. La lista de permitidos especifica las aplicaciones que usarán el túnel VPN para la comunicación de red. El tráfico de red para cualquier otra aplicación que no esté en la lista de permitidos o indicada expresamente en la lista de no permitidos, no atravesará el túnel VPN.	**allow list | block list: com.google.calendar; com.android.email; com.android.chrome**
connect_method	Cadena	El inicio de sesión del usuario para conectar al usuario automáticamente con el portal de GlobalProtect mediante sus credenciales de Windows o a demanda para conectar de forma manual el usuario con la puerta de enlace.	**user-logon | on-demand**
remove_vpn_config_via_restriction	Expresión booleana	Elimine de manera permanente toda la información de la configuración de VPN de GlobalProtect.	**true | false**

Ejemplo: Establecer la configuración de VPN

```
private static String RESTRICTION_PORTAL
= "portal";
private static String RESTRICTION_USERNAME = "username";
private static String RESTRICTION_PASSWORD = "password";
private static String RESTRICTION_CONNECT_METHOD = "connect_method";
private static String RESTRICTION_CLIENT_CERTIFICATE
= "client_certificate";
private static String RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE
= "client_certificate_passphrase";
private static String RESTRICTION_APP_LIST = "app_list";
private static String RESTRICTION_REMOVE_CONFIG =
 "remove_vpn_config_via_restriction";

Bundle config = new Bundle();
config.putString(RESTRICTION_PORTAL, "192.168.1.1");
config.putString(RESTRICTION_USERNAME, "john");
config.putString(RESTRICTION_PASSWORD, "Passwd!234");
```


© 2020 Palo Alto Networks, Inc.

```
config.putString(RESTRICTION_CONNECT_METHOD, "user-logon");
config.putString(RESTRICTION_CLIENT_CERTIFICATE, "DAFDSaweEWQ23wDSAFD….");
config.putString(RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE,
"PA$$W0RD$123");
config.putString(RESTRICTION_APP_LIST, "allow
 list:com.android.chrome;com.android.calendar");

DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(this),
"com.paloaltonetworks.globalprotect", config);
```

Ejemplo: Eliminar la configuración de VPN

```
Bundle config = new Bundle();
config.putBoolean(RESTRICTION_REMOVE_CONFIG, true );
DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.
getComponentName(this),"com.paloaltonetworks.globalprotect",
config);
```

GlobalProtect para dispositivos IoT

Con GlobalProtect para IoT, puede proteger el tráfico y extender la aplicación de políticas de seguridad a sus dispositivos IoT. Después de configurar GlobalProtect para IoT, la aplicación de GlobalProtect se autentica con el portal o las puertas de enlace de GlobalProtect mediante certificados de cliente y, opcionalmente, un nombre de usuario y contraseña. Tras una autenticación correcta, la aplicación de GlobalProtect establece un túnel IPSec. En el caso de que la conexión mediante IPSec no se realice correctamente, puede configurar la aplicación de GlobalProtect para que recurra a un túnel SSL. Consulte la Matriz de compatibilidad de Palo Alto Networks para obtener una lista de funciones compatibles con el sistema operativo para dispositivos IoT.

- Requisitos de GlobalProtect para IoT
- Configuración de los portales y puertas de enlace de GlobalProtect para dispositivos IoT
- Instalación de GlobalProtect para IoT en Android
- Instalación de GlobalProtect para IoT en Raspbian
- Instalación de GlobalProtect para IoT en Ubuntu
- Instalación de GlobalProtect para IoT en Windows

© 2020 Palo Alto Networks, Inc.

Requisitos de GlobalProtect para IoT

GlobalProtect para IoT tiene los siguientes requisitos:

- Suscripción a Prisma Access o a GlobalProtect
- El cortafuegos está utilizando PAN-OS 10.0 (actualizar ahora)
- Uno de los siguientes sistemas operativos:
  - Android
  - Raspbian
  - Ubuntu
  - Windows IoT Enterprise
- 128 MB de RAM
- 4 GB de almacenamiento
- x86, procesador ARMv7 o ARMv5
- Instalación con paquetes de aplicaciones de instantáneas de la CLI o WebDM

© 2020 Palo Alto Networks, Inc.

Configuración de los portales y puertas de enlace de GlobalProtect para dispositivos IoT

STEP 1 | Revise los Requisitos de GlobalProtect para IoT .

STEP 2 | Configure las puertas de enlace de GlobalProtect para admitir la aplicación de GlobalProtect para IoT.

1. Complete las tareas de requisitos previos para configurar una puerta de enlace de GlobalProtect.
2. Instale una suscripción a GlobalProtect para cada puerta de enlace que admita la aplicación de GlobalProtect para IoT. Si utiliza Prisma Access, no es necesaria una suscripción a GlobalProtect.
3. Personalice una configuración de puerta de enlace para sus dispositivos IoT:

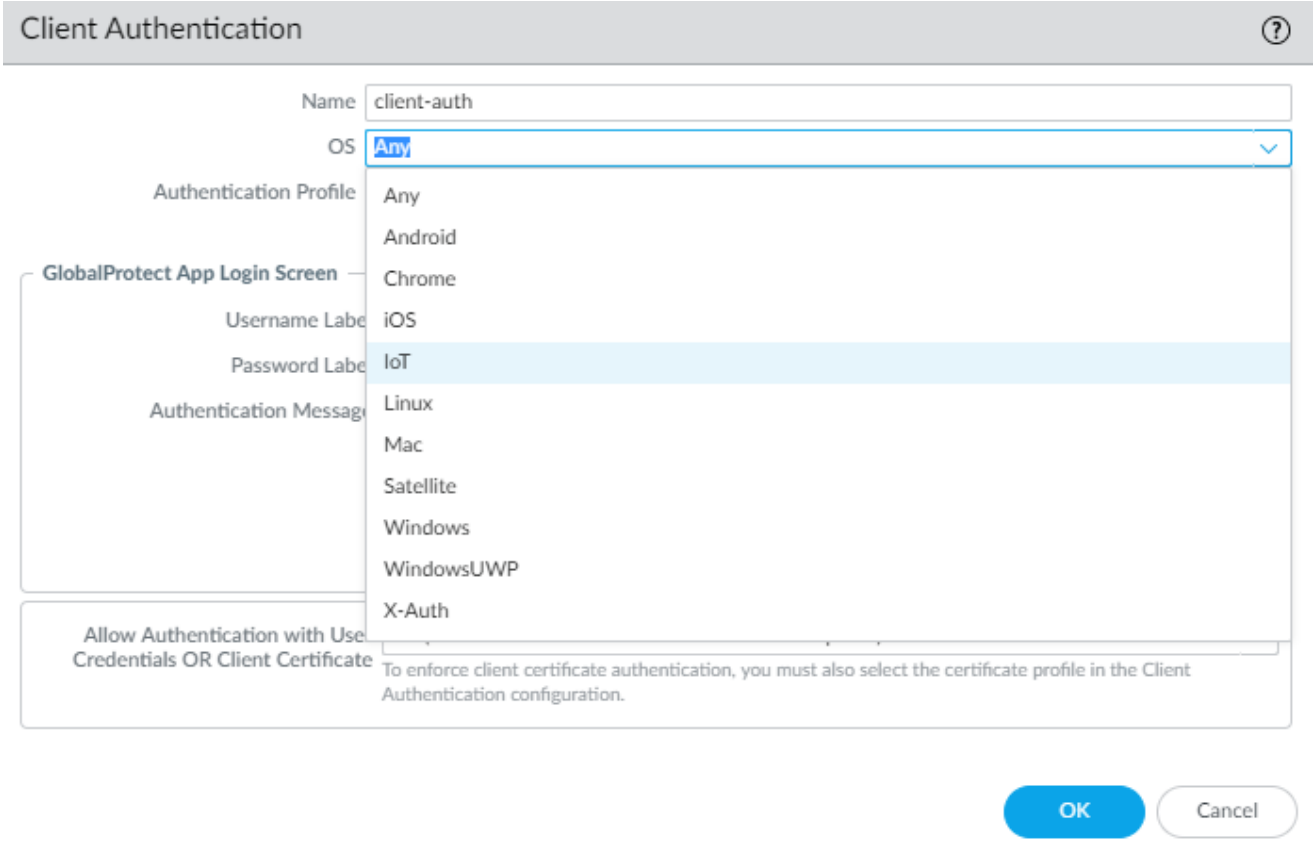
   Cuando ajuste una puerta de enlace, puede especificar la configuración de autenticación del cliente que se aplica específicamente a IoT. Por ejemplo, puede configurar los endpoints de Windows y macOS para usar la autenticación de dos factores y requerir que los dispositivos IoT utilicen la autenticación basada en certificados.

   También puede configurar los ajustes de red y cliente compatibles, como grupos de IP específicas, rutas de acceso y división de túnel, para dispositivos IoT.

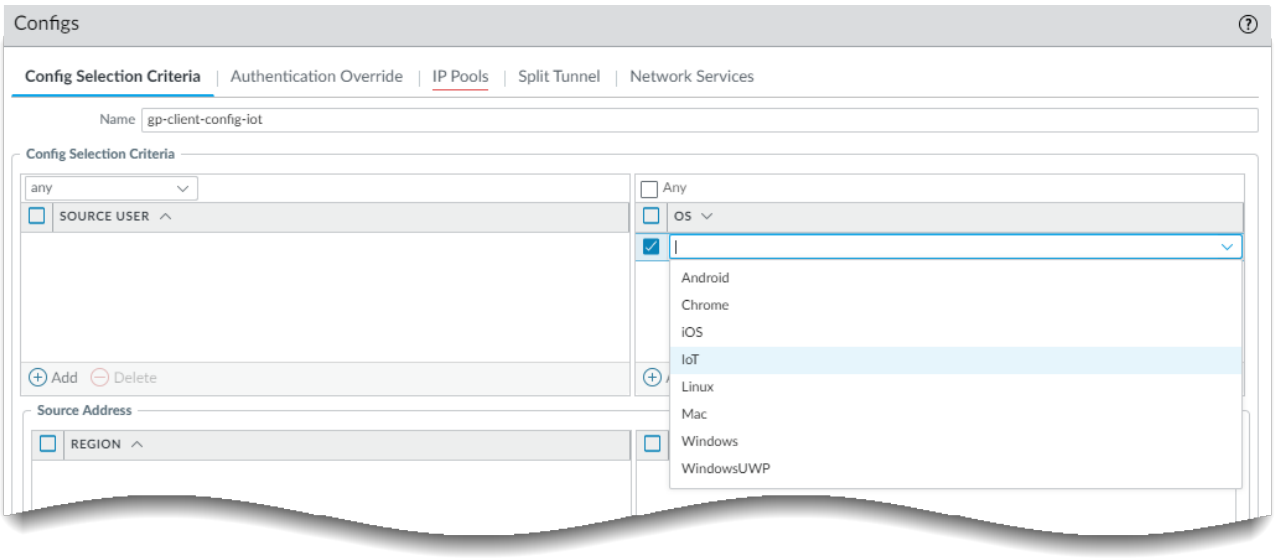
   1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y, a continuación, seleccione o **añada** una configuración de puerta de enlace.
   2. Para añadir una configuración de autenticación de cliente para dispositivos IoT, realice el siguiente procedimiento:

      1. Seleccione **Authentication (Autenticación)** y **añada** una nueva configuración de autenticación del cliente.
      2. Especifique un **nombre** para identificar la autenticación del cliente, establezca **OS** en **IoT** y especifique el **perfil de autenticación** que usar para la autenticación de usuarios en esta puerta de enlace. Elija un perfil que permita la autenticación del certificado del cliente.

© 2020 Palo Alto Networks, Inc.



   3. Haga clic en **OK (Aceptar)**.
3. Para configurar ajustes específicos del cliente que se aplican solo a los endpoints de IoT, establezca un nuevo ajuste de configuración del cliente.
   1. Seleccione **Agent (Agente)** y **añada** una nueva configuración de ajustes del cliente.
   2. Configure los ajustes de autenticación del cliente como desee.
   3. Seleccione **User/User Group (Usuario/Grupo de usuarios)** y, a continuación, **añada** un SO y seleccione **IoT**.



© 2020 Palo Alto Networks, Inc.

4. Haga clic en **OK (Aceptar)**.
4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 3 | Configure el portal para admitir la aplicación de GlobalProtect para dispositivos IoT.

Para admitir dispositivos IoT, debe configurar una o más puertas de enlace a las que se pueda conectar la aplicación de GlobalProtect y, después, configurar el portal y los ajustes de la aplicación. El portal envía información de configuración e información sobre las puertas de enlace disponibles a la aplicación. Después de recibir la configuración del portal de GlobalProtect, la aplicación detecta las puertas de enlace que aparecen en la configuración del cliente y selecciona la mejor puerta de enlace. Utilice el siguiente flujo de trabajo para configurar el portal de GlobalProtect para que sea compatible con la aplicación de GlobalProtect para dispositivos IoT.

1. Si aún no lo ha hecho, complete las tareas de requisitos previos para configurar un portal de GlobalProtect.
2. Defina la configuración del cliente para los dispositivos IoT para autenticarse en el portal.
   1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, seleccione una configuración del portal.
   2. Configure los ajustes de autenticación del cliente que se aplican a los dispositivos IoT cuando los usuarios acceden al portal:
      1. Seleccione **Authentication (Autenticación)** y, a continuación, **añada** una nueva configuración de autenticación del cliente.
      2. Especifique un **nombre** para identificar la autenticación del cliente, establezca **OS** en **IoT** y especifique el perfil de autenticación que usar para la autenticación de usuarios en este portal. Elija un perfil que permita la autenticación del certificado del cliente.
3. Personalice una configuración de agente para dispositivos IoT.

   La modificación de una configuración existente o la creación de una nueva dependen de su entorno. Por ejemplo, si usa puertas de enlace específicas del sistema operativo o desea recopilar información de host que sea específica para dispositivos IoT, considere crear una nueva configuración de agente.

   Para obtener información sobre las funciones compatibles, consulte la Matriz de compatibilidad de redes de Palo Alto para obtener una lista de las funciones compatibles con el sistema operativo para dispositivos IoT.

   1. Defina una configuración de agente de GlobalProtect:
   2. Seleccione **Agent (Agente)** y elija uno existente o **añada** una nueva configuración del agente del portal.
   3. Configure los ajustes de autenticación para dispositivos IoT.
   4. Seleccione **User/User Group (Usuario/Grupo de usuarios)** y, a continuación, añada un **SO** y seleccione **IoT**.
   5. Especifique las puertas de enlace externas a las que se podrán conectar los usuarios con esta configuración.
   6. (Opcional) Seleccione **App (Aplicación)** y personalice la configuración del portal correspondiente para la aplicación de GlobalProtect para IoT. La aplicación de GlobalProtect descarta cualquier configuración que no se aplique a IoT. Para obtener una lista de las funciones compatibles por sistema operativo, consulte la Matriz de compatibilidad de redes de Palo Alto para obtener una lista de las funciones compatibles con el sistema operativo para dispositivos IoT.
   7. Haga clic en **OK** dos veces.
   8. Haga clic en **Commit (Confirmar)** para confirmar la configuración.
4. Aplique políticas en dispositivos IoT (**Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)**).

   Ahora puede crear objetos HIP mediante la información del host específica para dispositivos IoT y usarla para condiciones de coincidencia en cualquier perfil HIP. A continuación, puede usar un perfil

© 2020 Palo Alto Networks, Inc.

HIP como condición de coincidencia en una regla de política para aplicar la política de seguridad correspondiente.

1. Seleccione **General** > **Host Info (Información del host)** > **OS (SO)**.
2. Seleccione **Contains (Contiene)** > **IoT**.
3. Haga clic en **OK (Aceptar)**.
4. Cree objetos HIP adicionales según sea necesario.
5. Configure la aplicación de políticas basadas en HIP.

STEP 4 | Instale y configure la aplicación de GlobalProtect para IoT.

Utilice las instrucciones proporcionadas para el sistema operativo de su dispositivo IoT.

- Instalación de GlobalProtect para IoT en Android
- Instalación de GlobalProtect para IoT en Raspbian
- Instalación de GlobalProtect para IoT en Ubuntu
- Instalación de GlobalProtect para IoT en Windows

© 2020 Palo Alto Networks, Inc.

Instalación de GlobalProtect para IoT en Android

Para usar GlobalProtect para IoT en dispositivos Android, debe compilar la aplicación y la configuración de GlobalProtect en la imagen del sistema operativo Android como una aplicación del sistema. Para permitir que GlobalProtect funcione en modo sin periféricos, debe implementar un archivo de preconfiguración con el paquete de la aplicación de GlobalProtect.

STEP 1 | Añada GlobalProtect.apk como una aplicación de sistema precompilada en la imagen de su sistema operativo Android.

1. En el sitio de soporte, seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** y descargue el APK de GlobalProtect.
2. Descodifique el archivo APK en el directorio `android_src_tree_root/packages/app/`.

   El descodificador desempaqueta la aplicación en una carpeta de GlobalProtect.
3. En la carpeta de GlobalProtect, cree el archivo `Android.mk`. Este archivo define las fuentes y las bibliotecas compartidas que el codificador usará para el sistema de compilación.

   Edite el archivo para incluir lo siguiente:

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE_TAGS := optional
LOCAL_MODULE := GlobalProtect
LOCAL_SRC_FILES := $(LOCAL_MODULE).apk
LOCAL_MODULE_CLASS := APPS
LOCAL_MODULE_SUFFIX := $(COMMON_ANDROID_PACKAGE_SUFFIX)
LOCAL_CERTIFICATE := PRESIGNED
include $(BUILD_PREBUILT)
```

4. Para cualquier archivo MK adicional en `android_src_tree_root/vendor/`, añada la siguiente línea:

```
PRODUCT_PACKAGES += GlobalProtect
```

5. Añada libgpjni.so a `/system/lib` o `/system/lib64`, según la arquitectura de CPU que admita el dispositivo IoT. El archivo libgpjni.so se puede recuperar del directorio lib después de que apktol descodifique GlobalProtect.apk.

STEP 2 | Modifique el código fuente de Android Framework para autorizar previamente la ventana emergente de solicitud de permiso para la conexión VPN.

Edite el archivo `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` para incluir el siguiente segmento de código:

```
private boolean isVpnUserPreConsented(String packageName) {

    if ("com.paloaltonetworks.globalprotect".equals(packageName)){
        Log.v(TAG, "IoT, isVpnUserPreConsented always true");
    return true;
    }
    AppOpsManager appOps =
        (AppOpsManager) mContext.getSystemService(Context.APP_OPS_SERVICE);
```


© 2020 Palo Alto Networks, Inc.

```
    // Verify that the caller matches the given package and has permission
 to activate VPNs.
    return
 appOps.noteOpNoThrow(AppOpsManager.OP_ACTIVATE_VPN,Binder.getCallingUid(),
        packageName) == AppOpsManager.MODE_ALLOWED;
    }
}
```

STEP 3 | Personalice el comportamiento de Android para suprimir el icono de GlobalProtect en la barra de notificaciones para Android 8.0 y versiones posteriores.

Edite el archivo `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` para incluir el siguiente segmento de código.

```
if ( r.packageName.equals("com.paloaltonetworks.globalprotect") ) {
    Slog.d(TAG, "not to show the foreground service running notification for
 IoT");
} else {
    r.postNotification();
}
```

STEP 4 | Configure los ajustes de VPN que desee implementar previamente para dispositivos Android IoT.

1. Cree un archivo de configuración (`globalprotect.conf`) en el siguiente formato y edite la dirección IP del portal de GlobalProtect y la configuración de autenticación, ya sea: nombre de usuario y contraseña, o ruta del certificado del cliente (client-cert-path) y el archivo de frase de contraseña (client-cert-passphrase).

   Username-password based authentication (Autenticación basada en nombre de usuario y contraseña)

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <username>user1</username>
                <password>mypassw0rd</password>
                <log-path-service>/home/gptest/Desktop/data/gps</log-path-
service>
                <log-path-agent>/home/gptest/Desktop/data/gpadata</log-
path-agent>
        </Settings>
</GlobalProtect>
```

   Client-certificate based authentication (Autenticación basada en certificados de cliente)

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
```


© 2020 Palo Alto Networks, Inc.

```
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <client-cert-path>/home/gptest/Desktop/data/
pan_client_cert.pfx</client-cert-path>
                <client-cert-passphrase>/home/gptest/Desktop/data/
pan_client_cert_passcode.dat</client-cert-passphrase>
                <username>user1</username>
                <password>paloalto</password>
                <log-path-service>/home/gptest/Desktop/data/gps</log-path-
service>
                <log-path-agent>/home/gptest/Desktop/data/gpadata</log-
path-agent>
        </Settings>
</GlobalProtect>
```

2. Codifique el archivo `globalprotect.conf` en formato Base64 y guárdelo en el directorio `android_src_tree_root/system/config/`.

   Si lo desea, puede guardar el archivo en una ubicación alternativa. Sin embargo, debe editar la ubicación de esta configuración en el archivo `android_src_tree_root/assets/gp_conf_location.txt`.

STEP 5 | Compile el archivo APK de GlobalProtect.

STEP 6 | Firme el archivo APK de GlobalProtect.

STEP 7 | Envíe el nuevo sistema operativo a los dispositivos Android como parte de la imagen del sistema y, a continuación, envíe el nuevo sistema operativo a los dispositivos Android.

© 2020 Palo Alto Networks, Inc.

Instalación de GlobalProtect para IoT en Raspbian

Para instalar GlobalProtect para IoT en dispositivos Raspbian, realice los siguientes pasos.

GlobalProtect para IoT para Raspbian y Ubuntu solo admite una arquitectura basada en ARM.

STEP 1 | En el sitio de soporte, seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** y descargue el paquete de GlobalProtect para su sistema operativo.

STEP 2 | Instale la aplicación de GlobalProtect para IoT.

Desde el dispositivo IoT, use el comando **`sudo dpkg -i GlobalProtect_deb_arm<version>.deb`** para instalar el software.

```
sudo dpkg -i GlobalProtect_deb_arm-5.1.0.0-84.deb
```

*Para desinstalar más tarde el software, use el comando **`sudo dpkg -P globalprotect`**.*

STEP 3 | Configure los ajustes de VPN que desee implementar previamente para dispositivos Raspbian IoT.

1. En la ruta `client-cert`, importe el certificado en formato pcks12 y guarde el archivo con una extensión .pfx (por ejemplo, **pan_client_cert.pfx**).
2. En la ruta `client-cert-passphrase`, guarde el archivo de contraseña con la extensión .dat (por ejemplo, **pan_client_cert_passcode.dat**).
3. En la ruta `log-path-service`, si no está utilizando la ruta predeterminada para PanGPS (por ejemplo, `/opt/paloaltonetworks/globalprotect`), asegúrese de que la carpeta de ruta `log-setting` tenga el mismo privilegio que la carpeta globalprotect en `opt/paloaltonetworks`.
4. Cree un archivo de configuración anterior a la implementación (`/opt/paloaltonetworks/globalprotect/pangps.xml`) en el siguiente formato y edite la dirección IP del portal de GlobalProtect y la configuración de autenticación, ya sea: nombre de usuario y contraseña, o ruta del certificado del cliente (**`client-cert-path`**) y el archivo de frase de contraseña (**`client-cert-passphrase`**). También puede especificar una carpeta opcional en la que almacenar registros del servicio de GlobalProtect (**`log-path-service`**) y logs de agente (**`log-path-agent`**).

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
         <receive-timeout>30</receive-timeout>
```


© 2020 Palo Alto Networks, Inc.

```
        <os-type>IoT</os-type>             //pre-deployed OS type for IoT.
 If this tag does not present, GP will automatic detect the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less mode
        <username>abc</username>    //optional pre-deployed username
        <password>xyz</password>       //optional pre-deployed password
        <client-cert-path>cli_cert_path</client-cert-path>       //optional
 pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase>       //optional pre-deployed client certificate passphrase file
 path
        <log-path-service>/tmp/gps</log-path-service>  //optional pre-
deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional pre-
deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | Reinicie el proceso de GlobalProtect para que la configuración anterior a la implementación surta efecto.

STEP 5 | Después de implementar el dispositivo IoT, puede recopilar logs según sea necesario con el comando **`globalprotect collect-log`**.

```
user@raspbianhost:~/Desktop/data$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | (Opcional) Si el método de autenticación es una combinación de nombre de usuario/contraseña y autenticación de certificado de cliente, asegúrese de que el **CommonName** del certificado de cliente coincida con el nombre de usuario.

© 2020 Palo Alto Networks, Inc.

Instalación de GlobalProtect para IoT en Ubuntu

Para instalar GlobalProtect para IoT en dispositivos Ubuntu, realice los siguientes pasos.

GlobalProtect para IoT para Raspbian y Ubuntu solo admite una arquitectura basada en ARM.

STEP 1 | En el sitio de soporte, seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** y descargue el paquete de GlobalProtect para su sistema operativo.

STEP 2 | Instale la aplicación de GlobalProtect para IoT.

Desde el dispositivo IoT, use el comando **`sudo dpkg -i GlobalProtect_deb-<version>.deb`** para instalar el software.

```
user@linuxhost:~$ sudo dpkg -i GlobalProtect_deb-4.1.0.0-19.deb
```

*Para desinstalar más tarde el software, use el comando **`sudo dpkg -P globalprotect`**.*

STEP 3 | Configure los ajustes de VPN que desee implementar previamente para dispositivos Ubuntu IoT.

1. En la ruta `client-cert`, importe el certificado en formato pcks12 y guarde el archivo con una extensión .pfx (por ejemplo, **pan_client_cert.pfx**).
2. En la ruta `client-cert-passphrase`, guarde el archivo de contraseña con la extensión .dat (por ejemplo, **pan_client_cert_passcode.dat**).
3. En la ruta `log-path-service`, si no está utilizando la ruta predeterminada para PanGPS (por ejemplo, `/opt/paloaltonetworks/globalprotect`), asegúrese de que la carpeta de ruta `log-setting` tenga el mismo privilegio que la carpeta globalprotect en `opt/paloaltonetworks`.
4. Cree un archivo de configuración anterior a la implementación (`/opt/paloaltonetworks/globalprotect/pangps.xml`) en el siguiente formato y edite la dirección IP del portal de GlobalProtect y la configuración de autenticación, ya sea: nombre de usuario y contraseña, o ruta del certificado del cliente (**`client-cert-path`**) y el archivo de frase de contraseña (**`client-cert-passphrase`**). También puede especificar una carpeta opcional en la que almacenar registros del servicio de GlobalProtect (**`log-path-service`**) y logs de agente (**`log-path-agent`**).

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
         <receive-timeout>30</receive-timeout>
```


© 2020 Palo Alto Networks, Inc.

```
        <os-type>IoT</os-type>             //pre-deployed OS type for IoT.
 If this tag does not present, GP will automatic detect the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less mode
        <username>abc</username>    //optional pre-deployed username
        <password>xyz</password>       //optional pre-deployed password
        <client-cert-path>cli_cert_path</client-cert-path>       //optional
 pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase>       //optional pre-deployed client certificate passphrase file
 path
        <log-path-service>/tmp/gps</log-path-service>  //optional pre-
deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional pre-
deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | Reinicie el proceso de GlobalProtect para que la configuración anterior a la implementación surta efecto.

