paloalto TECHDOCS

Gestión de Prisma Access

4.00 and later



docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

© 2022-2025 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

April 23, 2025

Table of Contents

Prisma Access Descripción general 13

Proteja el tráfico de Internet mediante Prisma Access 16

La importancia de la seguridad en Internet 16

Puerta de enlace web segura en la nube (SWG) de Prisma Access 16

Uso de Prisma Access para proteger a los usuarios y los endpoints 17

Cómo gestionar Prisma Access 18

Visibilidad y supervisión de Prisma Access con Strata Cloud Manager 22

Prisma Access Ubicaciones 24

Ubicaciones de cómputo, ciudad y país 25

Teatro y Grupo de ubicación 30

Ubicaciones por región 34

Ubicaciones de Proxy explícito 39

Ubicaciones de Colo-Connect 40

Regiones Strata Logging Service compatibles 41

Redes remotas: Alto rendimiento, Replicación de tráfico y Ubicaciones de acceso seguro entrante 42

Ubicaciones de Prisma Access en China 45

Ubicaciones de FedRAMP moderado y alto 45

Mapa de ubicaciones de América del Norte 45

Ubicaciones de la zona local 46

Prisma Access y ubicaciones de procesamiento de servicios asociados 47

Prisma Access Gestión de infraestructuras 49

API de Prisma Access 51

API para Prisma Access (Managed by Strata Cloud Manager) 51

API para Prisma Access (Managed by Panorama) 51

Acceda a la API de Prisma Access (Managed by Panorama) utilizando el navegador y la interfaz web 52

Utilice los comandos curl para recuperar los comandos de la API gestionada por Panorama 54

Utilice comandos de la CLI con Prisma Access (Managed by Panorama) 55

APIs de Insights de Prisma Access 55

Migrar Prisma Access de Panorama a Strata Cloud Manager 57

Prepárese para migrar a Prisma Access (Managed by Strata Cloud Manager) 57

Migra su implementación de Prisma Access (Managed by Panorama) a Strata Cloud Manager 58

Publicaciones y actualizaciones de Prisma Access 71

Tipos de versiones de Prisma Access 72

©2025 Palo Alto Networks, Inc.

Actualizaciones programadas urgentes 73
Tipos de actualización de Prisma Access 74
Cadencia para actualizaciones de software y contenido para Prisma Access 77
Actualizaciones del plano de datos dePrisma Access 84
Reciba alertas de actualización y novedades 90
Ver versiones de software de Prisma Access 95
Prisma Access (Managed by Strata Cloud Manager) 95
Prisma Access (Managed by Panorama) 96

Configuración de Prisma Access 101

Configurar Prisma Access 103
Configurar la Infraestructura de servicios de Prisma Access 110
Usuarios móviles: Asignación de dirección IP 125
Ejemplo: Ejemplos de escalado de direcciones IP públicas (usuarios móviles) 126
Asignación de direcciones IP de bucle invertido (usuarios móviles) 128
Redes remotas: Nodos de terminación IPSec y direcciones IP de servicio 131
Redes remotas: Cambios de dirección IP relacionados con la asignación de ancho de banda 132
Redes remotas: Dirección IP de servicio y asignación de direcciones IP de salida 135
Recuperar las direcciones IP para Prisma Access 136
Optimización de IP para las implementaciones de Usuarios móviles: GlobalProtect 165
Ejemplos de API para recuperar direcciones IP de Prisma Access 167
Obtenga notificaciones cuando las direcciones PI de Prisma Access cambian 170
Utilice scripts heredados para recuperar direcciones IP 172
Recuperar direcciones IP de usuarios móviles 174
Recuperar direcciones IP públicas, de bucle invertido y de salida 175
Zonas de Prisma Access 178
DNS para Prisma Access 180
Alta disponibilidad (HA) para Prisma Access 186
Plantillas predefinidas: Incorporar una conexión de servicio o red remota 189
Perfiles criptográficos IKE e IPSec compatibles para dispositivos SD-WAN comunes 194

Conexiones de servicio de Prisma Access 197

Planificar una conexión de servicio 199
Reúna esta información de la sede o del centro de datos 199
Configurar una Conexión de servicio en Prisma Access 201
Utilice una conexión de servicio para permitir el acceso entre usuarios móviles y redes remotas 231

 ©2025 Palo Alto Networks, Inc.

Consideraciones del enrutamiento dinámico para conexiones de servicio..... 233
Cómo Funciona : Enrutamiento para el tráfico de conexión de servicio..... 233
Enrutamiento predeterminado de Prisma Access..... 234
Enrutamiento Hot Potato..... 237

Prisma Access ZTNA Connector..... 243

Componentes de ZTNA Connector..... 245
Casos de uso de ZTNA Connector..... 246
Casos de uso admitidos para conexiones de servicio y ZTNA Connector..... 250
Principios del ZTNA Connector 2.0..... 251
Requisitos y directrices de ZTNA Connector..... 252
Requisitos y versiones compatibles de Prisma Access..... 252
Compatibilidad de aplicaciones..... 253
Restricciones de características y funcionalidades..... 253
Consideraciones sobre la capacidad de ampliación y el rendimiento..... 254
Entornos de alojamiento de aplicaciones compatibles..... 255
Requisitos de red..... 256
Direcciones IP y FQDN que se permiten para ZTNA Connector..... 258
Gestión de certificados..... 261
Habilitar el conector ZTNA..... 262
Configurar ZTNA Connector..... 269
Actualizar los conectores ZTNA..... 280
Herramientas de diagnóstico de ZTNA Connector..... 283
Eliminar Bloques IP del conector..... 291
Configurar el descubrimiento automático de aplicaciones mediante Cloud Identity Engine..... 296
Detección de objetivos de aplicaciones privadas..... 297
Política de seguridad para aplicaciones habilitadas con ZTNA Connector..... 305
Incorpore la máquina virtual de ZTNA Connector en su centro de datos..... 322
Implementaciones de ZTNA Connector compatibles..... 322
Implementaciones de Microsoft Azure compatibles con ZTNA Connector..... 326
Implementaciones de plataforma en Google Cloud compatibles con ZTNA Connector..... 343
Implementaciones de Amazon Web Services compatibles con el conector ZTNA..... 355
Implementaciones de VMware ESXi compatibles con Prisma Access ZTNA Connector..... 363
Implementaciones de KVM compatibles con Prisma Access ZTNA Connector..... 374
Implementaciones de Hyper-V compatibles con Prisma Access ZTNA Connector..... 379

 ©2025 Palo Alto Networks, Inc.

Supervisar ZTNA Connector....393
Ver logs del ZTNA Connector....396
Preservar la asignación de User-ID para las conexiones de ZTNA Connector con NAT de origen....399

Configurar la configuración de acceso a privilegios dinámicos....409

¿Qué es Acceso dinámico a privilegios?....410
Habilite el acceso dinámico a privilegios para Prisma Access a través de Common Services....412
Autoriza la asignación de grupos de usuarios en Cloud Identity Engine para el acceso dinámico a privilegios....414
Habilitar el agente de acceso....422
Configurar la infraestructura del agente para el acceso dinámico a privilegios....424
- Configure la configuración de infraestructura....424
- Seleccionar ubicaciones de Prisma Access....426
- Habilitar compatibilidad con SC-NAT para el acceso dinámico con privilegios....430
- Habilite Resumen de rutas para el Acceso dinámico con privilegios....431

Crear un fragmento....434
Configurar configuración de Prisma Access Agent específica de un proyecto....437
- Configurar perfiles de reenvío para gestionar el tráfico de agentes para agentes con acceso dinámico a privilegios....437
- Configurar los ajustes de aplicación de Prisma Access Agent para el Acceso dinámico a privilegios....451
- Configurar los configuración DNS para el Acceso dinámico a privilegios....457
- Configurar los ajustes de recopilación de datos HIP para el Acceso dinámico con privilegios....458

Crear un proyecto....463
Dirección de tráfico para el acceso dinámico a privilegios....466
Configurar el Prisma Access Agent para el Acceso dinámico con privilegios....468
- Configurar implementaciones por etapas para el Prisma Access Agent....468
- Configure los ajustes globales generales para Prisma Access Agents....478
- Configurar notificaciones HIP para el acceso dinámico a privilegios de Prisma Access Agent....482

Envíe la configuración de Prisma Access Agent....491
Descargue el paquete de Prisma Access Agent habilitado por acceso dinámico a privilegios....494
Utilice el Prisma Access Agent para acceder a sus proyectos....496
- Instalar el Prisma Access Agent....496
- Inicie sesión en Prisma Access Agent habilitado por acceso dinámico a privilegios....504
- Cambiar las preferencias para el acceso privilegiado dinámicamente habilitado de Prisma Access Agent....507

 ©2025 Palo Alto Networks, Inc.

Conecte el Prisma Access Agent habilitado por el Acceso dinámico a privilegios a una Ubicación diferente 508
Cambiar a un inquilino diferente 509
Conecte el Prisma Access Agent habilitado por el Acceso dinámico a privilegios a un servidor diferente 510
Cambie entre Prisma Access Agent y la aplicación GlobalProtect 512
Ver y supervisar usuarios con acceso dinámico a privilegios 514
Usuarios conectados 514
Ver y supervisar proyectos de acceso con privilegios dinámicos 520
Proyectos 520

Prisma Access Colo-Connect 523

Casos de uso de Colo-Connect 525
Acceso de gran ancho de banda a aplicaciones privadas 525
Conectividad privada para aplicaciones privadas 525
Uso de un proveedor de NaaS de terceros 525
¿En qué se diferencia Colo-Connect de las conexiones de servicio y el conector ZTNA? 527
Características y funcionalidades no compatibles de Colo-Connect 528
Requisitos y requisitos previos para Prisma Access Colo-Connect 529
Configurar Prisma Access Colo-Connect 531

Aceleración de aplicaciones en Prisma Access 587

Requisitos y directrices para la aceleración de aplicaciones 589
Configurar la aceleración de aplicaciones 592

Prisma Access usuarios móviles 617

Usuarios móviles: GlobalProtect 619
Lista de verificación de planificación para GlobalProtect en Prisma Access 620
Configurar usuarios móviles de GlobalProtect 623
GlobalProtect: Personalizar la configuración del túnel 658
GlobalProtect: Personalizar la configuración de la aplicación 663
Solicitud de ticket para desactivar GlobalProtect 674
Inicio de sesión previo de GlobalProtect 679
VPN sin cliente de GlobalProtect 695
Supervisar Usuarios móviles de GlobalProtect 697
Grupos de direcciones IP para una implementación de usuarios móviles de GlobalProtect 703
Cómo selecciona la aplicación GlobalProtect Ubicaciones de Prisma Access para usuarios móviles 709
Lista de permitidos de usuarios móviles de GlobalProtect 711
Actualizaciones de la aplicación GlobalProtect 723

 ©2025 Palo Alto Networks, Inc.

Integrar Prisma Access con las puertas de enlace GlobalProtect locales..... 732
Usuarios móviles: Proxy explícito..... 743
Directrices de la configuración de proxy explícito..... 746
GlobalProtect en modo proxy..... 750
GlobalProtect en modo Túnel y proxy..... 765
Visibilidad y aplicación de direcciones IP privadas para tráfico proxy basado en agentes..... 789
Autenticación SAML para Proxy explícito..... 791
Configurar Proxy explícito..... 794
Autenticación Kerberos para implementaciones de proxy explícito..... 818
Cloud Identity Engine Autenticación para implementaciones de proxy explícito..... 852
Modo proxy para redes remotas..... 858
Cómo el proxy explícito identifica a los usuarios..... 869
Perfiles de reenvío de proxy explícito..... 871
Directrices del archivo PAC..... 880
Prácticas recomendadas para Proxy explícito..... 887
Supervisar y solucionar problemas de proxy explícito..... 887
Configuración de bloques para proxy explícito..... 891
Utilice objetos especiales para restringir el tráfico de Internet proxy explícito a direcciones IP específicas..... 893
Acceda a su centro de datos usando proxy explícito..... 894
Integración de Office 365 basada en aplicaciones con proxy explícito..... 898
Configurar el encadenamiento de proxy con Blue Coat Proxy..... 902
Utilizar un proxy explícito con GlobalProtect (o una VPN de terceros)..... 908
Optimización de direcciones IP para usuarios de proxy explícito: Implementaciones de proxy..... 922
Resolución de DNS para implementaciones de Usuarios móviles: Proxy explícito..... 923
Ver asignaciones de usuarios a direcciones IP o grupos de usuarios..... 925
Reportar problemas de acceso al sitio de usuario móvil..... 931
Habilite usuarios móviles para autenticarse en Prisma Access..... 933
Soporte de autenticación y características..... 935
Configurar la autenticación..... 940
Permitir a los usuarios móviles acceder a los recursos corporativos..... 946

Redes remotas de Prisma Access..... 951

Lista de verificación de planificación para redes remotas..... 952
Asignar ancho de banda de red remota..... 957
Planifique su migración al nuevo modelo..... 972
Asignación de ancho de banda para una implementación de ancho de banda agregado migrado..... 975

 ©2025 Palo Alto Networks, Inc.

Directrices para la migración de QoS....977
Migrar la configuración de gestión del ancho de banda....982
Incorpore una red remota....989
Conectar un sitio de red remoto a Prisma Access....1015
Añadir túneles VPN IPSec primarios y secundarios....1015
Más opciones de IKE....1016
Más opciones de IPSec....1018
Habilitar el enrutamiento para su red remota....1019
Solucionar problemas de conexiones del sitio....1022
Integrar varias redes remotas....1024
Campos en la tabla de Redes remotas....1026
Compruebe si la red remota está conectada a Prisma Access....1036
Verificar el estado de la conexión remota BGP....1039
Configurar la red remota y la conexión de servicio conectada con un enlace WAN....1040
QoS para Redes remotas....1043
Cambiar el ancho de banda garantizado....1062
Redes remotas—Alto rendimiento....1066
Capacidades y directrices de Redes remotas: Alto rendimiento....1066
Integre una VDI de escritorio compartido con Prisma Access usando Terminal Server....1087

Supervisión y visibilidad de Prisma Access....1097

Logs de Prisma Access....1099
Logs externos y otros datos....1100
Paneles e informes de actividad de Prisma Access....1101
Ver y supervisar Prisma Access en Strata Cloud Manager....1102
Comience a utilizar la supervisión de acceso de Prisma en Strata Cloud Manager....1103
Visualización y supervisión de aplicaciones....1106
Ver y supervisar la aceleración de aplicaciones....1109
Ver Usuarios móviles....1110
Visualizar y supervisar IPv6 para usuarios móviles....1111
Visualizar y supervisar su sucursales....1112
Ver y supervisar centros de datos....1119
Ver y supervisar los servicios de red....1139
Ver uso de suscripciones....1144
Ver y supervisar ubicaciones de Prisma Access....1146
Ver y supervisar ID de dispositivos de terceros....1148
Ver y supervisar el Aislamiento remoto del navegador....1150
Prisma Access y Autonomous DEM....1152

 ©2025 Palo Alto Networks, Inc.

Política basada en el usuario de Prisma Access..... 1153

Configurar la política basada en usuario para Prisma Access..... 1154
Integrar Cloud Identity Engine con Prisma Access..... 1157
Recuperar asignaciones de grupos de User-ID para Prisma Access..... 1164
Redistribución de identidades..... 1174
Configurar el Device-ID de terceros en Prisma Access..... 1191
API de Device-ID de terceros..... 1198
Veredictos de actualización..... 1198
Borrar todos los veredictos..... 1201
Veredictos de consulta..... 1202
Veredictos de consulta por dirección IP..... 1204
Estadísticas de veredictos de consulta..... 1205

Multitenencia de Prisma Access..... 1207

Descripción general de la configuración de multitenencia..... 1208
Planificar su implementación multiinquilino..... 1213
Crear una implementación multiinquilino totalmente nueva..... 1216
Habilitar la multitenencia y migrar el primer inquilino..... 1217
Añadir inquilinos a Prisma Access..... 1224
Eliminar un inquilino..... 1230
Crear un usuario administrativo a nivel de inquilino..... 1236
Control de acceso basado en funciones para usuarios administrativos de nivel de inquilino..... 1240
Eliminar el acceso al complemento para un usuario administrativo de nivel de inquilino..... 1241
Ordenar logs por identificador de grupo de dispositivos en una implementación multiinquilino..... 1246

Prisma Access en un entorno de FedRAMP..... 1249

Requisitos de Prisma Access FedRAMP..... 1250
Requisitos previos a la instalación y activación del producto..... 1250
Versiones necesarias de Panorama, complemento y plano de datos de PAN-OS..... 1251
Ubicaciones de Prisma Access FedRAMP compatibles..... 1253
Características compatibles y no compatibles en un Implementación de Prisma Access FedRAMP..... 1253
Configurar Prisma Access en un entorno FedRAMP..... 1254

Implementaciones avanzadas de Prisma Access..... 1261

Añadir una nueva ubicación de cómputo para una ubicación de Prisma Access implementada..... 1263
Compatibilidad con IPv6..... 1265

 ©2025 Palo Alto Networks, Inc.

Descripción general de la compatibilidad nativa con IPv6....1268
Habilitar y configurar la red IPv6 y los grupos de direcciones IP en su infraestructura de Prisma Access....1271
Habilite la red IPv6 para la implementación de Usuarios móviles: GlobalProtect....1279
Habilitar redes IPv6 para conexiones de servicio....1284
Habilitar redes IPv6 para Redes remotas....1291
Resolución de DNS para Usuarios móviles: GlobalProtect e implementaciones de redes remotas....1300
Resolución de DNS para implementaciones de Usuarios móviles: GlobalProtect....1302
Resolución DNS para redes remotas....1304
Cómo BGP anuncia los grupos de direcciones IP de usuarios móviles para conexiones de servicio y conexiones de red remotas....1307
Soporte de proxy para Prisma Access y Strata Logging Service....1309
Bloquear conexiones entrantes de países específicos....1310
Tráfico de Internet seguro de AWS WorkSpace....1311
Configurar un archivo PAC en los clientes de AWS WorkSpace....1311
Configurar un túnel de sitio a sitio entre AWS y Prisma Access....1313
Prisma Access para redes sin ruta predeterminada....1314
¿Qué es una red sin ruta predeterminada?....1314
Consideraciones sobre la red sin ruta predeterminada....1314
Recomendaciones de implementación para proteger el acceso a Internet en redes sin ruta predeterminada....1314
Consideraciones clave....1315
Prisma Access implementaciones avanzadas de conexión de servicio....1316
Redundancia multicloud de conexión de servicio....1316
Uso de la dirección de tráfico para reenviar el tráfico enlazado a Internet a las conexiones de servicio....1327
Enrutamiento para el tráfico de conexión de servicio....1353
Cree una red de gran ancho de banda utilizando múltiples conexiones de servicio....1366
Conservar la asignación de User-ID y Device-ID para conexiones de servicio con NAT de origen....1380
Implementaciones avanzadas de Usuarios móviles de Prisma Access: GlobalProtect....1389
Configurar múltiples portales en Prisma Access....1389
Compatibilidad con el registro de DNS dinámico para la resolución de problemas y actualizaciones remotas....1399
Compatibilidad con el registro de DNS dinámico para usuarios móviles: GlobalProtect....1415
Identificación y cuarentena de dispositivos en riesgo en una implementación de Prisma Access GlobalProtect....1422

 ©2025 Palo Alto Networks, Inc.

Tráfico IPV6 de sinkhole en implementaciones de Usuarios móviles: GlobalProtect 1432
Redistribuir la información de HIP con Prisma Access 1436
Ver informes de HIP 1445
Soporte para codificación Gzip en VPN sin cliente 1447
Replicación de tráfico en Prisma Access 1449
Implementaciones avanzadas de Redes remotas de Prisma Access 1462
Puerta de enlace interna de Prisma Access 1462
Proporcionar acceso seguro entrante a ubicaciones de red remotas 1472

Prisma Access para Clean Pipe 1501

Descripción general de Prisma Access para Clean Pipe 1502
Casos de uso de Clean Pipe 1502
Ejemplos de Clean Pipe 1503
Requisitos de interconexión de Clean Pipe y socios 1504
Completar la configuración de Clean Pipe 1506
Habilitar la multitenencia y crear un inquilino 1511

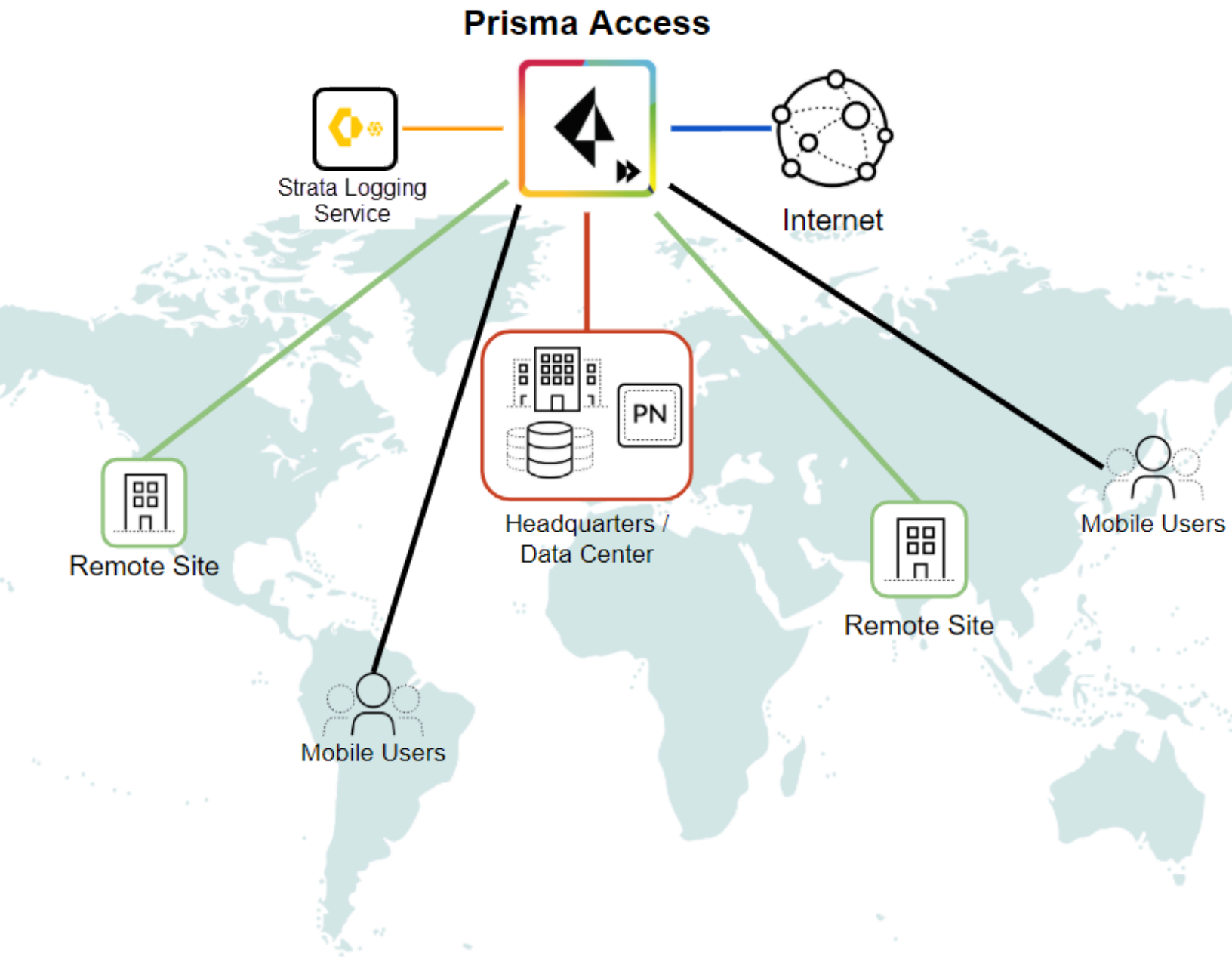
 ©2025 Palo Alto Networks, Inc.

Prisma Access Descripción general

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para mantener sus aplicaciones y datos seguros, debe proteger a todos los usuarios en todas las ubicaciones en todo momento. Pero, ¿cómo lograr esto cuando su presencia se está expandiendo globalmente, cada vez más usuarios son móviles y sus aplicaciones y datos se están trasladando fuera de su red hacia la nube? Prisma Access permite esta seguridad coherente al permitir de manera segura que sus usuarios accedan a aplicaciones en la nube y en centros de datos, así como a Internet, ya sea que se encuentren en su sede, sucursales o de viaje. Prisma Access inspecciona de forma coherente todo el tráfico en todos los puertos, lo que permite un acceso seguro a Internet, así como a sus aplicaciones SaaS autorizadas, entornos de nube pública y centros de datos y sedes centrales. La prevención de amenazas, la prevención de malware, el filtrado de URL, el descifrado SSL y las capacidades de políticas basadas en aplicaciones están integradas para brindarle el mismo nivel de seguridad sin importar dónde se encuentren sus usuarios o a qué recursos accedan. Todos los logs de Prisma Access se almacenan en el Strata Logging Service, proporcionando análisis, informes y análisis forenses centralizados para todos los usuarios, aplicaciones y ubicaciones.

Prisma Access ofrece protección a escala con cobertura global para que no tenga que preocuparse por cuestiones como el tamaño y la implementación de cortafuegos de hardware en sus sucursales o la construcción y gestión de dispositivos en instalaciones de coubicación. Prisma Access proporciona la infraestructura de red para conectar todas sus sucursales remotas, sus sitios de sede central, centros de datos y usuarios móviles sin necesidad de construir su infraestructura de seguridad global propia ni ampliar su capacidad operativa.



Con Prisma Access, Palo Alto Networks implementa y gestiona la infraestructura de seguridad a nivel mundial para proteger sus redes remotas y usuarios móviles. Prisma Access cifra los datos de extremo a extremo entre los nodos de procesamiento de seguridad de usuarios móviles (MU-SPN) y los nodos de procesamiento de seguridad de red remota (RN-SPN), entre los SPN y los nodos de acceso corporativo de conexión de servicio (SC-CAN), y entre los SC-CAN y el centro de datos.

- **Infraestructura de servicios**: Prisma Access utiliza una infraestructura de servicio interna para proteger la red de su organización. Usted proporciona una subred para la infraestructura y Prisma Access utiliza las direcciones IP dentro de esta subred para establecer una infraestructura de red entre sus ubicaciones de red remotas y usuarios móviles, y conexiones de servicio a sus recursos de red interna (si corresponde). La comunicación interna dentro de la nube se establece mediante enrutamiento dinámico.

 ©2025 Palo Alto Networks, Inc.

- **Conexiones de servicio**: si su licencia de Prisma Access lo incluye, tiene la opción de establecer túneles IPSec para permitir la comunicación entre los recursos internos de su red y los usuarios móviles, y los usuarios en sus ubicaciones de red remotas. Podría, por ejemplo, crear una conexión de servicio a un servidor de autenticación en la sede o centro de datos de su entidad.

  Incluso si no necesita una conexión de servicio para su sede o centro de datos, le recomendamos que cree una para permitir la comunicación de red entre usuarios móviles y ubicaciones de red remotas, y entre usuarios móviles en diferentes zonas geográficas.
- **Usuarios móviles**: proporciona seguridad coherente para sus usuarios móviles, ya sea que accedan a aplicaciones en su centro de datos, utilicen aplicaciones SaaS o naveguen por Internet. Puede permitir que sus usuarios móviles se conecten a Prisma Access a través de:
  - **GlobalProtect**

    Puede implementar la aplicación GlobalProtect a sus usuarios (disponible para teléfonos inteligentes, tabletas o portátiles con Microsoft Windows, Apple macOS e iOS, Android, Google Chrome OS y Linux) para que puedan tunelizar el tráfico a Prisma Access para la aplicación de políticas y la prevención de amenazas. La aplicación GlobalProtect también proporciona informes de perfil de información de host (HIP) para que pueda crear políticas granulares basadas en el estado del dispositivo para garantizar que los endpoints se adhieran a sus estándares de seguridad (por ejemplo, están equipados con los parches, cifrado y definiciones de virus más actualizados, para acceder a sus aplicaciones más sensibles. O, para permitir el acceso seguro a los usuarios en dispositivos no gestionados, puede habilitar **VPN sin cliente**. Prisma Access escala dinámicamente dentro y fuera por región según dónde se encuentren sus usuarios en ese momento.
  - **Proxy explícito**

    Si la red existente de su organización ya utiliza servidores proxy explícitos e implementa archivos PAC en los endpoints de sus clientes, puede migrar sin problemas a Prisma Access para proteger el tráfico saliente de Internet de los usuarios móviles.
- **Redes remotas**: utilice redes remotas para proteger ubicaciones de redes remotas, como sucursales, y usuarios en dichas sucursales con cortafuegos de nueva generación basados en la nube. Puede habilitar el acceso a las subredes en cada ubicación de red remota usando rutas estáticas, enrutamiento dinámico mediante BGP o una combinación de rutas estáticas y dinámicas. Todas las ubicaciones de red remotas que usted incorpora cuentan con una malla completa.
- **ZTNA Connector**: el conector Zero Trust Network Access (ZTNA) le permite conectarse a las aplicaciones privadas de su organización de forma sencilla y segura. ZTNA Connector brinda a los usuarios móviles y a los usuarios en sucursales acceso a sus aplicaciones privadas mediante un túnel seguro automatizado, que elimina el requisito de configurar túneles IPSec y definiciones de enrutamiento para acceder a las aplicaciones privadas. ZTNA Connector no requiere ningún enrutamiento desde la infraestructura del cliente y puede proporcionar acceso a aplicaciones que utilizan direcciones IP superpuestas en sus redes.
- **Strata Logging Service**—Prisma Access reenvía todos los logs a Strata Logging Service; como parte de la activación de Prisma Access, usted deberá especificar la instancia de Strata Logging Service a la que desea reenviar los de Prisma Access. El tráfico de logs no utiliza el ancho de banda con licencia que compró para Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Proteja el tráfico de Internet mediante Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access	❑ Licencia de Prisma Access

La importancia de la seguridad en Internet

La protección del acceso a Internet nunca ha sido tan importante y tan desafiante. Las soluciones heredadas existentes luchan por detectar phishing evasivo y dirigido, y otros ataques basados en la web y, al mismo tiempo, descuidan las nuevas amenazas planteadas por el tráfico DNS no seguro. Palo Alto Networks Prisma Access ofrece la mejor seguridad en Internet del sector con servicios de seguridad DNS y Advanced URL Filtering impulsados por aprendizaje automático. Con Prisma Access, puede evitar ataques evasivos y selectivos de phishing y ataques sin archivos en tiempo real, además de protegerse frente a los últimos ataques sofisticados basados en DNS.

Puerta de enlace web segura en la nube (SWG) de Prisma Access

Una puerta de enlace web segura es un elemento crucial en el panorama digital actual debido a la creciente complejidad y frecuencia de las ciberamenazas. Los ciberdelincuentes idean continuamente nuevas tácticas y técnicas para vulnerar las defensas de seguridad, una de las cuales es camuflar código malicioso en sitios web aparentemente legítimos. A medida que los usuarios acceden a estos sitios web comprometidos, filtran inadvertidamente credenciales o exponen a las organizaciones a código dañino, que puede causar estragos si pasa desapercibido.

En un entorno tan cargado de riesgos, la ausencia de una puerta de enlace de seguridad sólida amplifica significativamente el riesgo para los activos digitales de una organización. Este riesgo podría provocar accesos no autorizados, robo de datos e interrupción de las operaciones comerciales, especialmente con la creciente prevalencia de ataques generalizados de phishing y ransomware. Sin la barrera de seguridad proporcionada por SWG, un ataque de ransomware podría mantener a una organización como rehén, lo que provocaría daños financieros y reputacionales.

El uso del tráfico cifrado es ahora común, y HTTPS constituye la mayor parte del tráfico web. Una organización corre el riesgo de sufrir amenazas de seguridad ocultas dentro de los canales cifrados si carece de un puerta de enlace web segura (SWG) que pueda descifrar e inspeccionar eficazmente este tráfico.

Sin embargo, el uso de varios productos puntuales para SWG, acceso a aplicaciones privadas y CASB solo complica las cosas. Los productos aislados unidos como una única proposición dan como resultado brechas en la paridad de características y malos resultados de seguridad, lo que hace que quede vulnerable ante los ataques. Con estas soluciones, se obtiene una seguridad incoherente para Internet y las aplicaciones privadas.

Para hacer frente a estos desafíos, Prisma Access ofrece un producto unificado en el que convergen gestión, políticas y datos para todos los usuarios y aplicaciones en todas las capacidades, incluidas ZTNA, SWG, NG-CASB, FWaaS, DLP y más.

Los clientes pueden migrar fácilmente de soluciones de proxy heredadas en las instalaciones y basadas en la nube a Prisma Access para obtener visibilidad y control en línea del tráfico de

 ©2025 Palo Alto Networks, Inc.

aplicaciones de Internet y SaaS con protecciones de seguridad impulsadas por IA líderes del sector.

Uso de Prisma Access para proteger a los usuarios y los endpoints

Prisma Access está diseñado para prevenir ciberataques llevado a cabo con éxito, y es por eso que hace más que solo proteger la web. Para detener los ciberataques, es necesario inspeccionar todo el tráfico. Cualquier cosa que no sea una inspección completa de todo el tráfico introduce una brecha significativa en la seguridad. Prisma Access protege de forma coherente todo el tráfico en todos los puertos y desde todas las aplicaciones, lo que permite a su organización:

- Impedir que los ciberataques se lleven a cabo con éxito con filosofías de seguridad e inteligencia de amenazas comprobadas, para una visibilidad profunda y un control preciso que se extiende a toda su organización.
- Inspeccionar completamente todo el tráfico de aplicaciones de forma bidireccional, incluido el tráfico cifrado SSL o TLS, en todos los puertos, ya sea que se comuniquen con Internet, con la nube o entre sucursales.
- Beneficiarse de una inteligencia de amenazas integral impulsada por datos de amenazas automatizados de Palo Alto Networks y cientos de fuentes de terceros.

Leer más acerca de Prisma Access y sus soluciones.

 ©2025 Palo Alto Networks, Inc.

Cómo gestionar Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Hay dos formas de gestionar Prisma Access, pero no puede cambiar entre las interfaces de gestión después de activar su licencia de Prisma Access (con la excepción de usar el flujo de trabajo de migración para pasar de una Prisma Access (Managed by Panorama) a un implementación de Prisma Access (Managed by Strata Cloud Manager)). Por lo tanto, debes decidir cómo quiere gestionar Prisma Access antes de empezar:

- **Prisma Access (Managed by Strata Cloud Manager)**

  Para gestionar Prisma Access desde la nube, utilice Strata Cloud Manager. Con la gestión de la nube, puede incorporar rápidamente sucursales y usuarios móviles a través de flujos de trabajo basados en tareas que le permiten configurar y probar su entorno en minutos. La gestión de la nube con Strata Cloud Manager simplifica el proceso de incorporación al proporcionar reglas de políticas de descifrado y acceso a Internet predefinidas basadas en las prácticas recomendadas. Configure rápidamente túneles IPSec utilizando valores predeterminados adecuados para los dispositivos con capacidad IPSec más comunes y active el descifrado SSL para las categorías de URL recomendadas.

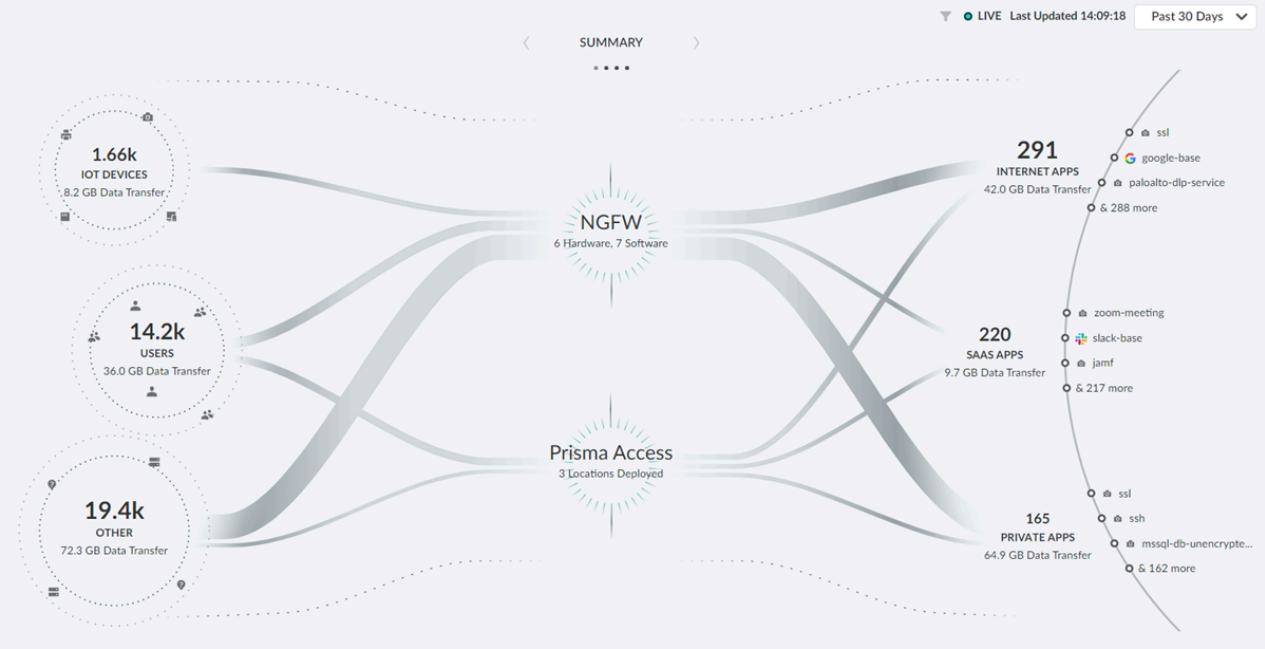
  Centro de control de Strata Cloud Manager

  La página del Centro de control de Strata Cloud Manager aparece cuando inicia su Strata Cloud Manager. Este centro de control le ayuda a evaluar el estado de su red, obtener una mejor

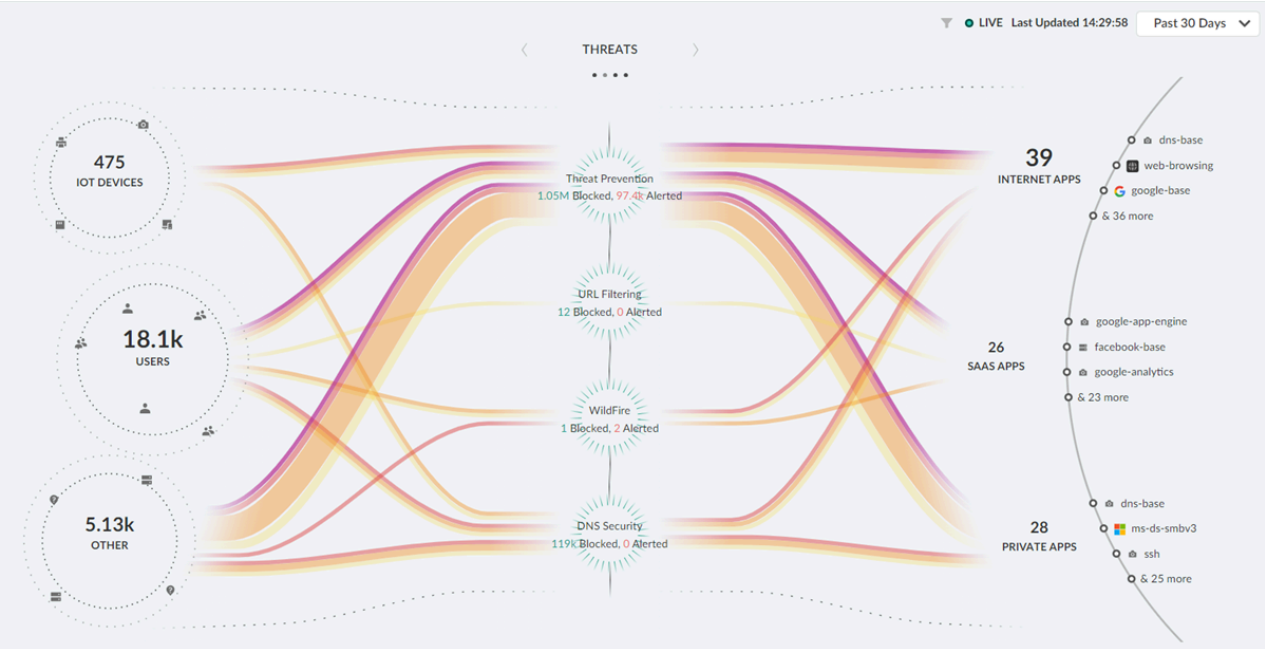
 ©2025 Palo Alto Networks, Inc.

visibilidad y una descripción general de sus datos. El centro de control tiene diferentes paneles para ver diferentes tipos de informes.

- **Resumen**: En el panel de resumen, puede ver los diferentes tipos de fuentes de datos, la infraestructura de la plataforma, como NGFW o Prisma Access, a través de la cual fluyen los datos desde varias fuentes de datos a diferentes aplicaciones en su red.

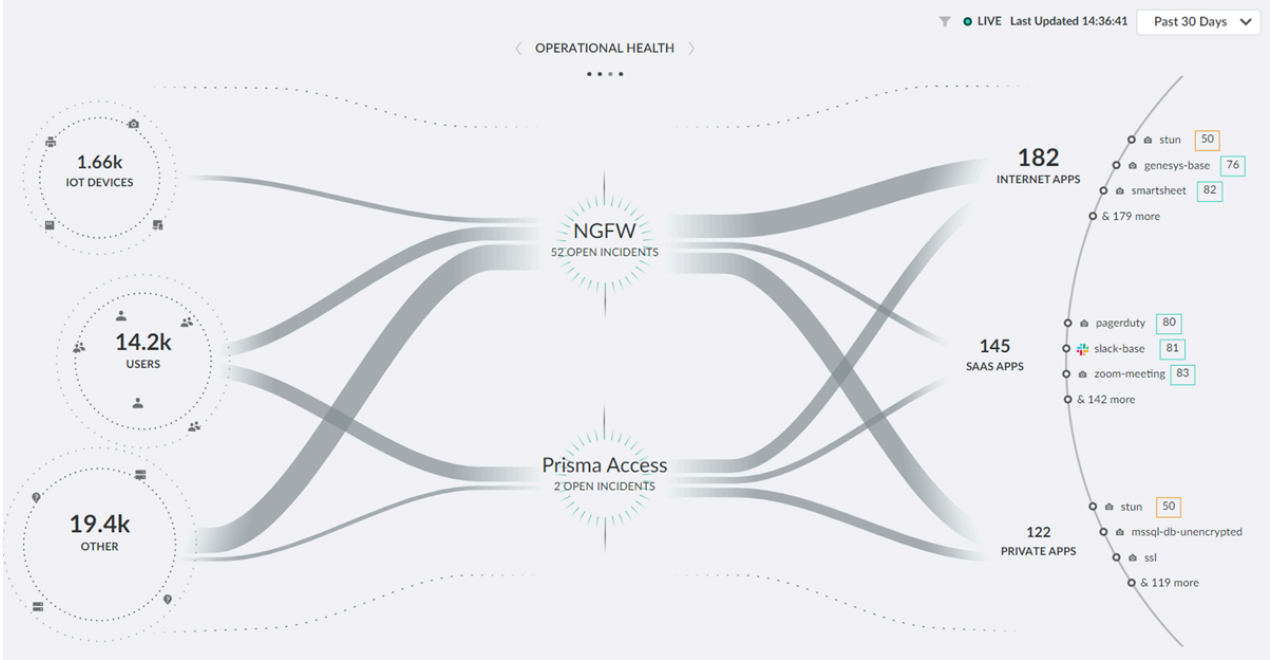


- **Amenazas**: En su panel de amenazas, puede ver las amenazas detectadas por sus aplicaciones de seguridad. Puede utilizar este panel para supervisar las amenazas bloqueadas y permitidas en su red, o investigar áreas de su red que puedan tener un bajo porcentaje de tráfico inspeccionado.



 ©2025 Palo Alto Networks, Inc.

- **Estado operativo**: Muestra el estado y la experiencia del usuario en su red tal como la supervisa ADEM. Puede utilizar esta vista para supervisar la experiencia del usuario en su red y revisar la gravedad de los incidentes abiertos.



- **Seguridad de datos**: Muestra el tráfico dentro de su red que se ha marcado como que contiene datos confidenciales por las suscripciones de seguridad DLP y SaaS. Puede utilizar esta vista para supervisar los datos que fluyen a través de sus cortafuegos y aplicaciones SaaS conectadas y supervisar la gravedad de cualquier riesgo de datos en su red.



Haga clic en cualquiera de estas categorías en sus paneles para filtrar los resultados según corresponda.

©2025 Palo Alto Networks, Inc.

- **Prisma Access (Managed by Panorama)**

  Utilice el Complemento de servicios en la nube en Panorama para configurar y gestionar Prisma Access. Esta es una buena opción si ya está utilizando Panorama para gestionar cortafuegos de nueva generación y tiene una política común que desea utilizar para acceder a sus aplicaciones corporativas.

  Incluso si está usando Panorama para gestionar Prisma Access, todavía puede usar Strata Cloud Manager para muchas funciones de visibilidad y supervisión de Prisma Access. Más información.

Después de decidir qué opción de gestión desea utilizar, comience siguiendo el flujo de trabajo de licencia y activación para la opción que haya seleccionado:

- Para empezar con el acceso de Prisma Access (Managed by Panorama), realice la activación de la licencia desde el portal de atención al cliente (CSP) e instale el complemento de servicios en la nube en Panorama.
- Para comenzar a utilizar Cloud Managed Prisma Access, realice la activación de la licencia desde el hub.



Paridad de características entre Panorama y la gestión de la nube

Existen algunas diferencias entre lo que es compatible en Prisma Access (Managed by Panorama) Access y Prisma Access (Managed by Strata Cloud Manager). Para obtener una lista de las funciones compatibles en Prisma Access (Managed by Panorama) y Prisma Access (Managed by Strata Cloud Manager), consulte la matriz de compatibilidad.

 ©2025 Palo Alto Networks, Inc.

Visibilidad y supervisión de Prisma Access con Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (gestionado por Panorama)	• Licencia de Prisma Access

Hay dos formas disponibles de gestionar Prisma Access:

- Para Prisma Access (Managed by Strata Cloud Manager), puede utilizar **Strata Cloud Manager**
- o puede usar **Panorama** para gestionar Prisma Access

Estas dos interfaces de gestión son la forma en que gestiona la incorporación, la configuración y la aplicación de políticas de seguridad para su entorno de Prisma Access. Sin embargo, Prisma Access también incluye una visibilidad y supervisión sólidas para su entorno de Prisma Access, y estas características se proporcionan en Strata Cloud Manager.

De modo importante:

Independientemente de la interfaz de gestión que utilice para Prisma Access (Strata Cloud Manager o Panorama), puede utilizar Strata Cloud Manager para muchas de sus funciones de visibilidad de Prisma Access e interactuar con suscripciones complementarias como AI-Powered Autonomous DEM.

Características de visibilidad y supervisión de Prisma Access en Strata Cloud Manager	
Autonomous DEM	Proporciona visibilidad e información nativas de extremo a extremo para todo el tráfico de usuarios en su entorno de Secure Access Service Edge (SASE). La funcionalidad ADEM está integrada de forma nativa en la aplicación GlobalProtect y Prisma Access, por lo tanto, no requiere que implemente ningún dispositivo o agente adicional. Puede aislar rápidamente la fuente de los problemas de experiencia digital y simplificar su solución. *Esta característica requiere la licencia Autonomous DEM adicional para usar con Prisma Access (Managed by Panorama) Access.*
Paneles e informes en Strata Cloud Manager	Las características de visibilidad de Strata Cloud Manager identifican los hallazgos clave que puede utilizar para informar las actualizaciones de políticas y cerrar las brechas de seguridad empresarial y productividad de los usuarios.

 ©2025 Palo Alto Networks, Inc.

Características de visibilidad y supervisión de Prisma Access en Strata Cloud Manager	
	• **Paneles interactivos** Explorar datos para las aplicaciones, amenazas, usuarios, suscripciones de seguridad en el trabajo en su red • **Informes** Muchos paneles admiten informes, donde puede compartir datos sin conexión y programar actualizaciones periódicas
Centro de control de Strata Cloud Manager	El Centro de control es un resumen visual interactivo de los dispositivos IoT, los usuarios, los hosts y el tráfico en su red. Al utilizar los datos de sus suscripciones de seguridad entregadas en la nube y ADEM, el Centro de control muestra información importante sobre las amenazas, la experiencia del usuario y la seguridad de los datos en su red. El Centro de control le permite interactuar con los datos y visualizar las relaciones entre eventos en la red para que pueda detectar anomalías o averiguar formas de mejorar su seguridad de red.

©2025 Palo Alto Networks, Inc.

Prisma Access Ubicaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Puede implementar Prisma Access en las ubicaciones que elija, basándose en las preferencias de ubicación de datos y donde tenga más usuarios. Prisma Access proporciona más de 100 ubicaciones en todo el mundo, para que sus usuarios tengan una experiencia adaptada a sus localidades. Todas las ubicaciones de Prisma Access están asignadas a una ubicación de cómputo de seguridad basada en un rendimiento y latencia optimizados. Esto significa que el tráfico en ciertos países se dirigirá a esa ubicación de cómputo definida.

Si tiene un requisito para limitar las ubicaciones de cómputo a países específicos, consulte la tabla que muestra el país de procesamiento para Prisma Access y sus servicios asociados.

Hay diferentes tipos de ubicación de Prisma Access:

- **Ubicaciones ordenadas por ubicación de cómputo**: cuando configura redes remotas, asigna ancho de banda por ubicación de cómputo. Al menos dos (a menudo más) ubicaciones de Prisma Access que están geográficamente cerca unas de otras se agrupan en *ubicaciones de cómputo*. Este es el nivel en el que asignas ancho de banda, en lugar de asignar ancho de banda para ubicaciones Prisma Access individuales o para sitios de red remotos específicos, y permite a Prisma Access asignar dinámicamente ancho de banda a sitios en una ubicación de cómputo en función de la carga o la demanda.
- **Teatro y grupo de ubicaciones**: cuando asigna grupos de direcciones IP en una implementación de Usuarios Móviles: GlobalProtect, puede especificar grupos de IP por grupo de ubicación (un grupo de ubicaciones que es más pequeño que el teatro), teatro o Mundial. Utilice grupos de direcciones IP específicas de la ubicación si tiene servicios que dependen de la dirección IP de origen del usuario para identificar los detalles del usuario (como servicios basados en la ubicación o servicios basados en un grupo o función de usuario) para que pueda aplicar políticas de control de acceso, o para realizar operaciones de enrutamiento o políticas en diferentes países si los países están en diferentes regiones de cómputo.
- **Ubicaciones por región**: cada ubicación de Prisma Access tiene una región asociada.
- **Ubicaciones de Proxy explícito**: Proxy explícito tiene su propio conjunto de ubicaciones que son un subconjunto de ubicaciones de Prisma Access.
- **Ubicaciones de Colo-Connect**: Colo-Connect tiene su propio conjunto de ubicaciones que son un subconjunto de ubicaciones de Prisma Access.
- **Regiones de Strata Logging Service**: Prisma Access admite un subconjunto de las regiones de Strata Logging Service.

 ©2025 Palo Alto Networks, Inc.

- **Redes Remotas: Alto Rendimiento, Replicación de tráfico y Ubicaciones de acceso entrante seguro**: Redes remotas de alto rendimiento, Replicación de tráfico e implementaciones de acceso entrante seguro utilizan un subconjunto de ubicaciones de Prisma Access.
- **Ubicaciones de Prisma Access en China**: las implementaciones de Prisma Access en China utilizan ubicaciones en la China continental.
- **Ubicaciones FedRAMP moderadas y altas**:Prisma Access las implementaciones FedRAMP moderadas y altas utilizan un subconjunto de ubicaciones de Prisma Access.
- **Mapa de ubicaciones de América del Norte**: para ayudarle a seleccionar ubicaciones en América del Norte, consulta este mapa que muestra la cobertura geográfica de las ubicaciones en América del Norte.
- **Zonas Locales**: Las zonas locales colocan computación, almacenamiento, bases de datos y otros servicios cerca de grandes centros industriales y de población. Estas ubicaciones tienen sus propias ubicaciones de cómputo.

  Para añadir una zona local, póngase en contacto con su representante de Palo Alto Networks.

  Tenga en cuenta las siguientes pautas cuando implementa zonas locales:

  - Las ubicaciones de la zona local no son compatibles con IPv6.
  - Las ubicaciones de la zona local no utilizan direcciones IP registradas de Palo Alto Networks.
  - El soporte de 1 Gbps para redes remotas no es compatible.
  - La redundancia de nodos de conexión de red y servicio remotos a través de zonas de disponibilidad no está disponible si los implementa en la misma zona local, ya que ambos nodos se aprovisionan en una sola zona.
  - Estas zonas locales no utilizan direcciones IP registradas de Palo Alto Networks. Si tiene problemas para acceder a las URL, informe del problema del sitio web utilizando https://reportasite.gpcloudservice.com/ o contacte con la asistencia de Palo Alto Networks.

Revise la hoja de datos de privacidad de Prisma Access para obtener más información sobre las ubicaciones de Prisma Access y dónde Prisma Access procesan los datos.

Ubicaciones de cómputo, ciudad y país

La primera ubicación que aparece en cada ubicación de cómputo (en negrita) muestra la ciudad y el país de la ubicación de cómputo.

Las ubicaciones denotadas con dos asteriscos (**) son *Zonas Locales*, que no admiten toda la funcionalidad de Prisma Access.

Ubicación de cómputo	Prisma Access Ubicación	Ciudad y País
Asia Noreste	**Japón Central**	**Tokio, Japón**
Asia Sur	**India Oeste**	**Mumbai, India**
	Bangladesh	Dhaka, Bangladés
	India del Sur	Chennai, India

 ©2025 Palo Alto Networks, Inc.

Ubicación de cómputo	Prisma Access Ubicación	Ciudad y País
	Pakistán Sur	Karachi, Pakistán
	Pakistán occidental	Lahore, Pakistán
Asia Sudeste (Indonesia)	**Indonesia**	**Yakarta, Indonesia**
Asia Sudeste (Singapur)	**Singapur**	**Singapur**
	Camboya	Phnom Penh, Camboya
	Malasia	Kuala Lumpur, Malasia
	Myanmar	Yangón, Birmania
	Pakistán Oeste (II)	Islamabad, Pakistán
	Filipinas	Ciudad Quezon, Filipinas
	Sri Lanka	Colombo, Sri Lanka
	Tailandia	Bangkok, Tailandia
	Vietnam	Ciudad Ho Chi Minh, Vietnam
Australia Sur	**Australia Sur**	**Melbourne, Australia**
Sureste de Australia	**Sureste de Australia**	**Sydney, Australia**
	Australia Este	Brisbane, Australia
	Nueva Zelanda	Auckland, Nueva Zelanda
	Papúa Nueva Guinea	Puerto Moresby, Papúa Nueva Guinea
Australia Oeste (Perth)**	**Australia Oeste (Perth)****	**Perth, Australia**
Baréin	**Baréin**	**Manama, Baréin**
Bélgica	**Bélgica**	**San Ghislain, Bélgica**
	Letonia	Riga, Letonia
	Senegal	Dakar, Senegal
Canadá Central (Montreal)	**Canadá Este**	**Quebec, Canadá**
Canadá Central (Toronto)	**Canadá Central**	**Toronto, Canadá**
Canadá Oeste (Calgary)	**Canadá Oeste**	**Calgary, Canadá**
Europa Central	**Alemania Central**	**Fráncfort, Alemania**
	Austria	Viena, Austria
	Bulgaria	Sofía, Bulgaria

©2025 Palo Alto Networks, Inc.

Ubicación de cómputo	Prisma Access Ubicación	Ciudad y País
	Croacia	Zagreb, Croacia
	República Checa	Praga, República Checa
	Egipto	El Cairo, Egipto
	Alemania Norte	Hamburgo, Alemania
	Alemania Sur	Múnich, Alemania
	Grecia	Atenas, Grecia
	Hungría	Budapest, Hungría
	Kuwait	Al Ahmadi, Kuwait
	Liechtenstein	Schaan, Liechtenstein
	Luxemburgo	Ciudad de Luxemburgo, Luxemburgo
	Moldavia	Chisinau, Moldavia
	Nigeria	Lagos, Nigeria
	Rumania	Bucarest, Rumanía
	Eslovaquia	Bratislava, Eslovaquia
	Eslovenia	Liubliana, Eslovenia
	Turquía	Estambul, Turquía
	Ucrania	Kiev, Ucrania
	Uzbekistán	Tashkent, Uzbekistán
Europa Central (Varsovia)	**Polonia**	**Varsovia, Polonia**
Europa Norte	**Finlandia**	**Hamina, Finlandia**
	Bielorrusia	Minsk, Bielorrusia
	Kazajstán	Astana, Kazajistán
	Lituania	Vilna, Lituania
	Noruega	Oslo, Noruega
	Rusia Central	Moscú, Rusia
	Noroeste de Rusia	San Petersburgo, Rusia
Europa Norte (Estocolmo)	**Suecia**	**Estocolmo, Suecia**
Europa Noroeste	**Reino Unido**	**Londres, Reino Unido**
	Ghana	Accra, Ghana
Europa Noroeste (París)	**Francia Sur**	**París, Francia**

©2025 Palo Alto Networks, Inc.

Ubicación de cómputo	Prisma Access Ubicación	Ciudad y País
Europa Sur	**Italia** Jordania Kenia Mónaco	**Milán, Italia** Amán, Jordania Mombasa, Kenia Mónaco
Europa Suroeste	**España Central** Andorra Portugal España Este	**Madrid, España** Andorra la Vella, Andorra Lisboa, Portugal Barcelona, España
Europa Oeste	**Países Bajos Central** Dinamarca Países Bajos del Sur	**Eemshaven, Países Bajos** Copenhague, Dinamarca Róterdam, Países Bajos
Francia Norte	**Francia Norte**	**París, Francia**
Hong Kong	**Hong Kong**	**Hong Kong, China**
India Norte	**India Norte**	**Nueva Delhi, India**
Irlanda	**Irlanda**	**Dublín, Irlanda**
Japón Sur	**Japón Sur**	**Osaka, Japón**
Medio Oriente Central (Catar)	**Qatar**	**Doha, Catar**
Medio Oriente Central (Arabia Saudita)	**Arabia Saudí**	**Riad, Arabia Saudita**
Oriente Medio Central (EAU)	**Emiratos Árabes Unidos**	**Dubái, Emiratos Árabes Unidos**
Medio Oriente Oeste	**Israel**	**Tel Aviv, Israel**
Nigeria (Lagos)**	**Nigeria (Lagos)****	**Lagos, Nigeria**
Nueva Zelanda (Auckland)**	**Nueva Zelanda (Auckland)****	**Auckland, Nueva Zelanda**
Sudáfrica Central	**Sudáfrica Central**	**Johannesburgo, Sudáfrica**
Sudáfrica Oeste	**Sudáfrica Oeste**	**Ciudad del Cabo, Sudáfrica**

©2025 Palo Alto Networks, Inc.

Ubicación de cómputo	Prisma Access Ubicación	Ciudad y País
Sudamérica Este	**Brasil Sur** Brasil Central Brasil Este Paraguay Venezuela	**Sao Paulo, Brasil** Brasilia, Brasil Río de Janeiro, Brasil Asunción, Paraguay Caracas, Venezuela
América del Sur Oeste	**Chile** Argentina Bolivia Perú Uruguay	**Santiago, Chile** Buenos Aires, Argentina Santa Cruz de la Sierra, Bolivia Lima, Perú Montevideo, Uruguay
Sudamérica Oeste (Lima)**	**Sudamérica Oeste (Lima)****	**Lima, Perú**
Corea del Sur	**Corea del Sur**	**Seúl, Corea del Sur**
Suiza	**Suiza** Uganda	**Zúrich, Suiza** Kampala, Uganda
Taiwán	**Taiwán**	**ChangHua, Taiwán**
EE.UU. Central	**EE.UU. Central**	**Council Bluffs, EE. UU.**
EE.UU.Central (Chicago)**	**EE.UU.Central (Chicago)****	**Chicago, EE. UU.**
EE. UU. Centro Oeste	**EE. UU. Centro Oeste**	**Salt Lake City, EE. UU.**
Este de EE. UU.	**Este de EE. UU.** EE. UU. Noreste Guatemala	**Ashburn, EE. UU.** Ciudad de Nueva York, EE. UU. Ciudad de Guatemala, Guatemala
Noroeste de EE.UU.	**Noroeste de EE.UU.**	**The Dalles, EE. UU.**
EE. UU. Sur	**EE. UU. Sur** México Central México Oeste	**Dallas, EE. UU.** Ciudad de México, México Guadalajara, México
EE. UU. Sureste	**EE. UU. Sureste**	**Moncks Corner, EE. UU.**

©2025 Palo Alto Networks, Inc.

Ubicación de cómputo	Prisma Access Ubicación	Ciudad y País
	Colombia	Bogotá, Colombia
	Costa Rica	San José, Costa Rica
	Ecuador	Guayaquil, Ecuador
	Panamá	Ciudad de Panamá, Panamá
EE. UU. Suroeste (Miami)	**EE. UU. Suroeste (Miami)**	**Miami, EE. UU.**
EE. UU. Suroeste	**EE. UU. Suroeste**	**Los Ángeles, EE. UU.**
	EE. UU. Oeste	San Francisco, EE. UU.

Teatro y Grupo de ubicación

Teatro/grupo de ubicaciones	ID de grupo del grupo de direcciones IP
Colombia Costa Rica Ecuador Guatemala México Central Panamá Este de EE. UU. EE. UU. Sureste EE.UU. Central Costa Rica EE. UU. Central norte EE. UU. Noreste EE. UU. Sur EE. UU. Sureste Venezuela	1
Canadá Este Canadá Central	2
Irlanda	3
Francia Sur Ghana	4

©2025 Palo Alto Networks, Inc.

Teatro/grupo de ubicaciones	ID de grupo del grupo de direcciones IP
RU	
Francia Norte	5
Asia, Australia y Japón	6
Andorra Austria Bulgaria Croacia República Checa Egipto Alemania Central Alemania Norte Alemania Sur Grecia Hungría Israel Italia Jordania Kenia Kuwait Liechtenstein Luxemburgo Moldavia Mónaco Nigeria Polonia Portugal Rumania Eslovaquia Eslovenia Arabia Saudí Sudáfrica Central	7

©2025 Palo Alto Networks, Inc.

Teatro/grupo de ubicaciones	ID de grupo del grupo de direcciones IP
España Central España Este Turquía Ucrania Emiratos Árabes Unidos Uzbekistán	
Bielorrusia Finlandia Kazajstán Lituania Noruega Rusia Central Noroeste de Rusia Suecia	8
Dinamarca Países Bajos Central Países Bajos del Sur	9
África, Europa y Oriente Medio	10
Suiza Uganda	11
Bélgica Letonia Senegal	12
Brasil Central Brasil Este Brasil Sur Paraguay Venezuela	13
Australia Este Australia Sur	14

©2025 Palo Alto Networks, Inc.

Teatro/grupo de ubicaciones	ID de grupo del grupo de direcciones IP
Sureste de Australia Nueva Zelanda Papúa Nueva Guinea	
Camboya Indonesia Malasia Myanmar Filipinas Singapur Tailandia Vietnam	15
Hong Kong	16
Taiwán	17
Corea del Sur	18
Bangladesh India Norte India del Sur India Oeste Pakistán occidental Pakistán Sur Qatar	19
Sudáfrica Oeste Suecia Sudáfrica Oeste	20
Japón Central Japón Sur	21
Baréin	22
Canadá Oeste México Central	23

©2025 Palo Alto Networks, Inc.

Teatro/grupo de ubicaciones	ID de grupo del grupo de direcciones IP
México Oeste EE. UU. Centro Oeste Noroeste de EE.UU. EE. UU. Suroeste EE. UU. Oeste	
Argentina Bolivia Chile Perú Uruguay	24

Ubicaciones por región

Ubicaciones
Región de África
Kenia
Nigeria
Senegal
Sudáfrica Central
Sudáfrica Oeste
Región de Asia
Bangladesh
Camboya
Hong Kong
India Norte
India del Sur
India Oeste
Indonesia

©2025 Palo Alto Networks, Inc.

Ubicaciones
Kazajstán
Malasia
Myanmar
Pakistán Sur
Pakistán occidental
Pakistán Oeste (II)
Papúa Nueva Guinea
Filipinas
Singapur
Corea del Sur
Sri Lanka
Taiwán
Tailandia
Vietnam
Región ANZ
Australia Este
Australia Sur
Sureste de Australia
Nueva Zelanda
Región de Europa
Andorra
Austria
Bielorrusia
Bélgica
Bulgaria

©2025 Palo Alto Networks, Inc.

Ubicaciones
Croacia
República Checa
Dinamarca
Finlandia
Francia Norte
Francia Sur
Alemania Central
Alemania Norte
Alemania Sur
Ghana
Grecia
Hungría
Irlanda
Italia
Letonia
Liechtenstein
Lituania
Luxemburgo
Moldavia
Mónaco
Países Bajos Central
Países Bajos del Sur
Noruega
Polonia
Portugal

©2025 Palo Alto Networks, Inc.

Ubicaciones
Rumania
Rusia Central
Noroeste de Rusia
Eslovaquia
Eslovenia
España Central
España Este
Suecia
Suiza
Uganda
RU
Ucrania
Uzbekistán
Región de Japón
Japón Central
Japón Sur
Región de Oriente Medio
Baréin
Egipto
Israel
Jordania
Kuwait
Qatar
Arabia Saudí
Turquía

©2025 Palo Alto Networks, Inc.

Ubicaciones
Emiratos Árabes Unidos
Región de América del Norte
Canadá Central
Canadá Este
Canadá Oeste
Costa Rica
México Central
México Oeste
Panamá
EE.UU. Central
EE. UU. Centro Oeste
Este de EE. UU.
EE. UU. Noreste
Noroeste de EE.UU.
EE. UU. Sur
EE. UU. Sureste
EE. UU. Suroeste
EE. UU. Oeste
Región de América del Sur
Argentina
Bolivia
Brasil Central
Brasil Este
Brasil Sur
Chile

©2025 Palo Alto Networks, Inc.

Ubicaciones
Colombia
Ecuador
Paraguay
Perú
Uruguay
Venezuela

Ubicaciones de Proxy explícito

Prisma Access es compatible con las siguientes ubicaciones para proxy explícito. El Proxy explícito utiliza GeoDNS para resolver y conectar al usuario móvil con la ubicación implementada de Prisma Access más cercana.

- **África, Europa y Oriente Medio:**
  - Bélgica
  - Finlandia
  - Francia Sur
  - Alemania Central
  - Israel
  - Italia
  - Países Bajos Central
  - Polonia
  - Qatar
  - Arabia Saudí
  - Sudáfrica Central
  - España Central
  - Suiza
  - RU

 ©2025 Palo Alto Networks, Inc.

- **Asia, Australia y Japón:**
  - Australia Sur
  - Sureste de Australia
  - China
  - Hong Kong
  - Japón Central
  - Japón Sur
  - India Norte
  - India Oeste
  - Indonesia
  - Singapur
  - Corea del Sur
  - Taiwán
- **América del Norte y América del Sur:**
  - Brasil Sur
  - Chile
  - Canadá Central
  - Canadá Este
  - EE.UU. Central
  - Este de EE. UU.
  - Noroeste de EE.UU.
  - EE. UU. Sur
  - EE. UU. Sureste
  - EE. UU. Suroeste
  - EE. UU. Centro Oeste

Ubicaciones de Colo-Connect

Prisma Access Colo-Connect es compatible con las siguientes ubicaciones de Prisma Access. Cuando cree conexiones de servicio para soportar Colo-Connect, asegúrese de crearlas solo en las siguientes ubicaciones.

Para enlaces de interconexión dedicados, utilice la lista de ubicaciones de GCP *donde puede crear conexiones de Interconexión dedicada.*

- Australia Sur
- Sureste de Australia
- Bélgica
- Brasil Sur

 ©2025 Palo Alto Networks, Inc.

- Canadá Central
- Canadá Este
- Chile
- Finlandia
- Francia Sur
- Alemania Central
- Hong Kong
- India Norte
- India Oeste
- Indonesia
- Italia
- Japón Central
- Japón Sur
- Países Bajos Central
- Qatar
- Arabia Saudí
- Singapur
- Sudáfrica Central
- España Central
- Suiza
- Taiwán
- RU
- EE.UU. Central
- EE. UU. Centro Oeste
- Este de EE. UU.
- Noroeste de EE.UU.
- EE. UU. Sur
- EE. UU. Sureste
- EE. UU. Suroeste

Regiones Strata Logging Service compatibles

Prisma Access admite las siguientes regiones de Strata Logging Service:

- Australia
- Canadá
- Francia
- Alemania

 ©2025 Palo Alto Networks, Inc.

- Japón
- India
- Indonesia
- Israel
- Países Bajos: Europa
- Qatar
- Arabia Saudí
- Singapur
- Suiza
- Taiwán
- Reino Unido
- Estados Unidos: Américas

Redes remotas: Alto rendimiento, Replicación de tráfico y Ubicaciones de acceso seguro entrante

Las siguientes ubicaciones de redes remotas de alto rendimiento son compatibles con Prisma Access:

- Andorra
- Argentina
- Australia Este
- Australia Sur
- Sureste de Australia
- Austria
- Bangladesh
- Bielorrusia
- Bélgica
- Bolivia
- Brasil Central
- Brasil Este
- Brasil Sur
- Bulgaria
- Camboya
- Canadá Central
- Canadá Este
- Chile
- Colombia

 ©2025 Palo Alto Networks, Inc.

- Costa Rica
- Croacia
- República Checa
- Dinamarca
- Ecuador
- Egipto
- Finlandia
- Francia Norte
- Francia Sur
- Alemania Central
- Alemania Norte
- Alemania Sur
- Ghana
- Grecia
- Guatemala
- Hong Kong
- Hungría
- India Norte
- India del Sur
- India Oeste
- Indonesia
- Israel
- Italia
- Japón Central
- Japón Sur
- Jordania
- Kazajstán
- Kenia
- Kuwait
- Letonia
- Liechtenstein
- Lituania
- Luxemburgo
- Malasia
- México Central
- México Oeste

 ©2025 Palo Alto Networks, Inc.

- Moldavia
- Mónaco
- Myanmar
- Países Bajos Central
- Países Bajos del Sur
- Nueva Zelanda
- Nigeria
- Noruega
- Pakistán Sur
- Pakistán occidental
- Pakistán Oeste (II)
- Panamá
- Papúa Nueva Guinea
- Paraguay
- Perú
- Filipinas
- Polonia
- Portugal
- Qatar
- Rumania
- Rusia Central
- Noroeste de Rusia
- Arabia Saudí
- Senegal
- Singapur
- Eslovaquia
- Eslovenia
- Sudáfrica Central
- Corea del Sur
- España Central
- España Este
- Sri Lanka
- Suiza
- Taiwán
- Tailandia
- Turquía

 ©2025 Palo Alto Networks, Inc.

- Uganda
- RU
- Ucrania
- Uruguay
- EE.UU. Central
- EE. UU. Centro Oeste
- Este de EE. UU.
- EE. UU. Noreste
- Noroeste de EE.UU.
- EE. UU. Sur
- EE. UU. Sureste
- EE. UU. Suroeste
- EE. UU. Oeste
- Uzbekistán
- Venezuela
- Vietnam

Ubicaciones de Prisma Access en China

Prisma Access China apoya las siguientes ubicaciones en China continental:

- China Norte—Pekín (utiliza la ubicación de cómputo de China Norte)
- China Noroeste—Ningxia (utiliza la ubicación de cómputo de China Noroeste)

Ubicaciones de FedRAMP moderado y alto

Encuentra la lista de ubicaciones de FedRAMP en la documentación FedRAMP de Prisma SASE.

Mapa de ubicaciones de América del Norte

Utilice el siguiente mapa como referencia para ayudarle a elegir ubicaciones de Prisma Access en América del Norte.

 ©2025 Palo Alto Networks, Inc.



Ubicaciones de la zona local

Las siguientes zonas locales son compatibles con IPv4 en Prisma Access:

- *Necesita trabajar con su representante de Palo Alto Networks para iniciar una solicitud de despliegue en una de las siguientes zonas locales.*
- *IPv6 no es compatible*

- Australia Oeste (Perth)
- Nueva Zelanda (Auckland)
- Nigeria (Lagos)
- Sudamérica Oeste (Lima)
- EE.UU. Central (Chicago)
- EE.UU.Sudeste (Miami)

©2025 Palo Alto Networks, Inc.

Prisma Access y ubicaciones de procesamiento de servicios asociados

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access ofrece una experiencia local en más de 100 ubicaciones en todo el mundo y asigna cada ubicación a una ubicación de cómputo de seguridad en función del rendimiento y la latencia optimizados.

Si tiene el requisito de limitar las ubicaciones de cómputo a países específicos, consulte la asignación de países para cada ubicación de Prisma Access e implemente solo aquellas ubicaciones que estén asociadas con esos países durante la configuración de Prisma Access.

La siguiente tabla le proporciona la ubicación de procesamiento del país para las regiones de Strata Logging Service, Strata Cloud Manager (para Prisma Access (Managed by Strata Cloud Manager), Prisma Access Insights, Autonomous DEM y SaaS Security Inline.

Strata Logging Service	Configuración de Strata Cloud Manager	Datos de Prisma Access Insights	Autonomous DEM	SaaS Security Inline
Reino Unido	Reino Unido	Reino Unido	Reino Unido	Reino Unido
Países Bajos	Alemania	Países Bajos	Países Bajos	Alemania (UE)
Alemania	Alemania	Alemania	Alemania	Alemania (UE)
Suiza	Suiza	Suiza	Suiza	Alemania (UE)
Francia	Alemania	Francia	Francia	Alemania (UE)
Singapur	Singapur	Singapur	Singapur	Singapur
India	India	India	India	India
Japón	Japón	Japón	Japón	Japón
Canadá	Canadá	Canadá	Canadá	Estados Unidos
Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos	Estados Unidos
Australia	Australia	Australia	Australia	Australia
Israel	Alemania	Israel	Israel	Alemania (UE)

©2025 Palo Alto Networks, Inc.

Strata Logging Service	Configuración de Strata Cloud Manager	Datos de Prisma Access Insights	Autonomous DEM	SaaS Security Inline
Qatar	Qatar	Qatar	Qatar	Alemania (UE)
Arabia Saudí	Alemania	Arabia Saudí	Arabia Saudí	Alemania (UE)
Taiwán	Singapur	Taiwán	Taiwán	Singapur
Indonesia	Singapur	Indonesia	Indonesia	Singapur

©2025 Palo Alto Networks, Inc.

Prisma Access Gestión de infraestructuras

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (gestionado por Panorama)	❑ Licencia de Prisma Access

Prisma Access utiliza un modelo de propiedad compartida. Palo Alto Networks administra la infraestructura de seguridad subyacente, garantizando que sea segura, resistente, esté actualizada y esté disponible para usted cuando la necesite. La responsabilidad de su organización es incorporar ubicaciones y usuarios, insertar políticas, actualizarlas, consultar logs y generar informes.

Palo Alto Networks gestiona las siguientes partes de la infraestructura de seguridad. Además de la infraestructura de seguridad, Prisma Access gestiona versiones y actualizaciones:

- **Prisma Access**
- **Strata Logging Service**: gestionamos el mecanismo de entrega de los logs.
- **Actualizaciones de contenido**: gestionamos versiones y actualizaciones, incluidas las actualizaciones de PAN-OS. Para sus usuarios móviles, Prisma Access aloja varias versiones de la aplicación GlobalProtect y puede seleccionar la versión activa de la aplicación GlobalProtect de esa lista.
- **Tolerancia a fallos**: gestionamos la disponibilidad del servicio.
- **Escalado automático**: ampliamos automáticamente el servicio cuando se añaden conexiones de servicio o redes remotas, o cuando usuarios móviles adicionales inician sesión en una o más puertas de enlace en una sola región.
- **Aprovisionamiento**: aprovisionamos la infraestructura con todo lo que se requiere.
- **Supervisión de servicios**: Supervisamos el estado del servicio y lo mantenemos funcionando.
- **Asignación de ubicación de cómputo**: Cada ubicación de Prisma Access se asigna a la ubicación de cómputo de seguridad en función del rendimiento y la latencia optimizados, lo que significa que, a menos que un administrador del sistema lo modifique de otro modo, el tráfico en determinados países se dirigirá a una ubicación de cómputo definida. Véase la Hoja de datos de privacidad de Prisma Access para la asignación de ubicación a cómputo.

Su organización gestiona los siguientes componentes de la infraestructura de seguridad.

- **Usuarios**: gestiona la incorporación de usuarios móviles.
- **Autenticación**: usted gestiona la autenticación de esos usuarios.
- **Gestión de dispositivos móviles (MDM)**: puede controlar los dispositivos móviles de su organización que están protegidos con Prisma Access utilizando su propio software MDM.
- (Prisma Access (Managed by Panorama) únicamente) **Complemento de Panorama y Servicios en la nube**: asegúrese de que el Panorama en el que está instalado el complemento de Servicios en la nube está ejecutando una versión de Panorama que admite el complemento Cloud

 ©2025 Palo Alto Networks, Inc.

Services). Además, usted actualiza el complemento Cloud Services en Panorama después de que le informemos que hay un nuevo complemento disponible.

- **Creación y gestión de políticas**: planifique y cree las políticas en Panorama para utilizarlas con Prisma Access.
- **Análisis de logs y análisis forenses**: Prisma Access proporciona los logs, usted proporciona el análisis y la generación de informes, utilizando herramientas integradas proporcionadas por nosotros o por otro proveedor.
- **Seguridad local**: proporciona la seguridad local entre las microsegmentaciones de su red local. En algunas implementaciones, también puede dirigir todo el tráfico para que se proteja con Prisma Access.
- **Redes**: proporciona la conectividad de red a Prisma Access.
- **Monitoring (Supervisión)**: supervisa el estado de la red local.
- **Conectividad de servicio**: usted proporciona la conectividad a la puerta de enlace de Prisma Access para usuarios móviles (por ejemplo, proporcionar un ISP) y también proporciona los dispositivos locales utilizados como endpoints para los túneles IPSec utilizados por las conexiones de servicio y las conexiones de red remotas.
- **Incorporación**: incorpora los usuarios móviles, los sitios de la sede central/centro de datos y las sucursales.
- (Prisma Access (Managed by Panorama) únicamente)**Hacer copia de seguridad**: usted gestiona la copia de seguridad de la configuración de Panorama.

 ©2025 Palo Alto Networks, Inc.

API de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

API para Prisma Access (Managed by Strata Cloud Manager)

Puede encontrar más información sobre las API para Prisma Access (Managed by Strata Cloud Manager) en pan.dev, el sitio de documentación para desarrolladores de Palo Alto Networks. Prisma Access (Managed by Strata Cloud Manager) utiliza estas API para la incorporación, configuración y operaciones del servicio.

API para Prisma Access (Managed by Panorama)

Además de las API XML que están disponibles para la configuración y gestión en Panorama, existen API XML para el complemento Cloud Services que puede usar para realizar tareas específicas de Prisma Access. Utilice estas API a través de un servicio, una aplicación o un script de terceros para automatizar las tareas de configuración y generación de informes para Prisma Access.



 ©2025 Palo Alto Networks, Inc.

Acceda a la API de Prisma Access (Managed by Panorama) utilizando el navegador y la interfaz web

Para acceder a la API mediante el navegador, inicie sesión en el Panorama que gestiona Prisma Access con privilegios de administrador, luego introduzca /api al final de la URL. La URL cambia a la interfaz del navegador API XML.

Las API de Prisma Access se encuentran en los siguientes nodos del lenguaje de ruta XML (XPath) en el árbol XML:

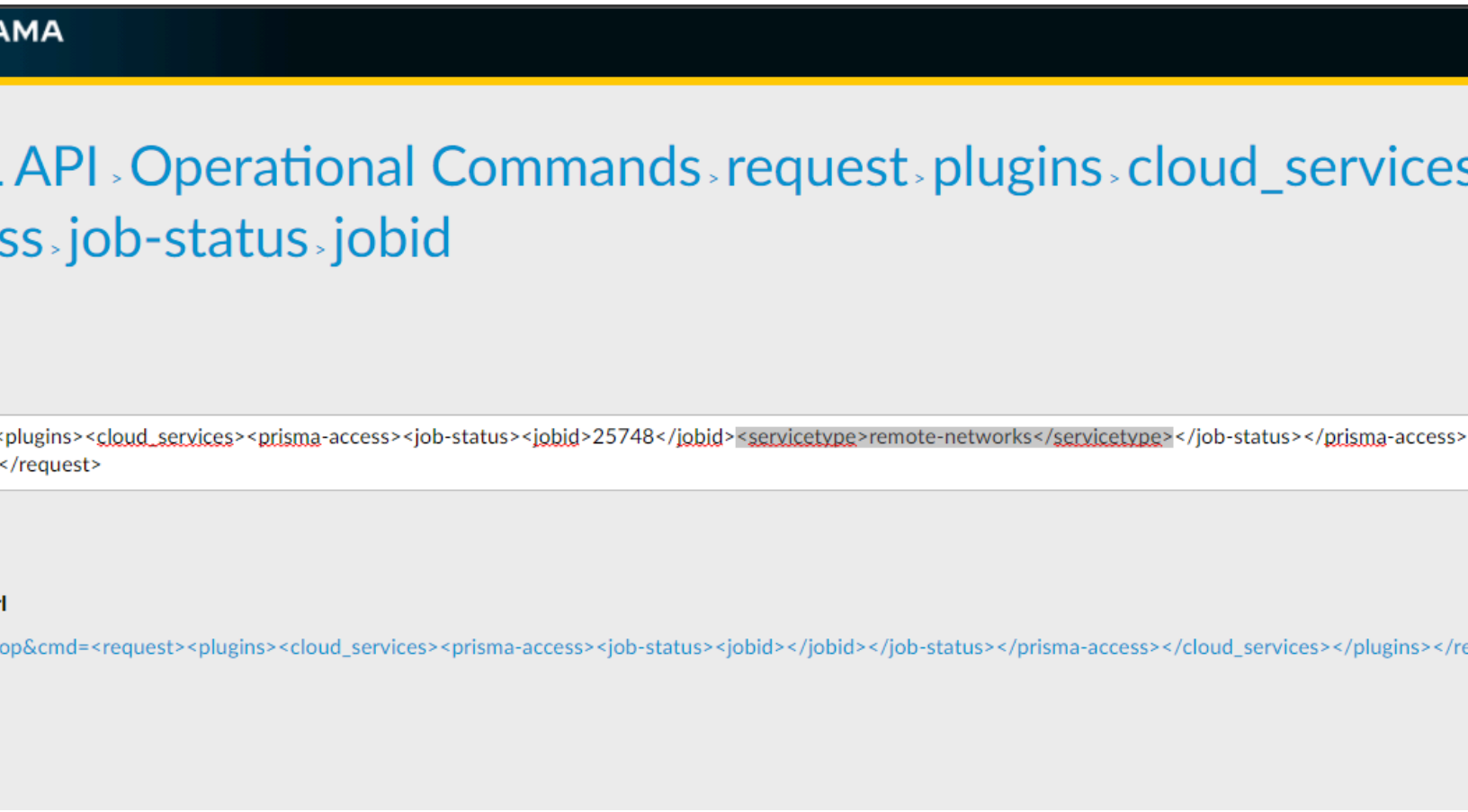
- Comandos de configuración: **XML API** > **Configuration Commands (Comandos de configuración)** > **devices (dispositivos)** > **entry[@name='localhost.localdomain']** > **plugins (complementos)** > **cloud_services**
- Comandos de operación: **XML API (API XML)** > **Operational Commands (Comandos operativos)** > **request (solicitud)** > **plugins (complementos)** > **cloud_services** > **prisma-access**

A medida que navega por el árbol XML, Prisma Access rellena el árbol en el área **XML** . Puede introducir los valores requeridos en el área **XML** y hacer clic en **Submit (Enviar)** para procesar una solicitud XML. Por ejemplo, para solicitar el estado de incorporación de un trabajo, vaya a **XML API** > **Operational Commands (Comandos de operación)** > **request (solicitud)** > **plugins (complementos)** > **cloud_services** > **prisma-access** > **job-status** > **jobid**, introduzca el ID del trabajo en el campo **jobid**, introduzca el área Tipo de servicio **servicetype** y haga clic en **Submit (Enviar)** para enviar su solicitud.



Este XML solo recupera el estado de incorporación de un trabajo. Para recuperar el estado de todas las operaciones de confirmación, utilice la Interfaz de usuario de Prisma Access.

©2025 Palo Alto Networks, Inc.



Prisma Access devuelve la salida en formato XML.

 ©2025 Palo Alto Networks, Inc.