STEP 5 | Después de implementar el dispositivo IoT, puede recopilar logs según sea necesario con el comando **`globalprotect collect-log`**.

```
user@linuxhost:~$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | (Opcional) Si el método de autenticación es una combinación de nombre de usuario/contraseña y autenticación de certificado de cliente, asegúrese de que el **CommonName** del certificado de cliente coincida con el nombre de usuario.

© 2020 Palo Alto Networks, Inc.

Instalación de GlobalProtect para IoT en Windows

Los dispositivos que utilicen Windows 10 IoT pueden usar la aplicación de GlobalProtect. Utilice el método de distribución de su empresa, como Microsoft System Center Configuration Manager (SCCM), para implementar e instalar la aplicación de GlobalProtect en sus dispositivos IoT con Windows 10 IoT Enterprise.

Una implementación de GlobalProtect Windows IoT admite la autenticación basada en certificados. Debe instalar el certificado utilizado para la autenticación en cada dispositivo IoT en su tienda de máquinas local. Si un dispositivo IoT tiene varios certificados con la misma CA raíz, GlobalProtect usa el primer certificado del almacén de máquinas local del dispositivo IoT para autenticarse; asegúrese de que sus certificados estén en el orden correcto en sus dispositivos.

Las siguientes secciones describen cómo instalar la aplicación de GlobalProtect en dispositivos que utilizan Windows IoT:

- Descarga e instalación el archivo MSIEXEC en el dispositivo IoT
- Modificación de las claves de registro en el dispositivo IoT (On-Demand (Bajo demanda) o Always On (Siempre activado))
- Modificación de las claves de registro en el dispositivo IoT (siempre activado, anterior al inicio de sesión)

Descarga e instalación el archivo MSIEXEC en el dispositivo IoT

Puede descargar e instalar el archivo `msiexec.exe` en sus dispositivos IoT para instalar la aplicación de GlobalProtect para el método de conexión **On-Demand (Bajo demanda)** o **Always On (Siempre activado)**. Utilice el mismo método para implementar el archivo msiexec.exe como lo hace en un dispositivo que no es IoT.

Modificación de las claves de registro en el dispositivo IoT (On-Demand (Bajo demanda) o Always On (Siempre activado))

Debe especificar el tipo de sistema operativo como IoT, el tipo de dispositivo como sin periféricos y la dirección del portal. Opcionalmente, puede especificar un nombre de usuario y contraseña. Si no especifica un nombre de usuario y contraseña, GlobalProtect usará la autenticación basada en certificados.

Puede utilizar los siguientes métodos de instalación para el método de conexión **On-Demand (Bajo demanda)** o **Always On (Siempre activado)**:

- Especifique el tipo de sistema operativo (obligatorio):

  Registry subkey (Subclave de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name (Nombre): os-type

  Type (Tipo): REG_SZ

  Data (Datos): IoT
- Especifique un dispositivo IoT sin periféricos (obligatorio):

© 2020 Palo Alto Networks, Inc.

Registry subkey (Subclave de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

Name (Nombre): head-less

Type (Tipo): REG_SZ

Data (Datos): yes

- Especifique la dirección del portal (obligatorio):

  Registry subkey (Subcalbe de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Nombre: Portal

  Type (Tipo): REG_SZ

  Data (Datos): Especifique el FQDN o la dirección IP del portal de GlobalProtect.

- Introduzca el nombre de usuario (opcional):

  Registry subkey (Subclave de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name (Nombre): username

  Type (Tipo): REG_SZ

  Data (Datos): Especifique el nombre de usuario que utilizar con el dispositivo IoT.

- Especifique la contraseña (opcional):

  Registry subkey (Subclave de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name (Nombre): password

  Type (Tipo): REG_SZ

  Data (Datos): Especifique la contraseña que utilizar con el dispositivo IoT.

Modificación de las claves de registro en el dispositivo IoT (siempre activado, anterior al inicio de sesión)

Debe especificar la dirección del portal, el valor de tiempo de espera anterior al inicio de sesión y el valor de solo servicio. Debe eliminar el valor de GlobalProtect para evitar que el dispositivo IoT inicie automáticamente la interfaz de la aplicación al reiniciar el sistema. Un túnel VPN anterior al inicio de sesión no asocia el nombre de usuario porque el usuario no ha iniciado sesión.

Puede utilizar los siguientes métodos de instalación para el método de conexión **Pre-logon (Always On) (Anterior al inicio de sesión (Siempre activado))**

- Especifique la dirección del portal (obligatorio):

  Registry subkey (Subcalbe de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Nombre: Portal

  Type (Tipo): REG_SZ

  Data (Datos): Especifique el FQDN o la dirección IP del portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

- Especifique el valor anterior al inicio de sesión (obligatorio):

  Registry subkey (Subcalbe de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Nombre: Prelogon

  Type (Tipo): REG_SZ

  Data (Datos): 1
- Especifique el valor de solo servicio (obligatorio):

  Registry subkey (Subclave de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name (Nombre): service-only

  Type (Tipo): REG_SZ

  Data (Datos): yes
- Elimine el valor de GlobalProtect (obligatorio):

  Registry subkey (Subclave de registro): `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

  Nombre: GlobalProtect

  Type (Tipo): REG_SZ

© 2020 Palo Alto Networks, Inc.

Información de host

Aunque tenga una seguridad estricta en su límite de red corporativa, su red realmente solo es tan segura como los endpoints que acceden a ella: El personal actual es cada vez más móvil y con frecuencia requiere acceso a recursos corporativos desde una variedad de ubicaciones (aeropuertos, cafeterías, hoteles) y desde diferentes endpoints (personales y proporcionados por la empresa), por lo que debe ampliar la seguridad de red a sus endpoints para garantizar el cumplimiento de la seguridad integral y consistente. La función de Perfil de información de host (Host Information Profile, HIP) de GlobalProtect™ le permite recopilar información sobre el estado de seguridad de sus endpoints (por ejemplo, si tiene los últimos parches de seguridad y definiciones antivirus instaladas, si tienen el cifrado de disco habilitado, si el endpoint está descodificado o descifrado, o si se ejecuta software específico que se requiere en su organización) y toma las decisiones de permitir o rechazar el acceso a un host específico sobre la base del cumplimiento con las políticas de host que define.

Las siguientes secciones brindan detalles sobre el uso de la información del host en el cumplimiento de políticas.

- Acerca de la información del host
- Configuración de la aplicación de políticas basadas en HIP
- Recopilación de datos de procesos y aplicaciones de endpoints
- Redistribución de informes de HIP
- Bloqueo del acceso al dispositivo
- Configurar el agente de User-ID de Windows para recopilar información de host
- Dispositivos en cuarentena que utilizan información del host

© 2020 Palo Alto Networks, Inc.

Acerca de la información del host

Una de las tareas de la aplicación de GlobalProtect consiste en recopilar información acerca del host en el que se ejecuta. A continuación, la aplicación envía la información del host a la puerta de enlace de GlobalProtect tras una conexión correcta. La puerta de enlace compara esta información del host sin procesar que envía la aplicación con cualquier objeto y perfil HIP que haya definido. Si encuentra una coincidencia, genera una entrada en el log de coincidencias HIP. Asimismo, si encuentra una coincidencia con un perfil HIP en una política de reglas, aplica la correspondiente política de seguridad.

Las verificaciones de HIP se realizan cuando la aplicación se conecta a la puerta de enlace y las comprobaciones posteriores se realizan cada hora mientras el agente de GlobalProtect está conectado. El agente de GlobalProtect puede solicitar un informe HIP actualizado si la verificación de HIP anterior ha cambiado. Solo se conserva el último informe de HIP en la puerta de enlace por endpoint.

El uso de los perfiles de información del host para la aplicación de políticas posibilita una seguridad granular que garantiza que los hosts remotos que acceden a sus recursos críticos posean un mantenimiento adecuado y cumplan con sus normas de seguridad antes de que se les permita acceder a los recursos de su red. Por ejemplo, antes de permitir el acceso a los sistemas de datos más importantes, tal vez quiera asegurarse de que los hosts que acceden a los mismos tienen habilitado el cifrado en sus unidades de disco duro. Puede aplicar esta política mediante la creación de una regla de seguridad que solo permita acceder a la aplicación si el sistema del endpoint tiene habilitado el cifrado. Además, en el caso de endpoints que no cumplan esta regla, puede crear un mensaje de notificación que alerte a los usuarios del motivo por el cual se les deniega el acceso y los redirija al recurso compartido de archivos, donde podrán acceder al programa de instalación del software de cifrado que les falta (evidentemente, para permitir al usuario acceder a dicho recurso compartido, debe crear la correspondiente regla de seguridad que permita acceder al recurso compartido a los hosts que coincidan con un perfil HIP concreto).

- ¿Qué datos recopila la aplicación de GlobalProtect?
- ¿Qué datos recopila la aplicación de GlobalProtect en cada sistema operativo?
- Cómo usa la puerta de enlace la información del host para aplicar las políticas
- ¿Cómo pueden saber los usuarios si sus sistemas cumplen los requisitos?
- ¿Cómo puedo consultar el estado de los endpoints?

¿Qué datos recopila la aplicación de GlobalProtect?

Por defecto, la aplicación de GlobalProtect recopila datos específicos del proveedor relativos a los paquetes de seguridad del usuario final que se ejecutan en el endpoint (según la compilación del programa de asociación global OPSWAT) y remite estos datos a la puerta de enlace de GlobalProtect para que se usen en la aplicación de la política. Consulte la tabla GlobalProtect OPSWAT Support (Soporte de OPSWAT de GlobalProtect) para obtener detalles sobre los productos de terceros que GlobalProtect puede detectar mediante el SDK de OPSWAT especificado.

Puesto que el software de seguridad debe evolucionar continuamente para garantizar la protección del usuario final, las licencias de puerta de enlace de GlobalProtect también le permiten recibir actualizaciones dinámicas del archivo de datos de GlobalProtect con los parches y las versiones de software más recientes disponibles para cada paquete.

Por defecto, la aplicación recopila datos acerca de las siguientes categorías de información para ayudarlo a identificar el estado de seguridad del host.

© 2020 Palo Alto Networks, Inc.

Table 8: Tabla: Categorías de recopilación de datos

Category	Datos recopilados
General	Información acerca del propio host, incluido el nombre del host, el dominio de inicio de sesión, el sistema operativo, la versión de la aplicación y, para sistemas Windows, el dominio al que pertenece el equipo. *Para el dominio de endpoints de Windows, la aplicación de GlobalProtect recopila el dominio definido para `ComputerNameDnsDomain`, que es el dominio DNS asignado al ordenador local o el clúster asociado al equipo local. Esta información se muestra para el Domain (Dominio) de endpoints de Windows en los detalles de registro de Coincidencias HIP (Monitor [Supervisar] > Logs [Registros] > HIP Match [Coincidencia HIP]).*
Dispositivo móvil	Información sobre el dispositivo móvil, incluido el nombre del dispositivo, el dominio de inicio de sesión, el sistema operativo, la versión de la aplicación y la información de la red a la que está conectado el dispositivo. Además, GlobalProtect recopila información de si el dispositivo está modificado o bloqueado. *Para recopilar atributos de dispositivos móviles y utilizarlos en políticas de aplicación de HIP, GlobalProtect requiere un servidor MDM. Actualmente, GlobalProtect admite la integración de HIP con el servidor MDM de AirWatch.* Para los dispositivos administrados por AirWatch, la información de host recopilada por la aplicación GlobalProtect se puede complementar con información adicional recopilada del servicio AirWatch. Consulte Configuración del agente de User-ID de Windows para recopilar información de host para obtener una lista de atributos que puede recuperarse de AirWatch.
Administración de parches	Información acerca de cualquier software de administración de parches habilitado o instalado en el host e información de cualquier parche que falte. *Si desea configurar el valor Severity (Gravedad) para los parches que faltan como una condición de coincidencia en su objeto HIP (Objects (Objetos) > GlobalProtect > HIP Objects (Objetos HIP) > <hip-object> > Patch Management (Gestión de parches) > Criteria (Criterios)), use las siguientes asignaciones entre los valores de gravedad de GlobalProtect y las calificaciones de gravedad de OPSWAT para comprender qué significa cada valor:* • ***0**—Low (Bajo)* • ***1**—Moderate (Moderado)*

© 2020 Palo Alto Networks, Inc.

Category	Datos recopilados
	• ***2**—Important (Importante)* • ***3**—Critical (Crítico)*
Rendimiento	Información acerca de cualquier cortafuegos instalado o habilitado en el host.
Antimalware	Información acerca del software antivirus o antispyware habilitado o instalado en el endpoint, si está habilitada o no la protección en tiempo real, la versión de definición de virus, la hora del último análisis, el proveedor y el nombre del producto. GlobalProtect utiliza la tecnología OPSWAT para detectar y evaluar aplicaciones de seguridad de terceros en el endpoint. Al integrarse con el marco OPSWAT OESIS, GlobalProtect le permite evaluar el estado de cumplimiento del endpoint. Por ejemplo, puede definir los objetos HIP y perfiles HIP que verifican la presencia de una versión específica del software antivirus de un proveedor específico en el endpoint y también garantiza que tenga los archivos de definición de virus más recientes. *OPSWAT no puede detectar la siguiente información de **Anti-Malware** para la función de seguridad Gatekeeper en endpoints de macOS:* • *Versión del motor* • *Versión de definición* • *Fecha* • *Último análisis*
Copia de seguridad de disco	Información de si está instalado el software de copia de seguridad del disco, la hora de la última copia de seguridad y el proveedor y el nombre de producto del software.
Cifrado de disco	Información acerca de si está instalado el software de cifrado del disco, las unidades o rutas configuradas para el cifrado y el proveedor y el nombre de producto del software.
Prevención de pérdida de datos	Información acerca de si está instalado o no el software de prevención de pérdida de datos (data loss prevention, DLP) para evitar que la información corporativa confidencial salga de la red o se almacene en un dispositivo potencialmente inseguro. Esta información solo se recopila de endpoints de Windows.
Certificado	Información sobre el certificado de equipo instalado en el terminal.
Comprobaciones personalizadas	Información sobre si están presentes claves del registro (solo en Windows), listas de propiedades (plists, solo en macOS) o bien procesos del sistema operativo y de las aplicaciones del espacio de usuarios concretos.

© 2020 Palo Alto Networks, Inc.

Puede excluir la recopilación de ciertas categorías de información en determinados hosts para evitar ciclos de CPU y mejorar el tiempo de respuesta. Para hacerlo, cree una configuración de agente en el portal y, luego, excluya las categorías en las que no esté interesado (**Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **Data Collection (Recopilación de datos)**). Por ejemplo, si no pretende crear políticas basadas en si los endpoints ejecutan software para la copia de seguridad del disco o no, puede excluir esa categoría para evitar que la aplicación recopile información sobre la copia de seguridad de disco.

También puede excluir información de la recopilación en endpoints personales a fin de brindarle privacidad al usuario. Por ejemplo, puede excluir la lista de aplicaciones instaladas en endpoints que no están gestionadas por el gestor de seguridad móvil externo.

¿Qué datos recopila la aplicación de GlobalProtect en cada sistema operativo?

La aplicación de GlobalProtect recopila datos para ayudar a identificar o recuperar el perfil de información del host (HIP, Host Information Profile) para el dispositivo para su uso en HIP-based policy enforcement (Aplicación de políticas basadas en HIP).

- ¿Qué datos recopila la aplicación de GlobalProtect en Windows?
- ¿Qué datos recopila la aplicación de GlobalProtect en macOS?
- ¿Qué datos recopila la aplicación de GlobalProtect en Windows UWP?
- ¿Qué datos recopila la aplicación de GlobalProtect en Android?
- ¿Qué datos recopila la aplicación de GlobalProtect en iOS?
- ¿Qué datos recopila la aplicación de GlobalProtect en Linux?

¿Qué datos recopila la aplicación de GlobalProtect en Windows?

La siguiente tabla describe los datos recopilados por la aplicación de GlobalProtect en dispositivos Windows para la aplicación de políticas basadas en HIP generadas por el cortafuegos:

Atributo de informes de HIP	Description (Descripción)
Report Generation Time (Hora de generación del informe)	Fecha y hora en que se generó el informe HIP.
Nombre de usuario	Nombre de usuario que se utiliza para iniciar sesión en la VPN.
User IP Address (Dirección IP de usuario)	Dirección IP del dispositivo Windows de los usuarios.
Machine Name (Nombre de la máquina)	Nombre de host y número de serie del dispositivo Windows.
Dominio	El campo está vacío en los dispositivos Windows.
SO	Nombre de la aplicación y nombre del proveedor del sistema operativo de destino.
ID de host	ID de host único asignado por GlobalProtect para identificar el host. El valor de ID de host es el GUID de la máquina en los dispositivos Windows. El GUID de la máquina se almacena en el Registro de

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
	Windows (HKEY_Local_Machine\Software\Microsoft\Cryptography \MachineGuid).
Versión de cliente	Número de versión de la aplicación de GlobalProtect instalada actualmente.
Network interface (Interfaz de red)	Se identifican las siguientes configuraciones para la interfaz de red: • **Interface (Interfaz)**: tipo de interfaz de red detectada en el dispositivo Windows. • **MAC Address (Dirección MAC)**: la dirección MAC es el identificador de hardware exclusivo asignado a cada interfaz de red en el dispositivo Windows. • **IP Address (Dirección IP)**: dirección IP asignada a cada interfaz de red en el dispositivo Windows.
Antimalware	Información sobre cualquier antivirus o antispyware que esté habilitado o instalado en el dispositivo, si la protección antivirus o antispyware en tiempo real está habilitada en el host, la versión de la definición de virus, la última hora de escaneo y el nombre del proveedor y del producto.
Copia de seguridad de disco	Información sobre el estado de la copia de seguridad del disco del dispositivo, como si el software de copia de seguridad del disco está instalado en el host, la hora de la última copia de seguridad y el nombre del proveedor y del producto del software.
Cifrado de disco	Información sobre el estado de cifrado del disco del dispositivo, como si el software de cifrado del disco está instalado en el host, la unidad o la ruta para verificar el cifrado del disco para determinar una coincidencia, el estado de la ubicación cifrada y el proveedor y el nombre del producto del software.
Administración de parches	Información sobre cualquier software de gestión de parches que esté instalado o habilitado en el host y si el host detectó parches que faltan y el valor de gravedad especificado. Consulte la categoría Patch Management (Gestión de parches) para obtener detalles sobre cada valor.
Rendimiento	Información sobre si el software del cortafuegos está habilitado o instalado en el host.
Prevención de pérdida de datos	Información sobre el estado del software de prevención de pérdida de datos (DLP, Data Loss Prevention) en los dispositivos Windows para evitar que la información corporativa salga de la red corporativa o se almacene en un dispositivo potencialmente inseguro.
Comprobaciones personalizadas	Información sobre el Registro de Windows recopilada por la aplicación de GlobalProtect de dispositivos Windows. Puede habilitar comprobaciones personalizadas para recopilar datos de dispositivos Windows para indicar a la aplicación que recopile información de registro específica (claves de registro y valores de clave de registro). El tipo de información recopilada puede incluir si una aplicación está

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
	instalada en el dispositivo, o atributos o propiedades específicas de esa aplicación.

¿Qué datos recopila la aplicación de GlobalProtect en macOS?

La siguiente tabla describe los datos recopilados por la aplicación de GlobalProtect en dispositivos macOS para la aplicación de políticas basadas en HIP generadas por el cortafuegos:

Atributo de informes de HIP	Description (Descripción)
Report Generation Time (Hora de generación del informe)	Fecha y hora en que se generó el informe HIP.
Nombre de usuario	Nombre de usuario que se utiliza para iniciar sesión en la VPN.
User IP Address (Dirección IP de usuario)	Dirección IP del dispositivo macOS de los usuarios.
Machine Name (Nombre de la máquina)	Nombre de host y número de serie del dispositivo macOS.
Dominio	El campo está vacío en dispositivos macOS.
SO	Nombre de la aplicación y nombre del proveedor del sistema operativo de destino.
ID de host	ID de host único asignado por GlobalProtect para identificar el host. El valor de ID de host es la dirección MAC de la primera interfaz física incorporada.
Versión de cliente	Número de versión de la aplicación de GlobalProtect instalada actualmente.
Network interface (Interfaz de red)	Se identifican las siguientes configuraciones para la interfaz de red: • **Interface (Interfaz)**: tipo de interfaz de red detectada en el dispositivo macOS. • **MAC Address (Dirección MAC)**: la dirección MAC es el identificador de hardware único asignado a cada interfaz de red en el dispositivo macOS. • **IP Address (Dirección IP)**: dirección IP asignada a cada interfaz de red en el dispositivo macOS.
Antimalware	Información sobre cualquier antivirus o antispyware que esté habilitado o instalado en el dispositivo, si la protección antivirus o antispyware en tiempo real está habilitada en el host, la versión de la definición de virus, la última hora de escaneo y el nombre del proveedor y del producto.
Copia de seguridad de disco	Información sobre el estado de la copia de seguridad del disco del dispositivo, como si el software de copia de seguridad del disco está

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
	instalado en el host, la hora de la última copia de seguridad y el nombre del proveedor y del producto del software.
Cifrado de disco	Información sobre el estado de cifrado del disco del dispositivo, como si el software de cifrado del disco está instalado en el host, la unidad o la ruta para verificar el cifrado del disco para determinar una coincidencia, el estado de la ubicación cifrada y el proveedor y el nombre del producto del software.
Administración de parches	Información sobre cualquier software de gestión de parches que esté instalado o habilitado en el host y si el host detectó parches que faltan y el valor de gravedad especificado. Consulte la categoría Patch Management (Gestión de parches) para obtener detalles sobre cada valor.
Rendimiento	Información sobre si el software del cortafuegos está habilitado o instalado en el host.
Comprobaciones personalizadas	Información sobre la lista de propiedades de macOS (plist) recopilada por la aplicación de GlobalProtect de los dispositivos macOS. Puede habilitar verificaciones personalizadas para recopilar datos de dispositivos macOS para indicar a la aplicación que recopile información plist específica (claves plist y plist). El tipo de información recopilada puede incluir si una aplicación está instalada en el dispositivo, o atributos o propiedades específicas de esa aplicación.

¿Qué datos recopila la aplicación de GlobalProtect en Windows UWP?

La siguiente tabla describe los datos recopilados por la aplicación de GlobalProtect en dispositivos Windows UWP para la aplicación de políticas basadas en HIP generadas por el cortafuegos:

Atributo de informes de HIP	Description (Descripción)
Report Generation Time (Hora de generación del informe)	Fecha y hora en que se generó el informe HIP.
Nombre de usuario	Nombre de usuario que se utiliza para iniciar sesión en la VPN.
User IP Address (Dirección IP de usuario)	Dirección IP del dispositivo Windows UWP de los usuarios.
Machine Name (Nombre de la máquina)	Nombre de host y número de serie del dispositivo Windows UWP.
Dominio	El campo está vacío en los dispositivos Windows UWP.
SO	Nombre de la aplicación y nombre del proveedor del sistema operativo de destino.

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
ID de host	ID de host único asignado por GlobalProtect para identificar el host. El valor de ID de host es el GUID en los dispositivos Windows UWP.
Versión de cliente	Número de versión de la aplicación de GlobalProtect instalada actualmente.
Network interface (Interfaz de red)	Se identifican las siguientes configuraciones para la interfaz de red: • **Interface (Interfaz)**: tipo de interfaz de red detectada en el dispositivo Windows UWP. • **MAC Address (Dirección MAC)**: la dirección MAC es el identificador de hardware exclusivo asignado a cada interfaz de red en el dispositivo Windows UWP. • **IP Address (Dirección IP)**: dirección IP asignada a cada interfaz de red en el dispositivo Windows UWP.

¿Qué datos recopila la aplicación de GlobalProtect en Android?

La siguiente tabla describe los datos recopilados por la aplicación de GlobalProtect en dispositivos Android para la aplicación de políticas basadas en HIP generadas por el cortafuegos:

La aplicación de GlobalProtect para Android en un Chromebook usa los mismos atributos de informe HIP.

Atributo de informes de HIP	Description (Descripción)
Report Generation Time (Hora de generación del informe)	Fecha y hora en que se generó el informe HIP.
Nombre de usuario	Nombre de usuario que se utiliza para iniciar sesión en la VPN.
User IP Address (Dirección IP de usuario)	Dirección IP del dispositivo Android de los usuarios.
Machine Name (Nombre de la máquina)	Nombre de host y número de serie del dispositivo Android.
Dominio	El campo está vacío en dispositivos Android.
Número de serie	Número de serie del dispositivo Android.
Gestionado	Valor que indica si se trata de un dispositivo Android gestionado: Si este valor se establece en **Yes (Sí)**, el dispositivo está gestionado. Si este valor se establece en **No**, el dispositivo no está gestionado.
SO	Nombre de la aplicación y nombre del proveedor del sistema operativo de destino.

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
ID de host	GlobalProtect asigna cadenas alfanuméricas únicas de 16 caracteres para identificar el host. El valor del ID de host es el ID de Android en los dispositivos Android.
Versión de cliente	Número de versión de la aplicación de GlobalProtect instalada actualmente.
WiFi SSID (SSID de WiFi)	Información específica sobre la conectividad de la red, como **WiFi SSID (SSID de WiFi)** en el dispositivo Android.
Network interface (Interfaz de red)	Se identifican las siguientes configuraciones para la interfaz de red: • **Interface (Interfaz)**: tipo de interfaz de red detectada en el dispositivo Android. • **MAC Address (Dirección MAC)**: la dirección MAC es el identificador de hardware único asignado a cada interfaz de red en el dispositivo Android. • **IP Address (Dirección IP)**: dirección IP asignada a cada interfaz de red en el dispositivo Android.
Dispositivo móvil	Información sobre el dispositivo móvil, incluido el nombre del dispositivo, el dominio de inicio de sesión, el sistema operativo, la versión de la aplicación y a red a la que está conectado el dispositivo.
Etiquetas	Etiquetas que le permiten cotejar con otros atributos basados en MDM.
Device Compliance (Cumplimiento del dispositivo)	El atributo **Rooted/Jailbroken** se utiliza para determinar el estado de cumplimiento del dispositivo Android que se ha rooteado o liberado para obtener privilegios administrativos. Las políticas de seguridad se pueden eliminar u omitir en el sistema operativo desde un dispositivo en riesgo.
MDM Attributes (Atributos de MDM)	Cuando integra su implementación de GlobalProtect con un proveedor de MDM, la aplicación de GlobalProtect para dispositivos Android puede obtener los siguientes atributos de datos y etiquetas del sistema MDM: • **udid**: identificador de dispositivo único (UDID, Unique Device Identifier) del dispositivo Android. • **managed-by-mdm**: valor que indica si el dispositivo Android está gestionado. Si este valor se establece en **Yes (Sí)**, el dispositivo Android está gestionado. Si este valor se establece en **No**, el dispositivo Android no está gestionado. • **tag**: etiquetas que le permiten cotejar con otros atributos basados en MDM. • **compliance (cumplimiento)**: estado de cumplimiento que indica si el dispositivo Android cumple con las políticas de cumplimiento que ha definido. • **ownership**: categoría de propiedad del dispositivo Android, por ejemplo, **Employee Owned (Propiedad del empleado)**. Este valor se anexa al atributo **Tag (Etiqueta)** del informe de HIP.

© 2020 Palo Alto Networks, Inc.

¿Qué datos recopila la aplicación de GlobalProtect en iOS?

La siguiente tabla describe los datos recopilados por la aplicación de GlobalProtect en dispositivos iOS para la aplicación de políticas basadas en HIP generadas por el cortafuegos:

Atributo de informes de HIP	Description (Descripción)
Report Generation Time (Hora de generación del informe)	Fecha y hora en que se generó el informe HIP.
Nombre de usuario	Nombre de usuario que se utiliza para iniciar sesión en la VPN.
User IP Address (Dirección IP de usuario)	Dirección IP del dispositivo iOS de los usuarios.
Machine Name (Nombre de la máquina)	Nombre de host y número de serie del dispositivo iOS.
Dominio	El campo está vacío en dispositivos iOS.
Número de serie	El campo está vacío en el dispositivo iOS.
Gestionado	Valor que indica si se trata de un dispositivo iOS gestionado: Si este valor se establece en **Yes (Sí)**, el dispositivo está gestionado. Si este valor se establece en **No**, el dispositivo no está gestionado.
SO	Nombre de la aplicación y nombre del proveedor del sistema operativo de destino.
ID de host	ID único asignado por GlobalProtect para identificar el host. El valor de ID de host es UDID en dispositivos iOS.
Versión de cliente	Número de versión de la aplicación de GlobalProtect instalada actualmente.
WiFi SSID (SSID de WiFi)	Información sobre la conectividad de la red, como **WiFi SSID (SSID de WiFi)** en el dispositivo iOS.
Network interface (Interfaz de red)	Se identifican las siguientes configuraciones para la interfaz de red: • **Interface (Interfaz)**: tipo de interfaz de red detectada en el dispositivo iOS. • **MAC Address (Dirección MAC)**: la dirección MAC es el identificador de hardware único asignado a cada interfaz de red en el dispositivo iOS. • **IP Address (Dirección IP)**: dirección IP asignada a cada interfaz de red en el dispositivo iOS.
Dispositivo móvil	Información sobre el dispositivo móvil, incluido el nombre del dispositivo, el dominio de inicio de sesión, el sistema operativo, la versión de la aplicación y a red a la que está conectado el dispositivo.
Device Compliance (Cumplimiento del dispositivo)	Los siguientes atributos se utilizan para determinar el estado de cumplimiento del dispositivo iOS:

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
	• **Rooted/Jailbroken (Con root/jailbreak)**: estado en el dispositivo iOS que se ha rooteado o liberado para obtener privilegios administrativos. Las políticas de seguridad se pueden eliminar u omitir en el sistema operativo desde un dispositivo en riesgo. • **Disk Encryption Not Set (Cifrado de disco no establecido)**: estado en el dispositivo iOS que está habilitado para el cifrado de disco. • **Passcode Not Set (Código de acceso no establecido)**: estado en el dispositivo iOS que está establecido en un código de acceso. • **Has Malware (Con malware)**: estado en el dispositivo iOS que tiene instaladas aplicaciones infectadas con malware.
MDM Attributes (Atributos de MDM)	Cuando integra su implementación de GlobalProtect con un proveedor de MDM, la aplicación de GlobalProtect para dispositivos iOS puede obtener los siguientes atributos de datos y etiquetas del sistema MDM: • **udid**: identificador de dispositivo único (UDID, Unique Device Identifier) del dispositivo iOS. • **managed-by-mdm**: valor que indica si el dispositivo iOS está gestionado. Si este valor se establece en **Yes (Sí)**, el dispositivo iOS está gestionado. Si este valor se establece en **No**, el dispositivo iOS no está gestionado. • **tag**: etiquetas que le permiten cotejar con otros atributos basados en MDM. • **compliance (cumplimiento)**: estado de cumplimiento que indica si el dispositivo iOS cumple con las políticas de cumplimiento que ha definido. • **ownership (propietario)**: categoría de propiedad del dispositivo iOS, por ejemplo, **Employee Owned (Propiedad del empleado)**. Este valor se anexa al atributo **Tag (Etiqueta)** del informe de HIP.

¿Qué datos recopila la aplicación de GlobalProtect en Linux?

La siguiente tabla describe los datos recopilados por la aplicación de GlobalProtect en dispositivos Linux para la aplicación de políticas basadas en HIP generadas por el cortafuegos en formato XML:

Atributo de informes de HIP	Description (Descripción)
`user-name`	Nombre de usuario que se utiliza para iniciar sesión en la VPN.
`dirección-ip`	Dirección IP del dispositivo Linux de los usuarios.
`generate-time (fecha/hora de generación)`	Fecha y hora en que se generó el informe HIP.
`host-info`	Las siguientes opciones están activadas para configurar la información del host: • `managed (gestionado)`: valor que indica si el dispositivo Linux está gestionado. Si este valor se establece en **Yes (Sí)**, el dispositivo está gestionado. Si este valor se establece en **No**, el dispositivo no está gestionado.

© 2020 Palo Alto Networks, Inc.

Atributo de informes de HIP	Description (Descripción)
	• `serial-number (número de serie)`: número de serie del dispositivo Linux. • `client-version (versión de cliente)`: número de versión de la aplicación de GlobalProtect instalada actualmente. • `os (so)`: nombre de la aplicación del sistema operativo de destino. • `os-vendor (proveedor de so)`: nombre del proveedor del sistema operativo de destino. • `domain (dominio)`: nombre de dominio del dispositivo Linux. • `host-name (nombre de host)`: nombre de host del dispositivo Linux. • `host-idD (ID de host)`: ID único asignado por GlobalProtect para identificar el host. El valor de ID de host es Product UDID (UDID de producto) en dispositivos Linux.
`network-interface`	Se identifican las siguientes configuraciones para la interfaz de red: • `interface (interfaz)`: tipo de interfaz de red detectada en el dispositivo Linux. • `mac-address (dirección MAC)`: la dirección MAC es el identificador de hardware único asignado a cada interfaz de red en el dispositivo iOS. • `Ip-address (dirección IP)`: dirección IP asignada a cada interfaz de red en el dispositivo Linux.
`anti-malware`	Información sobre cualquier antivirus o antispyware que esté habilitado o instalado en el dispositivo, si la protección antivirus o antispyware en tiempo real está habilitada en el host, la versión de la definición de virus, la última hora de escaneo y el nombre del proveedor y del producto.
`disk-backup`	Información sobre el estado de la copia de seguridad del disco del dispositivo, como si el software de copia de seguridad del disco está instalado en el host, la hora de la última copia de seguridad y el nombre del proveedor y del producto del software.
`disk-encryption`	Información sobre el estado de cifrado del disco del dispositivo, como si el software de cifrado del disco está instalado en el host, la unidad o la ruta para verificar el cifrado del disco para determinar una coincidencia, el estado de la ubicación cifrada y el proveedor y el nombre del producto del software.
`cortafuegos`	Información sobre si el software del cortafuegos está habilitado o instalado en el host.
`patch-management`	Información sobre cualquier software de gestión de parches que esté instalado o habilitado en el host y si el host detectó parches que faltan y el valor de gravedad especificado. Consulte la categoría Patch Management (Gestión de parches) para obtener detalles sobre cada valor.

© 2020 Palo Alto Networks, Inc.

Cómo usa la puerta de enlace la información del host para aplicar las políticas

Mientras la aplicación obtiene información acerca de la información que debe recopilar de la configuración del cliente descargada desde el portal, puede definir qué atributos del host le interesa supervisar o usar para la aplicación de la política mediante la creación de objetos HIP y perfiles HIP en las puertas de enlace:

- **Objetos HIP**: los criterios de coincidencia utilizados para filtrar la información de host que está interesado en usar para aplicar la política a partir de los datos sin formato informados por la aplicación. Por ejemplo, aunque los datos sin procesar del host pueden incluir información sobre varios paquetes antivirus instalados en el endpoint, puede que solo esté interesado en una aplicación concreta que necesite en su organización. En este caso, crearía un objeto HIP que coincidiera la aplicación específica que está interesado en aplicar.

  La mejor forma de determinar qué objetos HIP necesita es determinar cómo utilizará la información de host que recopila para aplicar la política. Tenga en cuenta que los objetos HIP son solo los ladrillos que le permiten crear los perfiles HIP que se utilizan en sus políticas de seguridad. Por lo tanto, es posible que desee mantener la sencillez de sus objetos, de forma que solo coincidan con un elemento, como la presencia de un tipo concreto de software necesario, la pertenencia a un dominio específico o la presencia del SO de un endpoint determinado. De este modo, tendrá la flexibilidad de crear una política aumentada HIP muy granular (y muy potente).
- **Perfiles HIP**: una colección de objetos HIP que deben evaluarse en conjunto, para supervisión o para la aplicación de políticas de seguridad. Cuando crea sus perfiles HIP, puede combinar objetos HIP que haya creado previamente (así como otros perfiles HIP) con lógica booleana, como la que se usa cuando un flujo de tráfico se evalúa con respecto del perfil HIP resultante con el que tiene o no coincidencias. Si existe una coincidencia, se aplica la regla de la política correspondiente. Si no hay coincidencias, el flujo se evalúa con respecto de la siguiente regla, como con cualquier otro criterio de coincidencia de política.

A diferencia de un registro de tráfico, que solo crea una entrada de registro si hay una coincidencia de política, el registro de coincidencias HIP genera una entrada siempre que los datos sin procesar enviados por una aplicación coincidan con un objeto HIP o un perfil HIP que haya definido. Por este motivo, el registro de coincidencias HIP es un buen recurso para supervisar el estado de los endpoints de su red a lo largo del tiempo, antes de adjuntar sus perfiles HIP a políticas de seguridad, para ayudarlo a determinar exactamente qué políticas cree que necesitan aplicarse. Consulte Configuración de la aplicación de políticas basadas en HIP para obtener información sobre cómo crear objetos HIP y perfiles HIP, y usarlos como criterio de coincidencia de políticas.

¿Cómo pueden saber los usuarios si sus sistemas cumplen los requisitos?

Por defecto, los usuarios finales no reciben información acerca de decisiones de políticas tomadas como consecuencia de la aplicación de una regla de seguridad HIP. Sin embargo, puede habilitar esta funcionalidad al configurar que se muestren mensajes de notificación HIP cuando un perfil HIP concreto coincida o no.

La decisión de cuándo mostrar un mensaje (es decir, si aparece cuando la configuración del usuario coincide con un perfil HIP en la política o cuando no coincide), depende en gran medida de su política y de lo que el usuario entiende por coincidencia (o no coincidencia) de HIP. Es decir, ¿significa la coincidencia que se concede total acceso a los recursos de su red? ¿O significa que tiene acceso limitado debido a un problema de incumplimiento?

Por ejemplo, imagínese estas situaciones:

- Crea un perfil HIP que coincide si el antivirus requerido por la empresa y los paquetes de software antispyware *no* están instalados. En este caso, tal vez quiera crear un mensaje de notificación HIP para los usuarios que coincidan con el perfil HIP y que les indique que necesitan instalar el software (y, de

© 2020 Palo Alto Networks, Inc.

manera opcional, les proporcione un enlace al recurso compartido de archivos, donde podrán acceder al instalador del software correspondiente).

- Cree un perfil HIP que coincida si estas mismas aplicaciones *están* instaladas. En este caso, quizás quiera crear el mensaje para usuarios que no coincidan con el perfil y dirigirlos a la ubicación del paquete de instalación.

Consulte Configuración de la aplicación de políticas basadas en HIP para obtener información sobre cómo crear objetos HIP y perfiles HIP, y usarlos en la definición de mensajes de notificación HIP.

¿Cómo puedo consultar el estado de los endpoints?

Siempre que un endpoint se conecta a GlobalProtect, la aplicación presenta sus datos HIP a la puerta de enlace. A continuación, la puerta de enlace usa estos datos para determinar qué objetos o perfiles HIP coinciden con el host. Para cada coincidencia, genera una entrada de log de coincidencias HIP. A diferencia de un registro de tráfico, que solo crea una entrada de registro si hay una coincidencia de política, el registro de coincidencias HIP genera una entrada siempre que los datos sin procesar enviados por una aplicación coincidan con un objeto HIP o un perfil HIP que haya definido. Por este motivo, el registro de coincidencias HIP es un buen recurso para supervisar el estado de los endpoints de su red a lo largo del tiempo, antes de adjuntar sus perfiles HIP a políticas de seguridad, para ayudarlo a determinar exactamente qué políticas cree que necesitan aplicarse.

Dado que solo se genera un registro de coincidencias HIP cuando el estado del host coincide con un objeto HIP que ha creado, para conocer completamente el estado del endpoint debe crear varios objetos HIP para generar registros de coincidencias HIP de los endpoints que cumplen con un estado particular (con fines de aplicación de políticas de seguridad) así como endpoints que no cumplen (por motivos de visibilidad). Por ejemplo, supongamos que quiere evitar que un endpoint que no tiene instalado ningún software antivirus o antispyware se conecte a la red. En este caso, debería crear un objeto HIP que coincida con hosts que tengan un software antivirus o antispyware concreto instalado. Al incluir este objeto en un perfil HIP y adjuntarlo a la regla de política de seguridad que permite acceder desde su zona VPN, puede asegurarse de que solo puedan conectarse los hosts protegidos por software antivirus o antispyware.

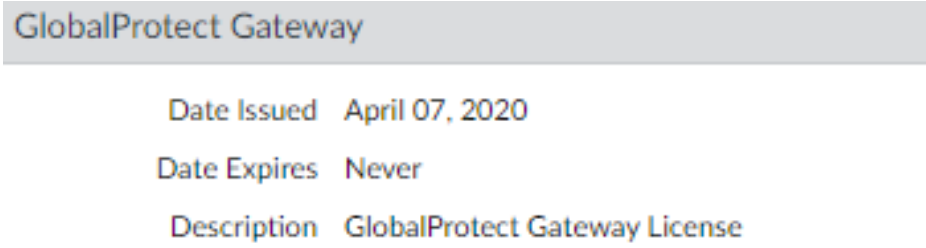
En este ejemplo, no podrá ver qué endpoints no cumplen con este requisito en el registro de coincidencia HIP. Si quiere ver también un registro de endpoints que no tienen software antivirus o antispyware instalado para poder hacer un seguimiento de estos usuarios, debe crear un objeto HIP que coincida con la condición de que no haya software antivirus ni antispyware instalados. Dado que este objeto solo es necesario para el inicio de sesión, no necesita añadirlo a un perfil HIP ni adjuntarlo a una regla de política de seguridad.

© 2020 Palo Alto Networks, Inc.

Configuración de la aplicación de políticas basadas en HIP

Para habilitar el uso de la información del host en la aplicación de políticas, debe seguir estos pasos. Para obtener más información sobre la función HIP, consulte Acerca de la información del host. Consulte ¿Qué datos recopila la aplicación de GlobalProtect en cada sistema operativo? para obtener más detalles sobre los datos que se recopilan para el dispositivo.

STEP 1 | Verifique que las comprobaciones HIP tienen la licencia adecuada.



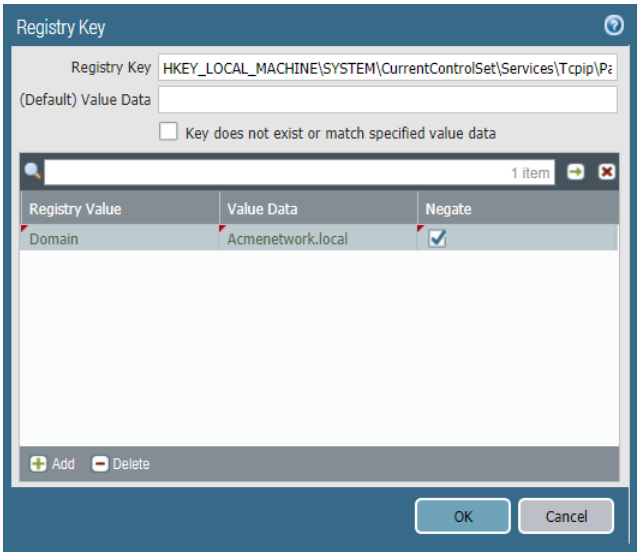
Para usar la función HIP, debe comprar e instalar una licencia de suscripción de GlobalProtect en cada puerta de enlace que vaya a realizar comprobaciones de HIP. Para verificar el estado de sus licencias en cada portal y puerta de enlace, seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.

Póngase en contacto con su ingeniero de ventas o distribuidor de Palo Alto Networks si no tiene todas las licencias necesarias. Si desea obtener más información sobre licencias, consulte Acerca de las licencias de GlobalProtect.

STEP 2 | (Opcional) Defina cualquier información de host personalizada que desee que recopile la aplicación. Por ejemplo, si tiene aplicaciones necesarias que no estén incluidas en la lista de productos o de proveedores para crear objetos HIP, puede crear una comprobación personalizada que le permita determinar si se instaló esa aplicación (tiene un registro o clave plist correspondiente) o se está ejecutando (tiene un proceso en ejecución correspondiente).

Tanto el paso 2 como el 3 dan por hecho que usted ya configuró un portal de GlobalProtect. Si aún no ha configurado su portal, consulte las instrucciones en Configuración del acceso al portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.



1. En el cortafuegos donde se aloja su portal de GlobalProtect, seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione la configuración del portal que desea modificar.
3. En la pestaña **Agent (Agente)**, seleccione la configuración del agente a la que desea añadirle una comprobación HIP personalizada o haga clic en **Add (Añadir)** para añadir una nueva.
4. Seleccione **HIP Data Collection (Recopilación de datos HIP)** y habilite la opción **Collect HIP Data (Recopilar datos de HIP)**.
5. En **Custom Checks (Comprobaciones personalizadas)**, defina los siguientes datos que desea recopilar de los hosts que ejecutan esta configuración de agente:
   - **Para recopilar información acerca de claves de registro específicas**: En la pestaña **Windows**, seleccione **Add (Añadir)** para añadir el nombre de una clave de registro en **Registry Key (Clave de registro)** para la cual desea recopilar datos en el área **Registry Key (Clave de registro)**. Para limitar la recopilación de datos a un **Registry Value (Valor de registro)** específico, seleccione **Add (Añadir)** y luego defina los valores de registro específicos. Haga clic en **OK (Aceptar)** para guardar los ajustes.
   - **Para recopilar información acerca de los procesos en ejecución**: Seleccione la pestaña correspondiente (**Windows** o **Mac**) y luego **Add (Añadir)** para añadir un proceso a la **Process List (Lista de procesos)**. Introduzca el nombre del proceso del que quiere que la aplicación recopile información.
   - **Para recopilar información acerca de listas de propiedades específicas**: En la pestaña **Mac**, haga clic en **Add (Añadir)** para añadir la **Plist** para la cual recopilar datos. Para limitar la recopilación de datos a valores de clave específicos, haga clic en **Add (Añadir)** para añadir valores de **Key (Clave)**. Haga clic en **OK (Aceptar)** para guardar los ajustes.
6. Si se trata de una nueva configuración de agente, defina las configuraciones de agente de GlobalProtect según sus necesidades.
7. Haga clic en **OK (Aceptar)** para guardar la configuración.
8. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 3 | (Opcional) Excluya categorías de la recopilación.

1. En el cortafuegos donde se aloja su portal de GlobalProtect, seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione la configuración del portal que desea modificar.
3. En la pestaña **Agent (Agente)**, seleccione la configuración del agente desde la cual desea excluir categorías o haga clic en **Add (Añadir)** para añadir una nueva.

© 2020 Palo Alto Networks, Inc.

4. Seleccione **Data Collection (Recolección de datos)** y luego verifique que **Collect HIP Data (Recolectar datos HIP)** esté habilitado.
5. En **Exclude Categories (Excluir categorías)**, haga clic en **Add (Añadir)** para añadir una categoría de exclusión nueva.
6. En **Category (Categoría)**, seleccione la categoría que desea excluir de la lista desplegable.
7. (Opcional) Si desea excluir proveedores o productos específicos dentro de la categoría seleccionada en lugar de excluir toda la categoría, haga clic en **Add (Añadir)**. En el cuadro de diálogo Edit Vendor (Editar proveedor), seleccione el **Vendor (Proveedor)** que desea excluir y, luego, haga clic en **Add (Añadir)** para excluir productos específicos de ese proveedor. Cuando haya terminado de definir a dicho proveedor, haga clic en **OK (Aceptar)**. Puede añadir a varios proveedores y productos a la lista de exclusión.
8. Repita del paso 5 al 7 con todas las categorías que desea excluir.
9. Si se trata de una nueva configuración de agente, defina las configuraciones de agente de GlobalProtect según sus necesidades.
10. Haga clic en **OK (Aceptar)** para guardar la configuración.
11. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

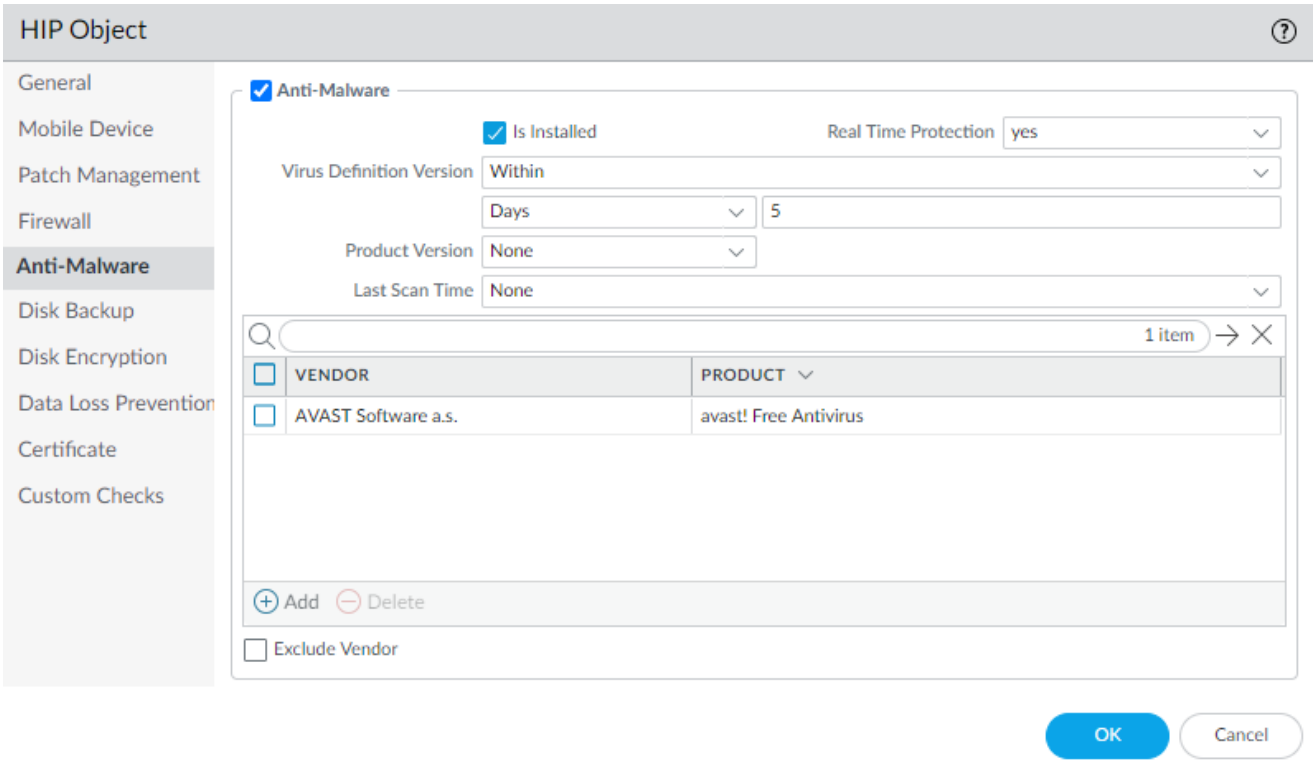
STEP 4 | Cree objetos HIP para filtrar los datos del host sin procesar recopilados por la aplicación.

La mejor forma de determinar qué objetos HIP necesita es determinar cómo utilizará la información de host que recopila para aplicar la política. Tenga en cuenta que los objetos HIP son solo los ladrillos que le permiten crear los perfiles HIP que se utilizan en sus políticas de seguridad. Por lo tanto, es posible que desee mantener la sencillez de sus objetos, de forma que solo coincidan con un elemento, como la presencia de un tipo concreto de software necesario, la pertenencia a un dominio específico o la presencia de un sistema operativo determinado. De este modo, tendrá la flexibilidad de crear una política aumentada HIP muy granular (y muy potente).

Para obtener información detallada sobre un campo o categoría HIP específicos, consulte la ayuda en línea.

1. En el cortafuegos que aloja sus puertas de enlace de GlobalProtect (o en Panorama si planea compartir los objetos HIP con varias puertas de enlace), seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** y **añada** un objeto HIP nuevo.
2. Introduzca un nombre para el objeto en **Name**.
3. Seleccione la pestaña que corresponde a la categoría de información del host que le interesa comparar y seleccione la casilla de verificación para habilitar la comparación del objeto con esta categoría. Por ejemplo, para crear un objeto que busque información acerca de software antivirus o antispyware, seleccione la pestaña **Anti-Malware** y, a continuación, seleccione la casilla de verificación **Anti-Malware** para habilitar los campos correspondientes. Complete los campos para definir los criterios de correspondencia que desea. Por ejemplo, la siguiente imagen muestra cómo crear un objeto HIP que coincida si el endpoint tiene instalada la aplicación de software AVAST Free Antivirus, tiene habilitada la opción **Real Time Protection (Protección en tiempo real)** y si se han actualizado las definiciones de virus en los 5 últimos días.

© 2020 Palo Alto Networks, Inc.



Repita este paso para cada categoría que quiera comparar con este objeto. Para obtener más información, consulte la Tabla: Categorías de recopilación de datos.

4. (Opcional) Configure etiquetas para buscar coincidencias con la categoría de pertenencia o el estado de cumplimiento del endpoint.

   Por ejemplo, puede crear una etiqueta para buscar coincidencia con endpoints de empleados de modo que pueda evitar que los usuarios accedan a recursos de red confidenciales en sus endpoint personales.

   El agente User-ID para Windows consulta al servidor de MDM la siguiente información:

   - Estado de cumplimiento del dispositivo móvil
   - Grupo inteligente (categoría de propiedad) al cual pertenece el dispositivo móvil

   El agente de User-ID convierte esta información en etiquetas que se incorporan en el informe de HIP. Puede crear objetos HIP sobre la base de estos valores de etiquetas para aplicar políticas basadas en HIP para los endpoints de su red. Para obtener más información, consulte Configuración del agente de User-ID de Windows para recopilar información de host.

   1. Seleccione la casilla de verificación **Mobile Device (Dispositivo móvil)** para habilitar la configuración de los parámetros de **Mobile Device (Dispositivo móvil)**.
   2. En la pestaña **Device (Dispositivo)**, seleccione un operador de coincidencias (como **Contains [Contiene]** o **Is Not [No es]**) en el menú desplegable **Tag (Etiqueta)**.
   3. (Opcional) Cuando se le solicite, introduzca uno de los siguientes valores de categoría de propiedad:

      La categoría de propiedad indica quién tiene la propiedad del endpoint.

      - **`Propiedad del empleado`**
      - **`Exclusivo de la empresa`**

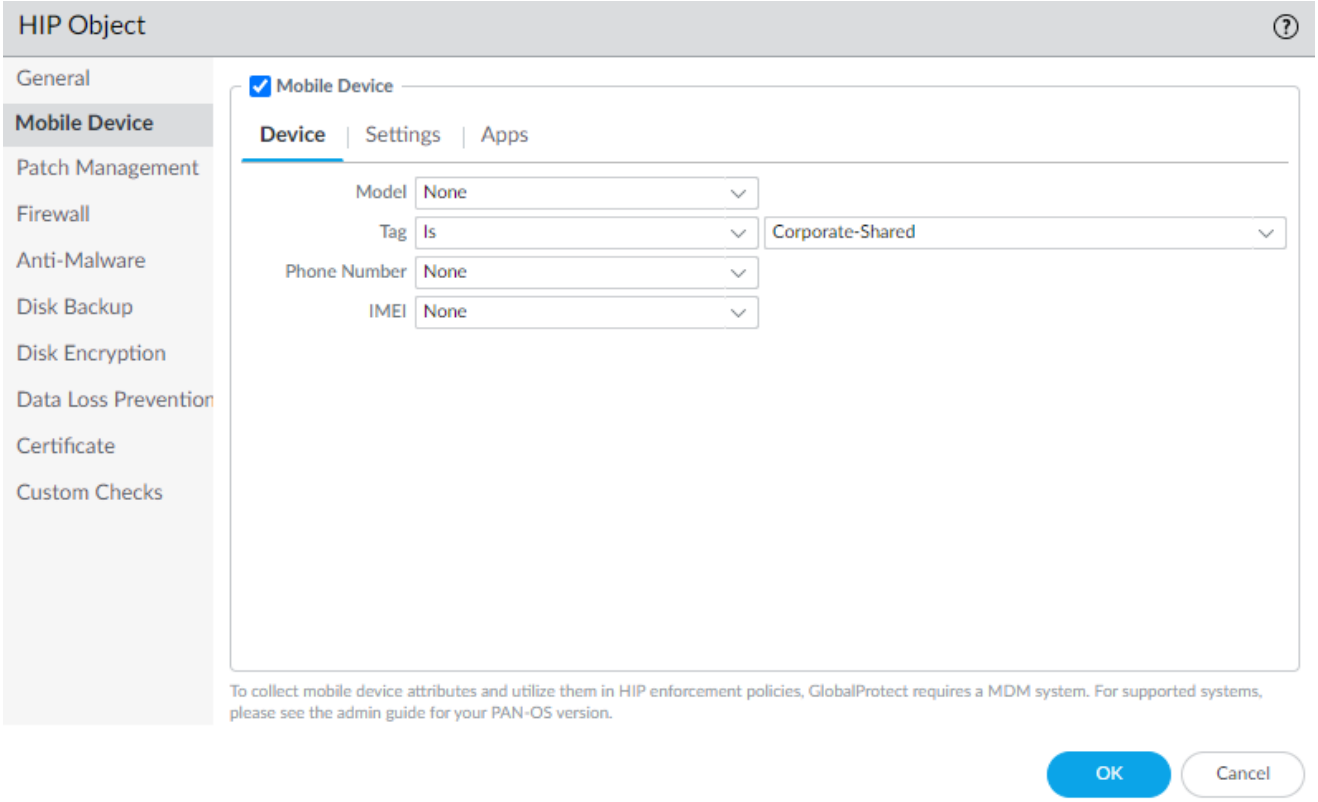
© 2020 Palo Alto Networks, Inc.

- **`Compartido de la empresa`**

4. (Opcional) Cuando se le solicite, introduzca uno de los siguientes valores de estado de cumplimiento:

   El estado de cumplimiento indica si el endpoint cumple con las políticas de seguridad que definió.

   - **`Compatible`**
   - **`No compatible`**
   - **`No disponible`**



5. Haga clic en **OK (Aceptar)** para guardar el objeto HIP.
6. Repita estos pasos para crear cada objeto HIP adicional que necesite.
7. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

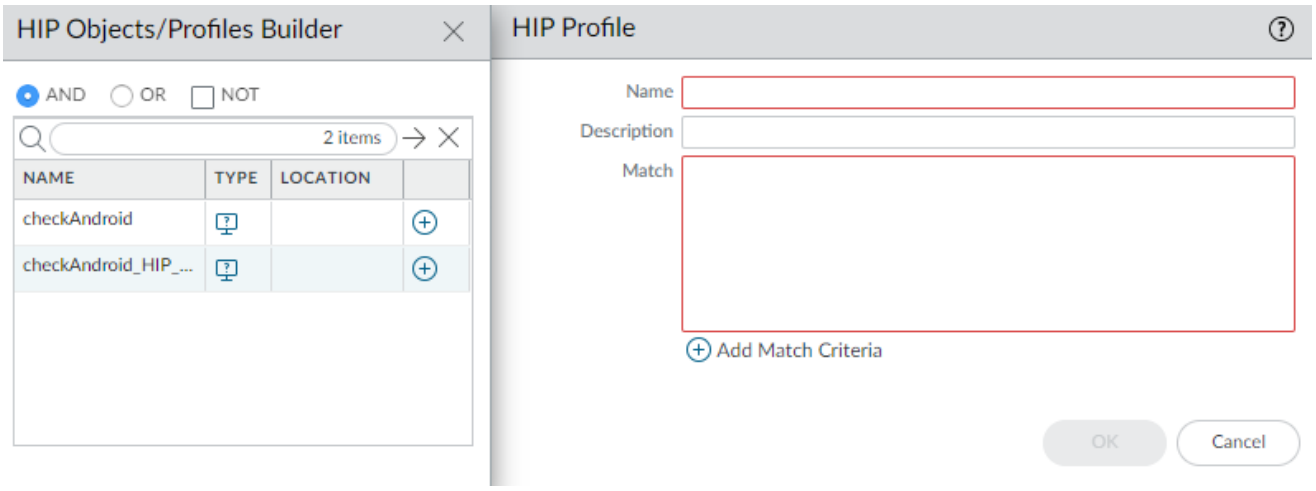
STEP 5 | Cree los perfiles HIP que planea usar en sus políticas.

Cuando crea sus perfiles HIP, puede combinar objetos HIP que haya creado previamente (así como otros perfiles HIP) con lógica booleana como la que se usa cuando un flujo de tráfico se evalúa con respecto del perfil HIP resultante con el que tendrá, o no, coincidencia. Si coincide, se aplicará la regla de política correspondiente, si no coincide, se evaluará el flujo con respecto de la siguiente regla, como con cualquier otro criterio de coincidencia de política.

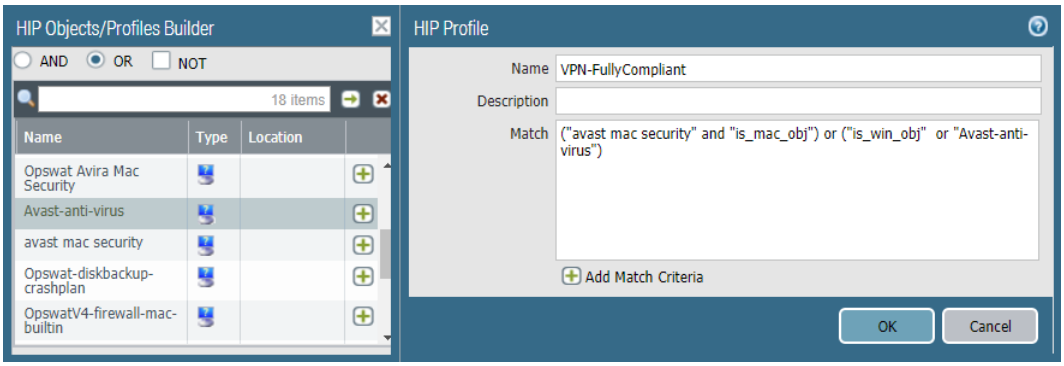
1. En el cortafuegos que aloja sus puertas de enlace de GlobalProtect (o en Panorama si planea compartir los perfiles HIP con varias puertas de enlace), seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Profiles (Perfiles HIP)** y **añada** un perfil HIP nuevo.
2. Introduzca un **Name (Nombre)** y una **Description (Descripción)** para identificar el perfil.
3. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** para abrir el creador de perfiles/objetos HIP.

© 2020 Palo Alto Networks, Inc.

4. Seleccione el objeto o perfil HIP que desea usar como criterio de coincidencia y, luego, haga clic en el icono de añadir (⊕) para moverlo al cuadro de texto **Match (Coincidencia)** del diálogo de perfil HIP. Si desea que el perfil HIP evalúe el objeto como una coincidencia solo cuando el criterio del objeto no sea verdadero para un flujo, seleccione la casilla de verificación **NOT (NO)** antes de añadir el objeto.



5. Continúe añadiendo criterios de coincidencia para el perfil que está creando. Para ello, seleccione el botón de opción del operador booleano apropiado (**AND [Y]** u **OR [O]**) cada vez que añada un elemento (y, de nuevo, use la casilla de verificación **NOT [NO]** cuando corresponda).
6. Si crea una expresión booleana compleja, debe añadir manualmente el paréntesis en los lugares adecuados del cuadro de texto **Match (Coincidencia)** para asegurarse de que el perfil HIP se evalúa usacon la lógica que desea. Por ejemplo, el siguiente perfil HIP buscará coincidencias con el tráfico desde un host que tenga cifrado de disco FileVault (en sistemas de macOS) o TrueCrypt (en sistemas Windows), que pertenezca al dominio requerido y que también tenga instalado un cliente antivirus de Symantec:



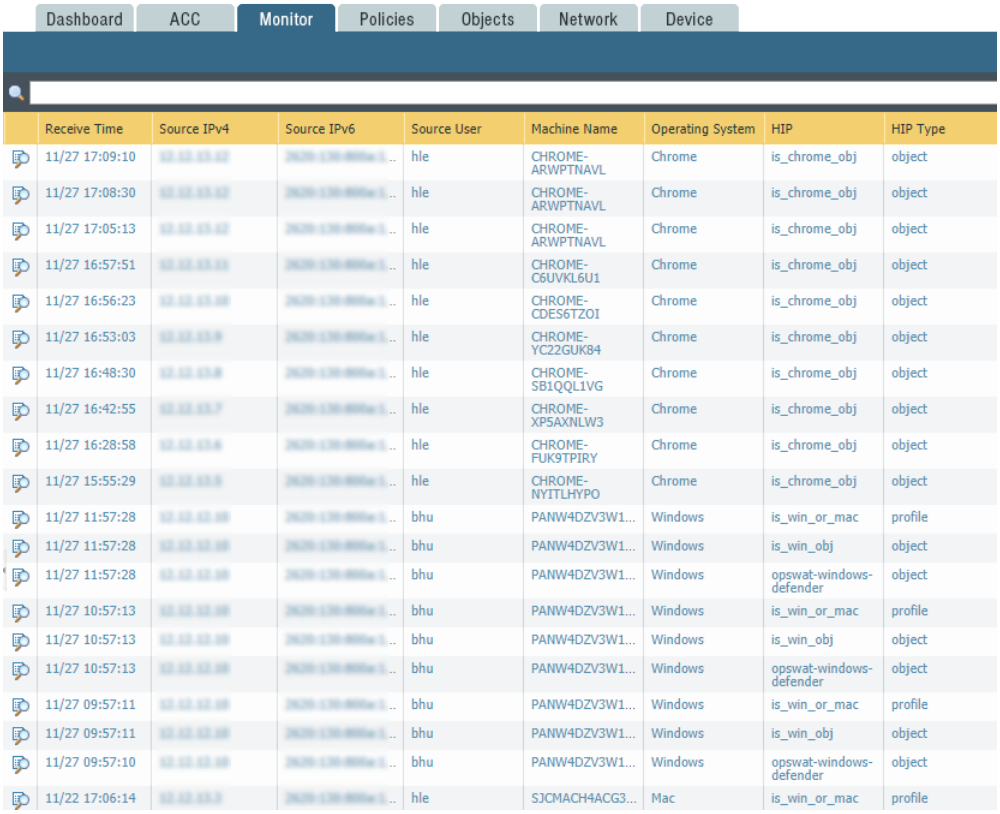
7. Cuando termine de añadir todos los criterios de coincidencia, haga clic en **OK (Aceptar)** para guardar el perfil.
8. Repita estos pasos para crear cada perfil HIP adicional que necesite.
9. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 6 | Compruebe que los objetos HIP y los perfiles HIP que creó coinciden con el tráfico de GlobalProtect según lo esperado.

Puede supervisar objetos y perfiles HIP para supervisar el estado de seguridad y la actividad de los extremos de su host. Cuando supervise la información del host durante un tiempo, podrá entender mejor dónde se encuentran sus problemas de seguridad y conformidad, lo que puede ayudarlo a crear una política útil. Para obtener más detalles, consulte ¿Cómo puedo consultar el estado de los endpoints?

© 2020 Palo Alto Networks, Inc.

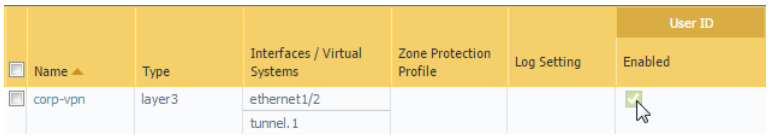
En las puertas de enlace a las que se conectan sus usuarios de GlobalProtect, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **HIP Match (Coincidencia HIP)**. Este registro muestra todas las coincidencias identificadas por la puerta de enlace durante la evaluación de los datos sin procesar de HIP suministrados por la aplicación en comparación con los objetos HIP y los perfiles HIP definidos. A diferencia de otros logs, una coincidencia HIP no requiere una coincidencia de política de seguridad para ser registrada.



Receive Time	Source IPv4	Source IPv6	Source User	Machine Name	Operating System	HIP	HIP Type
11/27 17:09:10	[illegible]	[illegible]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:08:30	[illegible]	[illegible]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:05:13	[illegible]	[illegible]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 16:57:51	[illegible]	[illegible]	hle	CHROME-C6UVKL6U1	Chrome	is_chrome_obj	object
11/27 16:56:23	[illegible]	[illegible]	hle	CHROME-CDES6TZOI	Chrome	is_chrome_obj	object
11/27 16:53:03	[illegible]	[illegible]	hle	CHROME-YC22GUK84	Chrome	is_chrome_obj	object
11/27 16:48:30	[illegible]	[illegible]	hle	CHROME-SB1QQL1VG	Chrome	is_chrome_obj	object
11/27 16:42:55	[illegible]	[illegible]	hle	CHROME-XP5AXNLW3	Chrome	is_chrome_obj	object
11/27 16:28:58	[illegible]	[illegible]	hle	CHROME-FUK9TPIRY	Chrome	is_chrome_obj	object
11/27 15:55:29	[illegible]	[illegible]	hle	CHROME-NYITLHYPO	Chrome	is_chrome_obj	object
11/27 11:57:28	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 11:57:28	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 11:57:28	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 10:57:13	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 10:57:13	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 10:57:13	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 09:57:11	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 09:57:11	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 09:57:10	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/22 17:06:14	[illegible]	[illegible]	hle	SJCMACH4ACG3...	Mac	is_win_or_mac	profile

STEP 7 | Habilite User-ID (ID de usuario) en las zonas de origen que contengan los usuarios de GlobalProtect que envían solicitudes que requieran controles de acceso basados en HIP. Debe habilitar User-ID incluso si no piensa usar la función de identificación de usuarios, ya que de lo contrario el cortafuegos no generará ninguna entrada de coincidencia HIP.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Haga clic en el **Name (Nombre)** de la zona en la que desee habilitar User-ID.
3. Seleccione **Enable User Identification (Habilitar identificación de usuario)** y haga clic en **OK (Aceptar)**.



Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	User ID Enabled
corp-vpn	layer3	ethernet1/2 tunnel.1			✓

STEP 8 | Cree las reglas de seguridad HIP en sus puertas de enlace.

Es recomendable que cree sus reglas de seguridad y que pruebe que coinciden con los flujos esperados (sobre la base de los criterios de origen y destino) antes de añadir sus perfiles de HIP. Esto le permitirá determinar mejor la ubicación adecuada de las reglas HIP dentro de la política.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla a la cual desea añadir el perfil HIP.
2. En la pestaña **Source (Origen)**, asegúrese de que **Source Zone (Zona de origen)** sea una zona para la que habilitó User-ID.
3. En la pestaña **Source (Origen)** en **Source Device (Dispositivo de origen)**, **añada** los **perfiles HIP** utilizados para identificar dispositivos (puede añadir hasta 63 perfiles HIP a una regla).
4. Haga clic en **OK (Aceptar)** para guardar la regla.
5. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

		Source				Destination	
Name	Tags	Zone	Address	User	HIP Profile	Zone	Address
iOSApps	none	corp-vpn	any	known-user	is iOS	trust	any

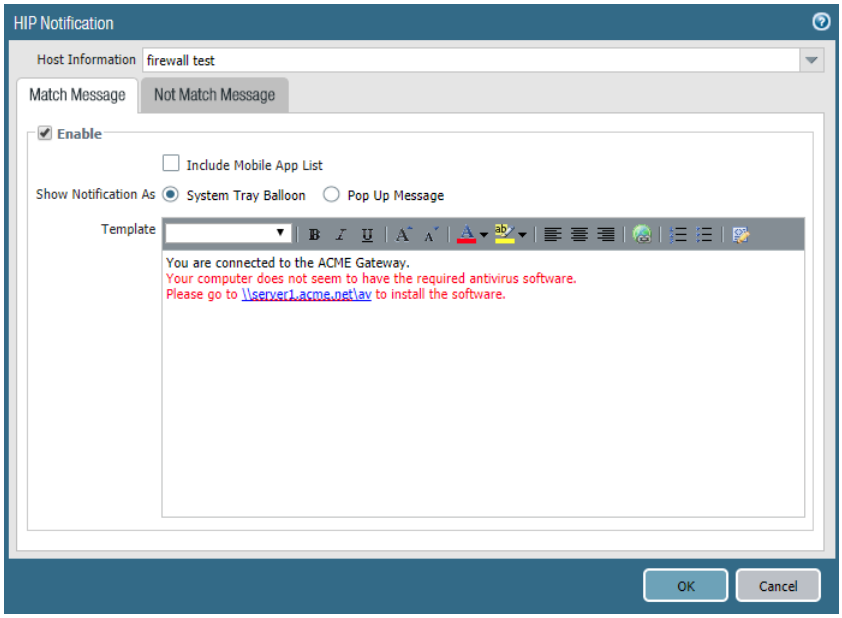
STEP 9 | Defina los mensajes de notificaciones que ven los usuarios finales cuando se aplica una regla de seguridad con un perfil HIP.

La decisión de cuándo mostrar un mensaje de notificación (es decir, si aparece cuando la configuración del usuario coincide con un perfil HIP en la política o cuando no coincide), depende en gran medida de su política y de lo que el usuario entiende por coincidencia (o no coincidencia) de HIP. Es decir, ¿significa la coincidencia que se concede total acceso a los recursos de su red? ¿O significa que tiene acceso limitado debido a un problema de incumplimiento?

Por ejemplo, suponga que crea un perfil HIP que coincide si el antivirus requerido por la empresa y los paquetes de software antispyware no están instalados. En este caso, puede que quiera crear un mensaje de notificación HIP para los usuarios que coincidan con el perfil HIP que les informe que necesitan instalar el software. Por el contrario, si su perfil HIP coincide cuando esas mismas aplicaciones están instaladas, puede que quiera crear el mensaje para aquellos usuarios que no coinciden con el perfil.

1. En el cortafuegos que se alojan sus puertas de enlace de GlobalProtect, seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**.
2. Seleccione la configuración de la puerta de enlace para la cual desea añadir los mensajes de notificación HIP.
3. Seleccione **Agent (Agente)** > **HIP Notification (Notificación HIP)** y luego haga clic en **Add (Añadir)**.
4. Seleccione el perfil HIP al que se aplica este mensaje en el menú desplegable **Host Information** (Información de host).
5. Según si desea mostrar el mensaje cuando el perfil de HIP correspondiente coincide o cuando no coincide, seleccione **Match Message (Mensaje de coincidencia)** o **Not Match Message (Mensaje sin coincidencia)**. En algunos casos, es posible que quiera crear mensajes para las dos, según los objetos en los que busca coincidencias y los objetivos de la política.
6. Seleccione **Enable (Habilitar)** para habilitar **Match Message (Mensaje de coincidencia)** o **Not Match Message (Mensaje sin coincidencia)** y, luego, seleccione si desea mostrar el mensaje como **Pop Up Message (Mensaje emergente)** o **System Tray Balloon (Globo de la bandeja del sistema)**.