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<response status="success">
  <result>
    <result>
      <status>pass</status>
      <msg>
        <response>
          <status>SUCCESS</status>
          <servicetype>remote-networks</servicetype>
          <workflow>jobStatusResponse</workflow>
          <InstanceSummary>
            <Remote-Network>
              <overview>
                <TotalInstances>0</TotalInstances>
                <ProvisioningInProgress>0</ProvisioningInProgress>
                <ProvisioningFailed>0</ProvisioningFailed>
                <ProvisioningComplete>0</ProvisioningComplete>
              </overview>
            </Remote-Network>
          </InstanceSummary>
          <percentageCompletion>100</percentageCompletion>
          <jobid>25748</jobid>
          <errorCode>0</errorCode>
          <apiVersion>2.0</apiVersion>
        </response>
      </msg>
    </result>
  </result>
</response>
```


También puede utilizar la interfaz web para encontrar las API en Panorama.

Utilice los comandos curl para recuperar los comandos de la API gestionada por Panorama

Si prefiere utilizar CLI para recuperar los resultados de los comandos API, puede utilizar las API junto con la API que utiliza para recuperar direcciones IP públicas y de infraestructura para Prisma Access. Para hacerlo, utilice el siguiente comando:

Comandos de configuración:

`curl -k -X GET "https://`*<panorama-ip-address>*`/api/?key=`*<api-key>*`&tipo=config&cmd=`*<api-parameters></api-parameters>*

Comandos de operación:

`curl -k -X GET "https://`*<panorama-ip-address>*`/api/?key=`*<api-key>*`&type=op&cmd=`*<api-parameters></api-parameters>*

Donde:

 ©2025 Palo Alto Networks, Inc.

- *<panorama-ip-address>* es la dirección IP del Panorama que gestiona Prisma Access.
- *<api-key>* es la clave API recupera direcciones IP para Prisma Access (**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicio)** > **Generate API Key (Generar clave de API)**).
- *<api-parameters>* y *</api-parameters>* son los parámetros de API que utiliza para recuperar la información solicitada de la API.

Si tiene una implementación de varios inquilinos, añada el nombre del inquilino para el cual desea recuperar información de API en la API.

Por ejemplo, dado una implementación Prisma Access que tiene los siguientes parámetros:

- **Dirección IP de Panorama:** 1.2.3.4
- **Clave API:** 12345abcde
- **Nombre del inquilino:** tenant-1

Si desea recuperar la cantidad de usuarios móviles activos para ese inquilino, deberá Introducir el siguiente comando curl:

```
curl -k -X GET "https://1.2.3.4/api/?
key=12345abcde&type=op&cmd=<request><plugins><cloud_services><prisma-
access><multi-tenant><tenant-name><entry%20name='tenant-1'></entry></
tenant-name><remote-active-users-count/></multi-tenant></prisma-
access></cloud_services></plugins></request>"
```

Utilice comandos de la CLI con Prisma Access (Managed by Panorama)

Prisma Access le permite utilizar CLI commands (Comandos CLI) para recuperar los datos de Prisma Access. Para acceder a la CLI, establezca una conexión SSH utilizando la dirección IP del Panorama que gestiona Prisma Access.

La CLI usa los mismos modos y tiene el mismo comportamiento que los comandos PAN-OS, con la excepción que introduce el nombre del inquilino para implementaciones de múltiples inquilinos; introduce el nombre del inquilino usando el comando *owner-name* **.** Por ejemplo, dado un nombre de inquilino de *tenant-1*, introduzca el siguiente comando para recuperar el recuento de usuarios activos en una implementación de múltiples inquilinos:

```
admin-Panorama> solicitar complementos cloud_services prisma-access
 multi-tenant remote-active-users-count owner-name owner-1 pasar
 Cantidad actual de usuarios: 253
```

APIs de Insights de Prisma Access

Las API de Insights de Prisma Access le permiten consultar sus inquilinos de Insights de Prisma Access para recursos de datos. Hay dos versiones de las API. Las API Insights 2.0 y 1.0 de Prisma Access le permiten consultar a su inquilino de Prisma Access sobre estado de su implementación de red de Prisma Access. Las llamadas a la API son las mismas para ambas versiones; sin embargo, cada versión utiliza diferentes tokens de acceso, y el mecanismo por el cual obtiene un token de acceso es diferente para cada versión.

 ©2025 Palo Alto Networks, Inc.

Para comenzar con las APIs de Insights de Prisma Access, vaya a la Guía del desarrollador en Bienvenido a Prisma SASE.

La API de Prisma Access Insights describe contenido específico de las API de Prisma Access Insights, así como información sobre la versión 2.0 de la API, la versión 1.0 de la API, ejemplos de la API de Prisma Access Insights y Preguntas frecuentes sobre PAI.

Acerca de las API 2.0

Las API de Prisma Access Insights 2.0 están destinadas a los clientes de Prisma Access (Managed by Strata Cloud Manager), donde Palo Alto Networks ha incorporado los inquilinos utilizando un identificador de Grupo de servicios de inquilinos (TSG). Para ver si su inquilino utiliza ID de TSG, vaya al hub de Prisma Access, haga clic en el nombre de la aplicación **Prisma Access Insights** y busque en la sección **Gestionar aplicaciones**.

Las API 2.0 también las pueden utilizar los clientes de Prisma Access (Managed by Panorama). En este caso, si la implementación de Prisma Access (Managed by Panorama) es multiinquilino, entonces solo el superinquilinos tiene el ID de TSG, y los subinquilinos están incluidos en el encabezado con el ID de inquilino de Strata Logging Service.

Caso API 2.0

Después de la migración del superinquilino al ID de TSG, al consultar un subinquilino:

El encabezado necesita la siguiente información: `Prisma-Tenant:tsg_id:sub_tenant_id`

Acerca de las API 1.0

Las API de Prisma Access Insights 1.0 están destinadas a todos los clientes de Prisma Access (Managed by Strata Cloud Manager) de un solo inquilino, así como a clientes de un solo inquilino y multiinquilino de Prisma Access (Managed by Panorama).

Caso API 1.0

Antes de la migración del superinquilino al ID de TSG, cuando consulta la información de un subinquilino utilizando las API 1.0, incluya el ID del superinquilino en el endpoint:

`/api/sase/v1.0/resource/tenant/{super_tenant_id}/`

Incluye el siguiente encabezado en la llamada: `Prisma-Tenant: {tenant_id}: {sub_tenant_id}`

 ©2025 Palo Alto Networks, Inc.

Migrar Prisma Access de Panorama a Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access Para comenzar la migración de Prisma Access (Managed by Panorama) a Prisma Access (Managed by Strata Cloud Manager), póngase en contacto con su equipo de cuentas de Palo Alto Networks.

Si tiene una implementación de Prisma Access existente para el cual la configuración es gestionada por Panorama y desea migrar a Strata Cloud Manager para la gestión de la configuración, Palo Alto Networks ofrece un flujo de trabajo en el producto que le permite migrar su configuración existente de Prisma Access a Strata Cloud Manager.

Gestionar su configuración de Prisma Access utilizando Strata Cloud Manager en lugar de Panorama puede ofrecerte beneficios como:

- Evaluaciones continuas de prácticas recomendadas
- Configuraciones predeterminadas seguras
- Optimización de configuración basada en aprendizaje automático (ML)
- Flujos de trabajo de seguridad web optimizados
- Un resumen visual interactivo (Centro de control) que le ayuda a evaluar la salud, la seguridad y la eficiencia de la red.
- Flujos de trabajo intuitivos para tareas complejas
- Gestión de las API simples y seguras
- La arquitectura nativa de la nube proporciona escalabilidad, resiliencia y alcance global.
- No hay hardware que gestionar ni software que mantener

Prepárese para migrar a Prisma Access (Managed by Strata Cloud Manager)

Antes de comenzar su migración, debe estar al tanto de los requisitos mínimos de software y de los tipos de implementaciones de Prisma Access (Managed by Panorama) que puede migrar.

- **Cuándo migrar**: no realice su actualización durante una actualización del plano de datos o de la infraestructura. Verifique sus preferencias de actualización para ver si tiene una próxima actualización del plano de datos.
- **Migración unidireccional de Panorama a Prisma Access (Managed by Strata Cloud Manager)**: solo puede migrar de un Prisma Access (Managed by Panorama) a una implementación de Prisma Access (Managed by Strata Cloud Manager). Después de migrar a Strata Cloud

©2025 Palo Alto Networks, Inc.

Manager, no puede volver a gestionar su implementación de Prisma Access utilizando Panorama.

- **Versión mínima de Panorama**: se requiere una versión mínima de Panorama de 10.0.
- **Función de administrador requerido**: debe haber iniciado sesión como superusuario en Strata Cloud Manager para comenzar la migración.
- **Requisitos de licencia**: se requiere una licencia de Prisma Access válida.
- **Cloud Identity Engine**: debe haber integrado el componente Directory Sync de Cloud Identity Engine con el inquilino de Prisma Access (Managed by Panorama) actual antes de migrar.
- **Funcionalidades no soportadas**: el programa de migración no soporta las siguientes funcionalidades de Prisma Access:
  - Implementaciones de varios inquilinos
  - IoT Security
  - Filtrado de datos (como una alternativa, utilice Enterprise DLP)
  - SSH proxy
  - Autenticación separada para portales y puertas de enlace de GlobalProtect
- **Config Diff Issues (Problemas de diferencia de configuración)**: cuando ejecuta la diferencia de configuración durante la migración, ignore cualquier diferencia que muestra los siguientes nombres de objeto porque tno afectan su configuración:
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

Migra su implementación de Prisma Access (Managed by Panorama) a Strata Cloud Manager

Para migrar su Prisma Access (Managed by Panorama) a una implementación de Prisma Access (Managed by Strata Cloud Manager), complete los siguientes pasos.

A un alto nivel, usted:

1. Asegúrese de haber enviado correctamente la última configuración a Prisma Access, haber guardado la última configuración y haber exportado un archivo de configuración .xml desde el Panorama que gestiona Prisma Access.
2. Inicie el programa de migración desde Strata Cloud Manager.
3. Verifique las diferencias de configuración (difs) entre la configuración de Panorama y la configuración migrada de Strata Cloud Manager.
4. Resuelve las diferencias y completa la migración.

 ©2025 Palo Alto Networks, Inc.

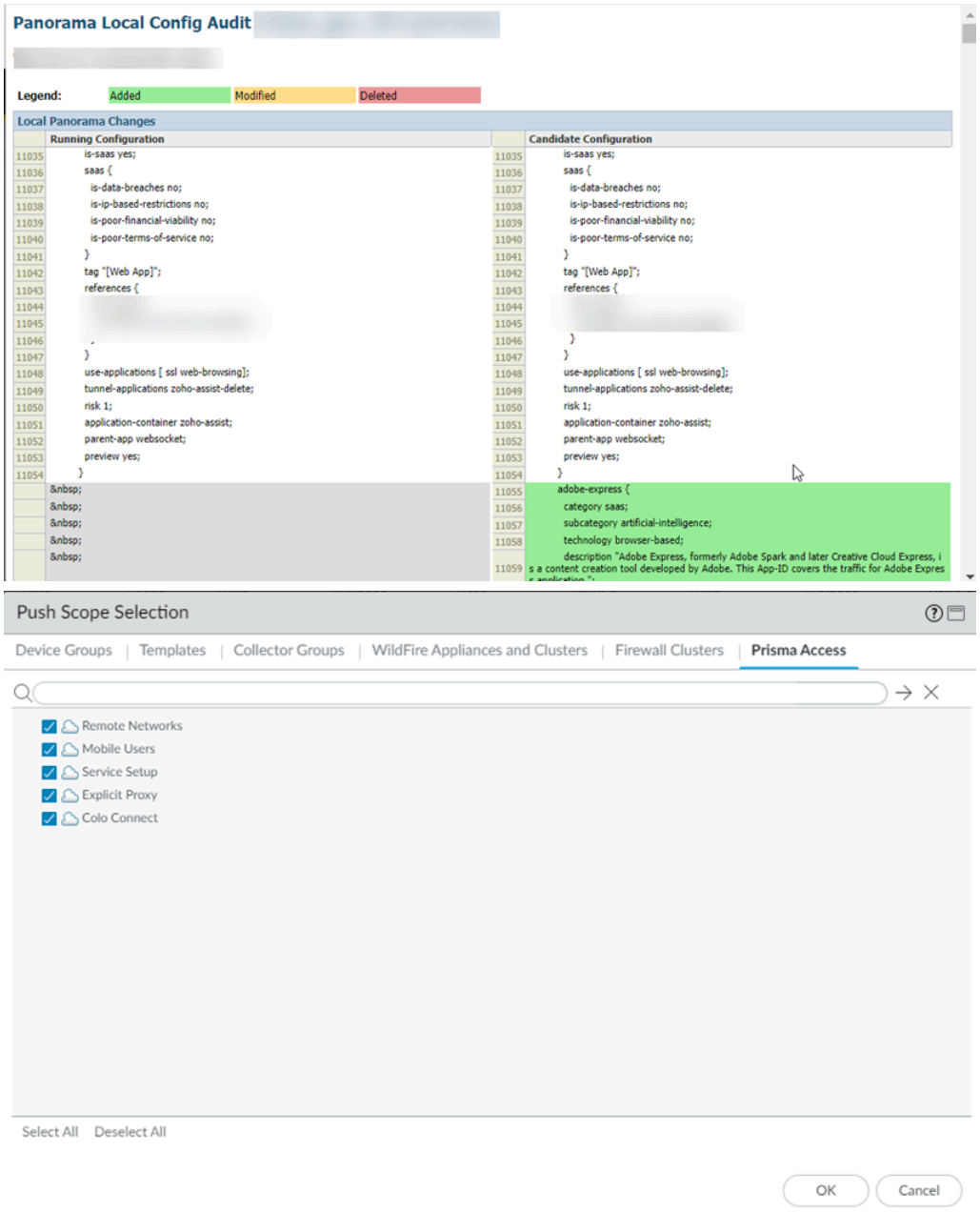
STEP 1 | Prepare su Panorama para la migración.

1. Inicie sesión en el Panorama que gestiona Prisma Access con una cuenta administrativa que tiene asignado la función de superusuario.
2. (Opcional) Si has configurado una Clave Maestra personalizada para su Panorama y para Prisma Access, haga una nota de ello.

   Si su implementación utiliza la clave maestra predeterminada, este paso no es necesario.
3. Asegúrese de que su configuración actual de Panorama esté actualizada y de que haya confirmado y enviado todos sus cambios a Panorama y a Prisma Access yendo a **Commit (Confirmar)** > **Commit & Push (Confirmar y enviar)** y **Preview Changes (Vista previa de cambios)**.
4. (Opcional) Verifique las diferencias entre la configuración en ejecución y la configuración candidata y determine si desea aplicar esos cambios. Si desea confirmar y enviar los

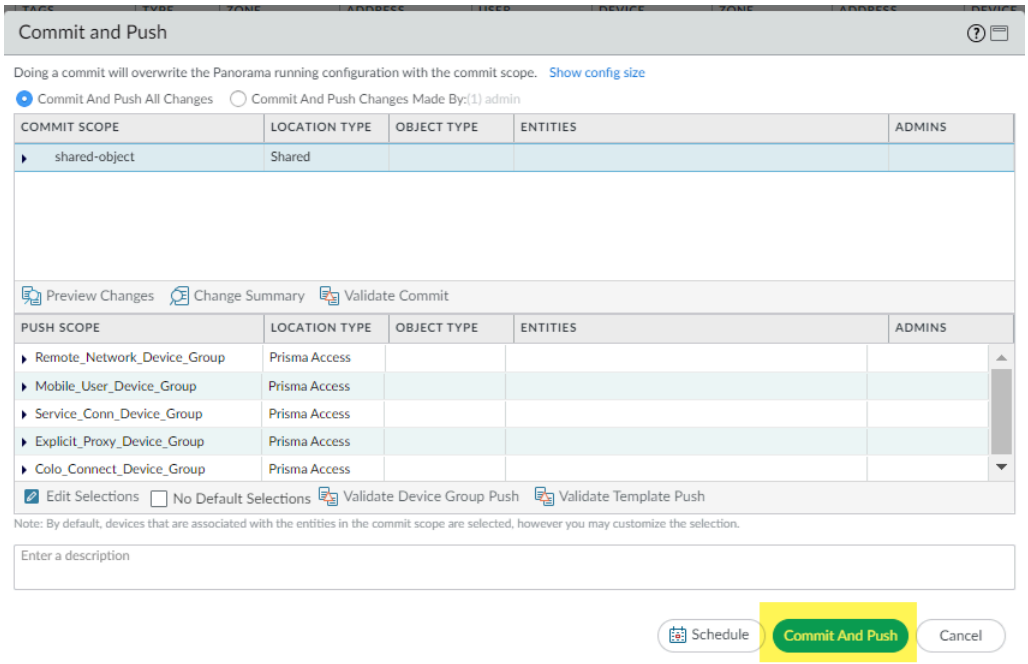
 ©2025 Palo Alto Networks, Inc.

cambios, deberá **Edit Selections (Editar las selecciones)** y seleccionar los componentes de Prisma Access que desea enviar en el **Push Scope (Ámbito de envío)**.



5. (Opcional) **Commit and Push (Confirmar y enviar)** sus cambios.

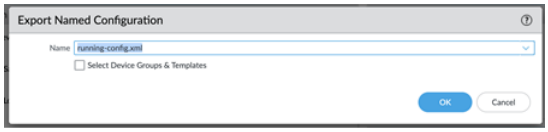
 ©2025 Palo Alto Networks, Inc.



6. Vaya a **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** y **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**.

   Este archivo .xml es necesario para cargar aStrata Cloud Manager durante el proceso de migración. **No suba un archivo de asistencia técnica ni ningún otro archivo excepto un archivo de configuración .xml.**

7. Seleccione el archivo de configuración **running-config.xml** y luego **OK (Aceptar)**.

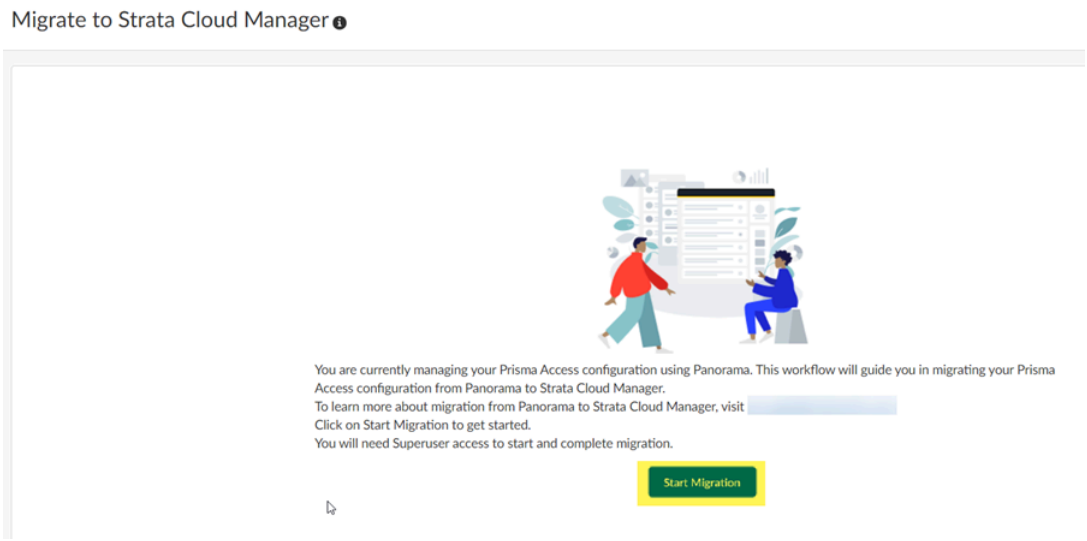


STEP 2 | Inicie sesión en Strata Cloud Manager como administrador con una función de Superusuario y vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**.

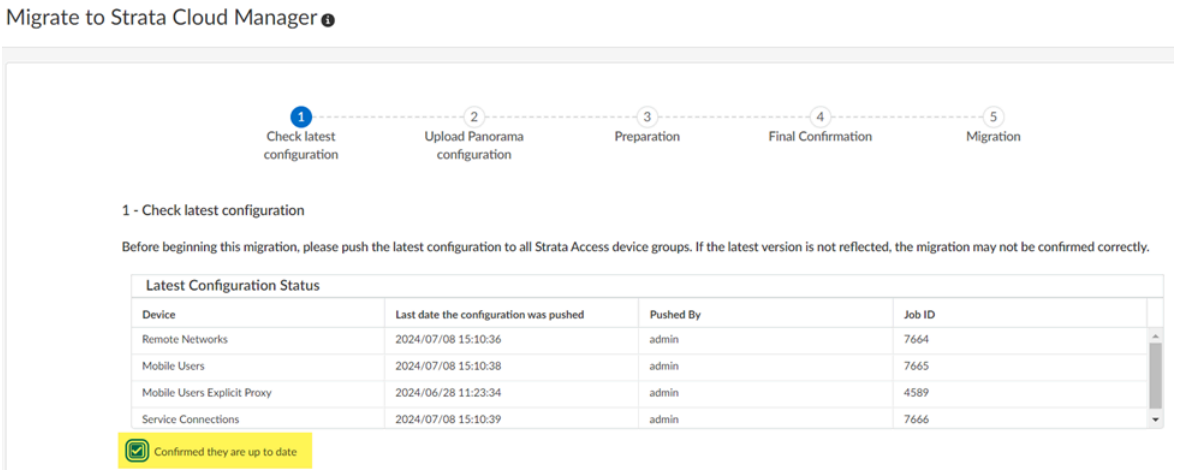
El programa de migración detecta que tiene una implementación gestionado por Panorama.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | **Iniciar la migración.**



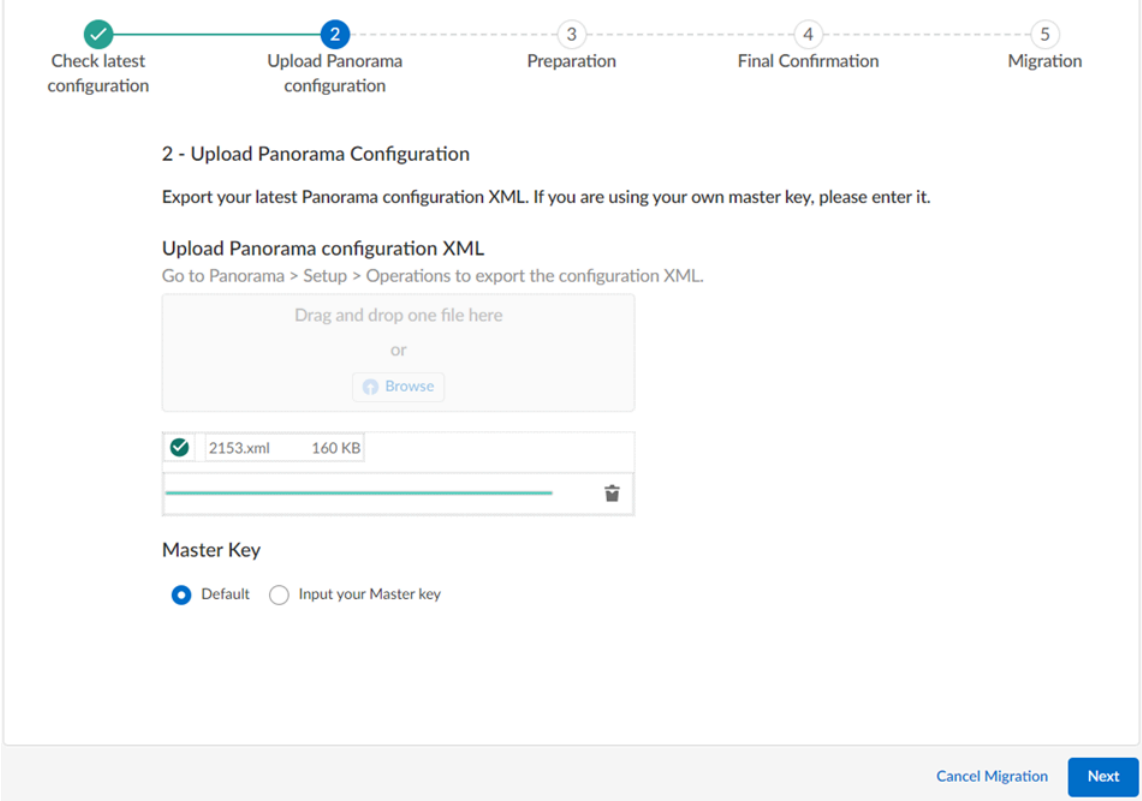
STEP 4 | El programa de migración le pide que se asegure de que su configuración esté actualizada y le muestra el último usuario que la actualizó. Después de haber verificado que esta configuración tiene los últimos cambios, seleccione **Confirmed they are up to date (Confirmado que están actualizados)** y haga clic en **Next (Siguiente)**.



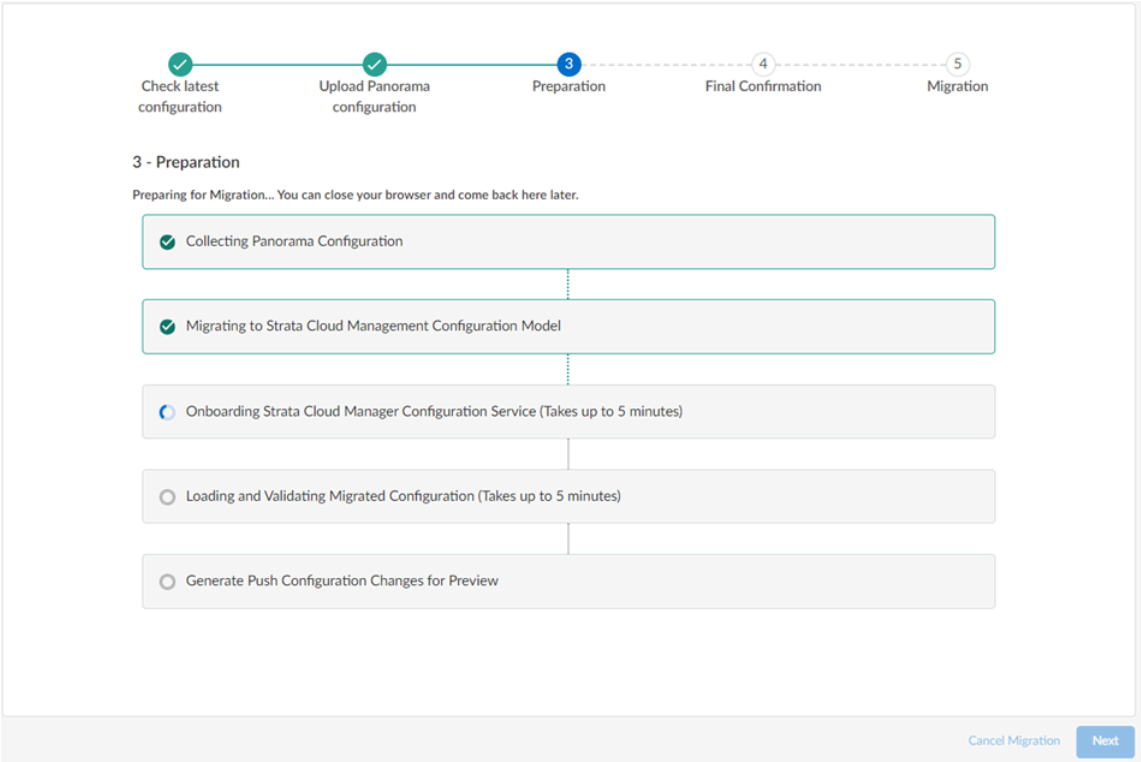
STEP 5 | Seleccione el archivo de configuración Panorama .xml que descargó en un paso anterior arrastrándolo y soltándolo o **Choose File (Seleccione el archivo)**.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Introduzca su **Master Key (Clave maestra)**, o si no creó una clave maestra personalizada, pida a Strata Cloud Manager usar la **predeterminada** y haga clic en **Next (Siguiente)**.



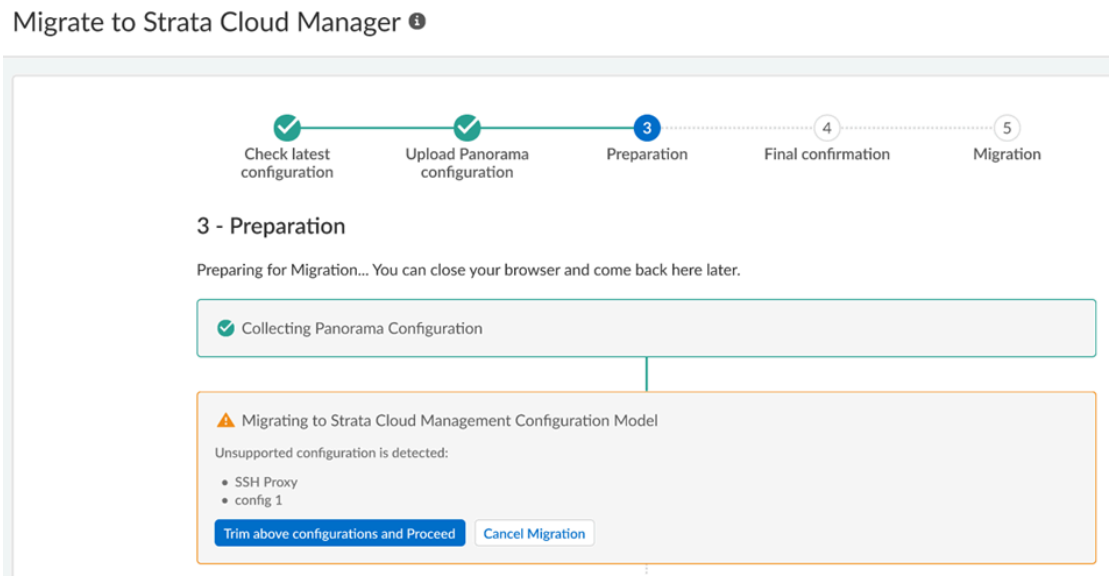
El programa de migración comienza.



 ©2025 Palo Alto Networks, Inc.

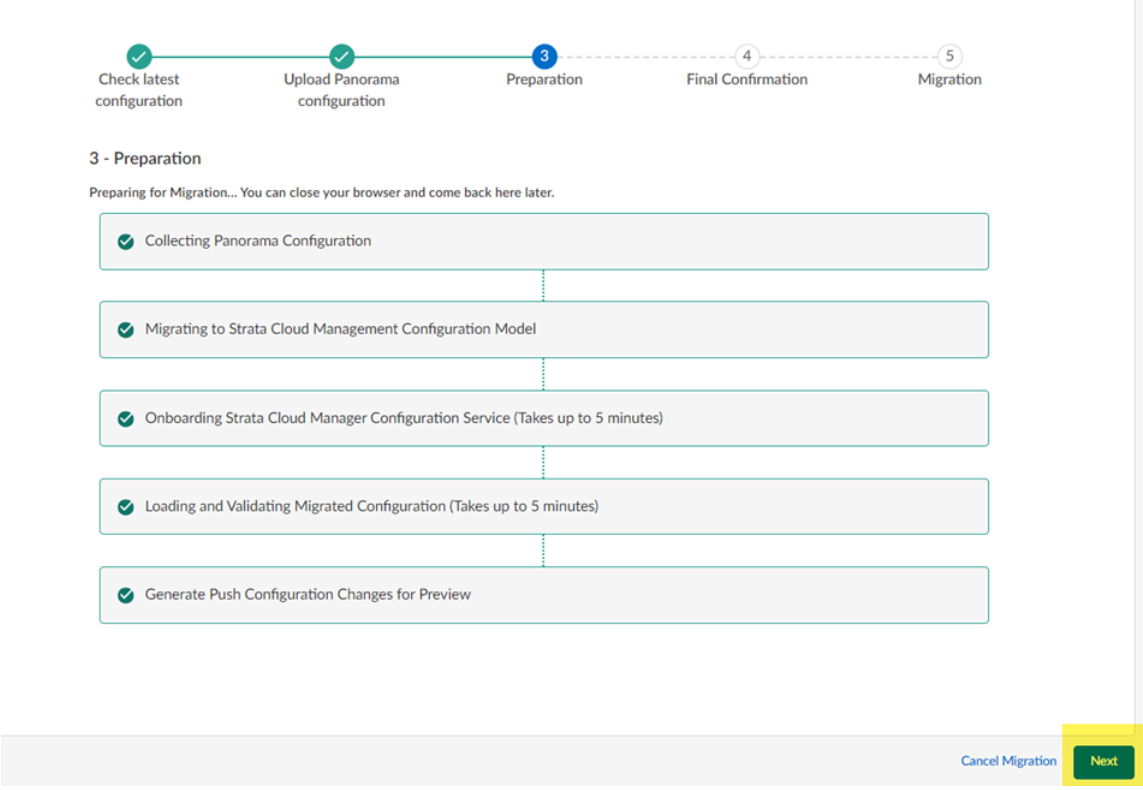
Espere a que se completen todos los pasos.

STEP 7 | Si, durante la migración, el programa indica que encontró una configuración no compatible, puede **recortar las configuraciones anteriores y continuar** o **cancelar la migración**.



Algunas configuraciones no compatibles (como una configuración de varios inquilinos) cancelan la migración y el programa de migración no puede resolver el problema; en este caso, opte por **Cancel Migration (Cancelar Migración)**.

STEP 8 | Después de que se complete la migración, haga clic en **Next (Siguiente)**.



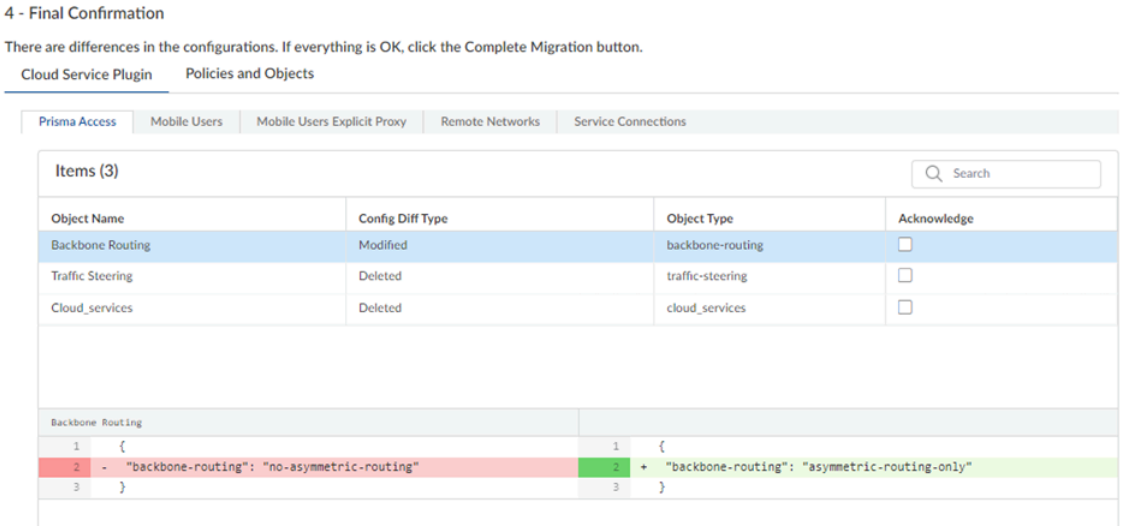
 ©2025 Palo Alto Networks, Inc.

STEP 9 | Si el programa de migración realizó cambios, revíselos en la pantalla de confirmación final.

El programa de migración podría hacer cambios en su configuración para tener en cuenta las diferencias en el Panorama y la configuración de Strata Cloud Manager o para corregir funcionalidades no soportadas. Si se requieren cambios, el programa de migración muestra esos cambios en una vista de diferencias con las nuevas líneas en verde y las líneas eliminadas en rojo.

Ignore cualquier diferencia que muestre los siguientes nombres de objeto; estos no afectan su configuración:

- *Clientless-vpn crypto-settings*
- *Renombrar perfiles hip*
- *Redundancia de usuario móvil*
- *Excluir tráfico de vídeo*



STEP 10 | (Opcional) Realizar cambios en las diferencias.

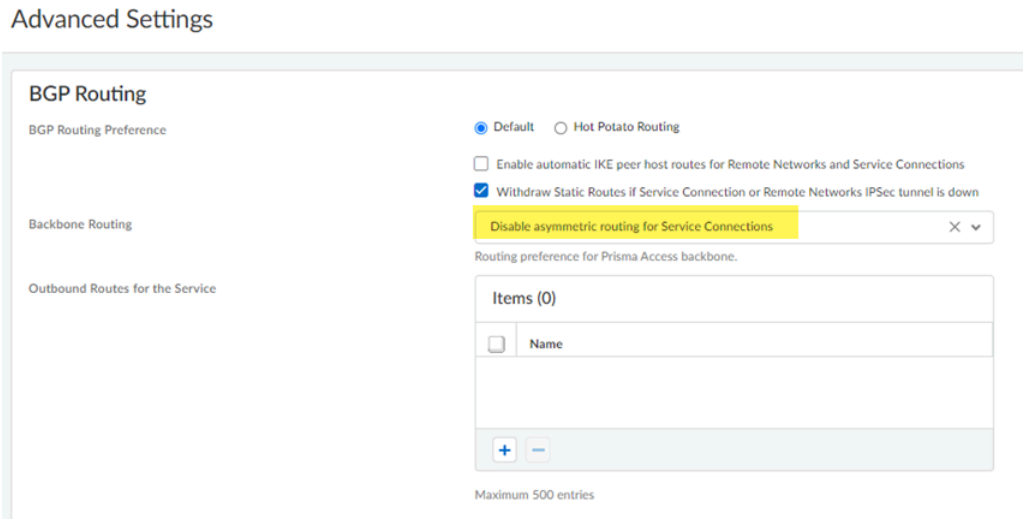
Cualquier cambio que realice no se guardará en su configuración hasta que complete la migración y envíe sus cambios a Strata Cloud Manager.

1. Navegue a la zona en la configuración de Prisma Access donde encontró las diferencias y haga cambios en la configuración.

   Para el ejemplo en el paso anterior, el programa de migración realizó un cambio en el enrutamiento de la red troncal (de **no-asymmetric-routing (no-enrutamiento-asimétrico)** a **asymmetric-routing-only (enrutamiento-asimétrico-sólo)**). Para cambiar esta configuración de vuelta a su configuración original, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)** > **Advanced Settings (Configuración avanzada)** > y cambie la configuración de **Backbone Routing (Enrutamiento de la red troncal)** a **Disable**

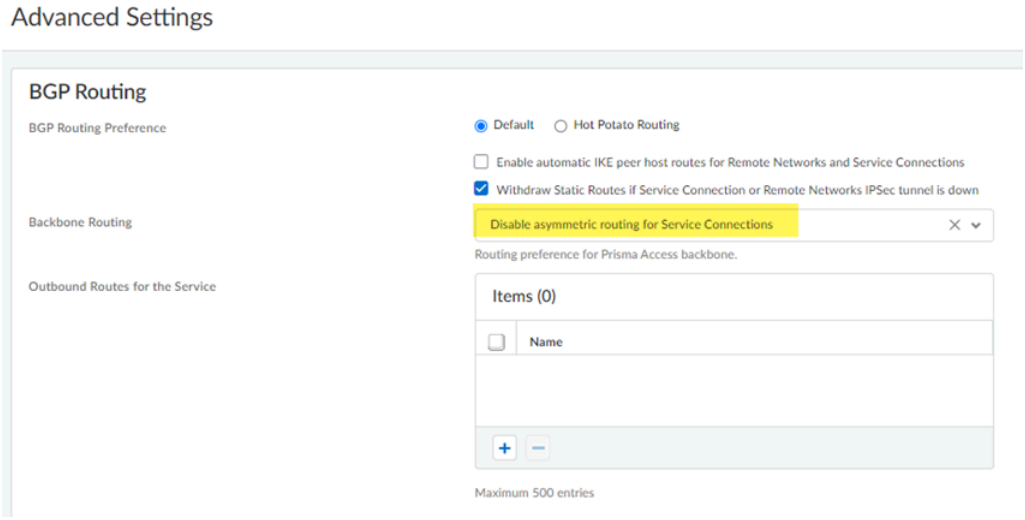
 ©2025 Palo Alto Networks, Inc.

Asymmetric Routing for Service Connections (Deshabilitar enrutamiento asimétrico para conexiones de servicio).



2. (Opcional) Para hacer un seguimiento de sus cambios, **reconózcalos** a medida que los complete.

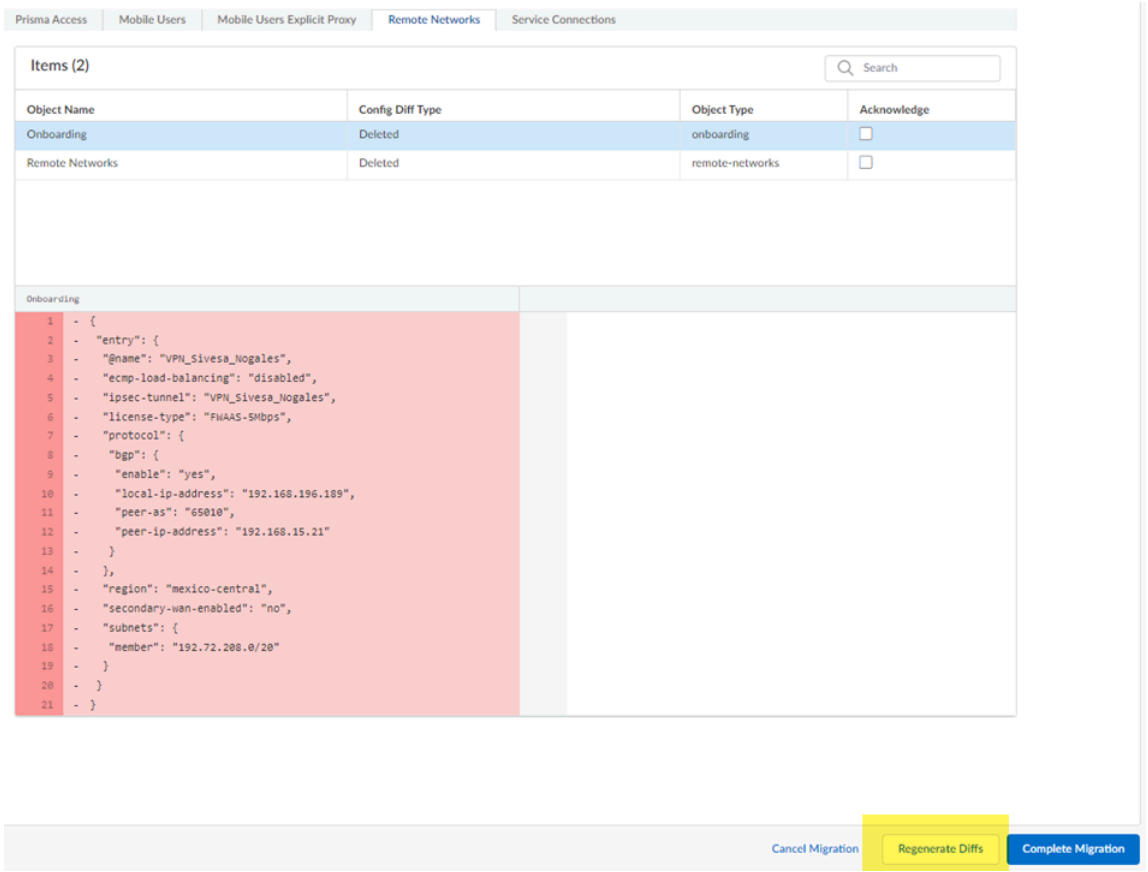
   Si bien no es obligatorio, puede ser útil reconocer cada cambio a medida que los realice, para que pueda hacer un seguimiento de ellos.



3. Continúe revisando los cambios, realice las modificaciones y confírmelos.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | (Opcional) Si ha realizado algún cambio en la configuración, deberá **Regenerate Diffs (Regenerar las diferencias)** para ver las diferencias actualizadas.

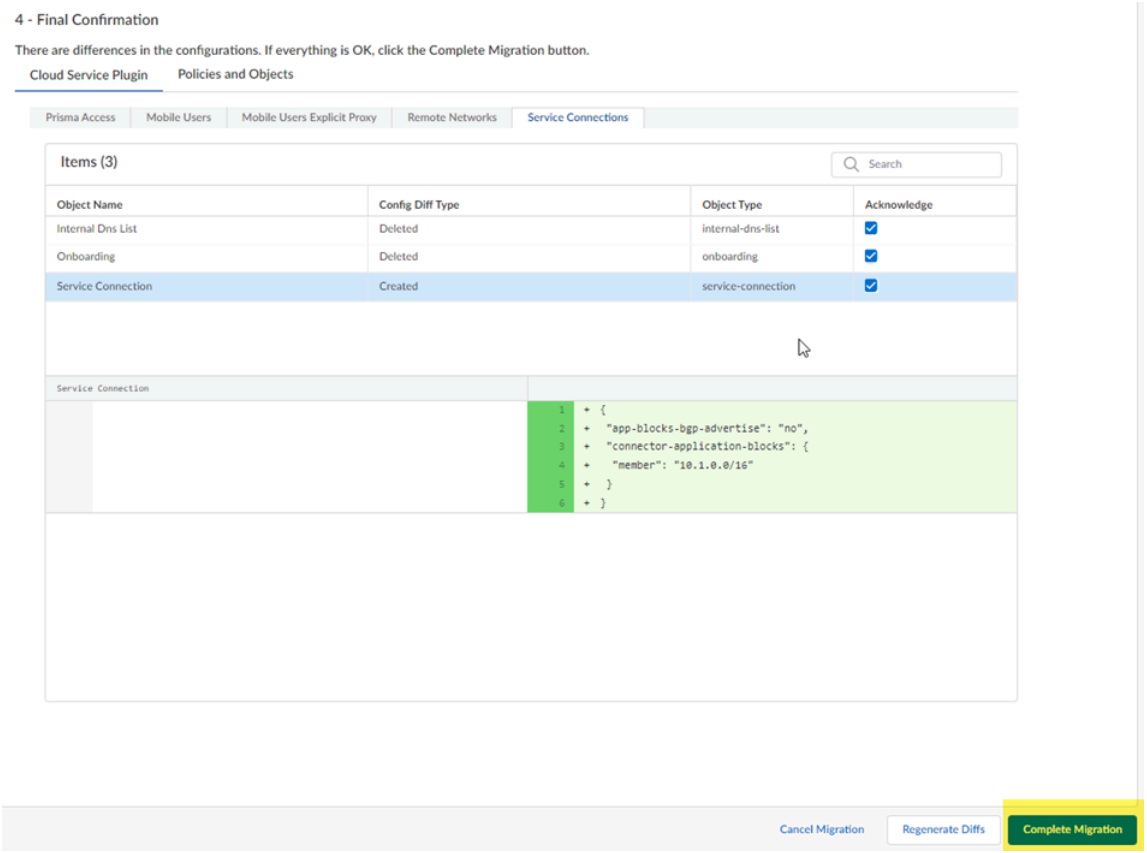


 ©2025 Palo Alto Networks, Inc.

STEP 12 | Completar migración:

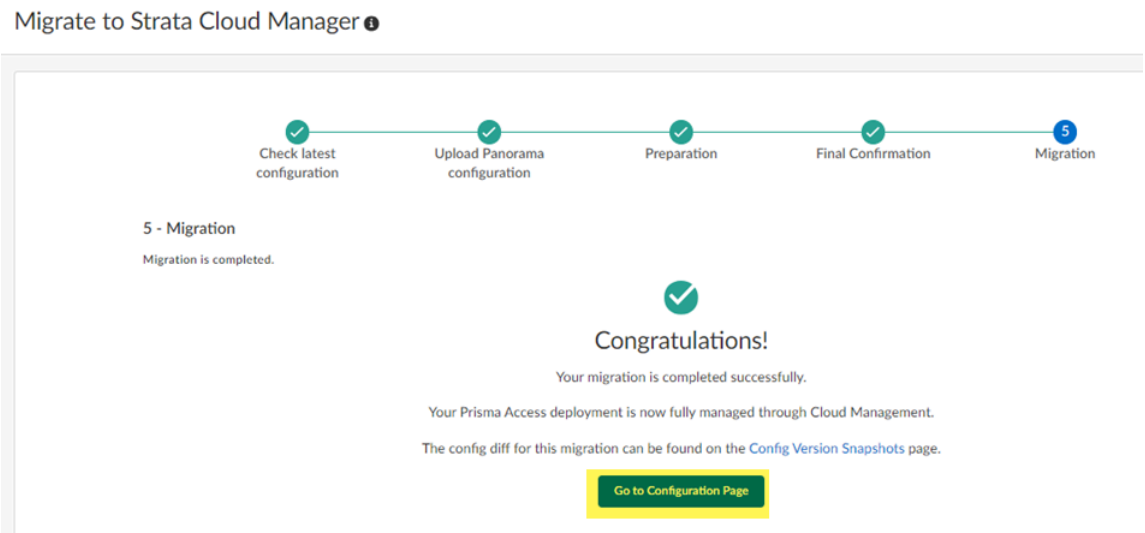
Si bien no es obligatorio, también puede **Acknowledge (Reconocer)** sus cambios.

Después de Complete Migration (Completar la migración), no puede volver a una implementación gestionada por Panorama y su implementación utiliza permanentemente Strata Cloud Manager para su gestión.

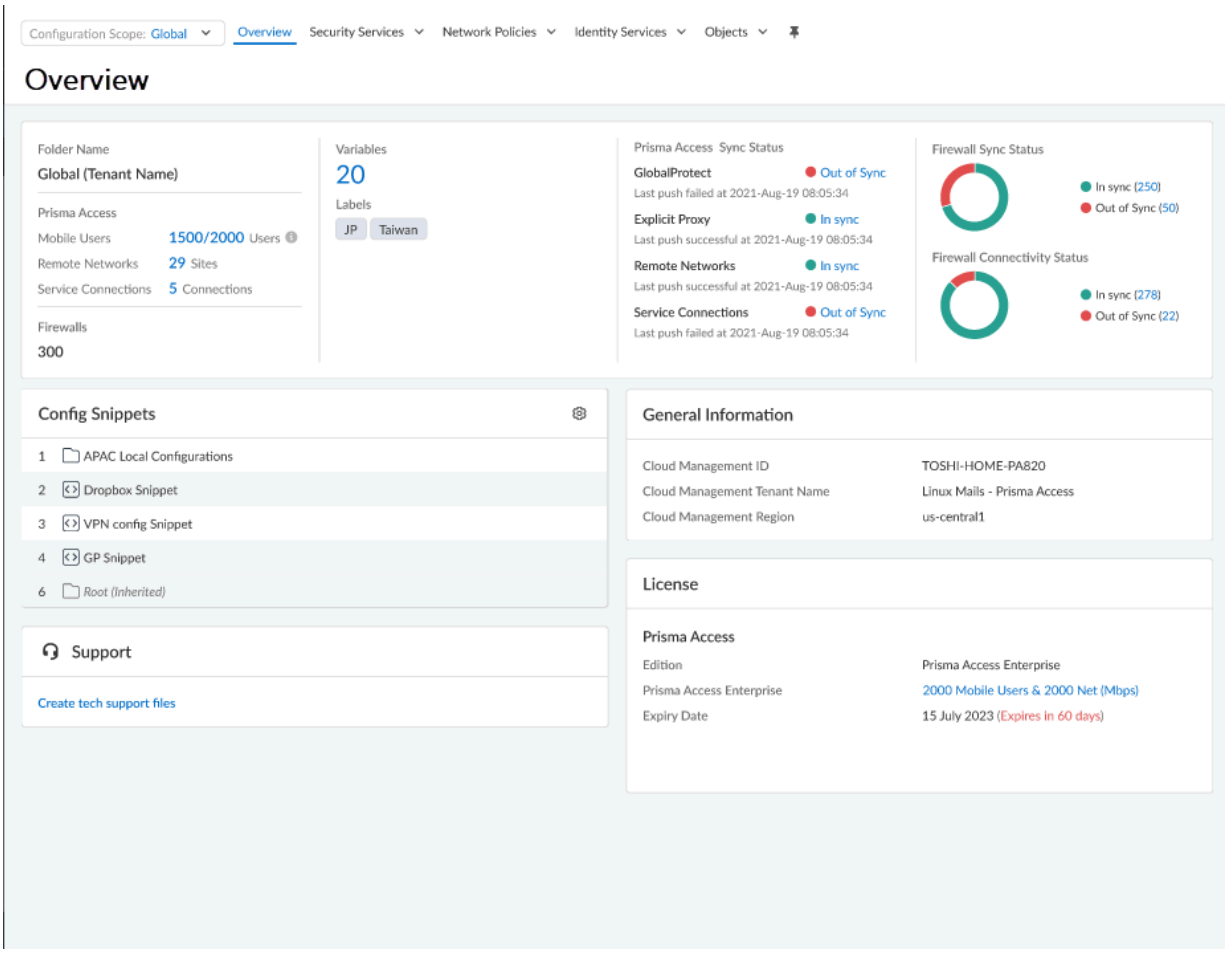


 ©2025 Palo Alto Networks, Inc.

STEP 13 | (Opcional) Seleccione **Go to Configuration Page (Ir a la página de configuración)** para ver su configuración migrada.



Su implementación migrada se muestra.



 ©2025 Palo Alto Networks, Inc.

STEP 14 | **Push Config (Enviar configuración)** > **Push (Enviar)** para aplicar los cambios de configuración migrados.

Esta operación de Envío garantiza que su migración se ha completado con éxito y que Prisma Access ha aplicado todos los cambios a su configuración migrada.

STEP 15 | Tome nota de cualquier mensaje que reciba durante la operación de Envío y, si ve algún problema, realice los cambios necesarios en su configuración.

 ©2025 Palo Alto Networks, Inc.

Publicaciones y actualizaciones de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Las versiones y actualizaciones de Prisma Access le permiten mantenerse al día y proteger a sus usuarios. Algunas de las actualizaciones son gestionadas por Palo Alto Networks, como actualizaciones de la infraestructura de Prisma Access y usted recibirá una notificación anticipada para que pueda planificar en torno a ellas. Otras actualizaciones son su responsabilidad y debe programar la versión especificada de la actualización de contenido, actualización de software y versión del complemento (según sea necesario), lo antes posible.

Puede recuperar el estado de todos los servicios en la nube, incluidos Prisma Access y Strata Logging Service, junto con un registro histórico del tiempo de actividad de cada servicio, accediendo al sitio web https://sase.status.paloaltonetworks.com/. *También puede inscribirse para recibir actualizaciones por correo electrónico o mensajes de texto en este sitio, para recibir notificaciones por adelantado cuando se planifiquen actualizaciones de infraestructura y notificaciones en tiempo real cuando se produzcan actualizaciones, y cuando Palo Alto Networks cree, actualice o resuelva un incidente.*

Tipos de versiones de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Prisma Access tiene actualizaciones, incluidos lanzamientos importantes y mantenimiento de infraestructura, que incluyen nuevas características y optimizaciones para brindar la mejor seguridad para sus redes remotas y usuarios móviles.

La siguiente lista define los tipos de lanzamiento, junto con la notificación anticipada que le proporcionamos para cada lanzamiento. Para asegurarse de recibir notificaciones de todos las publicaciones, regístrese para recibir notificaciones por correo electrónico o mensaje de texto sobre Prisma Access en el sitio web https://sase.status.paloaltonetworks.com/, y regístrese para recibir alertas en Strata Cloud Manager.

- **Versión principal**: una versión principal generalmente incluye nuevas características y optimizaciones importantes, y dichas actualizaciones se implementan dentro de una ventana de mantenimiento planificada establecida por Palo Alto Networks. Palo Alto Networks notifica a los clientes sobre dichas actividades de mantenimiento planificadas mediante notificaciones por correo electrónico a través de sase.status.paloaltonetworks.com.

  Notificación: Palo Alto Networks le proporciona las siguientes notificaciones sobre versiones importantes:

Tipo de implementación	Período de notificación
Implementaciones de producción	Palo Alto Networks le envía una notificación 21 días antes de un lanzamiento importante.
Implementaciones de laboratorio	Palo Alto Networks le envía una notificación 7 días antes de un lanzamiento importante.

Además de una actualización de versión importante programada, Palo Alto Networks podría necesitar realizar actualizaciones programadas urgentes, que siguen un cronograma diferente.

Los inquilinos de laboratorio no están cubiertos por el Acuerdo de Nivel de Servicio (SLA) de Prisma Access y se recomienda a los clientes que utilicen los inquilinos solo para fines de prueba y cualificación anterior a la producción.

©2025 Palo Alto Networks, Inc.

- **Mantenimiento de la infraestructura**: incluye funciones y optimizaciones incrementales. En algunos casos, Palo Alto Networks podría combinar una revisión con el mantenimiento de la infraestructura.

  Notificación: Palo Alto Networks le proporciona las siguientes notificaciones:

Tipo de implementación	Período de notificación
Implementaciones de producción	Palo Alto Networks le proporciona una notificación 10 días antes del mantenimiento de la infraestructura.
Implementaciones de laboratorio	Palo Alto Networks le proporciona una notificación 7 días antes del mantenimiento de la infraestructura.

  Además de una actualización de versión importante programada, Palo Alto Networks podría necesitar realizar actualizaciones programadas urgentes*, que siguen un cronograma diferente.*

- **Versión del complemento de Cloud Services (** **Implementaciones gestionadas de Panorama únicamente)** : si Prisma Access requiere un nuevo complemento, este está disponible para descargar a través del Portal de atención al cliente (CSP) de Palo Alto Networks y en Panorama en la fecha de disponibilidad general (GA) de la versión.

  Prisma Access podría obligar a todos los inquilinos a actualizar a una versión específica del complemento de Cloud Services para mantener la compatibilidad con versiones anteriores y las versiones de software compatibles. Dicha actividad de cumplimiento proporcionará un **aviso con 14 días de anticipación** (a través de la página sase.status.paloaltonetworks.com) para planificar la actualización del complemento. El servicio recomienda encarecidamente que actualice al complemento más reciente tan pronto como esté disponible para descargar.

Actualizaciones programadas urgentes

Ocasionalmente, Palo Alto Networks debe realizar actualizaciones urgentes del plano de datos o de la infraestructura, que incluyen revisiones o correcciones de errores de emergencia (por ejemplo, correcciones de amenazas de día cero o cambios de complementos). Palo Alto Networks hará todo lo posible para avisarle con 48 horas de antelación a una actualización programada urgente; sin embargo, en ocasiones, es posible que reciba un aviso para una actualización programada urgente en menos tiempo.

 ©2025 Palo Alto Networks, Inc.

Tipos de actualización de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Palo Alto Networks actualiza su infraestructura basada en la nube sin necesidad de intervención alguna por su parte. Algunas actualizaciones requieren que realice una acción, como instalar un nuevo complemento.

La siguiente lista incluye los diferentes tipos de actualizaciones de Prisma Access:

- **Actualización de infraestructura**: Palo Alto Networks actualiza la infraestructura de Prisma Access, también conocida como *Plano de control* de Prisma Access, que incluye el backend del servicio subyacente, la orquestación y la infraestructura de supervisión.

  Puede esperar recibir actualizaciones de infraestructura de 4 a 6 veces al año.
- **Actualización del plano de datos**: Palo Alto Networks actualiza el plano de datos de Prisma Access que permite la inspección del tráfico y la aplicación de políticas de seguridad en su red y el tráfico de usuarios.

  Utilice la aplicación para registrarse para recibir notificaciones de alerta por correo electrónico sobre actualizaciones del plano de datos e indicar sus preferencias de actualización.
- **Mantenimiento programado de Prisma Access**: Prisma Access reserva una ventana cada dos semanas para realizar mantenimiento relacionado con revisiones y correcciones de errores de emergencia en la infraestructura.
- (Solo implementaciones gestionadas por Panorama) **Actualización del complemento Cloud Services**: cuando haya una nueva versión de complemento disponible, su administrador de red deberá actualizar el complemento Cloud Services en el dispositivo Panorama que gestiona Prisma Access.
- (Implementaciones gestionadas por Panorama únicamente) **Actualización de la versión del software de Panorama**: es posible que se requiera una actualización de su software de Panorama para garantizar la compatibilidad continua con Prisma Access.

La siguiente tabla le muestra lo que se incluye con cada versión, incluida la ventana de mantenimiento que brindamos y cualquier impacto en su servicio de Prisma Access.

Tipo de actualización	Ventana de mantenimiento	Impacto
Actualización de la infraestructura	2-8 horas	No hay impacto en el tráfico de la red; sin embargo, no es posible realizar confirmaciones durante la ventana de mantenimiento.

©2025 Palo Alto Networks, Inc.

Tipo de actualización	Ventana de mantenimiento	Impacto
		Palo Alto Networks programa las actualizaciones en un horario local que interrumpa mínimamente las funciones comerciales.
Actualización del plano de datos	72 horas	Palo Alto Networks utiliza esta ventana para actualizar el plano de datos de todos los clientes. Puede realizar cambios de configuración y confirmaciones durante esta ventana. Nuestro objetivo es minimizar el impacto en el tráfico de la red, pero en algunos casos puede haber una breve interrupción. Consulte Actualizaciones del plano de datos dePrisma Access para obtener más información. Utilice la aplicación para registrarse para recibir notificaciones de alerta por correo electrónico sobre actualizaciones del plano de datos e indicar sus preferencias de actualización, incluido el período de tiempo preferido para su actualización.
Actualización del complemento Cloud Services (solo implementaciones gestionadas por Panorama)	Instala el complemento cuando esté disponible.	Prisma Access Es posible que sea necesario actualizar todos los inquilinos a una versión específica del complemento para mantener la compatibilidad con versiones anteriores y las versiones de software compatibles. Durante la actualización del complemento, no es posible realizar cambios de configuración ni confirmaciones en Panorama.

 ©2025 Palo Alto Networks, Inc.

Tipo de actualización	Ventana de mantenimiento	Impacto
Actualización de la versión del software Panorama (implementaciones gestionadas por Panorama únicamente)	Usted programa y realiza la actualización en el Panorama que gestiona Prisma Access.	Cuando Prisma Access actualiza su infraestructura y plano de datos después de un lanzamiento de versión importante, las actualizaciones pueden ser incompatibles con versiones anteriores de Panorama. Debido a la rápida publicación de Prisma Access y el complemento Cloud Services (Cloud Services), las fechas de compatibilidad del software (fin de soporte) para Panorama son más cortas que las fechas de fin de vida útil del software para las versiones de Panorama y se aplican a la compatibilidad de la versión de Panorama con Prisma Access únicamente. Para obtener más información, incluidas las fechas de finalización del soporte para Panorama cuando se utiliza con Prisma Access, consulte la Compatibilidad de versiones de Prisma Access y Panorama en la Matriz de compatibilidad de Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

Cadencia para actualizaciones de software y contenido para Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

- Strata Cloud Manager
- Panorama

Cadencia para actualizaciones de software y contenido para Prisma Access (Managed by Strata Cloud Manager)

En la tabla siguiente se describe cómo Prisma Access actualiza los componentes de su infraestructura, incluidas las actualizaciones de contenido y software. Esta tabla también indica si Prisma Access actualiza automáticamente el software. Si las actualizaciones no son automáticas, puede obtener información sobre cómo aplicar esas actualizaciones de infraestructura.

También puede comprobar el estado de todos los servicios en la nube desde el hub.

Componente	Calendario de actualización	Comentarios
Aplicación de GlobalProtect	• **Las principales versiones de la aplicación de GlobalProtect (por ejemplo, *x*.0 o 4.*x*):** Prisma Access actualiza la aplicación con la última versión principal de 7 a 10 días después de la disponibilidad general de la versión *x*.0.1 de dicha versión. Por ejemplo, dada una versión de aplicación 4.0, Prisma Access actualiza la aplicación entre 7 y 10 días después de la versión 4.0.1. • **Versiones secundarias de la aplicación GlobalProtect (por ejemplo, 4.1.*x*):**Prisma Access actualiza la aplicación con la versión secundaria más reciente entre 7 y 10 días después de la disponibilidad general de esa versión.	La nube controla la versión de la aplicación que está disponible para la actualización.
Actualizaciones de software	Palo Alto Networks® actualiza la infraestructura PAN-OS cuando una nueva	Regístrese para recibir actualizaciones de

 ©2025 Palo Alto Networks, Inc.

Componente	Calendario de actualización	Comentarios
PAN-OS en la Infraestructura de Prisma Access: programada	versión de Prisma Access se libera. Palo Alto Networks® le avisa con tres semanas de antelación antes de una actualización programada.	infraestructura por correo electrónico o notificaciones por mensaje de texto en el Hub.
Aplicaciones y actualizaciones de amenazas	Diariamente con un umbral de 24 horas. Palo Alto Networks® publica nuevos App-ID el tercer martes de cada mes. Planifique revisar e incorporar estos nuevos App-ID dentro del umbral de 24 horas. Use el nuevo filtro de App-ID para minimizar este posible impacto en el tráfico. La nueva característica de App-ID le permite ver nuevas aplicaciones en su red y muestra detalles sobre la actividad de la aplicación recién catalogada. La información que obtenga lo ayudará a tomar las decisiones correctas con respecto a cómo actualiza su política de seguridad para aplicar las App-ID con categoría nueva más recientes.	
Protección antivirus	Cada hora, 10 minutos después de la hora	Prisma Access siempre está actualizado con la última versión del antivirus.
WildFire	tiempo real	Prisma Access siempre está actualizado con la última versión de WildFire.
GlobalProtect Data File (Archivo de datos de GlobalProtect)	Cada hora	Prisma Access está siempre actualizado con la última versión de archivos de datos de GlobalProtect.
VPN sin cliente firmas de aplicaciones	Cada hora	Prisma Access siempre está actualizado con la última versión de la firma de la aplicación de VPN sin cliente.

©2025 Palo Alto Networks, Inc.

Cadencia para actualizaciones de software y contenido para Prisma Access (Managed by Panorama)

La siguiente tabla le informa de las actualizaciones de software y contenido para obtener las últimas aplicaciones y firmas de amenazas y aprovechar las capacidades de prevención de amenazas proporcionadas por Palo Alto Networks. Si la columna **Cloud Controlled? (¿Controlado por la nube?)** tiene un atributo de **No**, realice las acciones necesarias para actualizar el componente.

Componente	Calendario de actualización	¿Controlado en la Cloud? (Sí/No)	Comentarios

Actualizaciones al software de Panorama para compatibilidad con Prisma Access	Para las principales versiones de Prisma Access, es posible que necesite actualizar su versión Panorama para los siguientes casos de uso:
	• **Actualización requerida**: en ocasiones, deberá actualizar la versión de software en Panorama para mantener la compatibilidad con Prisma Access.
	  • **Ventana de mantenimiento**: su organización necesitará programar una ventana de mantenimiento para actualizar la versión de software de Panorama.
	  • **Impacto**: no puede usar la nueva versión del complemento hasta que actualice su
		No	Consulte Fechas de fin de compatibilidad (EoS) para la compatibilidad de versiones de software de Panorama con Prisma Access para saber cuándo una versión de Panorama deja de ser compatible con Prisma Access. Consulte la Versión de compatibilidad de Prisma Access y Panorama para las versiones de Panorama actualmente compatibles para usar con Prisma Access. Para actualizar Panorama a una nueva versión, consulte Instalar contenido y actualizaciones de software para Panorama.

 ©2025 Palo Alto Networks, Inc.

Componente	Calendario de actualización	¿Controlado en la Cloud? (Sí/No)	Comentarios
	versión de Panorama. • **Notificación**: Palo Alto Networks le proporcionará una notificación 100 días antes de la actualización de la versión principal programada. • **Actualización opcional**: en otros casos, es posible que deba actualizar la versión de software de Panorama para utilizar las nuevas características que admite Prisma Access en la versión principal. • **Ventana de mantenimiento**: su organización necesitará programar una ventana de mantenimiento para actualizar la versión de software de Panorama. • **Impacto**: no puede usar las nuevas funciones que admite Prisma Access hasta que actualice su Panorama.		

 ©2025 Palo Alto Networks, Inc.

Componente	Calendario de actualización	¿Controlado en la Cloud? (Sí/No)	Comentarios
	• **Notificación**: Palo Alto Networks le notificará de cualquier requisito de Panorama 21 días antes de una actualización programada de la versión principal como se define en Tipos de versiones de Prisma Access.		
Versión del complemento Cloud Services	Disponible después del lanzamiento del complemento.	No	Usted realiza las tareas para actualizar el complemento. Consulte Tipos de versiones de Prisma Access para obtener más detalles sobre cuándo Prisma Access actualiza su versión del complemento. Consulte Upgrade the Cloud Services Plugin (Actualizar el complemento Cloud Services) para actualizar el complemento en el dispositivo Panorama.
Aplicación de GlobalProtect	• **Principales lanzamientos de aplicaciones de GlobalProtect (por ejemplo, *x*.0 o 5.*x*):** Prisma Access actualiza el agente en el portal con	Sí	La nube controla las versiones de la aplicación que están disponibles para su actualización; sin embargo, puede elegir entre varias versiones alojadas

©2025 Palo Alto Networks, Inc.

Componente	Calendario de actualización	¿Controlado en la Cloud? (Sí/No)	Comentarios
	la última versión principal de 7 a 10 días después de la disponibilidad general de la versión x.0.1 de dicha versión. Por ejemplo, dada una versión 5.1 del agente, Prisma Access actualiza el agente en el portal 7 a 10 días después de la versión 5.1.1. • **Lanzamientos de aplicaciones de GlobalProtect secundarios (por ejemplo,, 5.1.*x*):** Prisma Access actualiza el agente en el portal con el mantenimiento de infraestructura más reciente de 7 a 10 días después de la disponibilidad general de esa versión.		diferentes de la aplicación y puede controlar cómo y cuándo implementar las actualizaciones de la aplicación GlobalProtect para los usuarios finales. Consulte Actualizaciones de la aplicación GlobalProtect para obtener más detalles. Si su implementación de Prisma Access requiere una revisión de la aplicación GlobalProtect, abra un Caso de soporte con la asistencia técnica de Palo Alto Networks para obtener asistencia.
Aplicaciones y actualizaciones de amenazas	Diariamente con un umbral de 24 horas. Palo Alto Networks publica nuevos App-IDs el tercer martes de cada mes. Planifique revisar e incorporar estos nuevos App-ID dentro del umbral de 24 horas. La nueva característica de App-	Sí	

©2025 Palo Alto Networks, Inc.

Componente	Calendario de actualización	¿Controlado en la Cloud? (Sí/No)	Comentarios
	ID le permite ver nuevas aplicaciones en su red y muestra detalles sobre la actividad de la aplicación recién catalogada. La información que obtenga lo ayudará a tomar las decisiones correctas con respecto a cómo actualiza su política de seguridad para aplicar las App-ID con categoría nueva más recientes.		
Protección antivirus	Cada hora, 10 minutos después de la hora	Sí	Prisma Access siempre está actualizado con la última versión del antivirus.
WildFire	En tiempo real	Sí	Prisma Access recupera firmas de WildFire para malware recién descubierto tan pronto como la nube pública de WildFire pueda generarlas.
GlobalProtect Data File (Archivo de datos de GlobalProtect)	Cada hora	Sí	Prisma Access está siempre actualizado con la última versión de archivos de datos de GlobalProtect.
Firmas de aplicaciones VPN sin cliente	Cada hora	Sí	Prisma Access siempre está actualizado con la última versión de la firma de la aplicación de VPN sin cliente.

©2025 Palo Alto Networks, Inc.

Actualizaciones del plano de datos dePrisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access (Managed by Strata Cloud Manager) realiza automáticamente actualizaciones del plano de datos, sin necesidad de intervención alguna por su parte.

Prisma AccessPrisma Access realiza actualizaciones del plano de datos para proporcionar nuevas características y capacidades de seguridad para ayudar a proteger a los usuarios finales, los activos y la transformación digital de su organización. Cuando una nueva versión de Prisma Access requiere una actualización del plano de datos, debe comprender cómo funciona el proceso de actualización y tener los requisitos previos necesarios antes de actualizar.

Puede esperar que su plano de datos se actualice una o dos veces al año. Algunas versiones pueden ofrecer una actualización de plano de datos opcional además de las actualizaciones de plano de datos requeridas para admitir características de Prisma Access que lo requieren.

- Descripción general de la actualización del plano de datos
- Ejemplo de actualización de plano de datos

Descripción general de la actualización del plano de datos

Prisma Access actualiza su plano de datos en dos fases en dos fechas de fin de semana y lo mantiene informado sobre la actualización mediante Strata Cloud Manager. A un alto nivel, durante el proceso de actualización se toman los siguientes pasos:

- Una notificación por correo electrónico de Strata Cloud Manager llega 21 días antes de la fecha de inicio programada de la actualización del plano de datos. Esta notificación por correo electrónico proporciona la fecha de inicio de la actualización del plano de datos para la fase 1.

  Es posible que vea una fecha completa en Strata Cloud Manager antes de la notificación de 21 días, pero esta fecha puede no ser definitiva hasta que reciba su notificación de 21 días.

- En el correo electrónico, se le solicita que seleccione y envíe la ubicación o ubicaciones para actualizar primero y el período de tiempo preferido para la actualización a través de Strata Cloud Manager.

  Puede cambiar y enviar las primeras ubicaciones para actualizar y programar la ventana de tiempo varias veces para un inquilino determinado. El último envío que se produjo siete días antes de la fecha de inicio programada será elegido por el servicio para la actualización. No se

©2025 Palo Alto Networks, Inc.

le pedirá que realice ningún cambio dentro de los 5 días posteriores a la fecha de inicio de la actualización.

Si realiza cambios, es posible que pasen hasta 30 minutos hasta que los cambios realizados se muestren en el Panel de actualizaciones en Insights. Se le notificará mediante una alerta por correo electrónico cuando el Prisma Access ha procesado y completado los cambios.

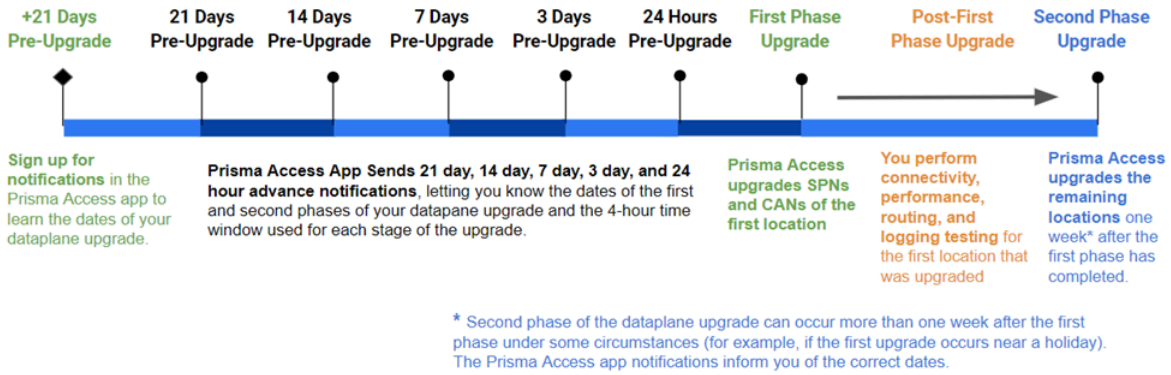
Palo Alto Networks recomienda encarecidamente que seleccione ubicaciones que reflejen toda su implementación. Por ejemplo, si tiene un usuario móvil, una conexión de servicio y una implementación de red remota, seleccione una ubicación o ubicaciones que tengan todos los tipos de implementación.

- Prisma Access realizará la fase n.° 1 de la actualización en la ubicación o ubicaciones seleccionadas dentro de la ventana de tiempo local seleccionada para esas ubicaciones.
- Si las ubicaciones de actualización seleccionadas tienen cualquier combinación de usuarios móviles (GlobalProtect), usuarios móviles (proxy explícito), conexiones de servicio o redes remotas, el plano de datos de cada implementación se actualizará a la versión del plano de datos requerida, como se describe más adelante en esta sección.
- Una vez que se complete la actualización en la primera ubicación, recibirá una notificación por correo electrónico a través de Strata Cloud Manager. Palo Alto Networks recomienda supervisar el servicio para detectar cualquier problema nuevo que se produzca inmediatamente después de la actualización del plano de datos.
- En el improbable caso de que vea un nuevo problema, informe del problema a la asistencia técnica de Palo Alto Networks.

  El equipo de asistencia técnica investigará el problema y tomará medidas correctivas que también pueden incluir la vuelta a la versión anterior del plano de datos. Esta decisión se le comunicará a través del caso de asistencia técnica.
- Si no hay nuevos problemas o un nuevo problema no está relacionado con la actualización, Prisma Access procederá con la actualización del plano de datos el siguiente fin de semana.
- La actualización de las ubicaciones restantes se llevará a cabo durante el mismo intervalo de tiempo que seleccionaste para la primera actualización (en hora local).
- Una vez completada la actualización del plano de datos, se le notificará mediante una alerta por correo electrónico.
- Si se requiere una actualización del complemento después de la actualización del plano de datos, Palo Alto Networks recomienda que actualice el complemento una vez que se complete la actualización del plano de datos.

La siguiente imagen muestra la línea de tiempo utilizada para la actualización e incluye las tareas que deberá realizar para la actualización del plano de datos (mostradas en verde), así como los pasos que Prisma Access realiza.

 ©2025 Palo Alto Networks, Inc.



La siguiente sección proporciona más detalles sobre el proceso de actualización del plano de datos.

Después de registrarse para recibir notificaciones, Prisma Access le informa las dos fechas de fin de semana que se utilizarán para el proceso de actualización y envía estas notificaciones 21 días, 14 días, 7 días, 3 días y 24 horas antes de que ocurra la primera fase de la actualización. El proceso de actualización se realiza en dos fases:

- La Fase n.° 1 actualiza la ubicación o las ubicaciones que usted eligió el primer fin de semana utilizando el período de tiempo que proporcionó y le notifica por correo electrónico cuando se completa la actualización. Si no seleccionó las ubicaciones para actualizar primero o no seleccionó un intervalo de tiempo, Prisma Access toma las decisiones por usted.

  Palo Alto Networks intenta actualizar las ubicaciones durante el período de cuatro horas que usted selecciona a través de Strata Cloud Manager. Sin embargo, completar las actualizaciones requeridas durante este período es la mejor opción y Palo Alto Networks no puede garantizar que las ubicaciones se actualizarán durante dicho tiempo. Si surge algún problema durante la actualización, Palo Alto Networks intentará realizar la actualización 24 horas después del plazo original de cuatro horas.

  Por este motivo, debe programar una ventana de solicitud de cambio durante 72 horas a partir de las 8:00 p. m., hora local, del viernes y hasta las 8:00 p. m., hora local, del lunes para cada uno de los dos fines de semana en los que se produce la actualización del plano de datos. Recibirá un correo electrónico cuando se complete la actualización.

  Prisma Access realiza los siguientes cambios en su implementación durante la Fase n.° 1 de la actualización.

Tipo de implementación	¿Qué es actualizado?
Usuarios móviles: Implementaciones de GlobalProtect	Actualizaciones de Prisma Access: • La puerta de enlace GlobalProtect, también conocida como *Nodo de procesamiento de seguridad de usuario móvil (MU-SPN)*, para la ubicación o las ubicaciones que especifique.

 ©2025 Palo Alto Networks, Inc.

Tipo de implementación	¿Qué es actualizado?
	• El portal GlobalProtect asociado con esa región.
Usuarios móviles: Implementaciones de proxy explícito	Prisma Access actualiza los nodos de proxy explícito para la ubicación o ubicaciones de proxy explícito que especifique.
Implementaciones de redes remotas	Prisma Access actualiza la red remota de respaldo (HA), también conocida como *Nodo de procesamiento de seguridad de red remota (RN-SPN)*, luego convierte la red remota de respaldo en el nodo activo para la ubicación o las ubicaciones que especifique. La conexión de red remota de respaldo no se actualiza hasta el siguiente fin de semana, cuando los nodos activos y de respaldo se actualizan para todas las ubicaciones. Si hay varios RN-SPN en la ubicación seleccionada, todos los nodos principales se actualizan a la nueva versión del plano de datos.
Conexiones de servicio	Prisma Access actualiza la conexión del servicio de respaldo (HA), también conocida como Nodo de acceso corporativo de conexión de servicio (SC-CAN), luego convierte la conexión del servicio de respaldo en el nodo activo para la ubicación o las ubicaciones que especifique. La conexión de servicio de respaldo no se actualiza hasta el siguiente fin de semana, cuando los nodos activos y de respaldo se actualizan para todas las ubicaciones. Si hay varios SC-CAN en la ubicación seleccionada, todos los nodos de respaldo se actualizan a la nueva versión del plano de datos.
Conectores ZTNA	Los ZTNA Connectors no se actualizan; puede actualizar los ZTNA Connectors según sea necesario.

Entre la primera y la segunda actualización, supervise las primeras ubicaciones actualizadas y realice pruebas de conectividad, rendimiento, enrutamiento y registro para asegurarse de que las ubicaciones se hayan actualizado correctamente. Si encuentra un fallo que afecte el servicio después de la actualización, abra un caso de asistencia técnica con la asistencia técnica

©2025 Palo Alto Networks, Inc.

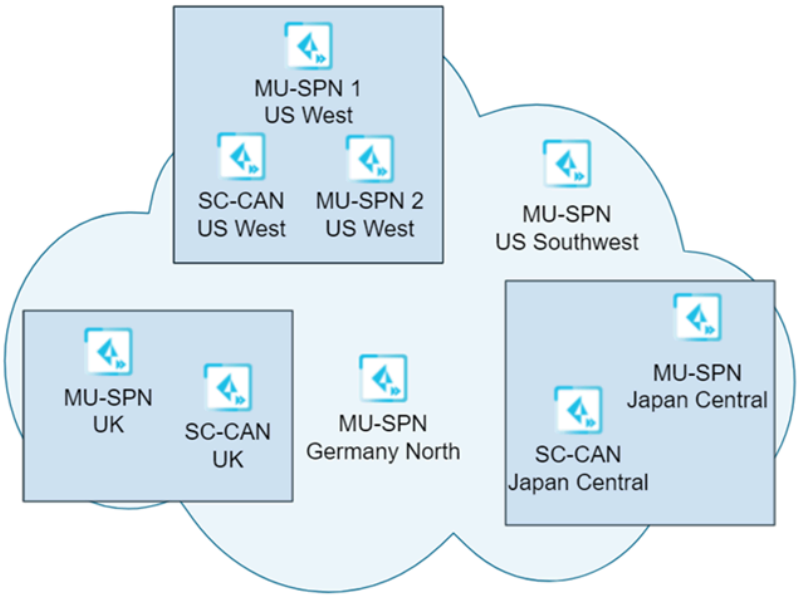
de Palo Alto Networks para obtener ayuda. Palo Alto Networks intentará resolver el problema revirtiendo el plano de datos a una versión anterior dentro de 24 horas.

- Siete días después de que Prisma Access mejora la primera ubicación, Prisma Access actualiza el resto de sus ubicaciones (actualización de fase n.° 2), utilizando el mismo intervalo de tiempo que seleccionó para la primera fase, y le notifica por correo electrónico cuando se completa la actualización.

> *La ventana de actualización puede ser más larga. Por ejemplo, si la Fase n.° 2 ocurre durante un festivo nacional en los Estados Unidos de América, la segunda fase de la actualización ocurre 14 días después de la primera fase en lugar de 7. Las notificaciones que recibe en Strata Cloud Manager le muestran el cronograma específico para la próxima actualización del plano de datos.*

Ejemplo de actualización de plano de datos

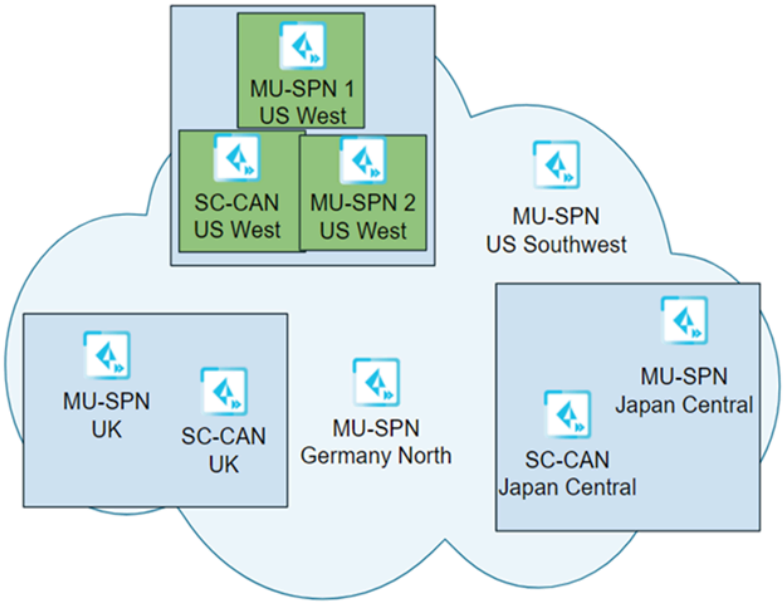
El siguiente ejemplo muestra un procedimiento de actualización del plano de datos para una implementación de usuarios móviles con cinco puertas de enlace (MU-SPN) y tres SC-CAN. La ubicación EE. UU. Oeste tiene dos MU-SPN como resultado de un evento de escalado automático (se agregó un MU-SPN adicional después de que una gran cantidad de usuarios móviles iniciaron sesión en esa ubicación).



En este ejemplo, seleccionó una sola ubicación (EE. UU. Oeste) para actualizar primero y solicitó un período de actualización de cuatro horas, de 8:00 a. m. a 12:00 del mediodía del sábado, para la actualización.

Durante el primer fin de semana de actualización (Fase n.° 1), la actualización de los SC-CAN y MU-SPN en la ubicación EE. UU. Oeste se lleva a cabo entre las 8:00 a. m. y las 12:00 p. m. Hora del Pacífico del sábado.

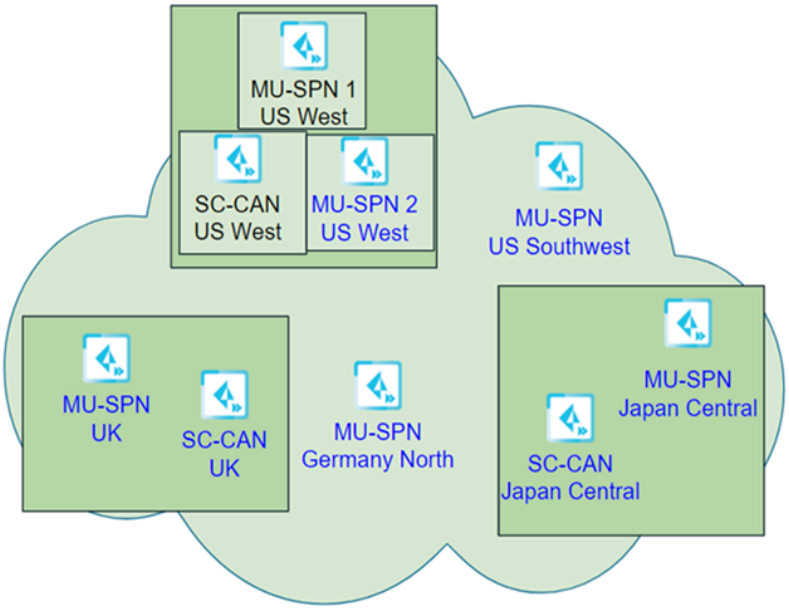
 ©2025 Palo Alto Networks, Inc.



Siete días después de actualizar la primera ubicación, Palo Alto Networks actualiza los componentes restantes (Fase n.° 2) utilizando el mismo período de cuatro horas que se utilizó para la primera fase de la actualización (de 8:00 a. m. a 12:00 p. m. del sábado).

En este ejemplo, Prisma Access utiliza la siguiente información de zona horaria al actualizar el plano de datos:

- El MU-SPN y SC-CAN de Japón Central se actualizan utilizando la hora local de Japón.
- Los MU-SPN y SC-CAN del Reino Unido se actualizan utilizando la hora local del Reino Unido.
- El MU-SPN de EE. UU. Suroeste se actualiza utilizando la hora del Pacífico.



 ©2025 Palo Alto Networks, Inc.

Reciba alertas de actualización y novedades

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Para mantenerse informado sobre el calendario de actualizaciones de su actualización de plano de datos y seleccionar sus preferencias de actualización, debe usar Strata Cloud Manager para suscribirse a notificaciones de Prisma Access. Strata Cloud Manager utiliza alertas por correo electrónico para informarle de las dos fechas de fin de semana en las que se realiza su actualización; usted selecciona la ubicación o ubicaciones que desea actualizar primero y la ventana de tiempo de cuatro horas que desea utilizar para la actualización.

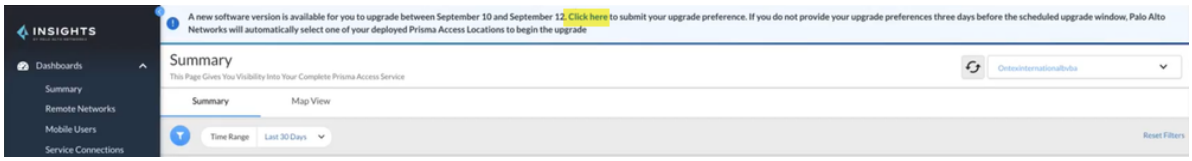
Después de que comience la actualización, también puede supervisar el estado de la actualización utilizando Strata Cloud Manager como se muestra en los siguientes pasos.

STEP 1 | Regístrese para recibir notificaciones de alerta de Strata Cloud Manager.

STEP 2 | Revise sus notificaciones para estar al tanto de las próximas actualizaciones del plano de datos; luego, seleccione sus preferencias de actualización utilizando uno de los siguientes métodos.

- Seleccione **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Prisma Access** > **Upgrade Preferences (Preferencias de actualización)**.

  El panel de actualización se muestra.

- Inicie sesión en Strata Cloud Manager, vea el banner en la parte superior de la página para su actualización programada y seleccione **Click here (Haga clic aquí)**.
- Revise su correo electrónico para notificaciones sobre su actualización programada y haga clic en el hipervínculo en el correo.
- Seleccione **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Prisma Access** > **Upgrade Preferences (Preferencias de actualización)**.

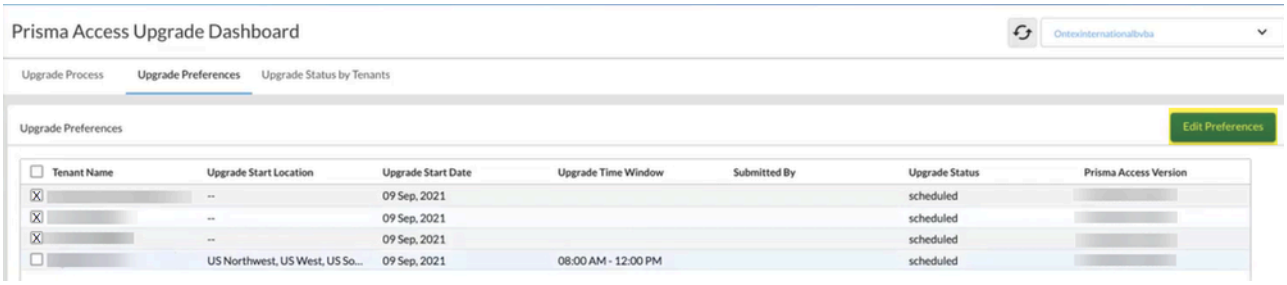
STEP 3 | (Opcional) Lee el **Upgrade Process (Proceso de actualización)** para aprender más sobre cómo funciona el proceso de actualización.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Seleccione sus **Preferencias de actualización**:

Si tiene una implementación multiinquilino, todos los inquilinos se muestran en esta área. Si ya ha seleccionado sus preferencias de actualización para su implementación, estas selecciones se muestran aquí.

1. Seleccione a los inquilinos para los que establecer preferencias de actualización, luego seleccione **Edit Preferences (Editar preferencias)**.



2. Selecciona las **ubicaciones de Prisma Access preferidas** que desea actualizar primero.

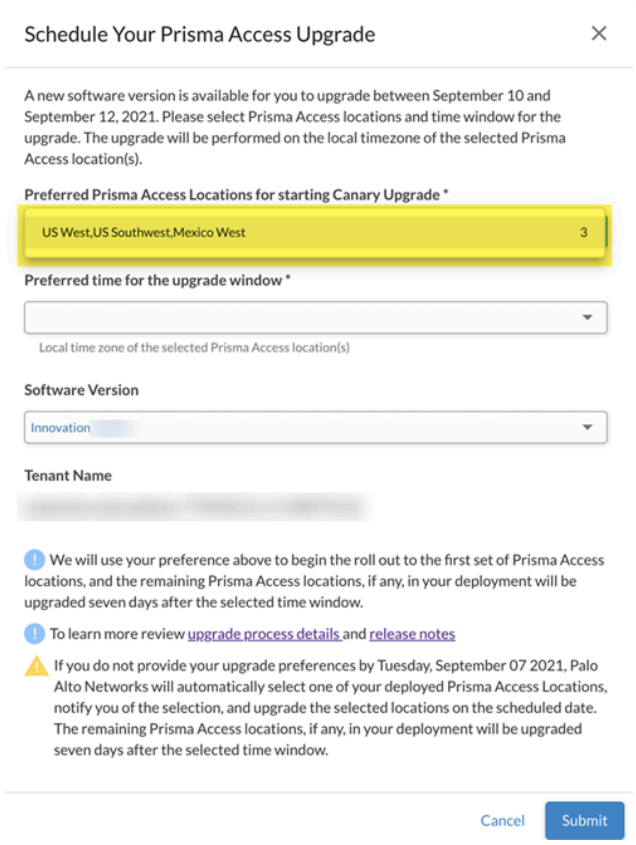
   Palo Alto Networks recomienda encarecidamente que seleccione ubicaciones que reflejen toda su implementación. Por ejemplo, si tiene un usuario móvil, una conexión de servicio y una implementación de red remota, seleccione una ubicación o ubicaciones que tengan todos los tipos de implementación.

   Seleccione de las opciones en la lista desplegable.

   - Prisma Accesssolo muestra las ubicaciones donde ha implementado usuarios móviles, redes remotas, conexiones de servicio o cualquier combinación de estos.
   - Los grupos en la lista desplegable pertenecen a la misma ubicación de cómputo.

   Prisma Access le informará a través de alertas por correo electrónico cuando las ubicaciones se hayan actualizado.

 ©2025 Palo Alto Networks, Inc.



Después de que el primer conjunto de ubicaciones de Prisma Access se actualice con éxito, el equipo de Prisma Access supervisa estas ubicaciones durante siete días y luego actualiza todas las ubicaciones de Prisma Access restantes. Seleccionar una única ubicación o un pequeño número de ubicaciones le da la oportunidad de supervisar estas ubicaciones antes de que el resto de sus ubicaciones se actualicen una semana después.

Si no se muestran ubicaciones en la lista desplegable, o bien seleccionó múltiples inquilinos que no tienen ubicaciones comunes implementadas o aún no has incorporado ninguna ubicación para los inquilinos que seleccionó.

3. Seleccione la **Preferred time for the upgrade window (Hora preferida para la ventana de actualización)** de la lista de opciones disponibles.

   Elige de entre las siguientes ventanas de tiempo de actualización. Las ventanas de tiempo son locales a la ubicación o ubicaciones que se están actualizando y son todas ventanas de cuatro horas:

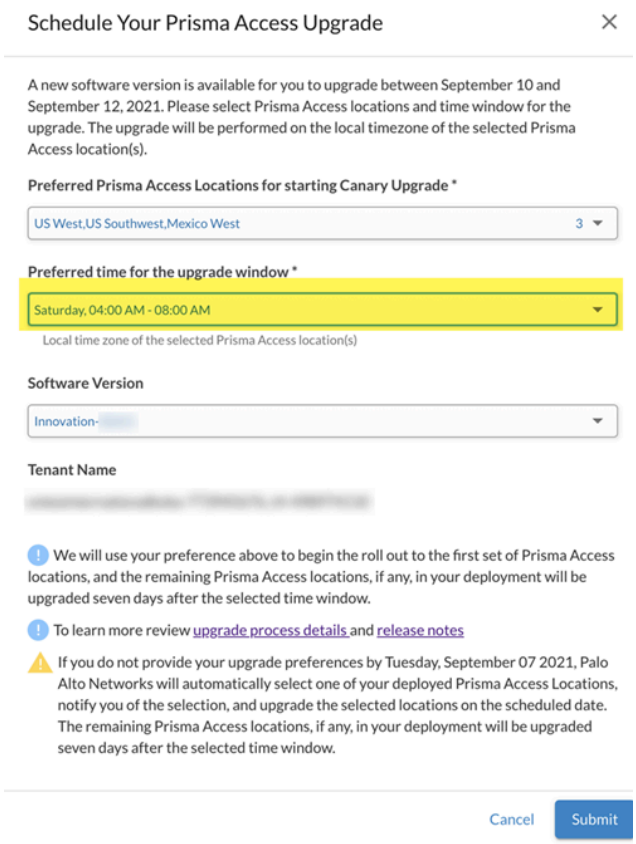
   - Viernes de 8:00 p.m. a 12:00 a.m. (medianoche)
   - Sábado de 12:00 a.m. (medianoche) a 4:00 a.m.
   - Sábado de 4:00 a.m. a 8:00 a.m.
   - Sábado de 8:00 a.m. a 12:00 p.m. (mediodía)
   - Sábado de 12:00 p.m. (mediodía) a 4:00 p.m.
   - Sábado de 4:00 p.m. a 8:00 p.m.

   Palo Alto Networks utiliza su preferencia para comenzar la implementación en la ubicación o ubicaciones de Prisma Access que seleccionó. La última presentación que

 ©2025 Palo Alto Networks, Inc.

se produjo siete días antes de la fecha de inicio programada será elegida por el servicio para la actualización. Si realiza cambios, es posible que pasen hasta 30 minutos hasta que los cambios realizados se muestren en el Panel de actualizaciones en Insights. Se le notificará mediante una alerta por correo electrónico cuando el Prisma Access ha procesado y completado los cambios.

Si no proporciona sus preferencias de actualización siete días antes de la ventana de actualización programada, Palo Alto Networks seleccionará automáticamente el primer conjunto de sus ubicaciones de Prisma Access implementadas, le notificará sobre la selección y actualizará las ubicaciones seleccionadas en la fecha programada. Las ubicaciones restantes de Prisma Access, si las hay, en su implementación se actualizarán siete días después de la ventana de tiempo seleccionada.



4. Seleccione la **versión del software** a la que desea actualizar, si hay más de una versión disponible.
5. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 5 | Después de que comience su implementación, seleccione **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > > **Prisma Access** > **Upgrade Status by**

 ©2025 Palo Alto Networks, Inc.

Tenants (Estado de actualización por parte de los inquilinos) y vea la **Upgrade Status by Location (Actualizar estado por ubicación)**.

Esta página muestra la siguiente información para cada ubicación que se está actualizando:

- El nombre del inquilino que se está actualizando.
- La fecha de inicio y finalización del proceso de actualización.
- La versión del plano de datos a la que se está actualizando el inquilino.
- Hora preferida para la ventana de actualización
- Las ubicaciones iniciales que se están actualizando.
- La fecha en que se actualizarán las ubicaciones restantes.

Además, una tabla muestra las ubicaciones que se están actualizando, la fecha de inicio y la ventana de tiempo de la actualización, y la zona horaria utilizada para la actualización. La columna **Upgrade Status (Estado de actualización)** te proporciona la siguiente información:

Estado de actualización	Descripción
Programado	La actualización del plano de datos se ha programado.
Comenzó	La actualización ha comenzado.
En curso	La actualización del plano de datos está en curso.
Reintentando	La actualización del plano de datos no se completó correctamente, pero Prisma Access sigue siendo operativa utilizando la versión anterior del plano de datos. Prisma Access volverá a intentar la actualización antes de que expire la ventana de mantenimiento del fin de semana.
Correcto	La actualización se completó correctamente.

STEP 6 | Después de que el primer conjunto de ubicaciones haya completado la actualización del plano de datos, supervise las ubicaciones actualizadas y realice pruebas de conectividad, rendimiento, enrutamiento y registro para asegurarse de que se hayan actualizado correctamente.

STEP 7 | Cuando se programe la actualización del segundo conjunto de ubicaciones, supervise esas ubicaciones y verifique su estado seleccionando **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Prisma Access** > **Upgrade Status by Tenants (Estado de actualización por parte de los inquilinos)**.

Prisma Access te envía una notificación por correo electrónico después de que se complete la actualización del plano de datos.

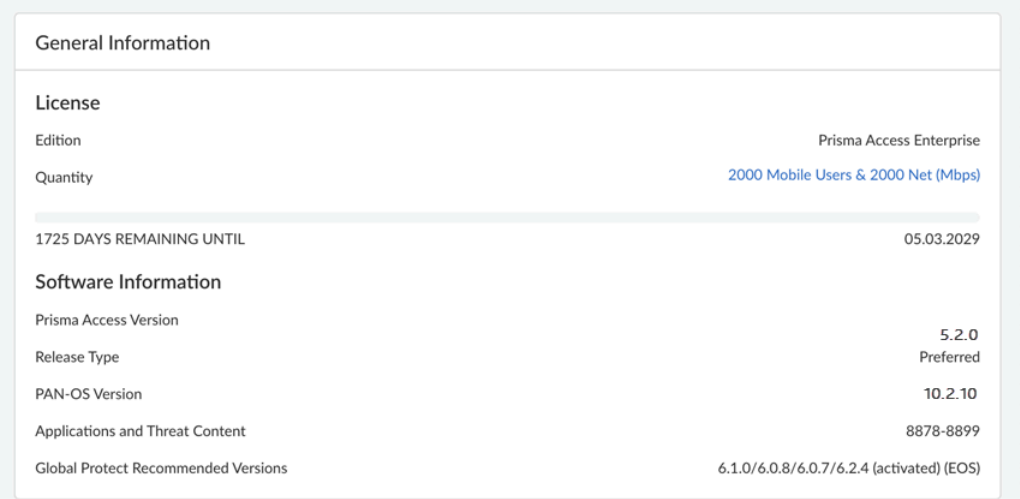
 ©2025 Palo Alto Networks, Inc.

Ver versiones de software de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Prisma Access (Managed by Strata Cloud Manager)

Puede encontrar información sobre la versión del software y del contenido en **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Descripción general)** > **General Information (Información general)**. Seleccione el ámbito de configuración de **Prisma Access**



La página de Información general le proporciona la siguiente información:

Área	Descripción
ID de inquilino	Permite compartir información de contacto (nombre de la empresa, nombre de contacto, correo electrónico y número de teléfono) para que puedan contactarle sobre las actualizaciones de servicio de Palo Alto Networks. El ID del inquilino.
Nombre de inquilino	El nombre del inquilino.
Región	La región del inquilino.

©2025 Palo Alto Networks, Inc.

Área	Descripción
Versión Prisma Access	La versión de Prisma Access actual
Versión de PAN-OS	La versión de PAN-OS que está ejecutando su plano de datos. El plano de datos es el componente de la infraestructura de Prisma Access que permite la inspección del tráfico y la aplicación de políticas en su red y el tráfico de los usuarios.
Tipo de versión	El tipo de lanzamiento que está ejecutando (ya sea Preferred o Innovation). Una versión de Innovation requiere un plano de datos PAN-OS más alto que una versión Preferred.
Contenido de aplicaciones y amenazas	La versión de actualizaciones de contenido de aplicaciones y amenazas que está ejecutando.

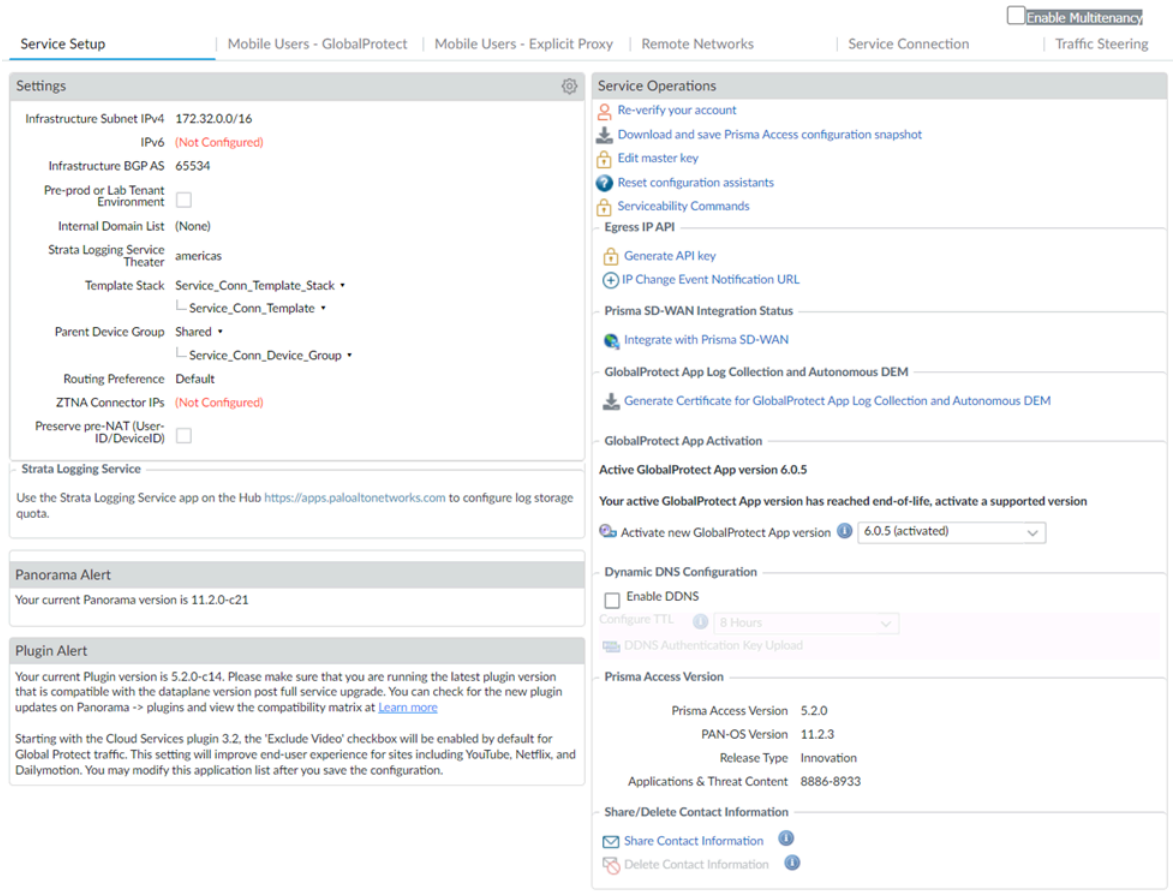
Prisma Access (Managed by Panorama)

Prisma Access consiste en componentes que gestiona, como Panorama y el complemento Cloud Services, componentes que Prisma Access gestiona, como la versión del plano de datos y componentes que Prisma Access gestiona pero cuya versión puede controlar (la versión de GlobalProtect alojada en el portal de Prisma Access). La página de configuración del servicio (**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicios)**) muestra el estado de estos componentes en una sola página. Esta página también contiene notificaciones que le muestran cuándo su versión actual de Panorama en ejecución y las versiones de los complementos llegarán al final del soporte (EoS) para su uso con Prisma Access. Palo Alto Networks le proporciona un aviso anticipado de las fechas de EoS para dar a su organización tiempo suficiente para planificar la actualización.

Todas las fechas están en Tiempo Universal Coordinado (UTC).

La página de configuración del servicio le proporciona la siguiente información:

 ©2025 Palo Alto Networks, Inc.



Área	Descripción
Alertas de Panorama	Muestra la versión actual de Panorama que está ejecutando. El área de **Upgrade requirements (Requisitos de actualización)** le proporciona información sobre las versiones de Panorama, incluidas las fechas en las que las versiones de Panorama actualmente compatibles alcanzan sus fechas de fin de soporte (EoS) para la gestión de Prisma Access. Utilice esta información para planificar su actualización de Panorama antes de su fecha de fin de soporte (EoS).
Alerta de complemento	Muestra el complemento Cloud Services que está instalado en el Panorama que gestiona Prisma Access. El área de **Upgrade requirements (Requisitos de actualización)** le proporciona fechas en las que se lanzará la próxima versión del complemento, la fecha límite para actualizar al siguiente complemento y la fecha en la que no podrá hacer cambios y confirmaciones utilizando

 ©2025 Palo Alto Networks, Inc.

Área	Descripción
	la versión anterior del complemento. Utilice esta información para planificar la próxima actualización del complemento Cloud Services.
Estado de integración de Prisma SD-WAN	Seleccione **Integrate with Prisma SD-WAN (Integrar con Prisma SD-WAN)** para activar el cliente ligero CloudBlade que permite la funcionalidad entre Prisma SD-WAN y Prisma Access.
Recopilación de logs de la aplicación GlobalProtect y Autonomous DEM	Si ha habilitado la Recopilación de logs de la aplicación GlobalProtect para la resolución de problemas, o para habilitar la Gestión de la experiencia digital autónoma (ADEM) para sus usuarios móviles, haga clic en **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Generar certificado para la recopilación de logs de la aplicación GlobalProtect y Autonomous DEM)** para generar un certificado. Este certificado permite a la aplicación de GlobalProtect autenticarse con Strata Logging Service (para recopilar logs) y Autonomous DEM. Cuando genere el certificado, Prisma Access también descarga el certificado en **Device Certificates (Certificados de dispositivos)** en Panorama **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivos)** en la plantilla **Mobile_User_Template** en el **Shared (Compartido)** que se va a enviar al dispositivo móvil.
Activación de la aplicación de GlobalProtect	Muestra la versión actualmente en ejecución (activa) de la aplicación de GlobalProtect que los usuarios móviles pueden descargar del portal Prisma Access, y le muestra las versiones disponibles de la aplicación GlobalProtect a las que puedes actualizar.
Configuración de DNS dinámico	Muestra si ha habilitado DNS Dinámico (DDNS) para la solución de problemas de red remota.
Versión Prisma Access	La versión de Prisma Access actual

©2025 Palo Alto Networks, Inc.

Área	Descripción
Versión de PAN-OS	La versión de PAN-OS que está ejecutando su plano de datos. El plano de datos es el componente de la infraestructura de Prisma Access que permite la inspección del tráfico y la aplicación de políticas en su red y el tráfico de los usuarios.
Tipo de versión	El tipo de lanzamiento que está ejecutando (ya sea Preferred o Innovation). Una versión de Innovation requiere un plano de datos PAN-OS más alto que una versión Preferred.
Contenido de aplicaciones y amenazas	La versión de actualizaciones de contenido de aplicaciones y amenazas que está ejecutando.
Compartir/eliminar información de contacto	Permite compartir información de contacto (nombre de la empresa, nombre de contacto, correo electrónico y número de teléfono) para que puedan contactarle sobre las actualizaciones de servicio de Palo Alto Networks. Si ha introducido anteriormente información de contacto, puede eliminar la información que introdujo en esta área. No utilice ninguno de los siguientes caracteres especiales en el área de información de contacto: • " (Comilla doble) • ' (Apóstrofe) • < (signo de menor que) • > (signo de mayor que) • Y comercial (&)

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Configuración de Prisma Access

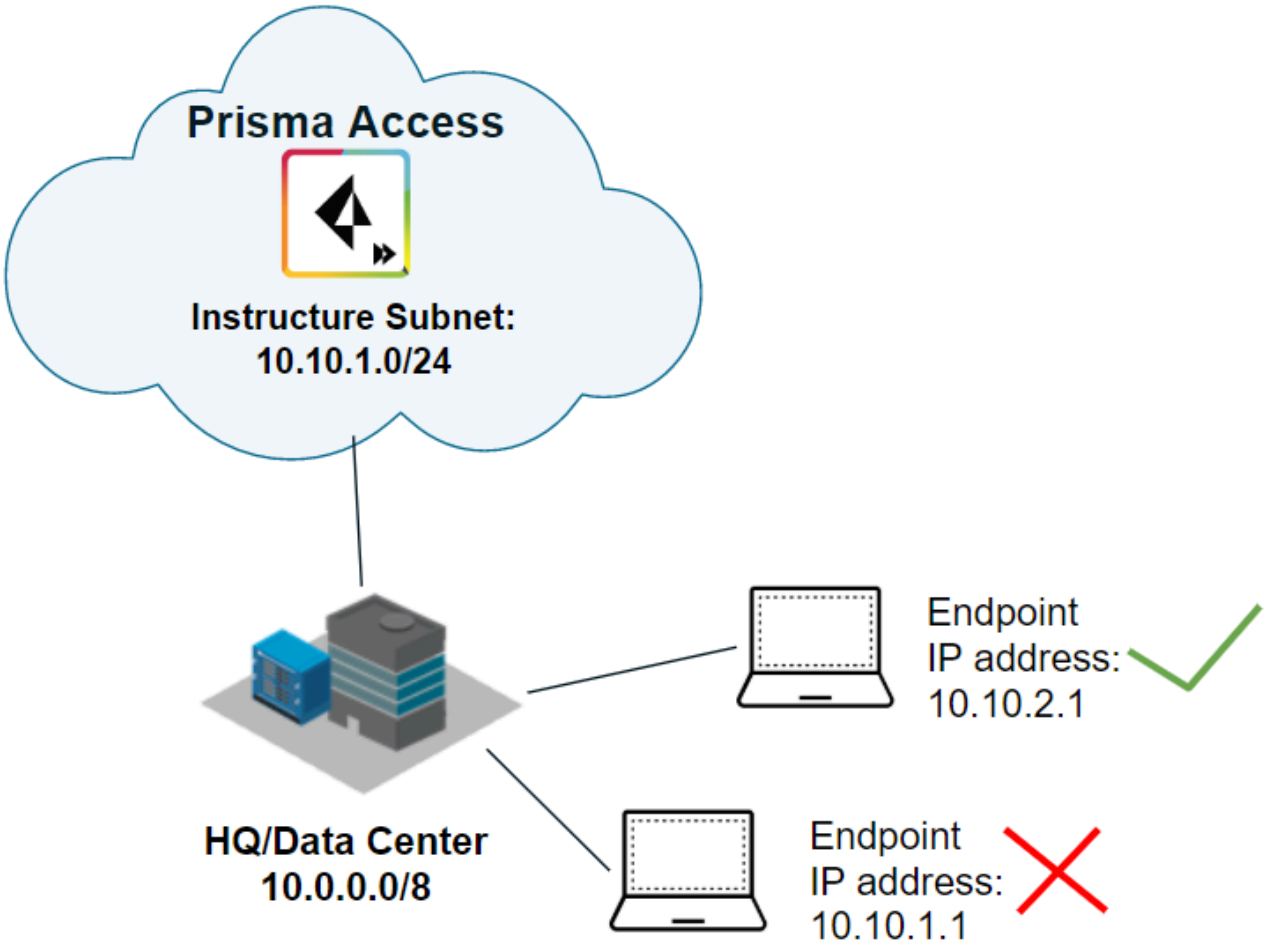
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Utilice las siguientes recomendaciones y requisitos cuando añada una subred de infraestructura:

- Puede asignar a Prisma Access una subred de infraestructura de una superred existente en el grupo de direcciones IP de su organización, pero no asigne ninguna de las direcciones IP de la subred de infraestructura para ningún otro uso en su red existente.

  En el ejemplo siguiente se muestra una subred de infraestructura de Prisma Access, 10.10.1.0/24, que asignó desde una superred existente, 10.0.0.0/8. Después de asignar 10.10.1.0/24 como subred de infraestructura, su organización no puede utilizar ninguna

dirección IP de esa subred. Por ejemplo, puede asignar 10.10.2.1 a un endpoint, pero 10.10.1.1 no se permite porque esa dirección IP es parte de la subred de infraestructura.



- Si crea una nueva subred para la subred de infraestructura, utilice una subred que no se solape con otras direcciones IP que utilice internamente.
- (Recomendado) Utilice una subred compatible con RFC 1918. Aunque se admite el uso de direcciones IP (públicas) no compatibles con RFC 1918, no lo recomendamos, debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.
- No especifique ninguna subred que se solape con las siguientes direcciones IP y subredes, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno.
  - 169.254.0.0/16
  - 100.64.0.0/10
- La subred no puede solaparse con los grupos de direcciones IP que planea utilizar para los grupos de direcciones que asigna para la implementación de usuarios móviles.
- Debido a que la infraestructura de servicios puede ser muy grande, debe designar una subred /24 como mínimo.

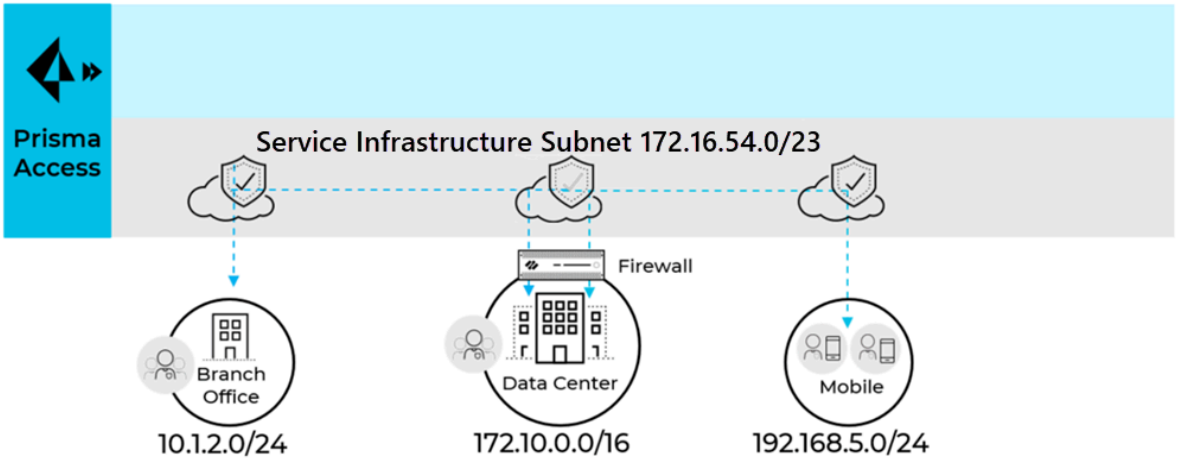
©2025 Palo Alto Networks, Inc.

Configurar Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Antes de poder usar Prisma Access para proteger las redes remotas y los usuarios móviles, configure una subred de infraestructura. Prisma Access utiliza direcciones IP dentro de esta subred para establecer una red entre las ubicaciones de red remotas, los usuarios móviles, la sede central y el centro de datos (si corresponde). Prisma Access También utiliza las conexiones de servicio para acceder a los recursos internos desde la sede central o la ubicación del centro de datos.

Esta subred será una extensión de su red existente. Por lo tanto, no debe superponerse con ninguna subred IP existente en su red. En el ejemplo siguiente se muestra una subred 172.16.54.0/23 que se utiliza para la subred de infraestructura de Prisma Access.



En el caso de redes pequeñas con menos de 50 sitios y 2500 usuarios móviles, considere una subred /24. Para redes de tamaño mediano con menos de 100 sitios y menos de 5000 usuarios móviles, considere una subred /23. En la mayoría de los casos, una subred /23 es suficiente. Si hay más de 100 sitios o 5000 usuarios móviles o se espera un crecimiento futuro, póngase en contacto con Palo Alto Networks para evaluar si necesita un tamaño de subred mayor.

Conozca cómo configurar Prisma Access.

- Strata Cloud Manager
- Panorama

Configurar Prisma Access (Strata Cloud Manager)

El siguiente flujo de trabajo le proporciona los pasos resumidos que debe seguir para instalar y configurar Prisma Access.

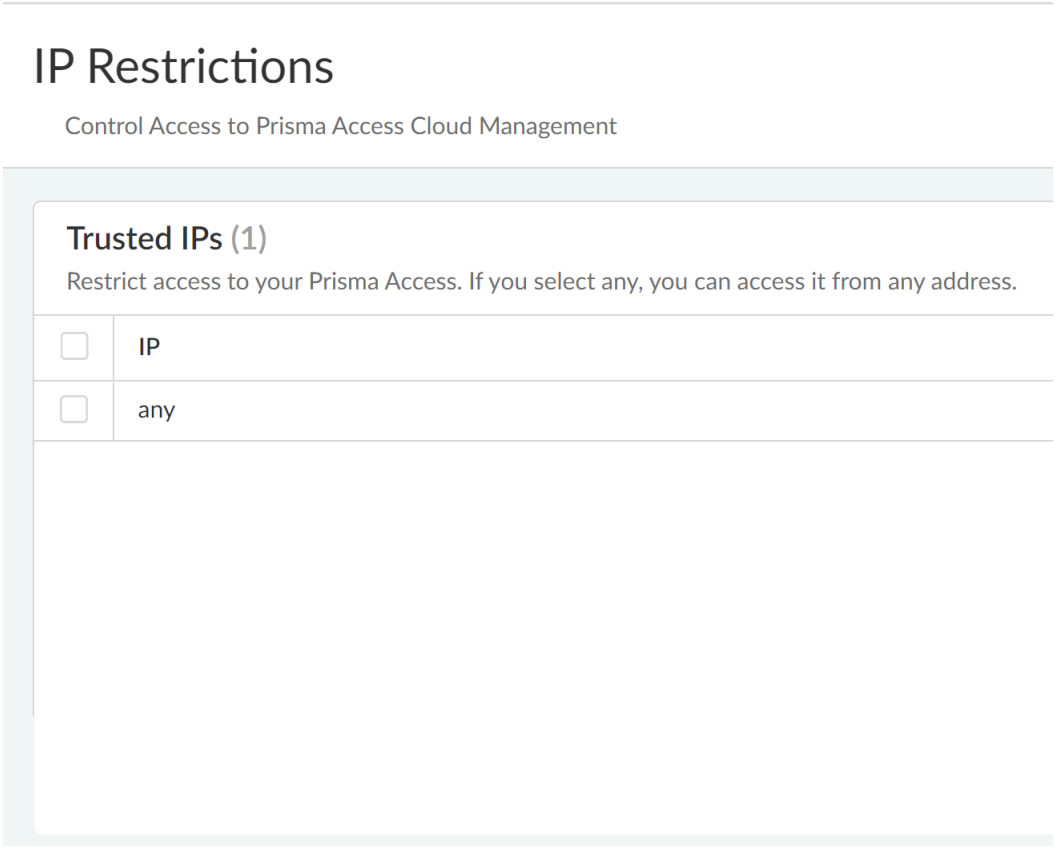
©2025 Palo Alto Networks, Inc.

STEP 1 | Inicie Strata Cloud Manager a través del hub.

1. Abra un navegador de Internet y seleccione **Sign In (Iniciar sesión)** en el hub.
2. Iniciar Strata Cloud Manager.

STEP 2 | Especifique direcciones IP fiables para administradores de Prisma Access (Managed by Strata Cloud Manager).

Solo los administradores que inician sesión desde estas direcciones IP de origen (y también que se autentican con éxito) pueden acceder a la gestión de la nube de Prisma Access (Managed by Strata Cloud Manager). Las direcciones IP deben ser direcciones públicas. De forma predeterminada, no se aplica ninguna dirección de confianza [la lista se establece en any (cualquiera)]. Para comenzar, busque el menú **Settings (Configuración)** en el panel de navegación izquierdo y haga clic en **IP Restrictions (Restricciones de IP)**.



STEP 3 | Identifique los requisitos de su licencia; luego Active e instale los componentes de Prisma Access.

STEP 4 | Habilite la infraestructura de servicio y las conexiones de servicio que permiten la comunicación entre los elementos de Prisma Access.

STEP 5 | Proteja a los usuarios móviles con GlobalProtect o Proxy explícito, según sea necesario para su implementación.

STEP 6 | Planificar, crear y configurar conexiones de red remotas.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | (Opcional) Cambie el método de autenticación de autenticación local al método de autenticación de su organización.

STEP 8 | (Opcional) Reenviar logs desde Strata Logging Service a un receptor Syslog externo.

STEP 9 | (Opcional) Verificar el estado de Prisma Access.

Puede recuperar el estado de todos los servicios en la nube, incluidos Prisma Access y Strata Logging Service, y un registro histórico del tiempo de actividad del servicio accediendo a la instancia de la aplicación desde el hub.

También puede registrarse para recibir notificaciones por correo electrónico o mensajes de texto para recibir notificaciones cuando se planifiquen actualizaciones de infraestructura, cuando se produzcan actualizaciones y cuando Palo Alto Networks® cree, actualice o resuelva un incidente. Para registrarse para recibir actualizaciones por correo electrónico, vaya a la sección Recursos de la página de inicio del hub y luego seleccione **Service Status (Estado del servicio)**. Luego puede **Subscribe (Suscribirse)** a actualizaciones e incidentes específicos para sus servicios en la nube.

Configurar Prisma Access (Panorama)

El siguiente flujo de trabajo proporciona los pasos resumidos que debe seguir para instalar y configurar Prisma Access (Managed by Panorama) Access.

Si está configurando una implementación que incluye varias instancias de Prisma Access en un solo Panorama (multitenencia), consulte . La mayoría de las organizaciones no tienen la necesidad de crear y gestionar varios inquilinos.

STEP 1 | Añada las siguientes direcciones URL y puertos a una lista de permitidos en cualquier dispositivo de seguridad que utilice con el dispositivo Panorama que gestiona Prisma Access.

Además, si su dispositivo Panorama utiliza un [**Panorama** > **Setup (Configuración)** > **Service (Servicio)** > **Proxy Server (Servidor proxy)**], o si utiliza un proxy de reenvío SSL con Prisma Access, asegúrese de añadir las siguientes direcciones URL y puertos a una lista de permitidos en el proxy o servidor proxy.

- api.gpcloudservice.com (para Prisma Access)
- api.paloaltonetworks.com (para Prisma Access)
- apitrusted.paloaltonetworks.com (para Prisma Access)
- Los FQDN y puertos necesarios para Strata Logging Service

*Si hay un cortafuegos de nueva generación de Palo Alto Networks entre el dispositivo Panorama e Internet, debe añadir una regla de política de seguridad en el cortafuegos para permitir que las App-ID **paloalto-logging-service** y **paloalto-shared-services** pasen desde el dispositivo Panorama a Internet. Estas aplicaciones permiten la comunicación segura por SSL con Prisma Access y con el Strata Logging Service que el dispositivo Panorama utiliza para consultar logs. Si el dispositivo Panorama está detrás de un cortafuegos de Capa 4 heredado, permita que los puertos 443 y 444 de salida desde Panorama permitan este tráfico desde Panorama. Tenga en cuenta que abrir puertos de Capa 4 en lugar de usar los App-ID de Palo Alto Networks es menos seguro y no se recomienda.*

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada los puertos utilizados por Panorama para permitir listas en su red.

STEP 3 | Identifique los requisitos de su licencia; luego Active e instale los componentes de Prisma Access.

STEP 4 | Importe su configuración de Panorama existente a Prisma Access o cree una nuevas plantillas y grupos de dispositivos para iniciar la configuración de Prisma Access.

Para enviar las configuraciones —como la política de seguridad, la política de autenticación, los perfiles de servidor, los perfiles de seguridad, los objetos de dirección y los grupos de aplicaciones— a Prisma Access, debe crear nuevas plantillas y grupos de dispositivos con los ajustes de configuración a los que desea enviar Prisma Accesso aprovechar los grupos de dispositivos y las plantillas existentes añadiéndolos a las pilas de plantillas y las jerarquías de grupos de dispositivos que Prisma Access crea cuando usted incorpora el servicio.

Prisma Access crea las siguientes plantillas y grupos de dispositivos, en función de lo que haya comprado (por ejemplo, si no compra una licencia de proxy explícito, no verá las plantillas y los grupos de dispositivos de proxy explícito):

- Plantillas:
  - **Explicit_Proxy_Template**
  - **Explicit_Proxy_Template_Stack**
  - **Mobile_User_Template**
  - **Mobile_User_Template_Stack**
  - **Remote_Network_Template**
  - **Remote_Network_Template_Stack**
  - **Service_Conn_Template**
  - **Service_Conn_Template_Stack**
- Grupos de dispositivos:
  - **Explicit_Proxy_Device_Group**
  - **Mobile_User_Device_Group**
  - **Remote_Network_Device_Group**
  - **Service_Conn_Device_Group**

La configuración se simplifica en Prisma Access porque no tiene que configurar ninguna de las opciones de infraestructura, como las interfaces y los protocolos de enrutamiento. Esta configuración se automatiza y se inserta desde Panorama en las plantillas y grupos de dispositivos que el servicio crea automáticamente. Puede configurar cualquier configuración de infraestructura que requiera el servicio, como la configuración necesaria para crear túneles VPN IPSec a los dispositivos compatibles con IPSec en sus ubicaciones de red remotas,

 ©2025 Palo Alto Networks, Inc.

directamente desde el complemento. Opcionalmente, puede añadir plantillas y jerarquías de grupos de dispositivos a la configuración para simplificar la configuración del servicio.

Para simplificar la configuración del servicio, cree o importe las plantillas y grupos de dispositivos que necesita antes de comenzar las tareas de configuración para usar Prisma Access.

Al crear plantillas y grupos de dispositivos para Prisma Access, no es necesario asignarle dispositivos gestionados. En su lugar, los añadirá a las pilas de plantillas y a las jerarquías de grupos de dispositivos que Prisma Access crea. No añada ninguna de las plantillas o grupos de dispositivos creados por Prisma Access a cualquier otra pila de plantillas o grupos de dispositivos.

STEP 5 | Regístrese para recibir notificaciones por correo electrónico usando Strata Cloud Manager.

Prisma Access le proporciona notificaciones sobre el servicio, incluidas las actualizaciones del plano de datos, mediante notificaciones de esta aplicación.

STEP 6 | Cambie la clave maestra predeterminada para Panorama y en el complemento Cloud Services.

Palo Alto Networks recomienda cambiar la clave maestra en Panorama y en el complemento Cloud Services como una práctica recomendada de seguridad y que se cambie la clave maestra mensualmente.

Dado que las claves maestras de Panorama y Prisma Access no se sincronizan, Palo Alto Networks recomienda que no gire automáticamente la llave maestra en Panorama sin sincronizar también la llave maestra en Prisma Access. Puede utilizar los comandos de la interfaz de usuario o de la API de Panorama para cambiar las claves maestras.

Asegúrese de realizar un seguimiento de la clave maestra que implemente, ya que las claves maestras no se pueden recuperar. Cuando una clave maestra caduca, debe introducir la clave maestra actual para configurar una nueva. Debe restablecer el dispositivo Panorama a los valores predeterminados de fábrica si no puede proporcionar la clave maestra actual cuando caduque.

1. Cambiar la clave maestra en Panorama.
   1. Seleccione **Panorama** > **Master Key and Diagnostics (Clave maestra y diagnóstico)**.

      No especifique una **Current Master Key (Clave maestra actual)**.
   2. Configure el valor oportuno en **New Master Key (Nueva clave maestra)** y en **Confirm Master Key (Confirmar clave maestra)**.

      Anote la clave maestra que ha configurado.
   3. Configure los valores oportunos para la clave maestra en Lifetime (Duración) y en Time for Reminder (Recordatorio).
   4. Haga clic en **OK (Aceptar)**.
2. Cambie la clave maestra para Prisma Access seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Operations**

 ©2025 Palo Alto Networks, Inc.

(Operaciones de servicio) > **Edit master key (Editar clave maestra)** y, a continuación, introduzca la misma clave maestra que introdujo para Panorama.

También puede cambiar la clave maestra mediante comandos de API. Esto requiere dos pasos: uno para cambiar la clave maestra de Panorama y otro para cambiar la clave maestra de Prisma Access. Utilice los siguientes comandos de API para cambiar la clave maestra:

- Panorama: **XML API** > **Operational Commands (Comandos de operación)** > **request (solicitar)** > **master-key (llave maestra)**
- Prisma Access: **XML API** > **Operational Commands (Comandos de operación** > **request (pedir)** > **plugins (complementos)** > **cloud_services** > **prisma-access** > **sync (sincronizar)**

STEP 7 | Habilite la infraestructura de servicio y las conexiones de servicio que permiten la comunicación entre los elementos de Prisma Access.

1. Planifique habilitar la infraestructura de servicios y conexiones de servicios.
2. Habilite la infraestructura de servicio.
3. Cree una conexión de servicio para permitir el acceso a sus recursos corporativos.

   Si no necesita acceso a sus recursos corporativos, aún deberá crear una conexión de servicio para permitir el acceso entre usuarios móviles y redes remotas.

STEP 8 | Implementaciones de usuarios móviles de Prisma Access y usuarios móviles seguros con GlobalProtect o Proxy explícito, según sea necesario para la implementación.

Para configurar GlobalProtect en Prisma Access (Managed by Panorama):

1. Configure zonas para usuarios móviles mediante la creación de dos zonas en la plantilla Mobile_User_Template (por ejemplo, Usuarios móviles e Internet) y asignación de las zonas. Debe asignar cualquier zona que no sean usuarios conectados o oficinas centrales o sucursales de Prisma Access a No confianza.

   En **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)**, asigne Internet a No confianza; Usuarios móviles a Confianza.
2. Configurar autenticación

   Recomendamos utilizar la autenticación local como primer paso para verificar que el servicio esté configurado y que sus usuarios tengan acceso a internet. Más adelante, puede cambiar al uso de sus métodos de autenticación corporativos.
3. Configure las políticas de seguridad para el grupo de dispositivos.

   Para crear una política de seguridad que permita el tráfico a Internet, seleccione la Mobile_User_Device_Group **Policies (Políticas)** > **Security (Seguridad)** > **Prerules (Reglas previas)** > **Add (Añadir)** una regla. Por ejemplo: Usuarios móviles a Internet.
4. Confirme y envíe sus cambios para comenzar a utilizar el servicio.
5. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Mobile Users (Usuarios móviles)** para ver el **Status (Estado)** y compruebe que puede hacer ping al FQDN del portal.
6. Valide que Prisma Access está protegiendo el tráfico de Internet para los usuarios móviles mediante la descarga e instalación de la aplicación GlobalProtect, utilizando la aplicación

 ©2025 Palo Alto Networks, Inc.

para conectarse al portal como usuario móvil (usuario local), navegando por algunos sitios web en Internet y comprobando los registros de tráfico en Panorama.

Para proteger a los usuarios móviles con un proxy explícito:

1. Lea la Directrices de la configuración de proxy explícito.
2. Configurar la autenticación SAML. La autenticación SAML es necesaria para el Proxy explícito.
3. Configure la asignación de grupos mediante Cloud Identity Engine.
4. Complete la configuración del proxy explícito.
5. Confirmar y enviar sus cambios.

STEP 9 | Planificar, crear y configurar conexiones de red remotas.

1. Añadir una o más redes remotas a Prisma Access.

   Puede incorporar una ubicación y luego añadir ubicaciones adicionales utilizando la capacidad de importación masiva.
2. Cree una regla de política de seguridad para permitir el tráfico desde las redes remotas a la sede central (por ejemplo: Confianza a confianza).
3. Valide la conectividad entre la conexión de servicio, la conexión de red remota y los usuarios móviles.

STEP 10 | Ejecute el script de API utilizado para recuperar las direcciones IP de Prisma Access y Use el script heredado para recuperar direcciones IP de usuarios móviles.

Agregue estas direcciones a una lista de permitidos en la red de su organización para limitar el acceso entrante a su red empresarial y a sus aplicaciones.

STEP 11 | (Opcional) Cambie el método de autenticación de autenticación local al método de autenticación de su organización.

1. Cree un perfil de autenticación que cumpla los requisitos de su organización (SAML, LDAP, RADIUS, etc).
2. Si su organización usa un servidor de autenticación local, como RADIUS o Active Directory, añada las direcciones IP que Prisma Access utiliza como dirección IP de origen para las solicitudes internas (Recuperar las direcciones IP para Prisma Access) para permitir listas de permitidos en su red, o permitir las direcciones IP de toda la subred de infraestructura (Prisma Access toma la dirección IP de bucle invertido de esta subred).
3. Actualice el perfil de autenticación para el portal y puerta de enlace de Prisma Access para utilizar este nuevo perfil de autenticación.

STEP 12 | (Opcional) Reenviar logs desde Strata Logging Service a un receptor Syslog externo.

 ©2025 Palo Alto Networks, Inc.

Configurar la Infraestructura de servicios de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Versión de Prisma Access mínima requerida para **Pre-prod or Lab Tenant (Inquilino de Pre-prod o Lab)**: 3.0-Preferred

Prisma Access utiliza esta subred para crear la red troncal de red para la comunicación entre las redes de sucursales, los usuarios móviles y la infraestructura de seguridad de Prisma Access, así como con las redes de la sede central y del centro de datos que planea conectar a Prisma Access a través de conexiones de servicio.

Para habilitar la comunicación entre las ubicaciones de red remotas, los usuarios móviles y la sede central o los centros de datos a los que planea conectar Prisma Access a través de conexiones de servicio, establezca la subred de infraestructura de servicio. Prisma Access utiliza esta subred para crear la red troncal para la comunicación entre las redes de sucursales, los usuarios móviles y la infraestructura de seguridad de Prisma Access, así como con las redes de la sede central y del centro de datos a las que planea conectar Prisma Access a través de conexiones de servicio.

- Strata Cloud Manager
- Panorama

Configure la Infraestructura de servicios de Prisma Access (Strata Cloud Manager)

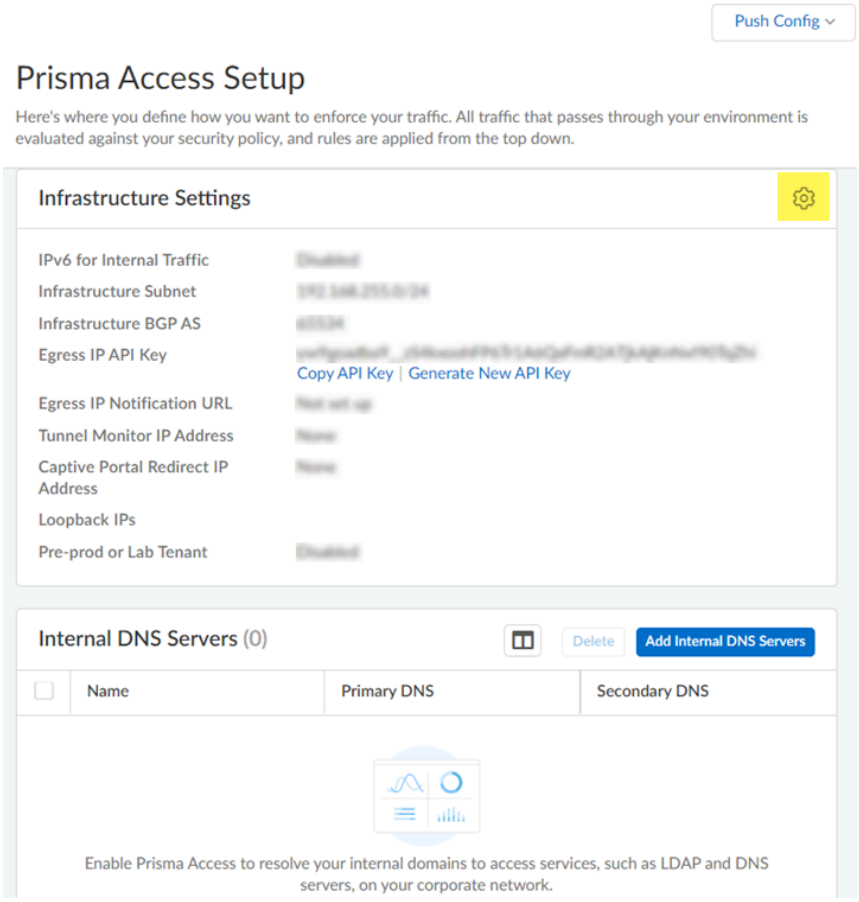
Utilice las siguientes recomendaciones y requisitos cuando añada una subred de infraestructura para Prisma Access:

- ❑ Utilice una subred compatible con RFC 1918. Aunque se admite el uso de direcciones IP (públicas) no compatibles con RFC 1918, no se recomienda debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.
- ❑ No especifique ninguna subred que se solape con el rango de subredes 169.254.0.0/16 y 100.64.0.0/10, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno.
- ❑ Esta subred es una extensión de la red existente y, por lo tanto, no puede solaparse con ninguna subred IP que utilice dentro de su red corporativa o con los grupos de direcciones IP que asigne a Prisma Access para usuarios o Prisma Access para redes.
- ❑ Debido a que la infraestructura de servicios requiere un gran número de direcciones IP, debe designar una subred /24 (por ejemplo, 172.16.55.0/24).
- ❑ Si utiliza enrutamiento dinámico para sus redes remotas o conexiones de servicio, también debe configurar un número AS privado de BGP compatible con RFC 6996.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Iniciar Prisma Access.

STEP 2 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)** y haga clic en el engranaje para editar la configuración.



STEP 3 | Introduzca una **subred de infraestructura** que Prisma Access pueda utilizar para habilitar la comunicación entre las ubicaciones de red remotas, los usuarios móviles y la sede o los centros de datos que planifica conectar a Prisma Access a través de conexiones de servicio.

Utilice una subred compatible con RFC 1918 para la subred de infraestructura. Aunque se admite el uso de direcciones IP (públicas) no compatibles con RFC 1918, no se recomienda debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.

STEP 4 | (Opcional) Si está configurando IPv6, seleccione **IPv6 for Internal Traffic (IPv6 para tráfico interno)** y seleccione una subred IPv6.

STEP 5 | Introduzca la **Infrastructure BGP AS (Infraestructura BGP AS)** que desea utilizar dentro de la infraestructura Prisma Access.

Si desea habilitar el enrutamiento dinámico para que Prisma Access pueda descubrir dinámicamente rutas a recursos en sus redes remotas y ubicaciones de sedes centrales o centros de datos, debe utilizar el Protocolo de puerta de enlace de borde (BGP). La **Infrastructure BGP AS (Infraestructura BGP AS)** es el número de sistema autónomo (AS)

 ©2025 Palo Alto Networks, Inc.

que identifica las rutas a través de las cuales BGP puede enviar tráfico. Si no proporciona un número AS, Prisma Access utiliza el número AS predeterminado (65534).

Si desea especificar su propio número AS, debe utilizar un número AS privado que cumpla con RFC 6996. Los formatos aceptados son notación AS Plain de 4 bytes [64512-65534], [4200000000-4294967294] o AS Dot [0,64512-0,65534], [64086,59904-65535,65534].

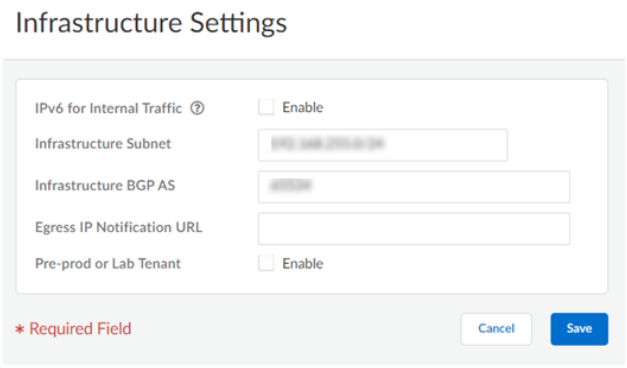
STEP 6 | Si permite que sus usuarios accedan a aplicaciones según la dirección IP de origen, necesitará obtener la lista de direcciones IP que el tráfico de Prisma Access utiliza como dirección de origen para que pueda permitirles en sus políticas de acceso a la aplicación.

Tiene que **Copy (Copiar)** la **Egress IP API Key (Clave API de IP de salida)** para habilitar el uso de la API de dirección IP de salida de Prisma Access. Además, debido a que las direcciones IP que Prisma Access usa cambian periódicamente, por ejemplo, cuando se añade una nueva ubicación, cuando Prisma Access necesita ampliar recursos en una ubicación existente o cuando hay una actualización de infraestructura, necesitará saber cuándo cambian las direcciones IP para poder actualizar sus reglas de políticas o automatizar estas actualizaciones definiendo una **Egress IP Notification URL (URL de notificación de IP de salida)**. Consulte Recuperar las direcciones IP para Prisma Access para obtener más detalles.

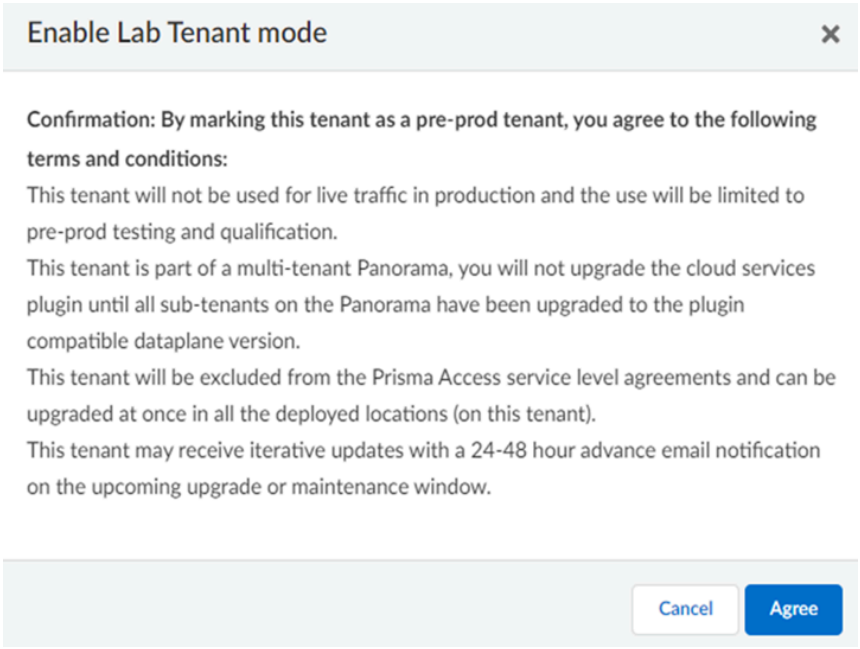
 ©2025 Palo Alto Networks, Inc.

STEP 7 | (Opcional) Habilite al inquilino como inquilino de preproducción o de laboratorio.

1. **Enable (Habilitar)** al inquilino como **Pre-prod or Lab Tenant (Inquilino de Pre-prod o Lab)**.



2. **Agree (Aceptar)** para confirmar.



   Cuando habilita a un inquilino como inquilino de preproducción o de laboratorio, puede programar actualizaciones solo para este inquilino antes de actualizar otros inquilinos de producción. El inquilino recibe notificaciones entre 24 y 48 horas antes de una próxima actualización. Cuando se deshabilita el inquilino de preproducción o de laboratorio, se lo considera un inquilino de producción.

3. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 8 | Para habilitar Prisma Access para resolver sus dominios internos, tiene que **Add Internal DNS Servers (Añadir servidores DNS internos)**.

Si planifica configurar conexiones de servicio para permitir el acceso a recursos en su red corporativa y también necesita que Prisma Access resuelva sus dominios internos, debe definir la lista de dominios internos. Las consultas DNS para los dominios de la lista interna

 ©2025 Palo Alto Networks, Inc.

de dominios se envían a los servidores DNS locales para asegurarse de que los recursos estén disponibles para los usuarios de red remotos de Prisma Access y los usuarios móviles.

1. Introduzca el servidor **Primary DNS (DNS primario)** y el servidor **Secondary DNS (DNS secundario)** que Prisma Access deberá usar para resolver nombres de dominio internos.
2. **Add (Añadir)** los **Domain Names (Nombres de dominio)** internos que desea que Prisma Access resuelva.

   Puede utilizar un comodín (*) delante de los dominios de la lista de dominios, por ejemplo, *.acme.local o *.acme.com

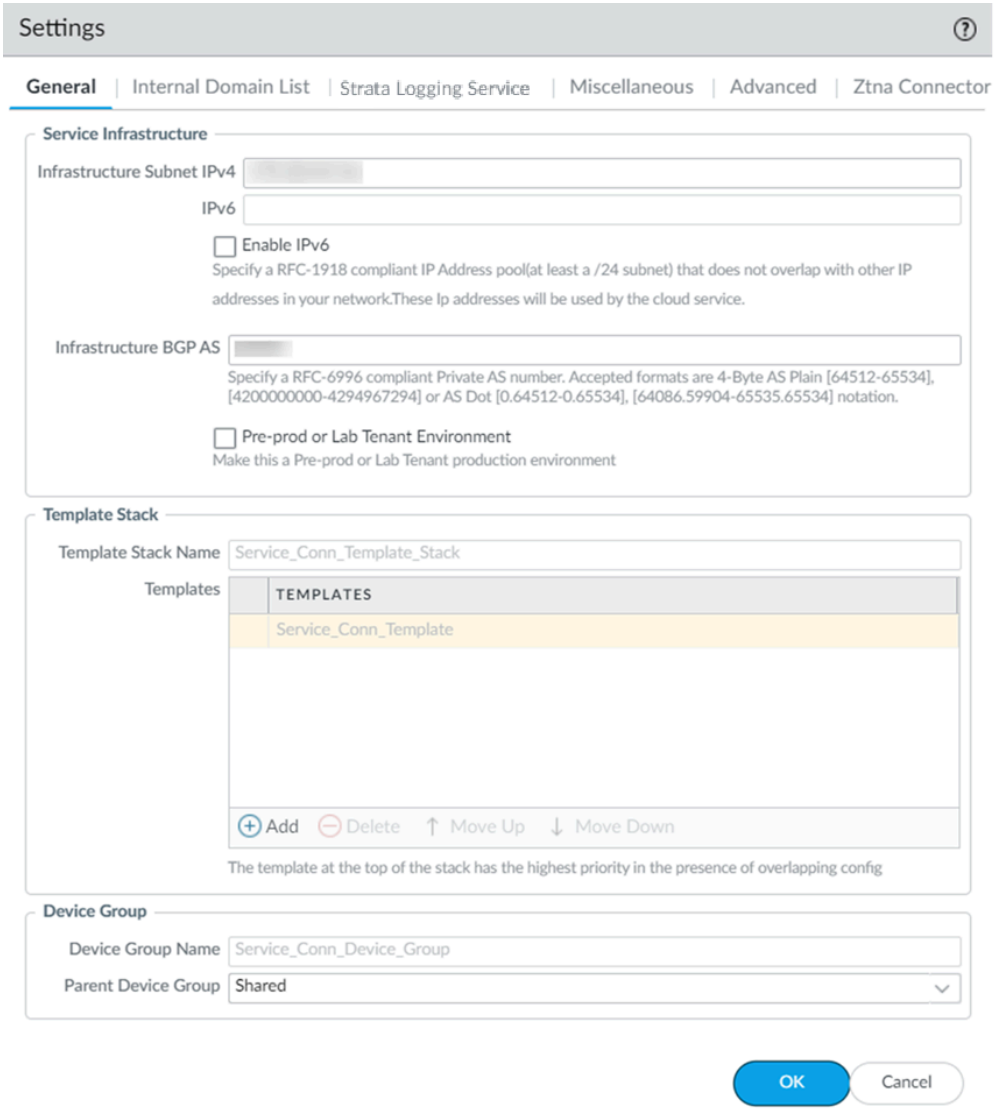
STEP 9 | **Push Config (Enviar configuración)** para guardar la configuración de la infraestructura de su servicio en Prisma Access.

Configure la Infraestructura de servicios de Prisma Access (Panorama)

Antes de empezar a configurar Prisma Access para que proteja sus redes remotas y/o usuarios móviles, debe configurar una subred de infraestructura, que Prisma Access utilizará para crear la red troncal para la comunicación entre las conexiones de servicio, las redes remotas y los usuarios móviles, así como con las redes corporativas a las que planea conectar Prisma Access a través de conexiones de servicio. Dado que se necesitará un gran número de direcciones IP para configurar la infraestructura, debe usar una subred /24 (por ejemplo, 172.16.55.0/24) como mínimo. ¡Asegúrese de seguir todas las directrices y requisitos.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y haga clic en el icono de engranaje para editar la Configuración.



STEP 2 | En la pestaña **General**, especifique una **Infrastructure Subnet (Subred de infraestructura)** que cumpla los requisitos, por ejemplo, 172.16.55.0/24.

STEP 3 | (Opcional) Si está configurando IPv6, seleccione **IPv6 for Internal Traffic (IPv6 para tráfico interno)** y seleccione una subred IPv6.

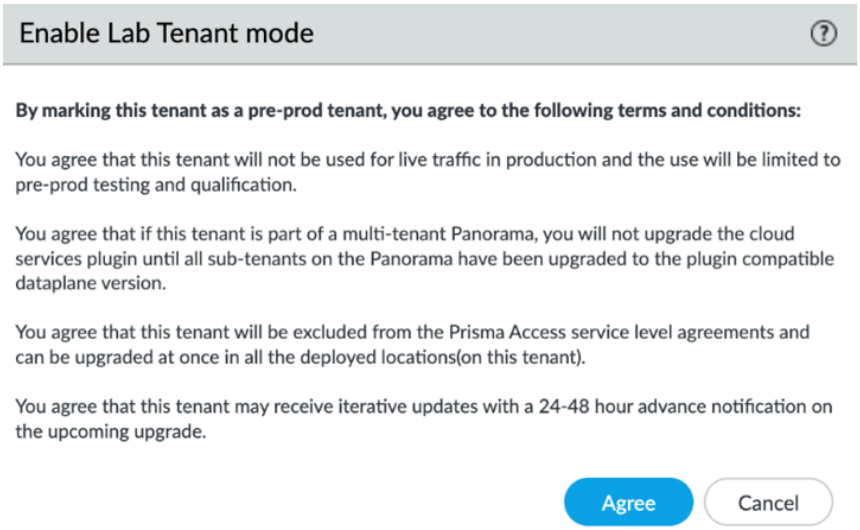
STEP 4 | (Opcional) Si desea habilitar Prisma Access para utilizar BGP para detectar dinámicamente rutas a los recursos en sus redes remotas y ubicaciones de HQ/centro de datos, introduzca la **Infrastructure BGP AS (Infraestructura BGP AS)** que desea utilizar dentro de la infraestructura de Prisma Access.

Si no proporciona un número AS, se utilizará el número AS predeterminado 65534.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Habilite un inquilino como **Pre-prod or Lab Tenant Environment (Entorno de inquilino de preproducción o de laboratorio)**.

Cuando habilita a un inquilino como inquilino de preproducción o de laboratorio, puede programar actualizaciones solo para este inquilino antes de actualizar otros inquilinos de producción. El inquilino recibe notificaciones entre 24 y 48 horas antes de una próxima actualización.



Cuando se deshabilita el inquilino de preproducción o de laboratorio, se lo considera un inquilino de producción.

Prisma Access para Clean Pipe no es compatible con esta funcionalidad.

STEP 6 | (Opcional) Habilite Prisma Access para resolver sus dominios internos utilizando sus servidores DNS corporativos.

Utilice este paso si necesita que Prisma Access pueda resolver sus dominios internos para acceder a servicios, como servidores LDAP, en su red corporativa a través de conexiones de servicio. Por ejemplo, si desea que una búsqueda de DNS para su dominio corporativo vaya exclusivamente al servidor DNS corporativo, especifique aquí el dominio corporativo y los servidores DNS corporativos.

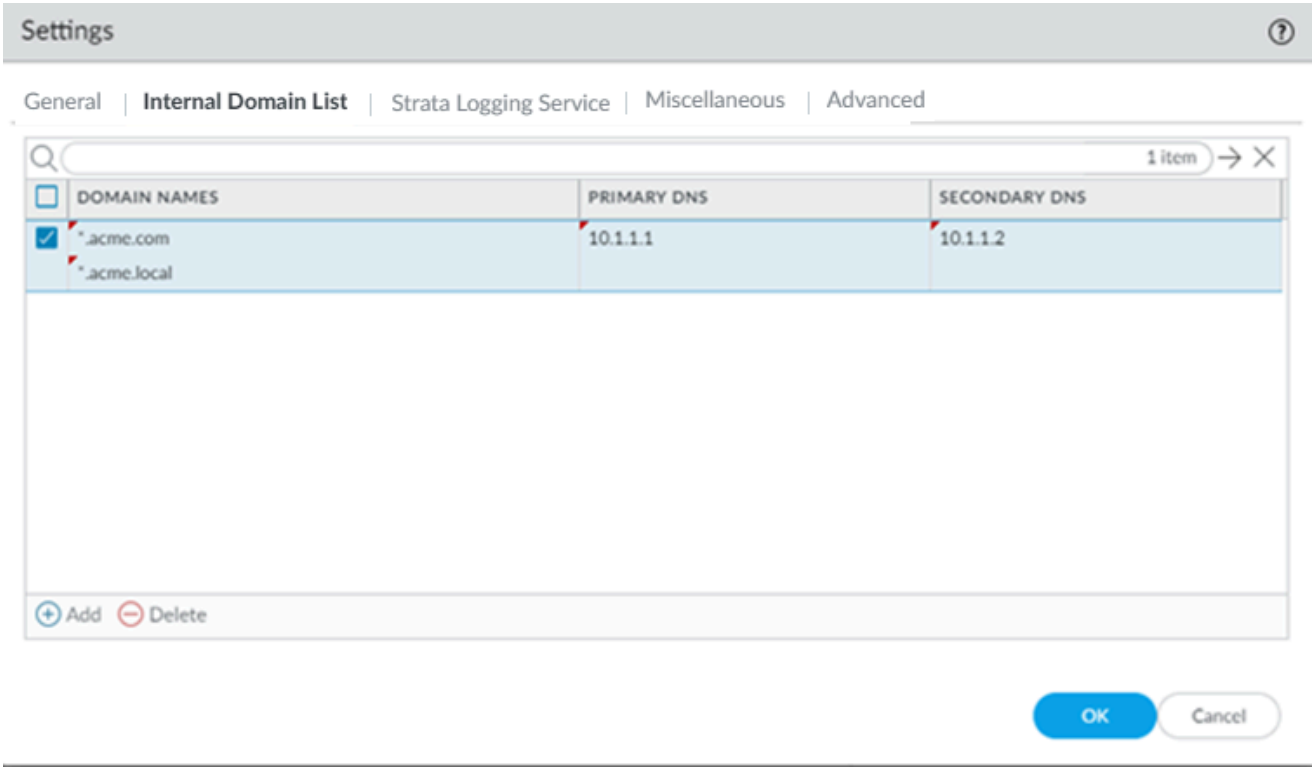
1. Seleccione la pestaña **Internal Domain List (Lista de dominios internos)**.

 ©2025 Palo Alto Networks, Inc.

2. Deberá **Add (Añadir)** los servidores **Domain Names (Nombres de dominio)**, **Primary DNS (DNS primario)** y **Secondary DNS (DNS secundario)** que desee que Prisma Access use para resolver sus nombres de dominio internos.

   Puede utilizar un comodín (*) delante de los dominios de la lista de dominios, por ejemplo, *.acme.local o *.acme.com

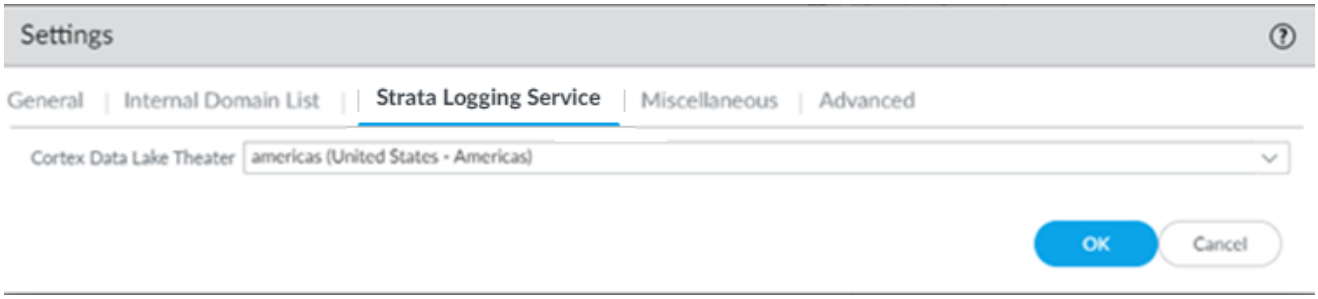
   No introduzca una dirección 127.0.0.1, ya que puede causar problemas de enrutamiento interno de Prisma Access.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Habilitar Strata Logging Service.

1. Seleccione la pestaña **Strata Logging Service**.
2. Seleccione un **Strata Logging Service Theater (Teatro de Strata Logging Service)** y haga clic en **OK (Aceptar)**.



3. Configure los grupos de dispositivos que está utilizando para enviar la configuración a Prisma Access con un Log Forwarding profile (Perfil de reenvío de logs) que reenvía los tipos de logs deseados a **Panorama/Strata Logging Service**.

   El complemento de Cloud Services añade automáticamente la siguiente configuración de logs [**Device (Dispositivo)** > **Log Settings (Configuración de logs)**] después de una nueva instalación o al retirar plantillas de Prisma Access de una pila de plantillas de Prisma Access:

   - La configuración de logs para los logs del sistema (**sistema-gpcs-default**), logs de User-ID (**userid-gpcs-default**), logs de coincidencias HIP (**hipmatch-gpcs-default**) y los logs de GlobalProtect (**gp-prismaaccess-default**) se añaden a Mobile_User_Template.
   - La configuración de logs para los logs del sistema (**sistema-gpcs-default**), los logs de User-ID (**userid-gpcs-default**) y los logs de GlobalProtect (**gp-prismaaccess-default**) se añaden a Remote_Network_Template.
   - La configuración de logs para los logs del sistema (**sistema-gpcs-default**) y los logs de GlobalProtect (**gp-prismaaccess-default**) se añaden a Service_Conn_Template.

   Estas configuraciones de configuración de logs reenvían automáticamente los logs del sistema, User-ID, HIP Match y GlobalProtect a Strata Logging Service.

   Para aplicar los cambios en la configuración de logs, realice los siguientes pasos y, a continuación, confirme y envíe los cambios:

   - Para aplicar la configuración de registro a la plantilla de usuario móvil, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)**, haga clic en el icono de engranaje para editar la configuración y haga clic en OK (Aceptar).
   - Para aplicar la configuración de logs a la plantilla de red remota, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, haga clic en el icono de engranaje para editar la configuración y haga clic en Aceptar.
   - Para aplicar la configuración de logs a la plantilla de conexión de servicio, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)**

 ©2025 Palo Alto Networks, Inc.

> **Service Setup (Configuración del servicio)**, haga clic en el icono de engranaje para editar la configuración y haga clic en Aceptar.

La forma de habilitar el reenvío de logs para otros tipos de logs depende del tipo. En el caso de los logs que se generan en función de una coincidencia de política, utilice un perfil de reenvío de logs. Consulte la Guía de inicio de Strata Logging Service para obtener más información.

STEP 8 | (Opcional) Configure los ajustes **Miscellaneous (Varios)**.

1. (Opcional) Anexe el token final para las URL en listas dinámicas externas (EDL) o categorías de URL personalizadas al seleccionar **Append the ending token to the URLs in the URL filtering configuration (Anexar el token final a las direcciones URL en la configuración de filtrado de direcciones URL)**.

   Si utiliza URL en EDL o categorías de URL personalizadas y no añade una barra inclinada (**/**) a la URL, es posible permitir más direcciones URL de las que pretendía. Por ejemplo, si introduce **`example.com`** como una URL coincidente en lugar de **`example.com/`** también coincidiría con example.com.website.info o example.com.br.

   Al seleccionar **Append the ending token to the URLs in the URL filtering configuration (Anexar el token final a las direcciones URL en la configuración de filtrado de direcciones URL)**, Prisma Access establece un token final para las direcciones URL en EDL o categorías de URL personalizadas para que, si introduce **`example.com`**, Prisma Access lo trata como trataría example.com/ y solo coincide con esa URL.
2. (Opcional) **Disable Traffic Logging on Service Connections (Deshabilitar el registro de logs de tráfico en conexiones de servicio)** para deshabilitar el registro de logs en las conexiones de servicio para la implementación de Prisma Access.

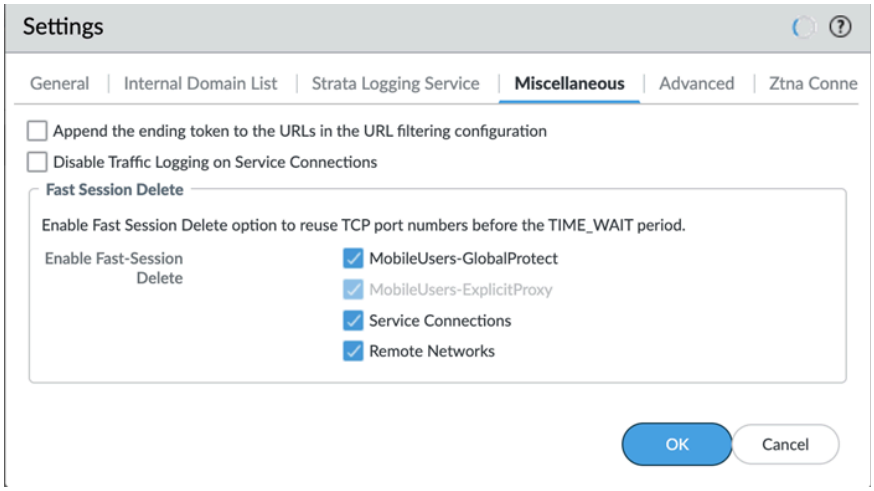
   Si la mayoría de los flujos de tráfico registrados por las conexiones de servicio son asimétricos, es posible que sea necesario desactivar el registro de logs de conexiones de servicio para reducir el consumo de almacenamiento de registros de logs de Strata Logging Service. Si su implementación no tiene flujos asimétricos a través de las conexiones de servicio, no necesita desactivar el registro de logs.
3. (Opcional) Para habilitar la eliminación de sesión rápida para redes remotas, conexiones de servicio o usuarios móviles, implementaciones de GlobalProtect, seleccione las casillas

 ©2025 Palo Alto Networks, Inc.

de verificación para **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**, **Service Connections (Conexiones de servicio)** o **Remote Networks (Redes remotas)**.

La eliminación rápida de sesión permite a Prisma Access reutilizar los números de puerto TCP antes de que expire el período de TIME_WAIT TCP y puede ser útil para sesiones de descifrado SSL que pueden ser de corta duración.

Para implementaciones de Usuarios móviles: Proxy explícito, la eliminación de sesión rápida es una parte clave de su funcionalidad y no se puede deshabilitar.



STEP 9 | (Opcional) Configure la configuración **Advanced (Avanzado)** (preferencias de enrutamiento, opciones de ruta de red simétrica para conexiones de servicio y redistribución de HIP).

1. Especifique la **Routing Preference (Preferencia de enrutamiento)** para usar con conexiones de servicio.

   Puede especificar las preferencias de red para utilizar la red de su organización o la red de Prisma Access, para procesar el tráfico de conexión de servicio.

   - **Default (Predeterminado)**: Prisma Access utiliza el enrutamiento predeterminado en su red interna.
   - **Hot potato routing (Enrutamiento Hot Potato)**: Prisma Access transfiere el tráfico de conexión de servicio a la WAN de su organización lo más rápido posible.

   Cambiando el método de enrutamiento de la conexión de servicio de Prisma Access requiere una comprensión profunda de la topología y los dispositivos de enrutamiento de su organización, junto con una comprensión de cómo funciona el enrutamiento de Prisma Access. Le recomendamos leer Enrutamiento para el tráfico de conexión de servicio *con cuidado antes de cambiar el método de enrutamiento predeterminado.*

2. Configure el **Backbone Routing (Enrutamiento de red troncal)** que se utilizará para las conexiones de servicio.

   De forma predeterminada, la red troncal de Prisma Access requiere que usted tenga una ruta de red simétrica para el tráfico que regresa desde el centro de datos o la ubicación de la sede central a través de una conexión de servicio. Si desea utilizar ECMP u otro

 ©2025 Palo Alto Networks, Inc.

mecanismo de equilibrio de carga para las conexiones de servicio desde su CPE, puede habilitar flujos asimétricos a través de la red troncal de Prisma Access.

- Seleccione **no-asymmetric-routing (sin enrutamiento asimétrico)** para requerir flujos simétricos a través de la red troncal de conexión de servicio.
- Seleccione **asymmetric-routing-only (solo enrutamiento asimétrico)** para permitir que Prisma Access utilice flujos asimétricos a través de la red troncal de conexión de servicio.
- Si tiene varias conexiones de servicio a una ubicación, puede aprovechar el equilibrio de carga en su implementación de Prisma Access seleccionando **asymmetric-routing-with-load-share (enrutamiento asimétrico con carga compartida)** (la configuración predeterminada). Sin embargo, el equilibrio de carga se realiza según el máximo esfuerzo y fallará si una de las conexiones de servicio falla.

3. Redistribuir la información de HIP con Prisma Access para utilizar conexiones de servicio para redistribuir la información de HIP de los usuarios móviles y los usuarios en redes remotas.
4. Identificación y cuarentena de dispositivos en riesgo en una implementación de Prisma Access GlobalProtect para que Prisma Access identifique y ponga en cuarentena los dispositivos comprometidos que están conectados con la aplicación GlobalProtect.
5. **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Retirar rutas estáticas si el túnel IPSec de Conexión de servicio o Redes remotas está inactivo)** si desea que Prisma Access elimine las rutas estáticas cuando un túnel deja de funcionar sin un túnel de respaldo.

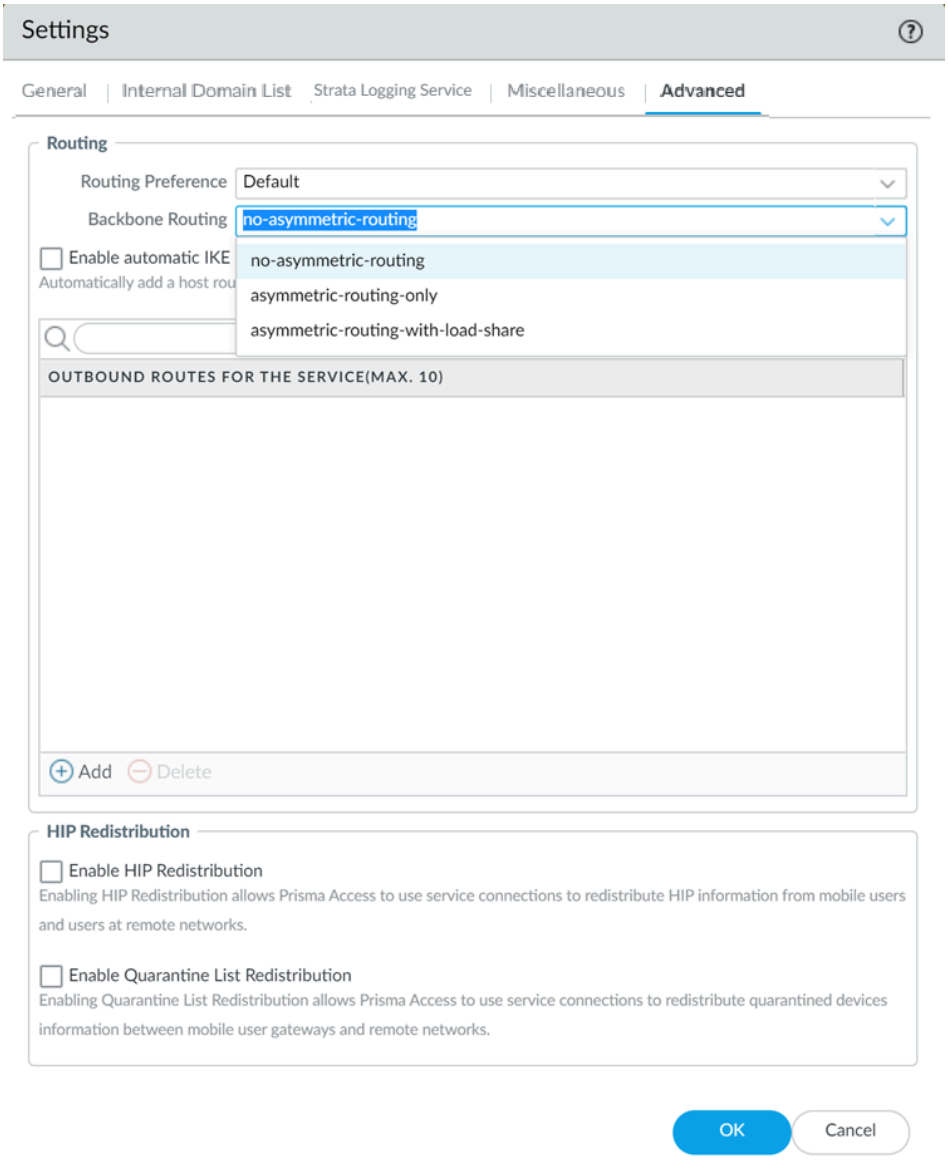
   Prisma Access elimina la ruta en las siguientes situaciones:

   - El túnel principal desciende y no hay túnel secundario.
   - Si se configura un túnel primario y uno secundario, pero ambos dejan de funcionar.

   No se puede aplicar este cambio si la supervisión del túnel no está habilitada.
6. (Opcional) Si desea enrutar paquetes de túnel IPSec de conexión de red y servicio remotos a las puertas de enlace IKE estáticas a través de Internet, deberá **Enable automatic IKE peer host routes for Remote Networks and Service Connections (Habilitar las rutas automáticas de host de par IKE para redes remotas y conexiones de servicio)**.
7. (Opcional) **Specify Outbound Routes for the Service (Especificar las rutas de salida para el servicio)** añadiendo hasta 10 prefijos para los cuales Prisma Access añade rutas

 ©2025 Palo Alto Networks, Inc.

estáticas en todas las conexiones de servicio y conexiones de red remotas. Prisma Access luego dirige el tráfico hacia estos prefijos a través de Internet.



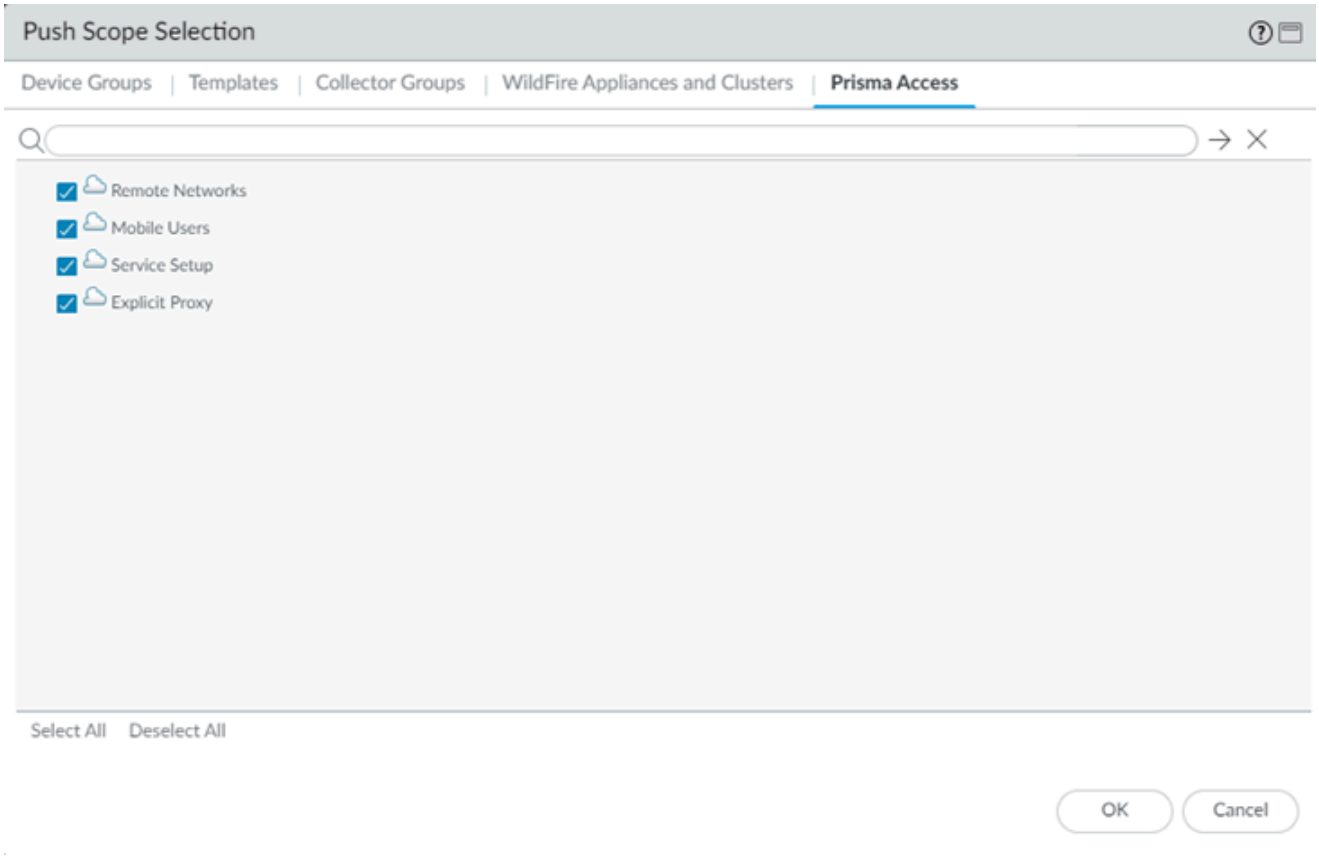
STEP 10 | haga clic en **OK (Aceptar)** para guardar la configuración de la configuración del servicio.

©2025 Palo Alto Networks, Inc.

STEP 11 | Confirme todos sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.
2. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y haga clic en **Edit Selections (Editar selecciones)**.
3. En el pestaña de **Prisma Access**, asegúrese de seleccionar **Service setup (Configuración de servicio)** y, a continuación, haga clic en **OK (Aceptar)**.

   Prisma Access debería seleccionar automáticamente los componentes que deben confirmarse.

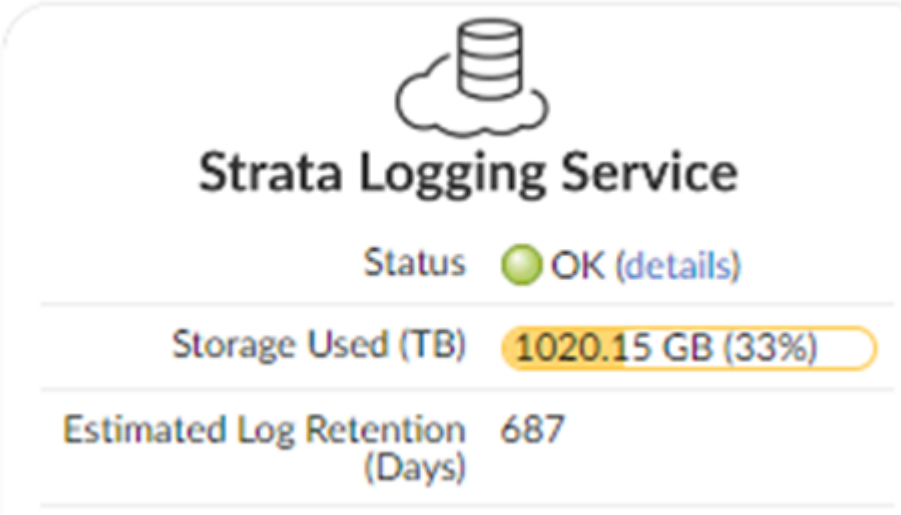


4. Haga clic en **Push (Enviar)**.

 ©2025 Palo Alto Networks, Inc.

STEP 12 | Verifique que Prisma Access se conecta correctamente a Strata Logging Service.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** > **Strata Logging Service** y verifique que el estado sea **OK (Aceptar)**.



Si el estado es **Error**, haga clic en el enlace de detalles para ver los errores.

STEP 13 | Continuar configurando Prisma Access:

- Crear una Conexión de servicio para permitir el acceso a aplicaciones privadas.
- Configurar Prisma Access para Redes
- Configurar Prisma Access para Usuarios

 ©2025 Palo Alto Networks, Inc.

Usuarios móviles: Asignación de dirección IP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Después de configurar su implementación de Prisma Access, es útil saber cuándo cambian las direcciones IP para que pueda planificar de forma proactiva su infraestructura, recuperar las direcciones IP y añadir las direcciones IP necesarias para permitir listas según corresponda. Los cambios de direcciones IP pueden ser el resultado de cambios que usted realizó (por ejemplo, añadir la ubicación de otro usuario móvil) o cambios que Prisma Access realiza automáticamente (por ejemplo, una gran número de usuarios móviles acceden a una única puerta de enlace de Prisma Access).

Después de la implementación de Prisma Access para los usuarios por primera vez, Prisma Access asigna dos *direcciones IP públicas y, si corresponde, de salida* para cada portal y puerta de enlace. Estas direcciones IP son únicas, no se comparten, están dedicadas a su implementación de Prisma Access y permanecerán asignadas a su inquilino hasta que la suscripción de Prisma Access caduque y el período de gracia haya terminado.

Si tiene una configuración multiinquilino, Prisma Access añade direcciones IP dedicadas para cada inquilino.

Dado que la dirección IP pública es la dirección IP de origen utilizada por Prisma Access para las solicitudes realizadas a un destino basado en Internet, es posible que necesite saber cuáles son las direcciones IP públicas y añadirlas a una lista de permitidos en su red para proporcionar a sus usuarios acceso a recursos como aplicaciones SaaS o aplicaciones de socios de acceso público.

Se pueden añadir nuevas direcciones IP públicas al inquilino si se producen los siguientes eventos:

- Una gran número de usuarios móviles accede a una ubicación en la misma ubicación.

  Para abordar la necesidad de capacidad para dar servicio a un gran número de usuarios, Prisma Access puede añadir una o más puertas de enlace, Prisma Access añade una o más puertas de enlace para dar cabida a la mayor cantidad de usuarios, asigna una o más de las direcciones IP públicas existentes a la nueva puerta de enlace y añade un nuevo conjunto de direcciones IP a las ubicaciones de los usuarios móviles para reemplazar las que se usaban.
- Añade una o más ubicaciones a su implementación.

  Al añadir más ubicaciones, Prisma Access añade otra puerta de enlace y un nuevo conjunto de direcciones IP para cada nueva ubicación que añada.

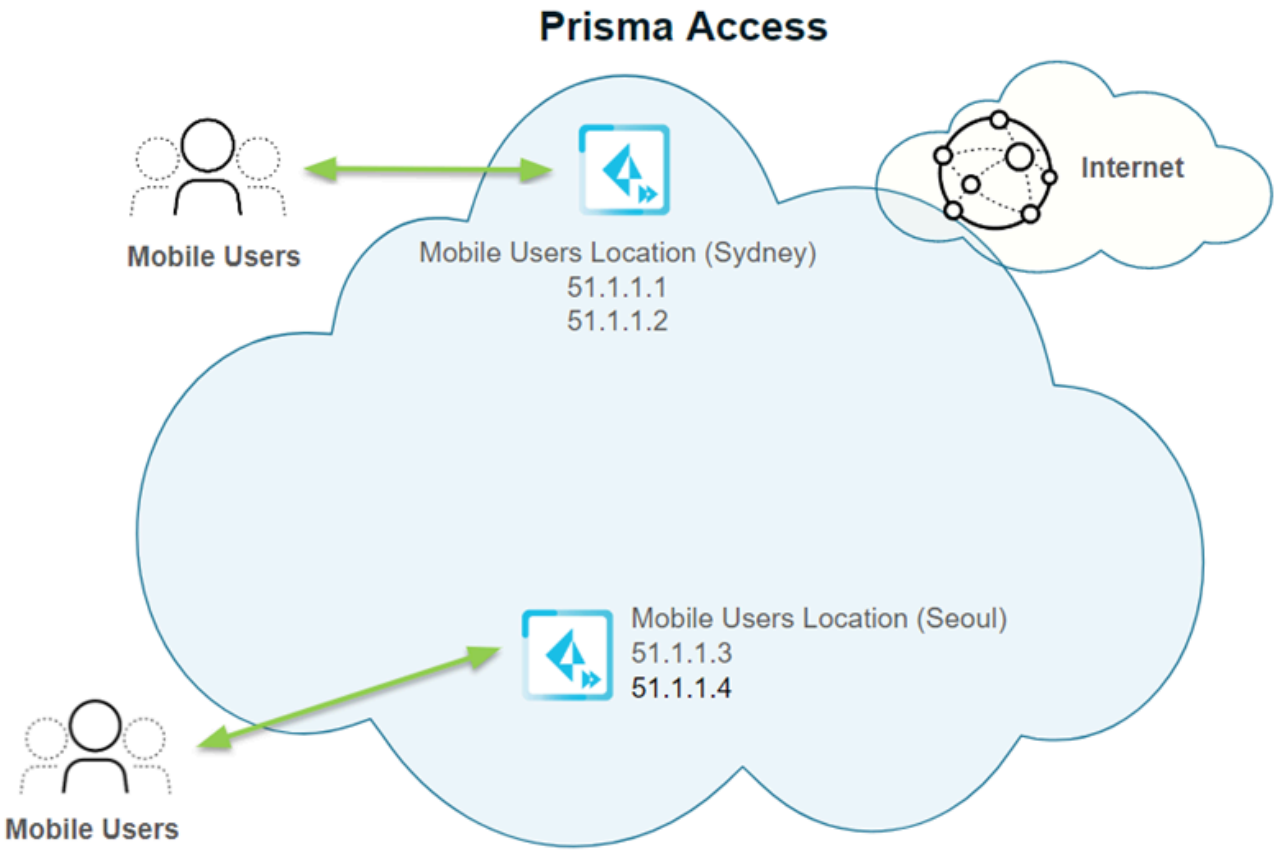
Dado que Prisma Access permite más direcciones IP públicas después de un evento de escalamiento y después de añadir una ubicación, debe añadir una URL de notificación de evento de cambio de IPo usar la API para recuperar direcciones de usuarios móviles, para recibir notificaciones de cambios de dirección IP en su infraestructura de Prisma Access. Luego puede añadir cualquier dirección agregada o modificada a una lista de permitidos.

 ©2025 Palo Alto Networks, Inc.

Ejemplo: Ejemplos de escalado de direcciones IP públicas (usuarios móviles)

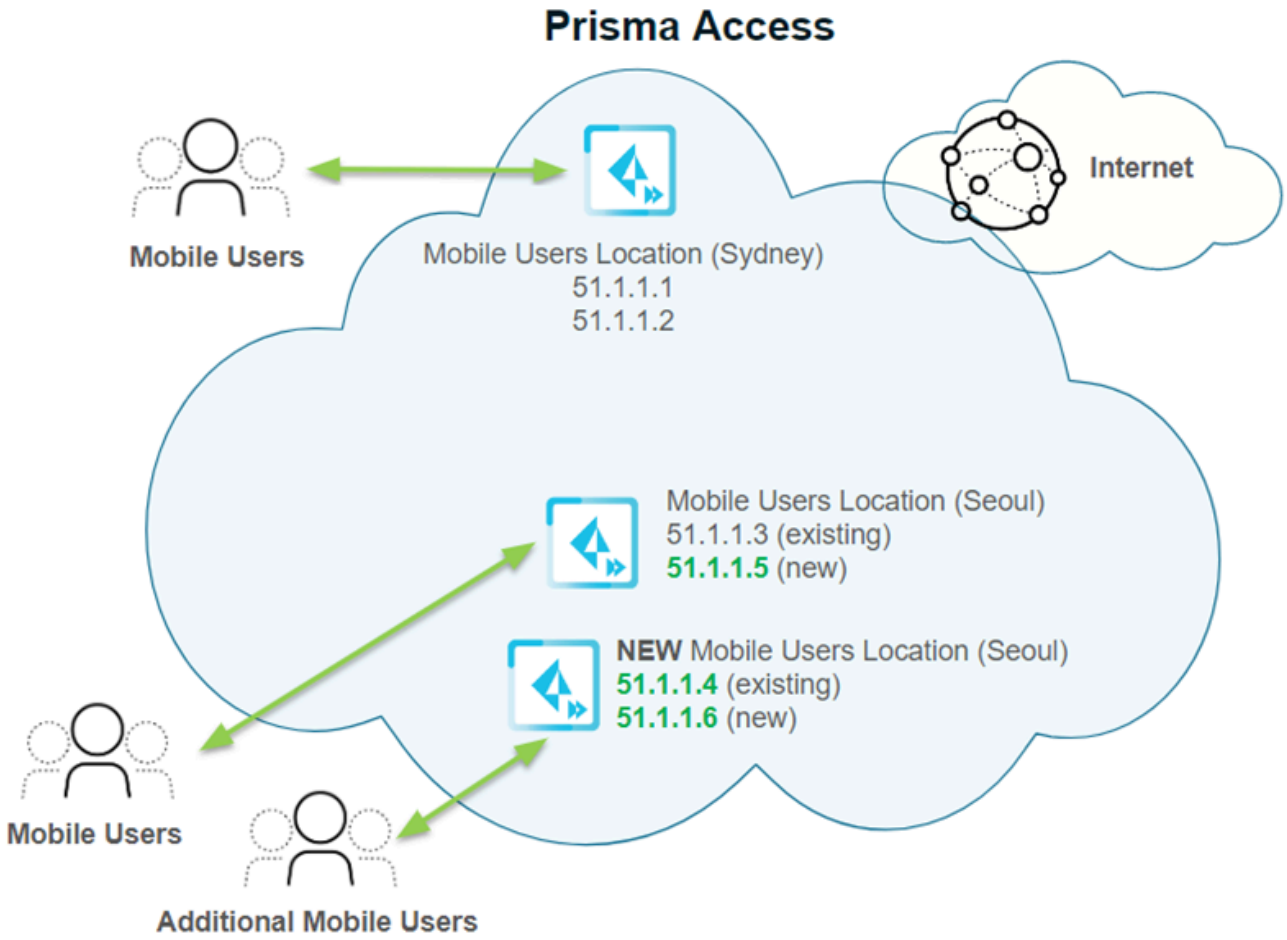
Los siguientes ejemplos ilustran el proceso de asignación de direcciones IP públicas de usuarios móviles que Prisma Access utiliza durante un evento de escalado o cuando añade una nueva ubicación.

En el ejemplo siguiente, especificó dos ubicaciones en la región de Asia y el Pacífico para una nueva implementación de usuarios móviles: Sydney y Seúl. Cada ubicación recibe dos direcciones IP de puerta de enlace.



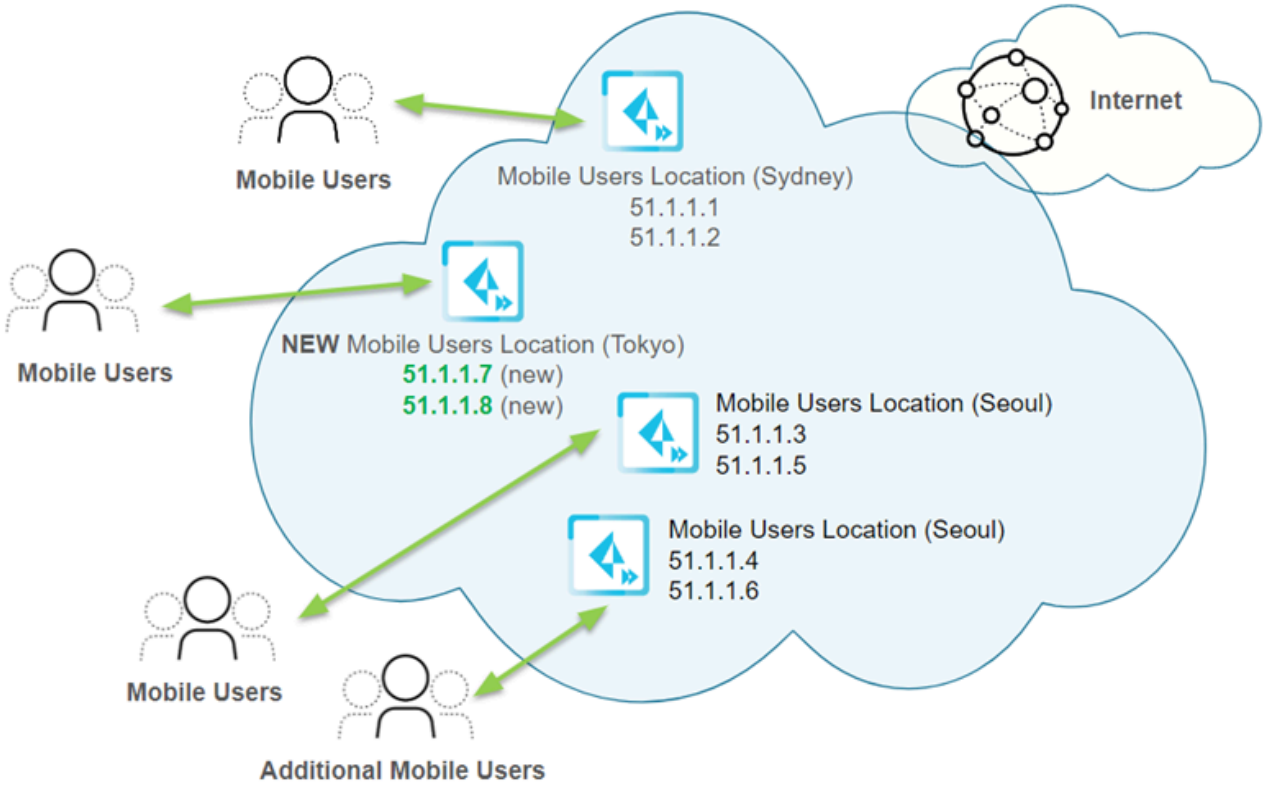
A continuación, un gran número de usuarios inicia sesión en la ubicación de Seúl. Para acomodar a estos usuarios adicionales, Prisma Access añade una segunda puerta de enlace para la ubicación de Seúl, toma una de las direcciones de puerta de enlace de la primera puerta de enlace de Seúl (51.1.1.4) y la asigna a la segunda puerta de enlace de Seúl. A continuación, añade dos direcciones IP adicionales (51.1.1.5 y 51.1.1.6 en este ejemplo) y las añade a las dos puertas de enlace de Seúl.

©2025 Palo Alto Networks, Inc.



A continuación, se añade otra ubicación, Tokio, en la región de Asia Pacífico. Prisma Access crea dos nuevas direcciones IP para la nueva puerta de enlace (51.1.1.7 y 51.1.1.8).

 ©2025 Palo Alto Networks, Inc.



Cada vez que añada una ubicación o tenga un evento de escalado, debe recuperar las nuevas direcciones IP de salida y puerta de enlace que Prisma Access asignó y añadirlas a una lista de permisos en su red. Prisma Access mantiene dos conjuntos de direcciones IP en todo momento para todas las puertas de enlace activas en cada ubicación.

Asignación de direcciones IP de bucle invertido (usuarios móviles)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Las direcciones de bucle invertido son direcciones IP utilizadas por Prisma Access para solicitudes realizadas a una fuente interna y se asignan desde la subred de infraestructura. Las direcciones IP de bucle invertido pueden cambiar para los usuarios móviles durante una actualización de la infraestructura o del plano de datos.

Las direcciones IP de bucle invertido no cambian para las conexiones de servicio o las conexiones de red remotas durante una actualización de infraestructura o plano de datos; solo las direcciones IP de bucle invertido de los usuarios móviles pueden cambiar.

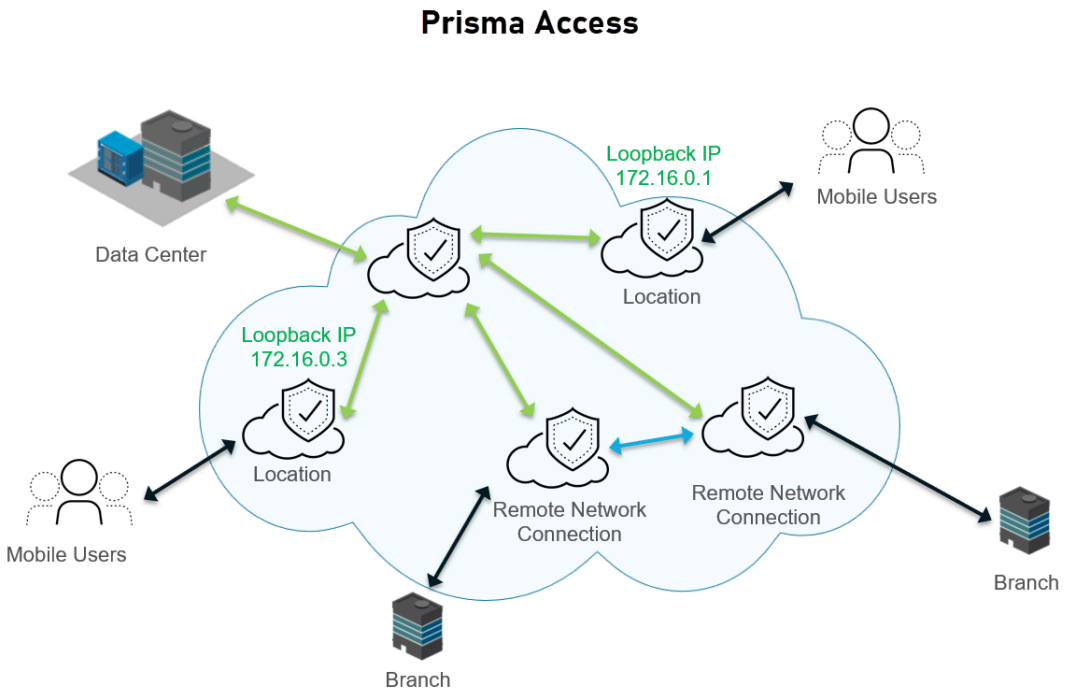
 ©2025 Palo Alto Networks, Inc.

Prisma Access asigna las direcciones IP de bucle invertido de la subred de infraestructura que usted especifica cuando habilita la infraestructura de Prisma Access. Puede añadir toda la subred de infraestructura a una lista de permitidos y evitar la planificación de cambios de IP de bucle invertido de usuarios móviles durante una actualización de infraestructura o plano de datos. Para encontrar la subred de infraestructura, seleccione:

- Prisma Access (Managed by Strata Cloud Manager): **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)** y visualice la **Infrastructure Subnet (Subred de infraestructura)**
- Prisma Access (Managed by Panorama): **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Infrastructure (Infraestructura del servicio)** y ver la **Infrastructure Subnet (Subred de infraestructura)**

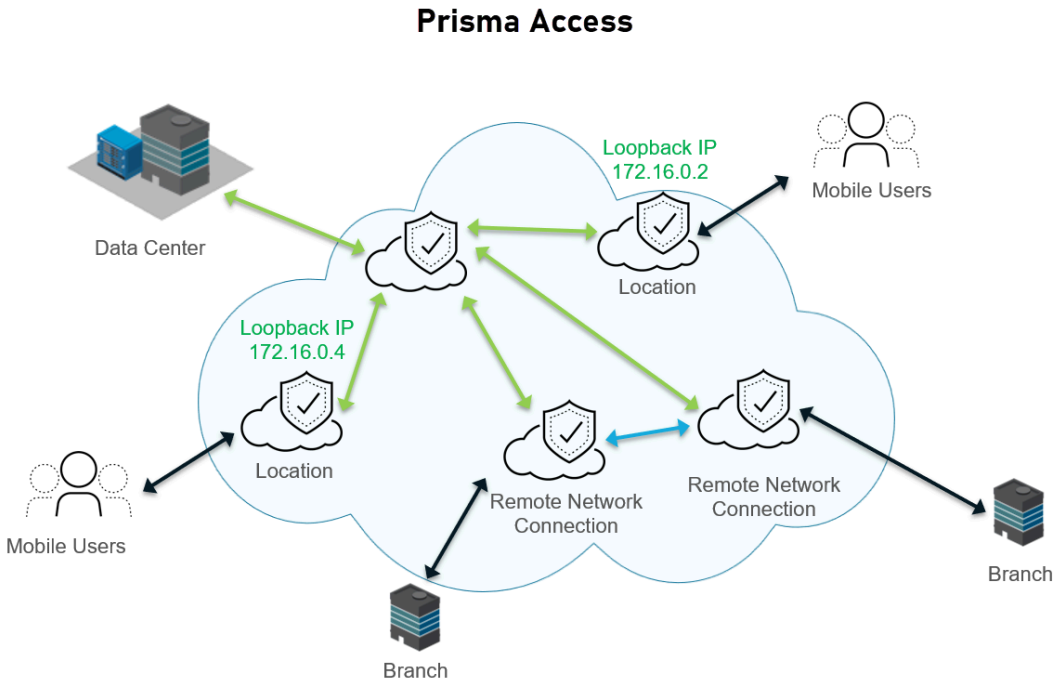
Recupere estas direcciones utilizando la API utilizada para recuperar direcciones IP públicas y direcciones IP de bucle invertido.

El siguiente ejemplo muestra una implementación de Prisma Access que tiene una subred de infraestructura de 172.16.0.0/16. Prisma Access ha asignado direcciones IP de bucle invertido 172.16.0.1 y 172.16.0.3 para usuarios móviles de la subred de infraestructura.



Después de una actualización de la infraestructura o del plano de datos (por ejemplo, para prepararse para una nueva versión del complemento de servicios en la nube), Prisma Access asigna dos direcciones IP diferentes para los usuarios móviles de la subred de infraestructura (172.16.0.1 se cambia a 172.16.0.2 y 172.16.0.3 se cambia a 172.16.0.4).

 ©2025 Palo Alto Networks, Inc.

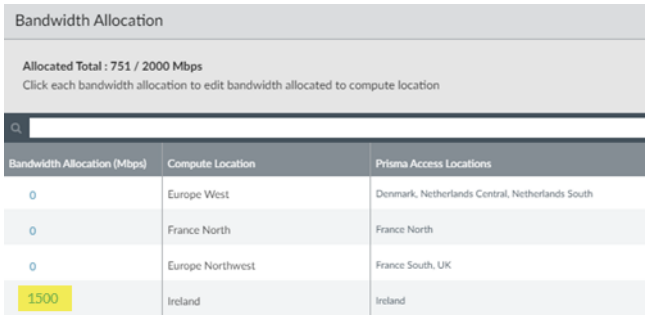


 ©2025 Palo Alto Networks, Inc.

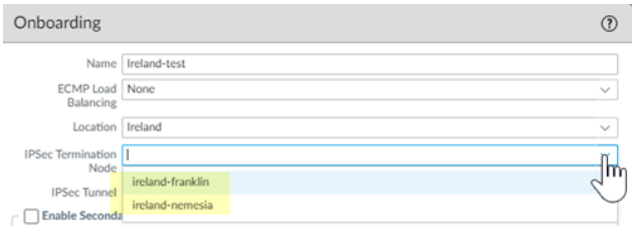
Redes remotas: Nodos de terminación IPSec y direcciones IP de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

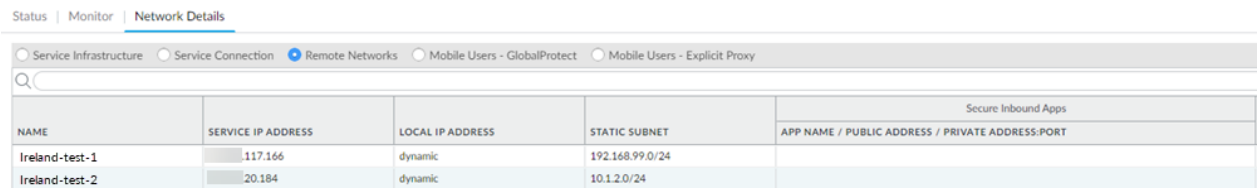
Cuando incorpora una red remota, la asocia con un *nodo de terminación IPSec*, y cada nodo de terminación IPSec tiene una **Service IP Address (Dirección IP de servicio)** asociada a él. Utilice esta dirección como dirección IP de par para su CPE cuando configure el túnel IPSec para la conexión de red remota. Cada nodo de terminación puede proporcionarle hasta 1000 Mbps de ancho de banda. Asociar más de 1000 Mbps de ancho de banda a una ubicación de cómputo le proporciona más de una **Service IP Address (Dirección IP de servicio)**.



Cuando incorpora una red remota en una ubicación de cómputo de Irlanda, tiene la opción de elegir entre dos nodos de terminación IPSec, porque el ancho de banda total es más de 1000 Mbps.



Cada nodo de terminación IPSec tiene su propia **Service IP Address (Dirección IP de servicio)**, como se puede ver en **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)**.



 ©2025 Palo Alto Networks, Inc.

Redes remotas: Cambios de dirección IP relacionados con la asignación de ancho de banda

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Esta sección se aplica si tiene una implementación de Prisma Access heredada que asigna ancho de banda por ubicación. Cualquier implementación nueva asigna ancho de banda por ubicación de cálculo; para obtener información sobre cómo Prisma Access asigna esas direcciones IP, consulte Redes remotas: Nodos de terminación IPSec y direcciones IP de servicio.

Las direcciones IP para conexiones de red remotas son únicas, no compartidas y están dedicadas a la implementación de Prisma Access. Estas direcciones IP no cambian después de que Prisma Access las cree como parte de la incorporación remota a la red, y las direcciones IP persisten después de una actualización. Sin embargo, tenga cuidado al aumentar el ancho de banda de una conexión existente, porque la dirección IP de una red remota puede cambiar si ese aumento hace que el ancho de banda en una ubicación supere los 500 Mbps.

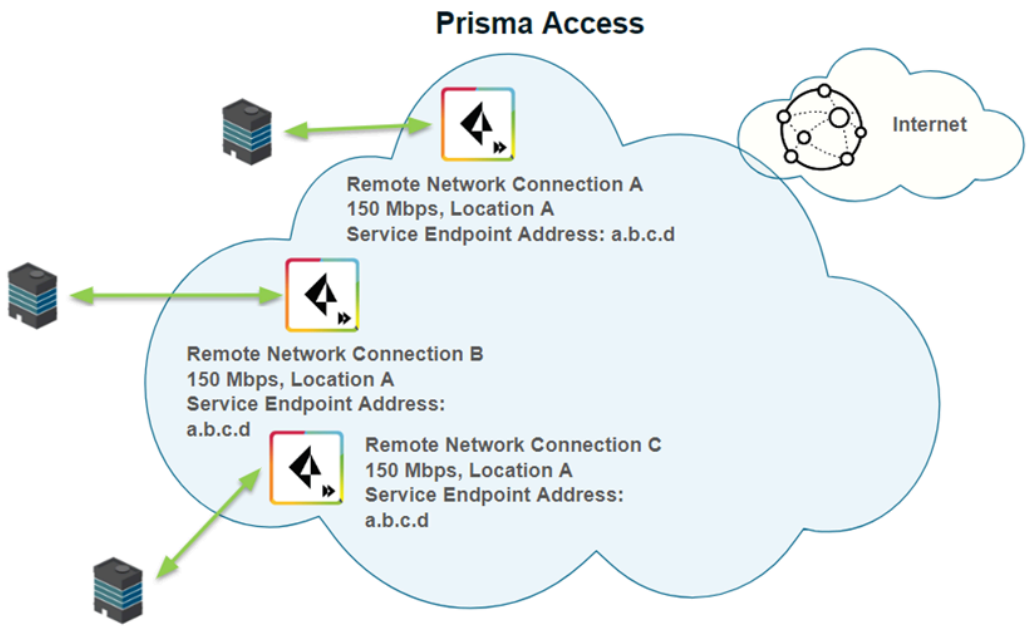
Además, las direcciones IP de salida pueden cambiar si Prisma Access crea una nueva ubicación de cálculo de Prisma Access y decide usar esta nueva ubicación de cálculo con ubicaciones que ya ha incorporado.

Estas directrices de ancho de banda solo se aplican cuando actualiza una conexión existente. Una única conexión de red remota, incluso una conexión de 1000 Mbps (Vista previa), siempre recibe una única **Service IP Address (Dirección IP de servicio)**, independientemente de su tamaño.

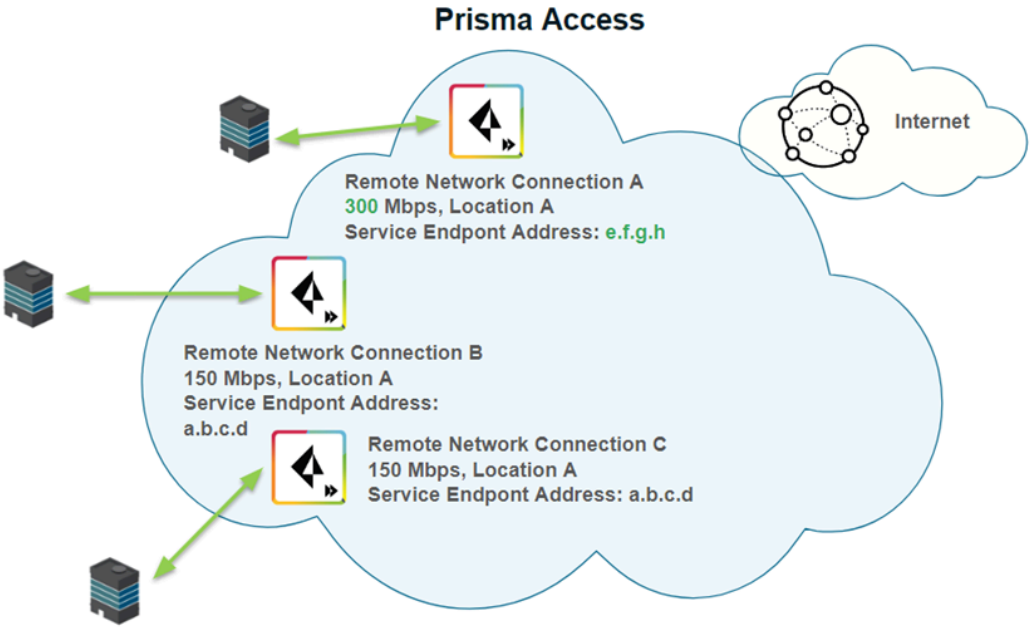
La opción de ancho de banda de 1000 Mbps está en modo de vista previa. El rendimiento durante la vista previa se entrega según el mejor esfuerzo y el rendimiento real variará dependiendo de la combinación de tráfico.

El siguiente ejemplo muestra tres conexiones de red remotas en la misma ubicación, cada una con un ancho de banda de 150 Mbps. Dado que el ancho de banda total es de 500 Mbps, Prisma Access asigna una única dirección IP para todas las conexiones en la ubicación.

 ©2025 Palo Alto Networks, Inc.



El siguiente ejemplo muestra el ancho de banda de la conexión de red remota A que se aumenta de 150 Mbps a 300 Mbps. Dado que el ancho de banda total de todas las conexiones es ahora superior a 500 Mbps, Prisma Access asigna una nueva dirección IP de servicio para la conexión con el ancho de banda adicional. Las demás direcciones IP de servicio permanecen inalteradas.



Por el contrario, dadas cuatro redes remotas con un ancho de banda de 100 Mbps, si aumenta el ancho de banda de una de las redes remotas a 100 Mbps, la **Service IP Address (Dirección IP de servicio)** de esa red remota no cambia porque el ancho de banda total es ahora de 500 Mbps.

 ©2025 Palo Alto Networks, Inc.

*Si reduce el ancho de banda de una conexión de red remota, la **Service IP Address (Dirección IP de servicio)** no cambia.*

Para encontrar las direcciones IP de servicio in Panorama, seleccione la pestaña **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** y haga clic en el botón de radio **Remote Networks (Redes remotas)** para mostrar la **Service IP Address (Dirección de IP de servicio)** para las redes remotas o utilizar la secuencia de comandos de la API.

 ©2025 Palo Alto Networks, Inc.

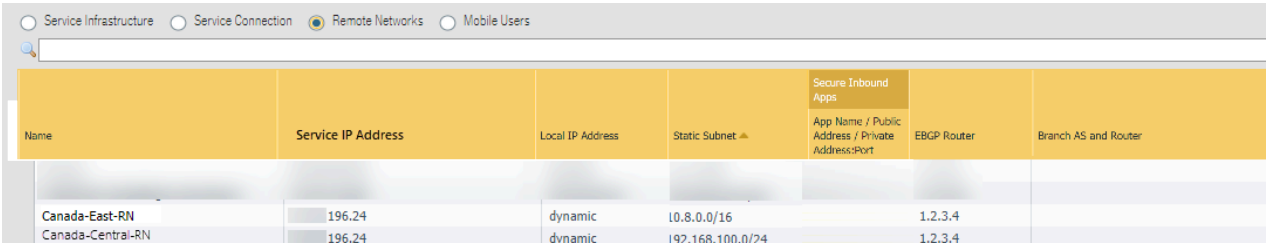
Redes remotas: Dirección IP de servicio y asignación de direcciones IP de salida

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access tiene más de 100 ubicaciones disponibles para acomodar implementaciones en todo el mundo y proporcionar una experiencia localizada. Es posible que dos ubicaciones se asignen a la misma , que se utiliza como dirección IP del mismo nivel al configurar el túnel IPSec para la conexión de red remota. Sin embargo, las ubicaciones pueden usar diferentes direcciones IP de salida para asegurarse de que el usuario obtiene el idioma predeterminado correcto para la región.

Las conexiones de servicio *no admiten la localización de idiomas porque no se admite la salida a Internet a través de conexiones de servicio. Prisma Access asigna solo una dirección IP de servicio, una (ya sea un FQDN o una dirección IP) por conexión de servicio, y esa dirección IP está registrada geográficamente en la* ubicación de cómputo *que corresponde a la ubicación que especifique durante la incorporación.*

En el ejemplo siguiente se muestra una implementación de cliente con dos ubicaciones de red remotas implementadas en Canadá: Canadá Central y Canadá Este. Prisma Access asignó la misma **Service IP Address (Dirección IP del servicio)** a ambas ubicaciones. Al configurar el túnel de red remoto, utilice esta dirección IP como la dirección IP del mismo nivel al crear el túnel IPSec para la conexión de red remota.



Sin embargo, Canadá Este utiliza un idioma predeterminado diferente (francés) que Canadá Central (inglés). Por este motivo, Prisma Access les asigna diferentes direcciones IP de salida. Si ejecuta el script de API para direcciones IP de salida, recibirá dos direcciones IP diferentes para estas dos ubicaciones.

 ©2025 Palo Alto Networks, Inc.

Recuperar las direcciones IP para Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si está añadiendo manualmente direcciones IP de su infraestructura de Prisma Access a una lista de permitidos en su red, o si está utilizando un script de automatización para hacer cumplir restricciones basadas en IP para limitar el acceso entrante a aplicaciones empresariales, debería entender qué hacen estas direcciones y por qué necesita permitirlas, así como las tareas que realiza para recuperarlas.

Prisma Access no proporciona estas direcciones IP hasta que complete su configuración de Prisma Access. Después de que complete su implementación, usted recupera estas direcciones IP utilizando un script de API. El script de API utiliza una clave API que se obtiene de la interfaz de usuario de Prisma Access y un archivo .txt que crea y que especifica las direcciones que desea recuperar.

Si bien no realiza estas tareas hasta que haya completado su configuración de Prisma Access, es útil comprender estos conceptos de antemano, para que sepa qué hacer una vez completada la implementación.

- Strata Cloud Manager
- Panorama

Recuperar las direcciones IP para Prisma Access (Strata Cloud Manager)

Direcciones IP de infraestructura de Prisma Access

La siguiente tabla le proporciona una lista de las direcciones IP que Prisma Access utiliza para cada tipo de implementación, junto con la palabra clave que utiliza cuando ejecuta el script de API para recuperar las direcciones IP y si necesita o no añadirlas a una lista de permitidos.

Tipo de implementación	Tipo de dirección IP:	Descripción
Usuario móvil	Puerta de enlace de Prisma Access (**gp_gateway**)	Recupere las direcciones IP de la puerta de enlace. Añada direcciones IP de puerta de enlace y portal para permitir listas para sus implementaciones de usuarios móviles. Los usuarios móviles se conectan a una puerta de enlace de Prisma Access para

 ©2025 Palo Alto Networks, Inc.

Tipo de implementación	Tipo de dirección IP:	Descripción
		acceder a recursos internos o de internet, como SaaS o aplicaciones públicas, para las cuales ha proporcionado acceso.
	Portal de Prisma Access (**gp_portal**)	Recupera las direcciones IP del portal. Añada direcciones IP de puerta de enlace y portal para permitir listas para sus implementaciones de usuarios móviles. Los usuarios móviles inician sesión en el portal de Prisma Access para recibir su configuración inicial y ubicación de la puerta de enlace.
	Direcciones IP de bucle invertido	Esta dirección es la dirección IP de origen utilizada por Prisma Access para solicitudes realizadas a una fuente interna, y se asigna desde la infraestructura. Añada la dirección IP de bucle invertido a una lista de permitidos en su red para dar Prisma Access a recursos internos como servidores de autenticación RADIUS o Active Directory. Palo Alto Networks recomienda que permita todas las direcciones IP de toda la subred de infraestructura en su red, porque las direcciones de bucle invertido para los usuarios móviles pueden cambiar.
Usuarios móviles: Proxy explícito	Servicio de caché de autenticación (ACS)	La dirección del servicio de Prisma Access que almacena el estado de autenticación de los usuarios de proxy explícito. Esta dirección solo se utiliza para implementaciones de usuario móvil (proxy explícito).
	Equilibrador de carga de red.	La dirección que Prisma Access utiliza para el equilibrador de carga de red de proxy explícito. Esta dirección solo se utiliza para implementaciones de usuario móvil (proxy explícito).
Red remota	Direcciones IP de red remota (**remote_network**)	Incluye **Service IP Addresses (Direcciones IP del servicio)** que Prisma Access asigna para la conexión de red remota de Prisma

 ©2025 Palo Alto Networks, Inc.

Tipo de implementación	Tipo de dirección IP:	Descripción
		Access, y direcciones IP de salida que Prisma Access utiliza para asegurarse de que los usuarios de la red remota obtengan el idioma predeterminado correcto para su región. Añada estas direcciones para permitir listas en su red para dar Prisma Access a los recursos de Internet.
	Direcciones IP de bucle invertido	Esta es la dirección IP de origen utilizada por Prisma Access para las solicitudes realizadas a una fuente interna y se asigna desde la subred de infraestructura. Añada la dirección IP de bucle invertido a una lista de permitidos para dar Prisma Access a recursos internos como servidores de autenticación RADIUS o Active Directory.

Ejecute el script de API utilizado para recuperar direcciones IP

Utilice los siguientes pasos para recuperar las direcciones IP que Prisma Access usa en su infraestructura.

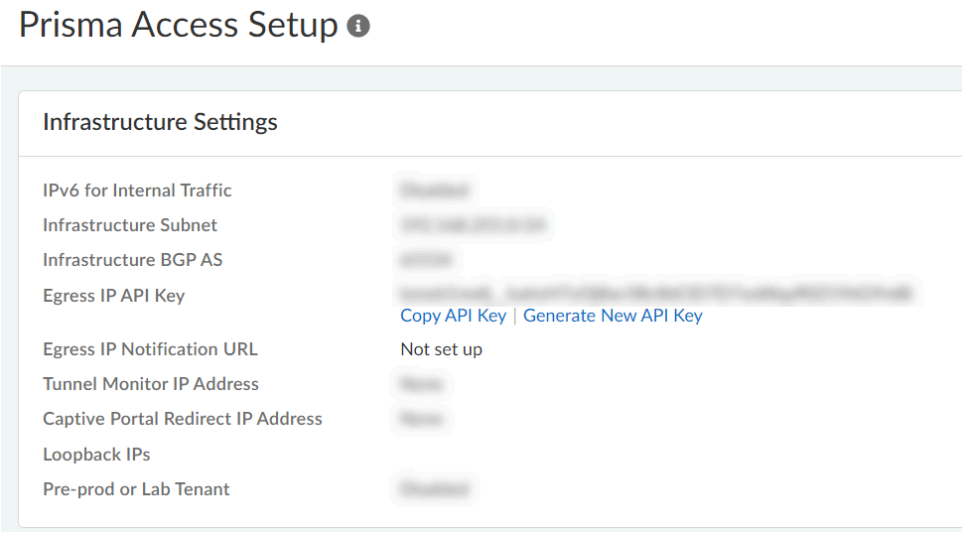
Este comando no recupera direcciones de bucle invertido; para recuperar direcciones IP de bucle invertido, utilice el comando API heredado.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenga la clave de API.

Necesita esta clave para autenticarse con Prisma Access y recuperar la lista de direcciones IP usando el comando API.

1. Vaya a Prisma Access (Managed by Strata Cloud Manager) y seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)**.
2. Seleccione **Generate New API Key (Generar una nueva clave de API)**



Si ya ha generado una clave API, se muestra la clave actual. Si aún no ha generado una clave o quiere reemplazar la clave existente para cumplir con la auditoría o la verificación de cumplimiento para la rotación de claves, haga clic en **Generate New API Key (Generar nueva clave API)** para obtener una nueva clave.

STEP 2 | Cree un archivo .txt y coloque las opciones del comando API en el archivo.

Usando la API, el comando a utilizar es un proceso de dos pasos. Primero, cree un archivo .txt, que especifique los parámetros de las direcciones IP a recuperar y guarde el archivo en una carpeta a la que se pueda acceder desde la ubicación donde ejecuta el comando. Luego, ejecute la API y especifique el nombre y la ubicación del archivo .txt que creó en el comando.

Especifique las siguientes palabras clave y argumentos en el archivo .txt. Los ejemplos en este tema utilizan un nombre de archivo de **options.txt**, pero puede especificar cualquier nombre de archivo, siempre que lo mencione en el comando.

Argumento	Posibles opciones (palabras clave)	Comentarios
tipo de servicio	**todas** **remote_network** **gp_gateway** **gp_portal** **proxy_swg**	**all (todas)**: recupera las direcciones IP que necesita añadir a una lista de permitidos para todos los tipos de servicios (redes remotas, usuarios móviles (tanto puertas de enlace como portales) y Clean Pipe, según corresponda con su implementación).

 ©2025 Palo Alto Networks, Inc.

Argumento	Posibles opciones (palabras clave)	Comentarios
	rbi	**remote_network**: recupera las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de redes remotas. **gp_gateway**: recupera las direcciones IP de puerta de enlace que necesita añadir a una lista de permitidos para implementaciones de usuarios móviles. **gp_portal** : recupera las direcciones IP del portal que necesita añadir a una lista de permitidos para implementaciones de usuarios móviles. **swg_proxy**: recupera las direcciones IP de salida para cada ubicación de proxy explícito implementada, el servicio de caché de autenticación (ACS) y los equilibradores de carga de red. **rbi**: recupera las direcciones IP de salida que necesita añadir a una lista de permitidos para las implementaciones de Aislamiento de navegador remoto (RBI) para conectarse a aplicaciones SaaS.
addrType	**todas** **activa** **service_ip** **auth_cache_service** **network_load_balancer**	**all (todos)** o **active (activo)**: recupera todas las direcciones IP que necesita añadir a una lista de permitidos. Esta API no recupera direcciones IP de bucle invertido. Para recuperar direcciones IP de bucle invertido, utilice el comando de la API heredado. **service_ip**: recupera la **Service IP Address (Dirección IP del servicio)**, que utiliza como la dirección IP del par cuando configura el túnel IPSec para la conexión de red remota. **auth_cache_service**: recupera la dirección IP para el ACS de proxy explícito (aplicable solo a implementaciones de Usuarios móviles: Proxy explícito). **network_load_balancer**: recupera la dirección IP para el equilibrador de carga de red de proxy explícito (aplicable solo a implementaciones de Usuarios móviles: Proxy explícito).

 ©2025 Palo Alto Networks, Inc.

Argumento	Posibles opciones (palabras clave)	Comentarios
tipo de acción	**pre_allocate**	Implementaciones de usuarios móviles únicamente: un **actionType (Tipo de acción)** de **pre_allocate** le permite recuperar direcciones IP o subredes para puertas de enlace y portales de Prisma Access para implementaciones de usuarios móviles. Utilice esto con un **serviceType** de **gp_gateway** para recuperar direcciones IP de puerta de enlace preasignadas y un **serviceType** de **gp_portal** para recuperar direcciones IP de portales preasignadas. Recuperar las direcciones IP preasignadas le permite añadir las direcciones IP de la puerta de enlace y del portal a las listas de permitidos de su organización antes de incorporar las ubicaciones de los usuarios móviles, lo que a su vez proporciona a los usuarios móviles acceso a aplicaciones SaaS externas inmediatamente después de que incorpore las ubicaciones.
ubicación	**todas** **implementado**	**all (todas)**: recupera las direcciones IP de todas las ubicaciones. Para las implementaciones de usuarios móviles, esta palabra clave recupera las direcciones IP de las ubicaciones que añadió durante la incorporación y las ubicaciones que no añadió. **deployed (implementado)**: recupera direcciones IP en todas las ubicaciones que agregó durante la incorporación de usuarios móviles. Esta palabra clave se aplica únicamente a implementaciones de usuarios móviles. Prisma Access asocia direcciones IP para cada ubicación de usuario móvil durante el aprovisionamiento, incluso si no seleccionó esa ubicación durante la incorporación del usuario móvil. Si especifica **all**, el comando API recupera las direcciones IP de todas las ubicaciones de usuarios móviles, incluidas aquellas que no seleccionó para la implementación. Si especifica **deployed (implementado)**, el comando API recupera

 ©2025 Palo Alto Networks, Inc.

Argumento	Posibles opciones (palabras clave)	Comentarios
		solo las direcciones IP de las ubicaciones que seleccionó durante la incorporación.

Especifique las opciones en el archivo .txt en el siguiente formato:

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

STEP 3 | Introduzca el siguiente comando para recuperar las direcciones IP:

- Para utilizar la API más nueva que se introdujo en Prisma Access 2.1, introduzca el siguiente comando:

```
  curl -X POST --data @option.txt -H header-api-key:Current-
API-Key "https://api.prod.datapath.prismaaccess.com/
getPrismaAccessIP/v2"
```

A partir de mayo de 2023, algunas implementaciones gestionadas por la nube utilizan https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 (observe el `prod6` en la URL en lugar de `prod`).

- Para utilizar la API heredada, introduzca el siguiente comando. Este comando utiliza un endpoint de API heredado que quedará obsoleto en mayo de 2022:

```
  curl -X POST --data @option.txt -k -H header-api-key:Current-
API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

Donde *option.txt* es el archivo .txt que creó en un paso anterior y *Current-API-Key* es la clave API de Prisma Access.

Por ejemplo, dado un nombre de archivo .txt de **option.txt** y una clave de API de **12345abcde**, utilice el siguiente comando de API para recuperar la dirección IP pública para todas las ubicaciones:

```
 curl -X POST --data @option.txt -H header-api-key:12345abcde
"https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

El comando API puede devolver una gran cantidad de información. Para que la salida sea más legible, si tiene Python instalado, puede añadir `| python -m json.tool` al final del comando cURL.

El comando API devuelve las direcciones en el siguiente formato:

```
{ "result": [ { "address_details": [ { "address": "1.2.3.4"
"allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

Donde:

- **address_details** muestra los detalles de la dirección de cada ubicación.
  - **serviceType (Tipo de servicio)** muestra el tipo de dirección IP [ya sea red remota (**remote_network**), puerta de enlace de Prisma Access (**gp_gateway**), portal de Prisma Access (**gp_portal**), Clean Pipe (**clean_pipe**) o Aislamiento remoto del navegador (**rbi**].
  - **AddressType (Tipo de dirección)** especifica el tipo de dirección especificado con la palabra clave `addrType` (ya sea **active (activa)** o **pre-allocated (preasignada)** si está preasignando direcciones IP para ubicaciones de usuarios móviles).
  - **address (dirección)** muestra la dirección IP que necesita añadir a sus listas de permitidos.

    Si la API devuelve varias direcciones IP, Prisma Access resume las direcciones IP en el campo **addresses (direcciones)**.
- **addresses (direcciones)** enumera todas las direcciones IP de la ubicación que necesita añadir a sus listas de permitidos.
- **La zona** es la Prisma Access Ubicación asociada a las direcciones IP.
- **zone_subnet** es la subred para portales y puertas de enlace de usuarios móviles. Prisma Access también proporciona esta subred si está preasignando direcciones IP para ubicaciones de usuarios móviles.

Si hay algún problema con las opciones en el archivo .txt, la API devuelve un error similar al siguiente:

```
 {"status": "error","result": "Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

STEP 4 | Actualice las listas de permitidos en sus servidores locales o las reglas de políticas de aplicaciones SaaS con las direcciones IP que recuperó.

Ejemplos de comandos de API

Utilice los siguientes ejemplos al introducir palabras clave y argumentos en el archivo .txt para el comando de API. Para cambiar la salida del comando, cambie las opciones en el archivo .txt; el comando en sí no cambia.

Recuperar estas direcciones IP	Especifique estos parámetros en el archivo .txt	Comentarios
Direcciones IP de usuarios móviles		
Todas las direcciones IP de usuarios móviles	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	Un *addrType* de *all* significa que Prisma Access recupera todas las direcciones IP de las puertas de enlace de usuarios móviles.

 ©2025 Palo Alto Networks, Inc.

Recuperar estas direcciones IP	Especifique estos parámetros en el archivo .txt	Comentarios
		Un *ubicación* de *todas* significa que Prisma Access recupera las direcciones IP de todas las ubicaciones disponibles, incluidas las que no se han incorporado. Prisma Access reserva las direcciones IP de ubicación no incorporadas para que pueda añadir estas direcciones IP a sus listas de permitidos antes de incorporarlas.
Direcciones IP para ubicaciones de usuarios móviles incorporados	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`	Un tipo de *location* de *deployed* significa que Prisma Access recupera solo las direcciones IP de las ubicaciones que seleccionó durante la incorporación del usuario móvil.
Todas las direcciones IP activas para las ubicaciones de los usuarios móviles incorporados	`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }`	Un *addrType* de *active* significa que Prisma Access recupera solo las direcciones IP de las ubicaciones que incorporó.
Direcciones IP de red remota		
Recuperar todas las direcciones IP de red remotas	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	Este comando recupera las direcciones IP públicas y de salida de las redes remotas que ha incorporado. No utilice una *location* de *deployed*. Puede utilizar un *addrType* de *active* pero este recupera las mismas direcciones que si especificara un *addrType* de *all*.
Direcciones IP de proxy explícito		
Recuperar las direcciones IP de ACS para las ubicaciones implementadas	`{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }`	Este comando recupera la dirección IP de ACS para su implementación de proxy explícito. Al introducir un *addrType* de *all* se recuperan todos los tipos de direcciones

 ©2025 Palo Alto Networks, Inc.

Recuperar estas direcciones IP	Especifique estos parámetros en el archivo .txt	Comentarios
		(las direcciones IP del ACS y del equilibrador de carga de red).
Direcciones IP de aislamiento remoto del navegador		
Recupere las direcciones IP de Aislamiento remoto del navegador (RBI) para ubicaciones implementadas	`{ "serviceType": "rbi", "location": "all", "addrType": "all" }`	Este comando recupera las direcciones IP de salida para cada ubicación RBI implementada. Puede añadir estas direcciones IP a una lista de permitidos para conectarse a aplicaciones SaaS.

Scripts heredados utilizados para recuperar direcciones IP y de bucle invertido

La siguiente tabla muestra las palabras clave y los parámetros que están disponibles en los scripts de API heredados utilizados con Prisma Access y proporciona información y recomendaciones sobre qué API utilizar para el tipo de implementación que tiene.

Estos comandos heredados recuperan dos tipos de direcciones IP: *public IP* y direcciones *egress IP* . Le proporcionamos dos comandos API heredados diferentes para que pueda recuperar todas las direcciones IP que necesita añadir a una lista de permitidos.

- Una *public IP address* es la dirección IP de origen que Prisma Access utiliza para solicitudes realizadas a una fuente basada en Internet. Añada la dirección IP pública a una lista de permitidos en su red para proporcionar Prisma Access a recursos de Internet, como aplicaciones SaaS o aplicaciones de socios de acceso público.

  Los usuarios móviles, las redes remotas y las implementaciones de clean pipe utilizan direcciones IP públicas.
- Una *dirección IP de salida* es una dirección IP que Prisma Access utiliza para el tráfico de salida a Internet, y también debe añadir estas direcciones a una lista de permitidos para otorgarle a Prisma Access acceso a los recursos de Internet.

  Entre otros fines, Prisma Access utiliza direcciones IP de salida para que los usuarios reciban páginas web en el idioma que esperan de una ubicación de Prisma Access. Todas

 ©2025 Palo Alto Networks, Inc.

las ubicaciones tienen direcciones IP públicas; sin embargo, no todas las ubicaciones tienen direcciones IP de salida. Las siguientes ubicaciones no utilizan direcciones IP de salida:

- Baréin
- Bélgica
- Francia Norte
- Francia Sur
- Hong Kong
- Irlanda
- Corea del Sur
- Taiwán
- Reino Unido

Los usuarios móviles, las redes remotas y las implementaciones de clean pipe utilizan direcciones IP de salida.

Comandos utilizados en implementaciones de usuarios móviles	
Nombre del comando	**Comentarios**
Comando **get_egress_ip_all=yes** `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes`	Este comando recupera todas las direcciones IP que añade a una lista de permitidos para dar Prisma Access a recursos de Internet, como aplicaciones SaaS o aplicaciones de socios de acceso público. Este comando tiene las siguientes restricciones: • Este comando puede recuperar una gran cantidad de direcciones (más de 200). Si su empresa no puede añadir esta cantidad de direcciones IP a una lista de permitidos, puede usar las palabras clave *gpcs_gp_gw* y *gpcs_gp_portal* para recuperar solo las direcciones IP que está usando actualmente; sin embargo, tendrá que volver a ejecutar estos comandos cada vez que añada una ubicación. Además, si ocurre un evento de escalado, necesitará añadir las nuevas direcciones IP a una lista de permitidos. • Prisma Access no enumera las ubicaciones asociadas con estas direcciones IP; por lo tanto, recomendamos que incluya todas las direcciones IP que se devuelven con este comando en una lista de permitidos. • Este comando no le proporciona direcciones de bucle invertido.
palabra clave **gpcs_gp_gw** and **gpcs_gp_portal** `curl -k -H header-api-key:`*Clave API*	Utilice este comando si su implementación limita el número de direcciones IP que puede añadir a una lista de permitidos. Añada todas las direcciones IP devueltas con este comando a una lista de permitidos en su red. También

 ©2025 Palo Alto Networks, Inc.

Comandos utilizados en implementaciones de usuarios móviles	
Nombre del comando	**Comentarios**
actual"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw | gpcs_gp_portal&addrType=public_ip | egress_ip_list | loopback_ip"	puede recuperar las direcciones IP de bucle invertido con este comando.

Comandos utilizados en implementaciones de redes remotas	
Nombre del comando	**Comentarios**
palabra clave **gpcs_remote_network** curl -k -H header-api-key:*Current-API-Key*"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip | egress_ip_list | loopback_ip"	Utilice este comando para encontrar las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de red remota. También puede utilizar este comando para encontrar las direcciones IP de salida para implementaciones de red remotas; las direcciones IP y de salida pueden ser diferentes en algunas situaciones.

Comandos utilizados en implementaciones de Clean Pipe	
Nombre del comando	**Comentarios**
palabra clave **gpcs_clean_pipe** curl -k -H header-api-key:*Clave API actual*"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip | egress_ip_list | loopback_ip"	Utilice este comando para encontrar las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de clean pipe.

Recuperar direcciones IP públicas y de salida para implementaciones de usuarios móviles

Este script heredado ha sido reemplazado por un script API más nuevo. Palo Alto Networks recomienda que utilice el script más nuevo para recuperar todas las direcciones IP excepto las direcciones de bucle invertido.

Si va a añadir direcciones IP públicas para permitir que las listas de usuarios móviles tengan acceso a SaaS o aplicaciones públicas, Prisma Access proporciona dos direcciones IP para cada puerta de enlace y dirección IP del portal, de modo que se pueda utilizar una dirección IP durante un escalado u otro evento. Puede añadir este conjunto de direcciones IP a una lista de permitidos

 ©2025 Palo Alto Networks, Inc.

antes de usarlas, lo que evita problemas con los usuarios móviles que puedan acceder a SaaS o aplicaciones públicas durante un evento de escalado.

Recupere estas nuevas direcciones completando la siguiente tarea:

STEP 1 | Obtenga la clave API seleccionando **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)** > **Generate New API Key (Generar nueva clave API)**.

Necesita esta clave para autenticarse en Prisma Access y recuperar la lista de direcciones IP utilizando el comando cURL que aparece a continuación. Sólo un administrador o superusuario de Panorama puede generar o acceder a esta clave API.

STEP 2 | Introduzca el siguiente comando para recuperar las direcciones IP públicas de los usuarios móviles:

```
  curl -k -H header-api-key:Current-API-Key "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

Donde *Current-API-Key* es la Clave API de Prisma Access.

Por ejemplo, dada una clave API de **12345abcde**, utilice el siguiente comando API para recuperar la dirección IP pública de todas las ubicaciones:

```
  curl -k -H header-api-key:12345abcde "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

Recuperar direcciones IP públicas, de bucle invertido y de salida

Para recuperar direcciones IP públicas, de bucle invertido y de salida, complete los siguientes pasos.

STEP 1 | Recupere las direcciones IP públicas, las direcciones IP de bucle invertido o ambas para Prisma Access.

Utilice la clave API y la URL del endpoint de la API de forma manual o en un script de automatización:

```
 header-api-key:Current API Key"https://api.gpcloudservice.com/
getAddrList/latest?fwType=$fwType&addrType=$addrType"
```

Donde debe reemplazar la Clave API actual con su clave API y usar una o ambas de las siguientes palabras clave y argumentos:

Palabra clave	Descripción
fwType palabra clave	
gpcs_gp_gw	Recupera direcciones IP de puerta de enlace (para implementaciones de usuarios móviles) dePrisma Access.

 ©2025 Palo Alto Networks, Inc.

Palabra clave	Descripción
gpcs_gp_portal	Recupera direcciones IP del portal (para implementaciones de usuarios móviles) de Prisma Access.
gpcs_remote_network	Recupera direcciones IP de red remota (para implementaciones de red remota) dePrisma Access.
gpcs_clean_pipe	Recupera direcciones IP de Clean Pipe de Prisma Access.
addrType palabra clave	
public_ip	. Recupera las direcciones IP de origen que Prisma Access utiliza para las solicitudes realizadas a una fuente basada en Internet. Para ubicaciones de usuarios móviles, Prisma Access enumera las direcciones IP por ubicación. Para redes remotas, Prisma Access enumera las direcciones IP por nombre de red remota.
egress_ip_list	Recupera las direcciones IP que Prisma Access utiliza con direcciones IP públicas para tráfico de salida adicional a Internet. Para ubicaciones de usuarios móviles, Prisma Access enumera las direcciones IP por ubicación. Para redes remotas, Prisma Access enumera las direcciones IP por nombre de red remota.
loopback_ip	Recupera las direcciones IP de origen utilizadas por Prisma Access para las solicitudes realizadas a una fuente interna (por ejemplo, un servidor RADIUS o Active Directory) y se asigna desde la subred de infraestructura.

Si no especifica una palabra clave, Prisma Access recupera todas las direcciones IP.

Por ejemplo, puede probar el siguiente comando Curl para recuperar manualmente la lista de direcciones IP públicas de todas las redes remotas:

```
curl -k -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

O utilice un script de Python simple para recuperar la lista de todas las direcciones IP, por ejemplo:

```
  #!/usr/bin/python import subprocess import json api_key =
 '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7' # Replace
 with your key api_end_point = 'https://api.gpcloudservice.com/
getAddrList/latest' # This call retrieves IP addresses
 for all your Prisma Access firewalls args = ['curl', '-
k', '-H', 'header-api-key:' + api_key, api_end_point] p =
 subprocess.Popen(args, stdout=subprocess.PIPE) output =
```

 ©2025 Palo Alto Networks, Inc.

```
p.communicate() dout = json.loads(output[0]) addrStrList
= dout['result']['addrList'] addrList = [] for addr_str
in addrStrList: addrList.append(addr_str.split(":")[1])
print(addrList)
```

STEP 2 | Actualice las listas de permitidos en sus servidores locales o las reglas de políticas de aplicaciones SaaS con las direcciones IP que recuperó.

Preasignar direcciones IP para ubicaciones de usuarios móviles

Prisma Access utiliza direcciones IP de puerta de enlace y portal para implementaciones de Usuarios móviles: GlobalProtect, y el servicio de caché de autenticación (ACS) y las direcciones IP del equilibrador de carga de red para implementaciones de Usuarios móviles: Proxy explícito. Las direcciones IP de Usuarios móviles: GlobalProtect se conocen como *egress IP addresses*.
Si necesita asignar previamente direcciones IP de usuarios móviles antes de incorporar la ubicación (por ejemplo, si su organización necesita añadir las direcciones IP para usuarios móviles: implementaciones de GlobalProtect para permitir listas para brindar a los usuarios móviles acceso a aplicaciones SaaS externas), puede ejecutar un script de la API para que Prisma Access asigne previamente estas direcciones IP para una ubicación con anticipación, antes de incorporarla. Luego, puede añadir las direcciones IP de salida de la ubicación a las listas de permitidos de su organización antes de incorporar la ubicación.

La respuesta de la API también incluye las subredes del grupo de IP públicas para las direcciones IP de salida de la ubicación solicitada. Las direcciones IP de salida de cualquier ubicación que añade son parte de esta subred. Añadir las subredes a sus listas de permitidos permite futuras incorporaciones de ubicaciones sin necesidad de realizar más modificaciones a las listas de permitidos.

Prisma Access no preasigna sus direcciones IP y subredes a menos que las solicite mediante el script de API. Después de ejecutar el script de preasignación, estos tienen un período de validez de 90 días. Estas direcciones IP y subredes son únicas, no se comparten y están dedicadas a su implementación de Prisma Access durante el período de validez. Debe incorporar sus ubicaciones antes de que finalice el período de validez o perderá las direcciones; para encontrar el período de validez en cualquier momento, ejecute el script API.

Palo Alto Networks recomienda que solo preasigne direcciones IP para las ubicaciones que desee incorporar más adelante.

Para preasignar direcciones IP, complete la siguiente tarea.

STEP 1 | Recuperar la Clave API de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Asigne previamente las direcciones IP de salida de los usuarios móviles creando un archivo .txt y especificando las siguientes opciones en el archivo .txt que cree.

Introduzca el siguiente texto en el archivo .txt:

- **Implementaciones de Usuarios móviles: GlobalProtect:**

```
 { "actionType": "pre_allocate", "serviceType": "gp_gateway",
"location": ["location"] }
```

- **Implementaciones de Usuarios móviles: Proxy explícito:**

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["location"]}
```

¿Dónde *location* es la ubicación de Prisma Access donde desea preasignar las direcciones IP.

Introduzca un máximo de 12 entradas. Introducir más de 12 ubicaciones puede causar errores de tiempo de espera cuando Prisma Access recupera las direcciones IP preasignadas.

STEP 3 | Introduzca este comando CURL.

STEP 4 | Recupere las direcciones IP y subredes que solicitó, incluido su período de validez, reabriendo el archivo .txt, eliminando la información existente y editándolo.

- **Implementaciones de Usuarios móviles: GlobalProtect:**
  - Para solicitar a Prisma Access que recupere todas las direcciones IP preasignadas, introduzca el siguiente texto en el archivo .txt.

```
 { "serviceType": "all", "addrType": "pre_allocated",
"location": "all" }
```

  - Para solicitar a Prisma Access que recupere todas las direcciones IP preasignadas para puertas de enlace de Prisma Access para una ubicación determinada, introduzca la

 ©2025 Palo Alto Networks, Inc.

misma información en el archivo .txt pero sustituya “`all`” con “`gp_gateway`” en el archivo .txt.

- Para solicitar a Prisma Access que recupere todas las direcciones IP preasignadas para portales de Prisma Access para una ubicación determinada, introduzca la misma información en el archivo .txt pero sustituya “`all`” con “`gp_portal`” en el archivo .txt.

- **Implementaciones de Usuarios móviles: Proxy explícito:**

  Para solicitar que Prisma Access preasigne todas las direcciones IP que necesita añadir a las listas de permitidos para una implementación de proxy explícito, introduzca el siguiente texto en el archivo .txt.

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["all"] }
```

Palo Alto Networks recomienda que introduzca `all` para poder recuperar todas las direcciones IP de salida preasignadas necesarias para añadirlas a sus listas de permitidos.

Para implementaciones de Usuarios móviles: GlobalProtect, el comando API puede devolver una gran cantidad de información. Para que la salida sea más legible, si tiene Python instalado, puede añadir | `python -m json.tool` al final del comando cURL.

STEP 5 | Vuelva a introducir este comando CURL para recuperar las direcciones preasignadas.

Prisma Access devuelve la información en el siguiente formato:

```
    "result": [ { "zone": "prisma-access-zone1", "addresses":
 [ ["ip-address1","ip-address2"] "zone_subnet" : [subnet-and-
mask1","subnet-and-mask2"] "address_details":[ {"address":"ip-
address1", "service_type":"service-type", "addressType":"pre-
allocated", "expiring_in" : "validity-period" }, {"address":"ip-
address2", "service_type":"gp_gateway", "addressType":"pre-
allocated", "validity_period_remaining" : "90 days" } , },
```

Donde las variables representan la siguiente salida del comando de API:

Variable	Explicación
prisma-access-zone1	La ubicación de Prisma Access para la que se recuperaron direcciones IP preasignadas.
dirección ip1 y *dirección ip2*	Las direcciones IP de salida que Prisma Access ha preasignado para la ubicación especificada. Prisma Access recupera dos direcciones IP para cada ubicación; debe añadir ambas direcciones IP a sus listas de permitidos.

 ©2025 Palo Alto Networks, Inc.

Variable	Explicación
subred-y-máscara1 y *subred-y-máscara2*	Las subredes que Prisma Access ha preasignado y reservado para las direcciones IP de salida en su implementación.
service-type	El tipo de dirección IP de salida preasignada (`gp_portal` para un portal de Prisma Access o `gp_gateway` para una puerta de enlace de Prisma Access).
periodo de validez	El tiempo restante, en días, durante el cual la dirección IP preasignada es válida. Incorpore la ubicación de su usuario móvil antes de que finalice el período de validez de las direcciones IP. Si las direcciones IP preasignadas caducan, puede volver a ejecutar el script de API para recuperar otro conjunto de direcciones IP preasignadas.

Podría recibir un error si intenta preasignar direcciones IP para ubicaciones que cumplan con uno de los siguientes criterios:

- Ya ha incorporado la ubicación.
- Ya incorporó y luego eliminó la ubicación.

  En este caso, introduzca el siguiente texto en el archivo .txt para recuperar las direcciones IP de Usuarios móviles: GlobalProtect para la ubicación:

```
 { "serviceType": "gp_gateway", "addrType": "all", "location":
"all" }
```

- Ha alcanzado el número máximo de ubicaciones de usuarios móviles permitidas por su licencia y no puede añadir más ubicaciones.
- Introdujo el nombre de la ubicación incorrectamente.
- Introdujo un **serviceType** distinto de **gp_gateway**.
- Introdujo un **actionType** distinto de **pre_allocate**.