7. Ingrese el texto del mensaje en el cuadro **Template (Plantilla)** y haga clic en **OK (Aceptar)**. El cuadro de texto permite una visualización del aspecto real del texto y una del código HTML, entre las que puede alternar usacon el icono de **Source Edit (Mostrar código fuente)**. La barra de herramientas ofrece asimismo muchas opciones para dar formato al texto y crear hiperenlaces a documentos externos (por ejemplo, para enlazar a los usuarios directamente a la URL de descarga de un programa de software requerido).

© 2020 Palo Alto Networks, Inc.

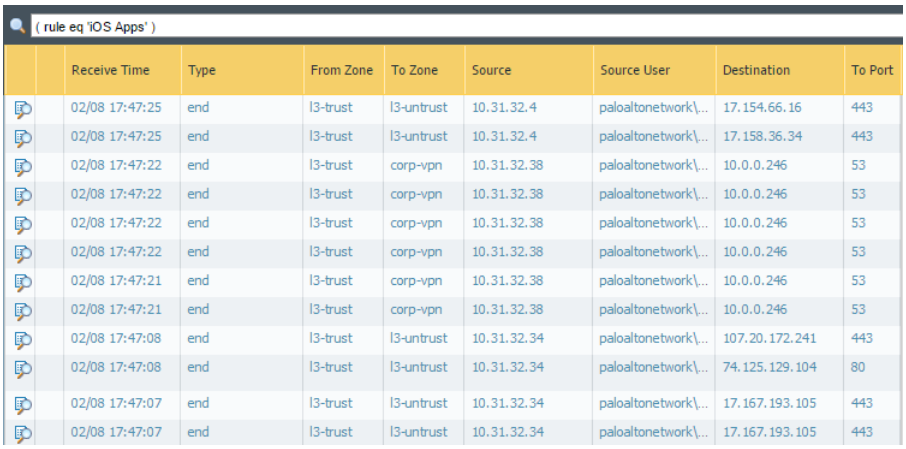


8. Repita este procedimiento para cada mensaje que quiera definir.
9. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 10 | Compruebe que sus perfiles HIP funcionan según lo esperado.

Puede supervisar qué tráfico cumple la política HIP usacon el registro de **tráfico** del siguiente modo:

1. En el cortafuegos que aloja su puerta de enlace, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Traffic (Tráfico)**.
2. Filtre el registro para mostrar solo el tráfico que coincida con la regla del perfil HIP que le interesa supervisar. Por ejemplo, para buscar tráfico que coincida con una regla de seguridad con el nombre "Apps iOS" debería introducir **(rule eq 'Apps iOS')** en el cuadro de texto de filtro del siguiente modo:



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port
02/08 17:47:25	end	l3-trust	l3-untrust	10.31.32.4	paloaltonetwork\...	17.154.66.16	443
02/08 17:47:25	end	l3-trust	l3-untrust	10.31.32.4	paloaltonetwork\...	17.158.36.34	443
02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
02/08 17:47:21	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
02/08 17:47:21	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
02/08 17:47:08	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	107.20.172.241	443
02/08 17:47:08	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	74.125.129.104	80
02/08 17:47:07	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	17.167.193.105	443
02/08 17:47:07	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	17.167.193.105	443

© 2020 Palo Alto Networks, Inc.

Recopilación de datos de procesos y aplicaciones de endpoints

El registro de Windows y la plist de macOS se pueden utilizar para configurar y almacenar ajustes para los sistemas operativos Windows y macOS, respectivamente. Puede crear una comprobación personalizada que le permita determinar si una aplicación está instalada (si tiene una clave de registro o de plist correspondiente) o está en ejecución (si tiene un proceso de ejecución correspondiente) en un endpoint de Windows o macOS. La habilitación de las comprobaciones personalizadas indica a la aplicación de GlobalProtect que debe recopilar información específica del registro (claves del registro y valores de claves del registro de endpoints de Windows) o información de listas de preferencias (plist y claves plist de endpoints de macOS). Los datos recopilados conforme a una comprobación personalizada se incluyen en la información de los hosts sin procesar que la aplicación de GlobalProtect recopila y, cuando se conecta, envía a la puerta de enlace de GlobalProtect.

Para supervisar los datos recopilados con comprobaciones personalizadas, puede crear un objeto HIP. A continuación, puede añadir un objeto HIP a un perfil HIP a fin de usar los datos recopilados para que coincidan con el tráfico del endpoint y aplicar las reglas de seguridad. La puerta de enlace usa el objeto HIP (que coincide con los datos definidos en la comprobación personalizada) para filtrar la información sin procesar del host que envió la aplicación. Cuando la puerta de enlace encuentra una coincidencia entre los datos del endpoint y un objeto HIP, se genera una entrada de registro de coincidencias HIP para los datos. El perfil HIP también permite que la puerta de enlace busque coincidencias entre los datos recopilados y una regla de seguridad. Si el perfil HIP se usa como criterio para una regla de política de seguridad, la puerta de enlace aplica esa regla de seguridad en el tráfico coincidente.

Use estos pasos para habilitar las comprobaciones personalizadas a fin de recopilar datos de los endpoints de Windows y macOS. Este flujo de trabajo también incluye pasos opcionales para crear un objeto HIP y un perfil HIP para una comprobación personalizada, que le permite usar los datos del endpoint como criterios de coincidencia para que las políticas de seguridad supervisen e identifiquen el tráfico, y reaccionen ante él.

Para obtener más información sobre cómo definir los ajustes de la aplicación directamente desde el registro de Windows o la plist global de macOS, consulte Implementación de la configuración de aplicación de forma trasparente.

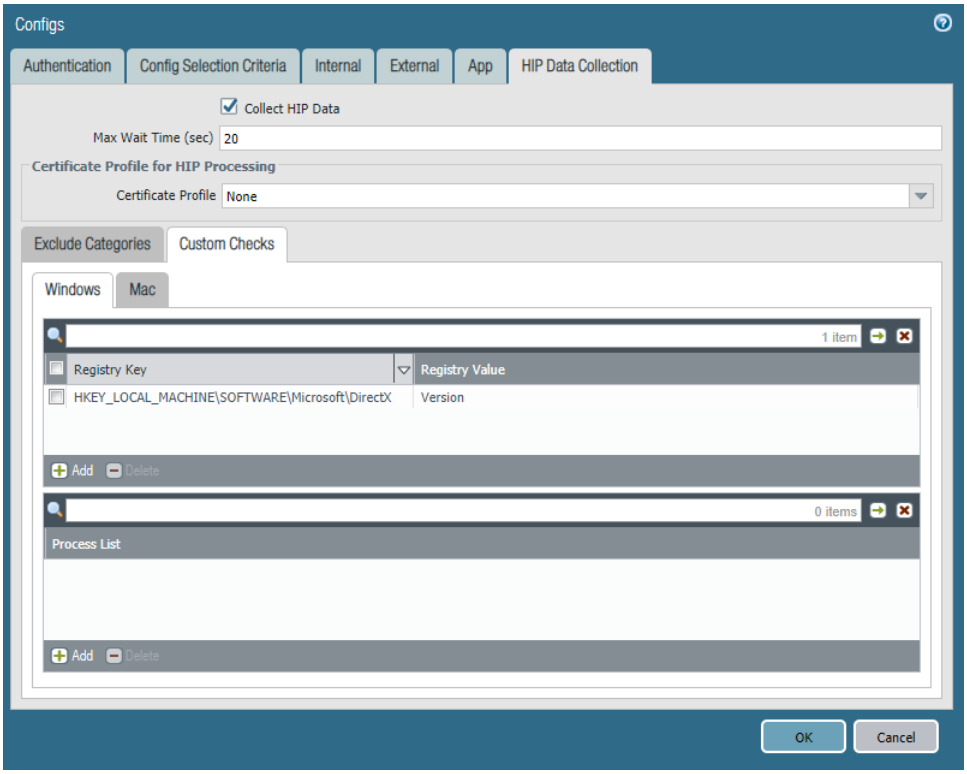
STEP 1 | Permita que la aplicación de GlobalProtect recopile información del registro de Windows de los endpoints de Windows o la información de plist de los endpoints de macOS. El tipo de información recopilada puede incluir si una aplicación está instalada o no en el endpoint, o atributos o propiedades específicas de esa aplicación.

Recopile datos desde un endpoint de Windows:

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione una configuración de portal existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Agent (Agente)**, seleccione la configuración del agente que desea modificar o haga clic en **Add (Añadir)** para añadir una nueva.
4. Seleccione **HIP Data Collection (Recopilación de datos de HIP)**.
5. Marque **Collect HIP Data (Recopilar datos de HIP)** para que la aplicación de GlobalProtect pueda recopilar información.
6. Seleccione **Custom Checks (Comprobaciones personalizadas)** > **Windows** y luego haga clic en **Add (Añadir)** para añadir una **Registry Key (Clave de registro)** sobre la que desee recopilar información.

© 2020 Palo Alto Networks, Inc.

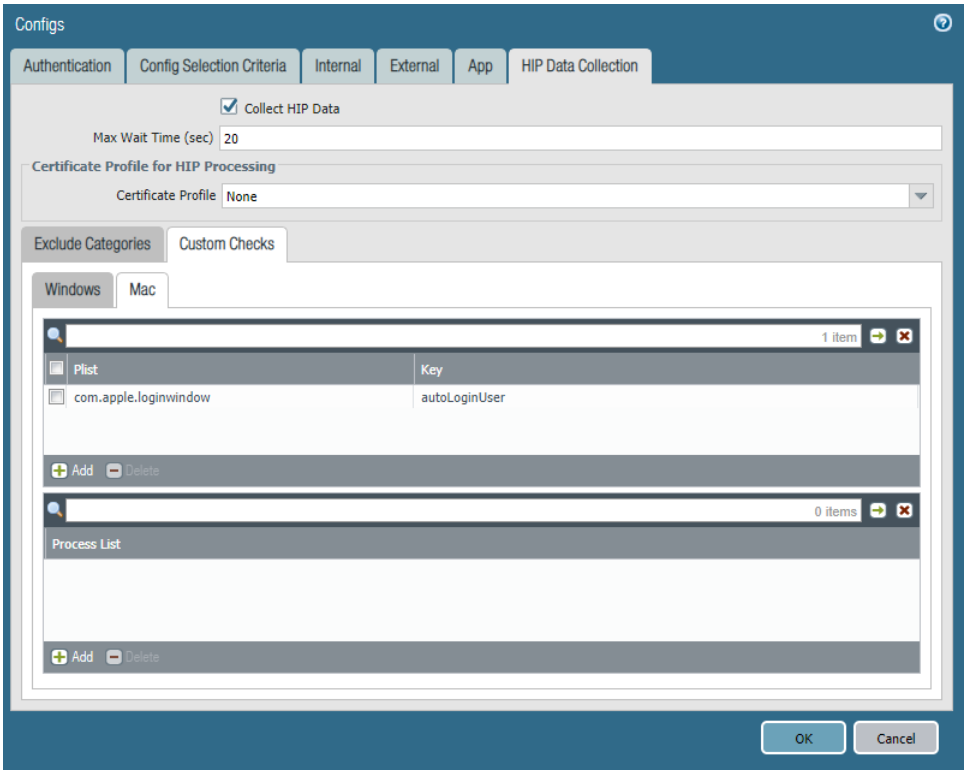
Si quiere restringir la recopilación de datos a un valor contenido en la clave del registro, añada el **Registry Value (Valor de registro)** correspondiente.



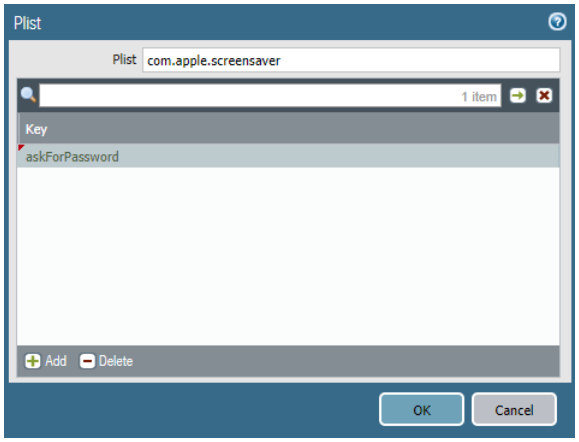
Recopile datos desde un endpoint de macOS:

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione una configuración de portal existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Agent (Agente)**, seleccione la configuración del agente que desea modificar o haga clic en **Add (Añadir)** para añadir una nueva.
4. Seleccione **HIP Data Collection (Recopilación de datos de HIP)**.
5. Marque **Collect HIP Data (Recopilar datos de HIP)** para que la aplicación de GlobalProtect pueda recopilar información.
6. Seleccione **Custom Checks (Comprobaciones personalizadas)** > **Mac** y luego haga clic en **Add (Añadir)** para añadir la **Plist (Lista de prioridades)** sobre la que desea recopilar información y la **Key (Clave)** de plist correspondiente para determinar si la aplicación está instalada.

© 2020 Palo Alto Networks, Inc.



Por ejemplo, seleccione **Add (Añadir)** para añadir la **Plist** `com.apple.screensaver` y la clave **Key (Clave)** `askForPassword` para recopilar información acerca de si se requiere contraseña para activar el endpoint de macOS una vez iniciado el protector de pantalla:



STEP 2 | (Opcional) Compruebe si se está ejecutando un proceso específico en el endpoint.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione una configuración de portal existente o haga clic en **Add (Añadir)** para añadir una nueva.
3. En la pestaña **Agent (Agente)**, seleccione la configuración del agente que desea modificar o haga clic en **Add (Añadir)** para añadir una nueva.
4. Seleccione **HIP Data Collection (Recopilación de datos de HIP)**.
5. Marque **Collect HIP Data (Recopilar datos de HIP)** para que la aplicación de GlobalProtect pueda recopilar información.
6. Seleccione **Custom Checks (Comprobaciones personalizadas)** > **Windows** o **Mac**.
7. Seleccione **Add (Añadir)** y añada el nombre del proceso sobre el que quiere recopilar información a la **Process List (Lista de procesos)**.

© 2020 Palo Alto Networks, Inc.

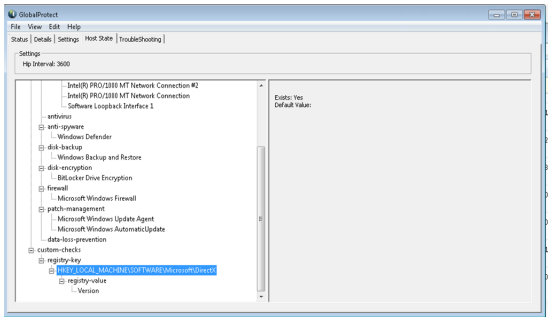
STEP 3 | Guarde la comprobación personalizada.

Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para aplicar los cambios.

STEP 4 | Verifique que la aplicación de GlobalProtect está recopilando los datos definidos en la comprobación personalizada desde el endpoint.

Para los endpoints de Windows:

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect para los endpoints de Windows. Se abre el panel de estado de GlobalProtect.
2. Haga clic en el icono de configuración ( ) para abrir el menú de ajustes.
3. Seleccione **Settings (Ajustes)** para abrir el panel **GlobalProtect Settings (Ajustes de GlobalProtect)**.
4. Seleccione la pestaña **Host Profile (Perfil de host)** para ver la información que la aplicación de GlobalProtect recopila desde el endpoint. Verifique que el menú desplegable **custom-checks (Comprobaciones personalizadas)** muestre los datos que definió para la recopilación.



Para los endpoints de macOS:

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect para los endpoints de macOS. Se abre el panel de estado de GlobalProtect.
2. Haga clic en el icono de configuración ( ) para abrir el menú de ajustes.
3. Seleccione **Settings (Ajustes)** para abrir el panel **GlobalProtect Settings (Ajustes de GlobalProtect)**.
4. Seleccione la pestaña **Host Profile (Perfil de host)** para ver la información que la aplicación de GlobalProtect recopila desde el endpoint. Verifique que el menú desplegable **custom-checks (Comprobaciones personalizadas)** muestre los datos que definió para la recopilación.

STEP 5 | (Opcional) Cree un objeto HIP para buscar coincidencias con una clave de registro (Windows) o plist (macOS), que le permita filtrar la información sin procesar del host recopilada por la aplicación de GlobalProtect a fin de supervisar los datos durante la comprobación personalizada.

Con un objeto HIP definido para los datos de la comprobación personalizada, la puerta de enlace busca coincidencias de los datos sin procesar enviados desde la aplicación al objeto HIP y se genera una entrada de registro de Coincidencia HIP para los datos (**Monitor [Supervisar]** > **HIP Match [Coincidencia HIP]**).

Para endpoints de Windows y macOS:

1. Seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos de HIP)**.
2. Seleccione un objeto de HIP existente o haga clic en **Add (Añadir)** para añadir uno nuevo.

© 2020 Palo Alto Networks, Inc.

3. En la pestaña **Custom Checks (Comprobaciones personalizadas)**, seleccione la casilla de verificación para habilitar **Custom Checks (Comprobaciones personalizadas)**.

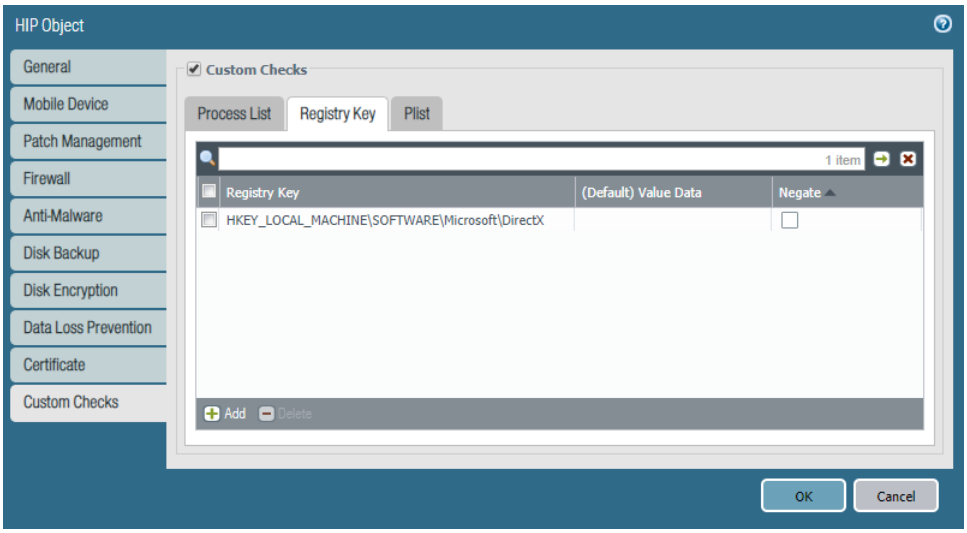
Solo para los endpoints de Windows:

1. Para buscar una clave de registro concreta en los terminales con Windows, seleccione **Custom Checks (Comprobaciones personalizadas)** > **Registry Key (Clave de registro)** y, a continuación, haga clic en **Add (Añadir)** para especificar la clave que se debe cotejar. Cuando se le indique, introduzca la clave en **Registry Key (Clave de registro)** y, a continuación, configure una de las siguientes opciones:
   - Para buscar coincidencias con los datos predeterminados de la clave de registro, introduzca un valor en **(Default) Value Data (Datos de valor predeterminados)**.
   - Para buscar coincidencias con los terminales que no tienen la clave de registro especificada, marque **Key does not exist or match specified value data (La clave no existe o no coincide con los datos de valor especificados)**.

   No configure las opciones (Default) Value Data (Datos de valor predeterminados) y Key does not exist or match specified value data (La clave no existe o no coincide con los datos de valor especificados) a la vez.
2. Para buscar coincidencias con valores concretos de la clave de registro, seleccione **Custom Checks (Comprobaciones personalizadas)** > **Registry Key (Clave de registro)** y, a continuación, haga clic en **Add (Añadir)** para especificar la clave que se debe cotejar. Cuando se le indique, introduzca la clave en **Registry Key (Clave de registro)**. Haga clic en **Add (Añadir)** y, a continuación, configure una de las siguientes opciones:
   - Para buscar coincidencias con valores concretos de la clave de registro, introduzca los valores oportunos en **Registry Value (Valor de registro)** y **Value Data (Datos de valor)**.
   - Para buscar coincidencias con los terminales que no tienen el valor especificado, introdúzcalo en **Registry Value (Valor de registro)** y marque la casilla de verificación **Negate (Negar)**.

   Cuando use esta opción, no introduzca ningún valor en el campo Value Data (Datos de valor) correspondiente a la clave especificada en Registry Key (Clave de registro).

   Si añade varios valores a la clave de registro, la puerta de enlace de GlobalProtect busca todos en los terminales.

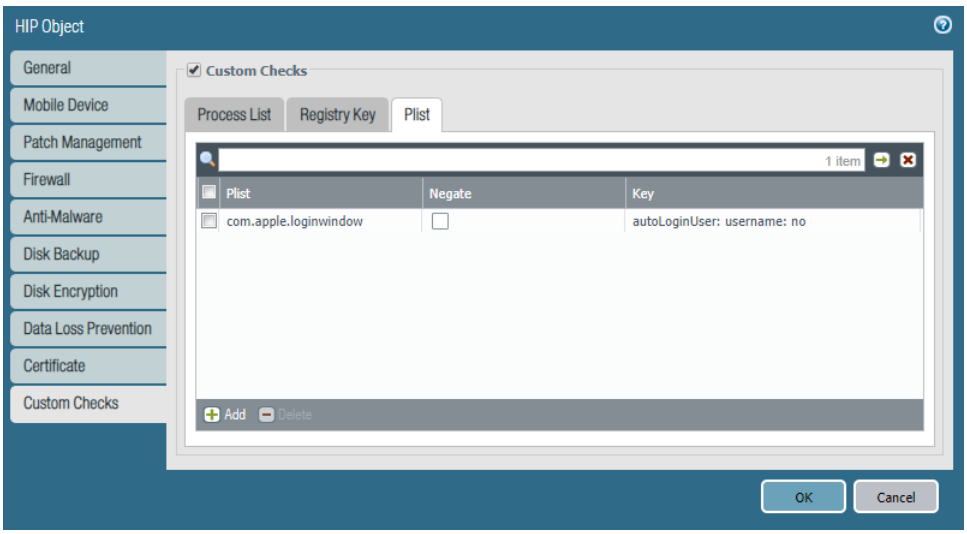


© 2020 Palo Alto Networks, Inc.

3. Haga clic en **OK (Aceptar)** para guardar el objeto HIP. Puede hacer clic en **Commit (Confirmar)** para aplicar los cambios y ver los datos en los registros de **HIP Match (Coincidencia HIP)** la próxima vez que se registre el dispositivo o continuar con el paso 6.

Solo para endpoints de macOS:

1. Para buscar una lista de propiedades concreta en los terminales con macOS, seleccione **Plist (Lista de propiedades)** y, a continuación, haga clic en **Add (Añadir)** para añadirla. Cuando se le indique, introduzca el nombre en **Plist (Lista de propiedades)**. Si desea buscar coincidencias de endpoints de macOS que no tengan la plist especificada, habilite la opción **Plist does not exist (Plist no existe)**.
2. Para buscar coincidencias con un par de clave y valor concreto de una lista de propiedades, seleccione **Plist (Lista de propiedades)** y, a continuación, haga clic en **Add (Añadir)** para añadir la lista. Cuando se le indique, introduzca el nombre en **Plist (Lista de propiedades)** y, a continuación, haga clic en **Add (Añadir)** para añadir en **Key (Clave)** y **Value (Valor)** los pares que se deben cotejar. De manera alternativa, si desea identificar endpoints que no tengan una clave y un valor específicos, puede seleccionar **Negate (Negar)** después de añadir la **Key (Clave)** y el **Value (Valor)**.



3. Haga clic en **OK (Aceptar)** para guardar el objeto HIP. Puede hacer clic en **Commit (Confirmar)** para aplicar los cambios y ver los datos en los registros de **HIP Match (Coincidencia HIP)** la próxima vez que se registre el dispositivo o continuar con el paso 6.

STEP 6 | (Opcional) Cree un perfil HIP para permitir que el objeto HIP se evalúe con respecto del tráfico.

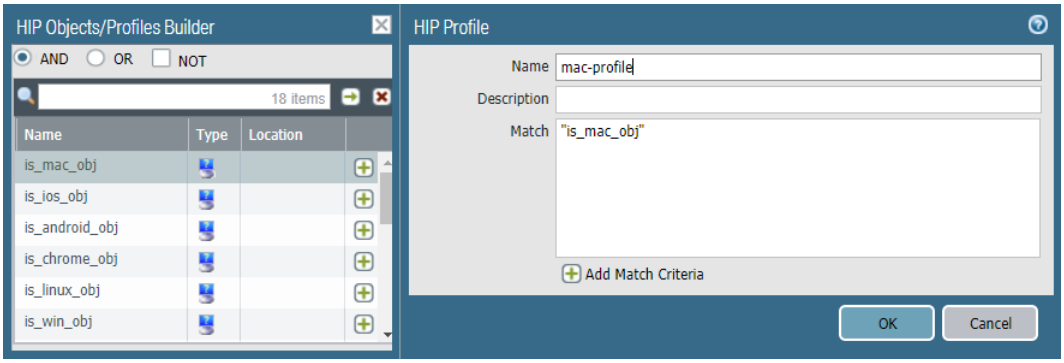
El perfil HIP se puede añadir a una política de seguridad como una comprobación adicional del tráfico que coincide con la política. Cuando se buscan coincidencias entre el tráfico y el perfil HIP, la regla de la política de seguridad se aplica al tráfico.

Para obtener más detalles sobre la creación de perfiles HIP, consulte Configuración de la aplicación de políticas basadas en HIP.

1. Seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Profiles (Perfiles HIP)**.
2. Seleccione un perfil HIP existente o haga clic en **Add (Añadir)** para añadir uno nuevo.
3. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** para abrir el creador de perfiles/objetos HIP.
4. Seleccione el **HIP object (Objeto HIP)** que desea usar como criterio de coincidencia y, luego, haga clic en el icono de añadir (

) para moverlo al área **Match (Coincidencia)** del perfil HIP.
5. Después de añadir los objetos al nuevo perfil HIP, haga clic en **OK (Aceptar)** y, a continuación, en **Commit (Confirmar)** para aplicar los cambios.

© 2020 Palo Alto Networks, Inc.



STEP 7 | Añada el perfil HIP a una política de seguridad de modo que los datos recopilados con la comprobación personalizada puedan usarse para buscar coincidencias y actuar sobre el tráfico.

Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego, seleccione una política de seguridad existente o haga clic en **Add (Añadir)** para añadir una nueva. En la pestaña **User (Usuario)**, haga clic en **Add (Añadir)** para añadir **HIP Profiles (Perfiles HIP)** a la política. Para obtener más información sobre componentes de políticas de seguridad y el uso de políticas de seguridad para buscar coincidencias y actuar sobre el tráfico, consulte Política de seguridad.

© 2020 Palo Alto Networks, Inc.

Redistribución de informes de HIP

Para garantizar la aplicación sistemática de las políticas sobre perfiles de información de hosts (host information profile, HIP) y para simplificar su gestión, distribuya los informes de HIP recibidos de las aplicaciones de GlobalProtect y enviados a puertas de enlace de GlobalProtect internas o externas entre otros dispositivos de la empresa, como puertas de enlace, cortafuegos, recopiladores de logs dedicados (dedicated log collectors, DLC) y dispositivos Panorama. La redistribución de los informes de HIP resulta útil en los casos siguientes:

- Para aplicar políticas coherentes a las puertas de enlace de GlobalProtect tanto internas como externas.
- Para aplicar políticas de HIP coherentes al tráfico de determinados usuarios cuando atraviesa varios cortafuegos.

A la hora de redistribuir los informes de HIP, siga las mismas recomendaciones de implementación que al redistribuir la información de User-ID.

Siga estos pasos para configurar la redistribución de informes de HIP.

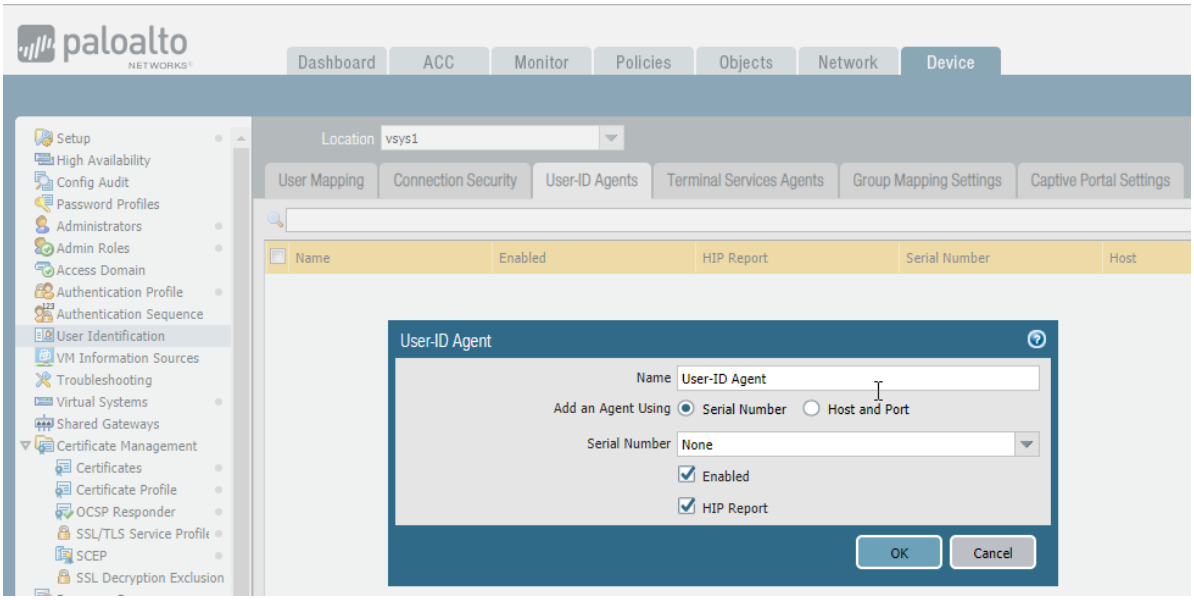
STEP 1 | Configuración de la aplicación de políticas basadas en HIP en las puertas de enlace y los cortafuegos.

STEP 2 | Configure la redistribución de informes de HIP.

1. Seleccione **Device (Dispositivo)** > **User Identificationn (Identificación de usuarios)** > **User-ID Agents (Agentes de User-ID)**.
2. Seleccione un agente de User-ID existente o haga clic en **Add (Añadir)** para añadir uno nuevo.

   El agente debe ser un cortafuegos de nueva generación de Palo Alto Networks, una puerta de enlace de GlobalProtect, un DLC o un dispositivo Panorama.

3. Seleccione **HIP Report (Informe de HIP)**.



4. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Si emplea cortafuegos o puertas de enlace de GlobalProtect para distribuir los informes de HIP, compruebe que su configuración de asignación de grupos coincide con los siguientes atributos de los cortafuegos o las puertas de enlace donde ha configurado User-ID.

Omita este paso si, en su lugar, utiliza dispositivos Panorama o DLC.

- En los cortafuegos o las puertas de enlace que usa para redistribuir los informes de HIP, configure atributos de usuarios que coincidan con los especificados en los cortafuegos o las puertas de enlace de User-ID.

  Por ejemplo, en los cortafuegos o las puertas de enlace empleados para redistribuir los informes de HIP, configure el mismo sAMAccountName en **Primary attribute (Atributo principal)** y el mismo nombre principal de usuario (user principal name, UPN) en **Alternate Username 1 (Nombre de usuario alternativo 1)** que los especificados en los cortafuegos o las puertas de enlace donde ha configurado User-ID.

  Los atributos no tienen que seguir el mismo orden; por ejemplo, puede configurar un sAMAccountName en Primary attribute (Atributo principal) y un UPN en Alternate Username 1 (Nombre de usuario alternativo 1) en el cortafuegos de redistribución y un sAMAccountName en Alternate Username (Nombre de usuario alternativo) y un UPN en Primary attribute 1 (Atributo principal 1) en el cortafuegos de User-ID.
- Si ha configurado dominios en la asignación de grupos de la implementación, configure los atributos de dominios de usuarios en los cortafuegos o las puertas de enlace empleados para redistribuir los informes de HIP de modo que coincidan con los especificados en los cortafuegos o las puertas de enlace de User-ID. Los atributos de dominios de usuarios deben ser iguales en todos los cortafuegos y todas las puertas de enlace.
- En los cortafuegos o las puertas de enlace de GlobalProtect para redistribuir los informes de HIP, configure los grupos de usuarios comunes (es decir, los que se conectan a los mismos servidores de autenticación y recuperan los mismos grupos de usuarios) de modo que coincidan con los grupos de usuarios de los cortafuegos o las puertas de enlace de User-ID.

STEP 4 | Para redistribuir los informes de HIP entre los dispositivos Panorama, las puertas de enlace, los cortafuegos y los sistemas virtuales gestionados, siga el mismo flujo de trabajo que para redistribuir la información de User-ID a los cortafuegos gestionados.

© 2020 Palo Alto Networks, Inc.

Bloqueo del acceso al endpoint

En caso de que un usuario pierda un endpoint que brinda acceso de GlobalProtect a su red, ese endpoint se robe o un usuario abandone la organización, puede bloquear el acceso del endpoint a la red colocándolo en una lista de bloqueados.

La lista de bloqueo es local en una ubicación de red lógica (vsys, 1 por ejemplo) y puede contener un máximo de 1000 endpoints por ubicación. Por lo tanto, puede crear listas de bloqueo diferentes para cada ubicación que aloje la implementación de GlobalProtect.

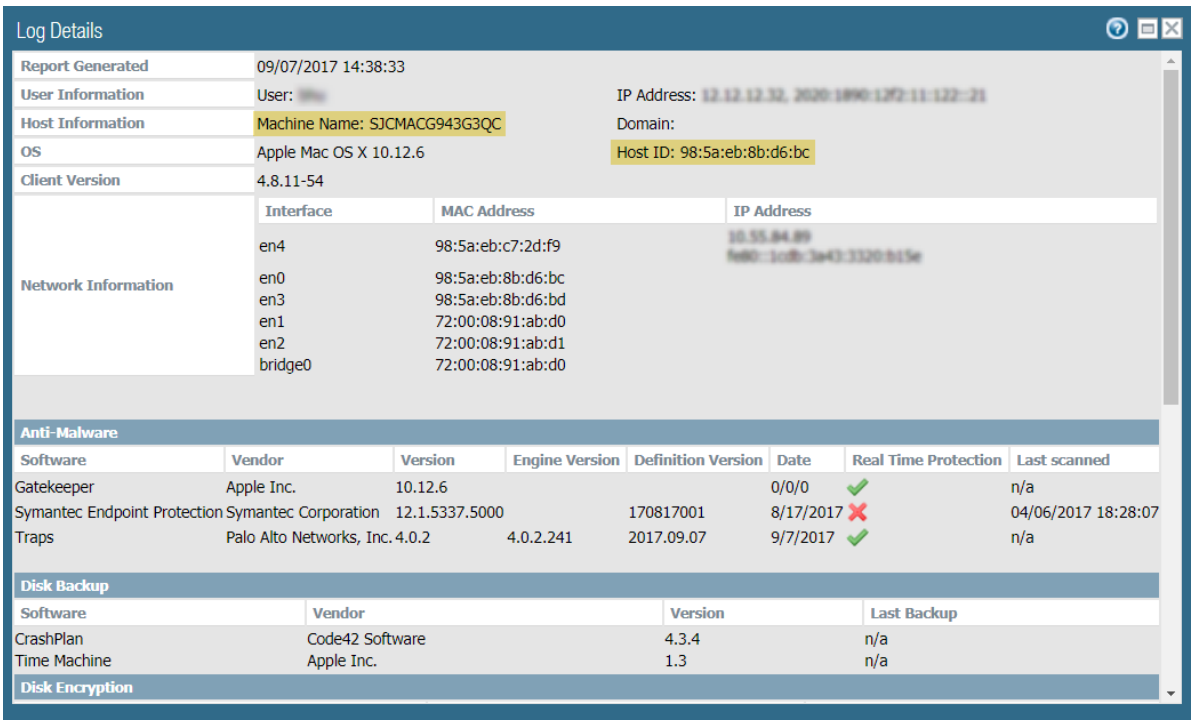
STEP 1 | Identifique la ID de host para los endpoints que desea bloquear.

El ID de host es un identificador único que GlobalProtect asigna para identificar el host. El valor de ID del host varía por tipo de endpoint:

- Windows: GUID de la máquina almacenado en el registro de Windows (HKEY_Local_Machine \Software\Microsoft\Cryptography\MachineGuid).
- macOS: dirección MAC de la primera interfaz de red física incorporada.
- Android: ID de Android.
- iOS: UDID
- Chrome: GlobalProtect asigna cadenas alfanuméricas únicas de 32 caracteres.

Si no conoce la ID de host, puede correlacionar la User-ID con la ID de host en los logs de Coincidencia HIP:

1. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **HIP Match (Coincidencias HIP)**.
2. Filtre los registros de coincidencia HIP para el usuario de origen asociado al endpoint.
3. Abra el registro de coincidencia HIP e identifique el ID de host en **OS (SO)** > **Host ID (ID de host)** y, de manera opcional, el nombre del host en **Host Information (Información del host)** > **Machine Name (Nombre de la máquina)**.



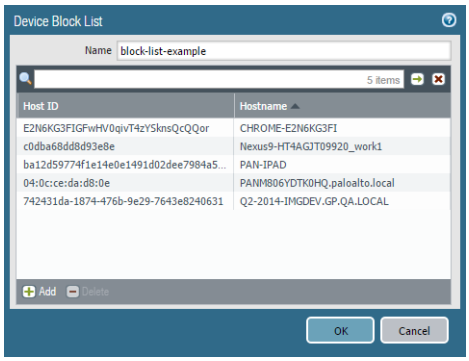
STEP 2 | Cree una lista de bloqueo de dispositivos.

© 2020 Palo Alto Networks, Inc.

No puede usar plantillas de Panorama para enviar una lista de bloqueo de dispositivos a los cortafuegos.

1. Seleccione **Network** > **GlobalProtect** > **Device Block List (Lista de bloqueo de dispositivos)** y **Add (Añadir)** para añadir una lista de bloqueo de dispositivos.
2. Introduzca un nombre descriptivo en **Name (Nombre)** para la lista.
3. En el caso de un cortafuegos con más de un sistema virtual (virtual system, vsys), seleccione en **Location (Ubicación)** la ubicación (vsys o **Shared (Compartido)**) en la que el perfil está disponible.

STEP 3 | Añada un dispositivo a la lista de bloqueo.



1. Haga clic en **Add (Añadir)** para añadir endpoints. Introduzca el ID del host (obligatorio) y el nombre del host (opcional) del endpoint que necesita bloquear.
2. Haga clic en **Add (Añadir)** para añadir endpoints adicionales, si es necesario.
3. Haga clic en **OK (Aceptar)** para guardar y activar la lista de bloqueo.

La lista de bloqueo de dispositivos no requiere una confirmación y se activa de inmediato.

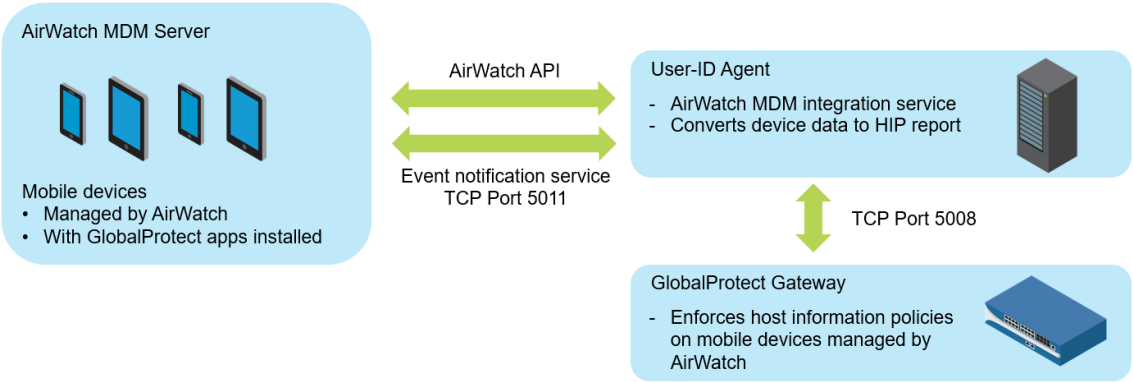
© 2020 Palo Alto Networks, Inc.

Configurar el agente de User-ID de Windows para recopilar información de host

El agente de User-ID basado en Windows se ha ampliado para admitir un nuevo servicio de integración de MDM de AirWatch. Este servicio permite a GlobalProtect utilizar la información del host recopilada por el servicio para aplicar políticas basadas en HIP en dispositivos administrados por AirWatch. El servicio de integración de MDM de AirWatch, que funciona como parte del User-ID basado en Windows, usa la API de AirWatch para recopilar información de endpoints móviles administrados por VMware AirWatch y traducir estos datos en información de host.

Para los endpoints de Android administrados por AirWatch, esta función es compatible con endpoints de Android for Work pero no con otros tipos de endpoints de Android.

- Resumen de la integración de MDM
- Información recopilada
- Requisitos del sistema
- Configuración de GlobalProtect para recuperar información del host
- Solucionar problemas del servicio de integración de MDM



Resumen de la integración de MDM

El servicio de integración de MDM incluido con el agente de User-ID basado en Windows realiza una consulta HIP completa en el servidor de MDM de AirWatch para recuperar toda la información del host de un dispositivo móvil. Las aplicaciones de GlobalProtect en dispositivos móviles también envían información de HIP a la puerta de enlace, la cual unifica la información de HIP de las aplicaciones de GlobalProtect y el servicio de integración de MDM. Cuando un dispositivo móvil que ejecuta la aplicación de GlobalProtect está conectado a una puerta de enlace de GlobalProtect, GlobalProtect puede aplicar políticas de seguridad con perfiles de información de host.

Puede configurar que el servicio de integración de MDM recupere la información del dispositivo de AirWatch en intervalos regulares y envíe esta información a las puertas de enlace de GlobalProtect. Además, el servicio puede supervisar las notificaciones de eventos de AirWatch y recuperar la información actualizada del dispositivo cuando ocurran eventos de AirWatch (como cambios de cumplimiento).

Información recopilada

La siguiente tabla muestra cómo la información recopilada de los endpoints que AirWatch administra se traduce a los atributos de informe HIP. La asignación se hace automáticamente.

© 2020 Palo Alto Networks, Inc.

Atributos de AirWatch	Atributos de informes HIP
Información de dispositivo	
Número de serie	serial-number
Dirección Mac	wifimac
IMEI	IMEI
Sistema operativo	versión
Modelo	modelo
Nombre fácil de dispositivo	Devname
Está supervisado	supervisado
Udid (identificador de dispositivo único)	UDID
Nombre de usuario	user
Última fecha de inscripción	enroll-time
Zero Trust	os
Estado de inscripción	managed-by-mdm
Visto última vez	last-checkin-time
Estado de cumplimiento (Agente de User-ID 8.0.3 y posterior)	Compatible No compatible No disponible
Titularidad (Agente de User-ID 8.0.3 y posterior)	Propiedad del empleado Exclusivo de la empresa Compartido de la empresa
Información de seguridad	
Protección de datos habilitada	disk-encrypted
El código de acceso está presente	passcode-set
El código de acceso cumple normativa	passcode-compliant
Información de red	
Movilidad de datos habilitada	data-roaming
Coordenadas GPS	

© 2020 Palo Alto Networks, Inc.

Atributos de AirWatch	Atributos de informes HIP
Latitud	latitud
Longitud	longitud
Tiempo de muestra	last-location-time
Detalles de la aplicación	
Nombre de la aplicación	appname
versión	versión
Identificador de aplicación	paquete

Requisitos del sistema

El servicio de integración AirWatch MDM requiere el siguiente software:

Software	Versión mínima compatible
Agente de ID de usuarios	8.0.1
PAN-OS	7.1.0
Aplicación de GlobalProtect para Android	4.0.0
Aplicación de GlobalProtect para iOS	4.0.1
Servidor AirWatch	8.4.7.0
Servidor Windows	2008 y 2012 2016 con agente de User-ID 8.0.4 y PAN-OS 8.0.4

Configuración de GlobalProtect para recuperar información del host

Use las siguientes instrucciones para configurar que GlobalProtect recupere la información del host de los dispositivos gestionados por AirWatch.

STEP 1 | Instale el agente de User-ID. El agente de User-ID debe estar en una ubicación que permita conexiones seguras al sistema de administración de dispositivos móviles (MDM) VMware AirWatch.

El servicio de integración de MDM de AirWatch se incluye con el agente de User-ID basado en Windows de PAN-OS.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Configure la autenticación SSL entre el agente de User-ID basado en Windows y la puerta de enlace de GlobalProtect.

Cuando configure la autenticación SSL, asegúrese de que:

- El certificado del servidor configurado en el agente User-ID basado en Windows tiene el mismo Nombre común (Common Name, CN) que el nombre del host/dirección IP del host del agente de User-ID.
- El cortafuegos confía en el certificado del servidor (incluido en la lista de CA de confianza en la configuración de MDM en el cortafuegos).
- El certificado de entidad de certificación (CA) raíz del certificado de cliente MDM configurado en el cortafuegos debe importarse al almacén de confianza de Windows del servidor de Windows.

1. Obtenga un certificado de servidor y una clave privada para la autenticación entre el agente de User-ID basado en Windows y la puerta de enlace de GlobalProtect. El paquete de certificados debe estar en el formato PEM que contenga un certificado PEM, una cadena de certificados completa y una clave privada.
2. Abra el agente de User-ID basado en Windows y seleccione **Server Certificate (Certificado de servidor)**.
3. Seleccione **Add (Añadir)** el certificado del servidor.

- Seleccione **Browse (Examinar)** para ir al archivo de certificado y seleccione **Open (Abrir)** el archivo para cargar el certificado al User-ID basado en Windows.
- Introduzca un **Private Key Password (Contraseña de clave privada)** para el certificado.
- Haga clic en **OK (Aceptar)**.

El agente verifica que el certificado sea válido y almacena la contraseña de cifrado de la clave privada en el almacén de credenciales de Windows del equipo host.

Si la instalación es correcta, la información detallada sobre el certificado (incluyendo nombre común, fecha de vencimiento y emisor) aparece en la pestaña **Server Certificate (Certificado de servidor)**.

1. Reinicie el agente de User-ID basado en Windows.

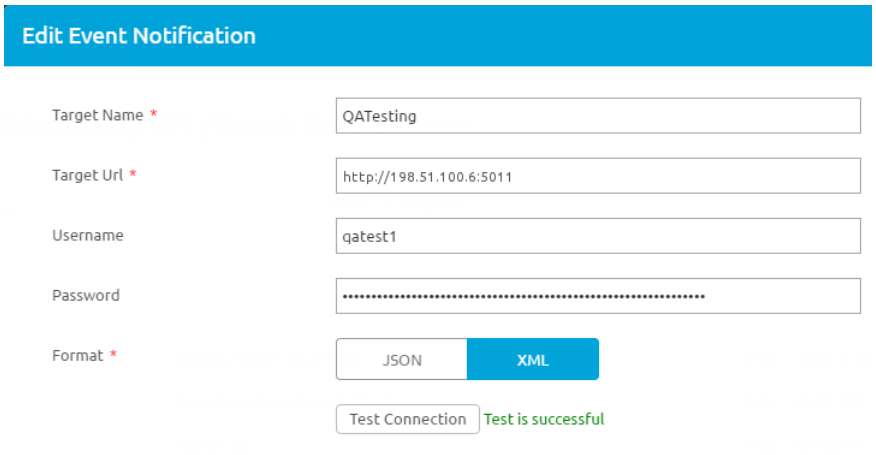
STEP 3 | Configure el servicio de integración de MDM en el agente de User-ID basado en Windows.

1. Seleccione **MDM Integration (Integración de MDM)** en el agente de User-ID basado en Windows.
2. Especifique un **Gateway Connection TCP Port (Puerto TCP de conexión de puerta de enlace)** para las comunicaciones TCP. El agente de User-ID basado en Windows escucha en este puerto todos los mensajes relacionados con MDM. El puerto predeterminado es 5008. Para cambiar el puerto, especifique un número de 1 a 65535.
3. En la pestaña **Setup (Configuración)**, haga clic en **Edit (Editar)**.
4. Seleccione **AirWatch** para el **MDM Vendor (Proveedor de MDM)**.

STEP 4 | Especifica la configuración de la **MDM Event Notification (Notificación de eventos MDM)** para supervisar y recopilar eventos de AirWatch (por ejemplo, inscripción de dispositivo, borrado de dispositivo y cambios en el cumplimiento). Cuando un evento tiene lugar, el servicio de integración de MDM obtiene la información actualizada del dispositivo de la API de AirWatch y envía esta información a todas las puertas de enlace configuradas de GlobalProtect.

En MDM Event Notification (Notificación de eventos MDM), asegúrese de que los valores que introduce aquí también estén configurados en la consola de AirWatch en Groups & Settings (Grupos y ajustes) > All Settings (Todos los ajustes) > System (Sistema) > Advanced (Avanzado) > API > Event Notifications (Notificaciones de eventos).

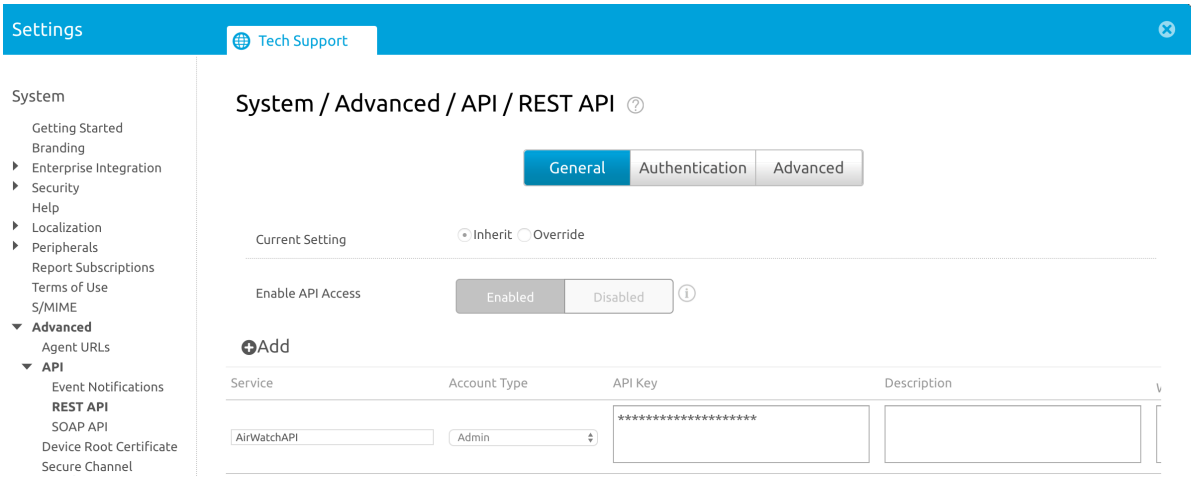
© 2020 Palo Alto Networks, Inc.



- Establezca el **TCP Port (Puerto TCP)** para comunicarse con el servicio de notificación de eventos. Utilice este formato: **`http://<external_hostname>/<ip_address>:<port>`** donde **`<ip-address>`** es la dirección IP para el servicio de integración de MDM. El puerto predeterminado es 5011. Para cambiar el puerto, especifique un número de 1 a 65535.