Configurar notificaciones de cambio de dirección IP de Prisma Access

Para recibir notificaciones sobre cambios de direcciones IP públicas para redes remotas y cambios de direcciones IP de bucle invertido para conexiones de servicio, conexiones de redes remotas y usuarios móviles, puede especificar una URL en la que pueda recibir alertas sobre un cambio. Prisma Access utiliza una solicitud HTTP POST para enviar la notificación. Esta solicitud POST incluye los siguientes datos de notificación en formato JSON:

 ©2025 Palo Alto Networks, Inc.

```
 {"addrType": "public_ip", "addrChangeType": "add", "utc_timestamp":
"2019-01-31 23:08:19.383894", "text": "Address List Change
Notification"}
```

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp": "2019-01-31 23:13:35.882151", "text": "Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp": "2019-01-31 23:29:27.100329", "text": "2018-05-11
23:29:27.100329"}
```

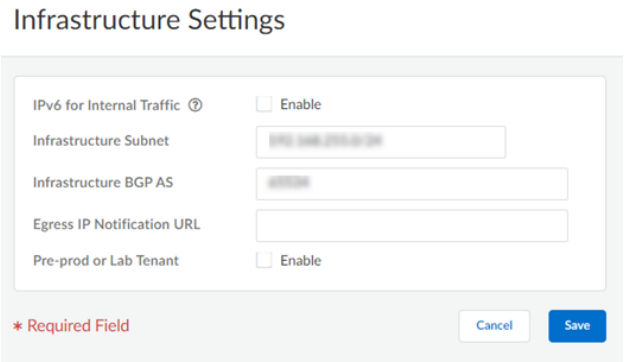
Cuando reciba una notificación, debe seguir un proceso de dos pasos. Primero, debe recuperar de forma manual o programática las direcciones IP o de bucle invertido. A continuación, debe actualizar las direcciones IP de la lista de permitidos adecuada de su organización para asegurarse de que los usuarios no experimenten ninguna interrupción en el servicio.

Prisma Access envía esta notificación unos segundos antes de que la nueva dirección IP se active. Le recomendamos que utilice scripts de automatización para recuperar y añadir las nuevas direcciones IP a una lista de permitidos en su red.

Para añadir una URL de notificación de IP, complete la siguiente tarea.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Configuration (Configuración)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)**.

STEP 2 | Añada una **Egress IP Notification URL (URL de notificación de IP de salida)** donde pueda recibir notificaciones de cambios de dirección IP en su infraestructura de Prisma Access.



Puede especificar una dirección IP o un FQDN para un servicio web HTTP o HTTPS que esté escuchando notificaciones de cambio. Prisma Access envía estas notificaciones desde Internet utilizando una dirección IP pública.

No es necesario enviar su configuración para que la URL de notificación surta efecto.

Recuperar las direcciones IP para Prisma Access (Panorama)

Si está añadiendo manualmente direcciones IP de su infraestructura de Prisma Access a una lista de permitidos en su red, o si está utilizando un script de automatización para hacer cumplir

 ©2025 Palo Alto Networks, Inc.

restricciones basadas en IP para limitar el acceso entrante a aplicaciones empresariales, debería entender qué hacen estas direcciones y por qué necesita permitirlas, así como las tareas que realiza para recuperarlas.

Prisma Access no aprovisiona estas direcciones IP hasta que complete su configuración de Prisma Access. Después de que complete su implementación, usted recupera estas direcciones IP utilizando un script de API. El script de API utiliza una clave API que se obtiene de la interfaz de usuario de Prisma Access y un archivo .txt que crea y que especifica las direcciones que desea recuperar.

Si tiene una implementación de Usuarios móviles: GlobalProtect, puede usar el UI de Prisma Access en lugar de esta API para gestionar la asignación de direcciones IP públicas y confirmar que las direcciones IP se han añadido a sus listas de permitidos antes de que Prisma Access libere las direcciones IP. De este modo, Prisma Access solo aprovisiona las direcciones IP que usted haya permitido en la lista.

La siguiente tabla le proporciona una lista de las direcciones IP que Prisma Access utiliza para cada tipo de implementación, junto con la palabra clave que usa cuando ejecuta el script de la API para recuperar las direcciones IP, y describe si debe o no añadirlas a las listas de permitidos de su organización.

Tipo de implementación	Tipo de dirección IP:	Descripción
Usuarios móviles: GlobalProtect	Puerta de enlace de Prisma Access (**gp_gateway**)	Direcciones IP de puerta de enlace Debe añadir las direcciones IP de la puerta de enlace y del portal a las listas de permitidos para sus implementaciones de usuarios móviles. Los usuarios móviles se conectan a una puerta de enlace de Prisma Access para acceder a recursos internos o de internet, como SaaS o aplicaciones públicas, para las cuales ha proporcionado acceso. Para los usuarios móviles, durante la implementación inicial, Prisma Access asigna dos direcciones IP para cada ubicación que implementa.
	Portal de Prisma Access (**gp_portal**)	Direcciones IP del portal. Debe añadir las direcciones IP de la puerta de enlace y del portal a las listas de permitidos para sus

 ©2025 Palo Alto Networks, Inc.

Tipo de implementación	Tipo de dirección IP:	Descripción
		implementaciones de usuarios móviles. Los usuarios móviles inician sesión en el portal de Prisma Access para recibir su configuración inicial y ubicación de la puerta de enlace.
	Direcciones IP de bucle invertido	La dirección IP de origen utilizada por Prisma Access para las solicitudes realizadas a una fuente interna, y se asigna desde Configure la Infraestructura de servicios de Prisma Access (Panorama). Añada la dirección IP de bucle invertido a una lista de permitidos en su red para dar Prisma Access a recursos internos como servidores de autenticación RADIUS o Active Directory. Palo Alto Networks recomienda que permita todas las direcciones IP de toda la subred de infraestructura en su red, porque las direcciones IP de bucle invertido pueden cambiar. Para encontrar la subred de infraestructura **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Infrastructure (Infraestructura de servicios)**. La subred se muestra en el área de **Infrastructure Subnet (Subred de infraestructura)**. Para recuperar direcciones IP de bucle invertido, utilice el script de la API heredada.
Usuarios móviles: Proxy explícito	Servicio de caché de autenticación (ACS)	La dirección del servicio de Prisma Access que almacena

 ©2025 Palo Alto Networks, Inc.

Tipo de implementación	Tipo de dirección IP:	Descripción
		el estado de autenticación de los usuarios de proxy explícito. Esta dirección solo se utiliza para proxy explícito para usuarios móviles.
	Equilibrador de carga de red.	La dirección que Prisma Access utiliza para el equilibrador de carga de red de proxy explícito. Esta dirección solo se utiliza para proxy explícito para usuarios móviles.
Red remota	Direcciones IP de red remota (**remote_network**)	Las **Service IP Addresses (Direcciones IP del servicio)** que Prisma Access asigna para la conexión de red remota de Prisma Access, y Redes remotas: Dirección IP de servicio y asignación de direcciones IP de salida que Prisma Access utiliza para asegurarse de que los usuarios de la red remota obtengan el idioma predeterminado correcto para su región. Añada estas direcciones para permitir listas en su red para dar Prisma Access a los recursos de Internet.
	Direcciones IP de bucle invertido	La dirección IP de origen utilizada por Prisma Access para las solicitudes realizadas a una fuente interna, y se asigna desde Configure la Infraestructura de servicios de Prisma Access (Panorama). Añada la dirección IP de bucle invertido a una lista de permitidos para dar Prisma Access a recursos internos como servidores de autenticación RADIUS o Active Directory. Para recuperar direcciones IP de

 ©2025 Palo Alto Networks, Inc.

Tipo de implementación	Tipo de dirección IP:	Descripción
		bucle invertido, utilice el script de la API heredada.
Clean Pipe	Direcciones IP de Clean Pipe (**clean_pipe**)	Añada estas direcciones IP a una lista de permitidos para dar acceso al servicio Clean Pipe a los recursos de internet.
	Direcciones IP de bucle invertido	La dirección IP de origen utilizada por Prisma Access para las solicitudes realizadas a una fuente interna, y se asigna desde Configure la Infraestructura de servicios de Prisma Access (Panorama). Añada la dirección IP de bucle invertido a una lista de permitidos para dar Prisma Access a recursos internos como servidores de autenticación RADIUS o Active Directory. Para recuperar direcciones IP de bucle invertido, utilice el script de la API heredada.

Ejecutar el script de API utilizado para recuperar direcciones IP de Prisma Access

Prisma Access proporciona un script de API que puede usar para recuperar las direcciones IP públicas y privadas que utiliza en su infraestructura. Si necesita añadir direcciones IP públicas a las listas de permitidos en la red de su organización, utilice los siguientes pasos para recuperar estas direcciones IP con el script de API.

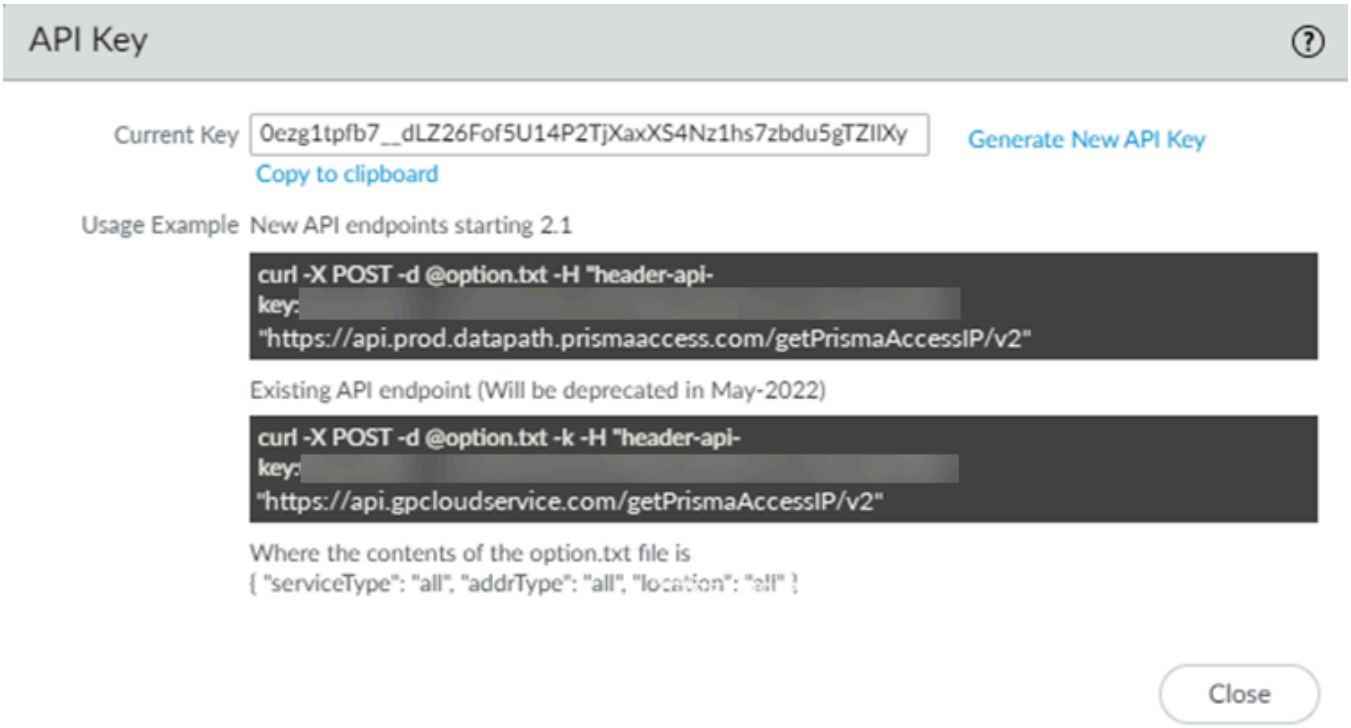
Este comando no recupera direcciones de bucle invertido; para recuperar direcciones IP de bucle invertido, utilice la API heredada.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenga la clave de API.

Necesita esta clave para autenticarse con Prisma Access y recuperar la lista de direcciones IP usando el comando API. Solo un administrador de Panorama o un superusuario pueden generar o acceder a esta clave API.

1. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.
2. Seleccione **Generate API Key (Generar clave de API)**.



Si ya ha generado una clave API, se muestra la **Current Key (Clave actual)**. Si aún no ha generado una clave o quiere reemplazar la clave existente para cumplir con la auditoría o la verificación de cumplimiento para la rotación de claves, haga clic en **Generate New API Key (Generar nueva clave API)** para obtener una nueva clave.

STEP 2 | Cree un archivo .txt y coloque las opciones del comando API en el archivo.

Usando la API, el comando a utilizar es un proceso de dos pasos. Primero, cree un archivo .txt, que especifique los parámetros de las direcciones IP a recuperar y guarde el archivo en una carpeta a la que se pueda acceder desde la ubicación donde ejecuta el comando. Luego, ejecute la API y especifique el nombre y la ubicación del archivo .txt que creó en el comando.

Especifique las siguientes palabras clave y argumentos en el archivo .txt. Ver Ejemplos de API para recuperar direcciones IP de Prisma Access para ver ejemplos. Los ejemplos en este

 ©2025 Palo Alto Networks, Inc.

documento utilizan un nombre de archivo de **options.txt**, pero puede especificar cualquier nombre de archivo, siempre que lo mencione en el comando.

Argumento	Posibles opciones (palabras clave)	Comentarios
tipo de servicio	**todas** **remote_network** **gp_gateway** **gp_portal** **clean_pipe** **proxy_swg** **rbi**	**all (todas)**: recupera las direcciones IP que necesita añadir a una lista de permitidos para todos los tipos de servicios (redes remotas, usuarios móviles (tanto puertas de enlace como portales) y Clean Pipe, según corresponda con su implementación). **remote_network**: recupera las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de redes remotas. **gp_gateway**: recupera las direcciones IP de la puerta de enlace de GlobalProtect para usuarios móviles que necesita añadir a una lista de permitidos para implementaciones de usuarios móviles. **gp_portal**: recupera las direcciones IP del portal de Usuarios móviles: GlobalProtect que necesita añadir a una lista de permitidos para implementaciones de usuarios móviles. **clean_pipe**: recupera las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de clean pipe. **swg_proxy**: recupera las direcciones IP de salida para cada ubicación de proxy

 ©2025 Palo Alto Networks, Inc.

Argumento	Posibles opciones (palabras clave)	Comentarios
		explícito implementada, el servicio de caché de autenticación (ACS) y los equilibradores de carga de red. **rbi**: recupera las direcciones IP de salida que necesita añadir a una lista de permitidos para las implementaciones de Aislamiento de navegador remoto (RBI) para conectarse a aplicaciones SaaS.
addrType	**todas** **activa** **service_ip** **auth_cache_service** **network_load_balancer**	**all (todos)** o **active (activo)**: recupera todas las direcciones IP que necesita añadir a una lista de permitidos. Esta API no recupera direcciones IP de bucle invertido. Para recuperar direcciones IP de bucle invertido, utilice la API heredada. **service_ip**: recupera la **Service IP Address (Dirección IP del servicio)**, que utiliza como la dirección IP del par cuando configura el túnel IPSec para la conexión de red remota. **servicio_cache_auth**: recupera la dirección IP para el proxy explícito ACS (aplicable solo a implementaciones de Proxy Explícito). **network_load_balancer**: recupera la dirección IP para el equilibrador de carga de red de proxy explícito (aplicable solo a implementaciones de Proxy explícito).
tipo de acción	**pre_allocate**	Implementaciones de usuarios móviles únicamente: un **actionType (Tipo de acción)** de **pre_allocate** le permite recuperar direcciones IP o

 ©2025 Palo Alto Networks, Inc.

Argumento	Posibles opciones (palabras clave)	Comentarios
		subredes para puertas de enlace y portales de Prisma Access para implementaciones de usuarios móviles. Utilice esto con un **serviceType (Tipo de servicio)** de **gp_gateway** para recuperar direcciones IP de puerta de enlace preasignadas y un **serviceType (Tipo de servicio)** de **gp_portal** para recuperar direcciones IP de portal preasignadas. Recuperar las direcciones IP preasignadas le permite añadir las direcciones IP de la puerta de enlace y del portal a las listas de permitidos de su organización antes de incorporar las ubicaciones de los usuarios móviles, lo que a su vez proporciona a los usuarios móviles acceso a aplicaciones SaaS externas inmediatamente después de que incorpore las ubicaciones.
ubicación	**todas** **implementado**	**all (todas)**: recupera las direcciones IP de todas las ubicaciones. Para las implementaciones de usuarios móviles, esta palabra clave recupera las direcciones IP de las ubicaciones que añadió durante la incorporación y las ubicaciones que no añadió. **deployed (implementado)**: recupera direcciones IP en todas las ubicaciones que agregó durante la incorporación de usuarios móviles. Esta palabra clave se aplica únicamente a implementaciones de usuarios móviles. Prisma Access asocia direcciones IP para cada

 ©2025 Palo Alto Networks, Inc.

Argumento	Posibles opciones (palabras clave)	Comentarios
		ubicación de usuario móvil durante el aprovisionamiento, incluso si no seleccionó esa ubicación durante la incorporación del usuario móvil. Si especifica **all**, el comando API recupera las direcciones IP de todas las ubicaciones de usuarios móviles, incluidas aquellas que no seleccionó para la implementación. Si especifica **deployed (implementado)**, el comando API recupera solo las direcciones IP de las ubicaciones que seleccionó durante la incorporación.

Especifique las opciones en el archivo .txt en el siguiente formato:

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Introduzca el siguiente comando para recuperar las direcciones IP:

- Para utilizar la API más nueva que se introdujo en Prisma Access 2.1, introduzca el siguiente comando:

```
curl -X POST --data @option.txt -H header-api-key:Current-API-Key "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

A partir de mayo de 2023, algunas implementaciones gestionadas por Panorama utilizan https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 (observe el `prod6` en la URL en lugar de `prod`).

- Para utilizar la API heredada, introduzca el siguiente comando. Este comando utiliza un endpoint de API heredado que quedará obsoleto en mayo de 2022:

```
curl -X POST --data @option.txt -k -H header-api-key:Current-API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

Donde *option.txt* es el archivo .txt que creó en un paso anterior y *Current-API-Key* es la clave API de Prisma Access.

Por ejemplo, dado un nombre de archivo .txt de **option.txt** y una clave de API de **12345abcde**, utilice el siguiente comando de API para recuperar la dirección IP pública para todas las ubicaciones:

```
curl -X POST --data @option.txt -H header-api-key:12345abcde "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

El comando API puede devolver una gran cantidad de información. Para que la salida sea más legible, si tiene Python instalado, puede añadir `| python -m json.tool` al final del comando cURL.

El comando API devuelve las direcciones en el siguiente formato:

```
{ "result": [ { "address_details": [ { "address": "1.2.3.4" "allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

Donde:

- **address_details** muestra los detalles de la dirección de cada ubicación.
  - **serviceType (Tipo de servicio)** muestra el tipo de dirección IP [ya sea red remota (**remote_network**), puerta de enlace de Prisma Access (**gp_gateway**), portal de Prisma Access (**gp_portal**), Clean Pipe (**clean_pipe**) o Aislamiento remoto del navegador (**rbi**].
  - **AddressType (Tipo de dirección)** especifica el tipo de dirección especificado con la palabra clave `addrType` (ya sea **active (activa)** o **pre-allocated (preasignada)** si está preasignando direcciones IP para ubicaciones de usuarios móviles).
  - **address (dirección)** muestra la dirección IP que necesita añadir a sus listas de permitidos.

    Si la API devuelve varias direcciones IP, Prisma Access resume las direcciones IP en el campo **addresses (direcciones)**.
- **addresses (direcciones)** enumera todas las direcciones IP de la ubicación que necesita añadir a sus listas de permitidos.
- **La zona** es la Prisma Access Ubicación asociada a las direcciones IP.
- **zone_subnet** es la subred para portales y puertas de enlace de usuarios móviles. Prisma Access también proporciona esta subred si está preasignando direcciones IP para ubicaciones de usuarios móviles.

Si hay algún problema con las opciones en el archivo .txt, la API devuelve un error similar al siguiente:

```
 {"status": "error","result": "Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

STEP 4 | Actualice las listas de permitidos en sus servidores locales o las reglas de políticas de aplicaciones SaaS con las direcciones IP que recuperó.

Optimización de IP para las implementaciones de Usuarios móviles: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Licencia de Prisma Access • Prisma Access versión 5.0 o posterior

La optimización de direcciones IP es un conjunto de mejoras de la arquitectura que reducen el número total de direcciones IP en la implementación, lo que simplifica los flujos de trabajo de listas de permitidos, al tiempo que mejora la resiliencia y permite una incorporación más rápida de los inquilinos de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

- **Lista de permitidos de direcciones IP públicas más sencilla para implementaciones de Usuarios móviles: GlobalProtect**: añadir una ubicación de Prisma Access o experimentar un evento de escalado en una ubicación de Prisma Access existente podría hacer que se asignen nuevas direcciones IP al nodo de procesamiento de seguridad de usuario móvil (MU-SPN). Es una práctica recomendada recuperar las nuevas direcciones IP de salida y puerta de enlace que Prisma Access asigna y añadirlas a una lista de permisos en su red para evitar la interrupción de la aplicación SaaS o el cortafuegos corporativo. Esto puede resultar en una situación en la que esté gestionando un gran número de direcciones IP. La optimización de IP reduce el número de direcciones IP que debe gestionar.
- **Incorporación más rápida de inquilinos de Prisma Access**: sin optimización de IP, necesitaría asignar direcciones IP privadas únicas a cada dispositivo en todo el Prisma Access y sus redes privadas, lo que le requeriría asignar grandes bloques de IP desde su limitado espacio de direcciones IP enrutable corporativas. La optimización de IP permite a Prisma Access asignar direcciones de un espacio de direcciones compartido de forma predeterminada y tráfico de aplicaciones privadas de NAT.



La optimización de IP es solo para las nuevas implementaciones de Prisma Access GlobalProtect. Las implementaciones existentes de GlobalProtect no son elegibles, incluidos los nuevos inquilinos que cree a partir de una implementación multiinquilino existente. Además, si migra su implementación de GlobalProtect de usar portales y puertas de enlace locales a Prisma Access, asegúrese de que todos los usuarios ejecutan una versión de aplicación de GlobalProtect de 6.1.4 y posterior, 6.2.3 y posterior o 6.3.0 y posterior antes de habilitar esta funcionalidad.

Tome nota de los siguientes requisitos adicionales para la optimización de IP:

- *La optimización de IP requiere Prisma Access 5.0 o posterior para la optimización de usuarios móviles , y se puede habilitar cuando se configura GlobalProtect por primera vez.*
- *Cuando configure GlobalProtect por primera vez, se le preguntará si desea habilitar o no la optimización IP de Prisma Access.*
- *Las implementaciones de optimización de IP no admiten IPv6 para el acceso a aplicaciones públicas (externas); el acceso a aplicaciones privadas es compatible. Para habilitar IPv6 para su nueva implementación de Prisma Access, póngase en contacto con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de TAC para encargarse de la solicitud.*
- *La API para recuperar direcciones IP de Prisma Access sigue funcionando como siempre, incluso con la optimización de IP habilitada.*

 ©2025 Palo Alto Networks, Inc.

Ejemplos de API para recuperar direcciones IP de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Utilice los siguientes ejemplos al introducir palabras clave y argumentos en el archivo de .txt para que el comando de la API recupere las direcciones IP de la infraestructura. Para cambiar la salida del comando, cambie las opciones en el archivo .txt; el comando en sí no cambia.

Recuperar estas direcciones IP	Especifique estos parámetros en el archivo .txt	Comentarios
Direcciones IP de usuarios móviles		
Todas las direcciones IP de usuarios móviles	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	Un *addrType* de *todo* significa que Prisma Access recupera todas las direcciones IP de las ubicaciones seleccionadas Configurar usuarios móviles de GlobalProtect (Panorama). Un *ubicación* de *todas* significa que Prisma Access recupera las direcciones IP de todas las ubicaciones disponibles, incluidas las que no se han incorporado. Prisma Access reserva las direcciones IP de ubicación no incorporadas para que pueda añadir estas direcciones IP a sus listas de permitidos antes de incorporarlas.

Direcciones IP para ubicaciones de usuarios móviles incorporados	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`
	O
	`{ "serviceType": "gp_gateway", "addrTy`
		Un tipo de *ubicación* de *implementado* significa que Prisma Access recupera solo las direcciones IP de las ubicaciones que usted incorporó.
		Utilice un *addrType* de *todo* o *activo* para recuperar estas

 ©2025 Palo Alto Networks, Inc.

Recuperar estas direcciones IP	Especifique estos parámetros en el archivo .txt	Comentarios
	`pe": "active", "location": "deployed" }`	direcciones IP de puerta de enlace.
Direcciones IP de red remotas		
Recuperar todas las direcciones IP de red remotas	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	Este comando recupera las direcciones IP públicas y de salida de las redes remotas que ha incorporado. No utilice un *ubicación* de *implementado*. Puede utilizar un *addrType* de *activo* pero este recupera las mismas direcciones que si especificara un *addrType* de *todo*.
Direcciones IP de Clean Pipe		
Recuperar todas las direcciones IP de clean pipe	`{ "serviceType": "clean_pipe", "addrType": "all", "location": "all" }`	Este comando recupera las direcciones IP públicas y de salida de las clean pipes que ha incorporado. No utilice un *ubicación* de *implementado*. Puede utilizar un *addrType* de *activo* pero este recupera las mismas direcciones que si especificara un *addrType* de *todo*.
Direcciones IP de proxy explícito		
Recuperar las direcciones IP de ACS para las ubicaciones implementadas	`{ "serviceType": "swg_proxy", "location": "all", "addrType": "all" }`	Este comando recupera las direcciones IP de salida para cada ubicación de proxy explícito implementada, el servicio de caché de autenticación (ACS) y los equilibradores de carga de red (relevantes solo para implementaciones de proxy explícito).
Direcciones IP de aislamiento remoto del navegador		

 ©2025 Palo Alto Networks, Inc.

Recuperar estas direcciones IP	Especifique estos parámetros en el archivo .txt	Comentarios
Recupere las direcciones IP de Aislamiento remoto del navegador (RBI) para ubicaciones implementadas	{ "serviceType": "rbi", "location": "all", "addrType": "all" }	Este comando recupera las direcciones IP de salida para cada ubicación RBI implementada. Puede añadir estas direcciones IP a una lista de permitidos para conectarse a aplicaciones SaaS.

 ©2025 Palo Alto Networks, Inc.

Obtenga notificaciones cuando las direcciones PI de Prisma Access cambian

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para recibir notificaciones de los cambios en las direcciones IP públicas de las redes remotas y de los cambios en las direcciones IP de bucle invertido para las conexiones de servicio, las conexiones de red remotas y los usuarios móviles, puede especificar una dirección URL en la que se le pueda alertar de un cambio. Prisma Access utiliza una solicitud HTTP POST para enviar la notificación. Esta solicitud POST incluye los siguientes datos de notificación en formato JSON:

```
 {"addrType": "public_ip", "addrChangeType": "add", "utc_timestamp":
"2019-01-31 23:08:19.383894", "text": "Address List Change
Notification"}
```

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp": "2019-01-31 23:13:35.882151", "text": "Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp": "2019-01-31 23:29:27.100329", "text": "2018-05-11
23:29:27.100329"}
```

Cuando reciba una notificación, debe seguir un proceso de dos pasos. En primer lugar, debe programar o de forma manual recuperar la direcciones IP o de bucle invertido. A continuación, debe actualizar las direcciones IP de la lista de permitidos adecuada de su organización para asegurarse de que los usuarios no experimenten ninguna interrupción en el servicio.

Prisma Access envía esta notificación unos segundos antes de que la nueva dirección IP se active. Le recomendamos que utilice scripts de automatización para recuperar y añadir las nuevas direcciones IP a una lista de permitidos en su red.

Para añadir una dirección URL de notificación de dirección IP, complete la siguiente tarea.

- Para implementaciones de Prisma Access (Managed by Strata Cloud Manager), vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de la infraestructura)**, haga clic en el engranaje para editar la configuración, añada una **Egress IP Notification URL (URL de notificación de IP de salida)** donde se le puede notificar de los cambios de dirección IP en su infraestructura de Prisma Access y **Save (Guardar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

- Para implementaciones de Prisma Access (Managed by Panorama), vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y añada una **IP Change Event Notification URL (URL de notificación de evento de cambio de IP)** donde se le puede notificar de los cambios de dirección IP en su infraestructura de Prisma Access, y haga clic en **OK (Aceptar)**.



Puede especificar una dirección IP o un FQDN para un servicio web HTTP o HTTPS que esté escuchando notificaciones de cambio. Prisma Access envía estas notificaciones desde Internet utilizando una dirección IP pública.

No es necesario confirmar los cambios para que la URL de notificación surta efecto.

 ©2025 Palo Alto Networks, Inc.

Utilice scripts heredados para recuperar direcciones IP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Los comandos descritos en esta sección son sustituidos por un script de API más nuevo a partir de la versión 1.5 de Prisma Access; sin embargo, todavía se admiten cuando necesita obtener la dirección de bucle invertido, o para implementaciones que los utilizan en scripts u otras herramientas automatizadas.

La siguiente tabla muestra las palabras clave y los parámetros que están disponibles en los scripts de API heredados utilizados con Prisma Access y proporciona información y recomendaciones sobre qué API utilizar para el tipo de implementación que tiene.

Estos comandos heredados también recuperan direcciones *IP públicas* y direcciones *IP de salida*; sin embargo, Palo Alto Networks recomienda que utilice el script de API más nuevo para recuperar estos comandos y solo utilice la API heredada para recuperar las direcciones IP de bucle invertido.

- Una *public IP address* es la dirección IP de origen que Prisma Access utiliza para solicitudes realizadas a una fuente basada en Internet. Añada la dirección IP pública a una lista de permitidos en su red para proporcionar Prisma Access a recursos de Internet, como aplicaciones SaaS o aplicaciones de socios de acceso público.

  Los usuarios móviles, las redes remotas y las implementaciones de clean pipe utilizan direcciones IP públicas.
- Una *dirección IP de salida* es una dirección IP que Prisma Access utiliza para el tráfico de salida hacia Internet, y también debes agregar estas direcciones a una lista de permitidos para dar acceso a Prisma Access a los recursos de Internet.

  Entre otros fines, Prisma Access utiliza direcciones IP de salida para que los usuarios reciban páginas web en el idioma que esperan de una ubicación de Prisma Access. Todas

 ©2025 Palo Alto Networks, Inc.

las ubicaciones tienen direcciones IP públicas; sin embargo, no todas las ubicaciones tienen direcciones IP de salida. Las siguientes ubicaciones no utilizan direcciones IP de salida:

- Cualquier ubicación que añadió antes del lanzamiento de Prisma Access 1.4.
- Baréin
- Bélgica
- Francia Norte
- Francia Sur
- Hong Kong
- Irlanda
- Corea del Sur
- Taiwán
- Reino Unido

Los usuarios móviles, las redes remotas y las implementaciones de clean pipe utilizan direcciones IP de salida.

Comandos utilizados en implementaciones de Usuarios móviles	
Nombre del comando	**Comentarios**
Comando **get_egress_ip_all=yes** `curl -H header-api-key:`*Current-API-Key*`https://api.prod.datapath.prismaaccess.com/getAddrList/latest?get_egress_ip_all=yes`	Este comando recupera todas las direcciones IP que añade a una lista de permitidos para dar Prisma Access a recursos de Internet, como aplicaciones SaaS o aplicaciones de socios de acceso público. Este comando tiene las siguientes restricciones: • Este comando puede recuperar una gran cantidad de direcciones (más de 200). Si su empresa no puede añadir esta cantidad de direcciones IP a una lista de permitidos, puede usar las palabras clave *gpcs_gp_gw* y *gpcs_gp_portal* para recuperar solo las direcciones IP que está usando actualmente; sin embargo, tendrá que volver a ejecutar estos comandos cada vez que añada una ubicación. Además, si ocurre un evento de escalado, necesitará añadir las nuevas direcciones IP a una lista de permitidos. • Prisma Access no enumera las ubicaciones asociadas con estas direcciones IP; por lo tanto, recomendamos que incluya todas las direcciones IP que se devuelven con este comando en una lista de permitidos. • Este comando no le proporciona direcciones de bucle invertido.

 ©2025 Palo Alto Networks, Inc.

Comandos utilizados en implementaciones de Usuarios móviles	
Nombre del comando	**Comentarios**
gpcs_gp_gw and **gpcs_gp_portal** palabras clave `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_gp_gw | gpcs_gp_portal&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilice este comando si su implementación limita el número de direcciones IP que puede añadir a una lista de permitidos. Debe añadir todas las direcciones IP devueltas con este comando a una lista de permitidos en su red. También puede recuperar las direcciones IP de bucle invertido con este comando.

Comandos utilizados en implementaciones de redes remotas	
Nombre del comando	**Comentarios**
palabra clave **gpcs_remote_network** `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_remote_network &addrType=public_ip | egress_ip_list | loopback_ip"`	Utilice este comando para encontrar las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de red remota. También puede utilizar este comando para encontrar las direcciones IP de salida para implementaciones de red remotas; las direcciones IP y de salida pueden ser diferentes en algunas situaciones.

Comandos utilizados en implementaciones de Clean Pipe	
Nombre del comando	**Comentarios**
palabra clave **gpcs_clean_pipe** `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilice este comando para encontrar las direcciones IP que necesita añadir a una lista de permitidos para implementaciones de clean pipe.

Recuperar direcciones IP de usuarios móviles

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

Este script heredado se ha reemplazado por un nuevo script API a partir de Prisma Access 1.5. Palo Alto Networks recomienda que utilice el script más reciente para recuperar todas las direcciones IP, con la excepción de las direcciones de bucle invertido.

Si va a añadir direcciones IP públicas para permitir que las listas de usuarios móviles tengan acceso a SaaS o aplicaciones públicas, Prisma Access proporciona dos direcciones IP para cada puerta de enlace y dirección IP del portal, de modo que se pueda utilizar una dirección IP durante un escalado u otro evento. Puede añadir este conjunto de direcciones IP a una lista de permitidos antes de usarlas, lo que evita problemas con los usuarios móviles que puedan acceder a SaaS o aplicaciones públicas durante un evento de escalado.

Recupere estas nuevas direcciones completando la siguiente tarea:

STEP 1 | Para obtener la clave API, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicio)**; luego seleccione **Generate API Key (Generar clave de API)**.

Necesita esta clave para autenticarse en Prisma Access y recuperar la lista de direcciones IP utilizando el comando curl que aparece a continuación. Solo un administrador de Panorama o un superusuario pueden generar o acceder a esta clave API.

STEP 2 | Introduzca el siguiente comando para recuperar las direcciones IP públicas de los usuarios móviles:

```
  curl -H header-api-key:Current-API-Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

Donde *Current-API-Key* es la Clave API de Prisma Access.

Por ejemplo, dada una clave API de **12345abcde**, utilice el siguiente comando API para recuperar la dirección IP pública de todas las ubicaciones:

```
  curl -H header-api-key:12345abcde "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

Cada vez que Prisma Access utiliza un conjunto de direcciones IP públicas, asigna otro conjunto de direcciones IP. Si cree que Prisma Access ha utilizado el conjunto añadido de direcciones IP públicas (por ejemplo, si un gran número de usuarios móviles ha accedido a una única ubicación), puede ejecutar este comando de la API de nuevo para encontrar el nuevo conjunto de direcciones IP públicas. Todas las direcciones IP persisten después de una actualización.

Recuperar direcciones IP públicas, de bucle invertido y de salida

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

Este script heredado se ha reemplazado con un script más nuevo a partir de Prisma Access 1.5. Palo Alto Networks recomienda que utilice el script más reciente para recuperar todas las direcciones IP, con la excepción de las direcciones de bucle invertido.

Para recuperar direcciones IP públicas, de bucle invertido y de salida, complete los siguientes pasos.

STEP 1 | Obtenga la clave API y añada una **URL de notificación de evento de cambio de IP** donde pueda recibir notificaciones de cambios de dirección IP en su infraestructura de Prisma Access.

Consulte Obtenga notificaciones cuando las direcciones PI de Prisma Access cambian para obtener más detalles.

STEP 2 | Recupere las direcciones IP públicas, las direcciones IP de bucle invertido o ambas para Prisma Access.

Utilice la clave API y la URL del endpoint de la API de forma manual o en un script de automatización:

```
 header-api-key:Clave API actual "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=$fwType&addrType=$addrType"
```

donde debe reemplazar la Clave API actual con su clave API y usar una o ambas de las siguientes palabras clave y argumentos:

Palabra clave	Descripción
fwType palabra clave	
gpcs_gp_gw	Recupera direcciones IP del portal (para implementaciones de usuarios móviles) de Prisma Access.
gpcs_gp_portal	Recupera direcciones IP de red remota (para implementaciones de red remota) de Prisma Access.
gpcs_remote_network	Recupera direcciones IP de red remotas (para implementaciones de red remotas) de Prisma Access.
gpcs_clean_pipe	Recupera direcciones IP de Clean Pipe de Prisma Access.
addrType palabra clave	
public_ip	Recupera las direcciones IP de origen que Prisma Access utiliza para las solicitudes realizadas a una fuente basada en Internet.

 ©2025 Palo Alto Networks, Inc.

Palabra clave	Descripción
	Para ubicaciones de usuarios móviles, Prisma Access enumera las direcciones IP por ubicación. Para redes remotas, Prisma Access enumera las direcciones IP por nombre de red remota.
egress_ip_list	Recupera las direcciones IP que Prisma Access utiliza con direcciones IP públicas para tráfico de salida adicional a Internet. Para ubicaciones de usuarios móviles, Prisma Access enumera las direcciones IP por ubicación. Para redes remotas, Prisma Access enumera las direcciones IP por nombre de red remota.
loopback_ip	Recupera las direcciones IP de origen utilizadas por Prisma Access para las solicitudes realizadas a una fuente interna (por ejemplo, un servidor RADIUS o Active Directory) y se asigna desde la subred de infraestructura.

Si no especifica una palabra clave, Prisma Access recupera todas las direcciones IP.

Por ejemplo, puede probar el siguiente comando Curl para recuperar manualmente la lista de direcciones IP públicas de todas las redes remotas:

```
curl -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

o utilice un script de Python simple para recuperar la lista de todas las direcciones IP, por ejemplo:

```
  #!/usr/bin/python import subprocess import json api_key
 = '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7'
 # Replace with your key api_end_point = 'https://
api.prod.datapath.prismaaccess.com/getAddrList/latest' # This call
 retrieves IP addresses for all your Prisma Access firewalls args =
 ['curl', '-k', '-H', 'header-api-key:' + api_key, api_end_point]
 p = subprocess.Popen(args, stdout=subprocess.PIPE) output
 = p.communicate() dout = json.loads(output[0]) addrStrList
 = dout['result']['addrList'] addrList = [] for addr_str
 in addrStrList: addrList.append(addr_str.split(":")[1])
 print(addrList)
```

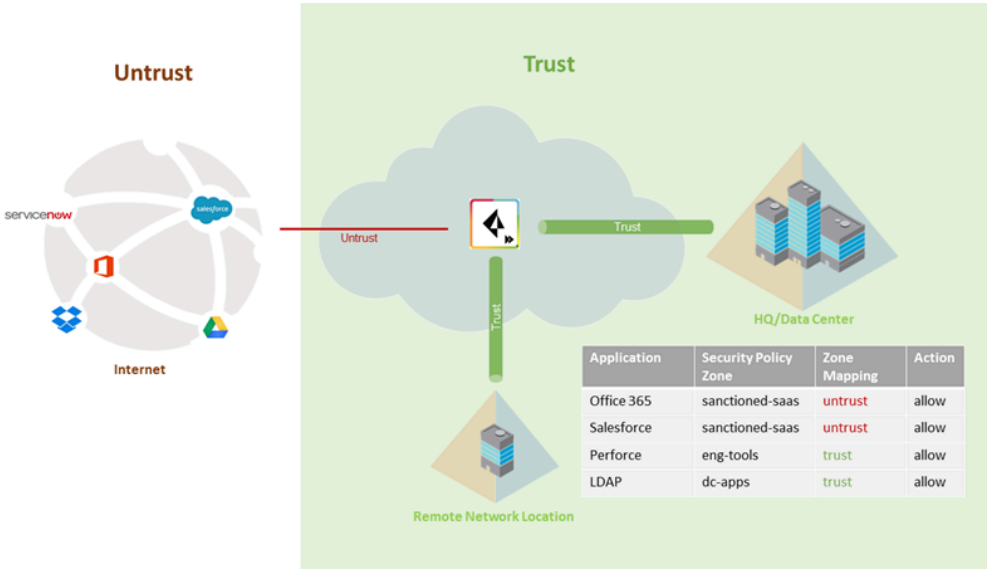
STEP 3 | Actualice las listas de permitidos en sus servidores locales o las reglas de políticas de aplicaciones SaaS con las direcciones IP que recuperó.

 ©2025 Palo Alto Networks, Inc.

Zonas de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En un cortafuegos, las zonas están asociadas con interfaces. Pero dentro de Prisma Access, la infraestructura de red se configura automáticamente para usted. Esto significa que ya no necesita preocuparse por configurar interfaces y asociarlas con las zonas que cree. Sin embargo, para habilitar la aplicación coherente de políticas de seguridad, debe crear asignaciones de zonas para que Prisma Access sepa si asociar una zona con una interfaz interna (de confianza) o una interfaz externa (de no confianza). Esto garantizará que sus reglas de política de seguridad se apliquen correctamente. De forma predeterminada, todas las zonas que envía a Prisma Access están configuradas como no fiables. Deberá dejar todas las zonas asociadas con el tráfico vinculado a Internet, incluidas sus aplicaciones SaaS autorizadas, configuradas como no fiables. Sin embargo, para todas las zonas que permiten el acceso a aplicaciones en su red interna o en su centro de datos, debe asignarlas a confianza. Observe que en el ejemplo a continuación, todas las aplicaciones SaaS autorizadas (Office 365 y Salesforce en este caso) están segmentadas en la zona SaaS autorizada para permitir la visibilidad y la aplicación de políticas sobre el uso de estas aplicaciones. Para habilitar a Prisma Access para que asocie la zona SaaS autorizada con una interfaz externa, debe asignar esta zona a no fiable. De manera similar, las zonas eng-tools y dc-apps proporcionan acceso a aplicaciones en la oficina corporativa y, por lo tanto, debe designarlas como zonas fiables.



Prisma Access es compatible con tres zonas (confianza, no confianza y VPN sin cliente) y simplifica la creación de políticas configurándolas por usted.

 ©2025 Palo Alto Networks, Inc.

Zona	Descripción
Fiable	Zona que contiene todas las direcciones IP, conexiones de servicio o usuarios móviles fiables e incorporados dentro de la red corporativa.
No fiable	Todas las direcciones IP, conexiones de servicio o usuarios móviles que no sean fiables fuera de la red corporativa. De manera predeterminada, cualquier dirección IP o usuario móvil que no sea fiable, inherentemente, no es fiable.
VPN sin cliente	Acceso remoto seguro a aplicaciones web empresariales comunes que utilizan tecnologías HTML, HTML5 y Javascript. Los usuarios tienen la ventaja de un acceso seguro desde los navegadores web habilitados para SSL sin instalar el software de GlobalProtect. Esto es útil cuando necesita habilitar el acceso de socios o contratistas a aplicaciones y para habilitar de manera segura activos no administrados, incluidos dispositivos personales. *La zona para VPN sin cliente está asignada a la zona de confianza de forma predeterminada; esta configuración no se puede cambiar.*

Los logs de Prisma Access que muestran una zona de **inter-fw** son logs utilizados para la comunicación dentro de la infraestructura de Prisma Access.

Al crear zonas, no utilice ninguno de los siguientes nombres para las zonas, ya que son nombres utilizados para zonas internas:

- fiable
- no fiable
- inter-fw
- Cualquier nombre que utilice para las redes remotas (los nombres de redes remotas se utilizan como zona de origen en logs de Strata Logging Service)

Los logs de Prisma Access que muestran una zona de inter-fw son logs utilizados para la comunicación dentro de la infraestructura de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

DNS para Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Prisma Access le permite especificar servidores DNS para resolver tanto los dominios internos de su organización como los dominios externos. Haga esto para proporcionar acceso a los servicios de su red corporativa, como los servidores LDAP y DNS, especialmente si planea configurar conexiones de servicio para proporcionar acceso a este tipo de recursos en la sede central o en los centros de datos. Prisma Access es compatible con la resolución de DNS para usuarios móviles: Global Protect e implementaciones de redes remotas. Las consultas DNS para los dominios de la Lista interna de dominios se envían a los servidores DNS locales para asegurarse de que los recursos estén disponibles para los usuarios de red remotos de Prisma Access y los usuarios móviles.

Por ejemplo, si desea que una búsqueda de DNS para su dominio corporativo vaya exclusivamente al servidor DNS corporativo, especifique aquí el dominio corporativo y los servidores DNS corporativos. Para asegurarse de que los endpoints utilizan la **DNS Proxy IP Address (Dirección IP del proxy de DNS)**, estos se deben configurar para resolver los DNS a través de la dirección IP que se muestra en **Workflow (Flujo de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Prisma Access DNS Proxy IP Address (Dirección IP del proxy DNS de Prisma Access**.

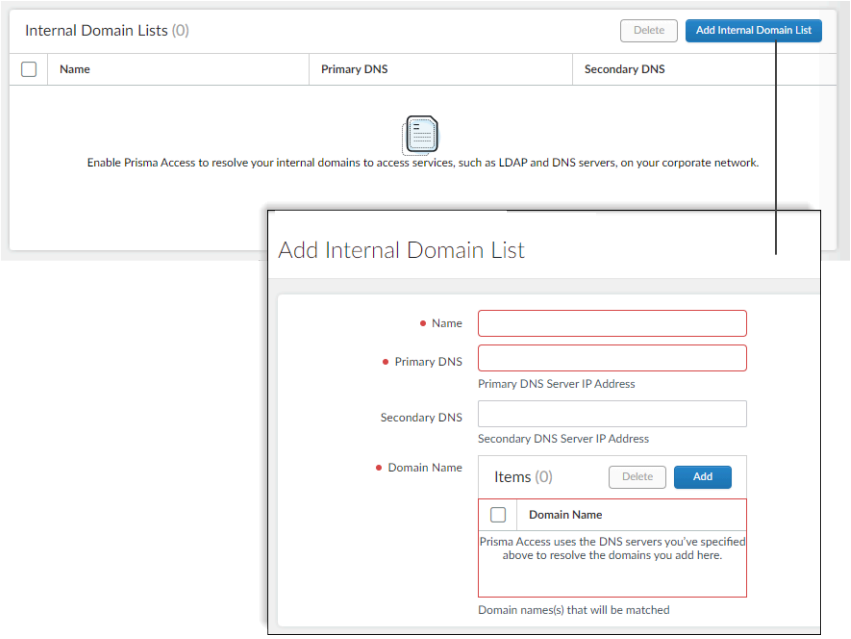
- Strata Cloud Manager
- Panorama

DNS para Prisma Access (Strata Cloud Manager)

Aquí le explicamos cómo configurar Prisma Access para resolver dominios internos y cómo personalizar la configuración de DNS (para resolver dominios internos y públicos) para implementaciones de usuarios móviles y sitios de red remotos.

 ©2025 Palo Alto Networks, Inc.

- Esto establecerá listas internas de dominios que se aplican a todo el tráfico.
  1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** y **Add Internal DNS Servers (Añadir servidores DNS internos)**.



  2. Introduzca el servidor DNS principal y el servidor DNS secundario que Prisma Access debe usar para resolver los nombres de dominio internos.
  3. Añada los nombres de dominio internos para enviar a estos servidores DNS para su resolución.

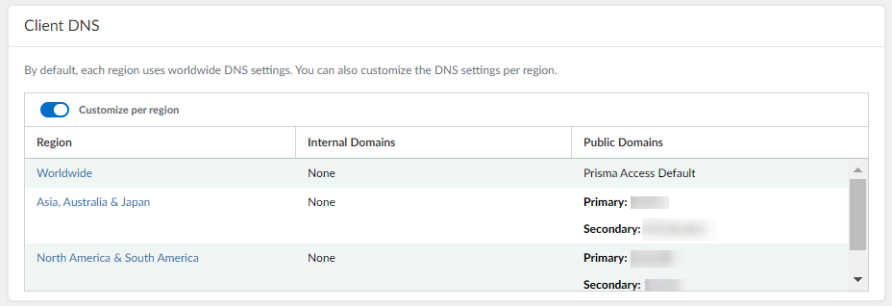
     Puede utilizar un comodín (*) delante de los dominios de la lista de dominios, por ejemplo, *.acme.local o *.acme.com

 ©2025 Palo Alto Networks, Inc.

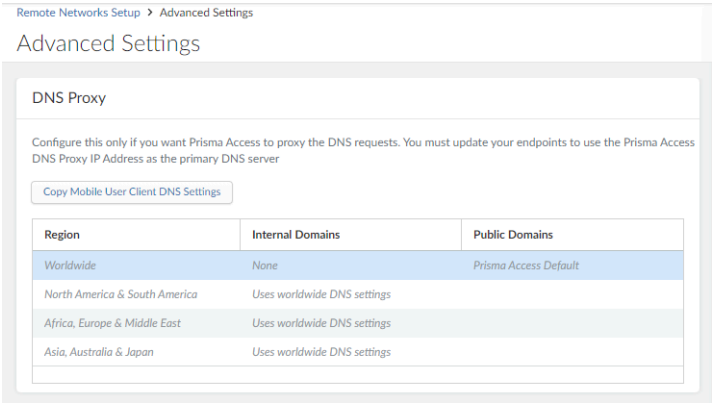
- Añada listas de dominios internos que se apliquen solo a implementaciones de usuarios móviles específicos o sitios de red remotos.

  1. Configure la Configuración DNS:

     - **Usuarios móviles**: Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure Settings (Configuración de infraestructura)** y encontrar **Client DNS (DNS de cliente)**.



     - **Redes remotas**: Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)** > **Advanced Settings (Configuración avanzada)** y encontrar **DNS Proxy (Proxy DNS)**.



  2. Utilice el valor predeterminado mundial (el servidor DNS predeterminado de Prisma Access) o personalice la configuración según la región. En cualquier caso, seleccione la región para ajustar y personalizar la configuración de DNS para esa región.
  3. Marque la opción para **utilizar esta configuración de DNS para resolver dominios internos** y, opcionalmente, **utilizar el servidor DNS interno también para resolver dominios públicos**. Si no selecciona esta opción, Prisma Access utiliza su servidor DNS predeterminado en la nube para resolver solicitudes de dominios públicos.
  4. Permita el tráfico desde todas las direcciones en su grupo de direcciones IP de usuarios móviles a sus servidores DNS.

     El proxy DNS en Prisma Access envía las solicitudes a los servidores DNS que usted especifique. La dirección de origen en la solicitud DNS es la primera dirección IP en el grupo de IP que asigna a la región. Para garantizar que sus solicitudes de DNS puedan llegar a los servidores, deberá asegurarse de permitir el tráfico desde todas las direcciones en su grupo de direcciones IP de usuarios móviles a sus servidores DNS.

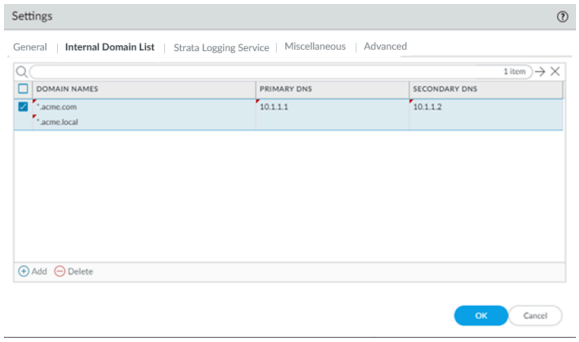
 ©2025 Palo Alto Networks, Inc.

DNS para Prisma Access (Panorama)

Configure Prisma Access para resolver los dominios internos

- Esto establecerá listas internas de dominios que se aplican a todo el tráfico.
  1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y haga clic en el icono de engranaje para editar la Configuración.
  2. Seleccione la pestaña **Internal Domain List (Lista de dominios internos)**.
  3. Añada los nombres de dominio, DNS primario y servidores DNS secundarios que desee que Prisma Access use para resolver sus nombres de dominio internos.

     Puede utilizar un comodín (*) delante de los dominios de la lista de dominios, por ejemplo, *.acme.local o *.acme.com



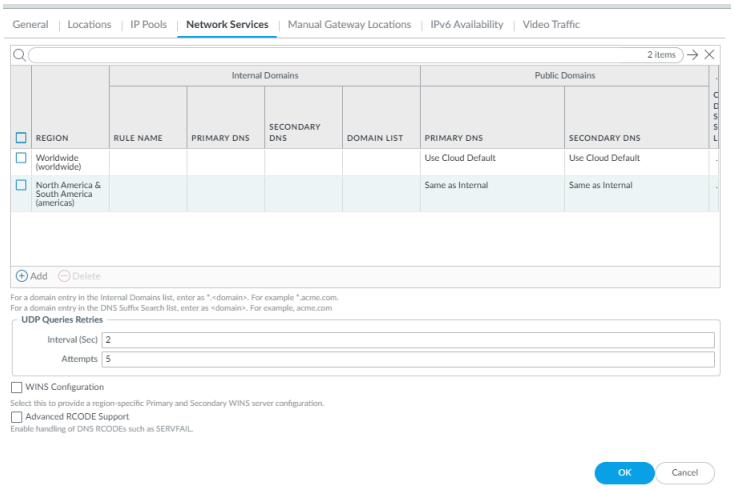
- Añada listas de dominios internos que se apliquen solo a implementaciones de usuarios móviles específicos o sitios de red remotos.

  1. Configure la Configuración DNS:

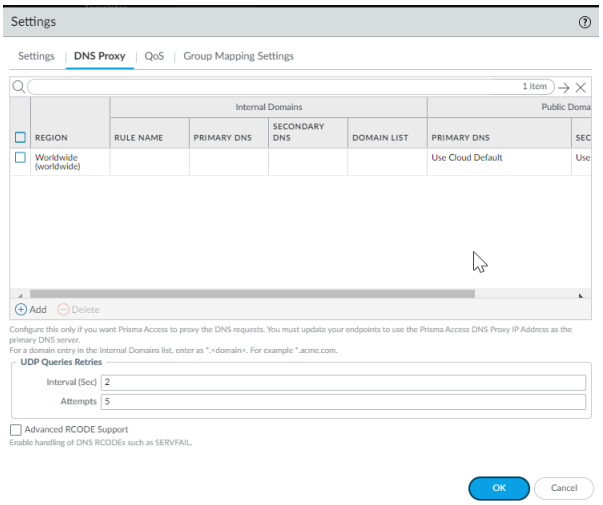
     - **Usuarios móviles**: Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users - GlobalProtect (Usuarios móviles -**

 ©2025 Palo Alto Networks, Inc.

GlobalProtect) y seleccione la puerta de enlace externa > y haga clic en **Network Services (Servicios de red)**.



- **Redes remotas**: Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** > **Settings (Configuración)** > **DNS Proxy (Proxy DNS)**.



2. Utilice el valor predeterminado mundial (el servidor DNS predeterminado de Prisma Access) o personalice la configuración según la región. En cualquier caso, seleccione la región para ajustar y personalizar la configuración de DNS para esa región.
3. Añada una o más reglas para configurar los ajustes de DNS para **Internal Domain (Dominio interno)**.
   - Introduzca un Nombre de regla único para la plantilla.
   - Sí desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios que desea resolver en la Lista de dominios. Especifique un asterisco delante del dominio; por ejemplo, *.acme.com. Puede especificar un máximo de 1.024 entradas de dominio.

     Prisma Access tiene una regla predefinida para resolver dominios *.amazonaws.com mediante el servidor predeterminado de nube. Si desea que los servidores DNS internos resuelvan un dominio *.amazonaws.com más específico (por ejemplo,

 ©2025 Palo Alto Networks, Inc.

*.s3.amazonaws.com), introduzca la URL en la lista de dominios. Prisma Access evalúa los nombres de dominio del más largo al más corto, y luego de la parte superior a la parte inferior en la lista.

- Si tiene un servidor DNS personalizado que puede acceder a sus dominios internos, especifique las direcciones IP del servidor DNS principal y del servidor DNS secundario, o seleccione Usar Cloud Default para usar el valor predeterminado del servidor DNS de Prisma Access.

4. Especifique la configuración de DNS para **Public Domains (Dominios Públicos)**.
   - **Use Cloud Default (Utilizar Cloud Default)**: utilice el servidor DNS predeterminado de Prisma Access.
   - **Internal DNS (DNS interno)**: utilice el mismo servidor que utiliza para resolver dominios internos. Al seleccionar esta opción, el servidor DNS utilizado para resolver dominios públicos es el mismo que el servidor configurado para la primera regla en la sección **Dominios internos**.
   - **Custom DNS server (Servidor DNS personalizado)**: si tiene un servidor DNS que puede acceder a sus dominios públicos (externos), introduzca la dirección del servidor DNS principal en ese campo.
5. (Opcional) Puede añadir un sufijo DNS para especificar el sufijo que el cliente deberá usar localmente cuando se introduce un nombre de host no cualificado que no puede resolver, por ejemplo, acme.local. Haga que la guía del administrador de Prisma Access (gestionada por Panorama) no introduzca un carácter comodín (*) delante del sufijo de dominio (por ejemplo, acme.com). Puede añadir varios sufijos.
6. Permita el tráfico desde todas las direcciones en su grupo de direcciones IP de usuarios móviles a sus servidores DNS.

   El proxy DNS en Prisma Access envía las solicitudes a los servidores DNS que usted especifique. La dirección de origen en la solicitud DNS es la primera dirección IP en el grupo de IP que asigna a la región. Para garantizar que sus solicitudes de DNS puedan llegar a los servidores, deberá asegurarse de permitir el tráfico desde todas las direcciones en su grupo de direcciones IP de usuarios móviles a sus servidores DNS.

 ©2025 Palo Alto Networks, Inc.

Alta disponibilidad (HA) para Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

La implementación de dispositivos Panorama en una configuración de alta disponibilidad (HA) proporciona redundancia en caso de un fallo del sistema o de la red, y garantiza que tenga conectividad continua con Prisma Access. En una configuración HA, un peer del dispositivo Panorama es el primario activo y el otro es el secundario pasivo. En caso de conmutación por error, el par secundario se vuelve activo y asume la función de gestión de Prisma Access.

Para simplificar la configuración de HA, configure los dispositivos Panorama en HA después de comprar Prisma Access y los códigos de autenticación y componentes de Strata Logging Service, y asocie el número de serie del dispositivo Panorama principal en el que planea instalar el Complemento Cloud Services con los códigos de autenticación, pero antes de activar e instalar Prisma Access gestionado por Panorama. Sin embargo, también puede utilizar este proceso para configurar dispositivos Panorama existentes que ya tienen el complemento instalado.

Ya sea que esté empezando a utilizar un nuevo par de dispositivos Panorama o que ya haya configurado su dispositivo Panorama independiente y completado los procedimientos de licencia e instalación, asegúrese de verificar los requisitos previos antes de habilitar HA:

- Debe registrar los pares HA del dispositivo Panorama en la misma cuenta de cliente en el Portal de atención al cliente (CSP).
- Los dispositivos Panorama que son peers deben tener el mismo factor de forma (dispositivos de hardware del mismo modelo o dispositivos virtuales idénticos) y la misma versión de sistema operativo y deben tener el mismo conjunto de licencias. Se requiere la licencia de soporte premium para Prisma Access y Strata Logging Service.
- El número de serie del dispositivo Panorama principal está vinculado a su Prisma Access y a los códigos de autenticación de Strata Logging Service. Si ha instalado y configurado el complemento en un dispositivo Panorama independiente, asegúrese de utilizar ese dispositivo Panorama como peer principal. Si necesita asignar este peer independiente como dispositivo Panorama secundario, póngase en contacto con la asistencia de Palo Alto Networks para obtener ayuda con la transferencia de la licencia al peer del dispositivo Panorama principal antes de continuar.

Si deshabilita HA para un par de Panorama y vuelve a una configuración donde un solo Panorama gestiona Prisma Access, debe volver a verificar su cuenta para evitar errores al recuperar el estado de componentes de Prisma Access.

Para configurar sus dispositivos Panorama en una configuración HA, complete los siguientes pasos.

STEP 1 | Configure HA en Panorama.

Establezca el dispositivo Panorama principal como **Primary (Principal)** y el dispositivo Panorama secundario como **Secondary (Secundario)** y asegúrese de que el número de serie

 ©2025 Palo Alto Networks, Inc.

de su dispositivo Panorama principal esté vinculado a sus códigos de autenticación de Prisma Access y Strata Logging Service.

STEP 2 | Asegúrese de que los dispositivos Panorama principal (activo) y secundario (pasivo) estén sincronizados y que el estado del enlace de alta disponibilidad entre ellos esté activo.

1. Acceda al **Dashboard (Panel)** en el Panorama principal y seleccione **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** para mostrar el widget de HA.
2. **Sync to peer (Sincronizar en el peer)**, haga clic en **Yes (Sí)** y espere a que la **Running Config (Configuración en ejecución)** se muestre como **Synchronized (Sincronizado)**.
3. Asegúrese de que el peer **local** esté **active (activo)**.
4. Acceda al **Dashboard (Panel)** en el dispositivo Panorama pasivo y seleccione **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** para mostrar el widget de HA.
5. Verifique que la **Running Config (Configuración en ejecución)** se muestre como **Synchronized (Sincronizado)**.
6. Asegúrese de que el peer **Local** sea **passive (pasivo)**.

STEP 3 | Instale los componentes de Prisma Access en el dispositivo Panorama principal.

1. Inicie sesión en el dispositivo Panorama y seleccione **Panorama** > **Licenses (Licencias)**.
2. Haga clic en **Retrieve the license keys from license server (Recuperar claves de licencia del servidor de licencias)**.
3. Active e instale Panorama Managed Prisma Access, incluida la generación de una contraseña de un solo uso (OTP) y la verificación de su cuenta.

STEP 4 | Verifique que la HA esté habilitado.

1. En el dispositivo Panorama principal, acceda a la CLI e introduzca el siguiente comando operativo:

   ```
   tail follow yes mp-log plugin_cloud_services.log
   ```

2. Encuentre el siguiente texto en la salida del registro de log, donde *X* es el número de serie del dispositivo Panorama principal e *Y* es el número de serie del dispositivo Panorama secundario:

```
2017-11-06 15:14:07.790 -0800 INFO: [hainfo] Sending
 update to CSP for HA peer serial information to https://
updates.paloaltonetworks.com/licensesvc/licenseservice.asmx/
PanoramaHAInfo (https://updates.paloaltonetworks.com/
licensesvc/licenseservice.asmx/PanoramaHAInfo)
 2017-11-06 15:14:07.791 -0800 INFO: [hainfo] Data
 string is primarypanoramasn=<varname>X</varname>
 &secondarypanoramasn=<varname>Y</varname> 2017-11-06
 15:14:17.595 -0800 INFO: [hainfo] HTTP_CODE 200, RESPONSE:
 <?xml version="1.0" encoding="utf-8"?> <PanoramaHA
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance (http://
www.w3.org/2001/XMLSchema-instance)" xmlns:xsd="http://
www.w3.org/2001/XMLSchema (http://www.w3.org/2001/
XMLSchema)" xmlns="http://www.paloaltonetworks.com/ (http://
www.paloaltonetworks.com/)"> <success>true</success> </
PanoramaHA> 2017-11-06 15:14:17.596 -0800 INFO: [hainfo]
 Cached HA Peer's serial number <varname>Y</varname>
```

 ©2025 Palo Alto Networks, Inc.

3. Inicie sesión en el Portal de atención al cliente (CSP) y seleccione **Assets (Activos)** > **Cloud Services (Servicios en la nube)** para verificar que ambos pares de Panorama estén vinculados a sus licencias de Prisma Access y Strata Logging Service.
4. Verifique los campos del dispositivo Panorama principal y secundario.

   Los campos Código de autorización, Nombre del modelo, Descripción de la licencia y Fecha de vencimiento deben ser los mismos para el dispositivo Panorama principal y secundario, porque Palo Alto Networks ha asociado la licencia de Prisma Access automáticamente al dispositivo Panorama secundario.

STEP 5 | Inicie sesión en el dispositivo Panorama secundario y active e instale Panorama Managed Prisma Access.

Cuando inicie sesión en el Portal de atención al cliente (CSP) para generar la OTP, asegúrese de especificar el número de serie del dispositivo Panorama secundario.

STEP 6 | Confirme sus cambios en el dispositivo Panorama principal y secundario.

1. **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** sus cambios.
2. Haga clic en **OK (Aceptar)** y **Push (Enviar)**.

STEP 7 | Verifique que los dispositivos Panorama principal y secundario aún estén en un estado sincronizado.

 ©2025 Palo Alto Networks, Inc.

Plantillas predefinidas: Incorporar una conexión de servicio o red remota

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access incluye plantillas IPSec predefinidas para dispositivos IPSec y SD-WAN comunes de terceros. Estos perfiles aceleran y simplifican la incorporación de conexiones de servicio y conexiones de red remotas que utilizan uno de estos dispositivos para finalizar la conexión.

Compartir una plantilla común también le permite incorporar múltiples conexiones remotas del tipo sano con criptografías, claves precompartidas e identificadores de peers compartidos de forma común.

- Plantillas predefinidas: Incorporar una conexión de servicio o red remota
- Perfiles criptográficos IKE e IPSec compatibles para dispositivos SD-WAN comunes

Prisma Access le proporciona las siguientes plantillas predefinidas que puede utilizar para configurar túneles IPSec entre su dispositivo local y Prisma Access:

- Túneles IPSec [**Network (Red)** > **IPSec Tunnels (Túneles IPSec)**] en Remote_Network_Template y Service_Conn_Template.
- Puertas de enlace IKE [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)**] en Remote_Network_Template y Service_Conn_Template.
- Perfil criptográfico de IPSec [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptografía IPSec)**] en Remote_Network_Template y Service_Conn_Template.
- Perfiles criptográficos IKE [**Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico de IKE)**] en Remote_Network_Template y Service_Conn_Template.

Actualmente, existen disponibles plantillas para los siguientes proveedores:

Además de las siguientes plantillas, ofrecemos una plantilla genérica que puede utilizar con cualquier dispositivo local que no se enumera aquí.

- Dispositivos de Cisco:
  - Enrutadores de servicios integrados (ISR) de Cisco
  - Cisco Adaptive Security Appliances (ASAs)
- Citrix
- Prisma SD-WAN (anteriormente CloudGenix)
- Riverbed
- Silver Peak

Para incorporar una conexión de servicio o una conexión de red remota utilizando las plantillas proporcionadas por Prisma Access, complete la siguiente tarea.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | En Panorama, realice la configuración para que las plantillas se muestren en Panorama.

Al actualizar el complemento Cloud Services, las nuevas plantillas no se muestran automáticamente. Complete este paso una vez después de actualizar para que las plantillas se muestren permanentemente. Las nuevas instalaciones realizan esta configuración inicial como parte de su configuración por primera vez y este paso adicional no es necesario.



También puede completar este paso si elimina estas plantillas y necesita recuperarlas.

- Para las conexiones de servicio, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicio)** haga clic en el icono de engranaje en el área **Settings (Configuración)** para abrir la **Settings (Configuración)** y, a continuación, haga clic en **OK (Aceptar)**.
- Para conexiones de red remotas, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, haga clic en el icono de engranaje en el área **Settings (Configuración)** para abrir la **Settings (Configuración)** y, a continuación, haga clic en **OK (Aceptar)**.

STEP 2 | Seleccione **Network (Red)** y, a continuación, seleccione la **Template (Plantilla)** correcta (**Remote_Network_Template** si está creando una conexión remota o **Service_Conn_Template** si está creando una conexión de servicio).

STEP 3 | Determine el tipo de dispositivo que se utiliza para finalizar la conexión de servicio o la conexión de red remota y encuentre una plantilla para utilizar con ese dispositivo.



Si su dispositivo SD-WAN o IPSec no está en la lista, utilice los perfiles genéricos.

STEP 4 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)** y realice los siguientes cambios en el perfil de puerta de enlace IKE de su dispositivo:

Puede usar los perfiles de criptografía IPSec e IKE sin cambios; sin embargo, debe realizar cambios específicos en el perfil de la puerta de enlace IKE para que coincida con la configuración de red.

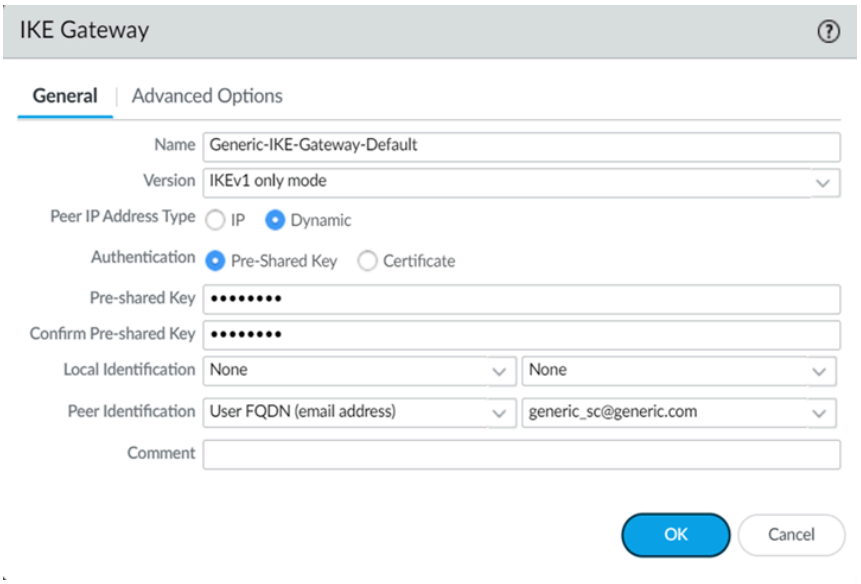
- (Opcional) Si conoce la dirección IP pública del dispositivo local que se utilizará para configurar el túnel IPSec con Prisma Access, establezca una dirección IP estática

 ©2025 Palo Alto Networks, Inc.

especificando un **Peer IP Address Type (Tipo de dirección IP del peer) IP** e introduzca la **Peer Address (Dirección del peer)** para el túnel IPSec.

- Si utiliza una clave precompartida para el túnel IPSec, especifique una **Pre-shared Key (Clave precompartida)**.
- Especifique una **Peer Identification (Identificación del peer** de **IP Address (Dirección IP)** o **User FQDN (FQDN de usuario)**.

  Asegúrese de que coincide con los ajustes que especifique aquí cuando configure el dispositivo utilizado para terminar el otro lado del túnel IPSec.



STEP 5 | Incorpore la conexión de servicio o conexión de red remota, especificando la configuración del **IPSec tunnel (Túnel IPSec)** que coincide con el dispositivo al otro lado del túnel IPSec.

 ©2025 Palo Alto Networks, Inc.

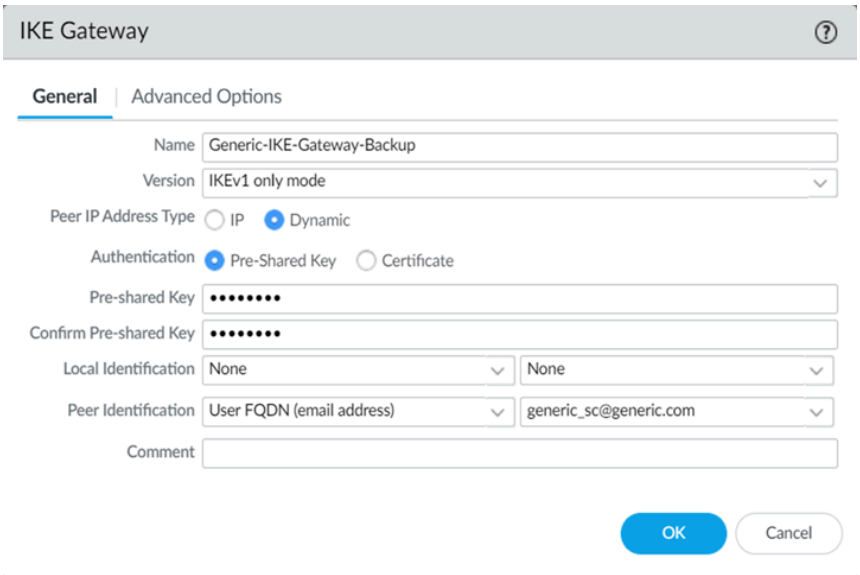
STEP 6 | (Opcional) Si necesita añadir un túnel de copia de seguridad (WAN secundaria) para una conexión de servicio o conexión remota, realice los siguientes pasos de configuración adicionales.

La configuración de una WAN secundaria no se admite en las siguientes implementaciones:

- Si su WAN secundaria está configurada en modo activo-activo con el túnel IPSec primario.
- Si el equipo de las instalaciones del cliente (CPE) está configurado en una configuración de enrutamiento multipath de igual coste (ECMP) con el túnel IPSec primario y secundario.

1. Cree una nueva puerta de enlace IKE para el túnel de copia de seguridad, copiando la configuración de la plantilla predefinida que desea duplicar.

   En el ejemplo siguiente se crea una configuración de túnel de copia de seguridad para dispositivos de red genéricos.

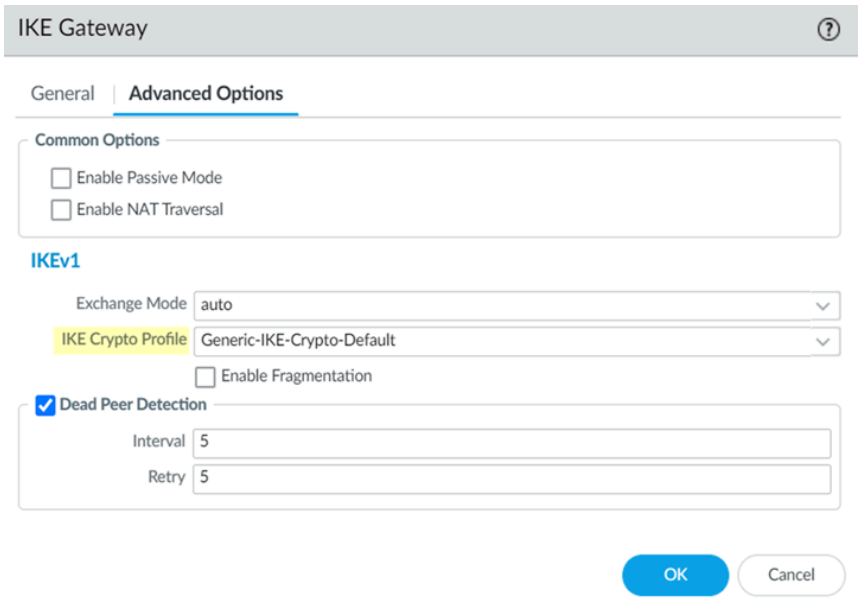


2. En **Advanced Options (Opciones avanzadas)**, especifique el **IKE Crypto Profile (Perfil criptográfico IKE)** para la plantilla predefinida que desea utilizar.

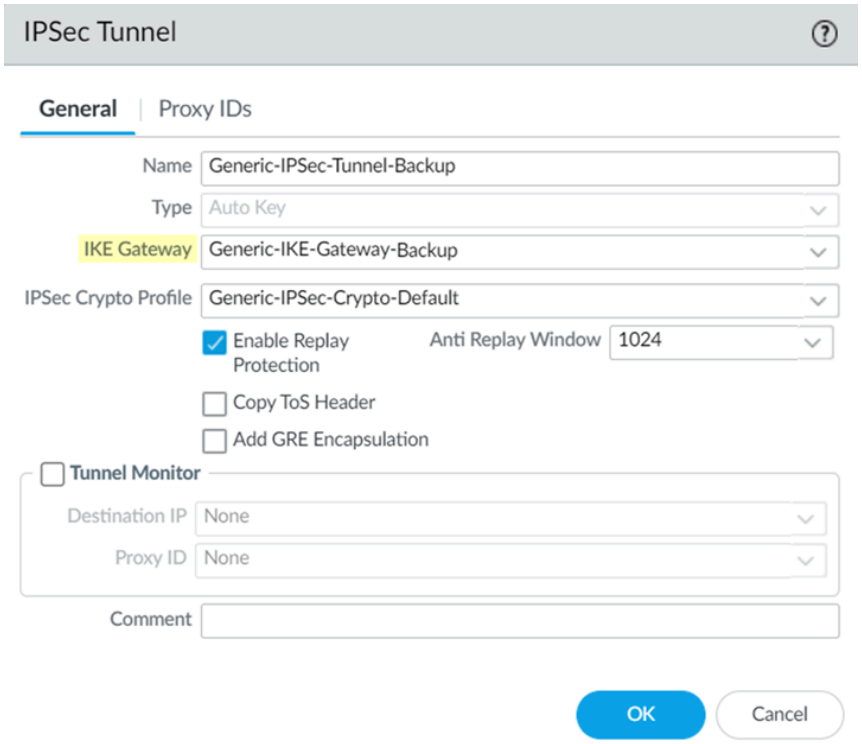
   Palo Alto Networks recomienda que utilice cifrados GCM en lugar de cifrados CBC para túneles IPSec.

   Si va a incorporar un Prisma SD-WAN, seleccione **Enable Passive Mode (Habilitar modo pasivo)**.

 ©2025 Palo Alto Networks, Inc.

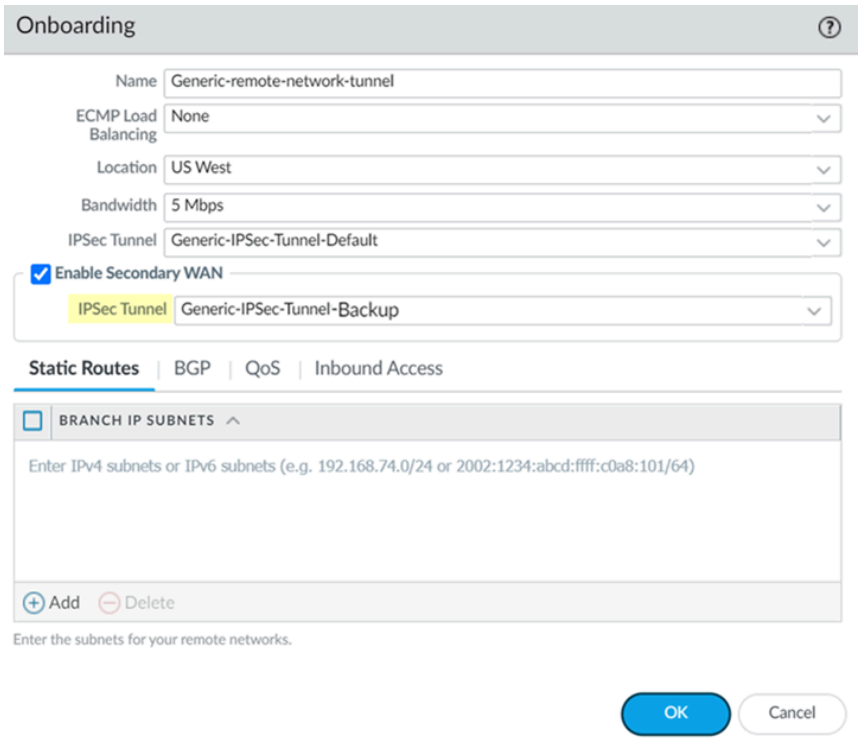


3. Cree un nuevo túnel IPSec, especificando la nueva puerta de enlace IKE que creó, pero copiando todos los demás ajustes de la plantilla predeterminada.



4. Cuando incorpore la conexión de servicio o la conexión de red remota, deberá **Enable Secondary WAN (Habilitar WAN secundaria)** y especificar el túnel que creó para la WAN de copia de seguridad.

 ©2025 Palo Alto Networks, Inc.



STEP 7 | Complete la configuración de la conexión de servicio o la conexión de red remota haciendo coincidir los identificadores de cifrado, clave precompartida y peers en el dispositivo que se utiliza para terminar el otro lado del túnel IPSec.

STEP 8 | (Opcional) Si necesita incorporar varias conexiones de red remotas que utilizan los mismos tipos de dispositivos de red, deberá **Export (Exportar)** la configuración de la red remota, editar los ajustes y, a continuación,**Import (Importar)** esa configuración.

Perfiles criptográficos IKE e IPSec compatibles para dispositivos SD-WAN comunes

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En esta sección se proporcionan los perfiles criptográficos compatibles con muchos dispositivos SD-WAN comunes. Si está configurando un dispositivo SD-WAN, utilice estos perfiles como guía en cuanto a lo que puede configurar para la red remota en Prisma Access.

- Perfiles criptográficos IKE e IPSec compatibles con Aruba SD-WAN
- Perfiles criptográficos IKE e IPSec compatibles con Aryaka SD-WAN
- Perfiles criptográficos IKE e IPSec compatibles con Citrix SD-WAN

 ©2025 Palo Alto Networks, Inc.

- El dispositivo Prisma SD-WAN admite perfiles criptográficos IKE e IPSec
- Perfiles criptográficos IKE e IPSec compatibles con SD-WAN de Nuage Networks
- Perfiles criptográficos IKE e IPSec compatibles con Riverbed SteelConnect SD-WAN
- Perfiles criptográficos IKE e IPSec compatibles con Silver Peak SD-WAN
- Perfiles de cifrado IKE e IPSec compatibles con Viptela SD-WAN

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Conexiones de servicio de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Una conexión de servicio, también conocida como un Nodo de Acceso Corporativo (CAN), permite a los usuarios móviles y a los usuarios de redes remotas acceder a aplicaciones y recursos privados, y permite que sus usuarios móviles y redes remotas se comuniquen entre sí.

Además de las Conexiones de servicio, Palo Alto Networks le ofrece otros servicios que puede utilizar para acceder a aplicaciones privadas:

- ZTNA Connector: el Conector de acceso a la red de confianza cero (ZTNA) le permite conectar Prisma Access a las aplicaciones privadas de su organización de manera sencilla y segura. ZTNA Connector proporciona a los usuarios móviles y a los usuarios en sucursales acceso a sus aplicaciones privadas mediante un túnel seguro automatizado. También puede descubrir automáticamente aplicaciones privadas para ZTNA que protegen utilizando Cloud Identity Engine.
- Prisma AccessColo-Connect: Colo-Connect le permite utilizar Prisma Access para asegurar aplicaciones privadas mediante una interconexión en la nube que puede proporcionar conexiones de servicio de alta capacidad.

Palo Alto Networks recomienda siempre crear una conexión de servicio en su implementación de Prisma Access. Todas las conexiones de servicio tienen estas características:

- Una conexión de servicio permite el acceso a los recursos en su sede o centro de datos.

  Por ejemplo, si su política de seguridad requiere la autenticación de usuarios utilizando un servicio de autenticación local, como su Active Directory, necesitará habilitar Prisma Access para acceder a la ubicación corporativa donde reside el servicio (y configurar una cuenta de servicio que el servicio pueda usar para acceder a ella). De manera similar, si tiene recursos corporativos a los que sus redes remotas y usuarios móviles necesitarán acceder, debe habilitar Prisma Access para acceder a la red corporativa correspondiente.

  Si crea conexiones de servicio por esta razón, debería planificar las conexiones de servicio antes de implementarlas.
- Una conexión de servicio permite que las redes remotas y los usuarios móviles se comuniquen entre sí.

  Incluso si no necesita acceso a su sede o centro de datos, podría necesitar permitir que sus usuarios móviles accedan a sus ubicaciones de red remotas. En este caso, puede crear una conexión de servicio con valores de marcador de posición. Esto es necesario porque, aunque todas las conexiones de red remotas están completamente interconectadas, los usuarios

móviles se conectan a redes remotas utilizando la conexión de servicio en una red de tipo hub-and-spoke. Por esta razón, también podría crear una conexión de servicio con valores de marcador de posición si su conexión de servicio existente no está en una ubicación geográfica ideal.

- Las conexiones de servicio no admiten la localización de idiomas porque no se admite la salida a Internet a través de conexiones de servicio. Prisma Access asigna solo una dirección IP de servicio, una por conexión de servicio, y esa dirección IP está registrada geográficamente en la ubicación de cómputo que corresponde a la ubicación que especifique durante la incorporación.

El número de conexiones de servicio que recibe depende de su licencia de Prisma Access.

- Si tiene una licencia ZTNA o Enterprise, el número de conexiones de servicio depende de la edición de su licencia. Si tiene una edición Local, puede configurar un máximo de dos conexiones de servicio; si tiene una edición Worldwide (Mundial), puede configurar un máximo de cinco conexiones de servicio.
  - ZTNA Connector le permite conectar Prisma Access a las aplicaciones privadas de su organización. ZTNA Connector proporciona a los usuarios móviles y a los usuarios en sucursales acceso a sus aplicaciones privadas mediante un túnel seguro automatizado. Para obtener más información, consulte Prisma Access ZTNA Connector.
- Si gestiona varios inquilinos y tiene una licencia ZTNA o Enterprise, el número de conexiones de servicio por inquilino depende del número de unidades que asigne por inquilino y del tipo de licencia que tenga.
  - Si tiene una licencia Global y asigna al menos 1,000 unidades para un inquilino, puede asignar un máximo de cinco conexiones de servicio para ese inquilino.
  - Si tienes una licencia Global y asigna entre 200 y 999 unidades para un inquilino, puede asignar un máximo de dos conexiones de servicio para ese inquilino (lo mismo que el número de conexiones para una implementación Local).
  - Si tiene una licencia Local, puede asignar un máximo de dos conexiones de servicio por inquilino, independientemente del número de unidades que asigne más allá del mínimo de 200.

  Para las licencias Globales y Locales, puede comprar licencias adicionales para conexiones de servicio si se requieren más. Para conexiones de servicio en implementaciones avanzadas, consulte Prisma Access implementaciones avanzadas de conexión de servicio.

Antes de que pueda empezar a configurar sus conexiones de servicio, revise qué información necesita recopilar primero.

 ©2025 Palo Alto Networks, Inc.

Planificar una conexión de servicio.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Crear conexiones de servicio para permitir que Prisma Access realice las siguientes tareas:

- **Permitir el acceso a los recursos en su sede o centro de datos.**

  Si tiene recursos corporativos a los que sus redes remotas y usuarios móviles necesitan acceder, debe habilitar Prisma Access para acceder a la red corporativa correspondiente.
- **Permitir que las redes remotas y los usuarios móviles se comuniquen entre sí.**

  Incluso si no necesita que sus usuarios de Prisma Access se conecten a su sede o centro de datos, es posible que deba permitir que sus usuarios móviles accedan a sus sitios de red remotos. Se requieren conexiones de servicio para este caso de uso porque, si bien todos los sitios de red remotos están completamente interconectados, la infraestructura del usuario móvil no lo está. La configuración mínima de una conexión de servicio establece la red central y radial que los usuarios móviles necesitan para acceder a una red de sucursal.

  Para mejorar la eficiencia de la red, coloque las conexiones de servicio cerca de la red remota o las redes a las que los usuarios móviles acceden con mayor frecuencia.

Reúna esta información de la sede o del centro de datos

Antes de comenzar a configurar una conexión de servicio, recopile la siguiente información para cada una de sus sedes o centros de datos a los que desee que Prisma Access se conecte para poder conectarse.

No es necesario recopilar esta información si está creando una conexión de servicio solo para permitir que los usuarios móviles accedan a ubicaciones de red remotas.

Para conexiones de servicio **Prisma Access (Managed by Strata Cloud Manager)** y **Prisma Access (Managed by Panorama)**

- ❑ Conexión de cortafuegos, enrutador o dispositivo SD-WAN con capacidad IPSec en su sitio corporativo.
- ❑ Configuración de IPSec para finalizar el túnel VPN principal desde Prisma Access al dispositivo compatible con IPSec en su red corporativa.
- ❑ Configuración de IPSec para finalizar el túnel VPN secundario desde Prisma Access al dispositivo compatible con IPSec en su red corporativa.

  Si tiene una plantilla existente que contiene configuraciones de túnel IPSec, supervisión de túnel y perfil criptográfico IPSec, puede añadir esa plantilla a la pila de plantillas para simplificar el proceso de creación de túneles IPSec. O bien, puede editar el Service_Conn_Template que se crea automáticamente y crear las configuraciones IPSec necesarias para crear el túnel IPSec

 ©2025 Palo Alto Networks, Inc.

de regreso al sitio corporativo. Prisma Access también le proporciona un conjunto de plantillas IPSec predefinidas para algunos dispositivos de red comúnmente utilizados y una plantilla genérica para cualquier dispositivo que no esté incluido en las plantillas predefinidas.

- Lista de subredes IP en el sitio.
- Lista de dominios internos que Prisma Access debe ser capaz de resolver.
- Dirección IP de un nodo de acceso corporativo en el sitio de su red al que Prisma Access puede enviar solicitudes de ping ICMP para la supervisión del túnel IPSec.

  Asegúrese de que esta dirección sea accesible por ICMP desde toda la subred de infraestructura de Prisma Access.
- Configuración de accesibilidad de red para la subred de infraestructura de servicio.

  Haga que toda la subred de infraestructura de servicio sea accesible desde la sede central o el centro de datos. Prisma Access utiliza direcciones IP para todo el tráfico del plano de control desde esta subred.

Para Conexiones de servicio de **Panorama Prisma Access** únicamente:



*Esta información solo es necesaria al planificar conexiones de servicio en **Prisma Access (Managed by Panorama)**.*

- La cuenta de servicio para su autenticación, si es necesaria para el acceso.
- El tipo de enrutamiento (estático o dinámico (BGP)) que se utilizará con las conexiones de servicio.

  Para que Prisma Access (Managed by Panorama) dirija a los usuarios a los recursos que necesitan, debe proporcionar las rutas a los recursos. Puede hacerlo de uno de estos modos:

  - Defina una ruta estática para cada subred o recurso específico al que desea que sus usuarios puedan acceder.
  - Configure BGP entre las ubicaciones de conexión de su servicio y Prisma Access.
  - Utilice una combinación de ambos métodos

 ©2025 Palo Alto Networks, Inc.

Configurar una Conexión de servicio en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Crear conexiones de servicio para permitir que Prisma Access realice las siguientes tareas:

- **Permitir el acceso a los recursos en su sede o centro de datos.**

  Si tiene recursos corporativos a los que sus redes remotas y usuarios móviles necesitan acceder, debe habilitar Prisma Access para acceder a la red corporativa correspondiente. Antes de comenzar a configurar una conexión de servicio, recopile la siguiente información para cada una de sus sedes o centros de datos a los que desee que Prisma Access se conecte para poder conectarse.

  - Conexión de cortafuegos, enrutador o dispositivo SD-WAN con capacidad IPSec en su sitio corporativo.
  - Configuración de IPSec para finalizar el túnel VPN principal desde Prisma Access al dispositivo compatible con IPSec en su red corporativa.
  - Configuración de IPSec para finalizar el túnel VPN secundario desde Prisma Access al dispositivo compatible con IPSec en su red corporativa.

    Si tiene una plantilla existente que contiene configuraciones de túnel IPSec, supervisión de túnel y perfil criptográfico IPSec, puede añadir esa plantilla a la pila de plantillas para simplificar el proceso de creación de túneles IPSec. O bien, puede editar el Service_Conn_Template que se crea automáticamente y crear las configuraciones IPSec necesarias para crear el túnel IPSec de regreso al sitio corporativo. Prisma Access también le proporciona un conjunto de plantillas IPSec predefinidas para algunos dispositivos de red comúnmente utilizados y una plantilla genérica para cualquier dispositivo que no esté incluido en las plantillas predefinidas.
  - Lista de subredes IP en el sitio.
  - Lista de dominios internos que Prisma Access debe ser capaz de resolver.
  - Dirección IP de un nodo de acceso corporativo en el sitio de su red al que Prisma Access puede enviar solicitudes de ping ICMP para la supervisión del túnel IPSec.

    Asegúrese de que esta dirección sea accesible por ICMP desde todo la subred de infraestructura de Prisma Access.
  - Configuración de accesibilidad de red para la subred de infraestructura de servicio.

    Haga que toda la subred de infraestructura de servicio sea accesible desde la sede central o el centro de datos. Prisma Access utiliza direcciones IP para todo el tráfico del plano de control desde esta subred.
  - (Para Prisma Access (Managed by Panorama) únicamente) La cuenta de servicio para su autenticación, si es necesaria para el acceso.

 ©2025 Palo Alto Networks, Inc.

- (Para Prisma Access (Managed by Panorama) solamente) El tipo de enrutamiento (estático o dinámico (BGP)) que se utilizará con las conexiones de servicio.
- (Para Prisma Access (Managed by Panorama) solamente) Para dirigir a los usuarios a los recursos que necesitan, debe proporcionar las rutas a los recursos. Puede hacerlo de uno de estos modos:
  - Defina una ruta estática para cada subred o recurso específico al que desea que sus usuarios puedan acceder.
  - Configure BGP entre las ubicaciones de conexión de su servicio y Prisma Access.
  - Utilice una combinación de ambos métodos

- **Permitir que las redes remotas y los usuarios móviles se comuniquen entre sí.**

  Incluso si no necesita que sus usuarios de Prisma Access se conecten a su sede o centro de datos, es posible que deba permitir que sus usuarios móviles accedan a sus sitios de red remotos. Se requieren conexiones de servicio para este caso de uso porque, si bien todos los sitios de red remotos están completamente interconectados, la infraestructura del usuario móvil no lo está. La configuración mínima de una conexión de servicio establece la red central y radial que los usuarios móviles necesitan para acceder a una red de sucursal.