- Para la notificación de eventos, introduzca las credenciales de **Username (Nombre de usuario)** y **Password (Contraseña)** necesarias para autenticar las solicitudes entrantes.
- Introduzca las direcciones de **Permitted IP (IP Permitidas)** para acceder a eventos MDM. Esta es una lista de direcciones IP separadas por comas desde donde se publican los eventos de MDM. Por ejemplo, la dirección IP del servidor AirWatch. Póngase en contacto con su equipo de asistencia técnica de AirWatch para obtener orientación sobre qué direcciones IP especificar.

STEP 5 | Añada la configuración de **MDM API Authentication (Autenticación de la API de MDM)** para conectarse con la API de AirWatch.

- Introduzca la **Server Address (Dirección de servidor)** del servidor MDM de AirWatch al que se conectará el agente de User-ID basado en Windows. Por ejemplo, **`api.awmdm.com`**.
- Introduzca las credenciales de **Username (Nombre de usuario)** y **Password (Contraseña)** necesarias para acceder a la API de MDM de AirWatch.
- Introduzca el **Tenant Code (Código de inquilino)**. Este es un número de código hexadecimal único requerido para acceder a la API de MDM de AirWatch. En la consola de AirWatch, puede encontrar el código de inquilino en **System (Sistema)** > **Advanced (Avanzado)** > **API** > **REST API (API de REST)** > **API Key (Clave de API)**.



© 2020 Palo Alto Networks, Inc.

- Introduzca el **Mobile Device State Retrieval Interval (Intervalo de recuperación de estado del dispositivo móvil)**. Esta configuración controla la frecuencia con la que se recupera la información del host de los dispositivos gestionados por AirWatch. El intervalo predeterminado es de 30 minutos. Para cambiar el intervalo, especifique un número de 1 a 600.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Haga clic en **Test Connection (Probar conexión)** para asegurarse de que el agente de User-ID basado en Windows se pueda conectar a la API de AirWatch.

STEP 8 | Configure la puerta de enlace de GlobalProtect para comunicarse con el servicio de integración de MDM para recuperar los informes de HIP para los dispositivos gestionados por AirWatch.

1. En la interfaz web de PAN-OS, seleccione **Network (Red)** > **GlobalProtect** > **MDM**.
2. Seleccione **Add (Añadir)** para añadir la siguiente información sobre el servicio de integración de MDM.

- **Name (Nombre)**: introduzca un nombre para el servicio de integración de MDM (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
- (Opcional) Seleccione el sistema virtual al que pertenece la puerta de enlace.
- **Server (Servidor)**: introduzca la dirección IP o FQDN de la interfaz en el servicio de integración de MDM donde la puerta de enlace se conecta para recuperar informes HIP. Asegúrese de contar con una ruta de servicio a esta interfaz.
- **Connection Port (Puerto de conexión)**: introduzca el puerto de conexión donde el servicio de integración de MDM escucha las solicitudes de informes HIP. El puerto predeterminado es 5008. Para cambiar el puerto, especifique un número de 1 a 65535.
- **Client Certificate (Certificado de cliente)**: seleccione el certificado de cliente que debe presentar la puerta de enlace al servicio de integración de MDM al establecer una conexión HTTPS. Puede elegir un certificado de cliente del menú desplegable o importar un nuevo certificado de cliente. El **Certificate Purpose (Objetivo del certificado)** debe indicar que es un certificado de autenticación del cliente.

El certificado de entidad de certificación (CA) raíz del certificado del cliente debe importarse al almacén de confianza de Windows del servidor de Windows donde está instalado el agente de User-ID.

1. Seleccione **Add (Añadir)** el certificado de CA raíz asociado con el certificado de servidor instalado en el host del servicio de integración de MDM. Necesita el certificado de CA raíz y el certificado de servidor para establecer una conexión segura entre la puerta de enlace y el servicio de integración de MDM. Puede elegir un certificado de CA raíz del menú desplegable, o *Importar* un nuevo certificado.
2. Haga clic en **OK (Aceptar)**.
3. **Commit (Confirmar)** los cambios.

STEP 9 | Verifique su conexión para asegurarse de que los datos del dispositivo AirWatch se transfieren a GlobalProtect.

1. Abra el agente de User-ID basado en Windows y seleccione **MDM Integration (Integración MDM)** > **Mobile Devices (Dispositivos móviles)**. Debería ver una lista de ID de dispositivos únicos y nombres de usuario para todos los dispositivos gestionados por AirWatch.
2. (Opcional) Usted puede **Filter (Filtrar)** la lista para encontrar un **Mobile device (Dispositivo móvil)** específico.
3. (Opcional). Seleccione un dispositivo de la lista de ID de dispositivos y haga clic en **Retrieve Device State (Recuperar estado del dispositivo)** para extraer la información más reciente sobre el dispositivo y ver cómo se asigna a los perfiles de información del host en la puerta de enlace de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Solucionar problemas del servicio de integración de MDM

Siga estas instrucciones si tiene problemas con las notificaciones de eventos o problemas para autenticarse en la API REST de AirWatch.

- El servicio de integración de MDM no recibe las notificaciones de eventos del servidor de MDM de AirWatch.
  1. Establezca la opción **Debug (Depurar)** [en el menú de **File (Archivo)**] en **Debug (Depurar)** o **Verbose (Detallado)**.
  2. Vaya a la carpeta de instalación del agente de User-ID en el servidor de Windows y abra el archivo `MaDebug`. Busque mensajes similares a los siguientes:

     ```
     The address x.x.x.x
     is not in the permitted ip list for event notifications.
     ```

  3. Añada esta dirección IP como una dirección **Permitted IP (IP permitida)** (**MDM Integration [Integración de MDM]** > **Setup [Configuración]** > **Permitted IP [IP permitida]**).

- La autenticación de la API REST de Airwatch ha fallado

  Asegúrese de que:

  - Las credenciales utilizadas para que el servicio de integración de MDM se autentique en el servicio de MDM de AirWatch son válidas.
  - La cuenta de usuario utilizada para acceder a la API REST de Airwatch tiene permisos de acceso API y permisos de solo lectura (como mínimo) para los datos de los dispositivos móviles y los usuarios gestionados por AirWatch.
  - El **Tenant Code (Código de inquilino)** (clave API) está correctamente asociado con la cuenta de usuario. Eliminar todas las claves API no utilizadas.

© 2020 Palo Alto Networks, Inc.

Dispositivos en cuarentena que utilizan información del host

GlobalProtect le permite añadir manual o automáticamente dispositivos en riesgo a una lista de cuarentena. Después de poner en cuarentena el dispositivo, puede no permitir a los usuarios que inicien sesión en la red desde ese dispositivo mediante GlobalProtect. También puede restringir el tráfico a un dispositivo en riesgo, desde un dispositivo en riesgo o ambos. Si usa un dispositivo Panorama, también puede redistribuir la información del dispositivo en cuarentena a otros cortafuegos de nueva generación. Utilice los siguientes temas para aprender cómo poner en cuarentena un dispositivo, incluidos los requisitos de licencia de suscripción de GlobalProtect, y cómo redistribuir la información de cuarentena.

- Descripción general de la identificación y cuarentena de dispositivos en riesgo y requisitos de licencia
- Visualización de información del dispositivo en cuarentena
- Adición y eliminación de dispositivos manualmente de la lista de cuarentena
- Cuarentena automática para un dispositivo
- Uso de políticas de seguridad y de GlobalProtect para bloquear el acceso a los dispositivos en cuarentena
- Redistribución de la información de cuarentena del dispositivo desde Panorama

Descripción general de la identificación y cuarentena de dispositivos en riesgo y requisitos de licencia

GlobalProtect le facilita el bloqueo de dispositivos en riesgo de su red mediante la identificación de un dispositivo en riesgo con su ID de host y, opcionalmente, el número de serie en lugar de su dirección IP de origen. Esta capacidad puede ser preferible a bloquear un endpoint en riesgo de una red en función de su dirección IP, ya que si la dirección IP de un dispositivo cambia (por ejemplo, si un usuario mueve su endpoint de un lugar de trabajo a su casa), las políticas de seguridad basadas en direcciones IP podrían permitir que el endpoint vuelva a la red.

Después de identificar un dispositivo como en riesgo (por ejemplo, si un dispositivo se ha infectado con malware y está realizando acciones de comando y control), puede añadir manualmente el ID de host del dispositivo a una lista de cuarentena y configurar GlobalProtect para evitar que los usuarios se conecten a la puerta de enlace de GlobalProtect desde un dispositivo en cuarentena. También puede poner en cuarentena automáticamente el dispositivo mediante perfiles de reenvío de logs con políticas de seguridad o configuraciones de log de coincidencias HIP.

Antes de comenzar a poner en cuarentena los dispositivos, asegúrese de que los usuarios de GlobalProtect utilicen la versión de la aplicación de GlobalProtect 5.1 como mínimo. Además, asegúrese de que haya una licencia de suscripción de GlobalProtect válida en el cortafuegos para que este pueda añadir dispositivos en riesgo a la lista de cuarentena. Los requisitos de licencia de suscripción de GlobalProtect para esta función se aplican como se describe en la siguiente lista.

- El cortafuegos requiere una licencia de suscripción de GlobalProtect para añadir dispositivos de forma manual o automática a la lista de cuarentena. Recibirá el siguiente mensaje de error si intenta añadir un dispositivo sin una licencia: `The device cannot be quarantined. You must have a valid GlobalProtect subscription to add the device to the quarantine list (El dispositivo no se puede poner en cuarentena. Debe tener una suscripción válida de GlobalProtect para añadir el dispositivo a la lista de cuarentena).`

  Sin embargo, puede eliminar los dispositivos en cuarentena de la lista de cuarentena sin una licencia.
- Si su licencia de suscripción de GlobalProtect caduca, la lista de cuarentena se conserva (no se elimina).

© 2020 Palo Alto Networks, Inc.

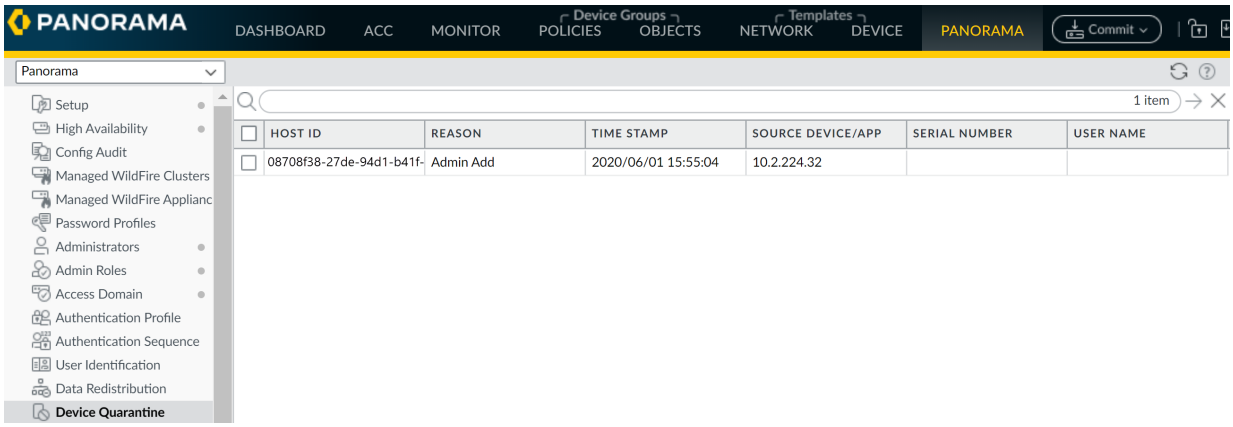
GlobalProtect realiza una verificación de licencia cada hora.

- Si no tiene una licencia de GlobalProtect válida y se cumple una de las siguientes condiciones, el cortafuegos o Panorama muestra un mensaje de advertencia cuando realiza el cambio:
  - Ha seleccionado **Quarantine List (Lista de cuarentena)** en un agente de redistribución de datos.
  - Ha seleccionado **Quarantine (Cuarentena)** como acción incorporada para un **perfil de reenvío de logs**.

Visualización de información del dispositivo en cuarentena

Puede ver la información del dispositivo en cuarentena en la página **Device Quarantine (Cuarentena del dispositivo)**. La ubicación de la página es distinta si la visualiza desde un cortafuegos de nueva generación o un dispositivo Panorama.

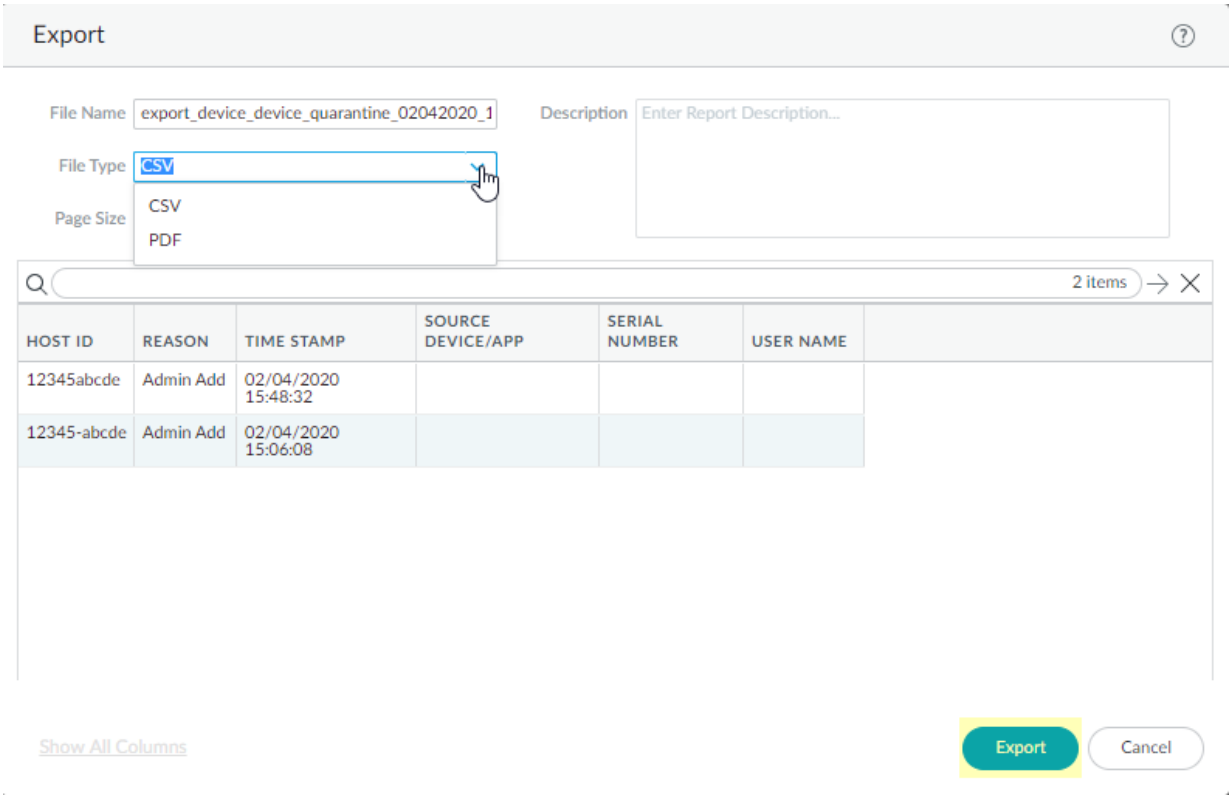
- En los cortafuegos de nueva generación, seleccione **Device (Dispositivo)** > **Device Quarantine (Cuarentena del dispositivo)** para consultar la lista de dispositivos en cuarentena.
- Para los dispositivos Panorama, vea **Device (Dispositivo)** > **Device Quarantine (Cuarentena del dispositivo)**. Para ello, seleccione **Panorama** > **Device Quarantine [Cuarentena del dispositivo]**.



- También puede ver la actividad de cuarentena de GlobalProtect desde ACC. La pestaña **GlobalProtect Quarantine Activity (Actividad de cuarentena de GlobalProtect)** en el ACC contiene un panel, **GlobalProtect Quarantine Activity (Actividad de cuarentena de GlobalProtect)**, que muestra un resumen de la vista de gráfico de los dispositivos que se han puesto en cuarentena. Utilice el conmutador de alternancia de la parte superior del gráfico para ver los dispositivos en cuarentena por las acciones que provocaron que GlobalProtect pusiera en cuarentena el dispositivo, el motivo por el que GlobalProtect puso en cuarentena el dispositivo y la ubicación de los dispositivos en cuarentena.

- Para exportar la lista de dispositivos en cuarentena a un archivo pdf o csv, seleccione **PDF/CSV** en la parte inferior de la página **Device Quarantine (Cuarentena del dispositivo)** para abrir la página **Export (Exportar)**.

© 2020 Palo Alto Networks, Inc.

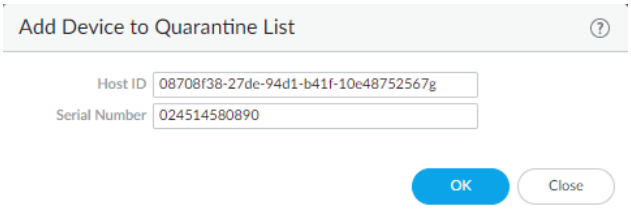


Adición y eliminación de dispositivos manualmente de la lista de cuarentena

Puede añadir un dispositivo manualmente desde las páginas de cuarentena, desde logs de GlobalProtect, amenazas, tráfico o unificados o mediante el uso de una API. También puede eliminar manualmente el dispositivo de las páginas de cuarentena, como se muestra en los siguientes pasos.

- Para añadir manualmente un dispositivo a la lista de cuarentena desde la página **Device Quarantine (Cuarentena de dispositivos)**, seleccione **Device (Dispositivo)** > **Device Quarantine (Cuarentena del dispositivo)** o **Panorama** > **Device Quarantine (Cuarentena del dispositivo)** y **añada** el dispositivo.

  Añada el **ID de host** y, opcionalmente, el **número de serie** del dispositivo. GlobalProtect utiliza el ID de host para identificar el dispositivo.



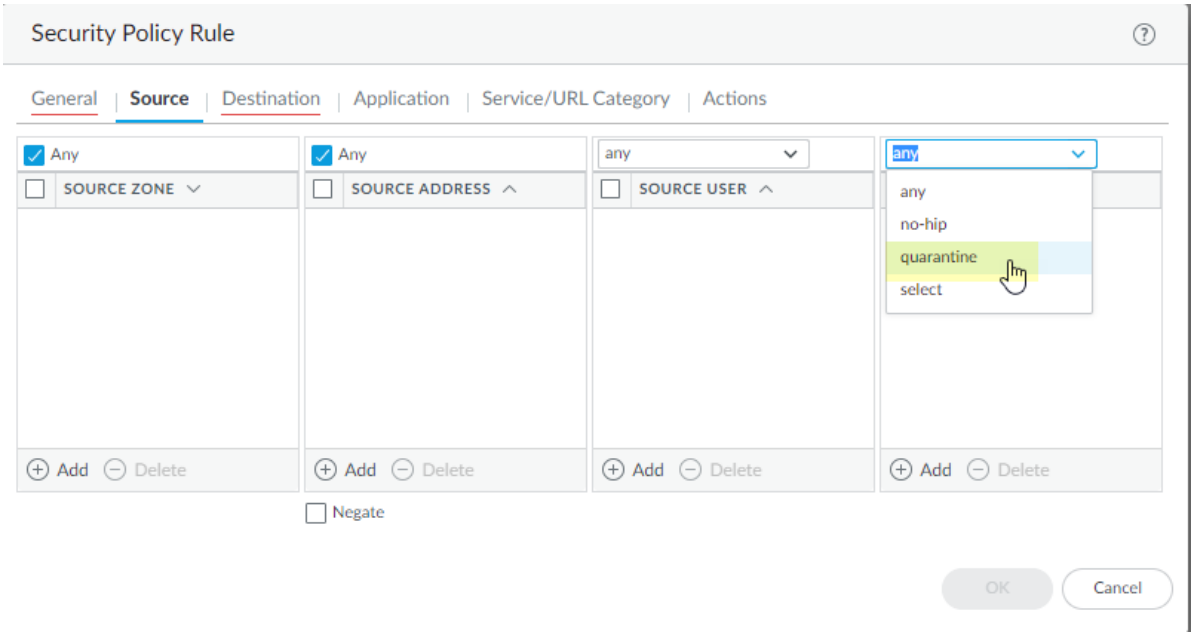
- Para añadir un dispositivo a la lista de cuarentena de los logs de GlobalProtect, amenazas, tráfico o unificados, complete los siguientes pasos.

  1. (Solo en logs de amenazas, tráfico y unificados) Para añadir información de ID de host a los logs de tráfico, amenazas y unificados, seleccione **Policies (Políticas)** > **Security (Seguridad)** y **añada** una regla

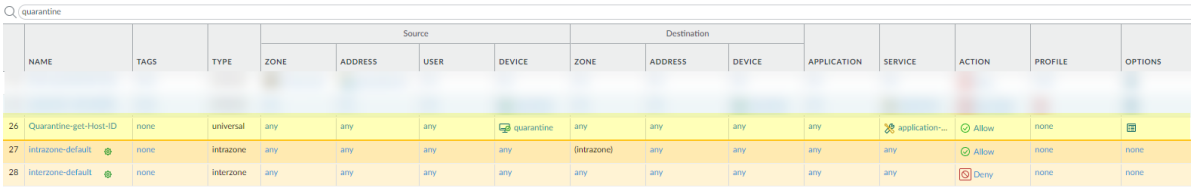
© 2020 Palo Alto Networks, Inc.

de políticas de seguridad; a continuación, seleccione **Quarantine (Cuarentena)** como **dispositivo de origen** para el tráfico de **origen**.

Se requiere un ID de host para añadir un dispositivo a la lista de cuarentena. Cuando un usuario se conecta a la red con la aplicación de GlobalProtect, GlobalProtect añade automáticamente información de ID de host para el endpoint conectado al log de GlobalProtect. Para que GlobalProtect añada automáticamente información de ID de host a los logs de tráfico, amenazas o unificados, debe añadir una regla de políticas que tenga la opción **Quarantine (Cuarentena)** seleccionada para el tráfico de origen.



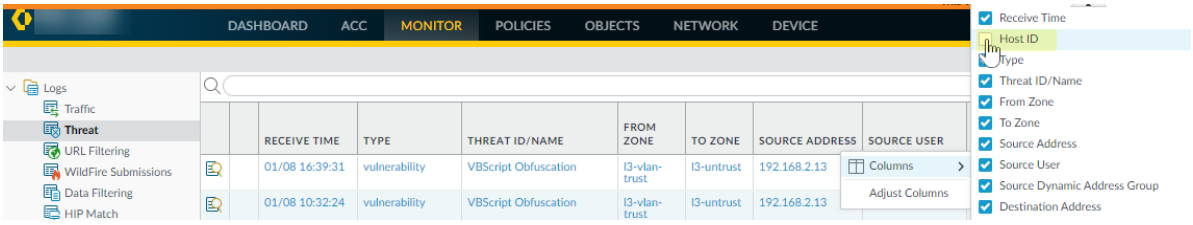
Para asegurarse de que está añadiendo el ID de host para todos los dispositivos que desea poner en cuarentena (ya sea de forma manual o automática), cree una política de seguridad que permita todo el tráfico y especifique Quarantine (Cuarentena) como dispositivo de origen. No importa en qué orden coloque esta política en la lista de políticas para que funcione.



2. Haga clic con el botón derecho en el **ID de host** asociado con el dispositivo y haga clic en **Block Device (Bloquear dispositivo)**.

Si la columna **Host ID (ID de host)** no aparece, seleccione el encabezado de cualquier columna y, a continuación, seleccione el campo **Host ID (ID de host)** para ver el ID de host.

© 2020 Palo Alto Networks, Inc.



- Para crear una API para añadir manualmente los dispositivos, consulte las instrucciones en la Guía de uso de la API de PAN-OS y Panorama.

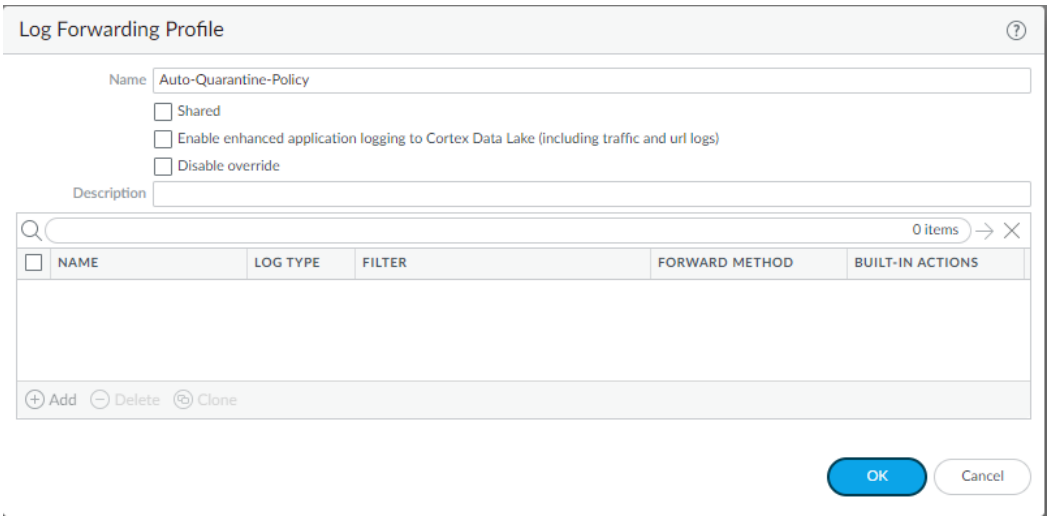
- Una vez que su administrador haya realizado la corrección en el dispositivo, podrá eliminarlo de la lista. Para ello, seleccione **Device [Dispositivo]** > **Device Quarantine [Cuarentena del dispositivo]** para cortafuegos de nueva generación o **Panorama** > **Device Quarantine (Cuarentena del dispositivo)** para dispositivos Panorama, elija uno o más dispositivos y, a continuación, seleccione **Delete (Eliminar)**.

Cuarentena automática para un dispositivo

Puede poner en cuarentena automáticamente el dispositivo mediante perfiles de reenvío de logs con políticas de seguridad o configuraciones de log de coincidencias HIP.

- Para poner en cuarentena un dispositivo con un perfil de reenvío de logs, complete los siguientes pasos.

  1. Seleccione **Object (Objeto)** > **Log Forwarding (Reenvío de logs)** y **añada** un nuevo perfil de reenvío de logs o seleccione un perfil existente para modificarlo.



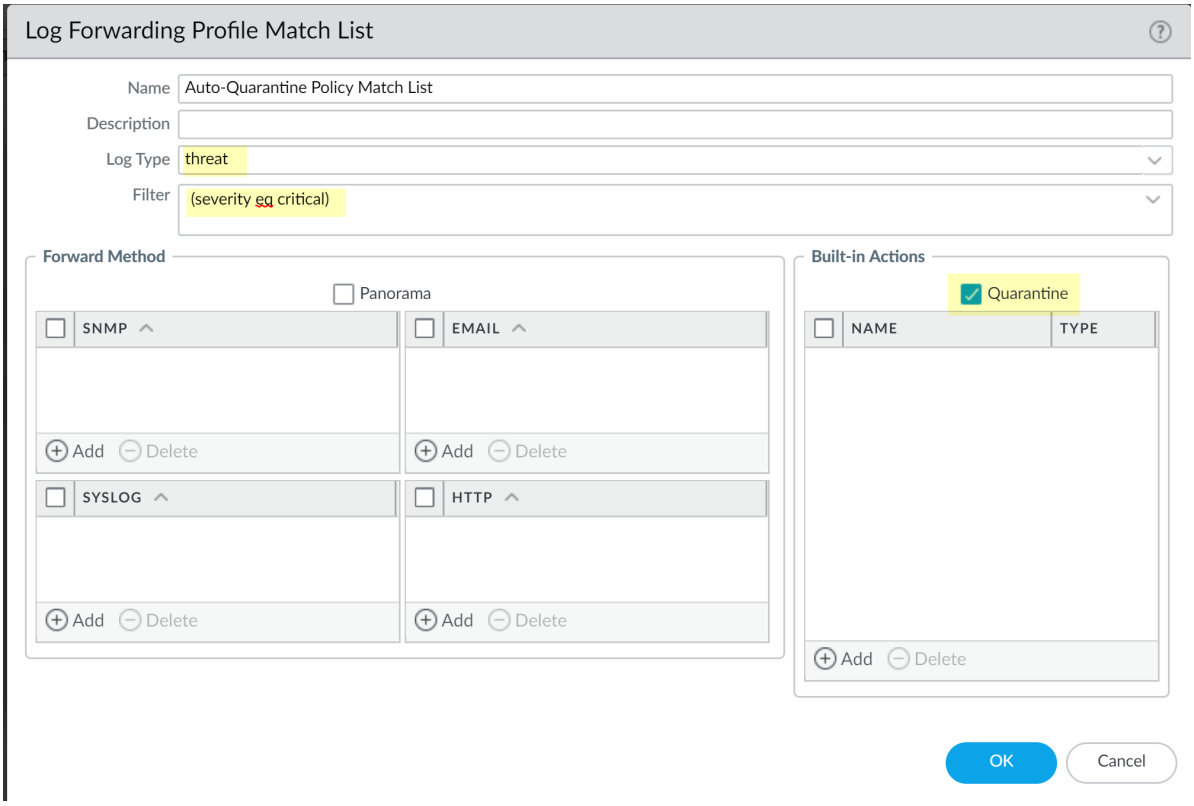
  2. **Añada** una **lista de coincidencia de perfiles de reenvío de logs** y, en la sección **Built-in Actions (Acciones integradas)**, seleccione **Quarantine (Cuarentena)**.

     Especifique un **tipo de log** de **GlobalProtect**, **amenazas** o **tráfico**.

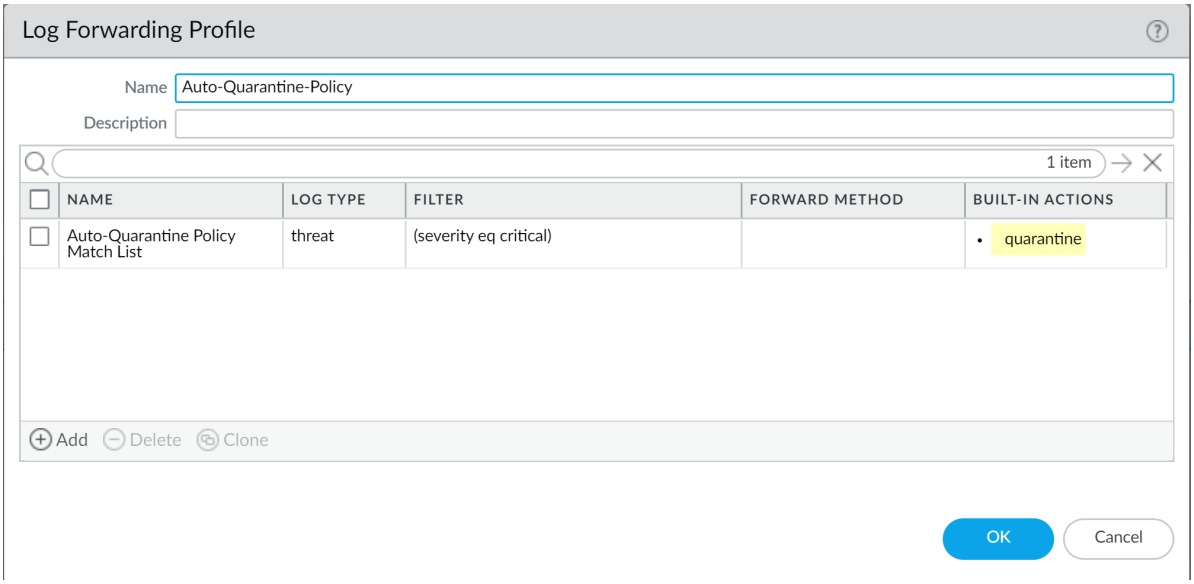
     Si especifica un tipo de log de amenazas o tráfico, asegúrese de que un ID de host esté asociado con un dispositivo. Para ello, cree una regla de la política de seguridad que tenga Quarantine (Cuarentena) como Source Device (Dispositivo de origen) para el tráfico de origen con el fin de añadir el ID de host. Sin un ID de host, no podrá añadir un dispositivo a la lista de cuarentena.

© 2020 Palo Alto Networks, Inc.

En el siguiente ejemplo se utiliza un **tipo de log** de **amenazas** y una gravedad crítica. Después de añadir este perfil a una política de seguridad y que los criterios coincidan, el cortafuegos añadirá dispositivos desde donde se originó el tráfico a la lista de cuarentena.

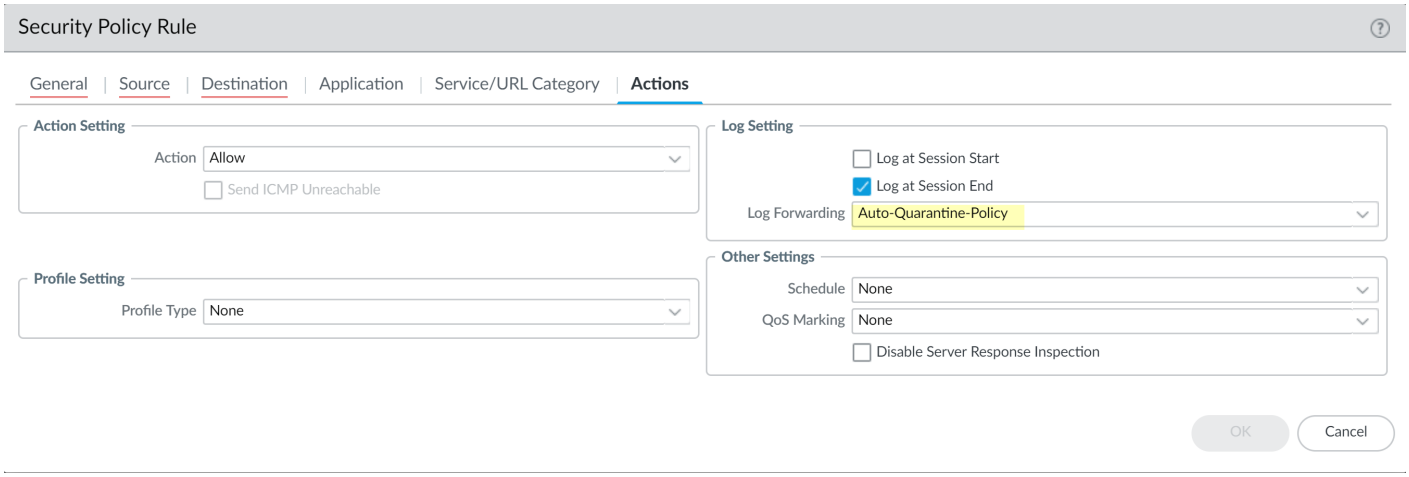


Después de añadir la lista de coincidencias, el perfil de reenvío de logs muestra **Quarantine (Cuarentena)** en **Built-In Actions (Acciones integradas)**.



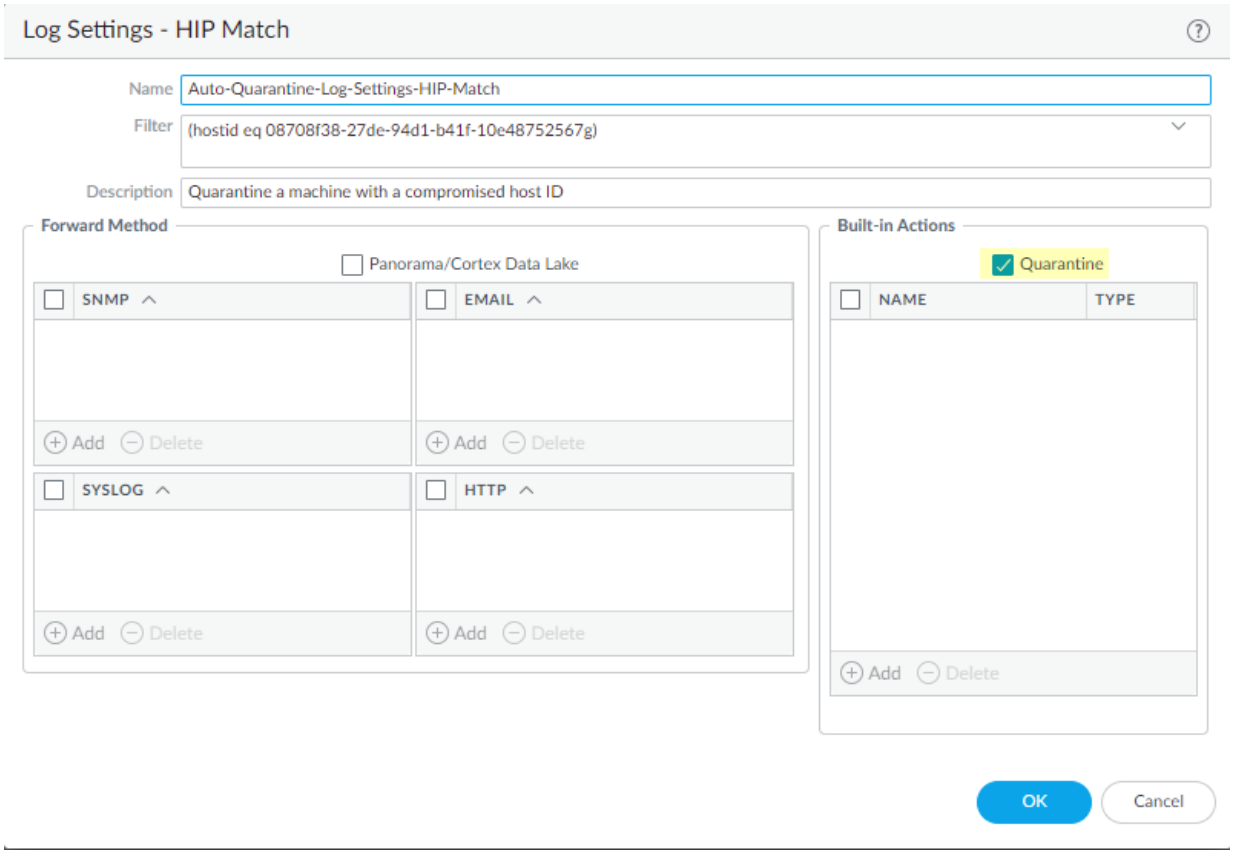
3. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)** para añadir una política de seguridad.
4. Seleccione **Actions (Acciones)** y, a continuación, seleccione el perfil de **Log Forwarding (Reenvío de logs)** que creó.

© 2020 Palo Alto Networks, Inc.



- Para poner en cuarentena automáticamente un dispositivo mediante la configuración de log de coincidencias HIP, seleccione **Device (Dispositivo)** > **Log Settings (Configuración de log)** > **HIP Match (Coincidencias HIP)** y **añada** una configuración de log con **Built-In Actions (Acciones integradas)** de **Quarantine (Cuarentena)**.

  La siguiente configuración de log tiene un **filtro** con un ID de host de 08708f38-27de-94d1-b41f-10e48752567g. Si los logs de coincidencias HIP detectan una coincidencia para ese ID de host, esta configuración de log añade ese dispositivo a la lista de cuarentena. A diferencia de un perfil de reenvío de logs, no es necesario adjuntar esta configuración de log a una política de seguridad para que surta efecto.

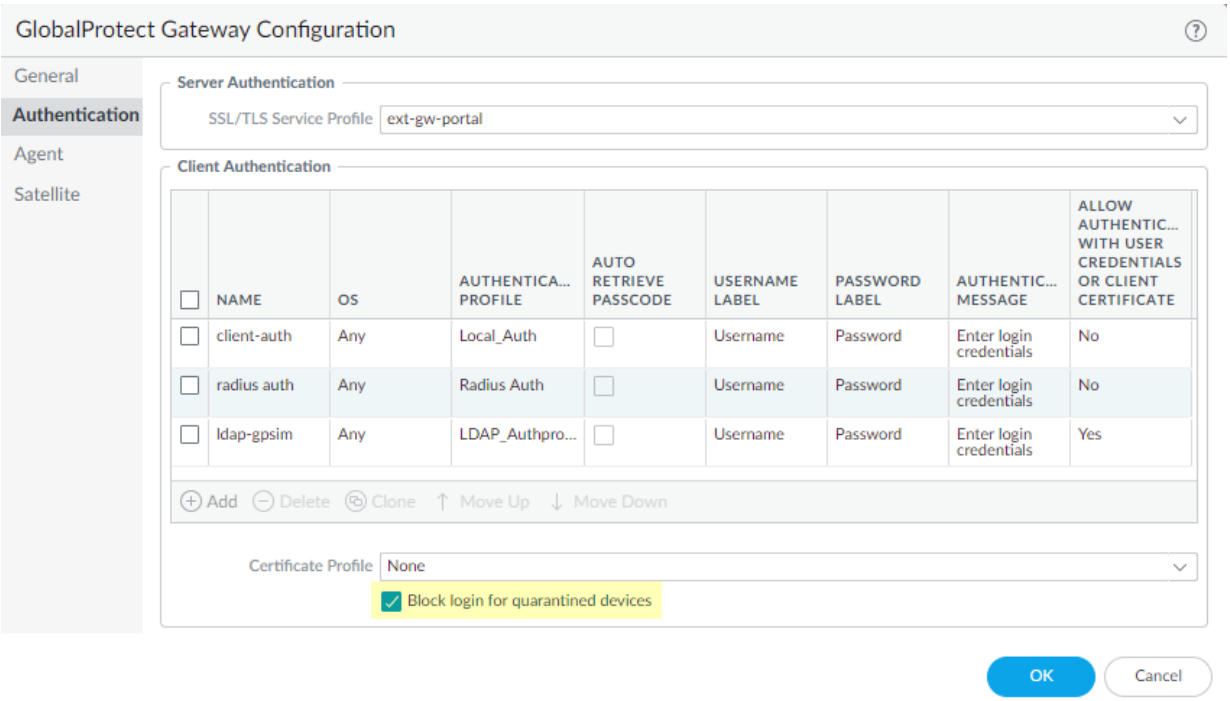


© 2020 Palo Alto Networks, Inc.

Uso de políticas de seguridad y de GlobalProtect para bloquear el acceso a los dispositivos en cuarentena

Puede configurar la autenticación de la puerta de enlace para evitar que los usuarios inicien sesión en GlobalProtect desde un dispositivo en cuarentena. Además, puede bloquear un dispositivo en cuarentena para que no envíe o reciba tráfico en la red. Para ello, especifique las opciones en una regla de política de seguridad. Utilice las siguientes tareas para bloquear usuarios de GlobalProtect o gestionar el acceso a la red para un dispositivo en cuarentena.

- Para impedir que los usuarios inicien sesión en GlobalProtect desde un dispositivo en cuarentena, configure la autenticación de la puerta de enlace de GlobalProtect (**Network [Red]** > **GlobalProtect** > **Gateways [Puertas de enlace]** > *gateway-configuration (configuración de puerta de enlace)* > **Authentication [Autenticación]**) y seleccione **Block login for quarantined devices (Bloquear inicio de sesión para dispositivos en cuarentena)**.



Si un usuario intenta iniciar sesión desde un dispositivo en cuarentena a una puerta de enlace que tiene **Block login for quarantined devices (Bloquear inicio de sesión para dispositivos en cuarentena)** habilitado, la aplicación de GlobalProtect notifica al usuario que el dispositivo está en cuarentena y que el usuario no puede iniciar sesión desde ese dispositivo. Si esta configuración no está habilitada, el usuario recibe la notificación pero puede iniciar sesión desde ese dispositivo.

- Para bloquear el acceso desde un dispositivo en cuarentena mediante una regla de la política de seguridad, especifique **Quarantine (Cuarentena)** para el tráfico de origen o de destino; a continuación, especifique una acción que bloquee el dispositivo en cuarentena.

  Especifique**Quarantine (Cuarentena)** en una regla de la política de seguridad significa que la regla utiliza dispositivos en la lista de cuarentena como criterio de coincidencia, tanto si especifica **Quarantine (Cuarentena)** como **Source Device (Dispositivo de origen)** para el tráfico de **origen** o **Destination Device (Dispositivo de destino)** para el tráfico de **destino**. En el siguiente ejemplo se muestra un **dispositivo** de origen de **Quarantine (Cuarentena)**, una dirección IP de destino del servidor HQ y una acción de **Deny**

© 2020 Palo Alto Networks, Inc.

(Denegar). Con esta regla de la política de seguridad, los dispositivos de la lista de cuarentena no podrán acceder al servidor HQ.

				Source				Destination					
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
26	Block-quarantined-devices-from-HQ-server	none	universal	any	any	any	quarantine	any	HQ-server	any	any	any	Deny
27	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
28	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Para que un dispositivo en cuarentena sea válido en una política en un cortafuegos, un usuario de GlobalProtect debe iniciar sesión correctamente en GlobalProtect desde el dispositivo en cuarentena, y el cortafuegos debe ser consciente de ese evento de inicio de sesión. Si el cortafuegos está configurado como una puerta de enlace de GlobalProtect, el usuario puede iniciar sesión en esa puerta de enlace desde el dispositivo en cuarentena para validar el dispositivo en la política. Después de que un usuario inicia sesión correctamente en una puerta de enlace desde un dispositivo en cuarentena, la puerta de enlace aplica la política y usted podrá redistribuir la información del dispositivo en cuarentena *y hacer que se aplique en una política en cualquier cortafuegos o puerta de enlace de su red. Si el usuario no puede iniciar sesión en la puerta de enlace (por ejemplo, si ha seleccionado Block login for quarantined devices [Bloquear inicio de sesión para dispositivos en cuarentena] en la configuración de la puerta de enlace), el inicio de sesión no se cuenta como un inicio de sesión correcto.*

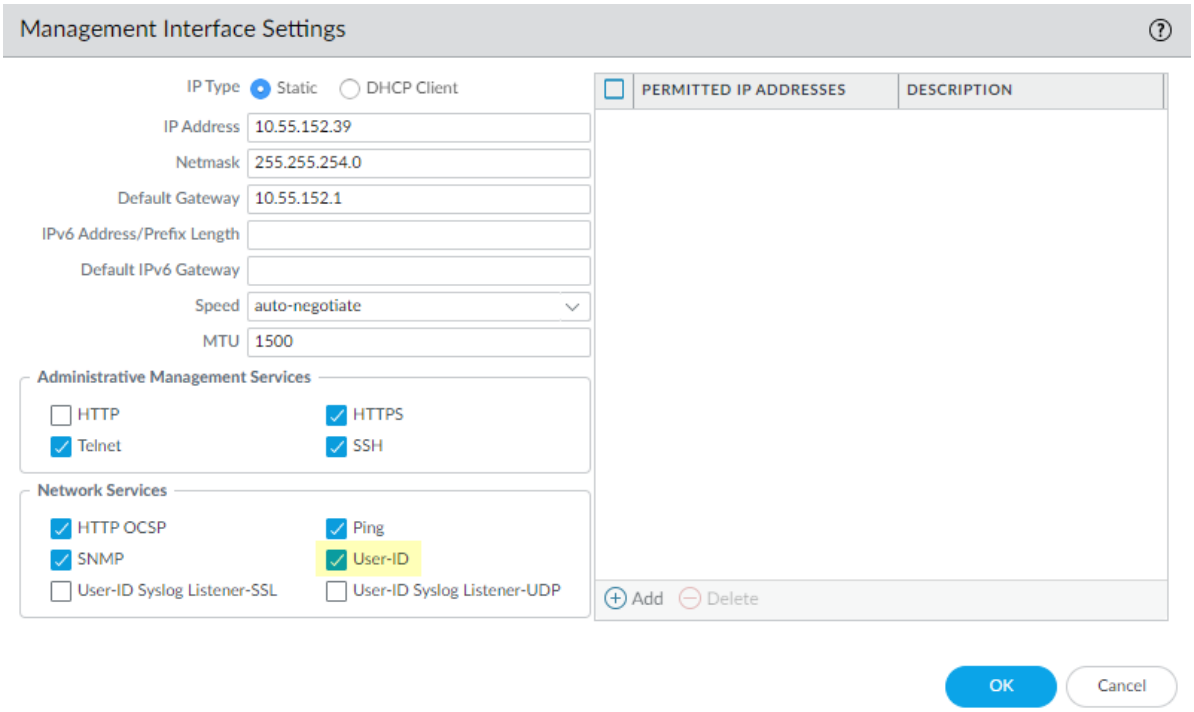
Redistribución de la información de cuarentena del dispositivo desde Panorama

Si gestiona sus cortafuegos de nueva generación con un dispositivo Panorama, puede crear una lista de cuarentena para todos los cortafuegos en **Panorama** > **Device Quarantine (Cuarentena del dispositivo)** y distribuir la información a sus cortafuegos gestionados. Redistribuya la información de cuarentena del dispositivo de la misma manera que redistribuye la información de User-ID. Complete los siguientes pasos para redistribuir la información de cuarentena de Panorama.

STEP 1 | Habilite User-ID en el servidor del agente si aún no lo ha hecho.

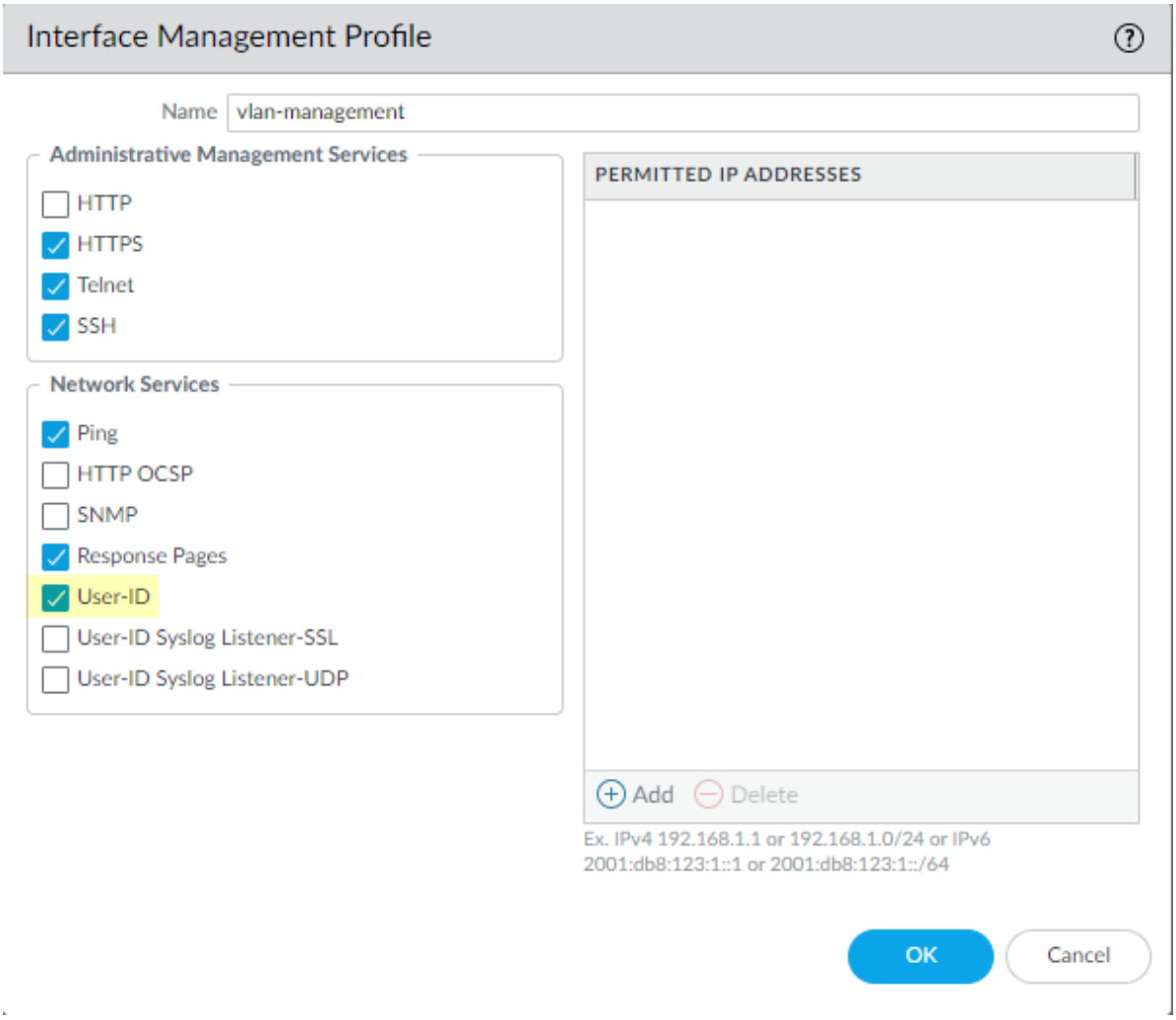
- Si el servidor del agente de redistribución usa la interfaz de gestión, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Interfaces (Interfaces)** > **Management (Gestión)** y elija **User-ID**.

© 2020 Palo Alto Networks, Inc.



- Si el agente de redistribución usa una interfaz en el plano de datos (por ejemplo, una interfaz Ethernet o VLAN), seleccione **Network (Red)** > **Interface Mgmt (Gestión de la interfaz)**, elija un perfil de gestión existente o **añada** uno nuevo y seleccione **User-ID**.

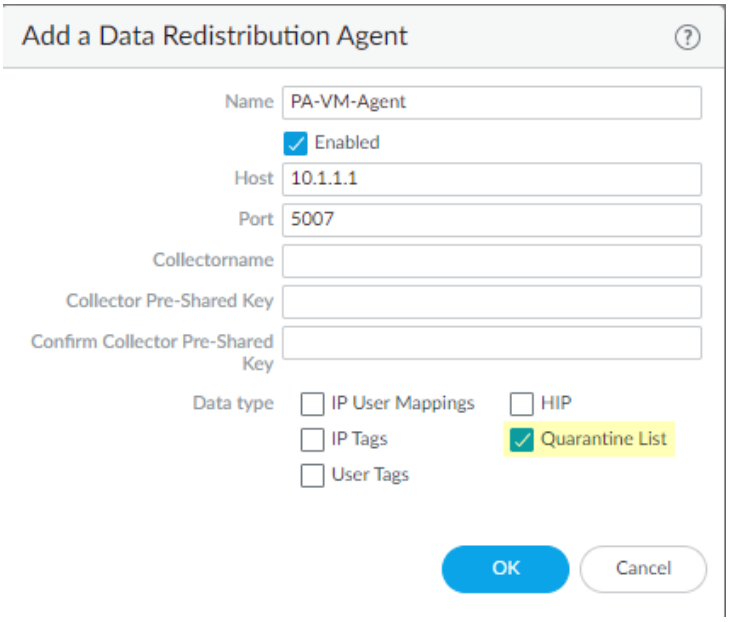
© 2020 Palo Alto Networks, Inc.



STEP 2 | Para crear un agente de redistribución de datos, seleccione **Panorama** > **Data Redistribution (Redistribución de datos)** y **añada** el agente.

El siguiente ejemplo muestra un agente de redistribución de datos en el que Panorama distribuye la información de la **lista de cuarentena** al cortafuegos con una dirección IP de 10.1.1.1 mediante el puerto 5007.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Certificaciones

Cuando habilita el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC), la aplicación de GlobalProtect™ para endpoints con Windows y macOS cumplen los requisitos de estos estándares (FIPS 140-2 y CC). Estas certificaciones de seguridad garantizan que se aplica un conjunto estándar de garantías y funciones de seguridad. Además, las suelen exigir tanto organismos públicos como otros órganos nacionales e internacionales de control de sectores regulados. Para obtener más información sobre las certificaciones de los productos y la validación externa, consulte la página de certificaciones de Palo Alto Networks.

Consulte las siguientes secciones para obtener información sobre cómo configurar la aplicación de GlobalProtect para terminales con Windows y macOS en el modo FIPS-CC y sobre cómo solucionar posibles problemas:

- Habilitación y verificación del modo FIPS-CC
- Funciones de seguridad de FIPS-CC
- Solución de problemas del modo FIPS-CC

© 2020 Palo Alto Networks, Inc.

Habilitación y verificación del modo FIPS-CC

Puede habilitar y verificar el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC) en la aplicación de GlobalProtect con uno de estos métodos:

- Habilitación y verificación del modo FIPS-CC con el registro de Windows
- Habilitación y verificación del modo FIPS-CC con la lista de propiedades de macOS

Para modificar el registro de Windows o la lista de propiedades de macOS, debe tener cuenta de administrador en Windows o en macOS, respectivamente.

Habilitación y verificación del modo FIPS-CC con el registro de Windows

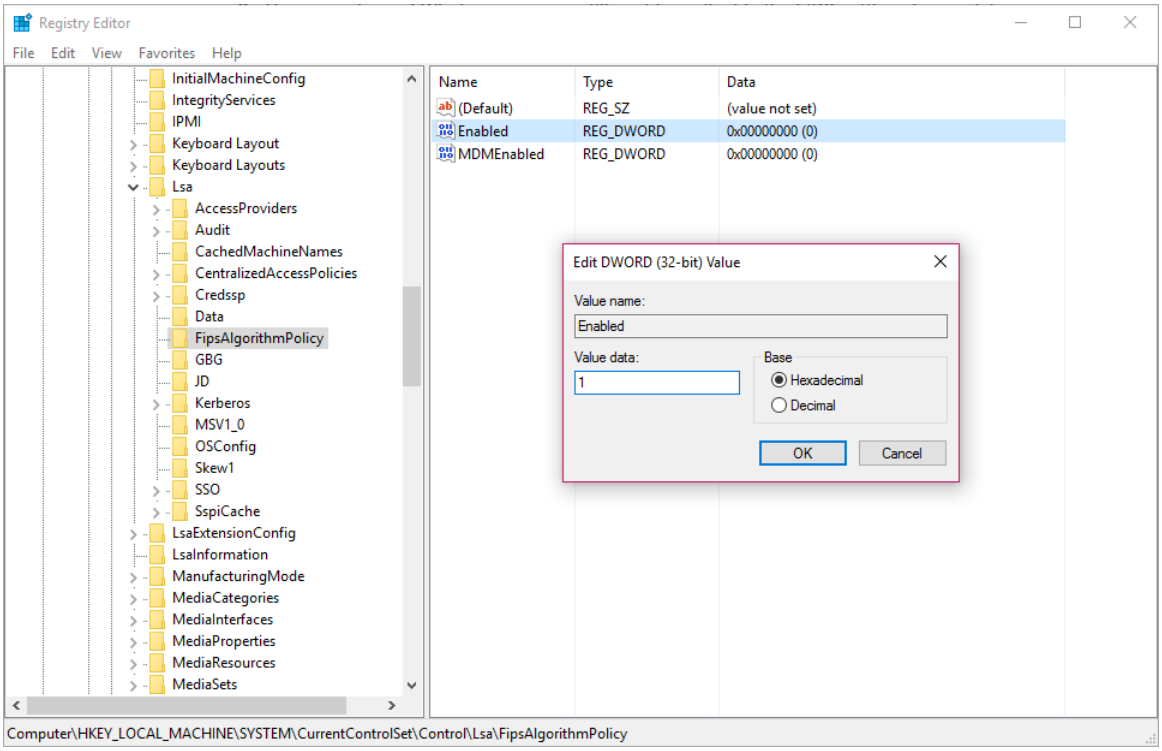
En los terminales con Windows, para habilitar y verificar el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC) en GlobalProtect™ con el registro de Windows, siga estos pasos:

STEP 1 | Habilite el modo FIPS en el sistema operativo Windows.

Si desea habilitar el modo FIPS-CC en GlobalProtect, habilite primero el modo FIPS en el sistema operativo Windows para comprobar si el terminal cumple los estándares FIPS 140-2.

1. Inicie el símbolo del sistema.
2. Introduzca **`regedit`** para abrir el registro de Windows.
3. En el registro de Windows, vaya a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\`.
4. Haga clic con el botón derecho en el valor de registro **Enabled (Habilitado)** y seleccione **Modify (Modificar)** para editarlo.
5. Para habilitar el modo FIPS, defina **`1`** en **Value Data (Información del valor)**. El valor predeterminado de **`0`** indica que el modo FIPS está deshabilitado.

© 2020 Palo Alto Networks, Inc.



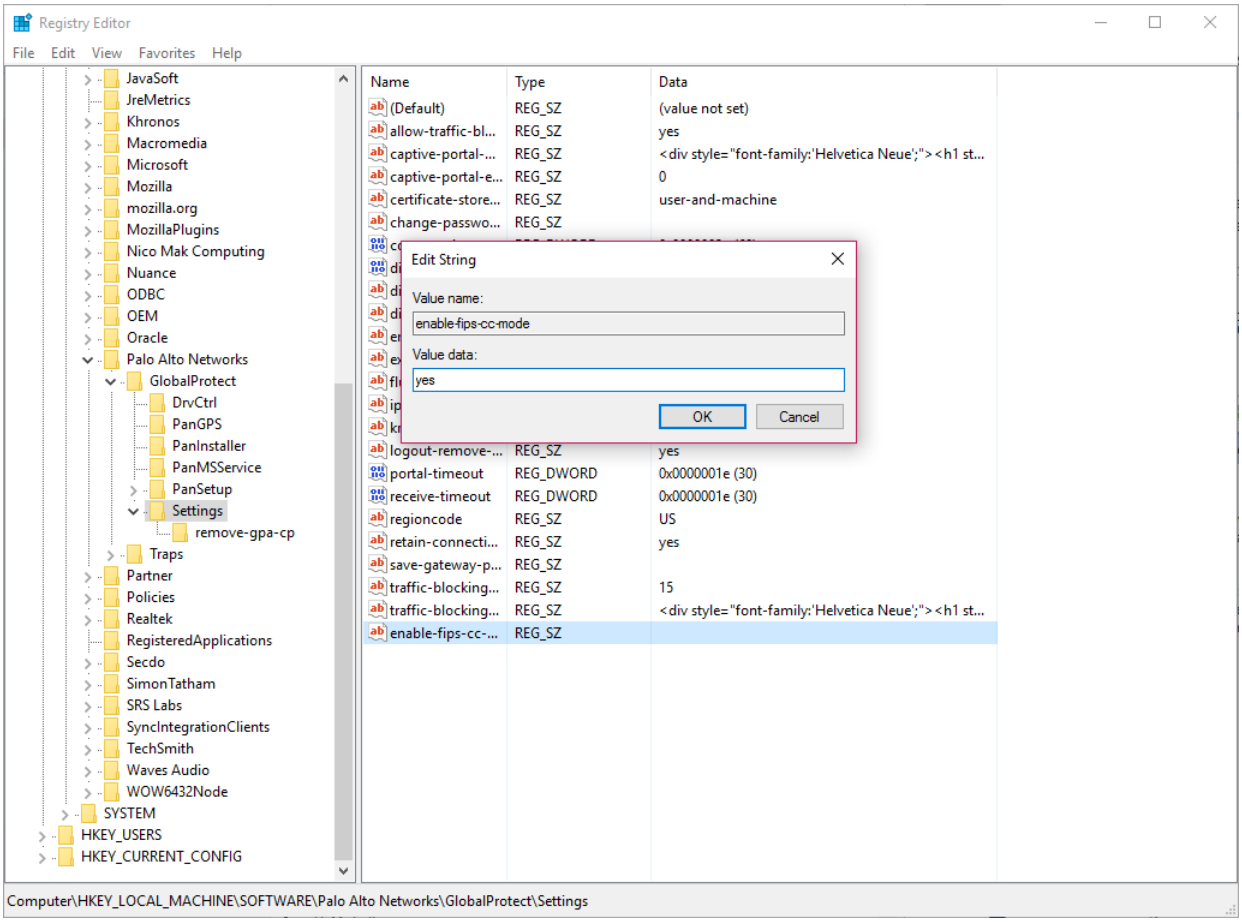
6. Haga clic en **OK (Aceptar)**.
7. Reinicie el terminal.

STEP 2 | Habilite el modo FIPS-CC en GlobalProtect.

No puede deshabilitar el modo FIPS-CC después de habilitarlo. Si los usuarios finales no desean ejecutar GlobalProtect en este modo, deben desinstalar la aplicación y volver a instalarla a continuación. De esa forma, se borra la configuración del modo FIPS-CC del registro de Windows.

1. Inicie el símbolo del sistema.
2. Introduzca **`regedit`** para abrir el registro de Windows.
3. En el registro de Windows, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`.
4. Haga clic en **Edit (Edición)** y seleccione **New (Nuevo)** > **String Value (Valor de cadena)**.
5. Cuando se le indique, especifique **`enable-fips-cc-mode`** como nombre del nuevo valor de registro.
6. Haga clic con el botón derecho en el nuevo valor de registro y seleccione **Modify (Modificar)** para editarlo.
7. Para habilitar el modo FIPS-CC, defina **`yes (sí)`** en **Value Data (Información del valor)**.
8. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

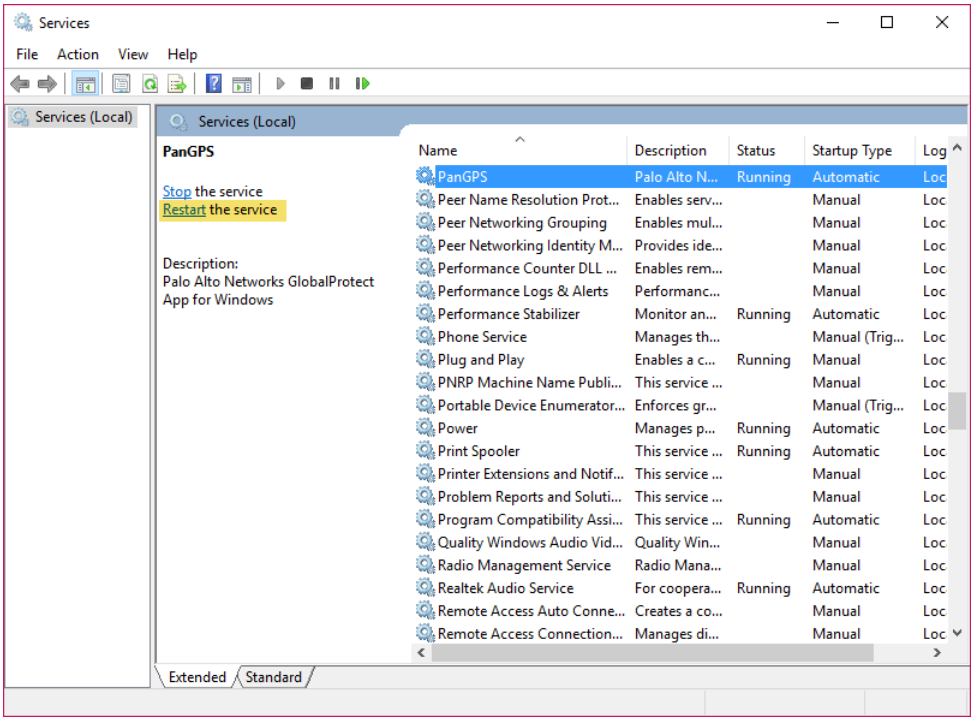


STEP 3 | Reinicie GlobalProtect.

Para que la aplicación de GlobalProtect se inicialice en el modo FIPS-CC, reinicie GlobalProtect con uno de estos métodos:

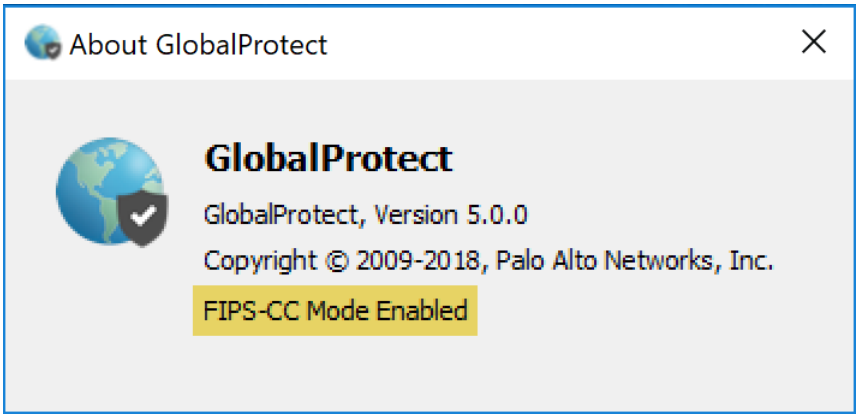
- Reinicie el terminal.
- Reinicie la aplicación de GlobalProtect y el servicio GlobalProtect (PanGPS):
  1. Inicie el símbolo del sistema.
  2. Introduzca **`services.msc`** para abrir el administrador de servicios de Windows.
  3. En la lista Services (Servicios), seleccione **PanGPS**.
  4. Haga clic en **Restart the service (Reiniciar el servicio)**.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Verifique que el modo FIPS-CC está habilitado en la aplicación de GlobalProtect.

1. Inicie la aplicación de GlobalProtect.
2. En el panel de estado, haga clic en para abrir el cuadro de diálogo de configuración.
3. Seleccione **About (Acerca de)**.
4. Verifique que el modo FIPS-CC está habilitado. Si es así, el cuadro de diálogo de información muestra el estado `FIPS-CC Mode Enabled (Modo FIPS-CC habilitado)`.



Habilitación y verificación del modo FIPS-CC con la lista de propiedades de macOS

En los terminales con macOS, para habilitar y verificar el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC) en GlobalProtect™ con la lista de propiedades de macOS, siga estos pasos:

© 2020 Palo Alto Networks, Inc.

Para habilitar el modo FIPS-CC en GlobalProtect, el terminal con macOS debe cumplir los estándares FIPS 140-2. El modo FIPS está habilitado de forma predeterminada en los endpoints macOS que ejecutan el sistema operativo macOS 10.8 y las versiones posteriores.

STEP 1 | Abra el archivo de lista de propiedades de GlobalProtect y busque los ajustes de personalización de GlobalProtect.

1. Inicie un editor de la lista de propiedades, como Xcode.
2. En el editor plist, abra el siguiente archivo plist: `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`.
3. Localice el diccionario de configuración de GlobalProtect: `/Palo Alto Networks/GlobalProtect/Settings`.

   Si no existe el diccionario de configuración, créelo. Puede añadir cada una de las claves en forma de cadena.

STEP 2 | Habilite el modo FIPS-CC en GlobalProtect.

No puede deshabilitar FIPS-CC después de habilitarlo. Si los usuarios finales no desean ejecutar GlobalProtect en este modo, deben desinstalar la aplicación y volver a instalarla a continuación. De esa forma, se borra la configuración del modo FIPS-CC de la lista de propiedades de macOS.

En el diccionario de configuración, añada el siguiente par de clave y valor para habilitar el modo FIPS-CC:

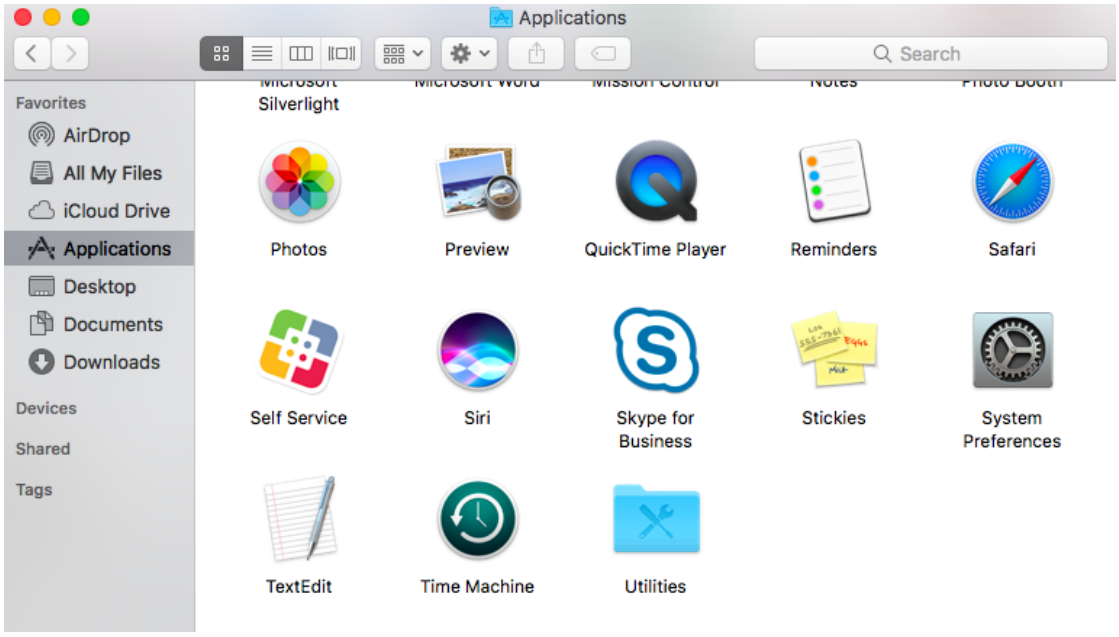
```
<key>enable-fips-cc-mode</key>
<string>yes (sí)</string>
```

STEP 3 | Reinicie GlobalProtect.

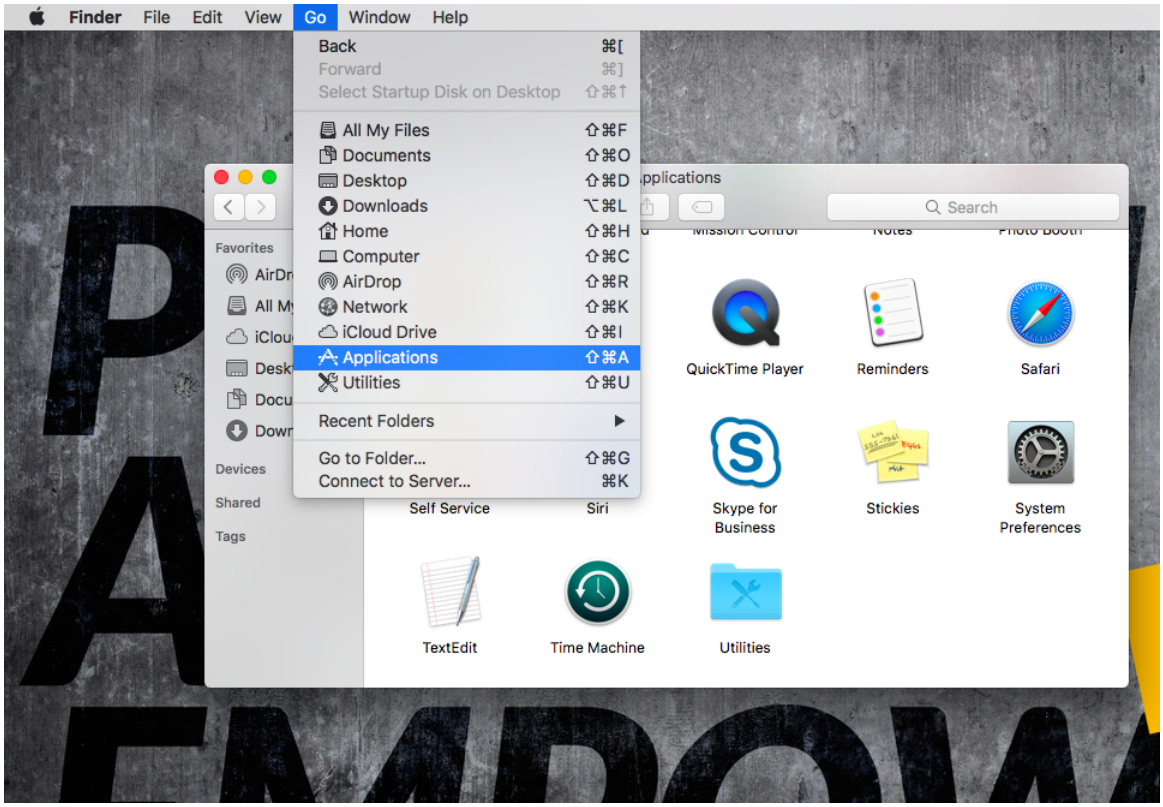
Para que la aplicación de GlobalProtect se inicialice en el modo FIPS-CC, reinicie GlobalProtect con uno de estos métodos:

- Reinicie el terminal.
- Reinicie la aplicación de GlobalProtect y el servicio GlobalProtect (PanGPS):
  1. Inicie el Finder.
  2. Abra la carpeta Applications (Aplicaciones):
     - En la barra lateral del Finder, seleccione **Applications (Aplicaciones)**.

© 2020 Palo Alto Networks, Inc.



- Si no aparece **Applications (Aplicaciones)** en la barra lateral del Finder, seleccione **Go (Ir)** > **Applications (Aplicaciones)** en la barra de menús del Finder.



Para mostrar Applications (Aplicaciones) en la barra lateral del Finder, seleccione Finder > Preferences (Preferencias) en la barra de menús del Finder. En Finder Preferences (Preferencias del Finder), seleccione Sidebar (Barra lateral) y marque la opción para mostrar las aplicaciones.

3. Abra la carpeta Utilities (Utilidades).

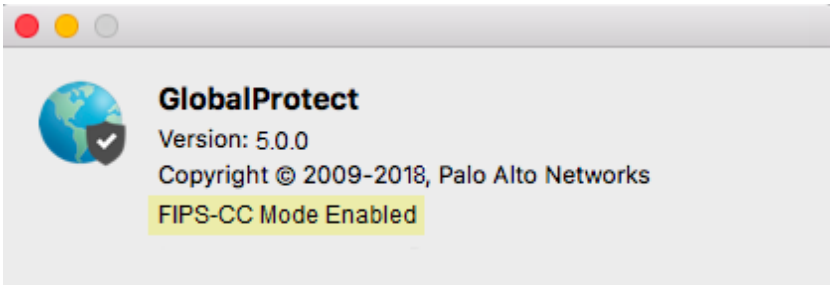
© 2020 Palo Alto Networks, Inc.

4. Inicie Terminal.
5. Ejecute los siguientes comandos:

```
username>$ launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist
```

STEP 4 | Verifique que el modo FIPS-CC está habilitado en la aplicación de GlobalProtect.

1. Inicie la aplicación de GlobalProtect.
2. En el panel de estado, haga clic en para abrir el cuadro de diálogo de configuración.
3. Seleccione **About (Acerca de)**.
4. Verifique que el modo FIPS-CC está habilitado. Si es así, el cuadro de diálogo de información muestra el estado `FIPS-CC Mode Enabled (Modo FIPS-CC habilitado)`.



© 2020 Palo Alto Networks, Inc.

Funciones de seguridad de FIPS-CC

Si habilita el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC) en GlobalProtect, se aplican las siguientes funciones de seguridad a la aplicación en los terminales con Windows y con macOS:

- Cifre todos los túneles de red privada virtual (virtual private network, VPN) entre la aplicación de GlobalProtect y las puertas de enlace mediante los protocolos de seguridad de capa de transporte (transport layer security, TLS) o de seguridad del protocolo de internet (internet protocol security, IPSec).
- Si configura un túnel de VPN de IPSec, debe seleccionar uno de los conjuntos de cifrado que se presentan durante la configuración de IPSec.
- Si configura un túnel de VPN de IPSec, especifique uno de los siguientes algoritmos de cifrado:
  - AES-CBC-128 (con el algoritmo de autenticación SHA1)
  - AES-GCM-128
  - AES-GCM-256
- Los certificados tanto de servidor como de cliente deben usar uno de los siguientes algoritmos de firma:
  - RSA de 2048 bits (o posterior)
  - ECDSA P-256
  - ECDSA P-384
  - ECDSA P-521

  Además, tiene que emplear SHA256, SHA384 o SHA512 como algoritmo de hash de firma.

© 2020 Palo Alto Networks, Inc.

Solución de problemas del modo FIPS-CC

Si se producen problemas tras habilitar el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC), consulte las siguientes secciones para solucionarlos:

- Consulta y recopilación de logs de GlobalProtect
- Solución de problemas del modo FIPS-CC

Consulta y recopilación de logs de GlobalProtect

Consulte los logs de GlobalProtect™ para ver más detalles sobre los problemas del modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC).

Para ver o recopilar los logs de GlobalProtect, siga estos pasos:

STEP 1 | Inicie la aplicación de GlobalProtect.

STEP 2 | En el panel de estado, haga clic en para abrir el cuadro de diálogo de configuración.

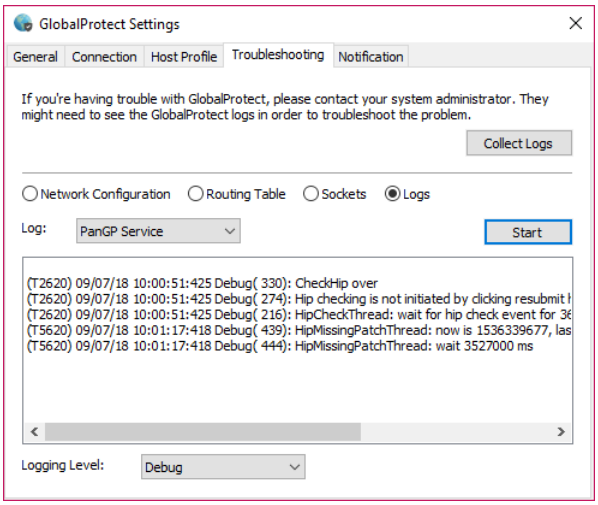
STEP 3 | Seleccione **Settings**.

STEP 4 | En el panel GlobalProtect Settings (Configuración de GlobalProtect), seleccione **Troubleshooting (Solución de problemas)**.

STEP 5 | Seleccione el valor oportuno en **Logging Level (Nivel de creación de logs)**.

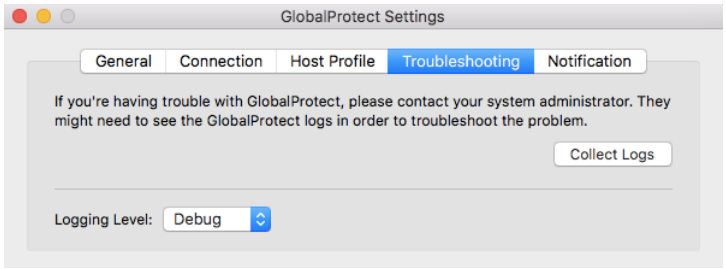
STEP 6 | (Opcional, solo en Windows) Para consultar los logs de GlobalProtect:

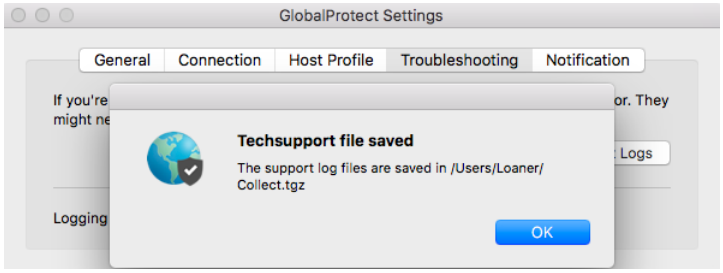
1. Marque **Logs**.
2. Seleccione el tipo en **Log**.
3. Haga clic en **Start (Iniciar)** para empezar a recopilar los logs.



STEP 7 | (Opcional) Haga clic en **Collect Logs (Recopilar logs)** para enviarlos al administrador de GlobalProtect que se encarga de solucionar los problemas.

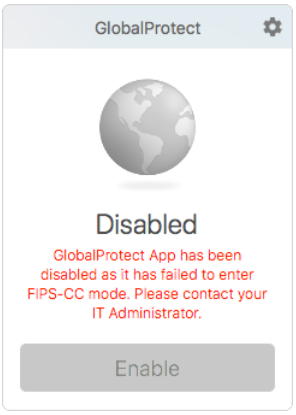
© 2020 Palo Alto Networks, Inc.



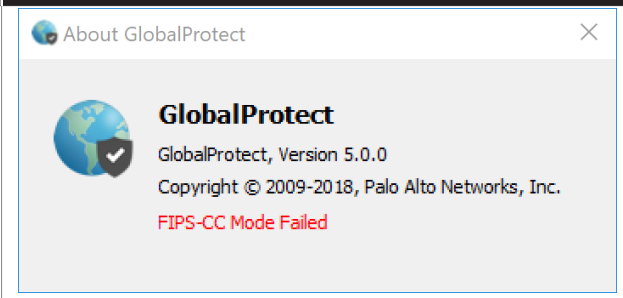


Solución de problemas del modo FIPS-CC

En la tabla siguiente se describen los problemas que se pueden producir en el modo de criterios comunes de los estándares estadounidenses de procesamiento de la información (Federal Information Processing Standards-Common Criteria, FIPS-CC) y sus correspondientes soluciones. Si surge otro problema, solicite ayuda al administrador de GlobalProtect™ para resolverlo.

Problema	Description (Descripción)	Solución
La aplicación de GlobalProtect no se inicializa en el modo FIPS-CC porque falla la prueba automática de encendido o la prueba de integridad de FIPS.	Si habilita el modo FIPS-CC, la aplicación de GlobalProtect ejecuta pruebas automáticas de encendido y pruebas de integridad de FIPS cuando se inicializa y cuando se reinician el sistema o la propia aplicación. Si cualquiera de ellas da un error, se deshabilita la aplicación de GlobalProtect y aparece la ventana de información con el mensaje de error `FIPS-CC Mode Failed (Error del modo FIPS-CC)`: 	Reinicie la aplicación para solucionar el error. Si aparece otra vez, desinstale la aplicación y vuelva a instalarla a continuación.

© 2020 Palo Alto Networks, Inc.

Problema	Description (Descripción)	Solución
		
La aplicación de GlobalProtect no logra establecer la conexión en el modo FIPS-CC porque falla la prueba condicional automática de FIPS.	Cuando la aplicación de GlobalProtect se inicializa en el modo FIPS-CC, ejecuta pruebas condicionales automáticas de FIPS. Si dan un error, la aplicación de GlobalProtect finaliza la sesión y permanece desconectada.	Para establecer la conexión de GlobalProtect, se tiene que volver a autenticar en el portal de GlobalProtect.

Si GlobalProtect no lograr inicializarse ni conectar en el modo FIPS-CC, vaya a la pestaña Troubleshooting (Solución de problemas) del panel GlobalProtect Settings (Configuración de GlobalProtect) para consultar y recopilar logs que faciliten la resolución. Las demás pestañas no están disponibles hasta que GlobalProtect se conecte.

© 2020 Palo Alto Networks, Inc.

Configuraciones rápidas de GlobalProtect

En la siguiente sección se proporcionan instrucciones detalladas para configurar algunas implementaciones comunes de GlobalProtect™:

> VPN de acceso remoto (Perfil de autenticación)
> VPN de acceso remoto (perfil del certificado)
> VPN de acceso remoto con autenticación en dos fases
> Configuración de VPN siempre activada
> VPN de acceso remoto con función anterior al inicio de sesión
> Configuración de varias puertas de enlace de GlobalProtect
> GlobalProtect para comprobación de HIP interna y acceso basado en usuario
> Configuración de puerta de enlace externa e interna combinada
> Portal cautivo y uso obligatorio de GlobalProtect para acceder a la red

Consulte el artículo de la base de conocimientos en https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGYCA0 para obtener información sobre cómo cambiar la contraseña de Active Directory mediante GlobalProtect.

© 2020 Palo Alto Networks, Inc.

VPN de acceso remoto (Perfil de autenticación)

En la VPN de GlobalProtect para acceso remoto, el portal y la puerta de enlace de GlobalProtect se configuran en **Ethernet1/2**, por lo que esta es la interfaz física donde se conectan los usuarios de GlobalProtect. Después de que un usuario se conecte y se autentique en el portal y en la puerta de enlace, el endpoint establece un túnel desde su adaptador virtual, al que se le ha asignado una dirección de IP en el grupo de direcciones IP asociado con la configuración tunnel.2 de la puerta de enlace, 10.31.32.3-10.31.32.118 en este ejemplo. Debido a que los túneles VPN de GlobalProtect terminan con una zona **`corp-vpn`** independiente, tendrá visibilidad sobre el tráfico de la conexión, así como la capacidad de adaptar las políticas de seguridad para usuarios remotos.

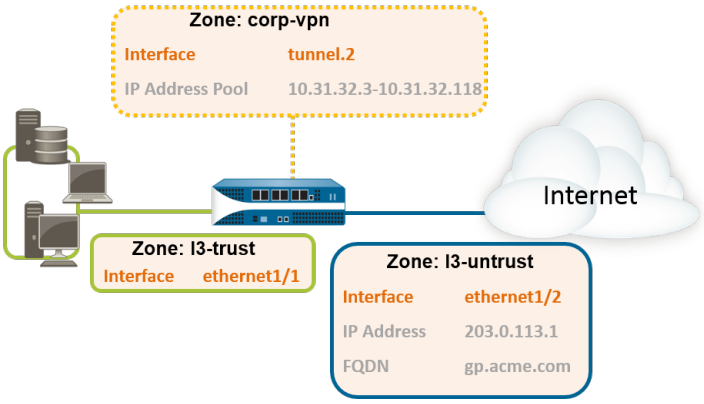


Figure 5: VPN de GlobalProtect para acceso remoto

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**. Configure **ethernet1/2** como interfaz de Ethernet de capa 3 con la dirección IP 203.0.113.1 y, luego, asígnela a la zona de seguridad **`l3-untrust`** y al enrutador predeterminado seleccionado en **Virtual Router (Enrutador virtual)**.
- Cree un registro "A" DNS que asigne la dirección IP **`203.0.113.1`** a **`gp.acme.com`**.
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir la interfaz **tunnel.2**. Haga clic en **Add (Añadir)** para añadir la interfaz de túnel a una zona de seguridad nueva denominada **`corp-vpn`** y, luego, asígnela al enrutador predeterminado seleccionado en **Virtual Router (Enrutador virtual)**.
- Habilite la identificación de usuario en la zona **`corp-vpn`**.

STEP 2 | Cree políticas de seguridad para habilitar el flujo de tráfico entre la zona **`corp-vpn`** y la zona **`l3-trust`**, y permitir el acceso a sus recursos internos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego, haga clic en **Add (Añadir)** para añadir una nueva regla.
2. Para este ejemplo, puede definir la regla con la siguiente configuración:
   - **Name (Nombre)** (pestaña **General**): acceso de VPN
   - **Source Zone (Zona de origen)** (pestaña **Source [Origen]**): corp-vpn
   - **Destination Zone (Zona de destino)** (pestaña **Destination [Destino]**): l3-trust

© 2020 Palo Alto Networks, Inc.

	Name	Tags	Source				Destination		Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address			
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | Use uno de los siguientes métodos para obtener un certificado de servidor para la interfaz que aloja el portal y la puerta de enlace de GlobalProtect:

- (Recomendado) Importación de un certificado de servidor desde una CA externa conocida.
- Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado.

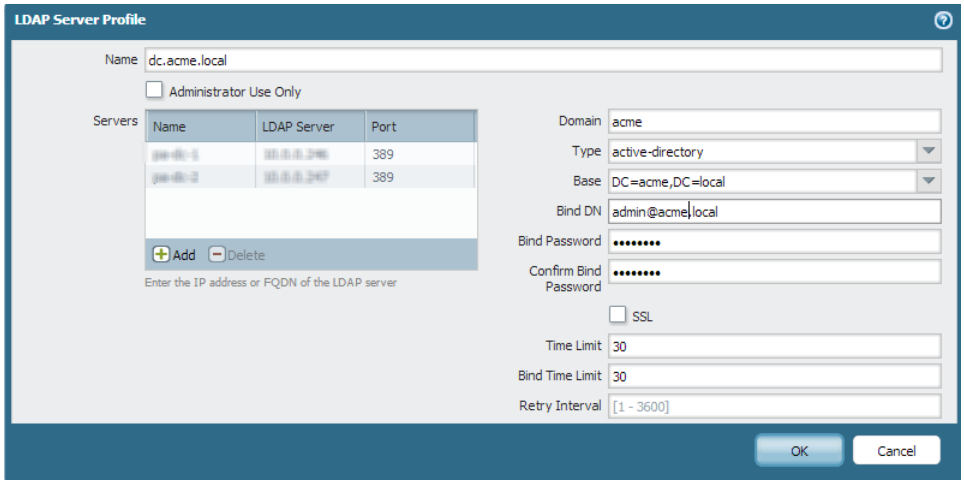
Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** para gestionar los certificados de la siguiente manera:

- Obtenga un certificado de servidor. Como el portal y la puerta de enlace se encuentran en la misma interfaz, se puede utilizar el mismo certificado de servidor para ambos componentes.
- El CN del certificado debe coincidir con el FQDN, gp.acme.com.
- Para permitir a los usuarios conectarse con el portal sin que reciban errores de certificado, utilice un certificado de servidor desde una CA pública.

STEP 4 | Cree un perfil de servidor.

El perfil de servidor indica al cortafuegos cómo conectarse al servicio de autenticación. Los métodos de autenticación Local, RADIUS, Kerberos, SAML y LDAP son compatibles. En este ejemplo se muestra un perfil de autenticación LDAP para autenticar a los usuarios con respecto a Active Directory.

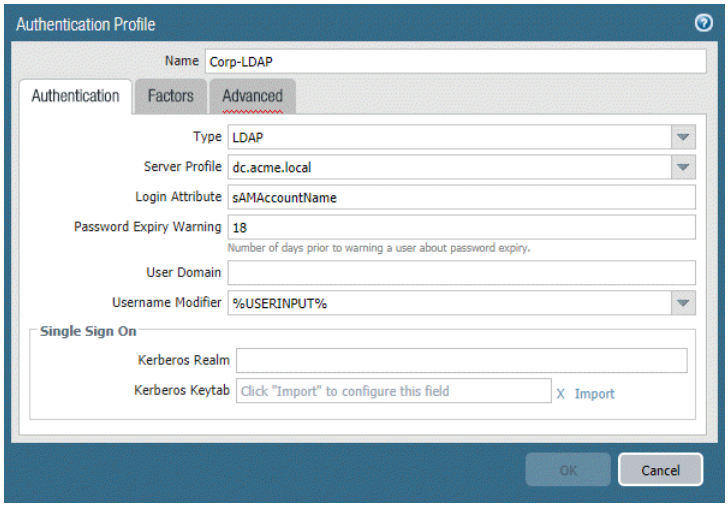
Cree el perfil de servidor para conectarse al servidor LDAP (**Device [Dispositivo]** > **Server Profiles [Perfiles de servidor]** > **LDAP**).



STEP 5 | (Opcional) Cree un perfil de autenticación.

Instale el perfil del servidor en un perfil de autenticación (**Device [Dispositivo]** > **Authentication Profile [Perfil de autenticación]**).

© 2020 Palo Alto Networks, Inc.



STEP 6 | Configuración de una puerta de enlace de GlobalProtect.

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración:

Interface (Interfaz): `ethernet1/2`

IP Address (Dirección IP): `203.0.113.1`

Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

Authentication Profile (Perfil de autenticación): `Corp-LDAP`

Tunnel Interface (Interfaz de túnel): `tunnel.2`

IP Pool (Grupo de IP): `10.31.32.3 - 10.31.32.118`

STEP 7 | Configure los Portales de GlobalProtect.

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración:

1. Configuración del acceso al portal de GlobalProtect:

   Interface (Interfaz): `ethernet1/2`

   IP Address (Dirección IP): `203.0.113.1`

   Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

   Authentication Profile (Perfil de autenticación): `Corp-LDAP`
2. Definición de las configuraciones de autenticación de cliente de GlobalProtect:

   Connect Method (Método de conexión): `On-demand` (conexión manual iniciada por el usuario).

   External Gateway Address (Dirección de puerta de enlace externa): `gp.acme.com`

STEP 8 | Implementación del software de la aplicación de GlobalProtect

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)**. Siga el procedimiento para alojar actualizacioes de la aplicación en el portal.

STEP 9 | (Optativo) Permita el uso de la aplicación móvil de GlobalProtect.

Adquiera e instale una suscripción a GlobalProtect (**Device [Dispositivo]** > **Licenses [Licencias]**) para habilitar el uso de la aplicación.

© 2020 Palo Alto Networks, Inc.

STEP 10 | Guarde la configuración de GlobalProtect.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

VPN de acceso remoto (perfil del certificado)

Con la autenticación de certificado, el usuario debe presentar un certificado de cliente válido que lo identifique en el portal o puerta de enlace de GlobalProtect. Para verificar que un certificado de cliente es válido, el portal o la puerta de enlace verifican si el cliente tiene la clave privada del certificado mediante el mensaje de verificación de certificado intercambiado durante el protocolo de enlace SSL. Además, el certificado del cliente está firmado por la entidad de certificación (CA, Certificate Authority) especificada en el campo **Issuer (Emisor)** de la cadena de certificados. Además del certificado en sí, el portal o la puerta de enlace pueden usar un perfil de certificado para determinar si el usuario que envió el certificado es el usuario para el cual se emitió el certificado.

Cuando un certificado es el único método de autenticación, el certificado que presenta el usuario debe contener el nombre de usuario en uno de los campos de certificado; normalmente, el nombre de usuario corresponde al nombre común (common name, CN) del campo Subject (Asunto) del certificado.

Cuando la autenticación es correcta, la aplicación de GlobalProtect establece un túnel con la puerta de enlace y se le asigna una dirección IP desde el grupo de IP en la configuración de túnel de la puerta de enlace. Para admitir la aplicación de políticas basadas en el usuario en sesiones de la zona **`corp-vpn`**, el nombre de usuario del certificado se asigna a la dirección IP asignada por la puerta de enlace. Si una política de seguridad exige un nombre de dominio además del nombre de usuario, el valor de dominio especificado en el perfil del certificado se anexa al nombre de usuario.

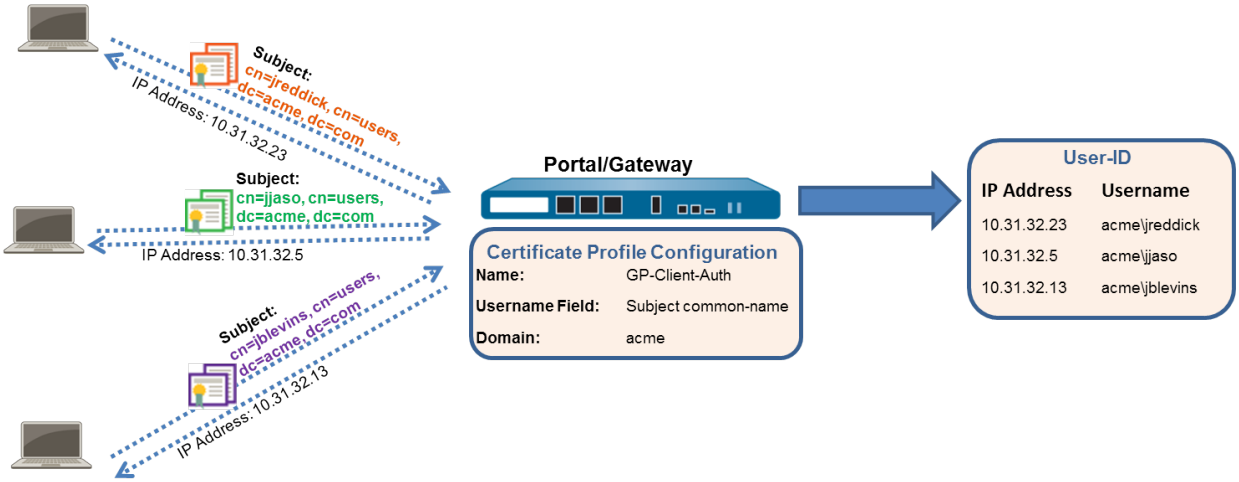


Figure 6: Configuración de autenticación del certificado de cliente de GlobalProtect

Esta configuración rápida usa la misma topología que VPN de GlobalProtect para acceso remoto. La única diferencia de configuración es que, en lugar de autenticar a los usuarios con respecto a un servidor de autenticación, esta configuración utiliza solo la autenticación del certificado de cliente.

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**. Configure **ethernet1/2** como la interfaz de Ethernet de capa 3 con la dirección IP **`203.0.113.1`** y luego asígnela a la **Security Zone (Zona de seguridad)** **`l3-untrust`** y al **Virtual Router (Enrutador virtual)** predeterminado.

© 2020 Palo Alto Networks, Inc.

- Cree un registro “A” DNS que asigne la dirección IP **`203.0.113.1`** a **`gp.acme.com`**.
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir la interfaz **tunnel.2**. Añada la interfaz del túnel a una nueva **Security Zone (Zona de seguridad)** llamada `corp-vpn` y, luego, asígnela al **Virtual Router (Enrutador virtual)** predeterminado.
- Habilite la identificación de usuario en la zona **`corp-vpn`**.

STEP 2 | Cree políticas de seguridad para habilitar el flujo de tráfico entre la zona **`corp-vpn`** y la zona **`l3-trust`**, y permitir el acceso a sus recursos internos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego, haga clic en **Add (Añadir)** para añadir una nueva regla.
2. Para este ejemplo, puede definir la regla con la siguiente configuración:
   - **Name (Nombre)** (pestaña **General**): **`VPN Access`**
   - **Source Zone (Zona de origen)** (pestaña **Source [Origen]**): **`corp-vpn`**
   - **Destination Zone (Zona de destino)** (pestaña **Destination [Destino]**): **`l3-trust`**

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | Use uno de los siguientes métodos para obtener un certificado de servidor para la interfaz que aloja el portal y la puerta de enlace de GlobalProtect:

- (Recomendado) Importación de un certificado de servidor desde una CA externa conocida.
- Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado.

Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** para gestionar los certificados de la siguiente manera:

- Obtenga un certificado de servidor. Como el portal y la puerta de enlace se encuentran en la misma interfaz, se puede utilizar el mismo certificado de servidor para ambos componentes.
- El CN del certificado debe coincidir con el FQDN, gp.acme.com.
- Para permitir a los usuarios conectarse con el portal sin que reciban errores de certificado, utilice un certificado de servidor desde una CA pública.

STEP 4 | Emita certificados de cliente para clientes y endpoints de GlobalProtect.

1. Utilice su PKI empresarial o CA pública para emitir un certificado de cliente único para cada usuario de GlobalProtect.
2. Instale certificados en el almacén de certificados personales de los endpoints.

STEP 5 | Cree un perfil de certificado de cliente.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de certificado y luego, introduzca un **Name (Nombre)** de perfil como **`GP-client-cert`**.
2. Seleccione **Subject (Asunto)** en el menú desplegable **Username Field (Campo de nombre de usuario)**.
3. En el área **CA Certificates (Certificados de CA)**, haga clic en **Add (Añadir)** para añadir el certificado de CA que emitió los certificados de cliente. Haga clic en **OK** dos veces.

STEP 6 | Configuración de una puerta de enlace de GlobalProtect.

Vea el diagrama de topología que se muestra en VPN de GlobalProtect para acceso remoto.

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración:

© 2020 Palo Alto Networks, Inc.

Interface (Interfaz): `ethernet1/2`

IP Address (Dirección IP): `203.0.113.1`

Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

Certificate Profile (Perfil del certificado): `GP-client-cert`

Tunnel Interface (Interfaz de túnel): `tunnel.2`

IP Pool (Grupo de IP): `10.31.32.3 - 10.31.32.118`

STEP 7 | Configure los Portales de GlobalProtect.

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración:

1. Configuración del acceso al portal de GlobalProtect:

   Interface (Interfaz): `ethernet1/2`

   IP Address (Dirección IP): `203.0.113.1`

   Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

   Certificate Profile (Perfil del certificado): `GP-client-cert`
2. Definición de las configuraciones de agente de GlobalProtect:

   Connect Method (Método de conexión): `On-demand` (conexión manual iniciada por el usuario).

   External Gateway Address (Dirección de puerta de enlace externa): `gp.acme.com`

STEP 8 | Implementación del software de la aplicación de GlobalProtect

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)**. Siga el procedimiento para alojar actualizacioes de la aplicación en el portal.

STEP 9 | (Optativo) Permita el uso de la aplicación móvil de GlobalProtect.

Adquiera e instale una suscripción a GlobalProtect (**Device [Dispositivo]** > **Licenses [Licencias]**) para habilitar el uso de la aplicación.

STEP 10 | Guarde la configuración de GlobalProtect.

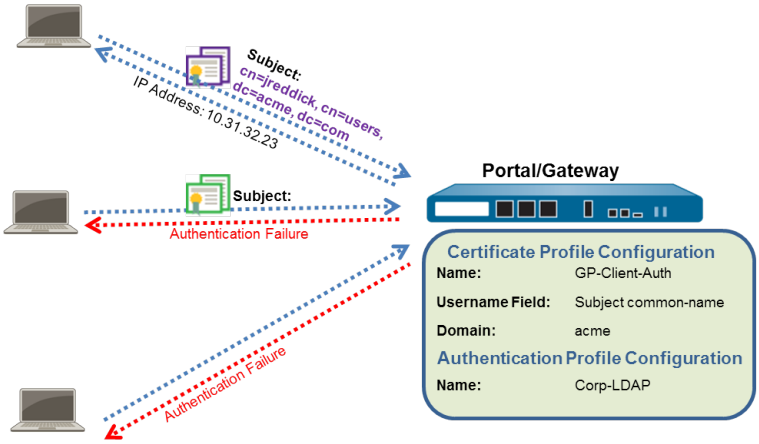
Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

VPN de acceso remoto con autenticación en dos fases

Si configura un portal o puerta de enlace de GlobalProtect con un perfil de autenticación y un perfil de certificado (los cuales, en conjunto, pueden proporcionar la autenticación en dos fases), el usuario final debe realizar correctamente la autenticación a través de ambos perfiles para obtener el acceso. En cuanto a la autenticación de portales, esto significa que los certificados deben implantarse previamente en endpoints antes de su conexión inicial al portal. Además, el certificado de cliente presentado por un usuario debe coincidir con lo definido en el perfil del certificado.

- Si el perfil del certificado no especifica un campo de nombre de usuario (es decir, **Username Field [Campo de nombre de usuario]** está definido como **None [Ninguno]**), el certificado de cliente no necesitará un nombre de usuario. En este caso, el usuario debe proporcionar el nombre de usuario cuando se autentique con el perfil de autenticación.
- Si el perfil del certificado especifica un campo de nombre de usuario, el certificado que presenta el usuario debe contener un nombre de usuario en el campo correspondiente. Por ejemplo, si el perfil del certificado especifica que el campo del nombre de usuario es **Subject (Asunto)**, el certificado presentado por el usuario debe contener un valor en el campo de nombre común o la autenticación fallará. Además, cuando se necesite el campo del nombre de usuario, el valor del campo de nombre de usuario del certificado se cumplimentará automáticamente con el nombre de usuario cuando el usuario trate de introducir las credenciales para la autenticación en el perfil de autenticación. Si no quiere obligar a los usuarios a autenticar con un nombre de usuario del certificado, no especifique ningún campo de nombre de usuario en el perfil del certificado.



Esta configuración rápida usa la misma topología que VPN de GlobalProtect para acceso remoto. Sin embargo, en esta configuración, los usuarios deben autenticarse con un perfil de certificado y un perfil de autenticación. Para obtener más detalles sobre un tipo específico de autenticación de dos factores, consulte los siguientes temas:

- Habilitación de la autenticación en dos fases con perfiles de autenticación y certificado
- Habilitación de la autenticación en dos fases mediante contraseñas de un solo uso (OTP)
- Habilitación de autenticación en dos fases mediante tarjetas inteligentes
- Habilitación de la autenticación de doble factor mediante una aplicación de token de software

© 2020 Palo Alto Networks, Inc.

Utilice el siguiente procedimiento para configurar el acceso remoto de VPN con la autenticación en dos fases.

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**. Configure **ethernet1/2** como la interfaz de Ethernet de **Layer3 (Capa 3)** con la dirección IP `203.0.113.1` y luego asígnela a la **Security Zone (Zona de seguridad)** `l3-untrust` y al **Virtual Router (Enrutador virtual)** predeterminado.
- Cree un registro "A" DNS que asigne la dirección IP `203.0.113.1` a `gp.acme.com`.
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir la interfaz **tunnel.2**. Añada la interfaz del túnel a una nueva **Security Zone (Zona de seguridad)** llamada `corp-vpn` y, luego, asígnela al **Virtual Router (Enrutador virtual)** predeterminado.
- Habilite la identificación de usuario en la zona `corp-vpn`.

STEP 2 | Cree una política de seguridad para habilitar el flujo de tráfico entre la zona `corp-vpn` y la zona `l3-trust` y permitir el acceso a sus recursos internos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego, haga clic en **Add (Añadir)** para crear una nueva regla.
2. Para este ejemplo, puede definir la regla con la siguiente configuración:
   - **Name (Nombre)** (pestaña **General**): `VPN Access`
   - **Source Zone (Zona de origen)** (pestaña **Source [Origen]**): `corp-vpn`
   - **Destination Zone (Zona de destino)** (pestaña **Destination [Destino]**): `l3-trust`

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | Use uno de los siguientes métodos para obtener un certificado de servidor para la interfaz que aloja el portal y la puerta de enlace de GlobalProtect:

- (Recomendado) Importación de un certificado de servidor desde una CA externa conocida.
- Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado.

Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** para gestionar los certificados de la siguiente manera:

- Obtenga un certificado de servidor. Como el portal y la puerta de enlace se encuentran en la misma interfaz, se puede utilizar el mismo certificado de servidor para ambos componentes.
- El CN del certificado debe coincidir con el FQDN, gp.acme.com.
- Para permitir a los usuarios conectarse con el portal sin que reciban errores de certificado, utilice un certificado de servidor desde una CA pública.

STEP 4 | Emita certificados de cliente para clientes y endpoints de GlobalProtect.

1. Utilice su PKI empresarial o CA pública para emitir un certificado de cliente único para cada usuario de GlobalProtect.
2. Instale certificados en el almacén de certificados personales de los endpoints.

STEP 5 | Cree un perfil de certificado de cliente.

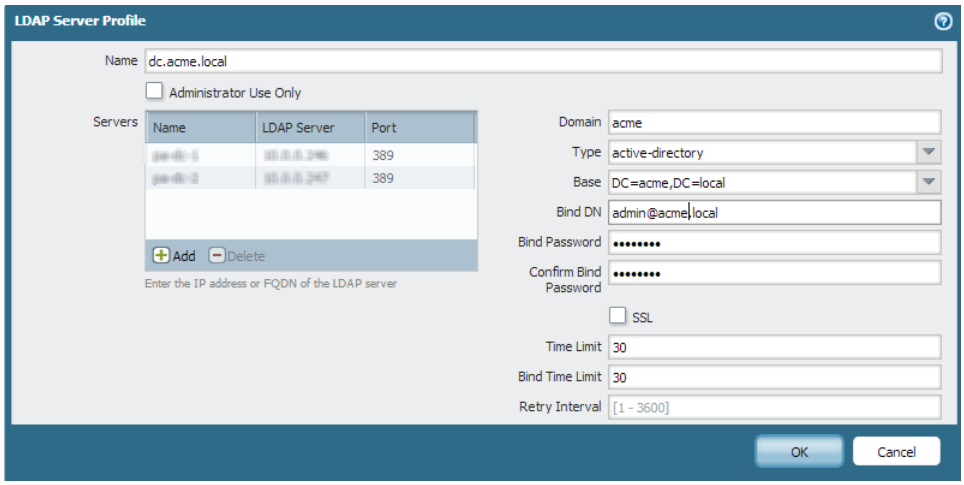
© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de certificado y luego, introduzca un **Name (Nombre)** de perfil como `GP-client-cert`.
2. Especifique dónde obtener el nombre de usuario que se utilizará para autenticar al usuario final:
   - **De usuario**: si quiere que el usuario final proporcione un nombre de usuario cuando se autentique en el servicio especificado en el perfil de autenticación, seleccione **None (Ninguno)** como **Username Field (Campo de nombre de usuario)**.
   - **De certificado**: si desea extraer el nombre de usuario del certificado, seleccione **Subject (Asunto)** como **Username Field (Campo de nombre de usuario)**. Si utiliza esta opción, el CN contenido en el certificado completará automáticamente el campo de nombre de usuario cuando al usuario se le solicite iniciar sesión en el portal/puerta de enlace. Al usuario se le pedirá que inicie sesión con ese nombre de usuario.
3. En el área **CA Certificates (Certificados de CA)**, haga clic en **Add (Añadir)** para añadir el certificado de CA que emitió los certificados de cliente. Haga clic en **OK** dos veces.

STEP 6 | Cree un perfil de servidor.

El perfil de servidor indica al cortafuegos cómo conectarse al servicio de autenticación. Los métodos de autenticación Local, RADIUS, Kerberos, SAML y LDAP son compatibles. En este ejemplo se muestra un perfil de autenticación LDAP para autenticar a los usuarios con respecto a Active Directory.

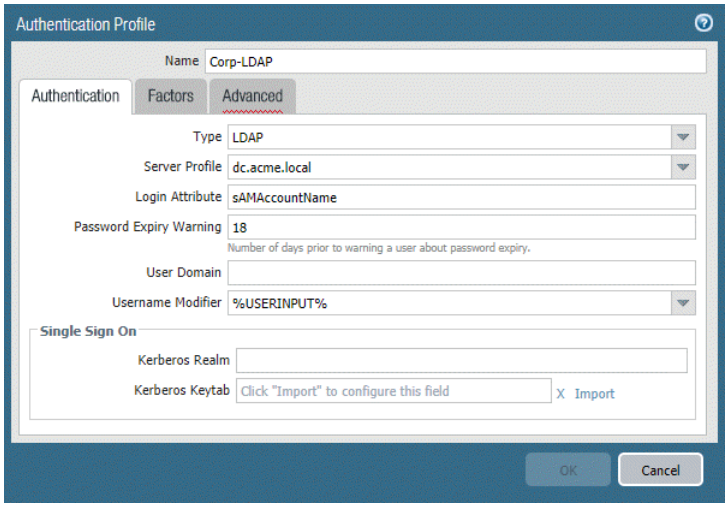
Cree el perfil de servidor para conectarse al servidor LDAP (**Device [Dispositivo]** > **Server Profiles [Perfiles de servidor]** > **LDAP**).



STEP 7 | (Opcional) Cree un perfil de autenticación.

Instale el perfil del servidor en un perfil de autenticación (**Device [Dispositivo]Authentication Profile [Perfil de autenticación]**).

© 2020 Palo Alto Networks, Inc.



STEP 8 | Configuración de una puerta de enlace de GlobalProtect.

Vea el diagrama de topología que se muestra en VPN de GlobalProtect para acceso remoto.

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración:

Interface (Interfaz): `ethernet1/2`

IP Address (Dirección IP): `203.0.113.1`

Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

Certificate Profile (Perfil del certificado): `GP-client-cert`

Authentication Profile (Perfil de autenticación): `Corp-LDAP`

Tunnel Interface (Interfaz de túnel): `tunnel.2`

IP Pool (Grupo de IP): `10.31.32.3 - 10.31.32.118`

STEP 9 | Configure los Portales de GlobalProtect.

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración:

1. Configuración del acceso al portal de GlobalProtect:

   Interface (Interfaz): `ethernet1/2`

   IP Address (Dirección IP): `203.0.113.1`

   Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

   Certificate Profile (Perfil del certificado): `GP-client-cert`

   Authentication Profile (Perfil de autenticación): `Corp-LDAP`
2. Definición de las configuraciones de agente de GlobalProtect:

   Connect Method (Método de conexión): `On-demand` (conexión manual iniciada por el usuario).

   External Gateway Address (Dirección de puerta de enlace externa): `gp.acme.com`

STEP 10 | Implementación del software de la aplicación de GlobalProtect

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)**. Siga el procedimiento para alojar actualizacioes de la aplicación en el portal.

© 2020 Palo Alto Networks, Inc.

STEP 11 | (Opcional) Implementación de la configuración de aplicación de forma trasparente.

Como alternativa a la implementación de los ajustes de la aplicación desde la configuración del portal, puede definir los ajustes directamente desde el registro de Windows o el archivo plist global de MAC. Algunos ejemplos de ajustes que puede implementar incluyen especificar la dirección IP del portal o habilitar GlobalProtect para que inicie un túnel VPN antes de que un usuario inicie sesión en el endpoint y se conecte al portal de GlobalProtect. En los endpoints de Windows únicamente, también puede configurar los ajustes con el instalador MSIEXEC. Para obtener más información, consulte Configuración de aplicación personalizable.

STEP 12 | (Optativo) Permita el uso de la aplicación móvil de GlobalProtect.

Adquiera e instale una suscripción a GlobalProtect (**Device [Dispositivo]** > **Licenses [Licencias]**) para habilitar el uso de la aplicación.

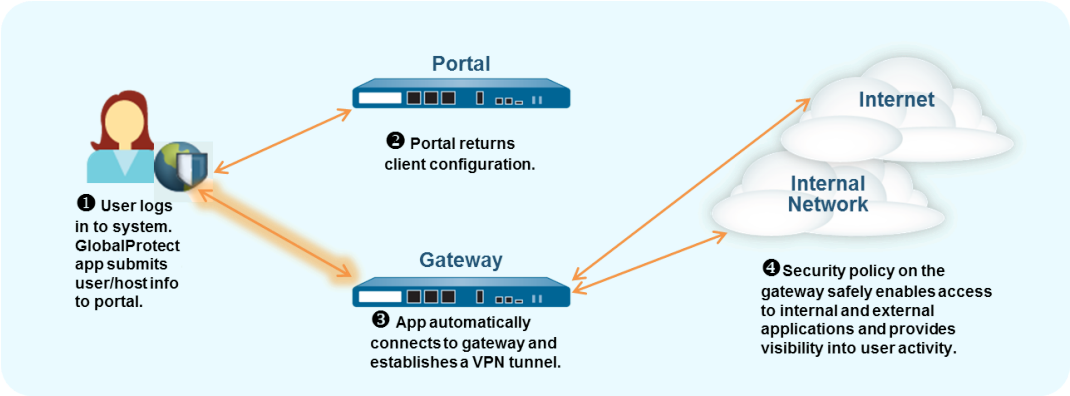
STEP 13 | Guarde la configuración de GlobalProtect.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de VPN siempre activada

En una configuración de GlobalProtect "siempre activada", la aplicación se conecta al portal de GlobalProtect (tras el inicio de sesión del usuario) para enviar información de usuario y del host y recibir la configuración del cliente. A continuación, la aplicación se conecta automáticamente y establece un túnel VPN a la puerta de enlace que se especificó en la configuración del cliente proporcionada por el portal, como se muestra en la siguiente imagen:



Para cambiar una de las configuraciones VPN de acceso remoto a una "siempre activada", puede modificar el método de conexión:

- VPN de acceso remoto (Perfil de autenticación)
- VPN de acceso remoto (perfil del certificado)
- VPN de acceso remoto con autenticación en dos fases

Use estos pasos para cambiar una configuración de VPN de acceso remoto a una "siempre activada".

STEP 1 | Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, seleccione una configuración del portal.

STEP 2 | En la pestaña **Agent (Agente)**, seleccione la configuración del agente que desea modificar.

STEP 3 | Seleccione **App (Aplicación)** y luego configure **Connect Method (Método de conexión)** en **User-logon (Always On) (Inicio de sesión del usuario [Siempre activado])**.

STEP 4 | Haga clic en **OK** para guardar la configuración de agente.

STEP 5 | Repita los pasos 2 al 4 para cada configuración de agente que desea modificar.

STEP 6 | Haga clic en **OK (Aceptar)** para guardar la configuración del portal y, a continuación, haga clic en **Commit (Confirmar)** para confirmar los cambios.

© 2020 Palo Alto Networks, Inc.

VPN de acceso remoto con función anterior al inicio de sesión

El *inicio de sesión previo* es un método de conexión que establece un túnel VPN antes de que un usuario inicie sesión. El propósito del inicio de sesión previo es autenticar el endpoint (no el usuario) y luego habilitar las secuencias de comando de dominio y otras tareas para que se ejecuten tan pronto como se encienda el endpoint. Los certificados de equipo habilitan el endpoint para establecer un túnel VPN en la puerta de enlace. Una práctica común de los administradores de TI es instalar el certificado del equipo mientras se almacena provisionalmente el endpoint para el usuario.

Un túnel VPN de inicio de sesión previo no tiene asociación de nombre de usuario debido a que el usuario no inició sesión. Para permitir que el endpoint tenga acceso a los recursos de la zona fiable, debe crear políticas de seguridad que coincidan con el usuario del inicio de sesión previo. Estas políticas deben permitir el acceso únicamente a servicios básicos necesarios para iniciar el sistema, como DHCP, DNS, Active Directory (por ejemplo, para cambiar una contraseña vencida), antivirus o servicios de actualización del sistema operativo. Una vez que el usuario se autentique con la puerta de enlace, la aplicación de GlobalProtect reasigna el túnel VPN a dicho usuario (la asignación de la dirección IP en el cortafuegos cambia del endpoint de inicio de sesión previo al usuario autenticado).

La pantalla de inicio de sesión del proveedor de credenciales de GlobalProtect para los endpoints de Windows 7 y Windows 10 también muestra el estado de conexión de inicio de sesión previo antes del inicio de sesión del usuario, lo que permite a los usuarios finales determinar si pueden acceder a los recursos de red después de iniciar sesión. Si la aplicación de GlobalProtect detecta un endpoint como interno, la pantalla del inicio de sesión muestra el estado de conexión de inicio de sesión previo **interno**. Si la aplicación de GlobalProtect detecta un endpoint como externo, la pantalla del inicio de sesión muestra el estado de conexión de inicio de sesión previo **conectado** o **no conectado**.

Los endpoints de Windows se comportan diferente de los endpoints de macOS con el inicio de sesión previo. Con los endpoints de macOS, se revoca el túnel de inicio de sesión previo y se crea un nuevo túnel cuando el usuario inicia sesión.

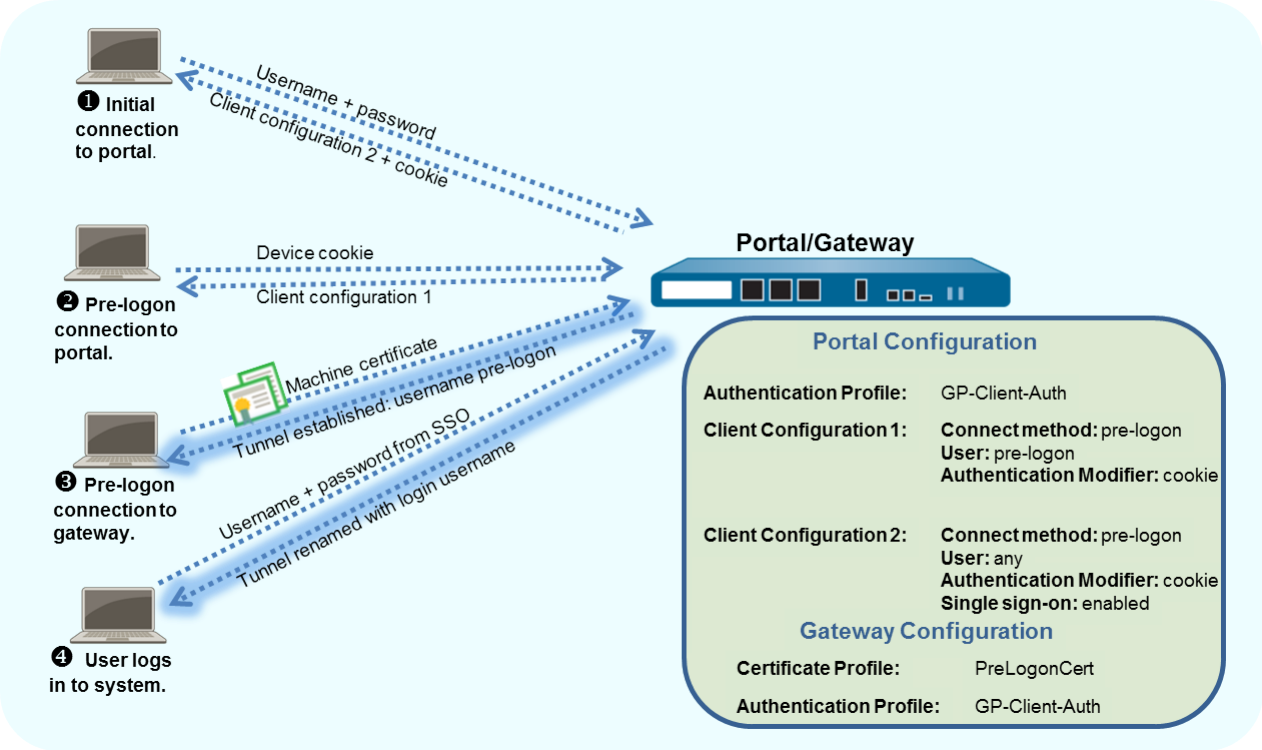
Cuando un usuario solicita una nueva conexión, el portal autentica al cliente mediante un perfil de autenticación. El portal también puede utilizar un perfil de certificado opcional que valide el certificado del cliente (si la configuración incluye un certificado de cliente). En este caso, el certificado debe identificar al usuario. Después de la autenticación, el portal determina si la configuración del endpoint de GlobalProtect es actual. Si la configuración del portal cambió, envía una configuración actualizada al endpoint.

Si la configuración del portal o la puerta de enlace incluye una autenticación basada en cookies, el portal o la puerta de enlace instala una cookie cifrada en el endpoint. Posteriormente, el portal o la puerta de enlace utiliza la cookie para autenticar a los usuarios y para actualizar la configuración del agente. Si el perfil de configuración de un agente incluye el método de conexión de inicio de sesión previo además de la autenticación de cookies, los componentes de GlobalProtect pueden usar la cookie para el inicio de sesión previo.

Si los usuarios inician sesión en un endpoint (por ejemplo, un dispositivo sin periféricos) o se necesita una conexión de inicio de sesión previo en un sistema en el que un usuario no inició sesión previamente, puede permitir que el endpoint inicie un túnel de inicio de sesión previo sin primero conectarse al portal para descargar la configuración del inicio de sesión previo. Para ello, debe anular el comportamiento por defecto al crear entradas en el registro de Windows o el archivo plist de macOS.

© 2020 Palo Alto Networks, Inc.

Luego, el endpoint de GlobalProtect se conectará con el portal especificado en la configuración, se autenticará con su certificado de equipo (según se especifica en un perfil de certificado configurado en la puerta de enlace) y establecerá la conexión de GlobalProtect. Cuando el usuario final inicia sesión posteriormente en el equipo y si el inicio de sesión único (single sign-on, SSO) está habilitado en la configuración del cliente, el nombre de usuario y la contraseña se capturan cuando el usuario inicia sesión. Si el SSO no está habilitado en la configuración del agente o si el SSO no es compatible con el endpoint (por ejemplo, un sistema macOS), las credenciales del usuario se deben almacenar en la aplicación (la opción **Save User Credentials [Guardar credenciales de usuario]** debe establecerse en **Yes [Sí]**). Tras una autenticación correcta en la puerta de enlace, el túnel cambiará de nombre (Windows) o se generará de nuevo (macOS) y se podrá aplicar la política basada en el usuario o en el grupo.



Este ejemplo usa la topología de GlobalProtect que se muestra en VPN de GlobalProtect para acceso remoto.

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

- Para este ejemplo, seleccione la pestaña **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, luego, configure los siguientes ajustes:
  1. Seleccione **ethernet1/2**.
  2. Seleccione **Layer 3 (Capa 3)** en el menú desplegable **Interface Type (Tipo de interfaz)**.
  3. En la pestaña **Config (Configuración)**, seleccione **Assign interface to (Asignar interfaz a)** para asignar la interfaz al **Virtual Router (Enrutador virtual)** predeterminado y a la **Security Zone (Zona de seguridad)** `l3-untrust`.
  4. En la pestaña **IPv4**, haga clic en **Add (Añadir)** para seleccionar la dirección IP `203.0.113.1` (o el objeto que asigna`203.0.113.1`) o añada una **New Address (Nueva dirección)** para crear

© 2020 Palo Alto Networks, Inc.

un nuevo objeto y asignación de la dirección (deje el tipo de dirección en **Static [Estática]**). Por ejemplo, cree un registro "A" DNS que asigne la dirección IP `203.0.113.1` a `gp.acme.com`.

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir una interfaz de túnel nueva.
  1. En **Interface Name (Nombre de interfaz)**, introduzca `tunnel.2`.
  2. En la pestaña **Config (Configuración)**, seleccione **Assign Interface To (Asignar interfaz a)** para asignar una interfaz a una **Security Zone (Zona de seguridad)** nueva denominada `corp-vpn` y al **Virtual Router (Enrutador virtual)** predeterminado.
- Habilite la identificación de usuario en la zona `corp-vpn`.

STEP 2 | Cree las reglas de política de seguridad.

Esta configuración requiere las siguientes políticas (**Policies [Políticas]** > **Security [Seguridad]**):

1. Haga clic en **Add (Añadir)** para añadir una regla que permita el acceso del usuario con inicio de sesión previo a los servicios básicos necesarios para que aparezca el endpoint, como servicios de autenticación, DNS, DHCP y actualizaciones de Microsoft.
2. Haga clic en **Add (Añadir)** para añadir una regla que deniegue el acceso de los usuarios con inicio de sesión previo a todos los demás destinos y aplicaciones.
3. Haga clic en **Add (Añadir)** para añadir reglas adicionales que permitan a diferentes usuarios o grupos de usuarios acceder a destinos y aplicaciones específicas. Al crear estas reglas, siga las sugerencias de la política recomendada de seguridad para puertas de enlace de internet.

STEP 3 | Use algunos de los siguientes métodos para obtener un certificado de servidor para la interfaz que aloja el portal y la puerta de enlace de GlobalProtect:

- (Recomendado) Importación de un certificado de servidor desde una CA externa conocida.
- Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado.

Seleccione **Device** > **Certificate Management** > **Certificates** para gestionar los certificados con los siguientes criterios:

- Obtenga un certificado de servidor. Como el portal y la puerta de enlace se encuentran en la misma interfaz, se puede utilizar el mismo certificado de servidor para ambos componentes.
- El CN del certificado debe coincidir con el FQDN, gp.acme.com.
- Para permitir a los endpoints conectarse con el portal sin que reciban errores de certificado, utilice un certificado de servidor desde una CA pública.

STEP 4 | Genere un certificado de equipo para cualquier endpoint que se conecte a GlobalProtect e impórtelo al almacén de certificados personales de cada máquina.

Si bien podría generar certificados autofirmados para cada endpoint, recomendamos utilizar su propia infraestructura de clave pública (public-key infrastructure, PKI) para emitir y distribuir certificados para sus endpoints.

1. Emita certificados de cliente para clientes y endpoints de GlobalProtect.
2. Instale certificados en el almacén de certificados personales de los endpoints. (Almacén del equipo local en endpoints de Windows o llavero del sistema en endpoints de macOS)

STEP 5 | Importe el certificado de CA raíz de confianza desde la CA que generó los certificados de equipo al portal y las puertas de enlace.

No necesita importar la clave privada.

1. Descargue el certificado de CA en el formato Base64.

© 2020 Palo Alto Networks, Inc.

2. Use los siguientes pasos para importar el certificado en todos los cortafuegos que alojen un portal o puerta de enlace:
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)** para importar el certificado.
   2. Introduzca un **Certificate Name (Nombre de certificado)** que identifique al certificado como su certificado de CA de cliente.
   3. Seleccione **Browse (Examinar)** para buscar el **Certificate File (Archivo de certificado)** que ha descargado desde la CA.
   4. Configure **File Format (Formato de archivo)** en **Base64 Encoded Certificate (PEM) (Certificado codificado en Base64 [PEM])**.
   5. Haga clic en **OK (Aceptar)** para guardar el certificado.
   6. En la pestaña **Device Certificates (Certificados de dispositivo)**, seleccione el certificado que acaba de importar.
   7. Seleccione la casilla de verificación **Trusted Root CA (CA raíz de confianza)** y, a continuación, haga clic en **OK (Aceptar)**.

STEP 6 | En todos los cortafuegos que alojan una puerta de enlace de GlobalProtect, cree un perfil de certificado para identificar qué certificado de CA utilizar para validar los certificados de equipo.

Si planea utilizar la autenticación de certificados del cliente para autenticar a los usuarios cuando inician sesión en el sistema, asegúrese de que en el perfil del certificado se haga referencia al certificado de CA que emite los certificados de cliente, además de al certificado de CA que emitió los certificados de equipo (si son distintos).

1. Seleccione **Device (Dispositivo)** > **Certificates (Certificados)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** y, luego, haga clic en **Add (Añadir)** para añadir un perfil de certificado.
2. Introduzca un **Name (Nombre)** para identificar el perfil, como **`PreLogonCert`**.
3. Configure el campo **Username (Nombre de usuario)** en **None (Ninguno)**.
4. (Opcional) Si quiere utilizar también la autenticación de certificado de cliente para autenticar a los usuarios al iniciar sesión, añada el certificado de CA que emitió los certificados del cliente si es distinto al que emitió los certificados de equipo.
5. En el campo **CA Certificates (Certificados de CA)**, haga clic en **Add (Añadir)** para añadir el certificado de CA.
6. Seleccione el certificado de CA raíz de confianza que importó en el paso 5 en **CA Certificate (Certificado de CA)** y luego haga clic en **OK (Aceptar)**.
7. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 7 | Configuración de una puerta de enlace de GlobalProtect.

Vea el diagrama de topología que se muestra en VPN de GlobalProtect para acceso remoto.

Aunque debe crear un perfil de certificado para el modo de acceso de inicio de sesión previo a la puerta de enlace, puede utilizar la autenticación de certificado del cliente o la autenticación basada en perfil para aquellos usuarios que han iniciado sesión. En este ejemplo, se usa el mismo perfil de LDAP que el usado para autenticar a usuarios en el portal.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración de puerta de enlace:

   Interface (Interfaz): **`ethernet1/2`**

   IP Address (Dirección IP): **`203.0.113.1`**

   Server Certificate (Certificado de servidor): **`GP-server-cert.pem issued by GoDaddy`**

© 2020 Palo Alto Networks, Inc.

Certificate Profile (Perfil del certificado): `PreLogonCert`

Authentication Profile (Perfil de autenticación): `Corp-LDAP`

Tunnel Interface (Interfaz de túnel): `tunnel.2`

IP Pool (Grupo de IP): `10.31.32.3 - 10.31.32.118`

2. Seleccione **Commit (Confirmar)** para aplicar la configuración de la puerta de enlace.

STEP 8 | Configure los Portales de GlobalProtect.

Configure los detalles del dispositivo en **Device (Dispositivo)** (parámetros de red, el perfil de servicio de autenticación y el certificado para el servidor de autenticación).

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, haga clic en **Add (Añadir)** para añadir la siguiente configuración del portal:

Configuración del acceso al portal de GlobalProtect:

Interface (Interfaz): `ethernet1/2`

IP Address (Dirección IP): `203.0.113.1`

Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy`

Certificate Profile (Perfil del certificado): `None`None (Ninguno)

Authentication Profile (Perfil de autenticación): `Corp-LDAP`

STEP 9 | Definición de las configuraciones de agente de GlobalProtect para obtener información sobre los usuarios con inicio de sesión anterior y para los usuarios que iniciaron sesión.

Utilice una configuración única si desea que los usuarios con inicio de sesión previo accedan a las mismas puertas de enlace antes y después de iniciar sesión.

Para dirigir a los usuarios con inicio de sesión previo a diferentes puertas de enlace antes y después de iniciar sesión, cree dos perfiles de configuración. En este **User/User Group (Usuario/grupo de usuarios)** de la primera configuración, seleccione el filtro **pre-logon (inicio de sesión previo)**. Con el inicio de sesión previo, el portal autentica primero el endpoint (no el usuario) para configurar una conexión, incluso si el parámetro de inicio de sesión previo está asociado con el usuario. Posteriormente, el portal autentica al usuario cuando este inicia sesión.

Después de que el portal autentica al usuario, implementa la segunda configuración. En este caso, **User/User Group** es **any**.

Se recomienda habilitar SSO en la segunda configuración para que se indique inmediatamente el nombre de usuario correcto a la puerta de enlace cuando el usuario inicia sesión en el endpoint. Si el SSO no está habilitado, se utilizará el nombre de usuario guardado en el panel de configuración del agente.

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **<portal-config>** y, a continuación, seleccione la pestaña **Agent (Agente)** de la ventana **GlobalProtect Portal Configuration (Configuración de portal de GlobalProtect)**. Después, haga clic en **Add (Añadir)** para añadir una de estas configuraciones:

- Utilice la misma puerta de enlace antes y después de que los usuarios con inicio de sesión anterior inicien sesión:

Use Single Sign-On (Usar inicio de sesión único): `enabled`

Método de conexión: `inicio de sesión previo`

External Gateway Address (Dirección de puerta de enlace externa): `gp1.acme.com`

© 2020 Palo Alto Networks, Inc.

User/User Group (Usuario/grupo de usuarios): `any`

Authentication Override (Anulación de la autenticación): autenticación de cookie para autenticar de manera transparente a los usuarios y para actualizar la configuración.

- Utilice puertas de enlace separadas para los usuarios con inicio de sesión anterior antes y después de que inicien sesión:

Primera configuración del agente:

Método de conexión: `inicio de sesión previo`

External Gateway Address (Dirección de puerta de enlace externa): `gp1.acme.com`

Usuario/grupo de usuarios: `inicio de sesión previo`

Authentication Override (Anulación de la autenticación): autenticación de cookie para autenticar de manera transparente a los usuarios y para actualizar la configuración.

Segunda configuración del agente:

Use Single Sign-On (Usar inicio de sesión único): `enabled`

Método de conexión: `inicio de sesión previo`

External Gateway Address (Dirección de puerta de enlace externa): `gp2.acme.com`

User/User Group (Usuario/grupo de usuarios): `any`

Authentication Override (Anulación de la autenticación): autenticación de cookie para autenticar de manera transparente a los usuarios y para actualizar la configuración.

Asegúrese de que la configuración en modo de inicio de sesión previo esté primera en la lista de configuraciones. Si no es así, selecciónela y haga clic en **Move Up (Mover hacia arriba)**.

STEP 10 | Guarde la configuración de GlobalProtect.

Haga clic en **Commit (Confirmar)**.

STEP 11 | (Opcional) Si los usuarios nunca inician sesión en un terminal (por ejemplo, uno sin periféricos) o hace falta una conexión anterior al inicio de sesión en un terminal en el que nunca han iniciado sesión, cree la entrada de registro `Prelogon (Anterior al inicio de sesión)` en el terminal.

También debe implementar previamente la dirección IP predeterminada del portal.

Para obtener más información sobre la configuración del registro, consulte Implementación de la configuración de la aplicación de forma trasparente.

1. Vaya a la siguiente ubicación del registro de Windows para ver la lista de ajustes de GlobalProtect:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
2. Seleccione **Edit (Editar)** > **New (Nuevo)** > **String Value (Valor de cadena)** para crear estas entradas en el registro:
   - En **String Value (Valor de cadena)**, cree una cadena denominada `Prelogon (Anterior al inicio de sesión)` con el valor `1`. Este ajuste permite a GlobalProtect iniciar una conexión antes de que el usuario inicie sesión en el endpoint.
   - Cree un **String Value (Valor de cadena)** denominado `Portal` que especifique la dirección IP o nombre de host del portal predeterminado para el endpoint de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Configuración de varias puertas de enlace de GlobalProtect

En Topología de varias puertas de enlace de GlobalProtect se añadió una segunda puerta de enlace a la configuración. En esta topología, debe configurar un cortafuegos adicional para alojar la segunda puerta de enlace de GlobalProtect. Cuando añade las configuraciones de cliente para que el portal las implemente, también puede especificar diferentes puertas de enlace para distintas configuraciones de cliente o permitir el acceso a todas las puertas de enlace.

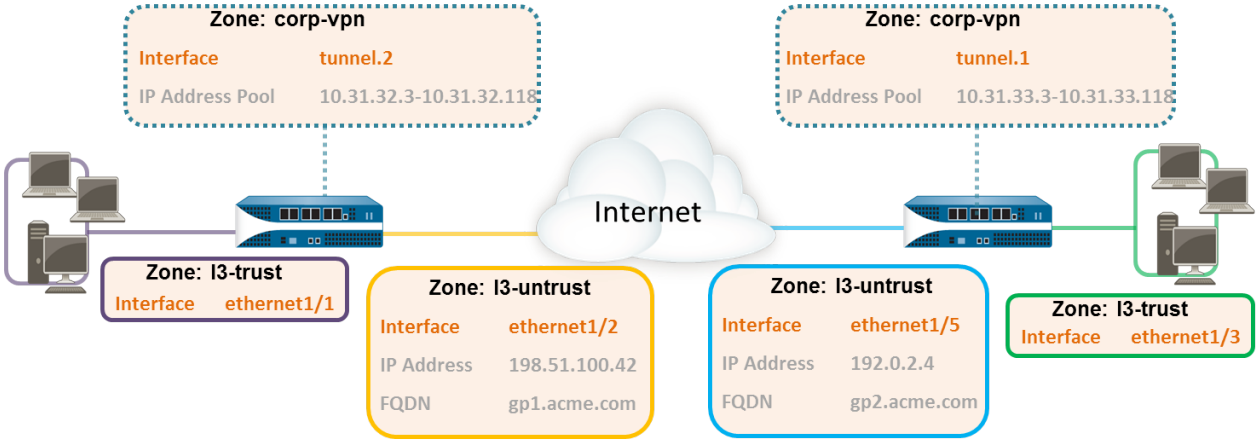


Figure 7: Topología de puerta varias puertas de enlace de GlobalProtect

Si una configuración de cliente contiene más de una puerta de enlace, la aplicación trata de conectarse a todas las puertas de enlace indicadas en su configuración de cliente. El agente utiliza la prioridad y el tiempo de respuesta para determinar a qué puerta de enlace se conectará. La aplicación solo se conecta a una puerta de enlace de menor prioridad solo si el tiempo de respuesta para la puerta de enlace de mayor prioridad es mayor que el tiempo de respuesta promedio de todas las puertas de enlace. Para obtener más información, consulte Prioridad de la puerta de enlace en una configuración de varias puertas de enlace.

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

En esta configuración, debe configurar las interfaces de cada cortafuegos que alberga una puerta de enlace.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

En el cortafuegos que aloja el portal/puerta de enlace (puerta de enlace 1):

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, luego, **ethernet1/2**.
- Configure **ethernet1/2** como la interfaz de capa 3 con la dirección IP `198.51.100.42` y luego asígnela a la zona **Security Zone (Zona de seguridad)** `l3-untrust` y al **Virtual Router (Enrutador virtual)** `default`.
- Cree un registro "A" DNS que asigne la dirección`198.51.100.42` a `gp1.acme.com`
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y, a continuación, haga clic en **Add (Añadir)** para añadir la interfaz `tunnel.2`. Añada la interfaz a una nueva **Security Zone (Zona de seguridad)** denominada `corp-vpn`. Asígnela al enrutador seleccionando `default (predeterminado)` en **Virtual Router (Enrutador virtual)**.

© 2020 Palo Alto Networks, Inc.

- Habilite la identificación de usuario en la zona **corp-vpn**.

En el cortafuegos que aloja la segunda puerta de enlace (puerta de enlace 2):

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, luego, **ethernet1/5**.
- Configure **ethernet1/5** como la interfaz de capa 3 con la dirección IP **192.0.2.4** y luego asígnela a la zona **Security Zone (Zona de seguridad)** **l3-untrust** y al **Virtual Router (Enrutador virtual)** **default**.
- Cree un registro "A" de DNS que asigne la dirección IP **192.0.2.4** a **gp2.acme.com**.
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir la interfaz **tunnel.1**. Añada la interfaz a una nueva **Security Zone (Zona de seguridad)** denominada **corp-vpn**. Asígnela al enrutador virtual predeterminado en **Virtual Router (Enrutador virtual)**.
- Habilite la identificación de usuario en la zona **corp-vpn**.

STEP 2 | Compre e instale una suscripción de GlobalProtect en cada puerta de enlace si sus usuarios finales utilizarán la aplicación de GlobalProtect en sus dispositivos móviles o si planea utilizar la política de seguridad habilitada para HIP.

Después de adquirir la suscripción de GlobalProtect y de recibir su código de activación, instale la licencia en el cortafuegos que aloja el portal de la siguiente forma:

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
2. Seleccione **Activate feature using authorization code (Activar característica mediante código de autorización)**.
3. Cuando se le indique, introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**.
4. Compruebe que la licencia se haya activado correctamente:

STEP 3 | Cree políticas de seguridad en cada cortafuegos que aloje una puerta de enlace de GlobalProtect.

Esta configuración requiere reglas de políticas para habilitar el flujo de tráfico entre la zona **corp-vpn** y la zona **l3-trust** para permitir el acceso a sus recursos internos (**Policies (Políticas)** > **Security (Seguridad)**).

STEP 4 | Use una de las siguientes recomendaciones para obtener certificados de servidor para la interfaz que aloja el portal y las puertas de enlace de GlobalProtect:

- (En el cortafuegos que aloja el portal o portal/puerta de enlace) Importe un certificado de servidor desde una CA externa reconocida.
- (En un cortafuegos que aloja solo una puerta de enlace) Use la CA raíz en el portal para generar un certificado de servidor autofirmado.

En todos los cortafuegos que alojan un portal/puerta de enlace o puerta de enlace, seleccione **Device** > **Certificate Management** > **Certificates** para gestionar certificados de la siguiente forma:

- Obtenga un certificado de servidor para la interfaz que aloja el portal/puerta de enlace1: Como el portal y la puerta de enlace se encuentran en la misma interfaz, debe utilizar el mismo certificado de servidor. El CN del certificado debe coincidir con el FQDN, `gp1.acme.com`. Para permitir a los endpoints conectarse con el portal sin que reciban errores de certificado, utilice un certificado de servidor desde una CA pública.

© 2020 Palo Alto Networks, Inc.

- Obtenga un certificado de servidor para la interfaz que aloja la puerta de enlace 2: Como esta interfaz aloja solo una puerta de enlace, puede utilizar un certificado autofirmado. El CN del certificado debe coincidir con el FQDN, `gp2.acme.com`.

STEP 5 | Defina cómo autenticará a los usuarios en el portal y las puertas de enlace.

Puede utilizar cualquier combinación de perfiles de certificado o perfiles de autenticación como sea necesario para garantizar la seguridad del portal y las puertas de enlace. Los portales y las puertas de enlace individuales también pueden utilizar distintos esquemas de autenticación. Consulte las siguientes secciones para obtener instrucciones detalladas:

- Configuración de autenticación externa (perfil de autenticación)
- Configuración de la autenticación de certificado de cliente (perfil de certificado)
- Configuración de la autenticación en dos fases (basada en token u OTP)

Luego, debe hacer referencia al perfil del certificado o perfiles de autenticación que define en las configuraciones de puerta de enlace y portal.

STEP 6 | Configuración de una puerta de enlace de GlobalProtect.

En el siguiente ejemplo, se muestra la configuración para gp1 y gp2 que aparece en la Topología de varias puertas de enlace de GlobalProtect.

En el cortafuegos que se aloja gp1, seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**. Configure los ajustes de la puerta de enlace de la siguiente manera:

Interface (Interfaz): **`ethernet1/2`**

IP address (Dirección IP): **`198.51.100.42`**

Server Certificate (Certificado de servidor): **`GP1-server-cert.pem issued by GoDaddy`**

Tunnel Interface (Interfaz de túnel): **`tunnel.2`**

IP Pool (Grupo de IP): **`10.31.32.3 - 10.31.32.118`**

En el cortafuegos que se aloja gp2, seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**. Configure los ajustes de la puerta de enlace de la siguiente manera:

Interface (Interfaz): **`ethernet1/2`**

IP Address (Dirección IP): **`192.0.2.4`**

Server Certificate (Certificado de servidor): **`self-signed certificate, GP2-server-cert.pem`**

Tunnel Interface (Interfaz de túnel): **`tunnel.1`**

IP Pool (Grupo de IP): **`10.31.33.3 - 10.31.33.118`**

STEP 7 | Configure los Portales de GlobalProtect.

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**. Configure los ajustes del portal de la siguiente manera:

1. Configuración del acceso al portal de GlobalProtect:

   Interface (Interfaz): **`ethernet1/2`**

   IP address (Dirección IP): **`198.51.100.42`**

   Server Certificate (Certificado de servidor): **`GP1-server-cert.pem issued by GoDaddy`**
2. Definición de las configuraciones de agente de GlobalProtect:

   El número de configuraciones cliente que crea depende de sus requisitos de acceso específicos, incluido si necesita la aplicación de una política basada en usuario/grupo o HIP.

© 2020 Palo Alto Networks, Inc.

STEP 8 | Implementación del software del agente de GlobalProtect.

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)**.

En este ejemplo, utilice el procedimiento de Alojamiento de actualizaciones de la aplicación en el portal.

STEP 9 | Guarde la configuración de GlobalProtect.

Haga clic en **Commit (Confirmar)** para confirmar la configuración en el cortafuegos que aloja el portal y las puertas de enlace.

© 2020 Palo Alto Networks, Inc.

GlobalProtect para comprobación de HIP interna y acceso basado en usuario

Junto con el ID de usuario o las comprobaciones HIP, se puede utilizar una puerta de enlace interna para ofrecer un método preciso y seguro con el cual identificar y controlar el tráfico por usuario o estado del dispositivo, y sustituir otros servicios de control de acceso para redes (network access control, NAC). Las puertas de enlace internas son útiles en entornos confidenciales que requieren acceso autenticado a los recursos críticos.

En una configuración que solo tenga puertas de enlace internas, todos los endpoints deben configurarse con inicio de sesión de usuario (siempre activado); el modo a demanda no es compatible. Se recomienda también que configure todas las configuraciones de cliente que se deben utilizar para el inicio de sesión único (single sign-on, SSO). Además, como los hosts internos no necesitan establecer una conexión de túnel con la puerta de enlace, se utiliza la dirección IP del adaptador de red físico del endpoint.

En esta configuración rápida, se utilizan las puertas de enlace internas para aplicar políticas basadas en grupos que permitan el acceso de los usuarios del grupo técnico a las bases de datos de errores y control de origen interno y el acceso de los usuarios del grupo de finanzas a las aplicaciones CRM. Todos los usuarios autenticados tienen acceso a recursos Web internos. Además, los perfiles HIP configurados en la puerta de enlace comprueban todos los hosts para garantizar el cumplimiento con los requisitos de mantenimiento internos (por ejemplo, si están instalados los parches de seguridad, si está habilitado el cifrado de disco o si está instalado el software necesario).

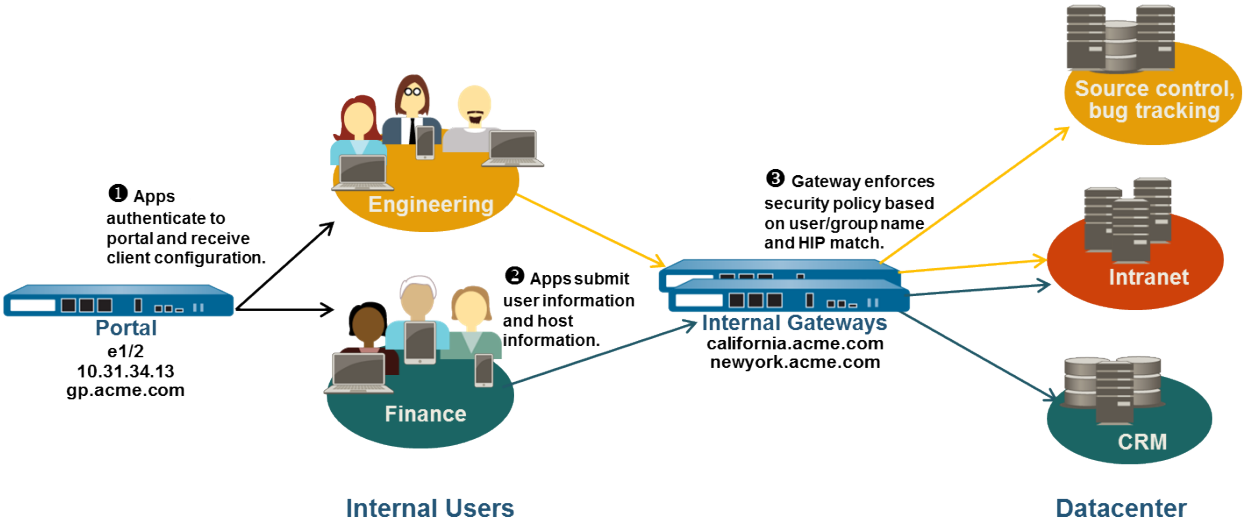


Figure 8: Configuración de puerta de enlace interna de GlobalProtect

Utilice los siguientes pasos para configurar una puerta de enlace interna de GlobalProtect.

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

En esta configuración, debe configurar las interfaces de cada cortafuegos que aloje un portal o puerta de enlace. Como esta configuración solo utiliza puertas de enlace internas, debe configurar el portal y las puertas de enlace en interfaces de la red interna.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

© 2020 Palo Alto Networks, Inc.

En todos los cortafuegos que alojan un portal/puerta de enlace:

1. Seleccione un puerto Ethernet para alojar el portal/puerta de enlace y, a continuación, configure una interfaz de capa 3 con una dirección IP en la **Security Zone (Zona de seguridad)** `l3-trust` (**Network (Red)** > **Interfaces** > **Ethernet**).
2. Marque **Enable User Identification (Habilitar identificación de usuarios)** en la zona `l3-trust`.

STEP 2 | Si sus usuarios finales accederán a la aplicación de GlobalProtect en sus dispositivos móviles o si planifica usar la política de seguridad con HIP, compre e instale una suscripción de GlobalProtect para cada cortafuegos que aloja una puerta de enlace interna.

Después de adquirir suscripciones de GlobalProtect y de recibir su código de activación, instale las suscripciones de GlobalProtect en los cortafuegos que alojan sus puertas de enlace de la siguiente forma:

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
2. Seleccione **Activate feature using authorization code (Activar característica mediante código de autorización)**.
3. Cuando se le indique, introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**.
4. Compruebe que la licencia se haya activado correctamente.

Póngase en contacto con su ingeniero de ventas o distribuidor de Palo Alto Networks si no tiene todas las licencias necesarias. Si desea obtener más información sobre licencias, consulte Acerca de las licencias de GlobalProtect.

STEP 3 | Obtenga certificados de servidor para el portal de GlobalProtect y cada puerta de enlace de GlobalProtect.

Para conectarse al portal por primera vez, los endpoints deben confiar en el certificado de CA raíz utilizado para emitir el certificado de servidor del portal. Puede utilizar un certificado autofirmado en el portal e implementar el certificado de CA raíz en los endpoints antes de la primera conexión de portal u obtener un certificado de servidor para el portal desde una CA de confianza.

Puede utilizar certificados autofirmados en las puertas de enlace.

El flujo de trabajo recomendado es el siguiente:

1. En el cortafuegos que aloja el portal:
   1. Importe un certificado de servidor desde una CA externa conocida.
   2. Cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect.
   3. Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado. Repita este paso para cada puerta de enlace.
2. En cada cortafuegos que aloja una puerta de enlace interna, implemente certificados de servidor autofirmados.

STEP 4 | Defina cómo autenticará a los usuarios en el portal y las puertas de enlace.

Puede utilizar cualquier combinación de perfiles de certificado o perfiles de autenticación como sea necesario para garantizar la seguridad del portal y las puertas de enlace. Los portales y las puertas de enlace individuales también pueden utilizar distintos esquemas de autenticación. Consulte las siguientes secciones para obtener instrucciones detalladas:

- Configuración de autenticación externa (perfil de autenticación)

© 2020 Palo Alto Networks, Inc.

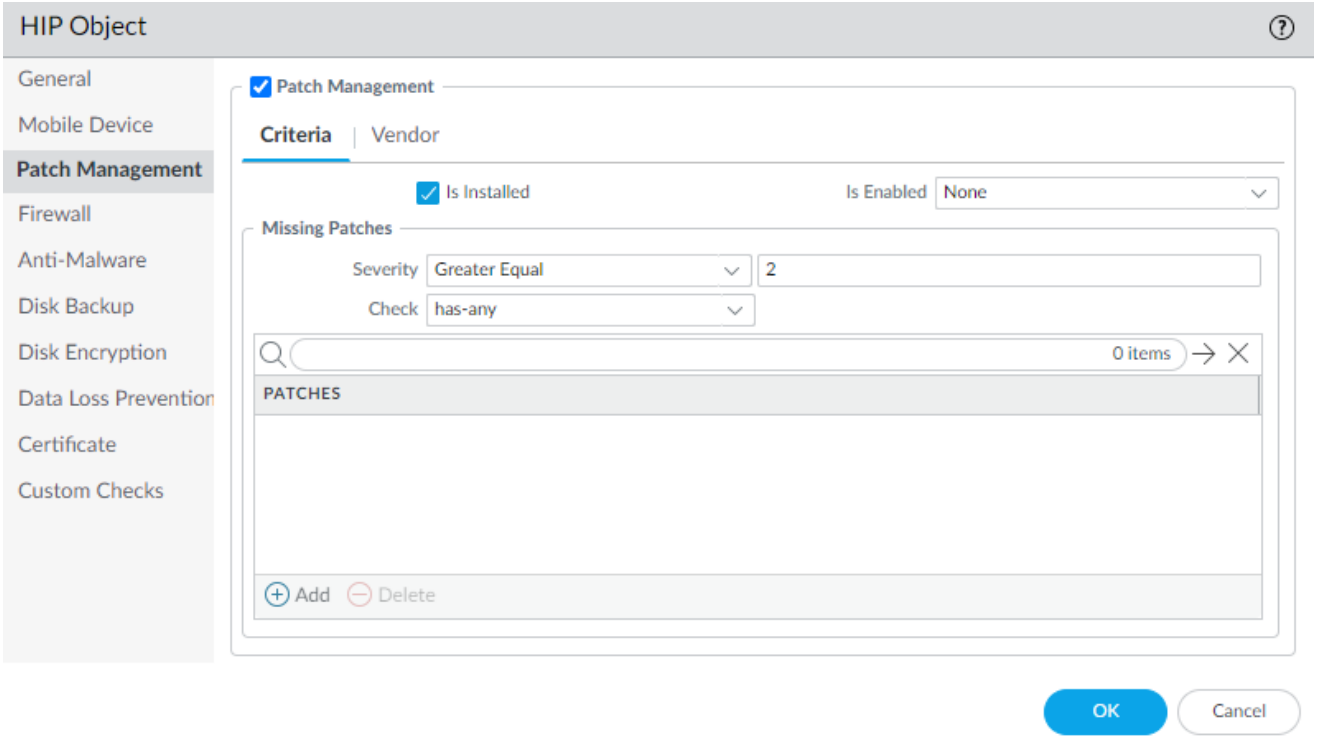
- Configuración de la autenticación de certificado de cliente (perfil de certificado)
- Configuración de la autenticación en dos fases (basada en token u OTP)

Luego, debe hacer referencia al perfil del certificado o perfiles de autenticación que ha definido en las configuraciones de puerta de enlace y portal.

STEP 5 | Cree los perfiles HIP que necesita para aplicar las políticas de seguridad en el acceso a la puerta de enlace.

Consulte la Información de host para obtener más información sobre las evaluaciones HIP.

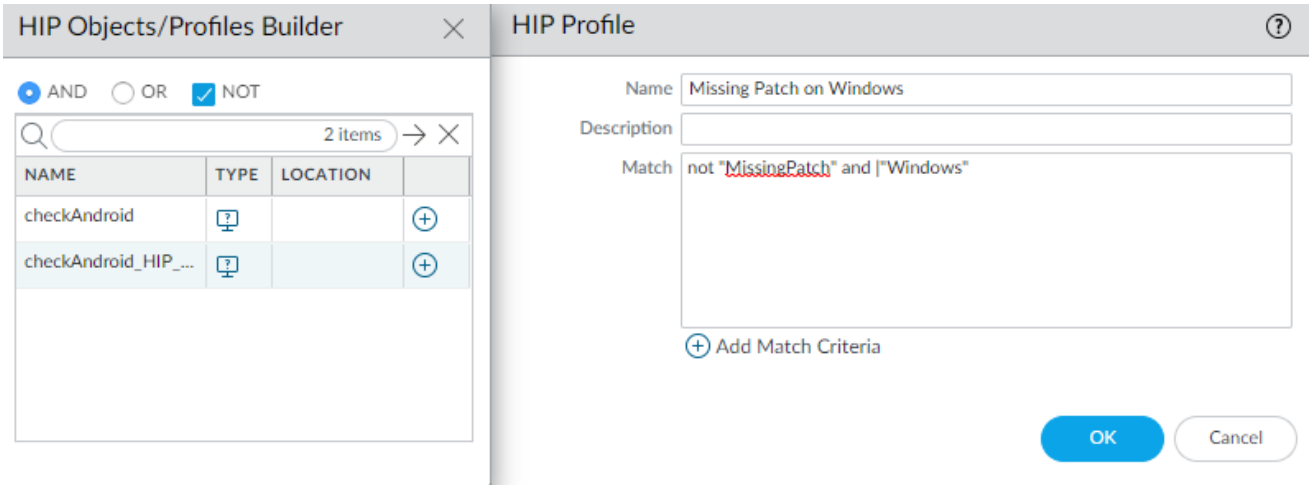
1. Cree objetos HIP para filtrar los datos del host sin procesar recopilados por la aplicación. Por ejemplo, si desea evitar que se conecten los usuarios que no estén actualizados con los parches requeridos, puede crear un objeto HIP con el cual coincidir si el software de gestión de parches está instalado y que todos los parches con una gravedad determinada estén actualizados.



2. Cree los perfiles HIP que planea usar en sus políticas.

   Por ejemplo, si quiere asegurarse de que solo los usuarios de Windows con parches actualizados puedan acceder a sus aplicaciones internas, puede que desee adjuntar el siguiente perfil HIP que coincidirá con los hosts a los que NO les falte ningún parche:

© 2020 Palo Alto Networks, Inc.



STEP 6 | Configure las puertas de enlace internas.

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y, luego, seleccione una Puertas de enlace interna existente o haga clic en **Add (Añadir)** para añadir una nueva. Configure los siguientes ajustes de la puerta de enlace:

- **Interface (Interfaz)**
- **Dirección IP**
- **Server Certificate (Certificado de servidor)**
- **Authentication Profile (Perfil de autenticación)** o **Configuration Profile (Perfil de configuración)**

Observe que no es necesario configurar los ajustes de cliente en las configuraciones de la puerta de enlace (salvo que desee establecer las notificaciones HIP) porque las conexiones de túnel no son necesarias. Consulte Configuración de una puerta de enlace de GlobalProtect para ver instrucciones detalladas sobre cómo crear configuraciones de puerta de enlace.

STEP 7 | Configure los Portales de GlobalProtect.

Si bien todas las configuraciones anteriores pueden utilizar los métodos de conexión User-logon (Always On) (Inicio de sesión de usuario [siempre activado]) o On-demand (Manual user initiated connection) (A demanda [conexión manual iniciada por el usuario]), la configuración de la puerta de enlace siempre debe estar activada y, por lo tanto, requiere el método de conexión User-logon (Always On) (Inicio de sesión de usuario [siempre activado]).

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, seleccione un portal existente o haga clic en **Add (Añadir)** para añadir uno nuevo. Configure el portal de la siguiente manera:

1. Configuración del acceso al portal de GlobalProtect:

   Interface (Interfaz): `ethernet1/2`

   IP Address (Dirección IP): `10.31.34.13`

   Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy` with `CN=gp.acme.com`
2. Definición de las configuraciones de autenticación de cliente de GlobalProtect:

   Use Single Sign-On (Usar inicio de sesión único): `enabled`

   Connect Method (Método de conexión): `User-logon (Always On)`

© 2020 Palo Alto Networks, Inc.

Internal Gateway Address (Dirección de puerta de enlace interna): `california.acme.com, newyork.acme.com`

User/User Group (Usuario/grupo de usuarios): `any`

3. Seleccione **Commit (Confirmar)** para aplicar la configuración del portal.

STEP 8 | Implementación del software de la aplicación de GlobalProtect

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)**.

En este ejemplo, utilice el procedimiento de Alojamiento de actualizaciones de la aplicación en el portal.

STEP 9 | Cree las reglas de seguridad HIP o basadas en grupo/usuario en sus puertas de enlace.

Agregue las siguientes reglas de seguridad para este ejemplo:

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.
2. En la pestaña **Source (Origen)**, establezca la **Source Zone (Zona de origen)** en **l3-trust (l3-fiable)**.
3. En la pestaña **User (Usuario)**, añada el perfil HIP y el usuario/grupo que se debe evaluar.
   - Haga clic en **Add (Añadir)** en la sección **HIP Profiles (Perfiles HIP)** y seleccione el perfil HIP **MissingPatch**.
   - Haga clic en **Add (Añadir)** para añadir el grupo **Source User (Usuario de origen)** (Finanzas o Técnico según la regla que esté creando).
4. Haga clic en **OK (Aceptar)** para guardar la regla.
5. Seleccione **Commit (Confirmar)** para aplicar la configuración de la puerta de enlace.

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	CRM access	none	l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	
2	Eng access	none	l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	

© 2020 Palo Alto Networks, Inc.

Configuración de puerta de enlace externa e interna combinada

En una configuración de puerta de enlace interna y externa combinada de GlobalProtect, puede configurar puertas de enlace independientes para el acceso de VPN y para el acceso a sus recursos internos confidenciales. Con esta configuración, la aplicación de GlobalProtect realiza la detección de host interno para determinar si se encuentra en una red interna o externa. Si la aplicación determina que la red es externa, tratará de conectarse a las puertas de enlace externas que se indican en su configuración de cliente y establecerá una conexión con la puerta de enlace con la prioridad más alta y el menor tiempo de respuesta.

*Si configura todas las puertas de enlace como puertas de enlace solamente manuales pero el método de conexión de GlobalProtect como User-Logon (Always On) (Inicio de sesión de usuario [siempre activado]) o Pre-Logon (Always On) (Inicio de sesión previo [siempre activado]), la aplicación de GlobalProtect no se conectará a ninguna puerta de enlace externa. GlobalProtect permanece en el estado **No conectado** hasta que el usuario externo establezca manualmente una conexión con la puerta de enlace. Este comportamiento le permite implementar GlobalProtect para derivar User-ID para usuarios internos y al mismo tiempo admitir el comportamiento de VPN **A demanda** para los usuarios externos.*

Como las políticas de seguridad se definen de forma independiente en cada puerta de enlace, dispondrá de un control granular sobre los recursos a los que tendrán acceso los usuarios externos e internos. Además, también tendrá un control granular sobre a qué puertas de enlace tendrán acceso los usuarios configurando el portal para que implemente las distintas configuraciones cliente según la pertenencia a un grupo/usuario o la coincidencia del perfil HIP.

En este ejemplo, los portales y las tres puertas de enlace (una externa y dos internas) se implementan en cortafuegos distintos. La puerta de enlace externa en gpvpn.acme.com proporciona acceso de VPN remoto a la red corporativa, mientras que las puertas de enlace internas proporcionan acceso granular a recursos confidenciales del centro de datos según la pertenencia a un grupo. Además, las comprobaciones HIP se utilizan para garantizar que los hosts que tienen acceso al centro de datos tienen los parches de seguridad actualizados.

© 2020 Palo Alto Networks, Inc.

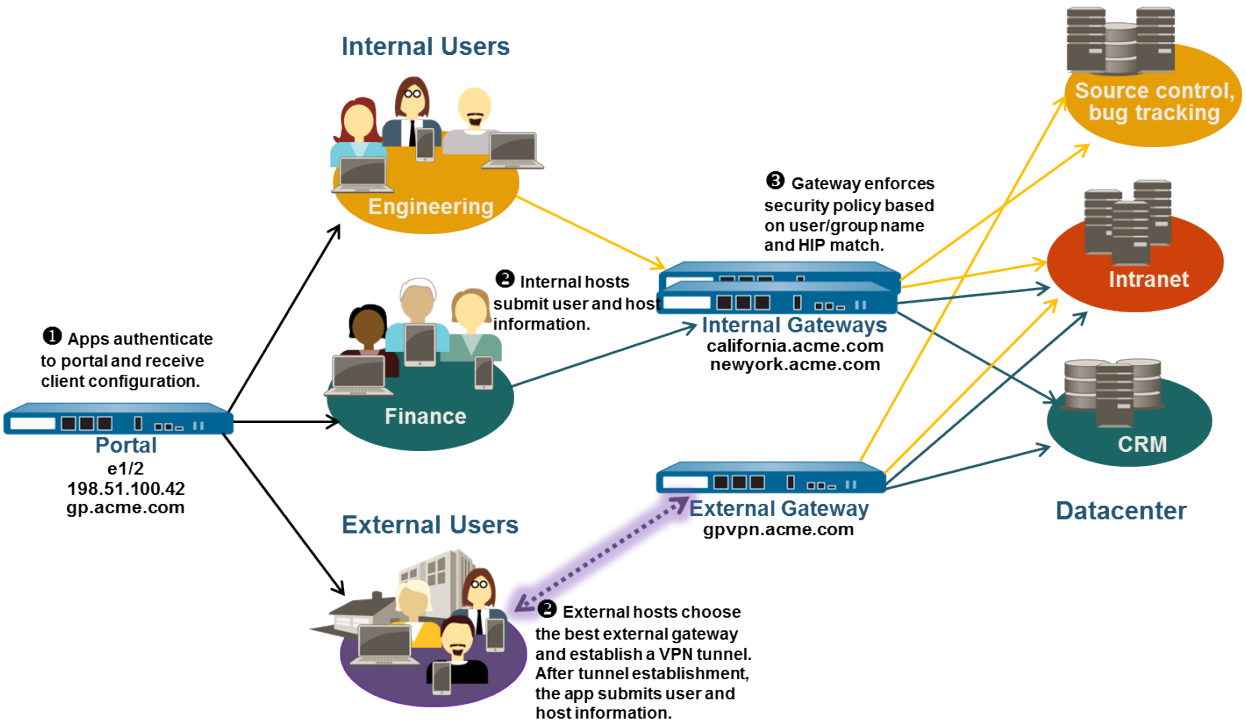


Figure 9: Implementación de GlobalProtect con puertas de enlace internas y externas

Utilice los siguientes pasos para configurar una combinación de puertas de enlace de GlobalProtect internas y externas.

STEP 1 | Creación de interfaces y zonas para GlobalProtect.

En esta configuración, debe configurar las interfaces en el cortafuegos que aloja un portal y en todos los cortafuegos que alojan una puerta de enlace.

No vincule un perfil de gestión de interfaces que permita HTTP, HTTPS, Telnet o SSH en las interfaces donde haya configurado un portal o una puerta de enlace de GlobalProtect, ya que franquearía el acceso a la interfaz de gestión desde internet. Siga las recomendaciones de las Prácticas recomendadas para proteger el acceso administrativo para garantizar la seguridad del acceso administrativo a sus cortafuegos, de forma que evitará ataques efectivos.

Utilice el enrutador virtual default (por defecto) para que todas las configuraciones de la interfaz eviten tener que crear el enrutamiento entre zonas.

En el cortafuegos que aloja la puerta de enlace del portal (gp.acme.com):

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y configure **ethernet1/2** como interfaz de Ethernet capa 3 con la dirección IP `198.51.100.42`. Asígnela a la **Security Zone** `l3-untrust` y al **Virtual Router (Enrutador virtual)** predeterminado.
- Cree un registro “A” de DNS que asigne la dirección IP 198.51.100.42 a gp.acme.com.
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir la interfaz `tunnel.2`. Añádala a una nueva **Security Zone (Zona de seguridad)** llamada `corp-vpn` y, luego, al **Virtual Router (Enrutador virtual)** predeterminado.
- Marque Enable User Identification (Habilitar identificación de usuarios) en la zona corp-vpn.

En el cortafuegos que aloja la puerta de enlace externa (gpvpn.acme.com):

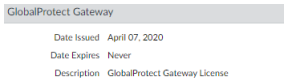
© 2020 Palo Alto Networks, Inc.

- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y configure **ethernet1/5** como interfaz de Ethernet capa 3 con la dirección IP **`192.0.2.4`**. Asígnela a la **Security Zone** **`l3-untrust`** y al **Virtual Router (Enrutador virtual)** predeterminado.
- Cree un registro "A" DNS que asigne la dirección IP 192.0.2.4 en gpvpn.acme.com.
- Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir la interfaz **`tunnel.3`**. Añádala a una nueva **Security Zone (Zona de seguridad)** llamada `corp-vpn` y, luego, al **Virtual Router (Enrutador virtual)** predeterminado.
- Marque Enable User Identification (Habilitar identificación de usuarios) en la zona corp-vpn.

En el cortafuegos que aloja las puertas de enlace internas (california.acme.com y newyork.acme.com):

- Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y configure una interfaz de Ethernet capa 3 con la dirección IP en la red interna. Asígnela a la **Security Zone** **`l3-trust`** y al **Virtual Router (Enrutador virtual)** predeterminado.
- Cree un registro "A" DNS que asigne las direcciones IP internas california.acme.com y newyork.acme.com.
- Habilite la identificación de usuarios en la zona l3-fiable.

STEP 2 | Compre e instale una suscripción de GlobalProtect para cada cortafuegos que aloje una puerta de enlace (interna y externa) si sus usuarios finales utilizarán la aplicación de GlobalProtect en sus endpoints móviles o si planea utilizar la política de seguridad habilitada para HIP.



Después de adquirir suscripciones de GlobalProtect y de recibir su código de activación, instale las suscripciones de GlobalProtect en los cortafuegos que alojan sus puertas de enlace:

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
2. Seleccione **Activate feature using authorization code (Activar característica mediante código de autorización)**.
3. Cuando se le indique, introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**.
4. Compruebe que la licencia y las suscripciones se hayan activado correctamente.

Póngase en contacto con su ingeniero de ventas o distribuidor de Palo Alto Networks si no tiene todas las licencias necesarias. Si desea obtener más información sobre licencias, consulte Acerca de las licencias de GlobalProtect.

STEP 3 | Obtenga certificados de servidor para el portal de GlobalProtect y cada puerta de enlace de GlobalProtect.

Para conectarse al portal por primera vez, los endpoints deben confiar en el certificado de CA raíz utilizado para emitir el certificado de servidor del portal.

Puede utilizar certificados autofirmados en las puertas de enlace e implementar el certificado de CA raíz para las aplicaciones en la configuración de cliente. Se recomienda generar todos los certificados del cortafuegos que aloja el portal e implementarlos en las puertas de enlace.

El flujo de trabajo recomendado es el siguiente:

1. En el cortafuegos que aloja el portal:
    1. Importe un certificado de servidor desde una CA externa conocida.
    2. Cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

3. Uso de la CA raíz en el portal para generar un certificado de servidor autofirmado. Repita este paso para cada puerta de enlace.

2. En todos los cortafuegos que alojan una puerta de enlace interna:
   - Implemente los certificados de servidor autofirmados.

STEP 4 | Defina cómo autenticar a los usuarios en el portal y las puertas de enlace.

Puede utilizar cualquier combinación de perfiles de certificado o perfiles de autenticación para garantizar la seguridad del portal y las puertas de enlace. Los portales y las puertas de enlace individuales también pueden utilizar distintos esquemas de autenticación. Consulte las siguientes secciones para obtener instrucciones detalladas:

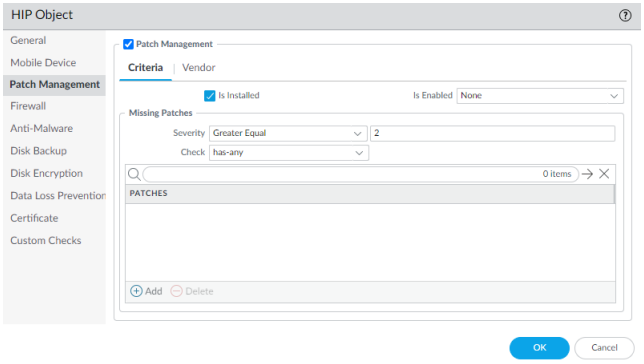
- Configuración de autenticación externa (perfil de autenticación)
- Configuración de la autenticación de certificado de cliente (perfil de certificado)
- Configuración de la autenticación en dos fases (basada en token u OTP)

Luego, debe hacer referencia al perfil del certificado o perfiles de autenticación que ha definido en las configuraciones de puerta de enlace y portal.

STEP 5 | Cree los perfiles HIP que necesitará para aplicar la política de seguridad en el acceso a la puerta de enlace.

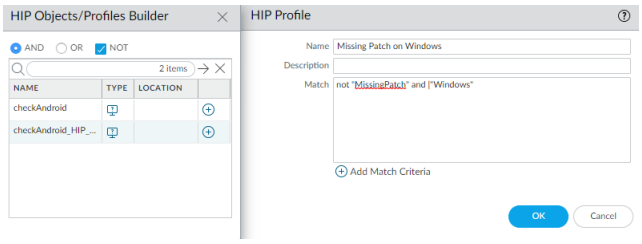
Consulte la Información de host para obtener más información sobre las evaluaciones HIP.

1. Cree objetos HIP para filtrar los datos del host sin procesar recopilados por la aplicación. Por ejemplo, si está interesado en avisar a usuarios no actualizados sobre los parches que necesitan, puede crear un objeto HIP con el cual coincidir si el software de gestión de parches está instalado y que todos los parches con una gravedad determinada estén actualizados.



2. Cree los perfiles HIP que planea usar en sus políticas.

   Por ejemplo, si quiere asegurarse de que solo los endpoints de Windows con parches actualizados puedan acceder a sus aplicaciones internas, puede que desee adjuntar el siguiente perfil HIP que coincida con los hosts a los que NO les falte ningún parche:



STEP 6 | Configure las puertas de enlace internas.

© 2020 Palo Alto Networks, Inc.

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y haga clic en **Add (Añadir)** para añadir la configuración de la puerta de enlace con los siguientes ajustes:

- **Interface (Interfaz)**
- **Dirección IP**
- **Server Certificate (Certificado de servidor)**
- **Authentication Profile (Perfil de autenticación)** o **Configuration Profile (Perfil de configuración)**

Observe que no es necesario configurar los ajustes de la configuración cliente en las configuraciones de la puerta de enlace (a no ser que desee establecer las notificaciones HIP) porque las conexiones de túnel no son necesarias. Consulte Configuración de una puerta de enlace de GlobalProtect para ver instrucciones detalladas sobre cómo crear configuraciones de puerta de enlace.

STEP 7 | Configure los Portales de GlobalProtect.

Aunque este ejemplo muestra cómo crear una configuración de cliente única que se implementará para todos los aplicaciones, también puede elegir crear configuraciones separadas para distintos usos y, luego, implementarlas según el nombre del grupo/usuario o el sistema operativo del endpoint en el que se ejecuta la aplicación.

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y haga clic en **Add (Añadir)** para añadir la siguiente configuración del portal:

1. Configuración del acceso al portal de GlobalProtect:

   Interface (Interfaz): `ethernet1/2`

   IP Address (Dirección IP): `10.31.34.13`

   Server Certificate (Certificado de servidor): `GP-server-cert.pem issued by GoDaddy` with `CN=gp.acme.com`
2. Definición de las configuraciones de autenticación de cliente de GlobalProtect:

   Internal Host Detection (Detección de host interno): `enabled`

   Use Single Sign-On (Usar inicio de sesión único): `enabled`

   Connect Method (Método de conexión): `User-logon (Always On)`

   External Gateway Address (Dirección de puerta de enlace externa): `gpvpn.acme.com`

   Internal Gateway Address (Dirección de puerta de enlace interna): `california.acme.com, newyork.acme.com`

   User/User Group (Usuario/grupo de usuarios): cualquiera
3. Seleccione **Commit (Confirmar)** para aplicar la configuración del portal.

STEP 8 | Implementación del software de la aplicación de GlobalProtect

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)**.

En este ejemplo, utilice el procedimiento de Alojamiento de actualizaciones de la aplicación en el portal.

STEP 9 | Cree reglas de políticas de seguridad en cada puerta de enlace para permitir que los usuarios de su VPN accedan de forma segura a las aplicaciones.