  Para mejorar la eficiencia de la red, coloque las conexiones de servicio cerca de la red remota o las redes a las que los usuarios móviles acceden con mayor frecuencia.

- Strata Cloud Manager
- Panorama

Configurar una Conexión de servicio en Prisma Access (Strata Cloud Manager)

Para configurar una conexión de servicio para Prisma Access (Managed by Strata Cloud Manager) para permitir el acceso a aplicaciones privadas o recursos corporativos internos, complete los siguientes pasos.

STEP 1 | Seleccione **Workflows (Workflows (Flujos de trabajo))** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicios)** y **Add Service Connection (Añadir conexión de servicio)**.

STEP 2 | Dé a la conexión de servicio un **Name (Nombre)**descriptivo.

STEP 3 | Seleccione la **Prisma Access Location (Ubicación de Prisma Access)** donde se encuentra su sede o centro de datos.

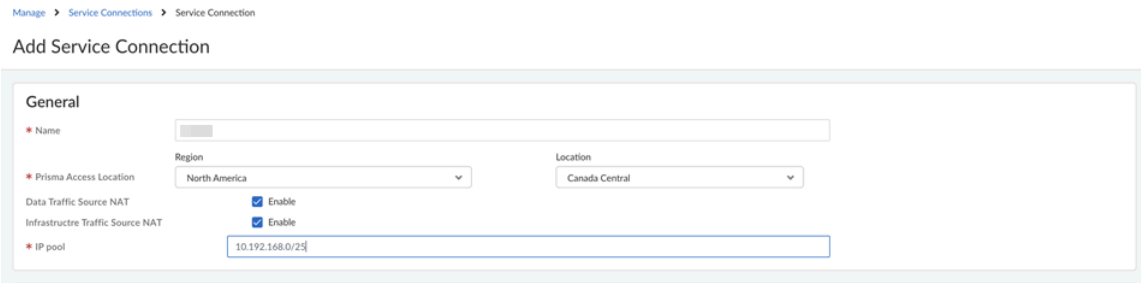
 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Habilite NAT de origen para usuarios móviles: direcciones IP del grupo de GlobalProtect, direcciones IP en la subred de infraestructura o ambas.

Puede especificar una subred en una o más conexiones de servicio que se utilizan para el tráfico NAT entre Prisma Access Usuarios móviles y aplicaciones y recursos privados de GlobalProtect en un centro de datos.

- **NAT de origen de tráfico de datos**: realiza NAT en las direcciones del grupo de direcciones IP del usuario móvil para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncien y enruten en el centro de datos.
- **NAT de origen de tráfico de infraestructura**: realiza NAT en las direcciones de la subred de infraestructura para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncian y enrutan en el centro de datos.
- **User-ID**: cuando se selecciona, Prisma Access utiliza esta conexión de servicio para la redistribución de identidad.

  ***Gestión de redistribución de User-ID**: a veces, se necesitan controles granulares para la redistribución de User-ID en implementaciones de Prisma Access de escala particularmente grande. Gestión de la redistribución de User-ID le permite desactivar manualmente el comportamiento de redistribución de identidad predeterminado para determinadas conexiones de servicio eliminando la marca de verificación en la columna **User ID (ID de usuario)** y, a continuación, seleccionar conexiones de servicio específicas que se utilizarán para la redistribución de identidad. No es necesario hacer esto para la mayoría de las configuraciones. Póngase en contacto con la asistencia de Palo Alto Networks para activar esta funcionalidad.*
- **Grupo NAT de origen**: especifique el grupo de direcciones IP utilizado para realizar NAT en el grupo de direcciones IP del usuario móvil, la subred de infraestructura o ambos.
  - Utilice una subred IP privada (RFC 1918) o una subred adecuada que sea enrutable en su dominio de enrutamiento.
  - Asegúrese de que la subred no se superponga con el grupo de direcciones IP de Usuarios móviles: GlobalProtect, la subred de Infraestructura o cualquier otra dirección NAT de origen utilizada para este inquilino.
  - Introduzca una subred entre /25 y /32.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Seleccione un **IPSec Tunnel (Túnel IPSec)**. Si aún no ha configurado un túnel IPSec primario o secundario, seleccione**Set Up (Configurar)** y siga los pasos a continuación.

1. Asigne un **Name (Nombre)** descriptivo al túnel.
2. Seleccione el **Branch Device Type (Tipo de dispositivo de sucursal)** para el dispositivo IPSec y la sede o el centro de datos que está utilizando para establecer el túnel con Prisma Access.
3. Para la **Branch Device IP Address (Dirección IP del dispositivo de sucursal)**, elija usar una dirección **Static IP (IP estática)** que identifique el endpoint del túnel o una dirección IP **Dynamic (Dinámica)**.

   Si establece la **Branch Device IP Address (Dirección IP del dispositivo de sucursal)** en **Dynamic (Dinámica)**, también debe añadir el ID de ICR para la sede/centro de datos [**IKE Local Identification (Identificación local de IKE)**] o para [**IKE Peer Identification (Identificación de peer IKE)**] de Prisma Access para permitir que los peers IPSec se autentiquen.

   Dado que no tiene los valores que se van a utilizar para el ID de IKE de Prisma Access [**IKE Peer Identification (Identificación de peers de IKE)**] hasta que la conexión del servicio esté completamente implementada, normalmente querrá establecer el ID de IKE para la sede o centro de datos [**IKE Local Identification (Identificación local de IKE)**] en lugar del ID de IKE de Prisma Access.

STEP 6 | Active la **Tunnel Monitoring (Supervisión de túneles)**

Introduzca una dirección de **Destination IP (IP de destino)** de supervisión de túnel en la red de la sede o base de datos para que Prisma Access la use, determine si el túnel está activo y, si su dispositivo IPSec de sucursal usa VPN basada en políticas, introduzca el **Proxy ID (ID de proxy)** asociado.

La dirección IP de supervisión de túnel que introduzca se añadirá automáticamente a la lista de redes secundarias de sucursales.

STEP 7 | Elija **Save (Guardar)** la configuración del túnel.

STEP 8 | Para añadir o ajustar la configuración de enrutamiento y calidad del servicio, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración)** > **Service Connections (Conexiones de servicio)**y **Add Service Connection (Añadir conexión de servicio)**. Deberá **Configure (Configurar)** o **Edit (Editar)** la configuración de **Routing (Enrutamiento)** o **QoS**.

STEP 9 | Configurar rutas estáticas.

1. Si utiliza rutas estáticas para enrutar el tráfico hacia y desde sitios de red remotos, seleccione **Add (Añadir)** para añadir las subredes IP o las direcciones IP que desea proteger en el sitio.

   Si realiza algún cambio en las subredes IP de su red central o del centro de datos, deberá actualizar manualmente las rutas estáticas.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Configurar enrutamiento dinámico.

1. Para que el enrutamiento dinámico anuncie subredes de la sede central o del centro de datos, seleccione **Enable BGP for Dynamic Routing (Habilitar BGP para enrutamiento dinámico)**.
2. (Opcional) Seleccione un valor de **MRAI Timer (Temporizador MRAI)**.

   El enrutamiento BGP ofrece un temporizador que puede utilizar para adaptar la convergencia del enrutamiento BGP en su red llamada el *Intervalo mínimo de anuncio de ruta (MRAI)*. El MRAI actúa para limitar la velocidad de las actualizaciones según el destino, y los enrutadores BGP esperan al menos el tiempo MRAI configurado antes de enviar un anuncio para el mismo prefijo. Un número menor le proporciona un tiempo de convergencia más rápido pero crea más anuncios en su red. Un número mayor disminuye la cantidad de anuncios que se pueden enviar, pero también puede hacer que la convergencia de enrutamiento sea más lenta. Usted decide el número que desea colocar en su red para lograr el mejor equilibrio entre una convergencia de enrutamiento más rápida y menos anuncios.

   Configure un rango de MRAI de entre 1 y 600 segundos, con un valor predeterminado de 30 segundos.
3. Para reducir la cantidad de anuncios de subred IP de usuarios móviles a través de BGP a su equipo local del cliente (CPE), especifique Prisma Access para resumir las subredes antes de anunciarlas seleccionando **Summarize Mobile User Routes before advertising (Resumir rutas de usuarios móviles antes de anunciarlas)**.

   De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred especificada. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.
4. (Opcional) Para que Prisma Access desarrolle un anuncio de ruta predeterminada para la red remota usando eBGP, seleccione **Advertise the Default Route (Anunciar la ruta predeterminada)**. Asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.
5. (Opcional) Si configuró una WAN secundaria y necesita cambiar la dirección de peer para el peer de BGP secundario (de respaldo), seleccione **Use different BGP Peer for Secondary Tunnel (Utilice un par BGP diferente para el túnel secundario)** e introduzca un peer único y, opcionalmente, una dirección IP local para la WAN secundaria.
6. Para añadir una comunidad desde las conexiones de servicio a los prefijos salientes desde los pares eBGP en el equipo de las instalaciones del cliente (CPE), establezca **Add no-export community (Añadir comunidad sin exportación)** en **Enabled Out (Habilitado de salida)**. Esta capacidad está **Disabled (Deshabilitada)** de manera predeterminada.

   No seleccione **Enabled In (Habilitado en)** o **Enabled Both (Habilitado ambos)** ya que estas opciones no son compatibles.

 ©2025 Palo Alto Networks, Inc.

7. (Opcional) Seleccione **Do Not Export Routes (No exportar rutas)** para evitar que Prisma Access reenvíe rutas a la sede central o al centro de datos.

   Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

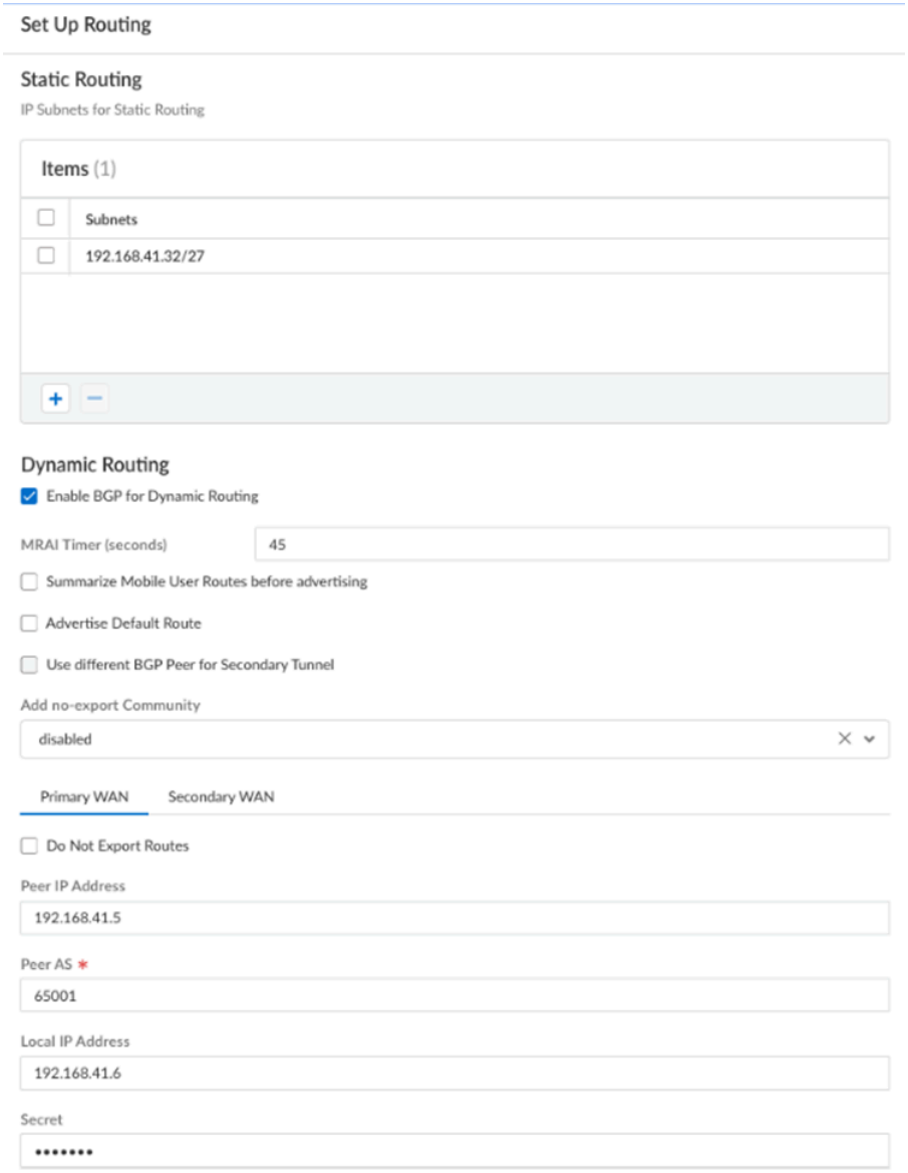
   Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en su equipo local para establecer rutas de regreso a Prisma Access.
8. Introduzca la **Peer IP Address (Dirección IP del peer)** asignada como ID del enrutador eBGP en la red de la sede central o del centro de datos.
9. Introduzca el **Peer AS (AS del peer)**, el sistema autónomo (AS) para su red.

   Utilice un número AS privado BGP compatible con RFC 6996.
10. Introduzca la **Local IP Address (Dirección IP local)** que Prisma Access utiliza como su dirección IP local para BGP.

    Solo se requiere una dirección local si su dispositivo de centro de datos o sede central la requiere para que el intercambio de BGP se realice correctamente. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP en la subred de infraestructura o subredes de la red remota.
11. Introduzca una contraseña **Secret (Secreta)** para autenticar las comunicaciones entre peers de BGP.

 ©2025 Palo Alto Networks, Inc.

12. Seleccione **Confirm Secret (Confirmar secreto)**.

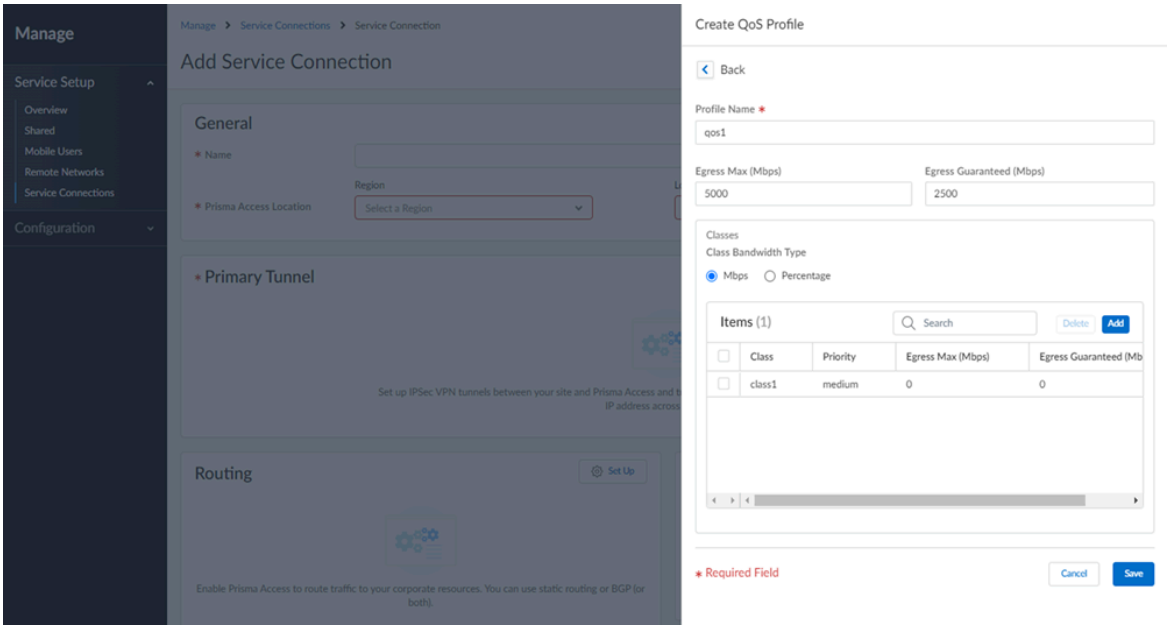


STEP 11 | (Optional) Configure QoS.

Para comenzar, añada un perfil de QoS para definir las clases de QoS que darán forma al tráfico entre la sede o el centro de datos y Prisma Access. Luego, creará una regla de política de QoS

 ©2025 Palo Alto Networks, Inc.

y añadirá el perfil a la regla para aplicar la QoS en el tráfico de la sede central o del centro de datos correspondiente.



1. Introduzca un nombre para su **QoS Profile (Perfil de QoS)**.
2. Seleccione **Create New (Crear nueva)**.
3. Establezca el rendimiento máximo (en Mbps) para el tráfico que sale de la conexión de servicio de la sede central o del centro de datos como **Egress Max (Máx. de salida)**.

   Puede especificar un valor hasta el ancho de banda máximo autorizado de su sede o centro de datos.
4. Establezca el ancho de banda garantizado como **Egress Guaranteed (Salida garantizada)** (en Mbps).

   Cualquier tráfico que supere el valor de Salida garantizada será la mejor opción pero no estará garantizado. Cualquier ancho de banda garantizado pero no utilizado permanece disponible para todo el tráfico.
5. Defina cada **Class (Clase)** de QoS y adjúntela a una regla de política.

   Una clase de QoS determina la prioridad y el ancho de banda del tráfico que coincide con una regla de la política de QoS. Hay hasta ocho clases de QoS definibles en un único

 ©2025 Palo Alto Networks, Inc.

perfil de QoS. A menos que esté configurado de otra forma, al tráfico que no coincida con una clase de QoS se le asignará la clase 4.

6. Configure la **Priority (Prioridad)** de una clase QoS.

   Las prioridades incluyen tiempo real, alta, media o baja.

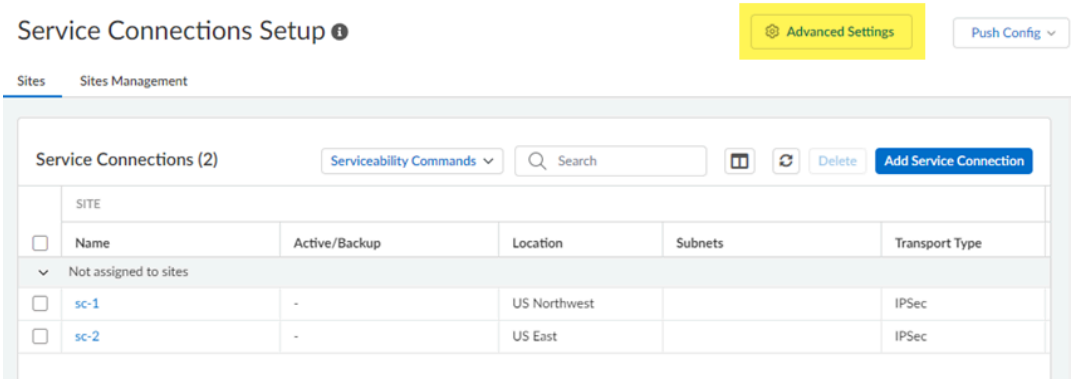
7. Configure el valor **Egress Max (Máx. de salida)**.

   El valor máximo de salida para una clase de QoS, o los valores máximos de salida combinados para múltiples clases de QoS, no deben exceder el valor máximo de salida del perfil de QoS.

8. Configure el valor de **Egress Guaranteed (Salida garantizada)**.

   El ancho de banda garantizado asignado a la clase QoS no está reservado para esa clase; el ancho de banda no utilizado permanece disponible para todo el tráfico. Todo el tráfico que supere el valor garantizado de salida será la mejor opción pero no estará garantizado.

STEP 12 | Configure la **Advanced Settings (Configuración avanzada)** para su conexión de servicio.



1. Especifique las **BGP Routing Preferences (Preferencias de enrutamiento BGP)** para usar con conexiones de servicio.

   Puede especificar las preferencias de red para utilizar la red de su organización o la red de Prisma Access, para procesar el tráfico de conexión de servicio.

   - **Default (Predeterminado)**: Prisma Access utiliza el enrutamiento predeterminado en su red interna.
   - **Hot potato routing (Enrutamiento Hot Potato)**: Prisma Access transfiere el tráfico de conexión de servicio a la WAN de su organización lo más rápido posible.

   > *Cambiando el método de enrutamiento de la conexión de servicio de Prisma Access requiere una comprensión profunda de la topología y los dispositivos de enrutamiento de su organización, junto con una comprensión de cómo funciona el enrutamiento de Prisma Access. Le recomendamos leer* Enrutamiento para el tráfico de conexión de servicio *con cuidado antes de cambiar el método de enrutamiento predeterminado.*

2. **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Retirar rutas estáticas si el túnel IPSec de Conexión de servicio o Redes remotas está**

 ©2025 Palo Alto Networks, Inc.

inactivo) si desea que Prisma Access elimine las rutas estáticas cuando un túnel deja de funcionar sin un túnel de respaldo.

Prisma Access elimina la ruta en las siguientes situaciones:

- El túnel principal desciende y no hay túnel secundario.
- Si se configura un túnel primario y uno secundario, pero ambos dejan de funcionar.

No se puede aplicar este cambio si la supervisión del túnel no está habilitada.

3. Configure el **Backbone Routing (Enrutamiento de red troncal)** que se utilizará para las conexiones de servicio.

   De forma predeterminada, la red troncal de Prisma Access requiere que usted tenga una ruta de red simétrica para el tráfico que regresa desde el centro de datos o la ubicación de la sede central a través de una conexión de servicio. Si desea utilizar ECMP u otro mecanismo de equilibrio de carga para las conexiones de servicio desde su CPE, puede habilitar flujos asimétricos a través de la red troncal de Prisma Access.

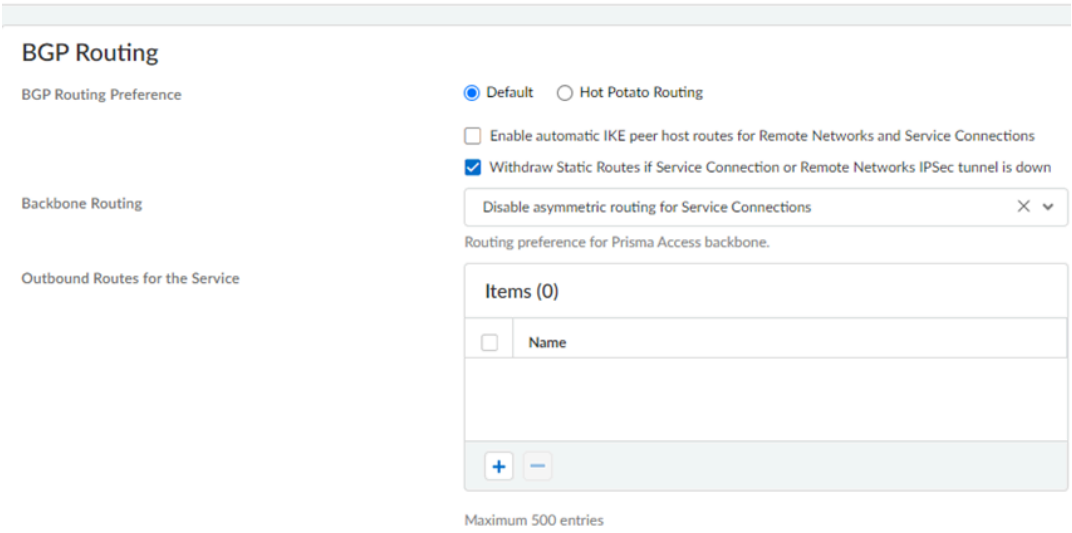
   - Seleccione **Disable asymmetric routing for Service Connections (Deshabilitar enrutamiento asimétrico para conexiones de servicio)** para requerir flujos simétricos a través de la red troncal de conexión de servicio.
   - Seleccione **Allow asymmetric routing for Service Connections (Permitir enrutamiento asimétrico para conexiones de servicio)** para permitir que Prisma Access utilice flujos asimétricos a través de la red troncal de conexión de servicio.
   - Si tiene varias conexiones de servicio a una ubicación, puede aprovechar el equilibrio de carga en su implementación de Prisma Access seleccionando **Allow asymmetric routing and load sharing across Service Connections (Permitir enrutamiento asimétrico y distribución de carga entre conexiones de servicio)** (el ajuste predeterminado). Sin embargo, el equilibrio de carga se realiza según el máximo esfuerzo y fallará si una de las conexiones de servicio falla.

     Cuando selecciona **Allow asymmetric routing and load sharing across Service Connections (Permitir enrutamiento asimétrico y distribución de carga entre conexiones de servicio)**, Prisma Access habilita la redundancia de red entre los portales y puertas de enlace de GlobalProtect, y las conexiones de servicio. Esta funcionalidad proporciona rutas de red redundantes entre el plano de datos del usuario móvil y las conexiones de servicio en diferentes ubicaciones de cómputo. Al habilitar la redundancia, los usuarios tienen acceso más resistente a los recursos detrás de las conexiones de servicio en un centro de datos o en las ubicaciones de las oficinas centrales. Dado que se requiere una conexión de servicio para que los usuarios móviles accedan a recursos desde redes remotas, los usuarios también tienen más capacidad de recuperación para acceder a recursos en ubicaciones de redes remotas.

4. (Opcional) Especifique las **Outbound Routes for the Service (Rutas de salida para el servicio)** añadiendo hasta 500 prefijos para los cuales Prisma Access añade rutas

 ©2025 Palo Alto Networks, Inc.

estáticas en todas las conexiones de servicio y conexiones de red remotas. Prisma Access luego dirige el tráfico hacia estos prefijos a través de Internet.



Más opciones de IKE

Según el tipo de dispositivo IPSec que haya seleccionado, Prisma Access proporciona un conjunto recomendado de cifrados y una vida útil de la clave para el proceso de intercambio de claves IKE de fase 1 entre el dispositivo en su sede o centro de datos y Prisma Access. Puede utilizar la configuración recomendada o personalizar la configuración según sea necesario para su entorno.

- Seleccione una **IKE Protocol Version (Versión del protocolo IKE)** para su dispositivo IPSec y Prisma Access para usar para la negociación IKE.

  Si selecciona **IKEv1 Only Mode (Modo de solo IKEv1)**, Prisma Access solo podrá usar el protocolo IKEv1 para la negociación. Si selecciona **IKEv2 Only Mode (Modo de solo IKEv2)**, Prisma Access solo podrá usar el protocolo IKEv2 para la negociación. Si selecciona el **IKEv2 Preferred Mode (Modo preferido de IKEv2)**, Prisma Access utiliza el protocolo IKEv2 solo si su dispositivo IPSec también admite IKEv2. Si su dispositivo IPSec no es compatible con IKEv2, Prisma Access recurre al protocolo IKEv1.

 ©2025 Palo Alto Networks, Inc.

- Añada un **IKEv1 Crypto Profile (Perfil criptográfico IKEv1)** para personalizar la configuración criptográfica de IKE que define los algoritmos de cifrado y autenticación utilizados para el proceso de intercambio de claves en la Fase 1 de IKE.

  Prisma Access utiliza automáticamente un perfil criptográfico IKE predeterminado según el **Branch Device Type (Tipo de dispositivo de sucursal)** que se utiliza para establecer dicho túnel.

  - **Encryption (Cifrado)**: especifique el algoritmo de cifrado utilizado en la negociación de SA de IKE.

    Prisma Access admite los siguientes algoritmos de cifrado: 3des (168 bits), aes-128-cbc (128 bits), aes-192-cbc (192 bits), aes-256-cbc (256 bits) y DES (56 bits). También puede seleccionar nulo (sin cifrado).
  - **Authentication (Autenticación)**: especifique el algoritmo de autenticación utilizado en la negociación de SA de IKE.

    Prisma Access es compatible con los siguientes algoritmos de autenticación: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) y md5 (128 bits). También puede seleccionar nulo (sin autenticación).
  - **Grupo DH:**especifique los grupos Diffie-Hellman (DH) utilizados para generar claves simétricas para IKE en la negociación de SA de IKE. El algoritmo Diffie Hellman usa la clave privada de una parte y la clave pública de la otra para crear un secreto compartido, que es una clave cifrada compartida por ambos peers del túnel VPN.

    Prisma Access es compatible con los siguientes grupos DH: grupo 1 (768 bits); grupo 2 (1.024 bits—predeterminado); grupo 5 (1,536 bits); grupo 14 (2,048 bits), grupo 19 (grupo de curva elíptica de 256 bits) y grupo 20 (grupo de curva elíptica de 384 bits). Para mayor seguridad, seleccione el grupo con el número más alto.
  - **Lifetime (Vida útil)**: especifique la unidad y el tiempo durante la cual la clave IKE de fase 1 es válida (el valor predeterminado es 8 horas). Para IKEv1, la asociación de seguridad (SA) no se vuelve a generar activamente antes de que caduque la vida útil de la clave. La nueva clave de IKEv1 de fase 1 se activa solo cuando caduca la SA. Para IKEv2, es necesario volver a introducir la clave de SA antes de que caduque la vida útil de la clave. Si no se vuelve a introducir la clave de la SA al vencimiento, la SA debe comenzar una nueva clave de fase 1.
  - **IKEv2 Authentication Multiple (Autenticación IKEv2 múltiple)**: Especifique el valor que se multiplica por la duración de la clave para determinar el recuento de autenticación (rango: 0-50; valor predeterminado: 0). El recuento de autenticaciones es el número de veces que el nodo de procesamiento de seguridad puede regenerar la clave de codificación de SA IKE IKEv2 antes de que deba volver a empezar con la reautenticación IKEv2. El valor predeterminado 0 deshabilita la función de reautenticación.

- Habilite el **IKE Passive Mode (Modo pasivo IKE)** para que Prisma Access solo responda a las conexiones IKE y no las inicie.

- **IKE NAT Traversal (NAT transversal de IKE)** está activado de forma predeterminada.

  Esto significa que la encapsulación UDP se utiliza en los protocolos IKE y UDP, lo que les permite pasar a través de dispositivos de traducción de direcciones de red (NAT) que se encuentran entre los endpoints del túnel IPSec VPN.

 ©2025 Palo Alto Networks, Inc.

Más opciones de IPSec

En base al tipo de dispositivo IPSec que haya seleccionado, Prisma Access proporciona un conjunto recomendado de protocolos IPSec y ajustes clave de vida útil para proteger los datos dentro del túnel IPSec entre su dispositivo IPSec y Prisma Access en IKE de fase 2 para la asociación de seguridad (SA). Puede utilizar la configuración recomendada o personalizar la configuración según sea necesario para su entorno.

- Personalice el **IPSec Crypto Profile (Perfil criptográfico de IPSec)** para definir cómo se protegen los datos dentro del túnel cuando Auto Key IKE genera automáticamente claves para las SA de IKE durante la fase 2 de IKE.

  Prisma Access configura automáticamente un perfil de cifrado IPSec predeterminado basado en el proveedor de **Branch Device Type (Tipo de dispositivo de sucursal)**. Puede usar el perfil predeterminado o crear un perfil personalizado.

  - **IPSec Protocol (Protocolo IPSec)**: proteja los datos que atraviesan el túnel VPN. El protocolo de carga de seguridad encapsulada (**ESP**) cifra los datos, autentica el origen y verifica la integridad de los datos. El protocolo de encabezado de autenticación **AH** autentica el origen y verifica la integridad de los datos.

    Si utiliza **ESP** como protocolo IPSec, especifique también el algoritmo de **Encryption (Cifrado)** utilizado en la negociación SA de IPSec.

    Prisma Access es compatible con los siguientes algoritmos de cifrado: aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits) y DES (56 bits). También puede seleccionar nulo (sin cifrado).

- **Authentication (Autenticación)**: especifique el algoritmo de autenticación utilizado en la negociación de SA de IPSec.

  Prisma Access es compatible con los siguientes algoritmos de autenticación: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) y md5 (128 bits). Si define el Protocolo IPSec en ESP, también podrá seleccionar ninguno (sin autenticación).

- **DH Group (Grupo DH)**: especifique los grupos Diffie-Hellman (DH) para IKE en la negociación de la asociación de seguridad (SA) IPSec.

  Prisma Access es compatible con los siguientes grupos DH: grupo 1 (768 bits); grupo 2 (1.024 bits—predeterminado); grupo 5 (1,536 bits); grupo 14 (2,048 bits), grupo 19 (grupo de curva elíptica de 256 bits) y grupo 20 (grupo de curva elíptica de 384 bits). Para mayor seguridad, seleccione el grupo con el número más alto. Si no desea renovar la clave que crea Prisma Access durante la fase 1 de IKE, seleccione **no-pfs** (sin secreto perfecto hacia adelante). Si selecciona esta opción, Prisma Access reutiliza la clave actual para la negociación SA de IPSec.

- **Lifetime (Vida útil)**: especifique la unidad y el tiempo durante el cual la clave negociada es válida (por defecto es 1 hora).

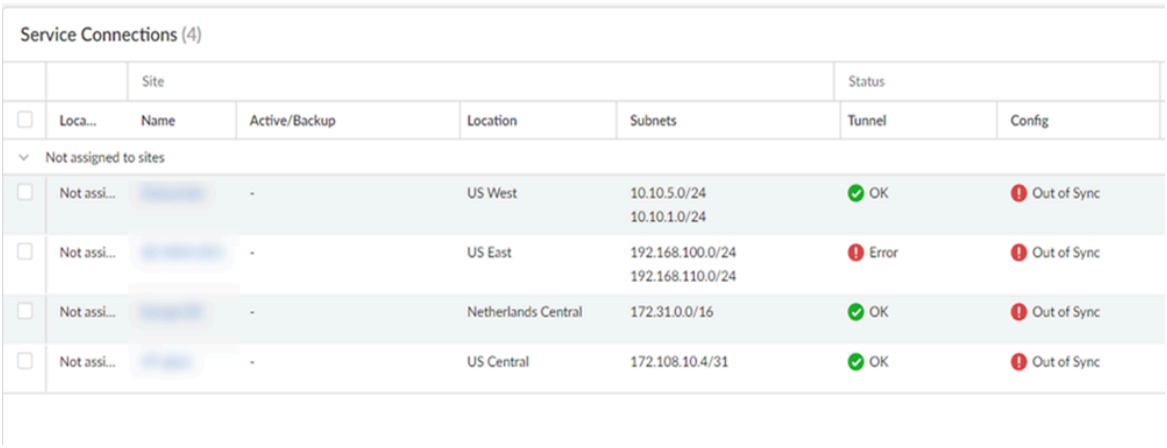
- **Lifesize (Tamaño real**: especifique la unidad y el volumen de datos que la clave puede utilizar para el cifrado.

 ©2025 Palo Alto Networks, Inc.

Verificar estado de la conexión del servicio

Para verificar que la conexión del servicio se haya configurado correctamente, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)** y verifique que el **Status (Estado)** sea **OK (Aceptar)**.

Si el estado no es **OK (Correcto)**, pase el cursor sobre el icono de Estado para ver los errores.



El área **Sites (Sitios)** le permite ver todas las conexiones de servicio incorporadas, junto con su estado y otros detalles sobre ellas.

Sitio

- **Name (Nombre)**: el nombre de la conexión de servicio.
- **Active/Backup (Activo/Copia de seguridad)**: las ubicaciones activas y de copia de seguridad de la conexión de servicio.
- **Subnets (Subredes)**: las subredes de infraestructura asignadas a la conexión de servicio.

estado

- **Tunnel (Túnel)**: el estado operativo de la conexión entre Prisma Access y su conexión de servicio.
- **Config (Configurar)**: el estado de la última configuración enviada al servicio. Si la configuración local y la configuración en la nube coinciden, el Estado de configuración es **In sync (Sincronizado)**. Si ha realizado un cambio localmente y aún no ha enviado la configuración a la nube, es posible que se muestre el estado **Out of sync (Fuera de sincronización)**. Pase el cursor sobre el indicador de estado para obtener información más detallada. Después de confirmar y enviar la configuración a Prisma Access, el estado de configuración cambia a **In sync (Sincronizado)**.

Prisma Access

- **Location (Ubicación)**: la ubicación donde se implementa la conexión del servicio.
- **Service IP (IP del servicio)**: la dirección IP de la conexión del servicio.
- **EBGP Router (Enrutador EBGP)**: la dirección IP del enrutador EBGP en la conexión de servicio.

Enlaces

- **BGP IPv4**: el estado del enrutamiento BGP con IPv4 en la conexión de servicio.
- **BGP IPv6**: el estado del enrutamiento BGP con IPv6 en la conexión de servicio.

 ©2025 Palo Alto Networks, Inc.

- **IPSec Tunnel (Túnel IPSec)**: el túnel IPSec de su conexión de servicio. El primer túnel IPSec que establezca será el túnel **(Primary) [principal]**. Si establece un segundo túnel IPSec, este será el túnel **(Secondary) [Secundario]**.
- **Peer IP Address (Dirección IP del peer)**: la dirección IP de la puerta de enlace de la conexión del servicio.

Configurar una Conexión de servicio en Prisma Access (Panorama)

Para configurar una conexión de servicio para Prisma Access Panorama, para permitir el acceso a aplicaciones privadas o recursos corporativos internos, complete los siguientes pasos.

No utilice la CLI para incorporar y configurar conexiones de servicio. Si necesita el uso de la CLI para integrar conexiones de servicio, póngase en contacto con su equipo de Palo Alto Networks.

STEP 1 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service connection (Conexión de servicio)**.

STEP 2 | **Add (Añadir)** una nueva conexión de servicio a uno de los sitios de su red corporativa.

STEP 3 | Especifique un **Name (Nombre)** para el sitio corporativo.

STEP 4 | Seleccione la **Location (Ubicación)** más cercana a donde se encuentra el sitio.

Consulte esta sección para obtener una lista de ubicaciones de Prisma Access.

Las ubicaciones denotadas con dos asteriscos son **Local Zones (Zonas locales)**. Estas ubicaciones colocan los servicios de cómputo, almacenamiento, bases de datos e infraestructura cerca de grandes centros de población e industrias, sin embargo, también tienen algunas limitaciones. Para añadir una zona local, póngase en contacto con su representante de Palo Alto Networks.

STEP 5 | Seleccione o añada una nueva configuración de **IPSec Tunnel (Túnel IPSec)** para acceder al cortafuegos, enrutador o dispositivo SD-WAN en la ubicación corporativa:

- Si usa una configuración de **IPSec Tunnel (Túnel IPSec)** existente, selecciónala en el menú desplegable. Tenga en cuenta que el túnel que crea para cada conexión de servicio conecta Prisma Access al dispositivo compatible con IPSec en cada ubicación corporativa. Las direcciones de peers en la configuración de IKE Gateway deben ser únicas para cada túnel. Sin embargo, puede reutilizar algunos de los otros elementos de configuración comunes, como los perfiles criptográficos.

  El túnel IPSec que seleccione de una plantilla debe utilizar el intercambio automático de claves e IPv4 únicamente. Además, asegúrese de que los nombres del túnel IPSec, la puerta de enlace IKE y el perfil criptográfico tengan 31 caracteres como máximo.

- Para crear una nueva configuración de túnel IPSec:

  Haga clic en **New IPSec Tunnel (Nuevo túnel IPSec)**, asígnele un **Name (Nombre)** y configure la IKE Gateway (Puerta de enlace IKE), el IPSec Crypto Profile (Perfil criptográfico IPSec), y los ajustes de la Tunnel Monitoring (Supervisión de túneles).

 ©2025 Palo Alto Networks, Inc.

- Si el dispositivo con capacidad IPSec en su sede o ubicación de centro de datos utiliza VPN basada en políticas:

  En la pestaña **Proxy IDs (ID de proxy)**, deberá **Add (Añadir)** un ID de proxy que coincida con la configuración configurada en su dispositivo IPSec local para garantizar que Prisma Access pueda establecer correctamente un túnel IPSec con su dispositivo local.
- Para detectar y neutralizar ataques de respuesta:

  Deje **Enable Replay Protection (Habilitar protección de reproducción)**.
- Para conservar la información original de ToS:

  Marque **Copy TOS Header (Copiar encabezado de TOS)** para copiar el encabezado del tipo de servicio (ToS) del encabezado de la IP interna en el encabezado de la IP externa de los paquetes encapsulados.
- Para habilitar la supervisión de túnel para la conexión de servicio:

  Seleccione **Tunnel Monitor (Supervisión de túnel)**:

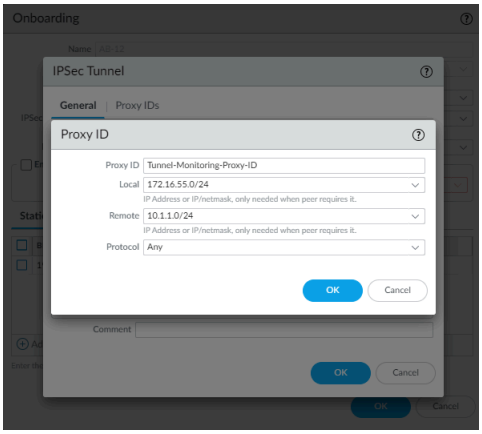
  - Introduzca una dirección **Destination IP (IP de destino)**.

    Especifique una dirección IP en su sede o centro de datos a la que Prisma Access pueda enviar solicitudes de ping ICMP para la supervisión del túnel IPSec. Asegúrese de que el ICMP pueda acceder a esta dirección desde toda la subred de la infraestructura de Prisma Access.
  - Si utiliza la supervisión de túnel con un dispositivo de peer que utiliza varios ID de proxy, especifique un **Proxy ID (ID de proxy)** o añada un **New Proxy ID (ID de proxy nuevo)** que permita el acceso desde la subred de la infraestructura a su sede central o al sitio del centro de datos.

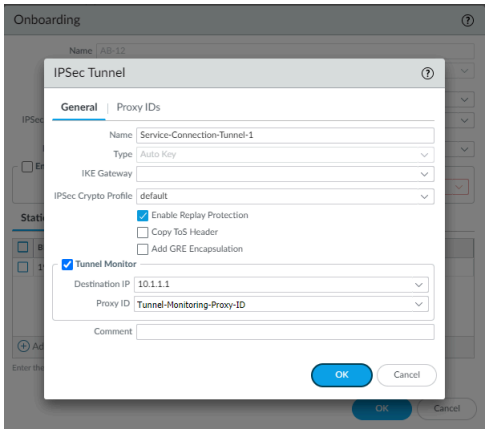
    La siguiente figura muestra un ID de proxy con la subred de infraestructura de servicio (172.16.55.0/24 en este ejemplo) como la subred de IP **Local (Local)** y la subred de la

 ©2025 Palo Alto Networks, Inc.

sede central o del centro de datos (10.1.1.0/24 en este ejemplo) como la subred **Remote (Remota)**.



La siguiente figura muestra el ID de proxy que creó aplicándose a la configuración del monitor de túnel mediante su especificación en el campo **Proxy ID (ID de proxy)**.



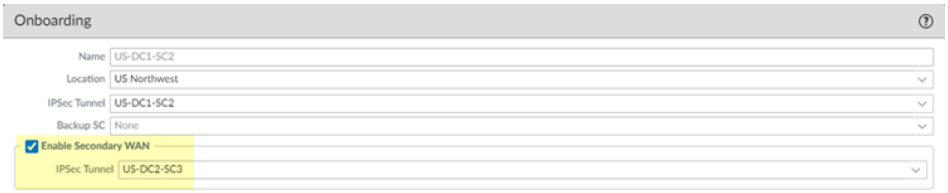
*Debe configurar en su CPE una ruta estática a la dirección IP del monitor de túnel para que funcione la supervisión del túnel. Para encontrar la dirección IP de destino que se utilizará para la supervisión de túneles desde su centro de datos o red de la sede hasta Prisma Access, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de red)**, haga clic en el botón de opción **Service Infrastructure (Infraestructura de servicio)** y busque la **Tunnel Monitor IP Address (Dirección IP de la supervisión del túnel**.*

STEP 6 | Solo implementaciones de enrutamiento de BGP y hot potato: seleccione una conexión de servicio para usar como copia de seguridad preferida [**Backup SC (SC de copia de seguridad)**].

Puede seleccionar cualquier conexión de servicio que ya haya añadido. Prisma Access utiliza la **Backup SC (Copia de seguridad SC)** que seleccione como la conexión de servicio preferida en caso de fallo del enlace. La selección de una conexión de servicio de respaldo puede evitar

 ©2025 Palo Alto Networks, Inc.

problemas de enrutamiento asimétrico si ha incorporado más de dos conexiones de servicio. Esta opción está disponible en el modo de ruta de hot potato únicamente.



STEP 7 | Si tiene un enlace WAN secundario en esta ubicación, seleccione **Enable Secondary WAN (Habilitar WAN secundaria)** y luego seleccione o configure un **IPSec Tunnel (Túnel IPSec)** de la misma manera que lo hizo para configurar el túnel IPSec primario.

Si el enlace WAN principal falla, Prisma Access detecta la interrupción y establece un túnel hasta la sede o la ubicación del centro de datos a través del enlace WAN secundario. Si el enlace WAN principal se activa, el enlace vuelve al enlace principal.

La configuración de una WAN secundaria no se admite en las siguientes implementaciones:

- Si su WAN secundaria está configurada en modo activo/activo con el túnel IPSec primario.
- Si el equipo de las instalaciones del cliente (CPE) está configurado en una configuración de enrutamiento multipath de igual coste (ECMP) con el túnel IPSec primario y secundario.

Si utiliza rutas estáticas, el tiempo de conmutación por error del túnel es inferior a 15 segundos desde el momento de la detección, dependiendo de su proveedor de WAN.

Si configura el enrutamiento de BGP y ha habilitado la supervisión del túnel, el tiempo de espera predeterminado más corto para determinar que un índice de parámetro de seguridad (SPI) está fallando es el monitor del túnel, que elimina todas las rutas a un par cuando detecta un fallo del túnel durante 15 segundos consecutivos. De esta forma, el monitor de túnel determina el comportamiento de las rutas BGP. Si no configura la supervisión del túnel, el temporizador de mantenimiento determina el tiempo que el túnel estará inactivo antes de eliminar la ruta. Prisma Access utiliza el valor BGP HoldTime predeterminado de 90 segundos según lo definido por RFC 4271, que es el tiempo máximo de espera antes de que Prisma Access elimine una ruta para un SPI inactivo. Si el dispositivo peer BGP tiene un tiempo de espera configurado más corto, el temporizador de espera BGP utilizará el valor más bajo.

Cuando el túnel secundario se instala correctamente, la ruta secundaria tiene prioridad hasta que el túnel principal vuelva a subir. Si tanto la ruta primaria como la secundaria están activas, la ruta principal tiene prioridad.

Si utiliza un peer BGP diferente para la conexión secundaria (de respaldo), Prisma Access no respeta los atributos del discriminador de salidas múltiples (MED) anunciados por el CPE. Esta advertencia se aplica si utiliza varios peers BGP en conexiones de red remotas o en conexiones de servicio.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | (Opcional) Habilite NAT de origen para usuarios móviles: direcciones IP del grupo de GlobalProtect, direcciones IP en la subred de infraestructura o ambas.

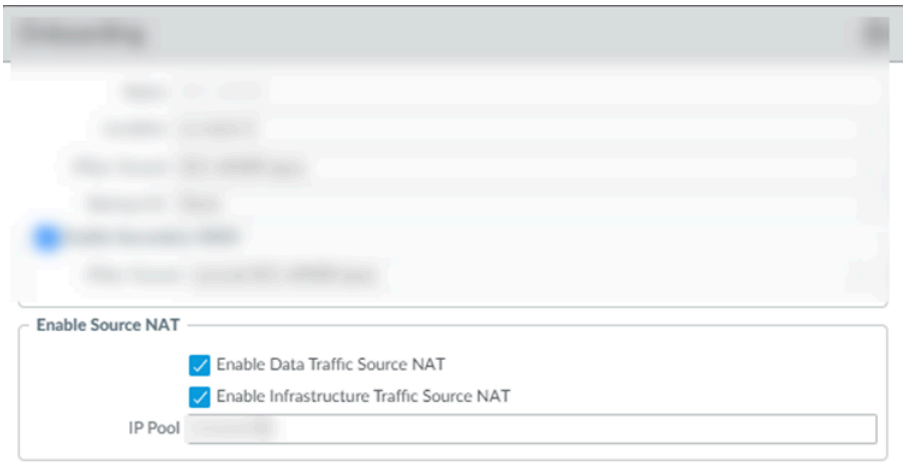
Puede especificar una subred en una o más conexiones de servicio que se utilizan para el tráfico NAT entre Prisma Access Usuarios móviles y aplicaciones y recursos privados de GlobalProtect en un centro de datos.

- **Habilitar NAT de origen de tráfico de datos**: realiza NAT en las direcciones del grupo de direcciones IP del usuario móvil para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncien y enruten en el centro de datos.
- **Habilitar NAT de origen de tráfico de infraestructura**: realiza NAT en las direcciones de la subred de infraestructura para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncian y enrutan en el centro de datos.
- **User-ID**: cuando se selecciona, Prisma Access utiliza esta conexión de servicio para la redistribución de identidad.

  ***Gestión de redistribución de User-ID**: a veces, se necesitan controles granulares para la redistribución de User-ID en implementaciones de Prisma Access de escala particularmente grande. Gestión de la redistribución de User-ID le permite desactivar manualmente el comportamiento de redistribución de identidad predeterminado para determinadas conexiones de servicio eliminando la marca de verificación en la columna **User ID (ID de usuario)** y, a continuación, seleccionar conexiones de servicio específicas que se utilizarán para la redistribución de identidad. No es necesario hacer esto para la mayoría de las configuraciones. Póngase en contacto con la asistencia de Palo Alto Networks para activar esta funcionalidad.*

- **Grupo IP**: especifique el grupo de direcciones IP utilizado para realizar la NAT en el grupo de direcciones IP del usuario móvil, la subred de infraestructura o ambos.

  Utilice una subred IP privada (RFC 1918) o una subred adecuada que se pueda enrutar en su dominio de enrutamiento y que no se solape con el grupo de direcciones IP de GlobalProtect o la subred de infraestructura. Introduzca una subred entre /25 y /32.



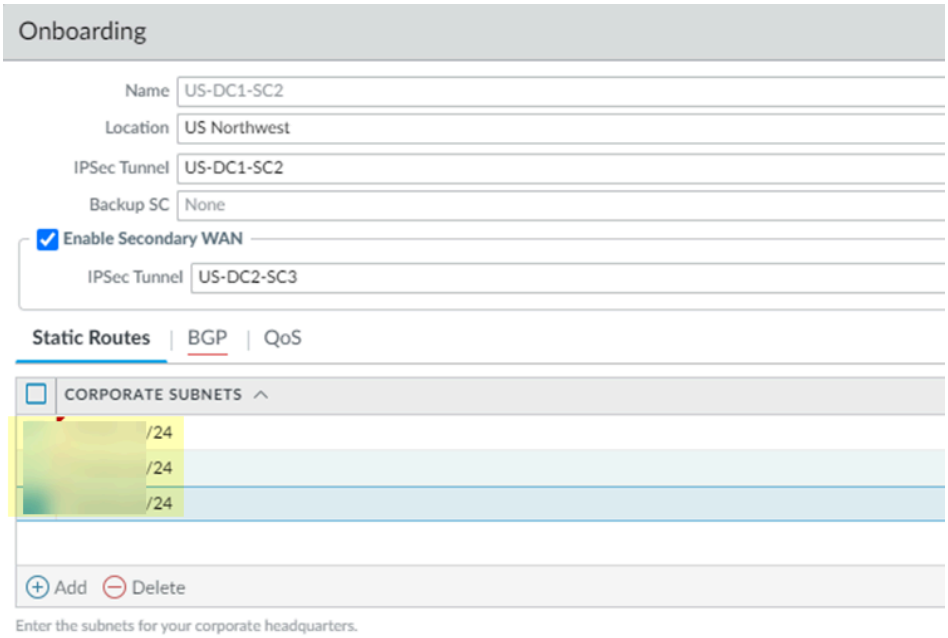
 ©2025 Palo Alto Networks, Inc.

STEP 9 | Habilite el enrutamiento a las subredes o direcciones IP individuales en el sitio corporativo a las que sus usuarios necesitarán acceder.

Prisma Access utiliza esta información para enrutar las solicitudes al sitio apropiado. Las redes de cada sitio no pueden solaparse entre sí ni con los grupos de direcciones IP que haya designado para la infraestructura de servicios o para los grupos IP de Prisma Access para usuarios. Puede configurar **Static Routes (Rutas estáticas)**, **BGP**o una combinación de ambas.

Para configurar **Static Routes (Rutas estáticas)**:

1. En la pestaña **Static Routes (Rutas estáticas)**, haga clic en **Add (Añadir)** e introduzca la dirección de subred (por ejemplo, 172.168.10.0/24) o la dirección IP individual de un recurso, como un servidor DNS (por ejemplo, 10.32.5.1/32) al que sus usuarios remotos necesitarán acceso.
2. Repita para todas las subredes o direcciones IP a las que Prisma Access necesitará acceder en esta ubicación.



Para configurar **BGP**:

1. En la pestaña **BGP**, seleccione **Enable (Habilitar)**.

   Cuando habilita BGP, Prisma Access establece el valor de tiempo de vida (TTL) para BGP externo (eBGP) en 8 para acomodar cualquier salto adicional que pueda ocurrir entre la

 ©2025 Palo Alto Networks, Inc.

infraestructura de Prisma Access y el equipo de las instalaciones del cliente (CPE) que termina la conexión eBGP.

Prisma Access No acepta anuncios de ruta predeterminados de BGP para conexiones de servicio o conexiones de red remotas.

2. (Opcional) Seleccione entre las siguientes opciones:

   - Para añadir una comunidad de **no-export (sin exportación)** para los nodos de acceso corporativo (conexiones de servicio) a los prefijos salientes de los pares de eBGP en el equipo local del cliente (CPE), establezca **Add no-export community (Añadir una comunidad sin exportación)** a **Enabled Out (Habilitado de salida)**. Esta capacidad está **Disabled (Deshabilitada)** por defecto.

     No utilice esta capacidad en el modo de enrutamiento hot potato.

   - Para evitar que el peer de BGP de Prisma Access reenvíe rutas a la red de su organización. **Don't Advertise Prisma Access Routes (No anunciar rutas de Prisma Access)**.

     De forma predeterminada, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Active esta casilla de verificación para evitar que Prisma Access envíe ningún anuncio BGP, pero siga utilizando la información BGP que recibe para conocer rutas de otros vecinos BGP.

     Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.

   - Para reducir el número de anuncios de subredes IP de usuarios móviles a través de BGP a su equipo local del cliente (CPE), especifique Prisma Access para resumir las subredes antes de anunciarlas seleccionando **Summarize Mobile User Routes before advertising (Resumir las rutas de los usuarios móviles antes de anunciarse)**.

     De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred que especificó. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede usar el resumen de grupos IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

     Si tiene habilitado el enrutamiento Hot Potato y habilita el resumen de rutas, Prisma Access ya no antepone AS-PATH, lo que podría causar enrutamiento asimétrico. Asegúrese de que el tráfico de retorno desde el centro de datos o la sede central haya garantizado un retorno simétrico antes de habilitar el resumen de rutas con el enrutamiento de hot potato.

 ©2025 Palo Alto Networks, Inc.

3. (Opcional) Seleccione un valor de temporizador **MRAI**.

   El enrutamiento BGP ofrece un temporizador que puede usar para adaptar la convergencia de enrutamiento BGP en su red llamado *intervalo mínimo de* publicidad de ruta. El MRAI actúa para limitar la velocidad de las actualizaciones según el destino, y los enrutadores BGP esperan al menos el tiempo MRAI configurado antes de enviar un anuncio para el mismo prefijo. Un número menor le proporciona un tiempo de convergencia más rápido pero crea más anuncios en su red. Un número mayor disminuye la cantidad de anuncios que se pueden enviar, pero también puede hacer que la convergencia de enrutamiento sea más lenta. Usted decide el número a poner en su red para el mejor equilibrio entre una convergencia de enrutamiento más rápida y menos anuncios.

   Configure un rango MRAI de entre 1 y 600 segundos, con un valor predeterminado de 30 segundos.
4. Introduzca la dirección IP asignada como el ID del enrutador del enrutador eBGP en el centro de datos/red de la sede para la que está configurando esta conexión de servicio como la **Peer Address (Dirección del peer)**.
5. Introduzca el **Peer AS (AS del peer)**, que es el sistema autónomo (AS) al que pertenece el enrutador virtual del cortafuegos o enrutador BGP en su centro de datos/red de la sede.
6. (Opcional) Introduzca una dirección que Prisma Access utilice como dirección IP local para BGP.

   Especificar una **Local Address (Dirección local)** es útil cuando el dispositivo del otro lado de la conexión (como una puerta de enlace privada virtual de Amazon Web Service (AWS)) requiere una dirección IP local específica para que el peering de BGP se realice correctamente. Asegúrese de que la dirección que especifique no entra en conflicto o se superpone con las direcciones IP de la subred de infraestructura o las subredes de la conexión de servicio.

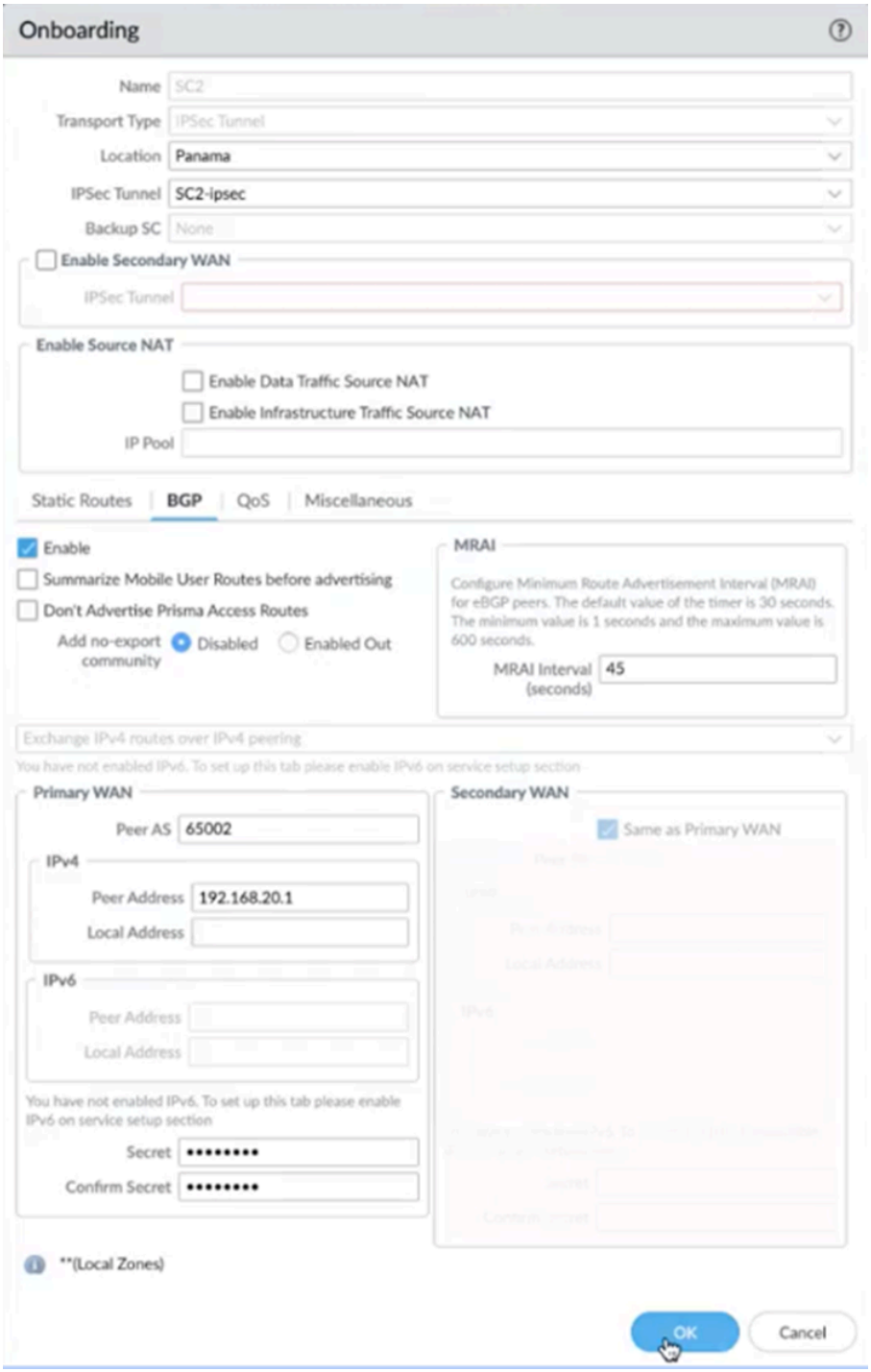
   *Debe configurar una ruta estática en su CPE a la **dirección local** de BGP.*

   Si utiliza compatibilidad con IPV6 para su conexión de servicio, puede configurar las direcciones **IPv6**, así como las direcciones **IPv4**. También necesita habilitar IPv6 networking globalmente en su infraestructura de Prisma Access antes de poder usar el direccionamiento IPv6.

 ©2025 Palo Alto Networks, Inc.

7. (Opcional) Introduzca y confirme una frase de contraseña **Secret (Secreta)** para autenticar las comunicaciones entre peers de BGP

.



STEP 10 | (Opcional) Si configuró una **Secondary WAN (WAN secundaria)** y necesita cambiar la **Peer Address (Dirección del peer)** o la **Local Address (Dirección local)** para el peer BGP secundario (copia de seguridad), anule la marca de **Same as Primary WAN (Igual que la WAN**

 ©2025 Palo Alto Networks, Inc.

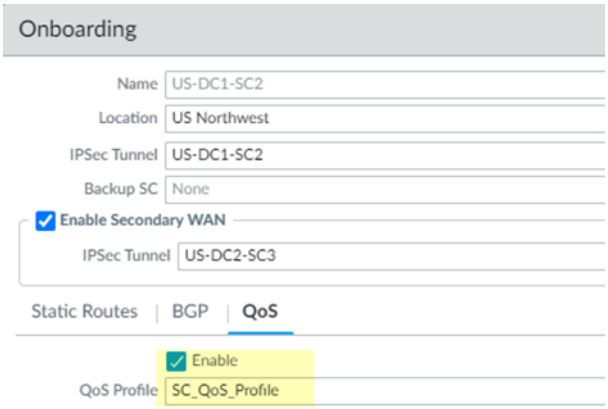
principal) e introduzca un peer único y, opcionalmente, una dirección IP local para la WAN secundaria.

En algunas implementaciones (por ejemplo, cuando se usa BGP para conectarse con una puerta de enlace VPN de AWS), el peer BGP para la WAN primaria y secundaria puede ser diferente. En esos escenarios, puede optar por configurar un par BGP diferente para la WAN secundaria.

*Para implementaciones BGP con WAN secundarias, Prisma Access establece los túneles primario y secundario en un estado **UP (Activo)**, pero sigue el comportamiento normal de respaldo activo de BGP para el tráfico de red. Prisma Access establece el túnel primario como activo y envía y recibe tráfico a través de ese túnel solamente; si el túnel primario falla, Prisma Access detecta el fallo usando reglas BGP, establece el túnel secundario como activo y usa solo el túnel secundario para enviar y recibir tráfico.*

STEP 11 | (Opcional) Habilite la **Quality of Service (Calidad de servicio)** para la conexión de servicio y especifique un QoS Profile (Perfil de QoS) o añada un **New QoS Profile (Nuevo perfil de QoS)**.

Puede crear perfiles de QoS para configurar el tráfico de QoS para conexiones remotas de red y servicio, y aplicar esos perfiles al tráfico que marcó con las políticas de seguridad de PAN-OS, al tráfico que marcó con un dispositivo local o al tráfico marcado con PAN-OS y local. Consulte QoS para Redes remotas para obtener más detalles.



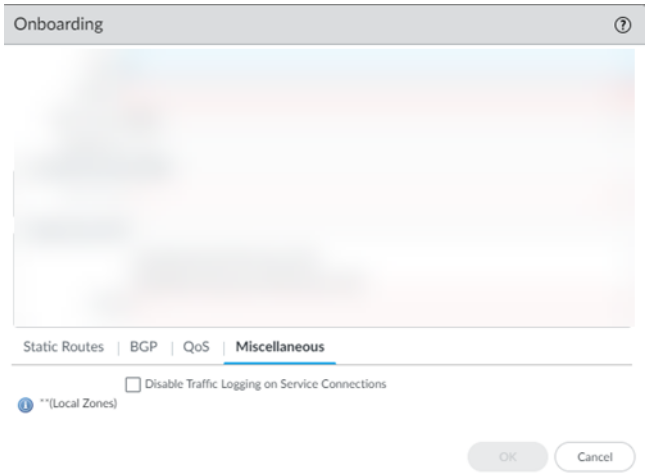
STEP 12 | (Opcional) Configure ajustes **Miscellaneous (varios)**.

1. (Opcional) **Disable Traffic Logging on Service Connections (Deshabilitar el registro de logs de tráfico en conexiones de servicio)** para deshabilitar el registro de logs en las conexiones de servicio para la implementación de Prisma Access.

   Si la mayoría de los flujos de tráfico registrados por las conexiones de servicio son asimétricos, es posible que sea necesario desactivar el registro de logs de conexiones de servicio para reducir el consumo de almacenamiento de registros de logs de Strata

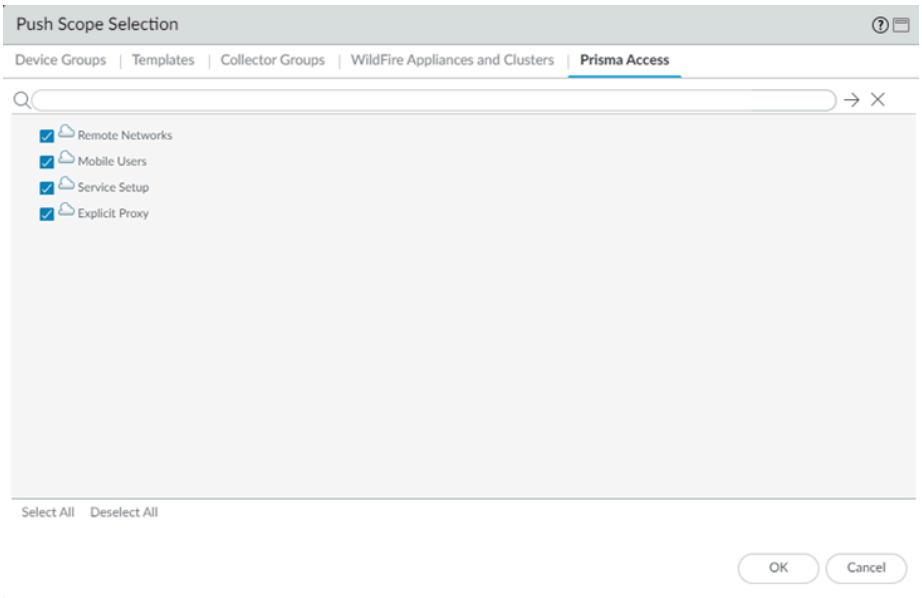
 ©2025 Palo Alto Networks, Inc.

Logging Service. Si su implementación no tiene flujos asimétricos a través de las conexiones de servicio, no necesita desactivar el registro de logs.



STEP 13 | Compruebe sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. En **Edit Selections (Editar selecciones)** y en la pestaña **Prisma Access**, asegúrese de que la **Service Configuration (Configuración del servicio)** está seleccionada en el **Push Scope (Ámbito de envío)** y, a continuación, haga clic en **OK (Aceptar)**.



3. Haga clic en **Commit and Push (Confirmar y enviar)**.

STEP 14 | Añada más conexiones de servicio repitiendo del Paso 2 al Paso 11.

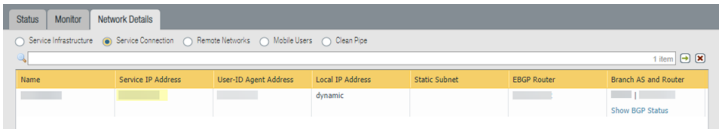
STEP 15 | Configure el túnel o túneles IPSec desde su dispositivo con capacidad IPSec en su red corporativa de nuevo a Prisma Access.

1. Para determinar la dirección IP del túnel dentro de Prisma Access, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de**

 ©2025 Palo Alto Networks, Inc.

la red), haga clic en el botón de radio **Service Connection (Conexión de servicio)** y anote la **Service IP Address (Dirección IP de servicio)** para el sitio.

La **Service IP Address (Dirección IP del servicio** es la dirección orientada al público a la que deberá conectarse cuando cree el túnel desde su dispositivo con capacidad IPSec de vuelta a la conexión de servicio.



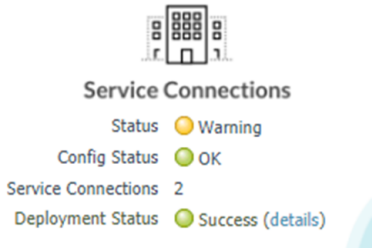
2. En su dispositivo con capacidad IPSec en la ubicación corporativa, configure un túnel IPSec que se conecte a la **Service IP Address (Dirección IP de servicio)**en Prisma Access y confirme el cambio en ese dispositivo para que se pueda establecer el túnel.

Verificar estado de la conexión del servicio

Para comprobar que la conexión de servicio se ha configurado correctamente, seleccione **Panorama > Cloud Services > Status > Status (Panorama > Servicios en la nube > Estado > Estado)** y compruebe que el estado está **OK (Aceptar)**.

Si creó una conexión de servicio con valores de marcador de posición para habilitar la comunicación entre usuarios móviles y usuarios en redes remotas, no es necesario verificar el estado de la conexión de servicio.

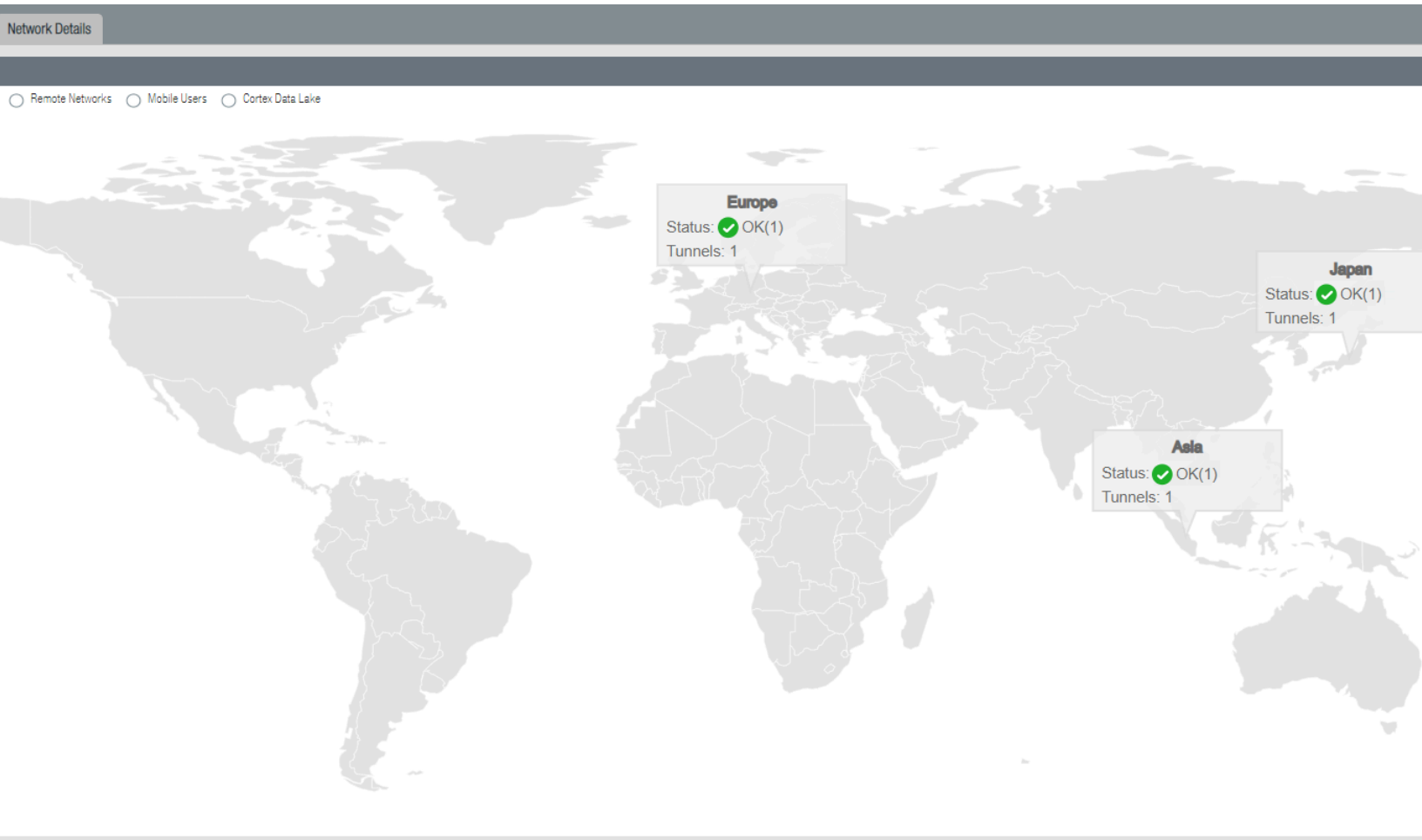
El área de **Deployment Status (Estado de implementación)** le permite ver el progreso de los trabajos de incorporación y implementación antes de que se completen, así como ver más información sobre el estado de los trabajos completados.



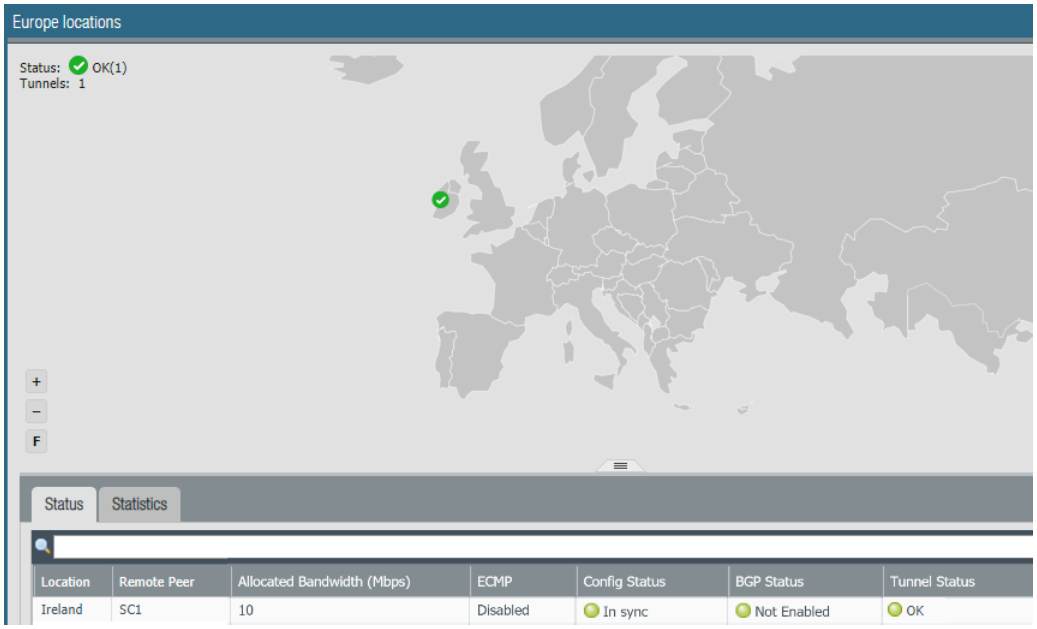
Si el estado no está **OK**, sitúe el cursor sobre el icono Estado para ver cualquier error.

Para ver una representación gráfica de la conexión de servicio junto con los detalles de estado, seleccione **Service Connection (Conexión de servicio)** en la pestaña **Monitor (Supervisar)**.

 ©2025 Palo Alto Networks, Inc.



Seleccione una región para obtener más detalles sobre esa región.



Haga clic en las pestañas debajo del mapa para ver información adicional sobre las conexiones de servicio.

 ©2025 Palo Alto Networks, Inc.

Pestaña **Status (Estado)**:

- **Location (Ubicación)**: la ubicación donde se implementa su conexión de servicio.
- **Remote Peer (Peer remoto)**: la ubicación corporativa a la que esta infraestructura de servicio está configurando un túnel IPSec.
- **Allocated Bandwidth (Ancho de banda asignado)**: el número de conexiones de servicio que ha asignado se multiplica por 300 Mbps.

  Este número no refleja el ancho de banda de conexión de servicio disponible.

  Si bien cada conexión de servicio proporciona aproximadamente 1 Gbps de rendimiento, el rendimiento real depende de varios factores, incluidos:

  - *Mezcla de tráfico (por ejemplo, tamaño de trama)*
  - *Latencia y pérdida de paquetes entre la conexión de servicio y la ubicación de la sede o el centro de datos*
  - *Límites de rendimiento del proveedor de servicios*
  - *Límites de rendimiento del dispositivo de terminación de cliente*
  - *Otro tráfico del centro de datos del cliente*
- **ECMP**: si tiene configurada la ruta múltiple de igual coste (ECMP) para esta conexión de servicio. Dado que ECMP no se utiliza para conexiones de servicio, este estado está **Disabled (Deshabilitado)**.
- **Config Status (Estado de configuración)**: el estado de su último envío de configuración al servicio. Si la configuración local y la configuración en la nube coinciden, el Estado de configuración es **In sync (Sincronizado)**. Si ha realizado un cambio localmente y aún no ha enviado la configuración a la nube, es posible que se muestre el estado **Out of sync (Fuera de sincronización)**. Pase el cursor sobre el indicador de estado para obtener información más detallada. Después de confirmar y enviar la configuración a Prisma Access, el estado de configuración cambia a **In sync (Sincronizado)**.
- **BGP Status (Estado de BGP)**: muestra información sobre el estado de BGP entre el cortafuegos o enrutador en su ubicación corporativa/sede y Prisma Access donde se establece la conexión de servicio. Aunque es posible que vea pasar temporalmente el estado a través de los diversos estados de BGP [**idle (inactivo)**, **active (activo)**, **open send (abrir envío)**, **open pend (abrir pendiente)**, **open confirm (abrir confirmación)**], lo más común es que el estado de BGP muestre:
  - **Connect (Conectar)**: el enrutador de su centro de datos/sede está tratando de establecer la relación de peers BGP con Prisma Access.
  - **Established (Establecido)**: se ha establecido la relación entre pares BGP.

  Este campo también mostrará si la conexión BGP está en un estado de error:

  - **Advertencia**: no se ha actualizado el estado del BGP en más de ocho minutos. Esto puede indicar un corte en el cortafuegos.
  - **Error**: se desconoce el estado de BGP.

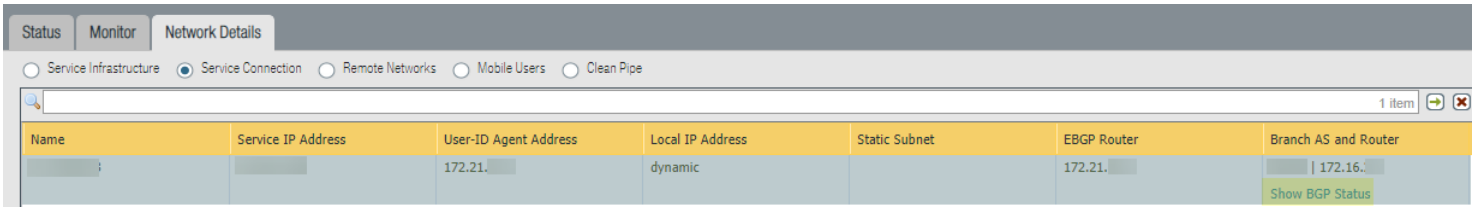
 ©2025 Palo Alto Networks, Inc.

- **Tunnel Status (Estado del túnel)**: estado operativo de la conexión entre Prisma Access y su conexión de servicio.

Pestaña **Statistics (Estadísticas)**

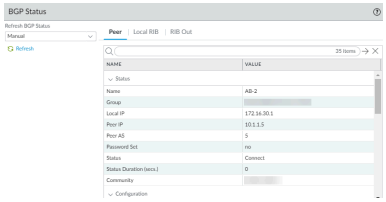
- **Location (Ubicación)**: la ubicación donde se implementa su conexión de servicio.
- **Remote Peer (Peer remoto)**: la ubicación corporativa a la que la conexión de servicio está configurando un túnel IPSec.
- **Ingress Bandwidth (Mbps) [Ancho de banda de entrada (Mbps)]**: el ancho de banda desde la ubicación del centro de datos hasta Prisma Access.
- **Ingress Peak Bandwidth (Mbps) [Ancho de banda máximo de entrada (Mbps)]**: la carga máxima desde la ubicación de la sede/centro de datos hacia el servicio en la nube.
- **Egress Bandwidth (Mbps) [Ancho de banda de salida (Mbps)]**: ancho de banda desde Prisma Access hasta la ubicación del centro de datos.
- **Egress Peak Bandwidth (Mbps) (Ancho de banda de salida (Mbps) pico**: la carga máxima desde Prisma Access hasta la ubicación de la sede o centro de datos.
- **QoS**: seleccione este botón para mostrar un gráfico que muestra estadísticas de QoS en tiempo real e históricas, incluyendo el número de paquetes perdidos por clase. Este gráfico se muestra solo para conexiones de servicio o conexiones de red remotas que tengan habilitada la QoS.

Si has configurado BGP, puede comprobar su estado seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **Show BGP Status (Mostrar estado de BGP)**.



Se muestra el cuadro de diálogo Estado de BGP. Esta tabla le proporciona la siguiente información:

- **Peer**: información de enrutamiento para el peer de BGP, incluido el estado, el número total de rutas, la configuración y las estadísticas y contadores de tiempo de ejecución. El número total de rutas que se muestran en el área **bgpAfiIpv4-unicast Counters (Contadores de bgpAfiIpv4-unicast**, en los campos **Incoming Total (Total entrante)** y **Outgoing Total (Total saliente)**.

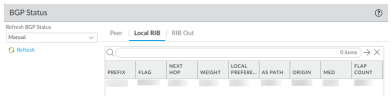


- **RIB local**: rutas BGP que Prisma Access utiliza localmente. Prisma Access selecciona esta información de la tabla BGP RIB-In, que almacena la información enviada por los dispositivos

 ©2025 Palo Alto Networks, Inc.

de red vecinos, aplica políticas de importación y decisiones de enrutamiento locales de BGP y almacena la información de RIB local en la base de información de enrutamiento (RIB).

Tenga en cuenta que solo se muestran las primeras 256 entradas. Para ver entradas adicionales, introduzca una subred o dirección IP en el campo de Filtro y haga clic en Aplicar filtro para ver un subconjunto de las entradas de enrutamiento hasta un máximo de 256.



- **Salida de RIB**: información de enrutamiento que Prisma Access anuncia a sus peers a través de mensajes de actualización BGP.

 ©2025 Palo Alto Networks, Inc.

Utilice una conexión de servicio para permitir el acceso entre usuarios móviles y redes remotas

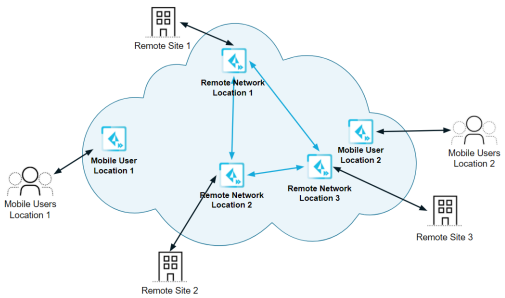
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access que incluye Interconexión de red para el acceso de sitio a sitio y de usuario a sitio

Para configurar una conexión de servicio para conectar usuarios móviles y redes remotas, debe **Add (Añadir)** una conexión de servicio utilizando los siguientes valores:

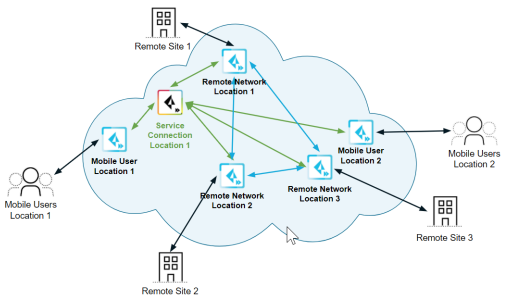
- Especifique un **Region (Región)** que está cerca de sus usuarios móviles.
- **Add (Añadir)** un **IPSec Tunnel (Túnel IPSec)** y **IKE Gateway (Puerta de enlace IKE)**, mediante valores de marcador de posición.
- Añadir marcador de posición de **Corporate Subnets (Subredes corporativas)**.

  Dado que Prisma Access no enruta ningún tráfico a través de este túnel, cualquier valor que no entre en conflicto o se superponga con otras subredes configuradas es válido.

En el ejemplo siguiente se muestra un implementación de Prisma Access con usuarios móviles en diferentes áreas geográficas y redes remotas. Las conexiones de red remotas están conectadas en una red de malla en la infraestructura de Prisma Access, pero los usuarios móviles no pueden conectarse a las redes remotas. Además, los usuarios móviles en diferentes áreas geográficas no pueden conectarse entre sí sin una conexión de servicio.