- Cree políticas de seguridad (**Policies [Políticas]** > **Security [Seguridad]**) para habilitar el flujo de tráfico entre la zona corp-vpn y la zona l3-trust.
- Cree reglas de políticas habilitadas para HIP o basadas en usuario/grupo para permitir el acceso granular a sus recursos internos del centro de datos.

© 2020 Palo Alto Networks, Inc.

- Para obtener visibilidad, cree reglas que permitan a todos los usuarios un acceso de navegación web a la zona l3-nofiable con perfiles de seguridad predeterminados que lo protejan de amenazas conocidas.

			Source				Destination					
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	CRM access	none	corp-vpn l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default		none
2	Eng access	none	corp-vpn l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default		none
3	GP access	none	corp-vpn l3-trust	any	any	any	l3-untrust	any	web-browsing	application-default		

STEP 10 | Guarde la configuración de GlobalProtect.

Haga clic en **Commit (Confirmar)** para confirmar la configuración del portal y la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

Portal cautivo y uso obligatorio de GlobalProtect para acceder a la red

En la mayoría de los casos, los usuarios móviles se conectan a redes wifi en las que se ha habilitado un portal cautivo, como las de cafeterías, aeropuertos y hoteles. Para acceder a Internet, tienen que entrar en dicho portal en una página de inicio de sesión del navegador o mediante un asistente basado en el sistema operativo especificando ciertos identificadores, como un nombre y una dirección de correo electrónico. Esta configuración permite limitar el tiempo que pueden permanecer conectados al portal cautivo. Si el usuario inicia sesión para acceder a internet, la aplicación de GlobalProtect establece una conexión automáticamente. Si no inicia sesión dentro del período especificado, se bloquea todo el tráfico.

Si desea reducir aún más el riesgo de exposición a las amenazas contra la seguridad, especifique también el uso obligatorio de GlobalProtect para acceder a la red. Si habilita esta opción, GlobalProtect bloquea todo el tráfico de red hasta que la aplicación se conecta a una puerta de enlace de GlobalProtect. Como debe atravesar el túnel de red privada virtual (virtual private network, VPN) para someterlo a inspección y aplicarle las políticas, mantiene total visibilidad y pleno control sobre el tráfico de los usuarios.

Para acceder a la red, los usuarios deben seguir distintos flujos de trabajo en función de si existe un portal cautivo y de si es obligatoria la conexión de GlobalProtect:

portal cautivo	Uso obligatorio de GlobalProtect para acceder a la red	Flujo de trabajo
yes (sí)	yes (sí)	Si es obligatoria la conexión de GlobalProtect para entrar en la red y si también es preciso iniciar sesión en el portal cautivo para acceder a internet, debe seguir estos pasos: 1. Conéctese a la red wifi. Una vez establecida la conexión, GlobalProtect detecta automáticamente el portal cautivo. Si el administrador configura un mensaje de detección de portal cautivo, la aplicación de GlobalProtect le indica que debe iniciar sesión en él para acceder a la red. *Los administradores también pueden configurar el tiempo que debe transcurrir para que se muestre el mensaje de detección del portal cautivo.* 2. Para iniciar sesión en el portal cautivo, elija una de estas opciones: • Abra un navegador web y vaya a la página de inicio de sesión en el portal cautivo. • Inicie sesión con el asistente del portal cautivo integrado en el sistema operativo del terminal.

© 2020 Palo Alto Networks, Inc.

portal cautivo	Uso obligatorio de GlobalProtect para acceder a la red	Flujo de trabajo
		Si el inicio de sesión es correcto, puede acceder a internet, y la aplicación de GlobalProtect se conecta de forma automática. Si la aplicación no se conecta de inmediato y el administrador configura una notificación de bloqueo del tráfico para señalar que se debe conectar a GlobalProtect a fin de tener acceso a la red, aparece ese mensaje hasta que se establezca la conexión. *Los administradores también pueden configurar el tiempo que debe transcurrir para que se muestre la notificación de bloqueo del tráfico.* Si no logra iniciar sesión y se agota el tiempo de espera de la página de inicio de sesión en el portal cautivo o si GlobalProtect no consigue establecer la conexión, no puede utilizar la red. Para empezar de cero el proceso y renovar el tiempo permitido, inicie la aplicación de GlobalProtect y, a continuación, seleccione **Refresh Connection (Actualizar conexión)** en el menú de configuración de la aplicación ( ).
yes (sí)	No	Si es preciso iniciar sesión en el portal cautivo para acceder a internet, pero la conexión de GlobalProtect no es obligatoria para entrar en la red, debe seguir estos pasos: 1. Conéctese a la red wifi. Una vez establecida la conexión, GlobalProtect detecta automáticamente el portal cautivo. 2. Para iniciar sesión en el portal cautivo, elija una de estas opciones: • Abra un navegador web y vaya a la página de inicio de sesión en el portal cautivo. • Inicie sesión con el asistente del portal cautivo integrado en el sistema operativo del terminal. Si el inicio de sesión es correcto, puede acceder a internet, y la aplicación de GlobalProtect se conecta de forma automática.
No	yes (sí)	Si es obligatoria la conexión de GlobalProtect para entrar en la red, pero no hace falta iniciar sesión en el portal cautivo para acceder a internet, se debe conectar a la red wifi. En cuanto se conecta a la red wifi, puede acceder a internet, y la aplicación de GlobalProtect se conecta de forma automática. Si la aplicación no se conecta de inmediato y el administrador configura una notificación de bloqueo del tráfico para señalar

© 2020 Palo Alto Networks, Inc.

portal cautivo	Uso obligatorio de GlobalProtect para acceder a la red	Flujo de trabajo
		que se debe conectar a GlobalProtect a fin de tener acceso a la red, aparece ese mensaje hasta que se establezca la conexión. Si GlobalProtect no consigue establecer la conexión, no puede utilizar la red. En ese caso, debe volver a detectar la red. Para ello, desconéctese y, a continuación, vuelva a conectar a la red wifi, reinicie el terminal o actualice la conexión de GlobalProtect.

Si desea personalizar la configuración del portal cautivo y especificar si la conexión de GlobalProtect es obligatoria para acceder a la red, siga estos pasos:

Configure la opción Enforce GlobalProtect for Network Access (Forzar el uso de GlobalProtect para acceder a la red) solo si configura el método de conexión siempre activa en GlobalProtect.

STEP 1 | Configuración del acceso al portal de GlobalProtect.

STEP 2 | Definición de las configuraciones de agente de GlobalProtect.

STEP 3 | Personalización de la aplicación de GlobalProtect.

- Para garantizar que la conexión de GlobalProtect esté activa siempre, defina **Connect Method (Método de conexión)** en **User-logon (Always On) (Inicio de sesión de usuario [siempre activo])**.
- Si los usuarios deben iniciar sesión en un portal cautivo para acceder a internet, defina las opciones siguientes para personalizar la configuración del portal:
  - En el campo **Captive Portal Exception Timeout (sec) (Tiempo de espera para excepción de portal cautivo [s])**, introduzca los segundos que tienen los usuarios para iniciar sesión en el portal cautivo; el intervalo es de 0 a 3600 y el valor predeterminado, 0 segundos. Si no inician sesión antes de que transcurra este tiempo, se agota el tiempo de espera de la página de inicio de sesión en el portal cautivo y se impide el uso de la red a los usuarios.
  - Para que la aplicación de GlobalProtect notifique que ha detectado un portal cautivo, configure **Display Captive Portal Detection Message (Mostrar mensaje de detección de portal cautivo)** en **Yes (Sí)**.
    - En el campo **Captive Portal Notification Delay (sec) (Demora de notificación de portal cautivo [s])**, introduzca los segundos que tarda la aplicación de GlobalProtect en mostrar el mensaje de detección del portal cautivo; el intervalo es de 1 a 120 y el valor predeterminado, 5 segundos. GlobalProtect inicia este temporizador después de detectar el portal cautivo, pero antes de poder acceder a internet.
    - En **Captive Portal Detection Message (Mensaje de detección de portal cautivo)**, personalice la notificación que se muestra cuando GlobalProtect detecta un portal cautivo.
- Para que todo el tráfico de red deba atravesar el túnel de VPN de GlobalProtect, configure estas opciones:
  - Defina la opción **Enforce GlobalProtect for Network Access (Forzar el uso de GlobalProtect para acceder a la red)** en **Yes (Sí)**.
  - Para que la aplicación de GlobalProtect notifique que es obligatorio establecer la conexión de GlobalProtect para acceder a la red, defina **Display Traffic Blocking Notification Message (Mostrar mensaje de notificación de bloqueo de tráfico)** en **Yes (Sí)**. La aplicación de

© 2020 Palo Alto Networks, Inc.

GlobalProtect muestra este mensaje cuando se puede acceder a internet, pero aún no se ha establecido la conexión de GlobalProtect.

- En el campo **Traffic Blocking Notification Delay (sec) (Demora de notificación de bloqueo de tráfico [s])**, introduzca los segundos que tarda la aplicación de GlobalProtect en mostrar el mensaje de notificación del bloqueo del tráfico; el intervalo es de 5 a 120 y el valor predeterminado, 15 segundos. GlobalProtect inicia este temporizador cuando ya se puede acceder a internet.
- En **Traffic Blocking Notification Message (Mensaje de notificación de bloqueo de tráfico)**, personalice la notificación que se muestra cuando es obligatoria la conexión de GlobalProtect para acceder a la red. Este mensaje puede tener 512 caracteres como máximo.

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

Arquitectura de GlobalProtect

En esta sección se describe una arquitectura de referencia de ejemplo para implementar GlobalProtect™, que protege el tráfico de internet y franquea el acceso seguro a los recursos de la empresa.

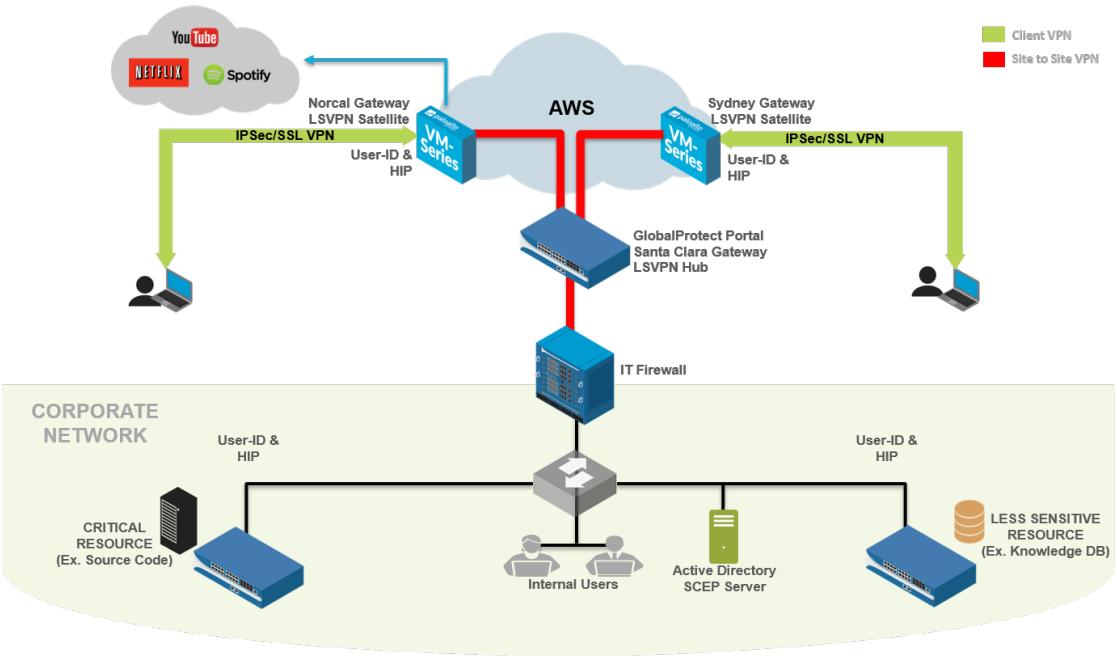
La arquitectura de referencia y las pautas descritas en esta sección proporcionan un escenario de implementación común. Antes de adoptar esta arquitectura, identifique los requisitos de seguridad, capacidad de gestión de infraestructura y experiencia del usuario final de su empresa y, luego, implemente GlobalProtect sobre la base de estos requisitos.

Aunque los requisitos pueden ser diferentes para cada empresa, puede aprovechar los principios comunes y las consideraciones de diseño descritas en este documento, junto con las pautas de configuración recomendadas, para cumplir las necesidades de seguridad de su empresa.

> Topología de la arquitectura de referencia de GlobalProtect
> Características de la arquitectura de referencia de GlobalProtect
> Configuraciones de la arquitectura de referencia de GlobalProtect

© 2020 Palo Alto Networks, Inc.

Topología de la arquitectura de referencia de GlobalProtect



- Portal GlobalProtect
- Puertas de enlace de GlobalProtect

Portal GlobalProtect

En esta topología, un PA-3020 en el espacio de ubicación compartida actúa como portal de GlobalProtect.

Los empleados y contratistas pueden autenticarse en el portal con la autenticación en dos fases (2FA), que consiste en credenciales de Active Directory (AD) y una contraseña de un solo uso (one-time password, OTP). El portal implementa configuraciones de cliente de GlobalProtect en función de la pertenencia de un usuario o grupo, y del sistema operativo.

Al establecer una configuración de cliente de portal separada que se aplica a un pequeño grupo o conjunto de usuarios piloto, usted puede probar las funciones antes de aplicarlas en una base de usuarios más amplia. Cualquier configuración de cliente que contenga funciones nuevas (como Enforce GlobalProtect o el Protocolo de inscripción de certificados simple [Simple Certificate Enrollment Protocol, SCEP], funciones disponibles con PAN-OS 7.1 y actualizaciones de contenido posteriores) se habilita en la configuración piloto primero y los usuarios piloto la validan antes de que esté disponible para los demás.

El portal de GlobalProtect también envía configuraciones a los satélites de GlobalProtect. Esta configuración incluye las puertas de enlace de GlobalProtect a las cuales los satélites pueden conectarse y establecer un túnel de sitio a sitio.

Puertas de enlace de GlobalProtect

El PA-3020 en el espacio de ubicación compartida (que se mencionó anteriormente) también se duplica como puerta de enlace de GlobalProtect (la puerta de enlace Santa Clara). Diez puertas de enlace adicionales se implementan en Amazon Web Services (AWS) y la nube pública de Microsoft Azure. Las

© 2020 Palo Alto Networks, Inc.

regiones o ubicaciones POP en las que se implementan estas puertas de enlace adicionales de WAS y Azure se basan en la distribución de empleados en todo el mundo.

- **Puerta de enlace Santa Clara**: los empleados y contratistas pueden autenticarse en la puerta de enlace Santa Clara (PA-3020 en el espacio de ubicación compartida) con 2FA. Esta puerta de enlace requiere que los usuarios proporcionen sus credenciales de Active Directory y su OTP. Debido a que esta puerta de enlace protege los recursos delicados, se configura como una puerta de enlace solo manual. Como resultado, los usuarios no se conectan a esta puerta de enlace de forma automática, sino que deben elegir conectarse de forma manual. Por ejemplo, cuando los usuarios se conectan a AWS-Norcal, que no es una puerta de enlace solo anual, ciertos recursos internos importantes no están disponibles. Entonces, el usuario debe cambiar manualmente y autenticarse con la puerta de enlace Santa Clara para acceder a estos recursos.

  Además, la puerta de enlace Santa Clara se configura como un punto de finalización de túnel VPN de gran escala (Large Scale VPN, LSVPN) para las conexiones satelitales desde puertas de enlace en AWS y Azure. La puerta de enlace Santa Clara también está configurada para establecer un túnel de seguridad de protocolo de Internet (Internet Protocol Security, IPSec) en el cortafuegos de TI de la sede corporativa. Este es el túnel que brinda acceso a los recursos de la sede corporativa.
- **Puertas de enlace de Amazon Web Services y Microsoft Azure**: estas puertas de enlace requieren 2FA: un certificado de cliente y credenciales de Active Directory. El portal de GlobalProtect distribuye el certificado de cliente necesario para autenticarse en estas puertas de enlace con la función SCEP de GlobalProtect.

  Estas puertas de enlace en la nube pública también actúan como satélites de GlobalProtect. Se comunican con el portal de GlobalProtect, descargan la configuración del satélite y establecen un túnel de sitio a sitio con la puerta de enlace Santa Clara. Los satélites de GlobalProtect inicialmente se autentican con números de serie y luego con certificados.
- **Puertas de enlace dentro de la sede corporativa**: dentro de la sede corporativa, tres cortafuegos funcionan como puertas de enlace de GlobalProtect. Estas son puertas de enlace internas que no requieren endpoints para configurar un túnel. Los usuarios se autentican en estas puertas de enlace usacon sus credenciales de Active Directory. Estas puertas de enlace internas usan GlobalProtect para identificar el ID de usuario y recopilar el Perfil de información del host (Host Information Profile, HIP) de los endpoints.

  Para que la experiencia de usuario sea óptima, puede configurar estas puertas de enlace internas de modo que autentiquen a los usuarios con certificados proporcionados por SCEP o con vales de servicio de Kerberos.

© 2020 Palo Alto Networks, Inc.

Características de la arquitectura de referencia de GlobalProtect

- Experiencia del usuario final
- Gestión y registro
- Control y alta disponibilidad

Experiencia del usuario final

Los usuarios finales remotos (que no están en la red corporativa) se conectan a una de las puertas de enlace en AWS o Azure. Cuando establezca la configuración de cliente del portal de GlobalProtect, asigne la misma prioridad a las puertas de enlace. Con esta configuración, la puerta de enlace a la cual se conectan los usuarios finales depende del tiempo de respuesta SSL de cada puerta de enlace, medido en el endpoint durante el tiempo de configuración del túnel.

Por ejemplo, un usuario en Australia generalmente se conectaría a la puerta de enlace AWS-Sydney. Una vez que el usuario se conecta a AWS-Sydney, la aplicación de GlobalProtect canaliza todo el tráfico desde el endpoint hacia el cortafuegos AWS-Sydney para su inspección. GlobalProtect envía el tráfico a los sitios públicos de Internet directamente por esta puerta de enlace y canaliza el tráfico a los recursos empresariales a través de un túnel de sitio a sitio entre dicha puerta y la puerta de enlace Santa Clara y, luego, a través de un túnel de sitio a sitio del protocolo de seguridad del protocolo de internet (internet protocol security, IPSec) hasta la sede empresarial. Esta arquitectura está diseñada para reducir la latencia que experimenta el usuario al acceder a internet. Si no se puede acceder a la puerta de enlace AWS-Sydney o a otra más cercana a Sídney, la aplicación de GlobalProtect restituye el tráfico de internet al cortafuegos de la sede empresarial y provoca problemas de latencia.

Los servidores de Active Directory residen dentro de la red corporativa. Cuando los usuarios remotos se autentican, la aplicación de GlobalProtect envía solicitudes de autenticación a través del túnel de sitio a sitio en AWS/Azure a la puerta de enlace Santa Clara. La puerta de enlace luego reenvía la solicitud a través de un túnel IPsec de sitio a sitio al servidor de Active Directory en la sede corporativa.

Para reducir el tiempo que lleva la autenticación del usuario remoto y la configuración del túnel, considere replicar el servidor de Active Directory y ponerlo a disposición en AWS.

Los usuarios finales dentro de la red corporativa se autentican en las tres puertas de enlace internas inmediatamente después de iniciar sesión. La aplicación de GlobalProtect envía el informe HIP a estas puertas de enlace internas. Los usuarios que están dentro de la oficina de la red corporativa deben reunir los requisitos de User-ID y HIP para acceder a cualquier recurso en el trabajo.

Gestión y registro

En esta implementación, usted puede gestionar y configurar todos los cortafuegos desde Panorama, que se implementa en el espacio de ubicación compartida.

Para proporcionar seguridad sistemática, todos los cortafuegos en AWS y Azure utilizan las mimas políticas y configuraciones de seguridad. Para simplificar la configuración de las puertas de enlace, Panorama también utiliza un grupo de dispositivos y una plantilla. En esta implementación, todas las puertas de enlace reenvían todos los registros a Panorama. Esto le permite controlar el tráfico de la red o resolver problemas desde una ubicación central, en lugar de tener que iniciar sesión en cada cortafuegos.

© 2020 Palo Alto Networks, Inc.

Cuando se necesitan actualizaciones de software, puede usar Panorama para implementar las actualizaciones de software en todos los cortafuegos. Panorama primero actualiza uno o dos cortafuegos, y verifica si la actualización se realizó correctamente antes de actualizar el resto de los cortafuegos.

Control y alta disponibilidad

Para supervisar los cortafuegos en esta implementación, puede usar Nagios, que es un software de supervisión de registros, red y servidor de código abierto. Configure Nagios para que verifique periódicamente la respuesta del portal y la página de inicio de sesión anterior de las puertas de enlace, y para que envíe un alerta si la respuesta no coincide con las expectativas. También puede configurar los objetos de la base de información de gestión (Management Information Base, MIB) del protocolo simple de gestión de red (Simple Network Management Protocol, SNMP) de GlobalProtect para controlar el uso de la puerta de enlace.

En esta implementación, solo existe una instancia del portal de GlobalProtect. Si el portal no estuviera disponible, los usuarios nuevos (que nunca antes se conectaron al portal) no podrán conectarse a GlobalProtect. Sin embargo, los usuarios existentes pueden usar la configuración de cliente del portal en la caché para conectarse a una de las puertas de enlace.

Varios cortafuegos de equipo virtual (virtual machine, VM) en AWS configurados como puertas de enlace de GlobalProtect proporcionan redundancia de puerta de enlace. Por lo tanto, no es necesaria la configuración de puertas de enlace como par de alta disponibilidad (high availability, HA).

© 2020 Palo Alto Networks, Inc.

Configuraciones de la arquitectura de referencia de GlobalProtect

Para alinear su implementación con la arquitectura de referencia, revise las siguientes listas de comprobación de configuración.

- Configuración de puerta de enlace
- Configuración portal
- Configuraciones de política

Configuración de puerta de enlace

- Desactive los túneles divididos. Para hacerlo, asegúrese de que no existan rutas de acceso especificadas en **Agent (Agente)** > **Client Settings (Ajustes de cliente)** > **Split Tunnel (Túnel dividido)**. Consulte Configuración de una puerta de enlace de GlobalProtect.
- Habilite **No direct access to local network (Sin acceso directo a la red local)** en **Agent (Agente)** > **Client Settings (Ajustes de cliente)** > **Split Tunnel (Túnel dividido)**. Consulte Configuración de una puerta de enlace de GlobalProtect.
- Habilite la opción de la puerta de enlace **Accept cookie for authentication override (Aceptar cookie para la invalidación de la autenticación)**. Consulte Configuración de una puerta de enlace de GlobalProtect.

Configuración portal

- Configure el **Connect Method (Método de conexión)** como **Always-on (User logon) (Siempre activado [inicio de sesión del usuario])**. Consulte Personalización de la aplicación de GlobalProtect.
- Configure **Use Single Sign-On (Windows only) (Usar inicio de sesión único [Windows únicamente])** como **Yes (Sí)**. Consulte Personalización de la aplicación de GlobalProtect.
- Configure el portal en **Save User Credentials (Guardar credenciales del usuario)** (configure el valor como **Yes [Sí]**). Consulte Definición de las configuraciones de agente de GlobalProtect.
- Habilite el portal en la opción **Accept cookie for authentication override**. Consulte Definición de las configuraciones de agente de GlobalProtect.
- Configure **Cookie Lifetime (Duración de la cookie)** en 20 horas. Consulte Definición de las configuraciones de agente de GlobalProtect.
- **Enforce GlobalProtect (Aplicar GlobalProtect)** para el acceso de red. Consulte Personalización de la aplicación de GlobalProtect.
- Cuando está habilitada la opción **Enforce GlobalProtect for Network Access (Aplicar GlobalProtect para el acceso de red)**, se permite que los usuarios inhabiliten la aplicación de GlobalProtect con un código de acceso. Consulte Personalización de la aplicación de GlobalProtect.
- Configure **Internal Host Detection**. Consulte Definición de las configuraciones de agente de GlobalProtect.
- Habilite la opción **Collect HIP Data** en Data Collection. Consulte Definición de las configuraciones de agente de GlobalProtect.
- Distribuya e instale el certificado de CA de proxy de reenvío SSL utilizado para el cifrado SSL. Consulte Definición de las configuraciones de agente de GlobalProtect.

Configuraciones de política

- Configure todos los cortafuegos para que utilicen políticas de seguridad y perfiles basados en la Política recomendada para la seguridad de la puerta de enlace de Internet. En esta implementación de referencia,

© 2020 Palo Alto Networks, Inc.

esto incluye la puerta de enlace Santa Clara en el espacio de ubicación compartida y las puertas de enlace de la nube pública AWS/Azure.

- Habilite Descifrado SSL en todas las puertas de enlace en AWS y Azure.
- Configure reglas de reenvío basado en políticas para todas las puertas de enlace en AWS para reenviar el tráfico a ciertos sitios web a través de la puerta de enlace Santa Clara. Esto garantiza que los sitios como www.stubhub.com y www.lowes.com que bloquean el tráfico desde los intervalos de direcciones IP de AWS aún estén disponibles cuando los usuarios se conectan a las puertas de enlace en AWS.

Criptografía de GlobalProtect

- Acerca de la selección de cifrado de GlobalProtect
- Intercambio de cifrado entre el agente y la puerta de enlace de GlobalProtect
- Referencias de criptografía de GlobalProtect
- Cifrados utilizados para configurar túneles de IPSec
- API para SSL

© 2020 Palo Alto Networks, Inc.

Acerca de la selección de cifrado de GlobalProtect

GlobalProtect admite los modos de túnel SSL e IPsec. GlobalProtect también admite la capacidad de habilitar y solicitar a la aplicación de GlobalProtect que siempre intente configurar primero un túnel IPsec antes de recurrir a un túnel SSL. Con un túnel IPsec, la aplicación de GlobalProtect usa SSL/TLS para intercambiar las claves y algoritmos de autenticación y cifrado. La selección del conjunto de cifrado que GlobalProtect utiliza para proteger el túnel SSL/TLS depende de:

- **Versiones SSL/TLS aceptadas por la puerta de enlace**: La puerta de enlace y el portal de GlobalProtect pueden restringir la lista de conjuntos de cifrado disponibles para la aplicación que usa perfiles SSL/TLS. En el cortafuegos, cree el perfil SSL/TLS, especifique el certificado y las versiones de protocolo permitidas, y asócielo al portal y la puerta de enlace de GlobalProtect.
- **Algoritmo del certificado de servidor de la puerta de enlace**: El sistema operativo del endpoint determina qué conjuntos de cifrado incluye la aplicación de GlobalProtect en su mensaje de bienvenida del cliente. Siempre que la aplicación de GlobalProtect incluya el conjunto de cifrado que la puerta de enlace prefiera usar, la puerta de enlace seleccionará ese conjunto de cifrado para la sesión SSL. El orden de los conjuntos de cifrado dentro del mensaje de bienvenida del cliente no afecta la selección de conjunto de cifrado: La puerta de enlace selecciona el conjunto de cifrado según el Perfil de servicio SSL/TLS y el algoritmo del certificado del servidor de puerta de enlace y su lista preferida. Seleccione el perfil de servicio de la configuración de autenticación de la puerta de enlace de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Intercambio de cifrado entre la puerta de enlace y la aplicación de GlobalProtect

La figura siguiente muestra el intercambio de cifrados entre las puertas de enlace y las aplicaciones de GlobalProtect cuando se crea el túnel VPN.

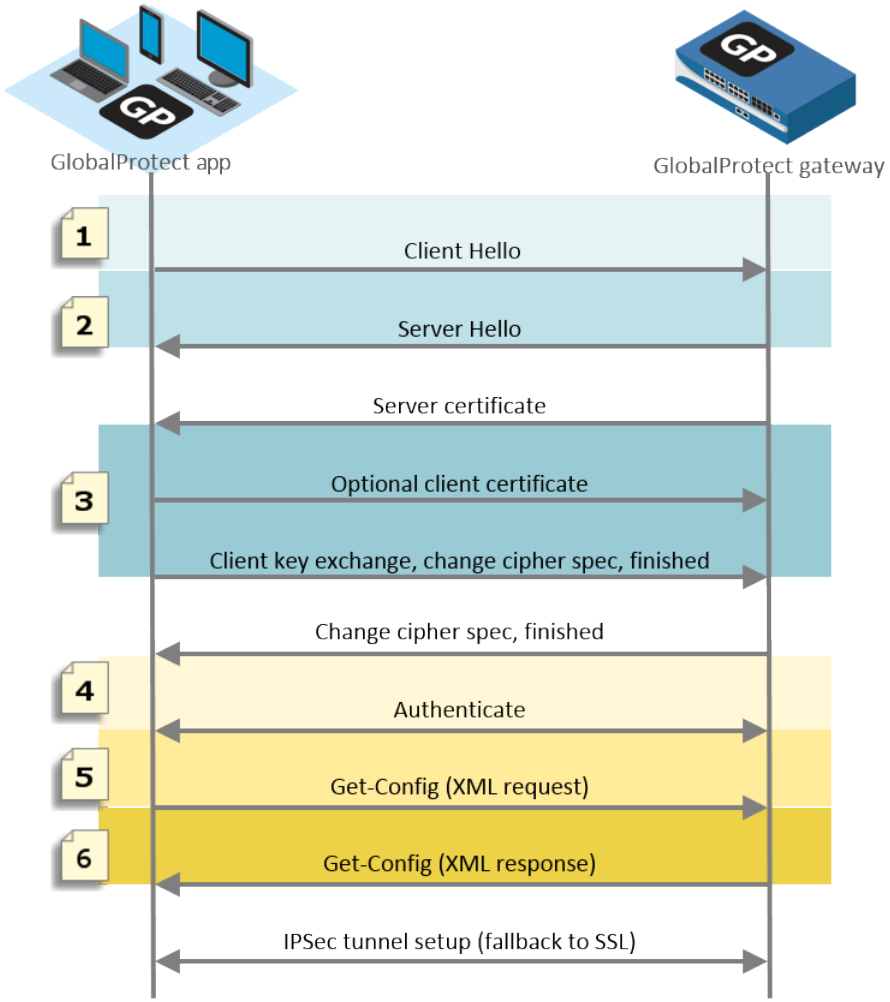


Figure 10: Intercambio de cifrado entre la puerta de enlace y la aplicación

La tabla siguiente describe estas etapas de forma más detallada:

Table 9: Intercambio de cifrado entre la puerta de enlace y la aplicación

Etapa de comunicación	Description (Descripción)
1. Mensaje de bienvenida del cliente	La aplicación brinda una lista de conjuntos de cifrado según el sistema operativo del endpoint.
2. Mensaje de bienvenida del servidor	La puerta de enlace selecciona el conjunto de cifrado brindado por la aplicación. Cuando se seleccionan los cifrados para configurar el túnel, la

© 2020 Palo Alto Networks, Inc.

Etapa de comunicación	Description (Descripción)
	puerta de enlace ignora la cantidad y el orden de estos y, en cambio, utiliza las versiones SSL/TLS y el algoritmo del certificado del servidor de la puerta de enlace y su lista de preferencia (como se describe en Acerca de la selección de cifrado de GlobalProtect).
3. Certificado de cliente opcional	De manera opcional, la puerta de enlace puede solicitar un certificado de cliente de la aplicación para usarlo a fin de confiar en la identidad del usuario o endpoint.
4. Sesión SSL	Luego de configurar la sesión SSL/TLS, la aplicación se autentica con la puerta de enlace y solicita la configuración de esta (Get-Config-Request). Para solicitar la configuración, la aplicación brinda los algoritmos de cifrado y autenticación y otros ajustes, como la dirección IP de preferencia de la interfaz del túnel. La puerta de enlace responde a la solicitud y selecciona el algoritmo de cifrado y autenticación que se utilizará en función de la configuración del perfil criptográfico de IPSec de GlobalProtect (Get-Config-Response).

La siguiente tabla muestra un ejemplo del intercambio de cifrado entre una aplicación en un endpoint de macOS y la puerta de enlace.

Table 10: Ejemplo: Intercambio de cifrado para endpoints de macOS

Etapa de comunicación	Ejemplo: endpoints macOS
1. Mensaje de bienvenida del cliente	TLS 1.2 37 conjuntos de cifrado (Referencia: Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de macOS)
2. Mensaje de bienvenida del servidor	• Cuando GlobalProtect utiliza un certificado ECDSA y se acepta TLS 1.2, la sesión SSL usa ECDSA-AES256-CBC-SHA. • Cuando GlobalProtect utiliza un certificado RSA y se acepta TLS 1.2, la sesión SSL usa RSA-AES256-CBC-SHA256.
3. Certificado de cliente opcional	Certificados de cliente firmados con ECDSA o RSA que utilizan SHA1, SHA256 o SHA384

4. Sesión SSL	• La sesión SSL utiliza ECDSA-AES256-CBC-SHA o RSA-AES256-CBC-SHA256
	• Get-Config-Request
	  • Cifrado: AES-256-GCM, AES-128-GCM, AES-128-CBC
	  • Autenticación: SHA1 y tipo de sistema operativo, dirección IP preferida, etc.
	• Get-Config-Response
	  • Cliente a servidor y SPI de servidor a cliente, claves de cifrado y claves de autenticación
	  • Tipo de túnel, puertos, modo de túnel dividido, IP y DNS, etc.

© 2020 Palo Alto Networks, Inc.

Referencias de criptografía de GlobalProtect

- Referencia: Funciones criptográficas de la aplicación de GlobalProtect
- Conjuntos de cifrados TLS compatibles con las aplicaciones de GlobalProtect
- Conjuntos de cifrados TLS compatibles con las puertas de enlace de GlobalProtect en PAN-OS 8.1

Referencia: Funciones criptográficas de la aplicación de GlobalProtect

La aplicación de GlobalProtect usa la biblioteca 1.0.1h de OpenSSL para establecer una comunicación segura con el portal y las puertas de enlace de GlobalProtect. La siguiente tabla enumera cada función de la aplicación de GlobalProtect que requiere una función criptográfica y las claves criptográficas que usa la aplicación de GlobalProtect:

Función criptográfica	Clave	Uso
Winhttp (Windows) y NSURLConnection (macOS) aes256-sha	Clave dinámica negociada entre la aplicación de GlobalProtect y el portal o la puerta de enlace de GlobalProtect para establecer la conexión HTTPS.	Sirve para establecer la conexión HTTPS entre la aplicación de GlobalProtect y el portal y la puerta de enlace de GlobalProtect para la autenticación.
OpenSSL aes256-sha	Clave dinámica negociada entre la aplicación de GlobalProtect y la puerta de enlace de GlobalProtect durante el protocolo de enlace SSL.	Sirve para establecer la conexión SSL entre la aplicación de GlobalProtect y la puerta de enlace de GlobalProtect para el envío de un informe HIP, la negociación de un túnel SSL y la detección de la red.
Cifrado y autenticación IPSec aes-128-sha1, aes-128-cbc, aes-128-gcm y aes-256-gcm	La clave de sesión enviada desde la puerta de enlace de GlobalProtect.	Sirve para establecer el túnel de IPSec entre la aplicación de GlobalProtect y la puerta de enlace de GlobalProtect. Utilice el algoritmo más sólido compatible con su red (se recomienda AES-GCM). Para proporcionar integridad de datos y protección de la autenticidad, el cifrado aes-128-cbc requiere el algoritmo de autenticación sha1. Debido a que los algoritmos de cifrado AES-GCM (aes-128-gcm y aes-256-gcm) proporcionan de forma nativa protección de integridad ESP, el algoritmo de autenticación sha1 es ignorado para estos cifrados incluso aunque sea necesario durante la configuración.

© 2020 Palo Alto Networks, Inc.

Conjuntos de cifrados TLS compatibles con las aplicaciones de GlobalProtect

Las siguientes secciones brindan ejemplos de cifrados TLS admitidos en las aplicaciones de GlobalProtect instaladas en diferentes sistemas operativos de endpoints. Las listas no son exhaustivas para todos los sistemas operativos compatibles.

- Referencia: Cifrados TLS compatibles con agentes de GlobalProtect en endpoints de macOS
- Referencia: Cifrados TLS compatible con agentes de GlobalProtect en endpoints de Windows 7
- Referencia: Cifrados TLS compatibles con agentes de GlobalProtect en endpoints de Android 6.0.1
- Referencia: Cifrados TLS compatibles con agentes de GlobalProtect en endpoints de iOS 10.2.1
- Referencia: Cifrados TLS compatibles con agentes de GlobalProtect en Chromebooks

Referencia: Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de macOS)

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de macOS)	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

© 2020 Palo Alto Networks, Inc.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de macOS)	
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002) TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c) TLS_RSA_WITH_RC4_128_SHA (0x0005) TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Referencia: Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de Windows 7

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de Windows 7	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Referencia: Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de Android 6.0.1

La aplicación de GlobalProtect para Android 6.0.1 admite 20 conjuntos de cifrados.

© 2020 Palo Alto Networks, Inc.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de Android 6.0.1	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Referencia: Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de iOS 10.2.1

La aplicación GlobalProtect para iOS 10.2.1 es compatible con 19 conjuntos de cifrado.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de iOS 10.2.1	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)

© 2020 Palo Alto Networks, Inc.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en endpoints de iOS 10.2.1	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Referencia: Cifrados TLS compatibles con las aplicaciones de GlobalProtect en Chromebooks

La aplicación GlobalProtect para Chrome OS 55.0.2883 admite 91 conjuntos de cifrado.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

© 2020 Palo Alto Networks, Inc.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en Chromebooks (Chrome OS 55.0.2883)	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038) TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037) TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088) TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087) TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4) TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2) TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067) TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040) TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f) TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e) TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033) TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032) TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031) TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030) TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a) TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099) TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098) TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097) TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045) TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044) TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043) TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) TLS_RSA_WITH_SEED_CBC_SHA (0x0096) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041) TLS_RSA_WITH_IDEA_CBC_SHA (0x0007) TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c) TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002) TLS_RSA_WITH_RC4_128_SHA (0x0005) TLS_RSA_WITH_RC4_128_MD5 (0x0004) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008) TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016) TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013) TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010) TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d) TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)

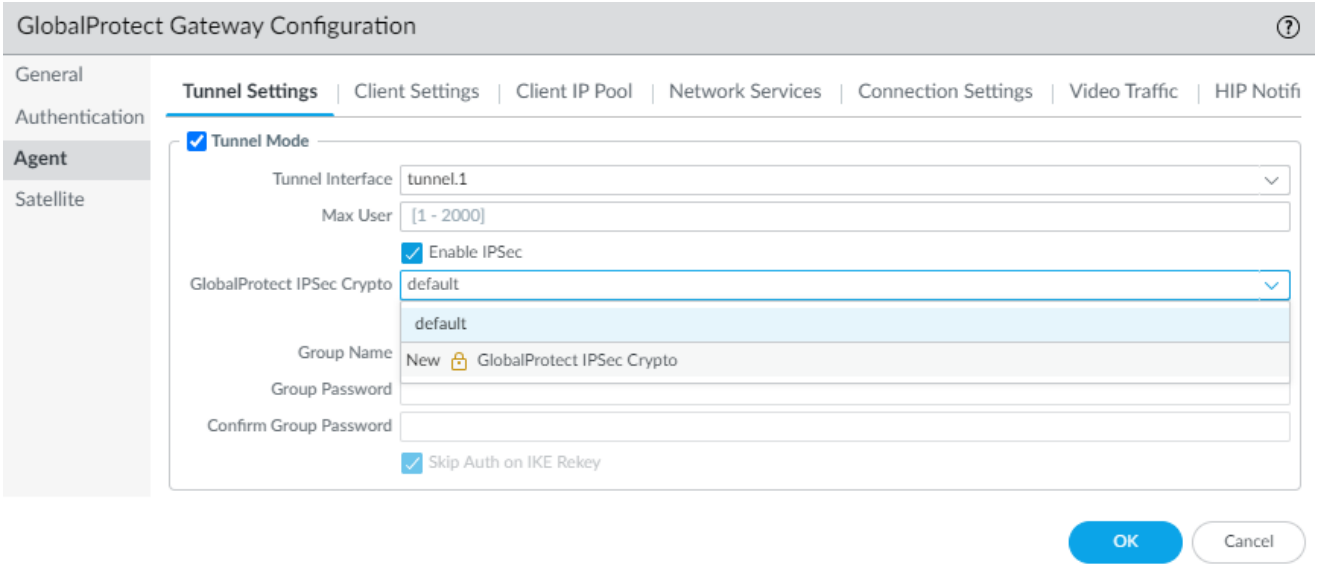
© 2020 Palo Alto Networks, Inc.

Cifrados TLS compatibles con las aplicaciones de GlobalProtect en Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)	TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_RSA_WITH_DES_CBC_SHA (0x0009)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

© 2020 Palo Alto Networks, Inc.

Cifrados utilizados para configurar túneles de IPsec

GlobalProtect puede restringir o establecer un orden preferencial para el algoritmo de cifrado y autenticación que la aplicación de GlobalProtect puede usar para el túnel IPsec. Los algoritmos y preferencias se definen en el **GlobalProtect IPSec Crypto Profile (Perfil criptográfico de IPSec de GlobalProtect)** que se configura cuando establece el túnel de la puerta de enlace de GlobalProtect (**Network [Red]** > **GlobalProtect** > **Gateways [Puertas de enlace]** > **<gateway-config>** > **GlobalProtect Gateway Configuration [Configuración de la puerta de enlace de GlobalProtect]** > **Agent [Agente]** > **Tunnel Settings [Configuración del túnel]**).



Cuando la aplicación de GlobalProtect configura una sesión SSL con una puerta de enlace de GlobalProtect, el conjunto de cifrado utilizado para esta sesión SSL se rige por el perfil SSL/TLS configurado en la puerta de enlace y el tipo de algoritmo utilizado por el certificado de puerta de enlace. Luego de que se establece la sesión SSL, la aplicación de GlobalProtect inicia una configuración de túnel VPN mediante la solicitud de la configuración por SSL.

La puerta de enlace de GlobalProtect responde con la misma sesión SSL y proporciona los algoritmos de cifrado y autenticación, claves y SPI que la aplicación debe usar para configurar el túnel IPsec.

Se recomienda AES-GCM para requisitos más seguros. Para proporcionar integridad de datos y protección de la autenticidad, el cifrado aes-128-cbc requiere el algoritmo de autenticación SHA1. Debido a que los algoritmos de cifrado AES-GCM (aes-128-gcm y aes-256-gcm) proporcionan de forma nativa protección de integridad ESP, el algoritmo de autenticación SHA1 es ignorado para estos cifrados incluso aunque sea necesario durante la configuración.

El **GlobalProtect IPSec Crypto Profile (Perfil criptográfico de IPSec de GlobalProtect)** que usted configuró en la puerta de enlace determina el algoritmo de cifrado y autenticación utilizado para configurar el túnel IPsec. La puerta de enlace de GlobalProtect responde con el primer algoritmo de cifrado coincidente enumerado en el perfil que coincide con la propuesta de la aplicación.

Luego, la aplicación de GlobalProtect intenta configurar un túnel sobre la base de la respuesta de la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

API para SSL

GlobalProtect usa las API del sistema nativo y OpenSSL para realizar protocolos de enlace SSL. Las operaciones tales como la medición de latencia de la puerta de enlace de GlobalProtect (utilizada por GlobalProtect para seleccionar la mejor puerta de enlace), el cierre de sesión de la puerta de enlace y la transmisión de informes y mensajes de verificación HIP se realizan en sesiones SSL que se configuran con la biblioteca OpenSSL. Las operaciones tales como el inicio de sesión previo, el inicio de sesión y la obtención de la configuración de la puerta de enlace se llevan a cabo en sesiones SSL que se configuran con la API del sistema nativo.