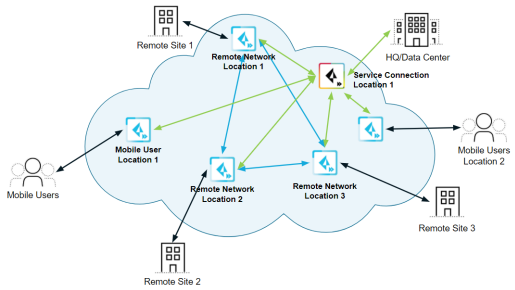


Después de añadir una conexión de servicio, la conexión de servicio conecta a los usuarios móviles y las redes remotas en una red radial.

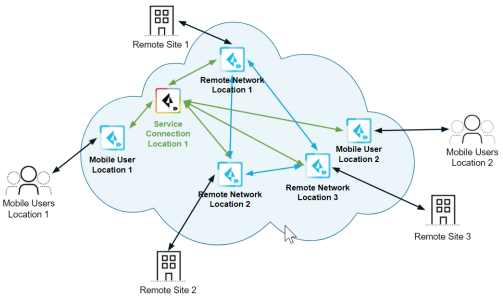


 ©2025 Palo Alto Networks, Inc.

Otro caso en el que una conexión de servicio de este tipo es útil es cuando la conexión de servicio está lejos de los usuarios móviles. En la siguiente figura se muestra un ejemplo de esta implementación de red.



Añadir una segunda conexión de servicio que esté más cerca de los usuarios móviles crea una red más eficiente entre los usuarios móviles y las redes remotas.



 ©2025 Palo Alto Networks, Inc.

Consideraciones del enrutamiento dinámico para conexiones de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Cómo Funciona : Enrutamiento para el tráfico de conexión de servicio

Prisma Access utiliza BGP para el enrutamiento dinámico y utiliza la selección de rutas de BGP para instalar rutas en la tabla de rutas. Cuando Prisma Access enruta el tráfico a su sede o centro de datos mediante conexiones de servicio, utiliza métodos de enrutamiento que dirigen ese tráfico de manera efectiva. Prisma Access utiliza un modelo de enrutamiento predeterminado que se diseñó para adaptarse a la mayoría de las implementaciones de red; sin embargo, no todas las redes de la organización son iguales. Para adaptarse a una gama más amplia de implementaciones, Prisma Access le permite elegir otro modo para el enrutamiento de la conexión de servicio. Las siguientes secciones describen los métodos de enrutamiento BGP que Prisma Access utiliza, junto con los factores que debe considerar en la red de su organización antes de cambiar el método de enrutamiento de conexión de servicio predeterminado de Prisma Access.

Cambiar el método de enrutamiento de la conexión de servicio de Prisma Access requiere una comprensión profunda de la topología y los dispositivos de enrutamiento de su organización, junto con una comprensión de cómo funciona el enrutamiento de Prisma Access, como se describe en esta sección. Recomendamos que lea esta sección cuidadosamente antes de cambiar el método de enrutamiento de la configuración predeterminada.

Prisma Access admite el enrutamiento estático y el enrutamiento dinámico mediante BGP para servicio y conexiones de red remotas; en esta sección se supone que utiliza el enrutamiento BGP para sus implementaciones de Prisma Access. Cuando seleccionas el enrutamiento BGP, la red de su organización aprende información BGP de Prisma Access.

Modos de enrutamiento para conexiones de servicio

Puede elegir entre los siguientes modos de enrutamiento con Prisma Access:

- Enrutamiento predeterminado: este es el modelo de enrutamiento actual que Prisma Access utiliza.

  Utilice este modo de enrutamiento si desea que Prisma Access utilice los mecanismos de selección de la mejor ruta de BGP sin ajustar ninguno de los atributos de BGP. En este modo, Prisma Access respetará cualquier atributo anunciado por el equipo de las instalaciones del cliente (CPE).

 ©2025 Palo Alto Networks, Inc.

- Enrutamiento Hot Potato: Prisma Access entrega el tráfico lo más rápido posible a la red de su organización.

  Utilice este método de enrutamiento si desea que la red de su organización realice la mayoría de las decisiones de enrutamiento.

Enrutamiento predeterminado de Prisma Access

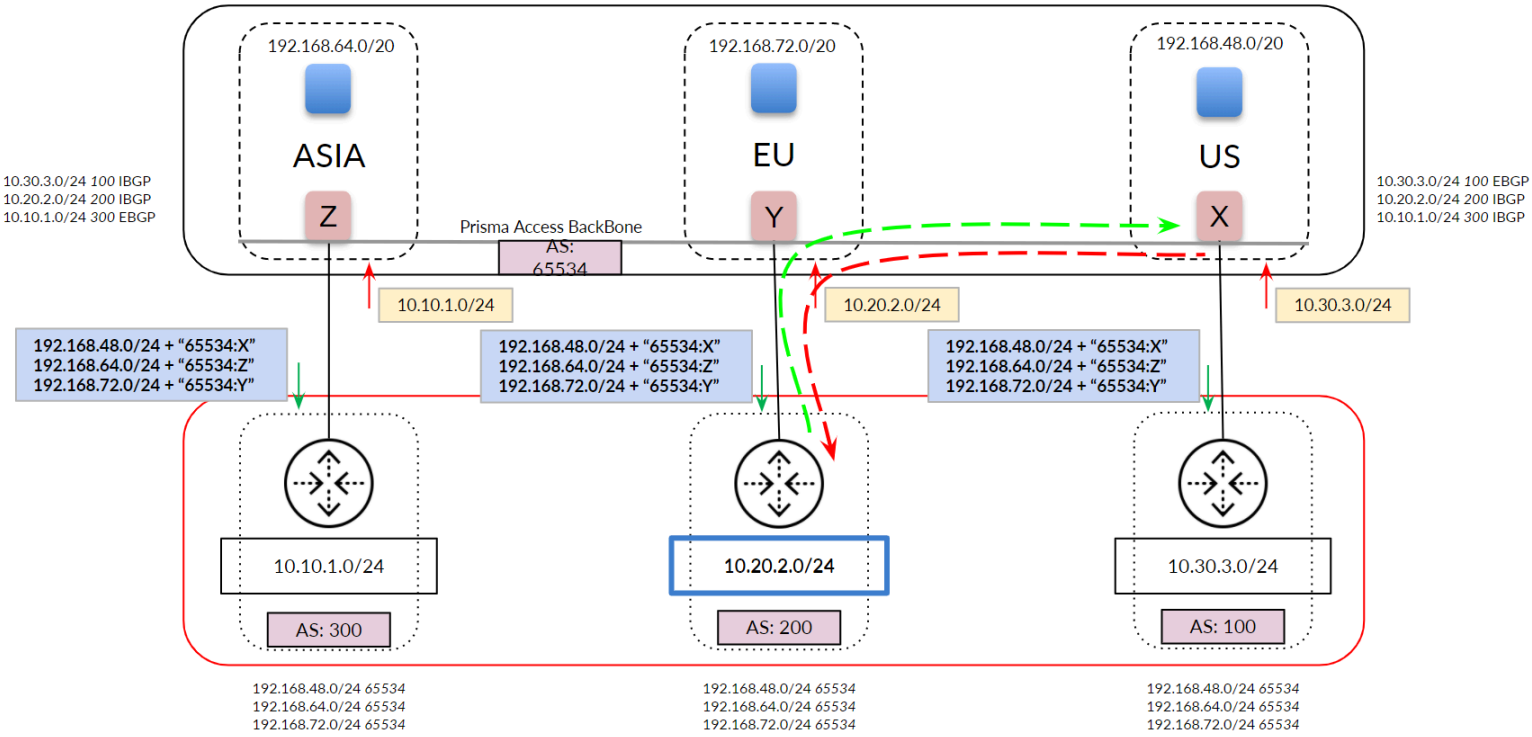
En la siguiente imagen se muestra un ejemplo del enrutamiento del tráfico de conexión del servicio de Prisma Access en el modo de enrutamiento predeterminado. La red de la organización tiene tres redes separadas en tres centros de datos y no tiene una red troncal que conecte las redes. En el modo de enrutamiento predeterminado, los grupos de usuarios móviles se anuncian por igual en las tres redes, como se muestra en la parte inferior de la imagen.

Tenga en cuenta que, cuando Prisma Access anuncia rutas de usuarios móviles, se hace antes de anunciarlas; así, se anuncian las subredes de usuarios móviles /20 en bloques de /24 a medida que los prefijos son consumidos por las puertas de enlace.

Tome nota de cómo Prisma Access utiliza anuncios de ruta BGP:

- Prisma Access no ajusta los atributos BGP predeterminados para las rutas anunciadas por el usuario móvil (Prisma Access añade su número de AS a los anuncios de ruta).
- Prisma Access anuncia rutas de usuarios móviles y añade valores de comunidad BGP en las rutas que declara a través de la conexión de servicio. La siguiente imagen muestra una implementación de usuario móvil con tres conexiones de servicio y tres bloques de direcciones IP diferentes especificados para la: `192.168.64.0/20` para la región de **Asia, Australia y Japón**, `192.168.72.0/20` para la región de **África, Europa y Oriente Medio** y `192.168.48.0/20` para la región de **América del Norte y América del Sur**. Prisma Access divide estas rutas en un bloque de /24 y las anuncia con un Número de AS de Prisma Access de **65534**, sino que también añade los valores de la comunidad BGP a los anuncios (**Z** para Asia, **Y** para la UE, y **X** para EE. UU.). Esas rutas se muestran en el centro de la imagen. De esta manera, puede diferenciar las conexiones de servicio en su red, aunque Prisma Access les asigna el mismo número de AS.

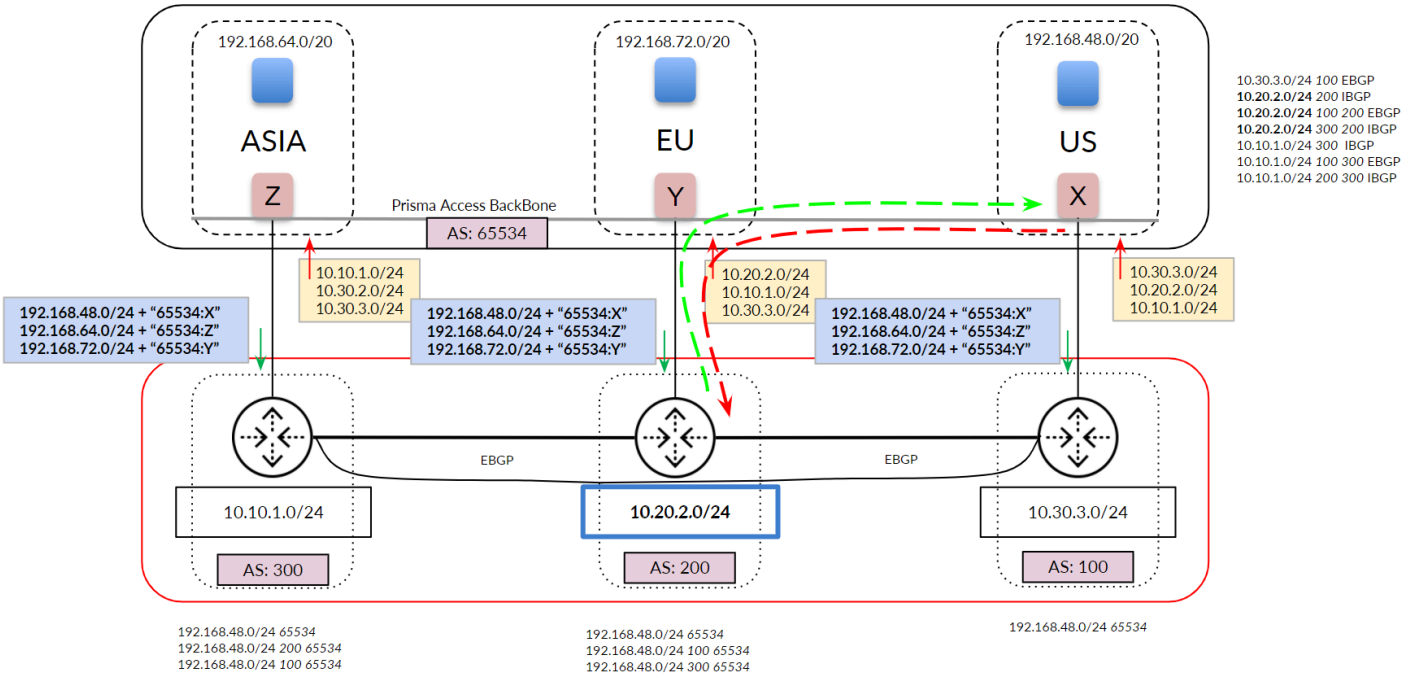
 ©2025 Palo Alto Networks, Inc.



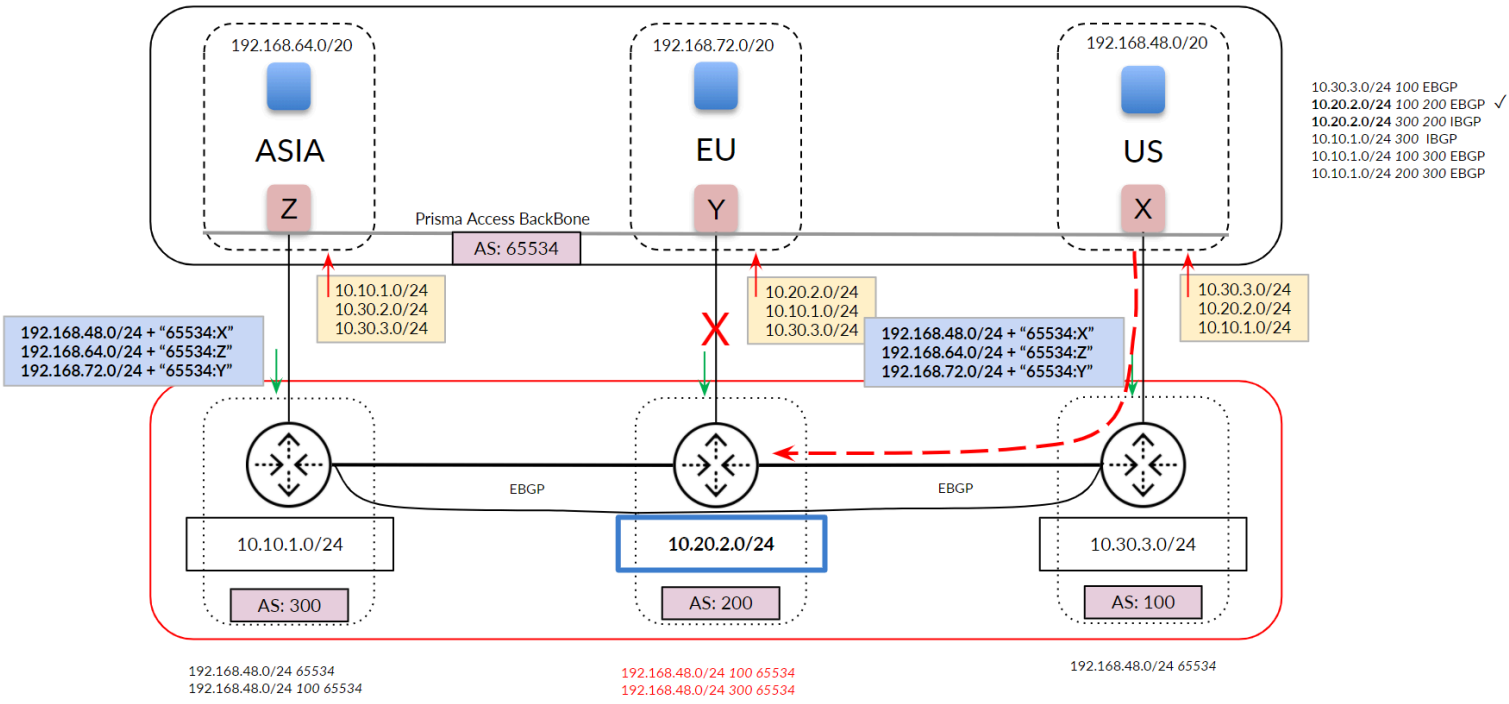
En la siguiente imagen se muestra una red más común con una red troncal eBGP de malla completa. En la imagen se muestran las rutas que Prisma Access ha aprendido de la red de su organización en la parte superior derecha. Tenga en cuenta las rutas adicionales que Prisma Access ha aprendido a través de la red troncal de Prisma Access (iBGP) y la red troncal de su organización (eBGP).

Para el tráfico entre usuarios móviles en la región de **North America & South America (América del Norte y América del Sur)** (EE. UU. en el diagrama) y el centro de datos de la región **Africa, Europe & Middle East (África, Europa y Oriente Medio)** (UE en el diagrama), Prisma Access selecciona la ruta a través de la conexión de servicio de la UE porque prefiere rutas con un AS-PATH más corto.

 ©2025 Palo Alto Networks, Inc.



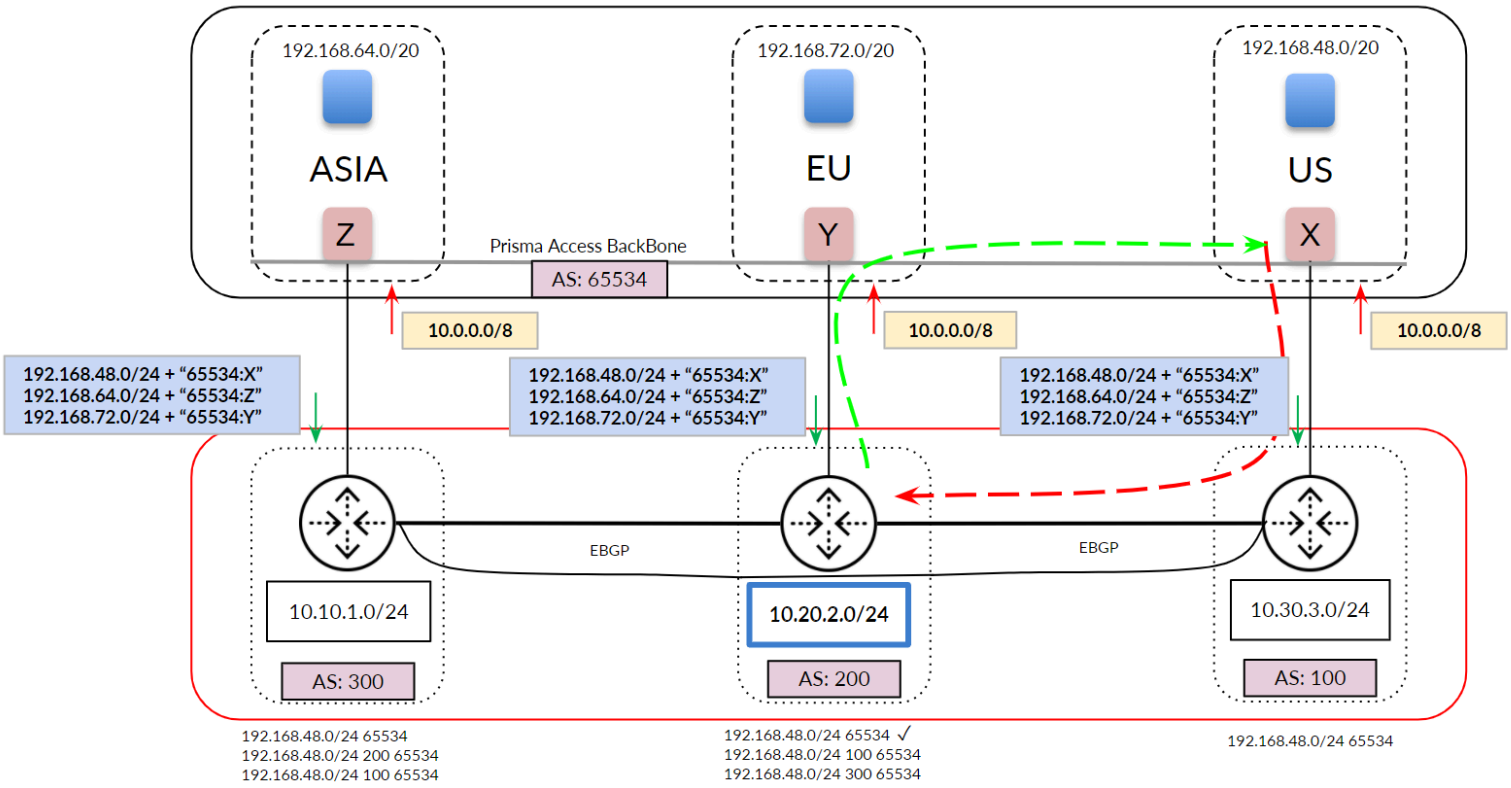
En implementaciones con una red troncal eBGP de malla completa, puede surgir asimetría cuando Prisma Access no puede llegar a un centro de datos en particular debido a un fallo de ISP/CPE en el centro de datos del cliente. La siguiente imagen muestra lo que podría suceder cuando el enlace a la conexión de servicio de la UE se cae. La red detecta el error de enlace y crea una nueva tabla de rutas para AS 200. El tráfico desde la conexión de servicio en EE. UU. hacia AS 200 utiliza la ruta a través de AS 100 porque la ruta eBGP para su red troncal entre AS 200 y AS 100 tiene prioridad sobre la ruta iBGP entre las conexiones de servicio en la UE y EE. UU. Sin embargo, el tráfico de retorno no está garantizado a través de la misma ruta porque el CPE local puede elegir cualquiera de las rutas (que se muestra en rojo) para devolver el tráfico.



 ©2025 Palo Alto Networks, Inc.

Los ejemplos anteriores muestran una red cuyas rutas no se han añadido (es decir, no ha realizado el resumen de rutas antes de enviar los anuncios de ruta BGP a Prisma Access). En el ejemplo siguiente se muestra una red que resume sus rutas a 10.0.0.0/8 antes de enviarlas a Prisma Access. Si selecciona el enrutamiento predeterminado, esta configuración puede provocar problemas de enrutamiento asimétrico, ya que Prisma Access no se puede determinar la ruta de retorno correcta a partir de las rutas resumidas.

Si su implementación de Prisma Access tiene redes remotas, Palo Alto Networks no recomienda el uso de resumen de rutas en conexiones de servicio. El resumen de rutas en las conexiones de servicio es solo para implementaciones de usuarios móviles.



Si utiliza la agregación de rutas para usuarios móviles, le recomendamos encarecidamente que habilite el enrutamiento de hot potato en lugar del enrutamiento predeterminado, donde Prisma Access entrega el tráfico a la red de su organización lo más rápido posible. Además, recomendamos que seleccione una **Backup SC (Copia de seguridad de SC)** como se describe en la siguiente sección para cada conexión de servicio para tener un comportamiento de enrutamiento determinista.

Enrutamiento Hot Potato

Cuando selecciona **Hot Potato Routing (Enrutamiento hot potato)**, Prisma Access egresa el tráfico destinado a conexiones de servicio/centros de datos de su red interna lo más rápido posible.

Con el enrutamiento hot potato, Prisma Access antepone la ruta AS (AS-PATH) a los anuncios de prefijo BGP enviados desde las puertas de enlace. Esta anteposición se realiza cuando los prefijos se anuncian fuera de la conexión de servicio al CPE local de su organización. Prisma Access antepone los AS-PATH para que su CPE dé la preferencia correcta a los túneles primario

 ©2025 Palo Alto Networks, Inc.

y secundario, de modo que si el túnel primario deja de funcionar, su CPE elige el túnel secundario como respaldo.

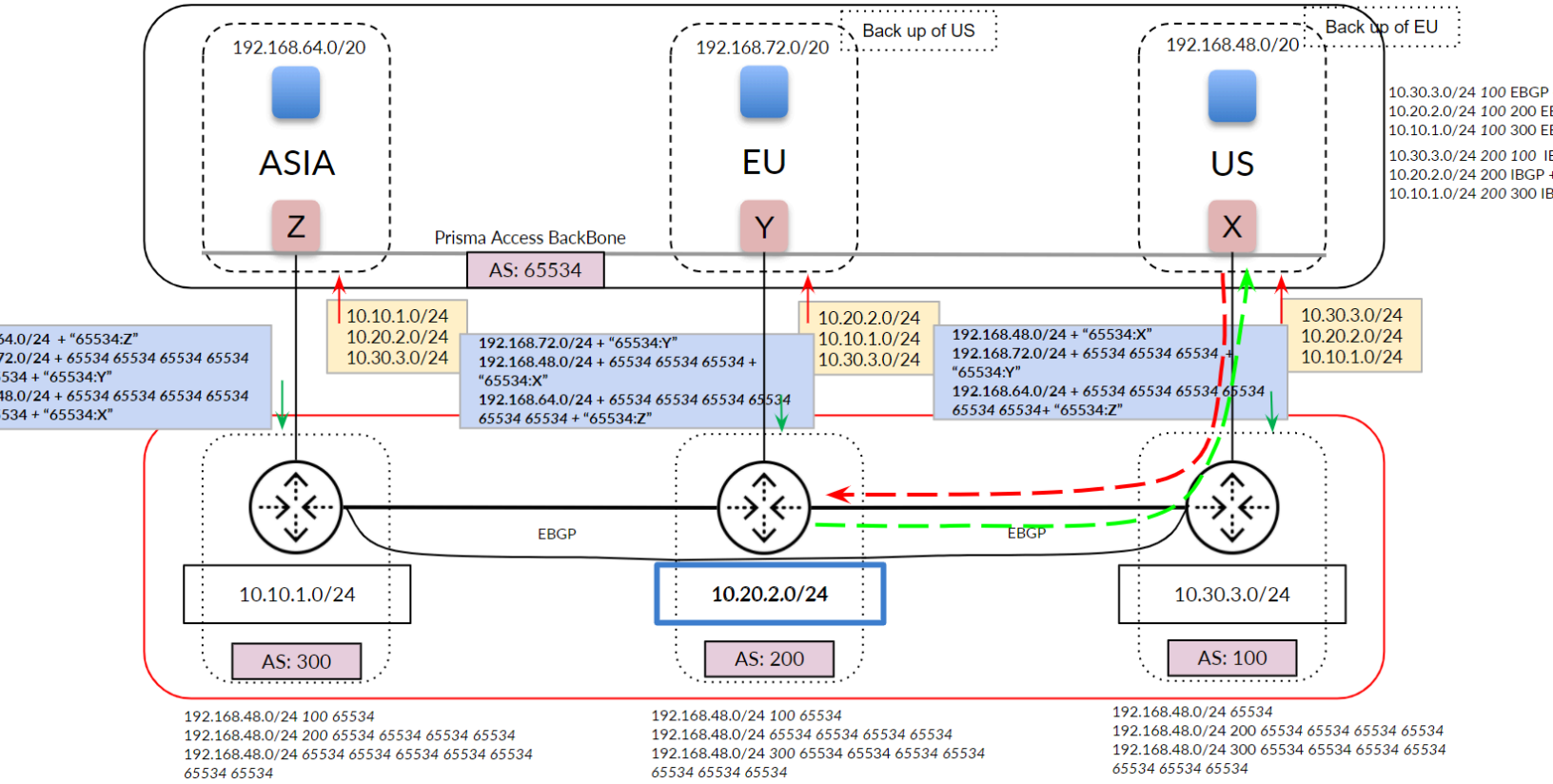
Si especificó una dirección IP diferente para el par BGP secundario (de respaldo), Prisma Access añade más prefijos según el tipo de túnel, como se muestra en la siguiente tabla.

Tipo de prefijo	Tipo de túnel de conexión de servicio	Número de anteposicion de As-Path	Número total de AS-PATH observados en el CPE
Prefijos de puerta de enlace de la conexión del servicio principal	Túnel primario o secundario con la misma dirección IP del peer de BGP	0	1
Prefijos de puerta de enlace de la conexión del servicio de copia de seguridad	Túnel primario o secundario con la misma dirección IP del peer de BGP	3	4
Prefijos de puerta de enlace de todas las demás conexiones de servicio	Túnel primario o secundario con la misma dirección IP del peer de BGP	6	7
Prefijos de puerta de enlace de la conexión del servicio principal	Túnel secundario con una dirección IP de peer BGP diferente	1	2
Prefijos de puerta de enlace de la conexión del servicio de copia de seguridad	Túnel secundario con una dirección IP de peer BGP diferente	4	5
Prefijos de puerta de enlace de todas las demás conexiones de servicio	Túnel secundario con una dirección IP de peer BGP diferente	7	8

Especifique una **Backup Service Connection (Conexión de servicio de copia de seguridad)** para que Prisma Access utilice esa conexión de servicio como respaldo cuando falle un enlace de conexión de servicio.

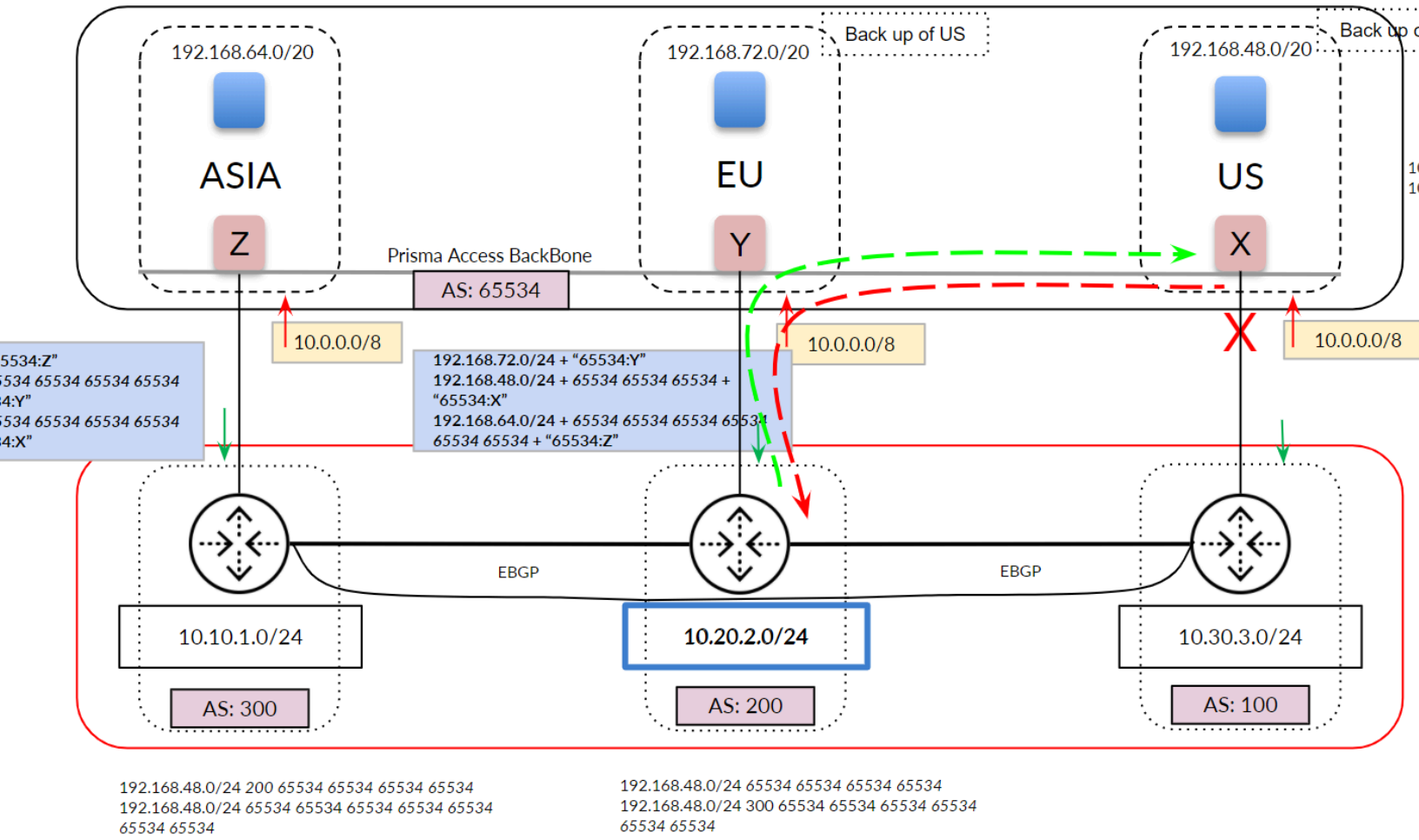
La siguiente figura muestra una configuración de enrutamiento hot potato para el tráfico entre la conexión de servicio de EE. UU. y AS 200, con la conexión de servicio de la UE configurada como **Backup Service Connection (Conexión de servicio de copia de seguridad)** de la conexión de EE. UU. Usando el enrutamiento hot potato, Prisma Access envía el tráfico desde su ruta de salida más cercana a través de la conexión de servicio de EE. UU. El tráfico de retorno toma la misma ruta a través de AS100 porque esta ruta tiene un AS-PATH más corto hacia el grupo de usuarios móviles en la ubicación de EE. UU. Prisma Access antepone AS-PATH a sus anuncios de prefijo dependiendo de si el túnel es un túnel principal, un túnel de respaldo o no se utiliza ni como túnel principal ni como túnel de respaldo.

 ©2025 Palo Alto Networks, Inc.



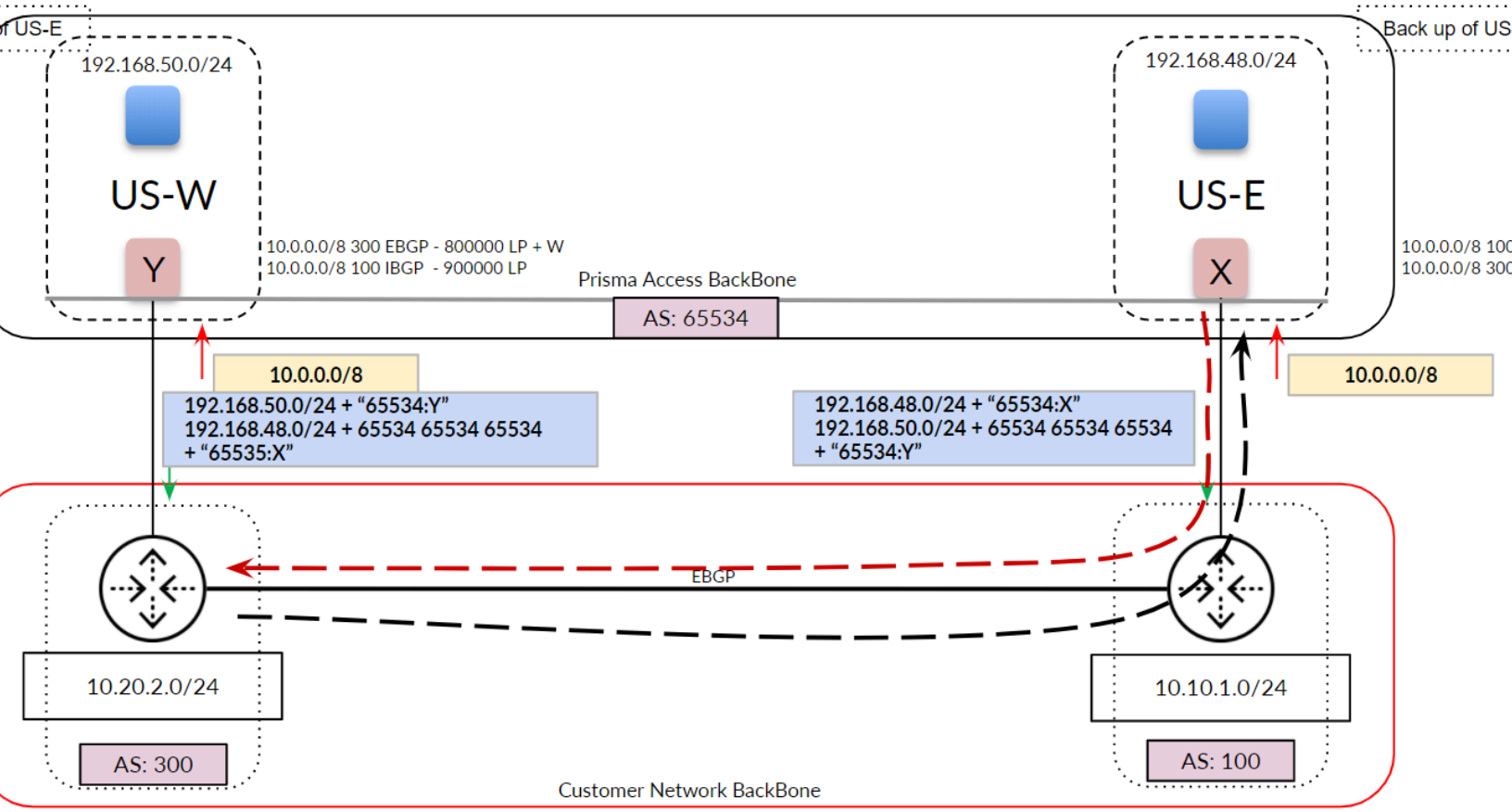
Debido a que ha configurado una conexión de servicio de respaldo, si el enlace a la conexión de servicio de EE. UU. deja de funcionar, el enrutamiento hot potato envía el tráfico utilizando su ruta más corta a través de la conexión de servicio de la UE. Este escenario de enrutamiento también se aplica a las redes que utilizan agregación de rutas.

 ©2025 Palo Alto Networks, Inc.



También puede utilizar conexiones de servicio de respaldo para múltiples conexiones de servicio en una sola región. La siguiente imagen muestra una implementación de Prisma Access con dos conexiones de servicio en la región de América del Norte. En este caso, se especifica una **Backup Service Connection (Conexión de servicio de copia de seguridad)** de US-E para la conexión de servicio US-W, y viceversa, para garantizar un enrutamiento simétrico.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Prisma Access ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

El Conector de acceso a la red de confianza cero (ZTNA) le permite conectar Prisma Access a las aplicaciones privadas de su organización de manera sencilla y segura. ZTNA Connector proporciona a los usuarios móviles y a los usuarios en sucursales acceso a sus aplicaciones privadas mediante un túnel seguro automatizado. Debido a que ZTNA Connector configura los túneles automáticamente,no tiene que configurar manualmente los túneles IPSec y el enrutamiento al centro de datos o a las ubicaciones de la sede, las ubicaciones de la nube pública y las redes de socios donde se encuentran sus aplicaciones privadas.

Las máquinas virtuales de ZTNA Connector que implementa se conectan automáticamente a la ubicación más cercana de Prisma Access garantizando así la mejor latencia posible, además de ampliar el acceso al ancho de banda hasta 2 Gbps por Conector y 8 Gbps por Grupo de conectores.

Prisma Access niega todo acceso de forma predeterminada, y un administrador debe permitir explícitamente el acceso a un recurso mediante una regla de política, basada en nuestras construcciones patentadas de User-ID, App-ID y Device-ID, lo que le ayuda a reducir la superficie de ataque y los riesgos de seguridad. Una vez que se permite una conexión, verificamos continuamente la confianza de esa conexión, inspeccionamos continuamente si hay amenazas

de seguridad e inspeccionamos continuamente si hay fugas de datos. Además, las direcciones IP privadas de sus aplicaciones no quedan expuestas cuando utiliza el Prisma Access ZTNA Connector.

 ©2025 Palo Alto Networks, Inc.

Componentes de ZTNA Connector

- **Conectores**: los conectores son las máquinas virtuales que construyen túneles para Prisma Access. ZTNA Connector automatiza la gestión del túnel sin que usted tenga que especificar configuraciones IPSec e IKE. Usted incorpora conectores en máquinas virtuales, que incorpora en un servicio en la nube (Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, o en un servidor virtual (VMware ESXi), o en una máquina virtual basada en kernel (KVM). Palo Alto Networks recomienda que implemente la máquina virtual en la misma subred que la aplicación incorporada a Prisma Access. También puede proporcionar una subred diferente, siempre que haya una ruta a las aplicaciones desde el Conector.

  Después de implementar la máquina virtual del conector, Prisma Access gestiona la máquina virtual, incluso proporcionándole opciones para actualizar la versión de la máquina virtual (VM). Después de instalar la máquina virtual de ZTNA Connector, esta descubre la ubicación más cercana de Prisma Access e inicia un túnel IPSec seguro a Prisma Access.
- **Grupos de conectores**: un grupo de conectores es una agrupación lógica de conectores y aplicaciones. Al añadir varios conectores en un grupo de conectores, proporciona redundancia de túnel y mayor ancho de banda para las aplicaciones dentro del grupo. Cada grupo de conectores admite hasta cuatro conectores.

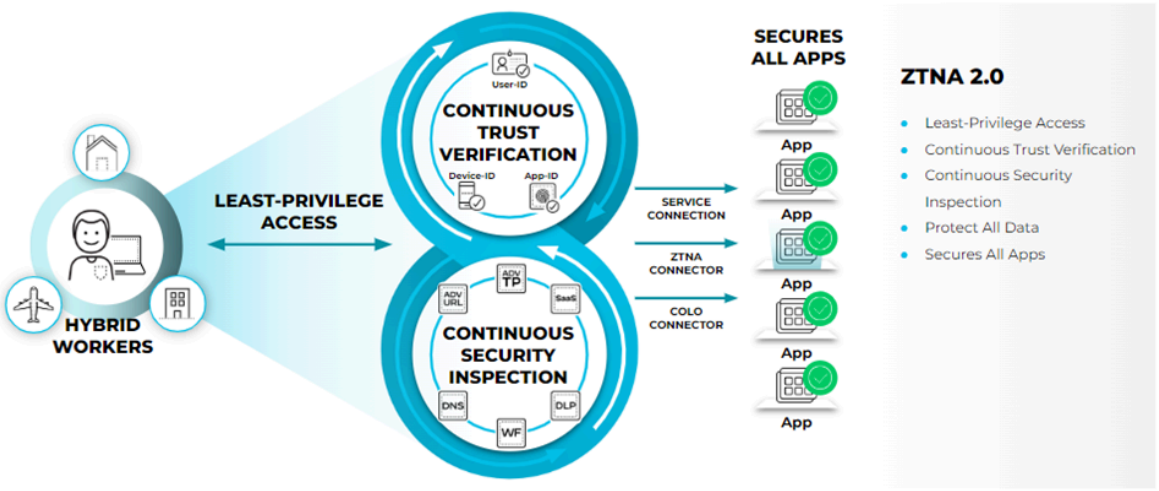
  Si desea proporcionar acceso a aplicaciones específicas mediante diferentes conectores, coloque los conectores en grupos separados.
- **Objetivos**: las aplicaciones privadas que ZTNA Connector incorpora a Prisma Access. Puede definir aplicaciones específicas a las que desea proporcionar acceso mediante FQDN [**FQDN Targets (Objetivos FQDN)**], comodines [**Wildcard Targets (Objetivos comodín)**] o direcciones IP o subredes donde se encuentran las aplicaciones. O bien, puede hacer que ZTNA Connector descubra automáticamente las aplicaciones extrayéndolas de un IdP conectado a CIE.

 ©2025 Palo Alto Networks, Inc.

Casos de uso de ZTNA Connector

Utilice ZTNA Connector en estos escenarios:

- **Conectarse a aplicaciones privadas**: utilice ZTNA Connector para todo el tráfico iniciado por el cliente que se conecta a aplicaciones privadas.



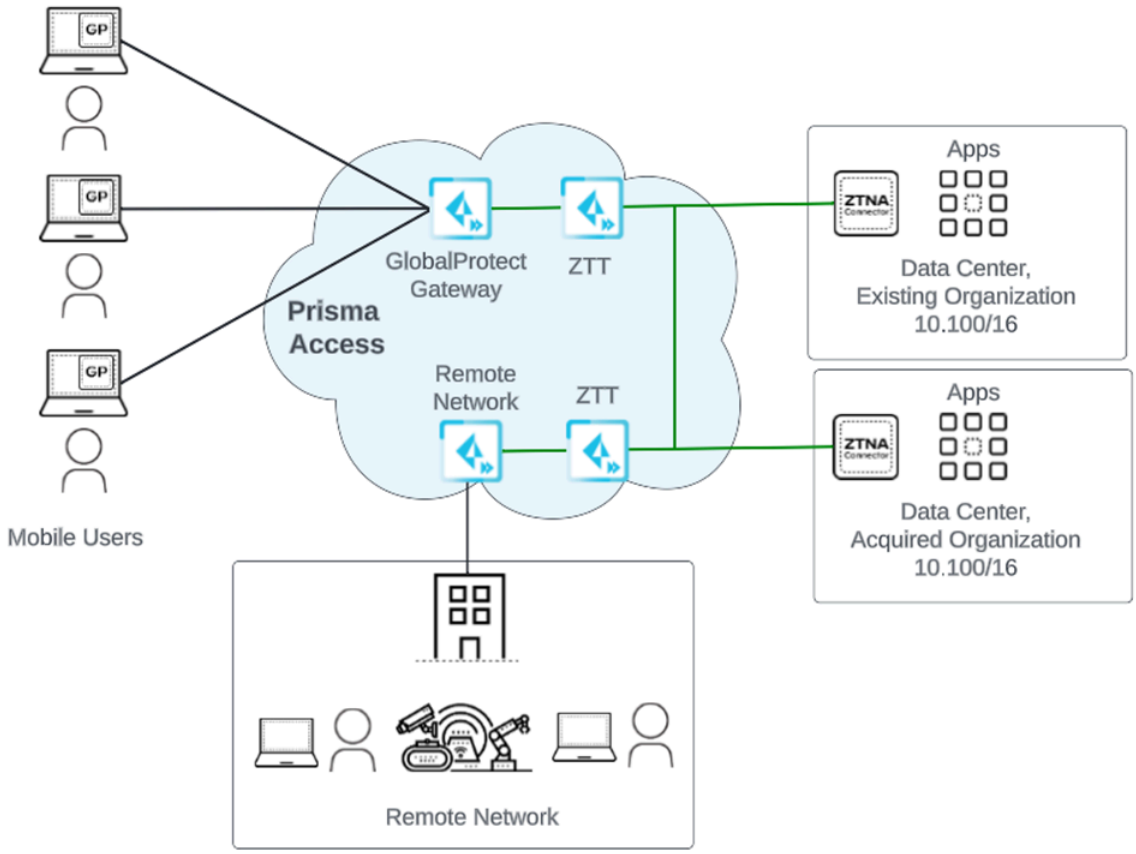
- **Redes privadas superpuestas**: si es administrador de red en una empresa grande que ha adquirido o se ha fusionado con otra organización, dos redes podrían usar rangos de direcciones que se superponen (por ejemplo, el espacio de direcciones de red privada RFC 1918). Proporcionar acceso a aplicaciones alojadas en redes superpuestas a sus usuarios, la configuración de enrutamiento y NAT puede volverse tediosa. ZTNA Connector simplifica el acceso a las aplicaciones en redes superpuestas al permitirle conectarse a aplicaciones usando FQDN, comodines FQDN y subredes IP, sin tener que configurar el enrutamiento IP.

  ZTNA Connector proporciona a sus usuarios acceso seguro a las aplicaciones privadas mediante ZTNA Connector Tunnel Terminators (ZTT).

  Cuando se activa un ZTNA Connector en una región de cómputo, los nodos ZTT se incorporan automáticamente. ZTNA Connector forma automáticamente túneles IPSec con ZTT. Los nodos ZTT de una región permanecen activos durante 24 horas después de que se eliminan todos los conectores de esa región. Si se implementa un nuevo conector dentro de las 24 horas

 ©2025 Palo Alto Networks, Inc.

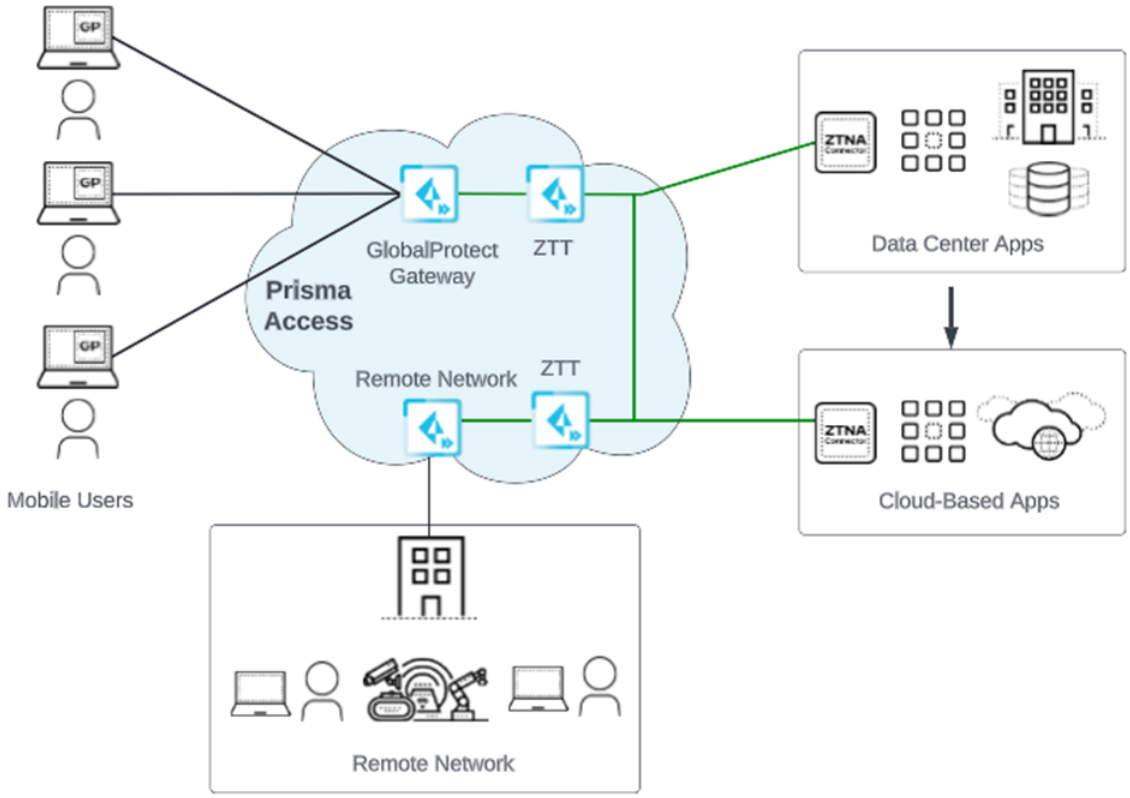
posteriores a que se eliminen todos los conectores en la misma región, se reutiliza el ZTT existente. Si se activa un nuevo ZTNA Connector después de 24 horas, se crea un nuevo ZTT.



- **Migración del centro de datos a la nube**: si su organización está migrando sus aplicaciones locales a la nube (ya sea migrando sus aplicaciones locales existentes mediante "lift and shift" o desarrollando aplicaciones nativas de la nube), puede alojar aplicaciones en VPC en la nube en AWS, GCP, Azure u otros proveedores de la nube. Si tiene cientos o miles de VPC, ZTNA

 ©2025 Palo Alto Networks, Inc.

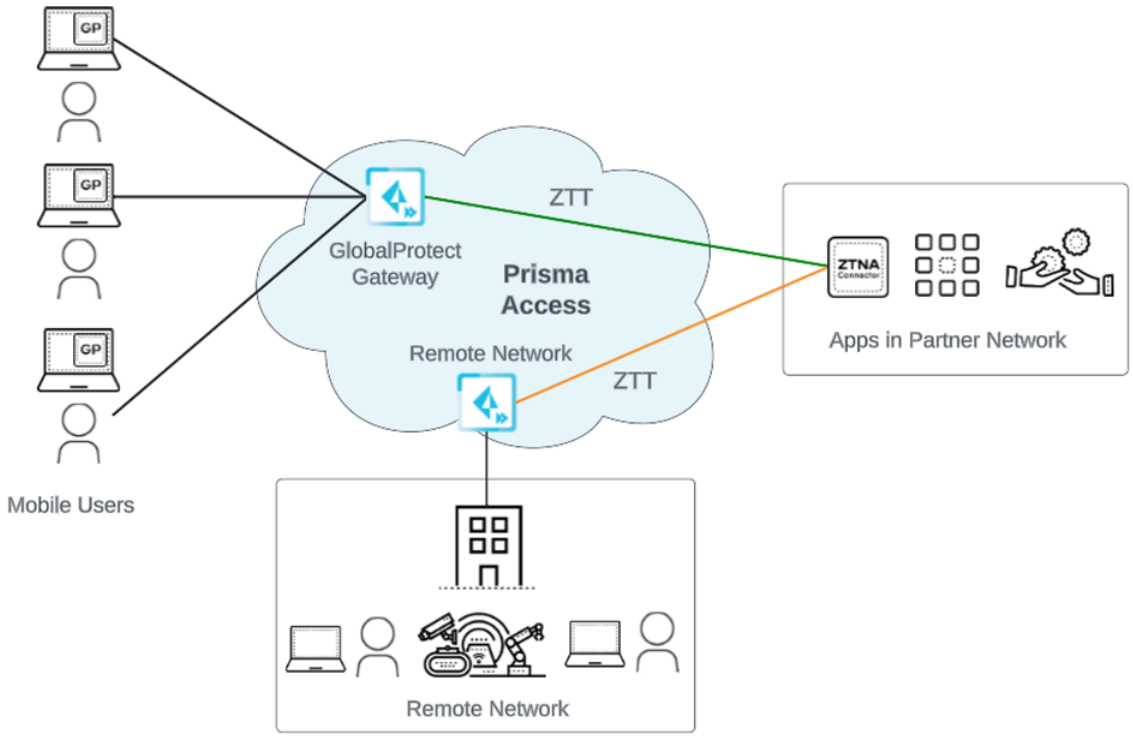
Connector puede acelerar el proceso de proporcionar acceso a aplicaciones distribuidas en la nube.



- **Acceso a aplicaciones en redes de socios comerciales**: algunas organizaciones acceden a aplicaciones alojadas en las redes de sus socios comerciales. El uso de conexiones de servicio para conectar estas aplicaciones requiere enrutamiento manual y configuración de NAT. ZTNA

 ©2025 Palo Alto Networks, Inc.

Connector le permite conectarse a estas aplicaciones sin realizar una configuración manual de enrutamiento de IP.



 ©2025 Palo Alto Networks, Inc.

Casos de uso admitidos para conexiones de servicio y ZTNA Connector

ZTNA Connector no es un sustituto de las conexiones de servicio. Puede complementar o coexistir con las conexiones de servicio, lo que le proporciona flexibilidad en cómo proteger las aplicaciones privadas. Si ya ha implementado conexiones de servicio, puede seguir usándolas, a menos que desee pasar a un modelo de acceso a aplicaciones diferente. La siguiente tabla muestra los casos de uso admitidos y no admitidos para conexiones de servicio o ZTNA Connector. Una marca de verificación indica que el caso de uso es compatible; un guión (—) indica que no es compatible.

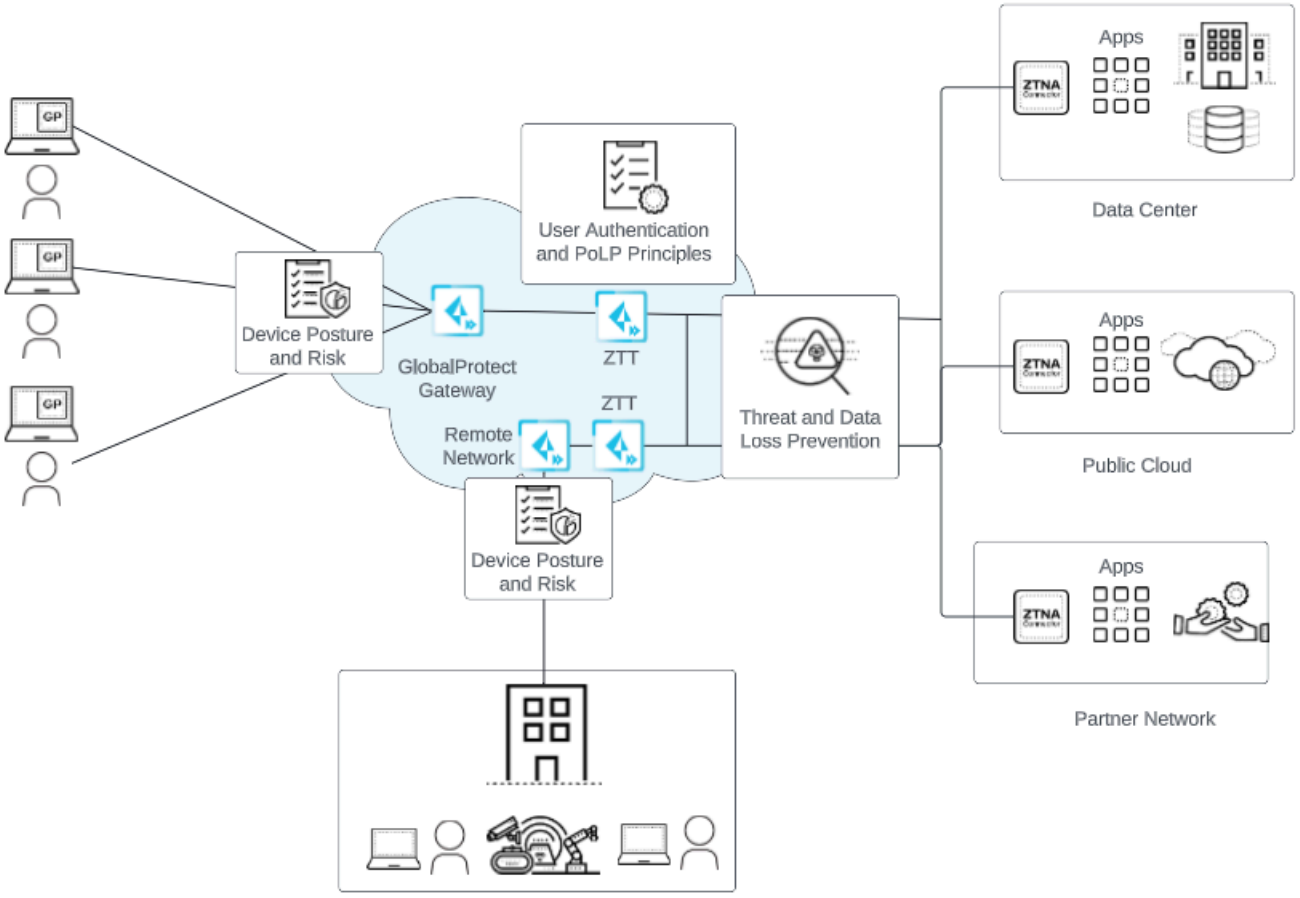
Caso de uso	Compatibilidad con ZTNA Connector	Compatibilidad con Conexiones de servicio
Acceso a aplicaciones en redes superpuestas	√	—
Acceso a todos los puertos y protocolos para el tráfico de aplicaciones iniciado por el cliente	√	√
Establecimiento automático de túneles para Prisma Access	√	—
Descubrimiento de ubicación de Prisma Access automático	√	—
Escalado automático de ubicaciones de Prisma Access para un rendimiento de hasta 10 Gbps	√	—
Acceso a aplicaciones privadas mediante direcciones IP y subredes	√	√
Tráfico iniciado por el servidor (como un servicio de asistencia técnica remoto) que llega a un dispositivo gestionado (usuario móvil o red remota de GlobalProtect).	—	√
Aplicaciones o servicios que requieren una dirección IP de cliente única	√	√
Acceso a aplicaciones con puertos dinámicos (como FTP modo activo o VoIP)	—	√
Implementaciones híbridas con cortafuegos de nueva generación donde se aplican reglas de políticas basadas en el User-ID	√	√

 ©2025 Palo Alto Networks, Inc.

Principios del ZTNA Connector 2.0

ZTNA Connector le permite conectar sus aplicaciones privadas a Prisma Access utilizando los siguientes principios de ZTNA Connector 2.0:

- **Postura y riesgo del dispositivo**: al utilizar reglas de políticas basadas en la identificación de usuario en Prisma Access, puede definir una postura para los usuarios y dispositivos (tanto usuarios móviles como dispositivos IoT) para evitar el acceso no autorizado a las aplicaciones privadas. También puede crear reglas de políticas comunes entre ZTNA Connector y Prisma Access.
- **Autenticación de usuario y acceso con mínimos privilegios**: al utilizar la autenticación de usuario y reglas de políticas basadas en el usuario o grupo, puede implementar el principio de mínimos privilegios (PoLP) para brindar a los usuarios acceso a las aplicaciones que necesitan, mientras bloquea el acceso a las aplicaciones que no necesitan.
- **Prevención de amenazas y pérdida de datos**:Prisma Access y ZTNA Connector utilizan funciones de seguridad avanzadas como Advanced Threat Prevention, Advanced URL Filtering, SaaS Security, Advanced WildFire y Enterprise DLP para garantizar que sus aplicaciones privadas y los datos de sus aplicaciones estén seguros.



 ©2025 Palo Alto Networks, Inc.

Requisitos y directrices de ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Antes de configurar ZTNA Connector, asegúrese de que entiende los requisitos y límites del conector, así como las pautas que debe seguir al implementarlo.

Requisitos y versiones compatibles de Prisma Access

- Prisma Access versión 4.0 con un Agente SaaS compatible.

  Actualice cualquier versión de Prisma Access anterior a 4.0, incluidas las versiones de Innovation, a una versión mínima de 4.0.

  Se requiere una versión mínima de Prisma Access 5.0 si desea usar comodines FQDN o subredes IP para acceder a aplicaciones. Además, Prisma Access 5.0 desbloquea el uso de las herramientas de diagnóstico de Resumen de volcado, Captura de paquetes y Asistencia técnica.
- Debe actualizar las versiones de su conector a un mínimo de 6-2-2-ztna-connector-b1 para utilizar la funcionalidad 5.0.
- Para Prisma Access (Managed by Panorama), actualice la versión del complemento Cloud Services a una versión 4.0., como mínimo. Actualice al último complemento de Cloud Services para desbloquear las últimas funciones.

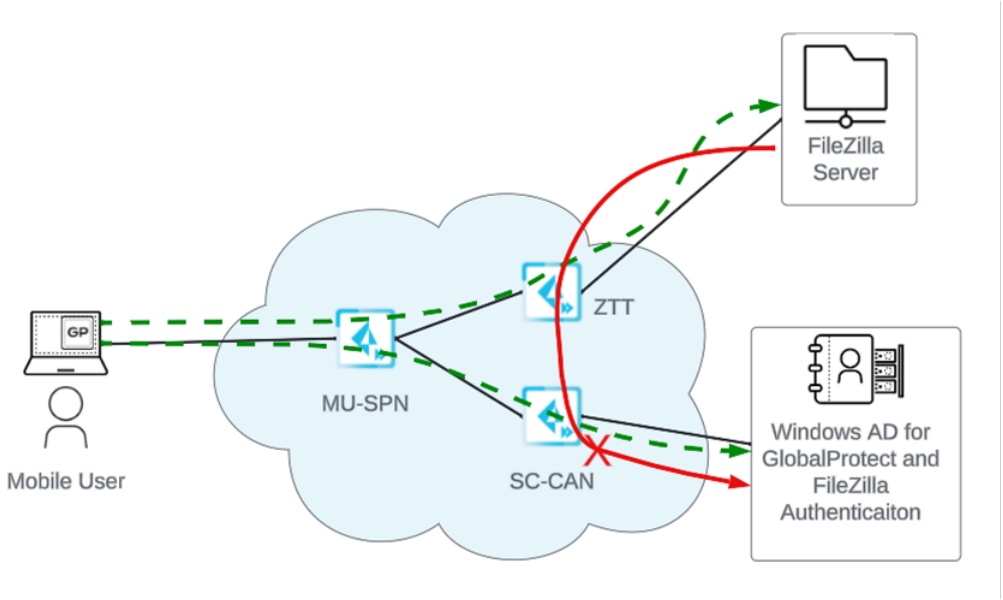
 ©2025 Palo Alto Networks, Inc.

Compatibilidad de aplicaciones

ZTNA Connector proporciona acceso a todo el tráfico de sus aplicaciones privadas, con las siguientes excepciones:

- ZTNA Connector no admite lo siguiente:
  - Tráfico originado desde el centro de datos (como el tráfico de SCCM o de asistencia remota)
  - Redistribución de ID de usuario
  - Aplicaciones que realizan saltos de puerto (como VoIP o FTP en modo activo).
  - Aplicaciones de puerta de enlace a nivel de aplicación (ALG) como FTP en modo activo y SIP.
  - La autenticación integrada de Windows para aplicaciones (como NTLM o Kerberos) solo es compatible si incorpora los controladores de dominio del centro de datos y los recursos como subredes de direcciones IP. SAML, OAuth y LDAP son compatibles.
  - La comunicación entre aplicaciones detrás de una conexión de servicio y aplicaciones detrás de un ZTNA Connector.

    Por ejemplo, tiene un servidor de Active Directory (AD) de Windows detrás de una conexión de servicio (ya que los servidores AD no son compatibles detrás de ZTNA Connector) y tiene un servidor FTP (Filezilla) detrás de un ZTNA Connector. Si el servidor FTP requiere autenticación con el servidor AD de Windows, la autenticación falla, porque no se puede usar Prisma Access como área troncal entre el Nodo de acceso corporativo de conexión de servicio (SC-CAN) y el Terminador de túnel de ZTNA Connector (ZTT).



Restricciones de características y funcionalidades

Tenga en cuenta las siguientes restricciones al configurar y establecer una implementación de ZTNA Connector:

- No utilice caracteres especiales, incluidos < > ! @ # $ % ^ & y caracteres chinos, japoneses o coreanos, en los nombres de objetos ZTNA.

 ©2025 Palo Alto Networks, Inc.

- Las siguientes funcionalidades no son compatibles con la implementación predeterminada de Prisma Access; póngase en contacto con su equipo de Palo Alto Networks para activarlas:
  - Uso de direcciones RFC 6598 para sus direcciones IP de infraestructura de Prisma Access con ZTNA Connector
- **Directrices del Grupo de Conectores**: al añadir grupos de conectores, utilice las siguientes recomendaciones:
  - Todas las aplicaciones en un único Grupo de Conectores deben utilizar el mismo servidor DNS para la resolución DNS.
  - Si está accediendo a aplicaciones desde un centro de datos o una sede central, todas las aplicaciones en el Grupo de conectores deben ser del mismo centro de datos o sede.
  - No añada conectores en dos o más regiones en un solo Grupo de conectores. Todos los conectores en un Grupo de conectores deben estar en la misma región.
  - A partir de Prisma Access 5.01, puede especificar hasta cuatro grupos de conectores por objetivo FQDN o objetivo comodín (la versión 5.0 y anteriores admiten un solo grupo de conectores por objetivo FQDN o objetivo comodín). Asegúrese de que, cuando asigne grupos de conectores por objetivo FQDN o objetivo comodín, no asigne la misma aplicación a más de cuatro conectores por región.

    Por ejemplo, ha asignado la misma aplicación (ya sea un objetivo FQDN o un objetivo comodín) a cuatro grupos de conectores, cada grupo tiene un solo conector, y todos los conectores están en la misma región. Esta configuración es aceptable porque no está asignando más de cuatro conectores por aplicación en una sola región.

    Sin embargo, si asigna la misma aplicación (ya sea un objetivo FQDN o un objetivo comodín) a tres grupos de conectores, cada grupo tiene dos conectores, y todos los conectores están en la misma región, eso es una configuración no válida, porque está asignando seis conectores a la misma aplicación en una única región.
- Algunos conectores ZTNA, como los conectores basados en AWS o los conectores basados en Azure, admiten escalado automático, donde AWS o Azure supervisan la utilización del ancho de banda de la red en los conectores y ajustan automáticamente la capacidad para mantener el rendimiento de la aplicación. Cuando la utilización del ancho de banda de la red en los conectores disminuye, AWS o Azure activan el escalado automático. Si se produce una reducción de escalado en un ZTNA Connector, las sesiones existentes de larga duración gestionadas por ZTNA Connector marcadas para la reducción de escalado se terminan prematuramente. Este comportamiento no afecta a las nuevas sesiones de tráfico iniciadas después de la reducción de escala. Para sesiones de larga duración, como SSH o RDP, ZTNA Connector termina la sesión durante la reducción de escalado y, por tanto, debe reconectar esa sesión.

Consideraciones sobre la capacidad de ampliación y el rendimiento

ZTNA Connector admite los siguientes valores máximos:

- 4.096 aplicaciones por inquilino en todos los grupos de conectores
- 200 conectores por inquilino
- 512 aplicaciones por grupo de conectores
- 4 conectores por grupo de conectores

 ©2025 Palo Alto Networks, Inc.

- 200.000 sesiones concurrentes por conector

  Cada conector puede soportar 200.000 conexiones concurrentes. Un Grupo de conectores puede tener un máximo de 4 conectores para hasta 800,000 conexiones concurrentes por Grupo de conectores.
- 26 regiones de cómputo
- 1 Gbps de rendimiento por conector, con un máximo de 10 Gbps por ubicación de cómputo de Prisma Access

Entornos de alojamiento de aplicaciones compatibles

Puede implementar sus VMs de conector ZTNA en los siguientes entornos de centros de datos con los requisitos mínimos especificados:

Proveedor de nube	Tamaño de la instancia	Tamaño de CPU	Tamaño de la memoria	Tamaño de disco
Amazon AWS	m5.xlarge por región	4 vCPU	16 GB	40 GB
Google Cloud Platform (GCP)	n2-standard-4 por región	4 vCPU	16 GB	40 GB
Microsoft Azure	Standard_D4_v3 por región	4 vCPU	16 GB	40 GB
KVM	Usa imagen qcow	4 vCPU	16 GB	40 GB
Hyper-V	Usa imagen vhd	4 vCPU	8 GB de memoria por máquina virtual	40 GB
VMware ESXi	Usa imagen OVA. Compatible con vSphere y directamente en Hosts ESXi	4 vCPUs por máquina virtual	8 GB de memoria por máquina virtual	40 GB de disco (aprovisionamiento grueso)

Para VMware ESXi, vMotion, instantáneas de VM o migraciones no son compatibles con las VM del conector.

Para KVM, las migraciones en tiempo real y las instantáneas no son compatibles con las máquinas virtuales del conector.

Es su responsabilidad alojar las VM y asegurarse de que puedan conectarse a Internet.

 ©2025 Palo Alto Networks, Inc.

AWS, GCP y Azure tienen conectores ZTNA que puede adquirir en sus respectivos marketplaces. Puede descargar el archivo de Aplicación de Virtualización Abierta (OVA) de VMware ESXi y el archivo qcow de KVM desde el Portal de Soporte al Cliente de Palo Alto.

Requisitos de red

Los siguientes requisitos de red permiten la conectividad entre ZTNA Connector y Prisma Access:

- Después de habilitar ZTNA Connector Prisma Access configura un proxy DNS para las solicitudes DNS utilizando las reglas DNS establecidas para Redes remotas y Usuarios móviles: GlobalProtect.
- El tamaño de la carga útil de UDP, incluidos los encabezados, no debe superar un tamaño de MTU de 1.300 bytes en el camino hacia el servidor de aplicaciones ZTNA. Palo Alto Networks recomienda mantener los paquetes en o por debajo de este tamaño de MTU.
- Permita el tráfico saliente a través de los puertos UDP 4500 y UDP 500 desde la dirección IP de la interfaz WAN (puerto 1) para la conectividad IPSec e IKE con ZTNA Tunnel Terminator (ZTT). Si desea limitar la habilitación de una conexión UDP saliente en el puerto 500 y 4500 a una única dirección IP, habilítela para la dirección **PA Service IP (IP del servicio PA)** (en**Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**) del ZTNA Connector.



- Si ZTNA Connector utiliza una dirección IP pública para su interfaz de internet, debe permitir un carga de seguridad encapsulada (ESP) IP/50.
- Permitir el tráfico saliente del puerto TCP 443 desde la dirección IP de la interfaz WAN (puerto 1) para la conectividad HTTPS con los controladores de ZTNA Connector.
- ZTNA Connector se configura automáticamente tanto el lado de ZTT de Prisma Access del túnel IPSec como el lado del ZTNA Connector. Los algoritmos configurados para el grupo/encriptación/hash DH para IKE y ESP son: ecp384/aes256/sha512.
- No termine el túnel IPSec que crea y utiliza ese ZTNA Connector para acceder a las aplicaciones privadas.
- (Implementaciones de Usuarios móviles: GlobalProtect únicamente) Cuando inicie por primera vez una aplicación en ZTNA Connector, debe actualizar la aplicación GlobalProtect para que los usuarios móviles reciban la configuración actualizada del servidor DNS. Si eliminó una aplicación del ZTNA Connector, debe actualizar la aplicación de GlobalProtect para que los usuarios móviles puedan recibir la configuración actualizada del servidor DNS.
- Si hay un cortafuegos entre ZTNA Connector y la aplicación privada, el cortafuegos debe permitir el acceso a la aplicación desde ZTNA Connector (es decir, debe permitir el acceso a las direcciones IP resueltas del servidor de la aplicación, protocolos y puertos para la aplicación privada).

  Además, necesita permitir el protocolo (ya sea TCP o ICMP) que configuró para las sondas de estado del objetivo de la aplicación a la app. La aplicación del conector sondea el servidor de aplicaciones para determinar si puede proporcionar acceso a la aplicación, y puede configurar el Tipo de sondeo para el Objetivo de la aplicación como **tcp ping**, **icmp ping** o **none (ninguno)**

 ©2025 Palo Alto Networks, Inc.

(sin sondeo). Si especifica **ping tcp**, el cortafuegos debe permitir el acceso TCP a la aplicación; si especifica **ping icmp**, el cortafuegos debe permitir la solicitud y respuesta de eco ICMP para la aplicación.

- Asegúrese de permitir ICMP en su centro de datos antes de usar las herramientas de diagnóstico ping y traceroute. Algunos entornos en la nube tienen ICMP deshabilitado por razones de seguridad; en este caso, estas herramientas no muestran ninguna actividad.

  La herramienta de diagnóstico traceroute también utiliza puertos UDP aleatorios, por lo que debe permitir todas las respuestas de error UDP e ICMP para que la herramienta traceroute funcione.
- Asegúrese de haber configurado las entradas DNS en las interfaces locales para permitir que ZTNA Connector resuelva los FQDNs de la aplicación, y que ZTNA Connector pueda acceder al servidor DNS en el puerto UDP 53 (el puerto utilizado para la resolución DNS).
- (Versiones del ZTNA Connector 5.0 y posteriores) Asegúrese de haber configurado reglas de seguridad en su red para permitir que los conectores ZTNA realicen sondeos de aplicaciones en su centro de datos. Los conectores ZTNA utilizan la dirección IP de la interfaz de su centro de datos como la dirección IP de origen de la aplicación que sondea a los servidores de aplicaciones. Si la exploración de la aplicación es correcta, el estado de la aplicación está **UP (Activa)** y las sesiones de usuario al ZTNA Connector tienen la misma dirección IP de interfaz de centro de datos que la dirección IP de origen. Si la exploración de la aplicación no tiene éxito, el estado de la aplicación está **Down (Inactiva)**; en este caso, puedes utilizar las herramientas de diagnóstico ping y tcp ping para que la aplicación pruebe las conexiones.
- Si utiliza direcciones compartidas RFC 6598 dentro de su red, debe especificar bloques de direcciones IP que ZTNA Connector puede usar para el enrutamiento entre Prisma Access y sus conectores y entre Prisma Access y sus aplicaciones privadas.
- Si necesita restringir la lista de direcciones IP y FQDN que añade a las listas de permitidos de su organización, añada las que se enumeran en Direcciones IP y FQDN que se permiten para ZTNA Connector.

  Por ejemplo, si está configurando un ZTNA Connector en los Estados Unidos, añade las siguientes URL a las listas de permitidos de su organización:

  - https://controller.cgnx.net
  - https://locator.cgnx.net
  - https://controller.hood.cgnx.net
  - https://vmfg.hood.cgnx.net
  - https://sdwan-stats-hood-us.cgnx.net
  - time.nist.gov (for NTP)
  - 0.cloudgenix.pool.ntp.org (for NTP)
  - 1.cloudgenix.pool.ntp.org (for NTP)
  - 2.cloudgenix.pool.ntp.org (for NTP)
  - 3.cloudgenix.pool.ntp.org (for NTP)

  Limite la resolución DNS de los FQDNs anteriores a la resolución IPv4. ZTNA Connector no admite el establecimiento de conexión a los FQDN del controlador utilizando IPv6.

 ©2025 Palo Alto Networks, Inc.

- Deshabilitar el descifrado SSL para las sesiones a los Controladores.

Direcciones IP y FQDN que se permiten para ZTNA Connector

Para garantizar el funcionamiento fluido de ZTNA Connector, añada las siguientes URL y direcciones IP a sus listas de permitidos.

Nombre del servicio	Puerto	DIRECTION	Interfaz de protocolo de internet de origen	Destino y direcciones IP
Acceso de ZTNA Connector a Prisma Access	443	Saliente	Puerto WAN del ZTNA Connector	https://controller.cgnx.net Dirección: 52.8.93.87 Dirección: 52.8.25.40 https://locator.cgnx.net Dirección: 13.56.217.238 Dirección: 13.56.201.169 hood: 52.40.98.31 34.218.98.185 sugarloaf: 18.200.102.82 18.200.135.33 faber: 18.139.242.53 54.255.61.109 https://vmfg.cgnx.net Dirección: 52.53.122.104 Dirección: 52.53.102.7 https:// controller.elcapitan.cgnx.net Dirección: 52.8.93.87 Dirección: 52.8.25.40 https://vmfg.elcapitan.cgnx.net Dirección: 52.53.122.104 Dirección: 52.53.102.7 https:// controller.hood.cgnx.net

©2025 Palo Alto Networks, Inc.

Nombre del servicio	Puerto	DIRECTION	Interfaz de protocolo de internet de origen	Destino y direcciones IP
				Dirección: 52.32.167.5 Dirección: 54.70.168.33 https://vmfg.hood.cgnx.net Dirección: 50.112.136.184 Dirección: 34.210.34.87 https://controller.sugarloaf.cgnx.net Dirección: 108.128.176.192 Dirección: 18.200.144.58 https://vmfg.sugarloaf.cgnx.net Dirección: 99.81.179.99 Dirección: 99.80.52.255 https://sdwan-stats-hood-us.cgnx.net https://sdwan-stats-elcapitan-us.cgnx.net https://sdwan-stats-hood-jp.cgnx.net https://sdwan-stats-elcapitan-jp.cgnx.net https://sdwan-stats-hood-sg.cgnx.net https://sdwan-stats-elcapitan-sg.cgnx.net https://sdwan-stats-hood-au.cgnx.net https://sdwan-stats-elcapitan-au.cgnx.net https://sdwan-stats-hood-in.cgnx.net https://sdwan-stats-elcapitan-in.cgnx.net https://sdwan-stats-hood-ca.cgnx.net

©2025 Palo Alto Networks, Inc.

Nombre del servicio	Puerto	DIRECTION	Interfaz de protocolo de internet de origen	Destino y direcciones IP
				https://sdwan-stats-elcapitan-ca.cgnx.net https://sdwan-stats-sugarloaf-eu.cgnx.net https://sdwan-stats-sugarloaf-de.cgnx.net https://sdwan-stats-sugarloaf-uk.cgnx.net https://controller.bowfell.cgnx.net Address: 13.41.243.90 Dirección: 18.171.17.23 https://vmfg.bowfell.cgnx.net Dirección: 52.56.35.36 Dirección: 52.56.224.242 https://controller.faber.cgnx.net Dirección: 52.74.47.220 Dirección: 13.251.109.27 https://vmfg.faber.cgnx.net Dirección: 18.142.153.59 Dirección: 52.74.58.219 h ttps://controller.townsend.cgnx.net Dirección: 13.55.31.41 Dirección: 3.106.168.215 https://vmfg.townsend.cgnx.net Dirección: 52.64.177.240 Dirección: 13.55.164.51 https://sdwan-stats-faber-sg.cgnx.net

 ©2025 Palo Alto Networks, Inc.

Nombre del servicio	Puerto	DIRECTION	Interfaz de protocolo de internet de origen	Destino y direcciones IP
				https://sdwan-stats-bowfell-uk.cgnx.net https://sdwan-stats-townsend-au.cgnx.net
NTP	123	Saliente	Puertos WAN y LAN del ZTNA Connector	time.nist.gov 0.cloudgenix.pool.ntp.org 1.cloudgenix.pool.ntp.org 2.cloudgenix.pool.ntp.org 3.cloudgenix.pool.ntp.org
DNS:	53	Saliente	Puertos WAN y LAN del ZTNA Connector	Servidores DNS de cliente o proveedor

Gestión de certificados

Para garantizar la confianza entre las partes en una sesión de comunicación segura, Prisma Access utiliza certificados digitales. Cada certificado contiene una clave criptográfica para cifrar el texto sin formato o descifrar el texto cifrado. Cada certificado también incluye una firma digital para autenticar la identidad del emisor. Este debe estar incluido en la lista de entidades de certificación (CA) de confianza de la parte que realiza la autenticación. De manera opcional, la parte que realiza la autenticación verifica que el emisor no haya revocado el certificado. Prisma Access utiliza certificados para proteger funciones como el descifrado y la autenticación, y para asegurar la comunicación entre todos los clientes, servidores, usuarios y dispositivos que se conectan a su red.

Para las aplicaciones incorporadas a Conector ZTNA, configure sus certificados, añada autoridades de certificación y defina las comprobaciones de certificados utilizando la Prisma Access Certificate Management (Gestión de certificados de Prisma Access).

 ©2025 Palo Alto Networks, Inc.

Habilitar el conector ZTNA

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Antes de que pueda configurar el conector ZTNA Connector, debe habilitarlo en Prisma Access. Antes de habilitar ZTNA Connector, haga lo siguiente:

- Revise los Requisitos y directrices de ZTNA Connector.
- Identifique los bloques de direcciones IP de su aplicación y de su conector. Debe reservar un grupo de direcciones separado para reservar para su uso internamente en Prisma Access para enrutar el tráfico a los conectores y aplicaciones privadas que va a incorporar. Prisma Access resuelve los FQDN de las aplicaciones que incorpora a ZTNA Connector a las direcciones IP en el bloque de direcciones IP de la aplicación. De manera similar, Prisma Access utiliza el bloque de direcciones IP del conector para enrutar el tráfico desde la red remota o el usuario móvil hacia el ZTNA Connector apropiado.

  Debería reservar al menos una subred /16 para el grupo de direcciones. Utiliza direcciones RFC 1918 o RFC 6598. Puede especificar un grupo de direcciones RFC 1918 durante la configuración de ZTNA Connector en lugar de RFC 6598; sin embargo, no puede cambiar el tipo de grupo de direcciones de nuevo a RFC 6598 después de especificar RFC 1918.
- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

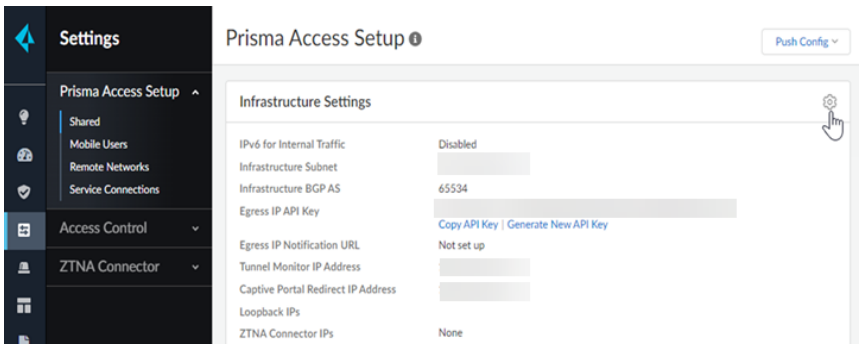
Habilitar ZTNA Connector (Strata Cloud Manager)

Utilice el siguiente flujo de trabajo para habilitar el conector ZTNA Connector en Cloud Managed Prisma Access.

STEP 1 | Configure los bloques de direcciones IP que Prisma Access usará internamente para enrutar el tráfico al conector ZTNA y a las aplicaciones privadas que incorpore.

Debe definir bloques de direcciones IP separados para sus conectores y sus aplicaciones, y los bloques no pueden superponerse entre sí, con la subred de infraestructura de Prisma Access o con su grupo de direcciones IP de GlobalProtect.

- Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de la infraestructura)**.



- Añada **ZTNA Connectors Application IP Blocks (Bloques IP de aplicaciones de ZTNA Connectors)**.

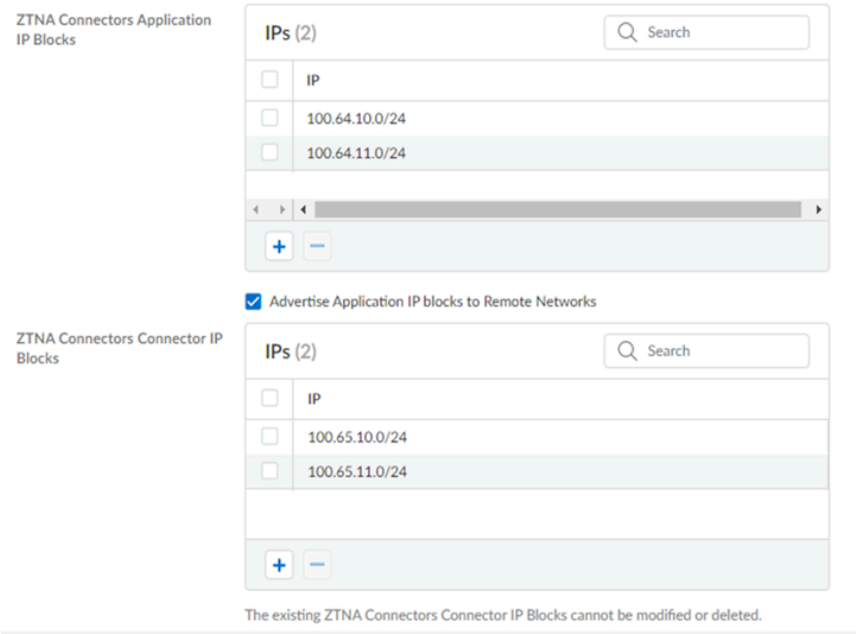
  Puede añadir un único Bloque de direcciones IP de aplicaciones o varios bloques en función de la implementación. Por ejemplo, introduzca 100.64.10.0/24 y 100.64.11.0/24. También puede hacer lo siguiente: **Advertise Application IP blocks to Remote Networks (Anunciar bloques de IP de aplicaciones a redes remotas)** para proporcionar acceso remoto a la red.

- Añadir **ZTNA Connectors Connector IP Blocks (Bloques IP de conector deZTNA Connector)** que Prisma Access utilizará internamente para enrutar el tráfico entre los

 ©2025 Palo Alto Networks, Inc.

usuarios móviles, las redes remotas y las máquinas virtuales del conector en sus centros de datos.

Puede añadir un solo bloque de IP de conector o varios bloques en función de su implementación. Por ejemplo, introduzca 100.65.10.0/24 y 100.65.11.0/24.

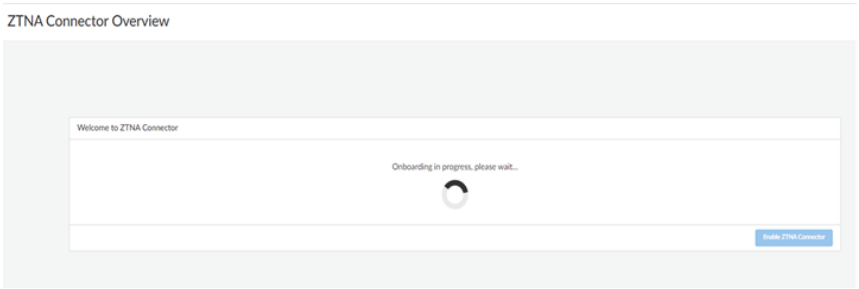


- Haga clic en **Save (Guardar)** para guardar la configuración del bloque de direcciones IP y, a continuación, **Commit (Confirmar)** y enviar la configuración.

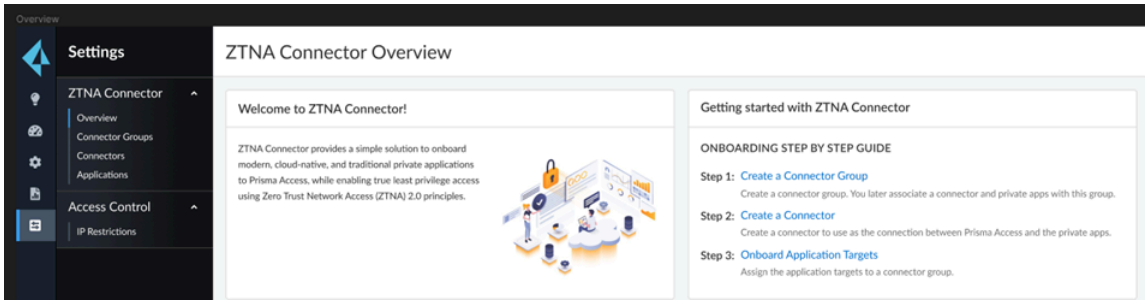
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Inicie ZTNA Connector desde Strata Cloud Manager.

- Seleccione **Workflows (Flujos de trabajo)** > **Conector ZTNA**.
- Prisma Access comienza a configurar la infraestructura para el conector ZTNA. Esto puede requerir unos minutos.



- Cuando finaliza la incorporación, se muestra la descripción general de ZTNA Connector.



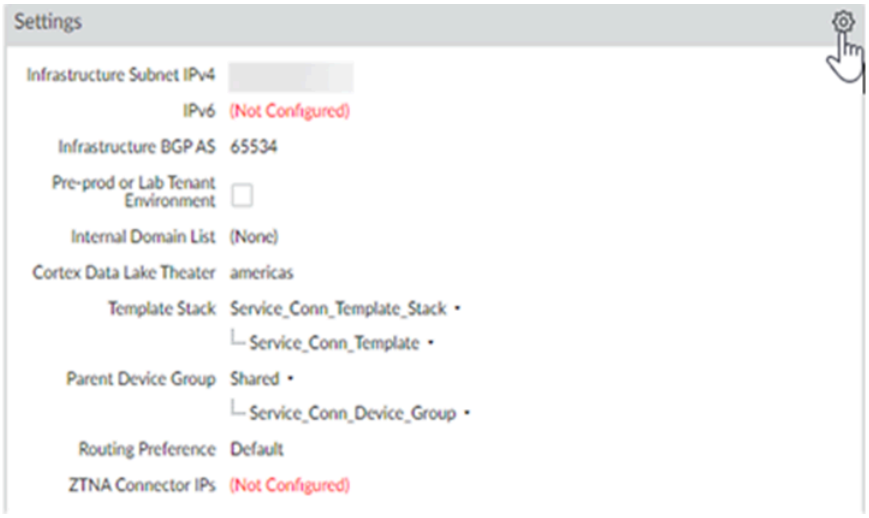
Habilitar ZTNA Connector (Panorama)

Utilice el siguiente flujo de trabajo para habilitar ZTNA Connector en Prisma Access (Managed by Panorama).

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configure los bloques de direcciones IP que Prisma Access usará internamente para enrutar el tráfico al conector ZTNA y a las aplicaciones privadas que incorpore.

- Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y **Edit (Editar** la **Settings (Configuración)**.



- En la pestaña **ZTNA Connector**, seleccione **Add (Añadir)** un **Application IP Block (Bloque de IP de** aplicaciones).

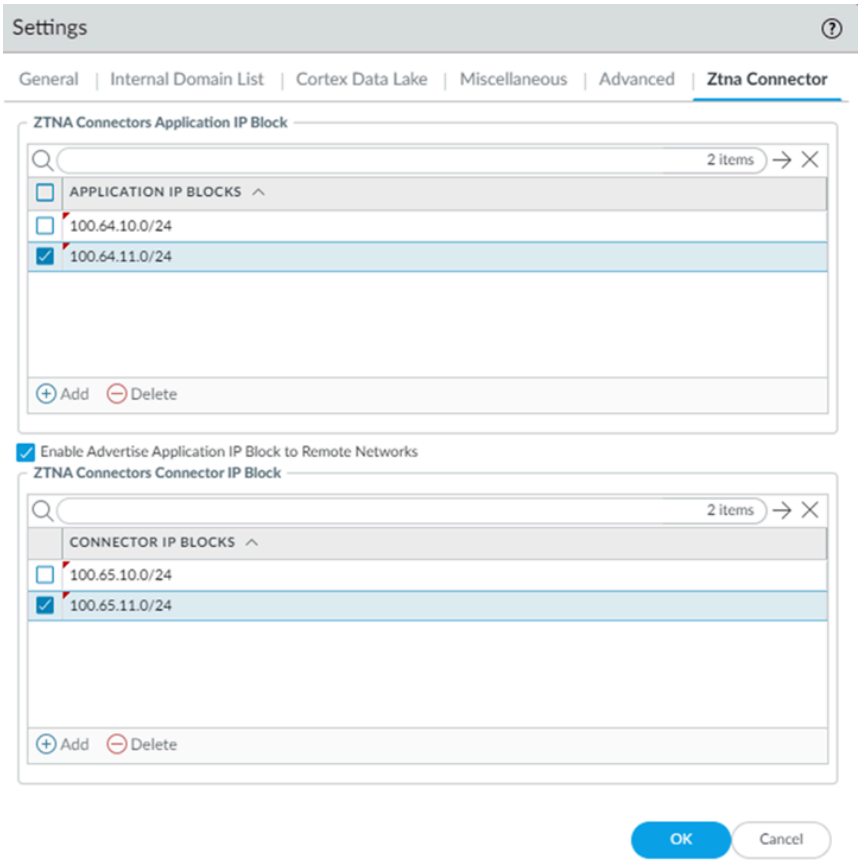
  Puede añadir un solo bloque IP de aplicaciones o varios bloques según su implementación. Por ejemplo, si 100.64.10.0/24 y 100.64.11.0/24. También puede **Enable Advertise**

 ©2025 Palo Alto Networks, Inc.

Application IP Block to Remote Networks (Habilitar Anunciar bloque de IP de aplicaciones a redes remotas).

- Establezca los **Connector IP Blocks (Bloques IP del conector)** que Prisma Access utilizará internamente para enrutar el tráfico entre usuarios móviles, redes remotas y las máquinas virtuales conectoras en sus centros de datos.

  Puede añadir un solo bloque de direcciones IP del conector o varios bloques según su implementación. Por ejemplo, introduzca 100.65.10.0/24 y 100.65.11.0/24.

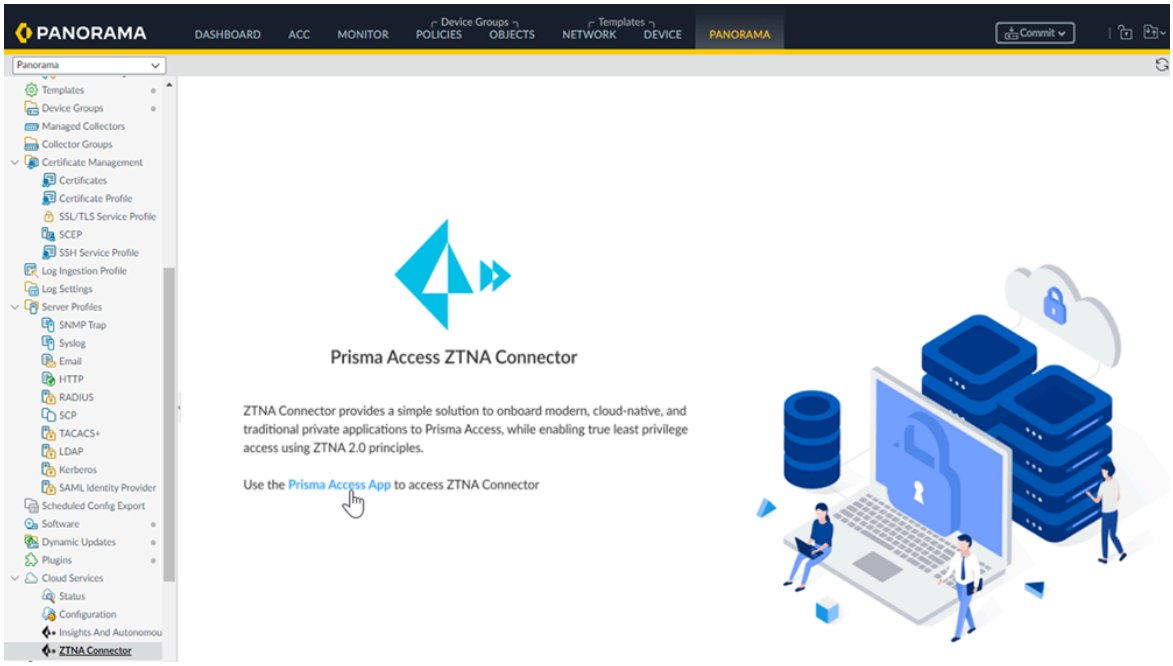


- Haga clic en **OK (Aceptar)** para guardar la configuración del bloque de direcciones IP y, a continuación, seleccione **Commit (Confirmar)** y enviar la configuración.

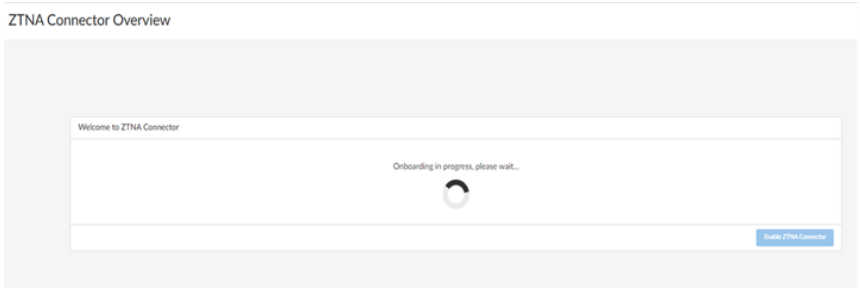
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Inicie ZTNA Connector desde el complemento Cloud Services en Panorama.

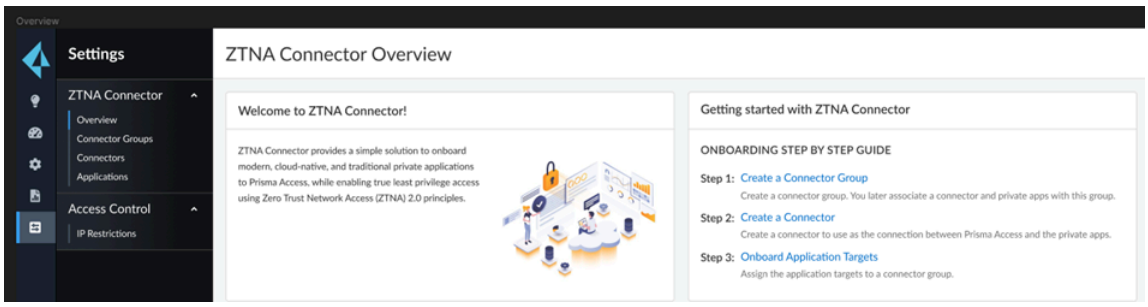
- Seleccione**Panorama** > **Cloud Services (Servicios en la nube)** > **ZTNA Connector**.
- Haga clic en Strata Cloud Manager para iniciar ZTNA Connector en Strata Cloud Manager en el hub.



- Desde Strata Cloud Manager, seleccione **Settings (Configuración)** > **ZTNA Connector**.
- Prisma Access comienza a configurar la infraestructura para el conector ZTNA. Esto puede requerir unos minutos.



- Cuando finaliza la incorporación, se muestra la descripción general de ZTNA Connector.



 ©2025 Palo Alto Networks, Inc.

Configurar ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Después de que usted Habilitar el conector ZTNA puede comenzar a configurar los componentes de ZTNA Connector:

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Identifique los bloques de direcciones IP de la aplicación y del conector y añada los bloques de direcciones IP en Prisma Access.

Consulte la siguiente recomendación para los bloques de direcciones IP:

- *Asigne una dirección IP independiente para cada aplicación.*
- *Asigne a cada conector un bloque de direcciones IP /27 como mínimo (mínimo de 32 direcciones IP por conector).*
- *Asigne una dirección IP única a cada Grupo de conectores.*

Puede añadir más conectores o bloques de aplicación para acomodarlos según sea necesario.

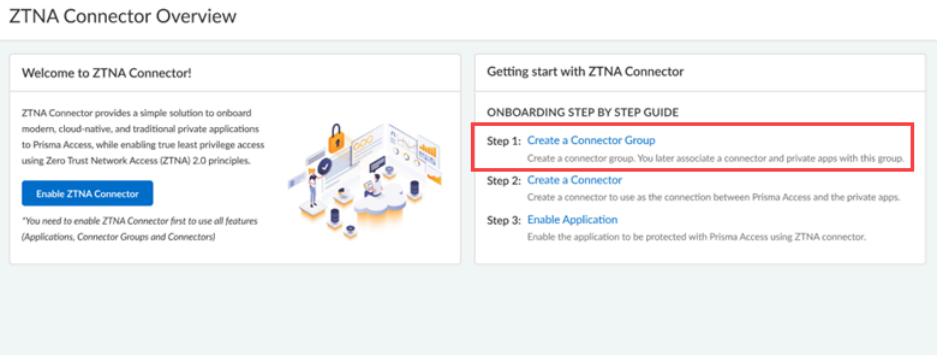
Si utiliza direcciones RFC 6598 dentro de su red, debe reservar un grupo de direcciones IP RFC 6598 independiente para reservar para su uso dentro de Prisma Access internamente para enrutar el tráfico a los conectores y las aplicaciones privadas que va a incorporar.

STEP 2 | Crear un grupo de conectores.

Los grupos de conectores son agrupaciones lógicas de conectores y aplicaciones. Hay muchas formas diferentes de agrupar aplicaciones y conectores. Puede agrupar conectores en diferentes ubicaciones geográficas para obtener redundancia. O bien, puede crear varios conectores en el mismo centro de datos para aumentar el rendimiento. Para simplificar la gestión de directivas, es posible que desee agrupar las aplicaciones que utilizan los mismos grupos de usuarios. Cree primero los grupos de conectores y, a continuación, añada los conectores y las aplicaciones a los grupos.

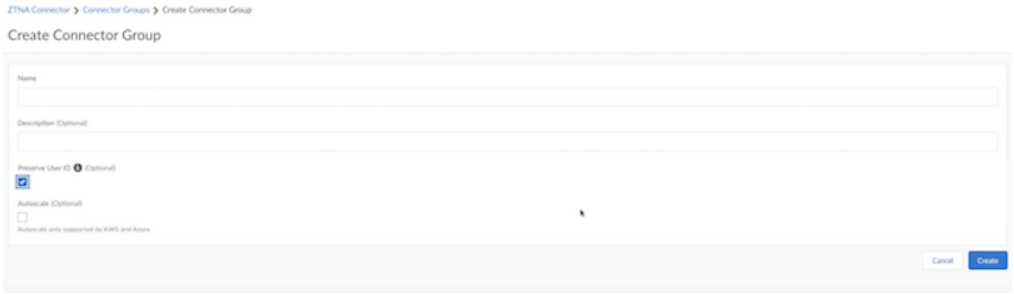
Repita este paso tantas veces como sea necesario para crear todos los grupos de conectores que necesite para agrupar los conectores y las aplicaciones.

1. Seleccione**Workflows (Flujos de trabajo)** > **ZTNA Connector (Conector ZTNA)**, seleccione **Overview (Visión general)** o **Connector Groups (Grupos de conectores)** y **Create Connector Group (Crear grupo de conectores)**.



 ©2025 Palo Alto Networks, Inc.

2. Asigne un **Name (Nombre)** al grupo de conectores, habilite **Preserve User ID (Conservar el ID de usuario)**y, opcionalmente, proporcione una **Description (Descripción)** para ello.



3. (Opcional) Si el centro de datos está en Azure o AWS y desea utilizar la funcionalidad de escalado automático, seleccione **Autoscale (Escalado automático)**. Si ha habilitado esta funcionalidad, no es necesario crear un conector.
4. **Create (Crear)** grupo de conectores

STEP 3 | *Cree un conector y añádalo a un grupo de conectores solo cuando seleccione un grupo de conectores que no sea de escalado automático.*

Cree conectores y agréguelos al grupo de conectores.

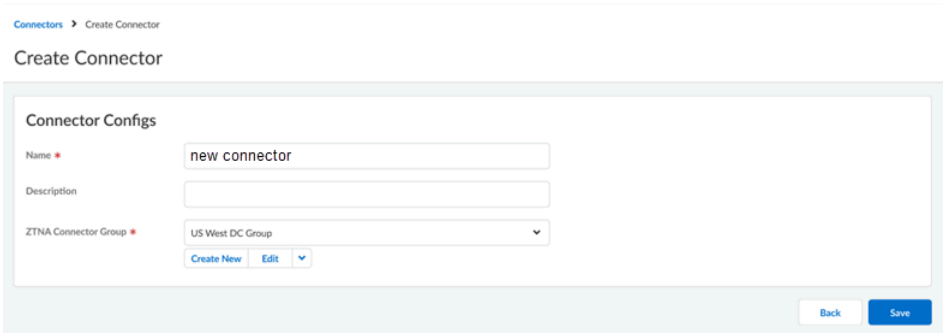
Los conectores representan las máquinas virtuales que se ejecutan en los centros de datos y que se conectan a Prisma Access. Debe crear el conector dentro de Prisma Access y

 ©2025 Palo Alto Networks, Inc.

usar el secreto o la clave proporcionados para incorporar la máquina virtual del conector correspondiente en el centro de datos.

Repita este paso según sea necesario para crear tantos conectores como necesite para conectar las aplicaciones del centro de datos a Prisma Access.

- Seleccione**Workflows (Flujos de trabajo)** > **ZTNA Connector (Conector ZTNA)**, seleccione **Overview (Visión general)** o **Connectors (Conectores)** y luego **Create Connector (Crear conector)**.
- Introduzca un **Name (Nombre)** para el Conector.



- (Opcional) Añada una **Description (Descripción)** para el Conector.
- Seleccione el **Connector Group (Grupo de conectores)** donde se debe añadir el conector.

Para simplificar el enrutamiento y obtener un acceso más rápido a los servidores del centro de datos, Palo Alto Networks recomienda que los conectores y los servidores estén en la misma subred.

- **Create (Crear)** el conector.

Para mantener los conectores ZTNA actualizados, puede actualizar su versión de software*. Los iconos de la clase* ***ZTNA Connector (Conector ZTNA)*** *>* ***Connector Groups (Grupos de conectores)*** *muestra el estado de los conectores y si hay una actualización disponible.*

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Recupere la clave y el secreto que usará para configurar el conector.

Los valores Clave y Secreto se usan al configurar las máquinas virtuales en un paso posterior.

1. Grupo de conectores de escalado automático—Siga los pasos que se indican a continuación:
   1. Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connector Groups (Grupos de conectores)**.
   2. Seleccione **Copy Token (Copiar token)** en el área **Actions (Acciones)** del grupo de conectores de escalado automático; a continuación, copie los valores **Key (Clave)** y **Secret (Secreto)**.

      Utilice la clave y el secreto para asociar la instancia de nube o la máquina virtual que cree con el Conector.
2. Grupo de conectores que no tienen escalado automático—Siga los pasos que se indican a continuación:
   - Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**.
   - Seleccione el conector que desea implementar.
   - Seleccione **Copy Token (Copiar token)** en el área **Actions (Acciones)**, a continuación, copie los valores **Key (Clave)** y **Secret (Secreto)**.

     Utilice la clave y el secreto para asociar la instancia de nube o la máquina virtual que cree con el Conector.

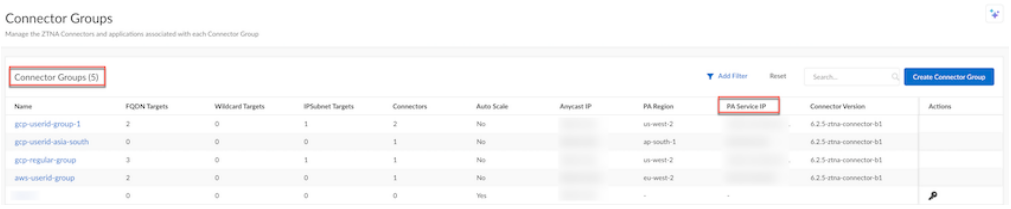


STEP 5 | Implemente sus máquinas virtuales de ZTNA Connector en su centro de datos.

STEP 6 | (Opcional) Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector (Conector ZTNA)** > **Conector Groups (Grupos de conectores)**, tome nota de la dirección **PA Service IP (IP de servicio de PA)** del grupo de conectores y añada esta dirección IP a las listas de permitidos de su organización.

*Puede ver **PA Service IP (IP del servicio de PA)** en **Connector Groups (Grupos de conectores)** solo después de incorporar su conector.*

Si es necesario, añada esta dirección IP a sus listas de permitidos para que su red pueda transmitir y recibir tráfico del conector ZTNA.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Añada los destinos a los grupos de conectores.

Configure destinos para acceder a las aplicaciones privadas en los centros de datos a través de las máquinas virtuales de ZTNA Connector. Puede añadir destinos en función de comodines de FQDN, FQDN o subredes IP; ZTNA Connector realiza el trabajo de configurar la configuración de red y DNS necesaria para que sus usuarios móviles y usuarios en sucursales accedan a las aplicaciones de forma segura a través de Prisma Access.

1. Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)**.
2. Seleccione el tipo de destino que desea crear.



Con la mejora de la incorporación de aplicaciones sin compromiso, la incorporación de aplicaciones ahora tarda menos de un minuto, lo que permite un acceso rápido a las aplicaciones. Esta función también le permite incorporar un mayor número de aplicaciones.

Limitaciones:

- *No se puede añadir el mismo FQDN en varios destinos de aplicación (con diferentes puertos o protocolos).*
- *Al añadir o eliminar un destino comodín, se produce una confirmación en MU o RN para añadir o eliminar reglas de reenvío de proxy DNS. Sin embargo, la detección posterior de aplicaciones comodín de FQDN que coincidan con el comodín no requiere ninguna confirmación adicional, por lo tanto, la incorporación rápida de aplicaciones para que tenga acceso inmediato a ellas.*

Para habilitar la función de incorporación de aplicaciones sin compromiso, actualice el archivo el plano de datos de Prisma Access a la versión 11.2.3 y posteriores.

- **Wildcard Targets (Objetivos comodín)**: utilice un comodín (por ejemplo, *.example.com) para el objetivo. Cuando los usuarios acceden a sitios que coinciden con el comodín, esas aplicaciones se incorporan automáticamente para acceder desde ZTNA Connector para sus usuarios móviles y usuarios de red remotos. Por ejemplo, dado un comodín de *.example.com, cuando los usuarios acceden a la aplicación en app1.example.com, el conector ZTNA crea automáticamente la configuración para incorporar esa aplicación secundaria con su FQDN, protocolo y puerto específicos.

  Además, cuando los usuarios acceden a una aplicación basada en un comodín (por ejemplo, app1.example.com basada en el comodín *.example.com), la aplicación se detecta y se incorpora automáticamente como un **FQDN Target (Destino de FQDN)**.

  1. Vaya a **Wildcard Targets (Objetivos comodín)** y seleccione **Create Wildcard Target (Crear objetivo comodín)**.
  2. Introduzca un **Name (Nombre)** único para el objetivo.

 ©2025 Palo Alto Networks, Inc.

3. Introduzca el **Connector Group (Grupo de conectores)** para asociarlo con el destino.

   El Grupo debe ser un tipo de **FQDN/Wildcard (FQDN/comodín)**.

   A partir de Prisma Access 5.0.1, puede seleccionar varios grupos de conectores para destinos comodín y FQDN, hasta un máximo de cuatro grupos de conectores por destino comodín o FQDN. Utilice las directrices al seleccionar varios grupos de conectores por destino.

4. Introduzca el archivo **Wildcard (Comodín)** para usar con el destino.

   Escríbalo en el formato .example.com o .my.example.com (la interfaz de usuario añade implícitamente el asterisco al frente del comodín). No permita todos los sitios especificando un comodín de *.*, ejemplo.*.com o *.com.

5. Seleccione **Protocol (Protocolo)** (**TCP**, **UDP** o ambos).

6. (Opcional) Para habilitar el protocolo ICMP de un usuario de GlobalProtect a un centro de datos de Conector ZTNA, seleccione **Allow ICMP Protocol (Permitir el protocolo ICMP)**.

7. Seleccione la opción **Port (Puerto)** para usar en la aplicación.

   Introduzca un solo puerto, varios puertos mediante comas entre los puertos, un rango de puertos mediante guiones o ambos. No añada espacios después de las comas. Seleccione **Any (Cualquier)** puerto para que coincida con los puertos que especifique, o seleccione **Match (Coincidencia)** e introduzca el puerto o los puertos que coincidan.

   Si ha seleccionado **both (ambos)** en **Protocol (Protocolo)**, tiene que añadir puertos a **TCP Port (Puerto TCP)** y **UDP Port (Puerto UDP)**

   Al introducir un rango en el campo **TCP Port (Puerto TCP)**, en **Advanced Settings (Ajustes avanzados)**, **icmp ping** y **none (ninguno) Probing Type (Tipo de sondeo)** se activa.

8. Introduzca un **Probing Type (Tipo de sondeo)** de **tcp ping (ping tcp)**, **icmp ping (ping icmp)**o **none (ninguno)**, en función del protocolo que seleccione.

   Si selecciona **tcp ping (ping tcp)**, seleccione un **probing port (puerto de sondeo)** e introduzca un solo puerto. El puerto no tiene que estar en el rango de puertos que introdujo en el área **port (puerto)** y **protocol (protocolo)**. El conector ZTNA determina la accesibilidad de la aplicación mediante la realización de un ping tcp desde el puerto de sondeo a la dirección IP resuelta del FQDN. Si el ping se realiza correctamente, se considera que la aplicación está **Up (Activa)**.

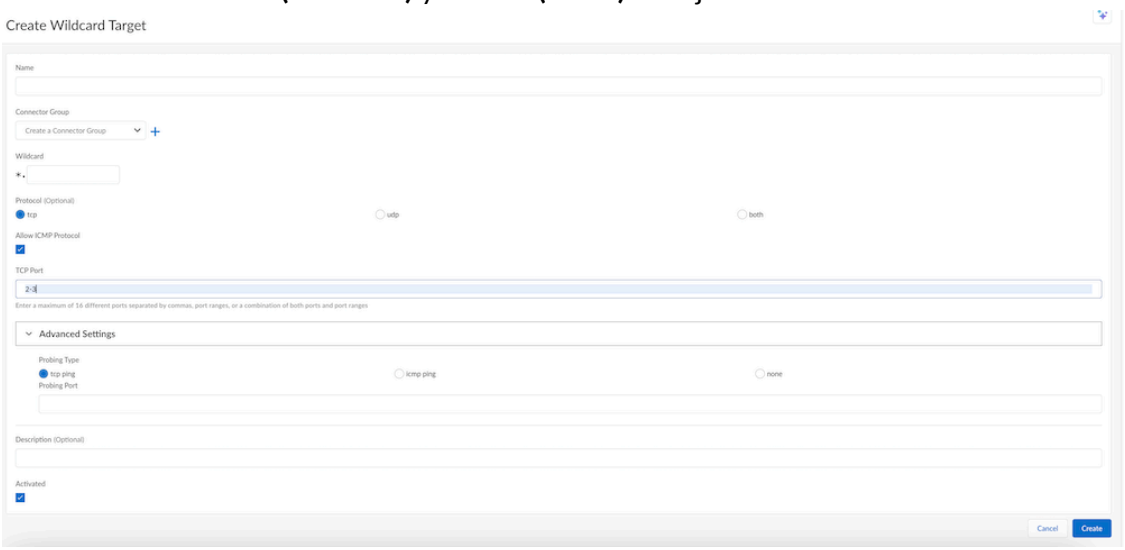
   También puede editar el puerto de sondeo, que ha añadido durante la incorporación de la aplicación. Cuando el puerto de sondeo se actualiza, el conector ZTNA inicia la aplicación de sondeo tcp en el puerto actualizado y el estado de la aplicación se actualiza en consecuencia.

   Si selecciona **icmp ping (ping icmp)**, el conector ZTNA realiza un ping ICMP a la dirección IP resuelta del FQDN. Si se recibe una respuesta al ping ICMP, se considera que la aplicación **UP (Activa)**.

   Si selecciona **none (ninguno)**, no se realiza ningún sondeo y la aplicación siempre se marca como **Up (Activa)**.

 ©2025 Palo Alto Networks, Inc.

9. Seleccione **Activated (Activado)** y **Create (Crear)** el objetivo.



- **FQDN Targets (Destinos FQDN)**: para crear un destino para un único FQDN, cree un destino FQDN.

  A partir de Prisma Access 5.0, para los grupos de conectores que tienen una versión 5.0 o superior del conector ZTNA, si un FQDN de aplicación se resuelve en varias direcciones IP privadas, el conector ZTNA realiza un sondeo de aplicación para determinar el estado de todas las direcciones IP resueltas y equilibra la carga del acceso FQDN a varias direcciones IP resueltas que tienen un estado de aplicación Activo.

  Para crear un destino FQDN, vaya a **FQDN Targets (Destinos de FQDN)** y **Create FQDN Target (Crear un destino de FQDN)**. Se crea un destino de FQDN de la misma manera que se crea un comodín de FQDN, sustituyendo el comodín de FQDN por un único FQDN.

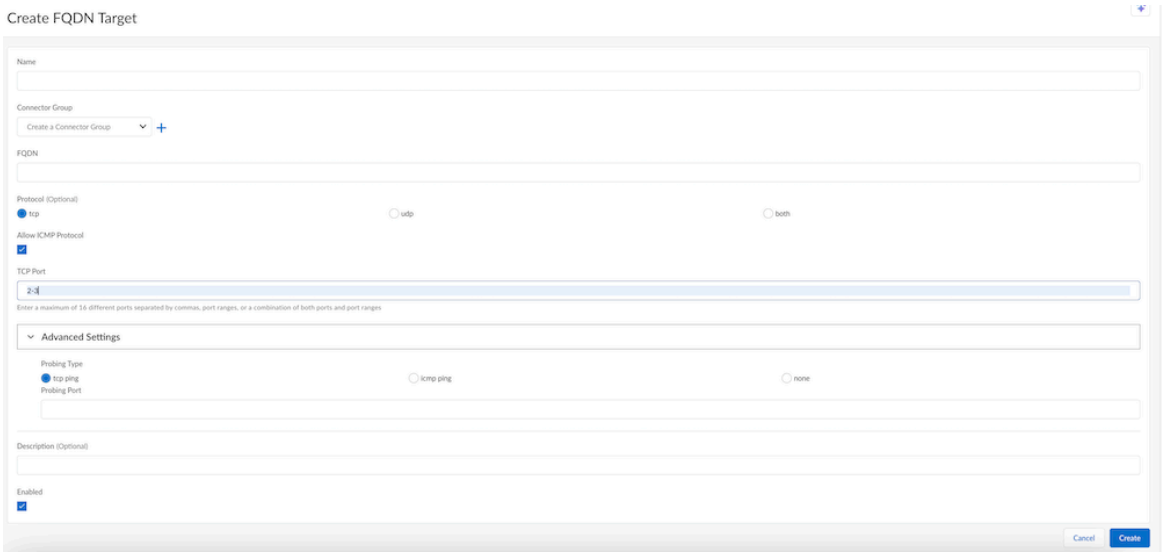
  A partir de Prisma Access 5.0.1, puede seleccionar varios grupos de conectores por destino de FQDN, así como destinos comodín, hasta un máximo de cuatro grupos de conectores por FQDN u destinos comodín. Utilice las directrices al configurar varios grupos de conectores por destino.

  Las aplicaciones que se detectan como resultado de un destino comodín también se muestran aquí. Cuando los usuarios acceden a sitios que coinciden con el comodín, esas aplicaciones se incorporan automáticamente para acceder desde ZTNA Connector para sus usuarios móviles y usuarios de red remotos. Por ejemplo, dado un comodín de *.example.com, cuando los usuarios acceden a la aplicación en app1.example.com, el Conector ZTNA añade automáticamente esa aplicación a la lista de destinos de FQDN.

  Una vez que se detecta una aplicación FQDN a partir de un destino comodín primario, los cambios en el destino comodín no se actualizan en la aplicación detectada. Además, el mismo FQDN detectado no se vuelve a detectar. Si es necesario actualizar las

 ©2025 Palo Alto Networks, Inc.

características de la aplicación FQDN detectada, realice una actualización manual de la aplicación detectada mediante estos pasos.



- **IP Subnet (Subred IP)**: cree un destino basado en subred IP para buscar aplicaciones basadas en subredes IP en lugar de FQDN.

  1. Vaya a **IP Subnets (Subredes IP)** y **Create Subnet Rule (Crear regla de subred)**.
  2. Introduzca un **Name (Nombre)** único para el objetivo.
  3. Introduzca el **Connector Group (Grupo de conectores)** para asociarlo con el objetivo.

     El Grupo debe ser un tipo de **IP Subnet (Subred IP)**.
  4. Especifique las **IP Subsets (Subredes IP)** del centro de datos al que el conector del grupo proporciona acceso de enrutamiento IP.

     Todos los conectores del grupo proporcionan acceso de enrutamiento a las subredes IP especificadas. Puede seleccionar una sola dirección IP en forma de 10.1.1.1/32,

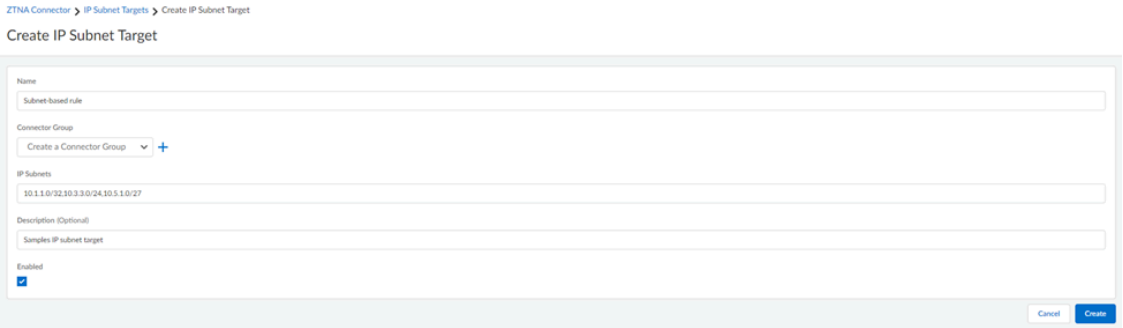
 ©2025 Palo Alto Networks, Inc.

una sola subred o varias subredes separadas por comas. Introduzca un máximo de 16 subredes.

La subred IP debe ser enrutable dentro del tejido IP del inquilino y las subredes IP no pueden superponerse con ninguna otra subred IP del inquilino, entre las que se incluyen:

- Otras subredes IP enrutables, incluidas las rutas estáticas configuradas por el usuario en Panorama, las rutas anunciadas desde la sucursal a la red remota o las rutas anunciadas desde el centro de datos a la conexión de servicio.
- Subredes IP de aplicación FQDN ZTNA
- Subredes IP del conector ZTNA
- Direcciones IP de subred de infraestructura
- Usuarios móviles: grupos de direcciones IP de GlobalProtect

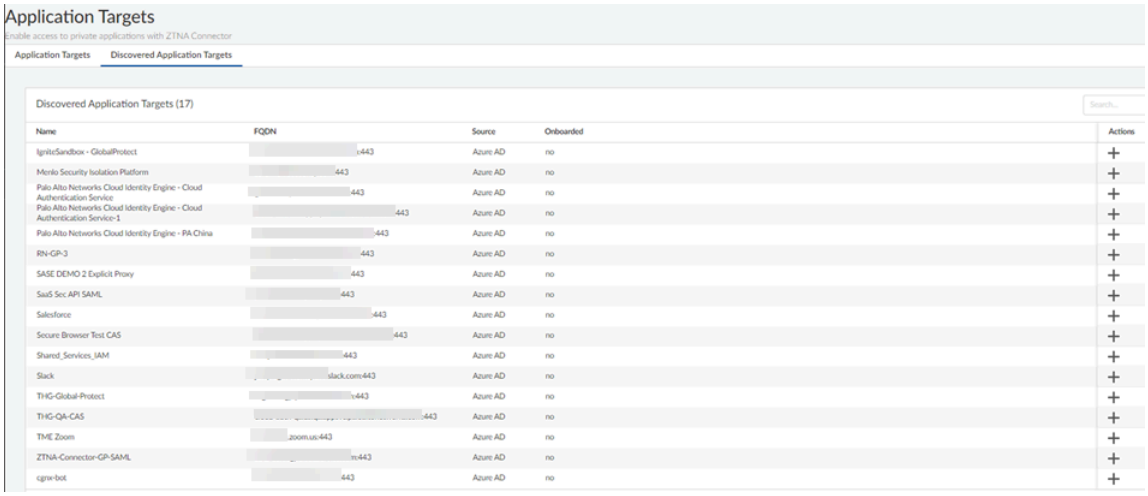
5. Seleccione **Activated (Activado)** y **Create (Crear)** el objetivo.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Añada las aplicaciones detectadas automáticamente por el conector ZTNA al grupo de conectores.

1. Configurar el descubrimiento automático de aplicaciones mediante Cloud Identity Engine
2. Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **Discovered Application Targets (Objetivos de aplicaciones descubiertos)**.



3. Haga clic en + en **Actions (Acciones)** para añadir la aplicación a un grupo de conectores.
4. Dé a la aplicación un **Name (Nombre)** único.
5. Seleccione la opción **ZTNA Connector Group (Grupo de conectores ZTNA)** para asociarlo con la aplicación.
6. Introduzca el **Probing Type (Tipo de sondeo)** [**Ping TCP**, **Ping ICMP**o **none (ninguno)**].
   - Si selecciona **ping tcp**, también seleccione un **probing port (puerto de sondeo)**. El puerto no tiene que estar en el rango de puertos que introdujo en el área **port (puerto)** y **protocol (protocolo)**. Si selecciona **tcp ping (ping tcp)** para el tipo de sondeo, Palo Alto Networks recomienda que utilice este mismo puerto para el **probing port (puerto de sondeo)**.

     El conector ZTNA determina la accesibilidad de la aplicación mediante la realización de un ping tcp desde el puerto de sondeo a la dirección IP resuelta del FQDN. Si el ping se realiza correctamente, se considera que la aplicación está **Up (Activa)**.
   - También puede editar el puerto de sondeo, que ha añadido durante la incorporación de la aplicación. Cuando se actualiza el puerto de sondeo, el conector ZTNA inicia la aplicación de sondeo tcp en el puerto actualizado y el estado de la aplicación se actualiza en consecuencia.
   - Si selecciona **icmp ping (ping icmp)**, el conector ZTNA realiza un ping ICMP al FQDN. Si se recibe una respuesta al ping ICMP, el conector ZTNA establece el estado de la aplicación como **UP (Activo)**.
   - Si selecciona **none (ninguno)**, no se realiza ningún sondeo y la aplicación siempre se marca como **Up (Activa)**.
7. Seleccione **Enabled (Habilitado)**.
8. **Create (Crear)** el objetivo de la aplicación.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Cree reglas de política de seguridad para permitir que los usuarios accedan a las aplicaciones en los conectores.

STEP 10 | (Opcional) Vea y supervise los conectores ZTNA para ver el estado y el rendimiento de sus grupos de conectores y conectores ZTNA.

STEP 11 | (Opcional) Si tiene problemas para acceder a aplicaciones privadas mediante el conector ZTNA, utilice las herramientas de diagnóstico ping, traceroute y nslookup para comprobar la accesibilidad de la aplicación.

Actualizar los conectores ZTNA

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Para mantener los ZTNA Connectors actualizados, puede actualizar su versión de software. También puede que se requiera actualizar sus conectores para soportar una nueva característica o funcionalidad.

Cuando se lanza una nueva versión de ZTNA Connector, se comprueban los conectores en su implementación y, si la versión lanzada es más reciente que la versión existente, o si todos los conectores en el grupo no están en la misma versión, los iconos en el área del grupo de conectores muestran que hay una actualización disponible. Si elige actualizar los conectores, se le da la opción de actualizar todo el grupo junto. Actualizar un grupo actualiza automáticamente todos los conectores en ese grupo en paralelo. No puede actualizar conectores individuales.

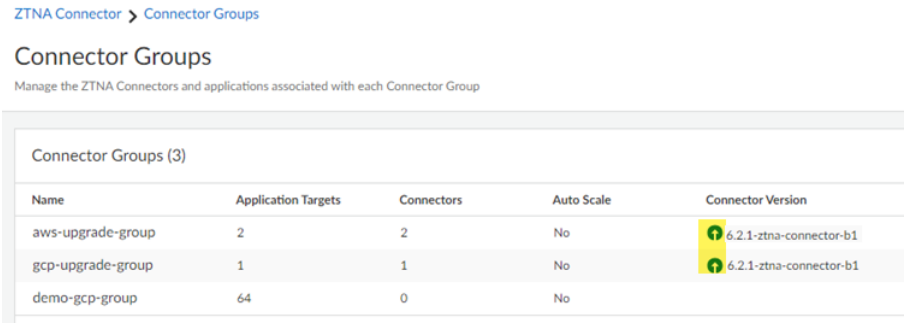
 ©2025 Palo Alto Networks, Inc.

ZTNA Connector tarda aproximadamente de 8 a 10 minutos en actualizarse y el conector se reinicia durante este proceso. Palo Alto Networks recomienda que programe una actualización del conector durante un tiempo de inactividad o una interrupción programada de la red.

STEP 1 | Vaya a **ZTNA Connector** > **Connector Groups (Grupos de conectores)**. Las flechas verdes indican que hay una actualización disponible.

Solo puede actualizar a la última versión de imagen que esté disponible para el inquilino.

STEP 2 | Haga clic en la flecha verde junto al grupo de conectores.

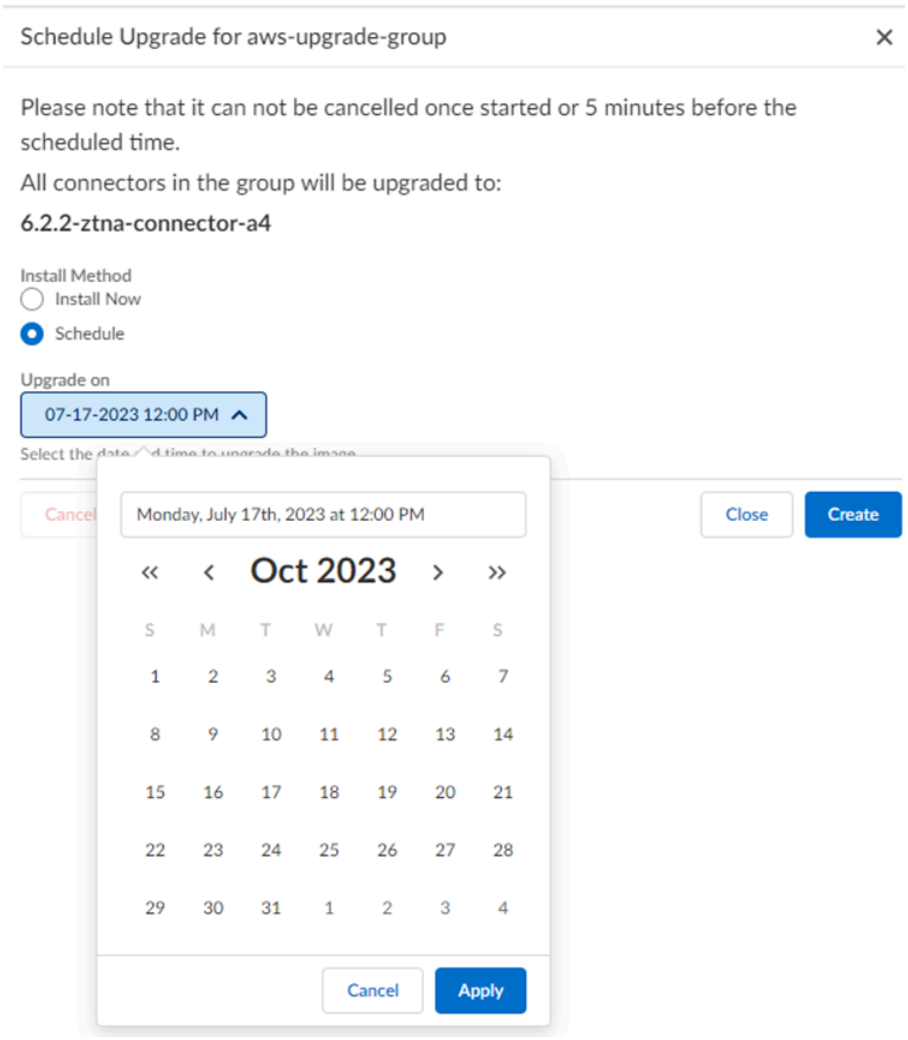


STEP 3 | Seleccione **Install Now (Instalar ahora)** para actualizar el grupo de conectores ahora, o seleccione **Schedule (Programar)** y proporcione una hora y fecha para la actualización. La

 ©2025 Palo Alto Networks, Inc.

hora mostrada es la zona horaria local para el administrador que utiliza la interfaz de usuario ZTNA. .

Puede **Cancel Scheduled Upgrade (Cancelar la actualización programada)** hasta cinco minutos antes de que comience.



STEP 4 | Verifique el estado de los conectores consultando el icono en **Connector Version (Versión del conector)**.

Icono	Descripción
	La actualización está disponible.
	La actualización se ha programado.

 ©2025 Palo Alto Networks, Inc.

Icono	Descripción
	La actualización ha comenzado y está en curso.
Sin icono (Solo se muestra la versión del conector) 6.1.1-ztna-connector-a8	La actualización se realizó correctamente
	No todos los conectores se actualizados.
	Error de actualización.

Herramientas de diagnóstico de ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

 ©2025 Palo Alto Networks, Inc.

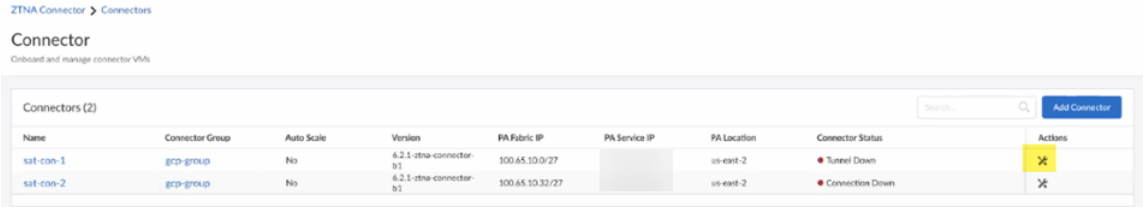
Si tiene problemas para acceder a aplicaciones privadas mediante ZTNA Connector, puede ejecutar pruebas desde la interfaz de usuario de ZTNA Connector para ayudarle a encontrar el problema, utilizando las siguientes herramientas de red:

- ping
- Ping TCP
- traceroute
- nslookup
- Descripción general de volcado
- También puede tomar capturas de paquetes para ayudar a determinar la causa de cualquier problema con ZTNA Connector.

Asegúrese de que ICMP esté permitido en su red antes de utilizar las herramientas ping y traceroute. Algunos entornos de nube tienen ICMP deshabilitado por cuestiones de seguridad y estas herramientas no muestran ninguna actividad.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**.

STEP 2 | Seleccione **Actions (Acciones)** > **Diagnostics (Diagnóstico)** para el conector.



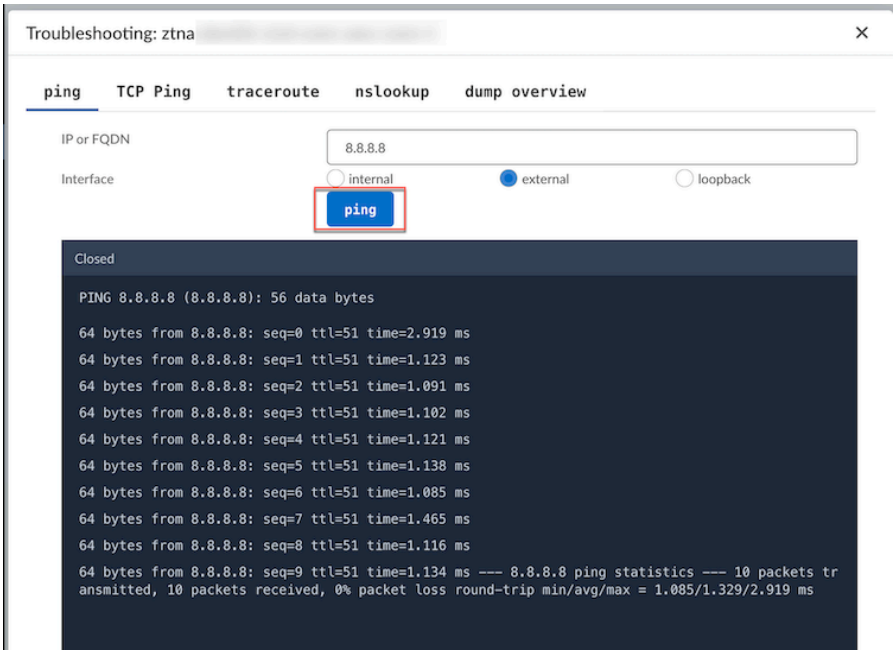
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Ejecute las herramientas de diagnóstico ping, TCP Ping, traceroute o nslookup.

- **ping**:
  1. Seleccione la **IP o FQDN** de la aplicación a la que intenta acceder.
  2. Seleccione la **interface (interfaz)** desde la que está probando el ping.

     Si ha configurado su VM con una implementación de dos interfaces, seleccione **internal (interna)** para verificar el lado LAN (puerto 2) de la VM y seleccione **external (externo)** para verificar el lado WAN (puerto 1).

     Para una implementación de un solo brazo, elija **internal (interno)** o **external (externo)**, ya que tanto el lado WAN como el lado LAN se asignan al puerto 1.
  3. Seleccione **ping**.



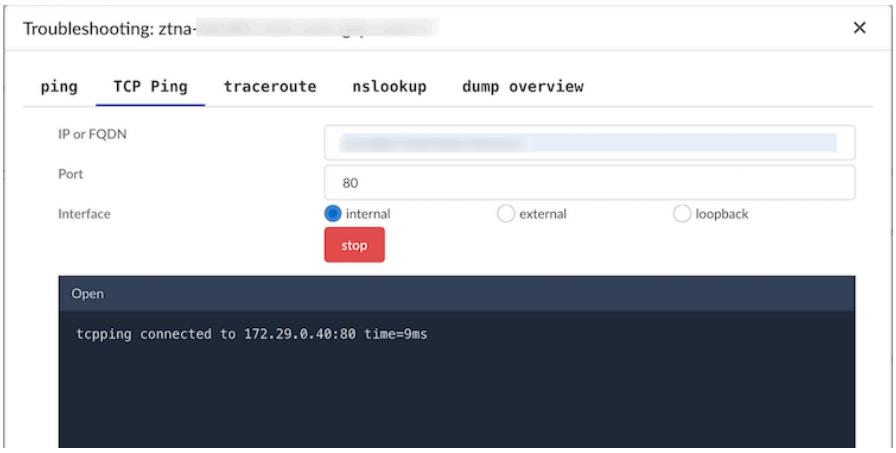
     Se muestra el resultado del ping.
  4. Para finalizar la prueba, **Stop (Detener)**.
- **Ping TCP (TCP Ping)**:

  *Actualice el conector a la versión ZTNA Connector 6.2.5-b1. Si el conector no está actualizado con esta versión, entonces la interfaz de usuario de Strata Cloud Manager no ofrecerá **TCP Ping (Ping TCP)** como herramienta de diagnóstico.*

  1. Seleccione la **IP o FQDN** de la aplicación a la que intenta acceder.
  2. Seleccione la **interface (interfaz)** desde la que está probando el ping.

     Si ha configurado su VM con una implementación de dos interfaces, seleccione **internal (interna)** para verificar el lado LAN (puerto 2) de la VM y seleccione **external (externo)** para verificar el lado WAN (puerto 1).
  3. Seleccione **TCP Ping (Ping TCP)**.

 ©2025 Palo Alto Networks, Inc.

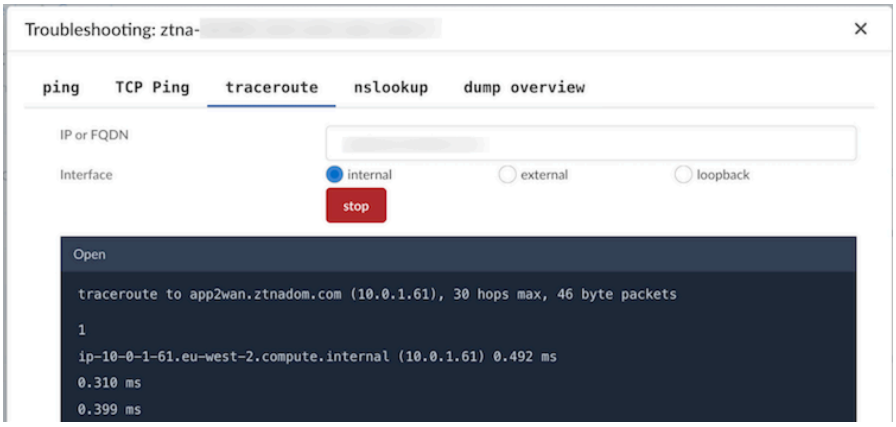


4. Para finalizar la prueba, **Stop (Detener)**.

- **traceroute**:

1. Seleccione la **IP o FQDN** de la aplicación a la que intenta acceder.
2. Seleccione la **interface (interfaz)** desde la que está probando el ping.

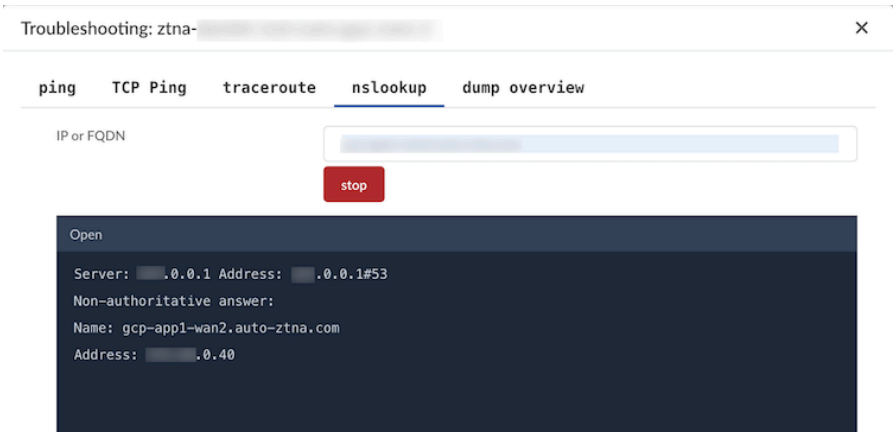
   Si ha configurado su VM con una implementación de dos interfaces, seleccione **internal (interna)** para verificar el lado LAN (puerto 2) de la VM y seleccione **external (externo)** para verificar el lado WAN (puerto 1).
3. Seleccione **traceroute**.
4. Para finalizar la prueba, **Stop (Detener)**.



- **nslookup**:

1. Seleccione la **IP o FQDN** de la aplicación a la que intenta acceder.
2. Seleccione **nslookup**.
3. Para finalizar la prueba, **Stop (Detener)**.

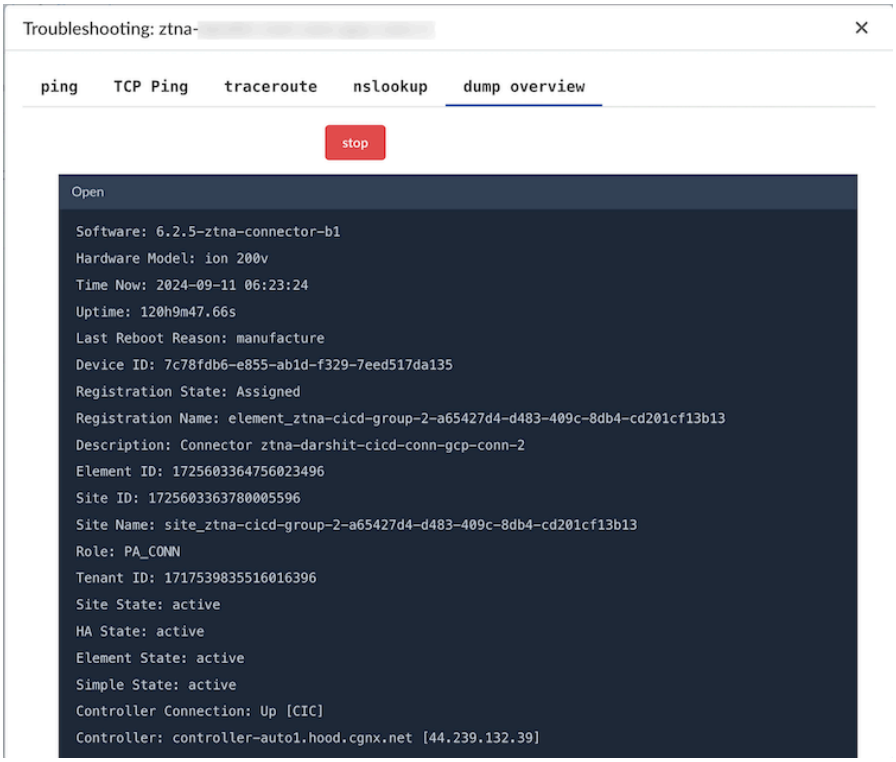
 ©2025 Palo Alto Networks, Inc.



- **Descripción general de volcado**

  1. Haga clic en **Start (Iniciar)** para descargar un volcado del sistema y haga clic en **Stop (Detener)** para detenerlo.

     La descripción general del volcado proporciona la versión del software, el estado de la interfaz y la conexión, y la información de identificación del conector necesaria para la resolución de problemas de PANW.



Realización de capturas de paquetes

Si necesita capturas de paquetes para solucionar problemas a nivel de red, puede realizar capturas de paquetes que capturen datos de red de conectores específicos. También puede capturar paquetes basados en direcciones IP o protocolos específicos (por ejemplo, TCP).

Tomar capturas de paquetes es útil en los siguientes casos de uso:

 ©2025 Palo Alto Networks, Inc.

- Si el túnel no por llegar. Capturar la negociación IKE entre el conector y ZTT ayudaría a determinar el problema. En este caso, seleccione la interfaz de **internet** y utilice la dirección IP de la conexión de servicio como interfaz de origen o destino.
- Si su aplicación deja de funcionar, puede verificar el sondeo de las aplicaciones obteniendo un tcpdump usando la dirección IP y el puerto del servidor en la interfaz del centro de datos.
- Si el plano de datos de extremo a extremo no funciona, pero el túnel está activo y la aplicación está activa. En este caso de uso, sería beneficioso obtener un tcpdump del tráfico del usuario en el túnel IPSec destinado a la dirección IP de la estructura de la aplicación.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**.

STEP 2 | Seleccione **packet capture (captura de paquetes)** (la lupa) para el conector cuyo problema desea solucionar.



STEP 3 | Seleccione la interfaz donde se capturarán los paquetes [**internal (interna)**, **external (externa)**o **Tunnel (túnel)**].

STEP 4 | (Opcional) Especifique la dirección **IPv4 de origen o destino** desde la que se capturan los paquetes.

Si especifica esta opción, solo se capturarán los paquetes de esta dirección IP.

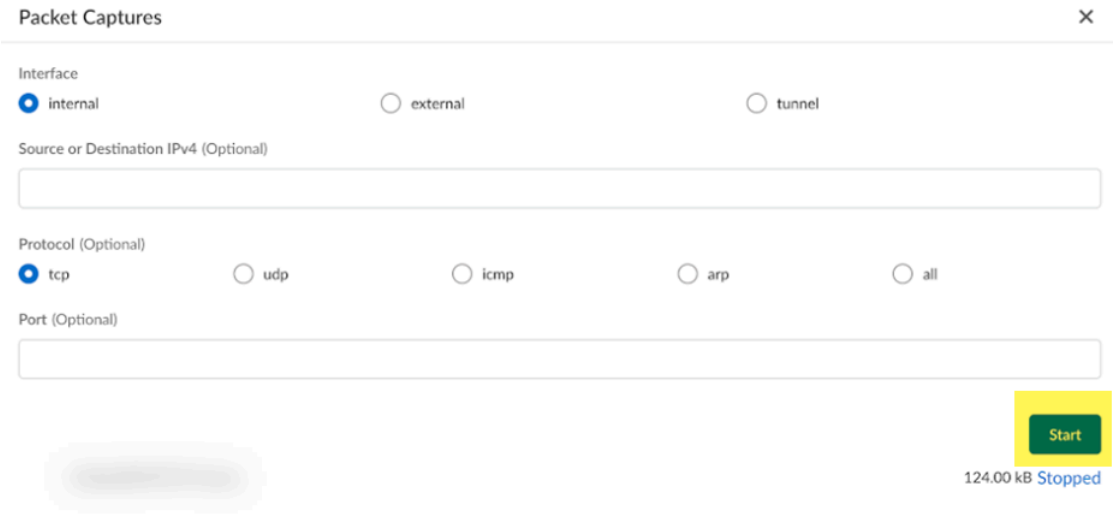
STEP 5 | (Opcional) Seleccione el tipo de paquetes a capturar.

Puede seleccionar paquetes de un protocolo específico para capturar (**tcp**, **udp**, **icmp**o **arp**) o seleccionar **all (todos)** para capturar todos los paquetes.

STEP 6 | (Opcional) Seleccione un **Port (Puerto)** desde el cual se capturarán los paquetes.

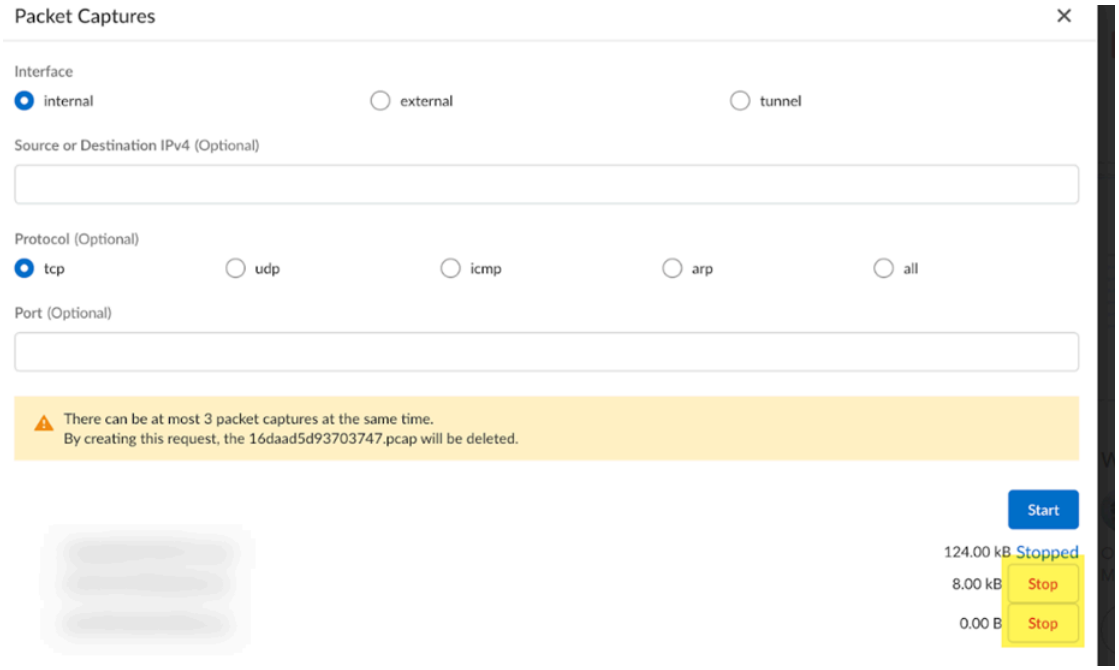
Si especifica esta opción, solo se capturarán los paquetes de este puerto.

STEP 7 | **Start (Iniciar)** las capturas de paquetes.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Para detener la captura de paquetes, haga clic en **Stop (Detener)**.



- El tamaño máximo de archivo para capturas de paquetes es de 5 MB. Si no detiene las capturas antes de alcanzar el tamaño máximo, el archivo se sobrescribirá.
- Se permite un máximo de tres capturas de paquetes en un conector al mismo tiempo. Si se inicia una cuarta sesión, se finaliza la primera sesión en ejecución.

Recopilar archivos de asistencia técnica

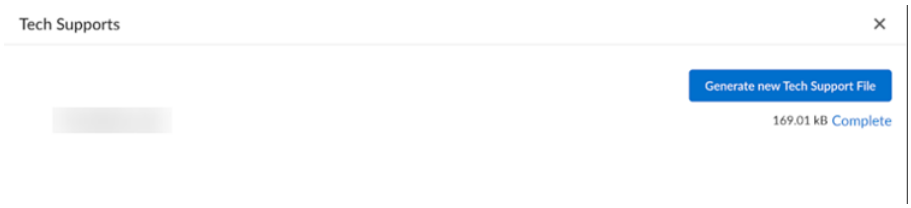
El archivo de soporte técnico contiene la configuración de su dispositivo, información del sistema y algunos logs (no tráficos). Palo Alto Networks puede solicitarle que cargue un archivo de asistencia técnica para ayudar a solucionar problemas con ZTNA Connector.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**.

STEP 2 | Seleccione **tech support (asistencia técnica)** (la mano) para el conector cuyo problema desea solucionar.



STEP 3 | **Generate new Tech Support File (Generar nuevo archivo de asistencia técnica)**



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Complete (Completar)** para descargar el archivo de asistencia técnica localmente.

 ©2025 Palo Alto Networks, Inc.

Eliminar Bloques IP del conector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Usted Habilitar el conector ZTNA y añade los bloques de IP de conector necesarios que Prisma Access utilizará internamente para enrutar el tráfico entre usuarios móviles, redes remotas y las máquinas virtuales del conector en sus centros de datos. Anteriormente, no era posible realizar ningún cambio en los bloques IP del conector después de su creación. Sin embargo, ahora puede eliminar o actualizar los **bloques de IP del conector**. Siga el procedimiento mencionado para eliminar o actualizar los bloques.

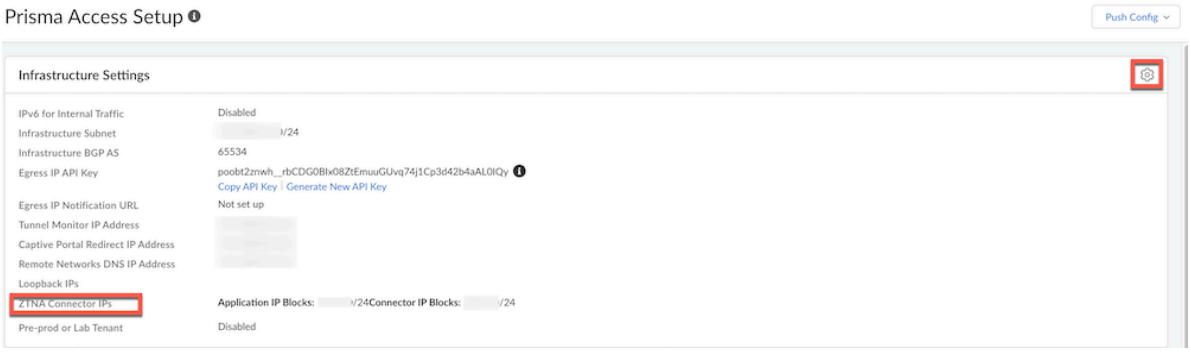
- Panorama
- Strata Cloud Manager

Eliminar bloques de IP del conector (Gestionado en la nube)

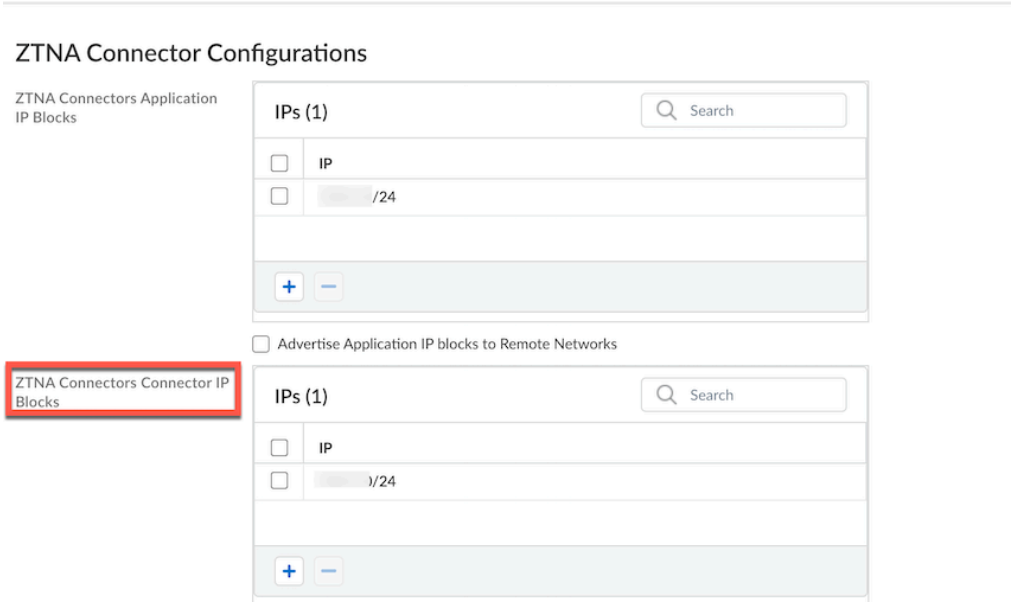
Complete el siguiente procedimiento para eliminar los bloques de IP del conector.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)** y haga clic en el engranaje para editar la **Settings (Configuración)**.



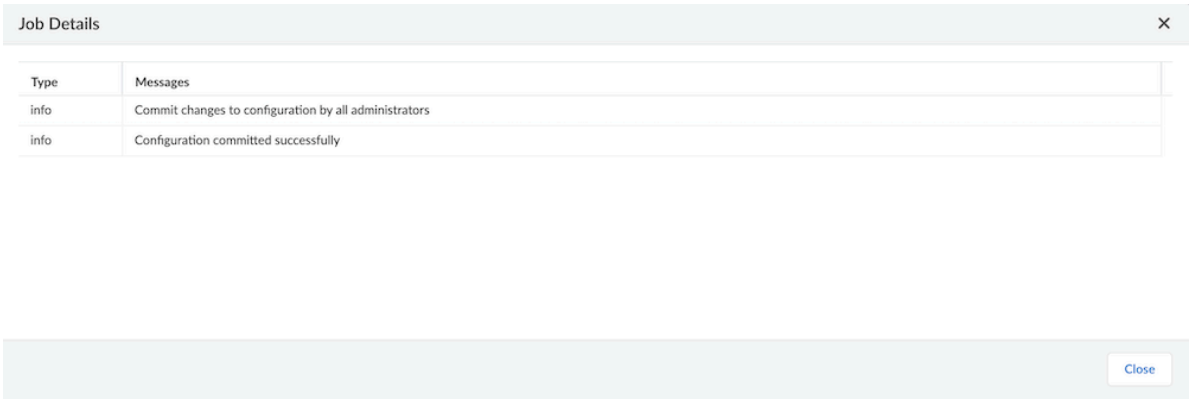
STEP 2 | En **ZTNA Connector Configurations (Configuraciones de ZTNA Connector)** > **ZTNA Connectors Connector IP Blocks (Bloques IP de conectores de ZTNA Connectors)**, seleccione la casilla de verificación junto al bloque del conector que desea eliminar y haga clic en **Save (Guardar)**.



 ©2025 Palo Alto Networks, Inc.

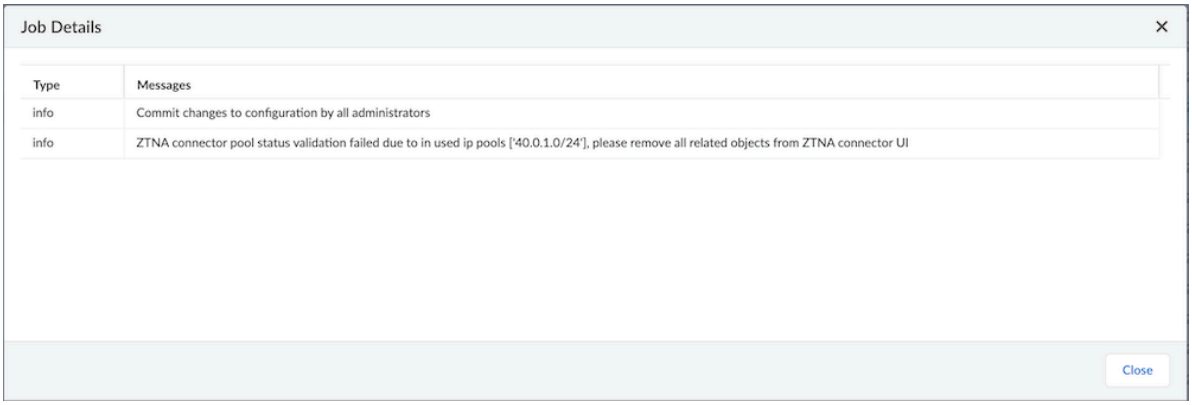
STEP 3 | Haga clic en **Commit (Confirmar)** y enviar los cambios de configuración.

Aparece un mensaje después de que la confirmación se pasa.



Si ha creado algún objeto del ZTNA Connector, como conectores, aplicaciones, comodines y grupos de conectores, e intenta eliminar el **Connector IP Block (Bloque IP del conector)** sin eliminar primero los objetos del ZTNA Connector, la confirmación y el envío fallarán.

En este caso, elimine los objetos de conector ZTNA Connector, elimine el **Connector IP Block (Bloque de IP del conector)** requerido y entonces seleccione **Commit (Confirmar)**. La primera confirmación falla, pero la segunda pasa.

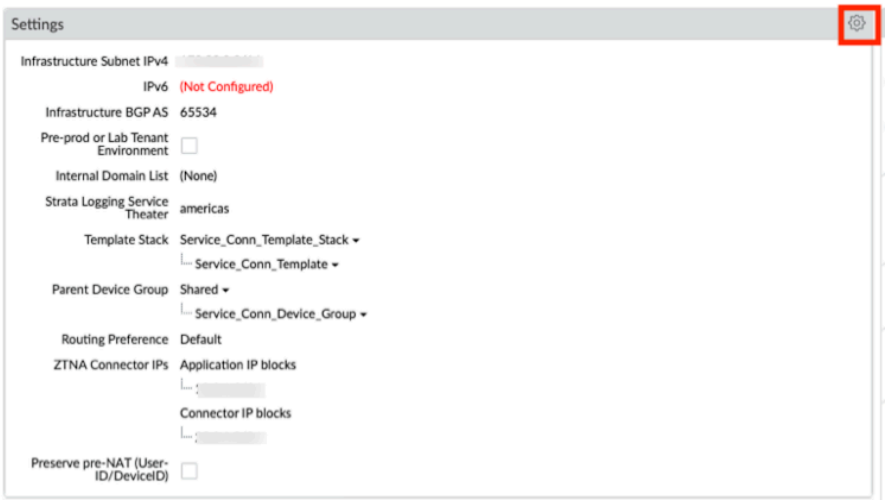


Eliminar bloques IP del conector (Panorama)

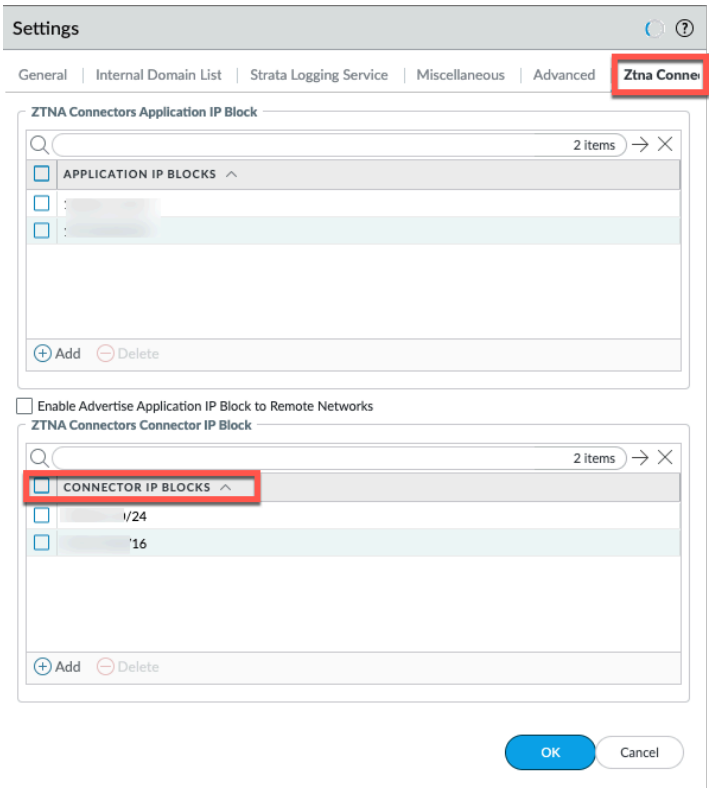
Complete el siguiente procedimiento para eliminar los bloques de IP del conector.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y haga clic en el engranaje para editar la **Settings (Configuración)**.



STEP 2 | Habilitar **ZTNA Connector**

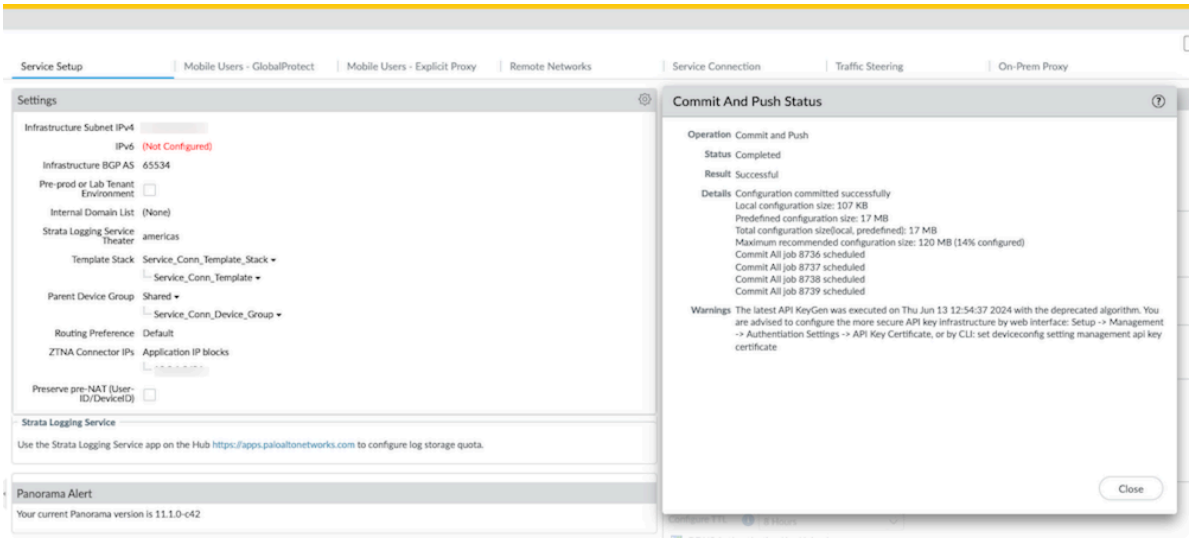


STEP 3 | Seleccione la casilla de verificación situada junto al bloque de conectores que desea eliminar y haga clic en **OK (Aceptar)** para guardar la configuración.

 ©2025 Palo Alto Networks, Inc.

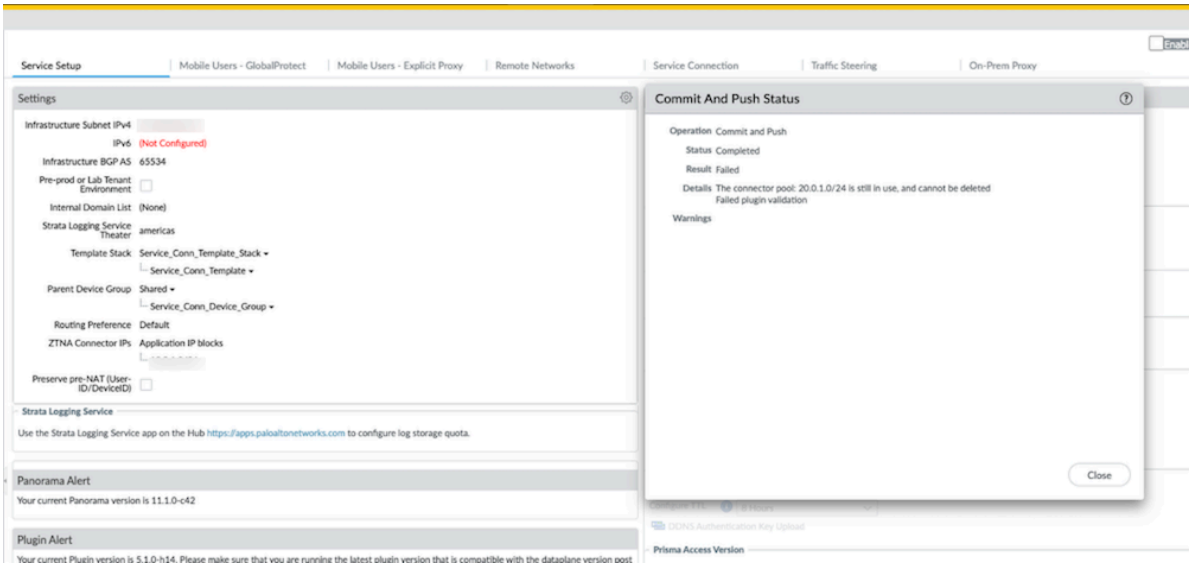
STEP 4 | Haga clic en **Commit (Confirmar)** para enviar el cambio de configuración.

Un mensaje aparece después de pasar la confirmación.



Si ha creado cualquier objeto de ZTNA Connector, como conectores, aplicaciones, comodines y grupos de conectores, e intenta eliminar el **Connector IP Block (Bloque IP del conector)** sin eliminar los objetos de ZTNA Connector, se produce un error en la confirmación y la inserción.

En este caso, elimine los objetos del conector ZTNA Connector, elimine el **Connector IP Block (Bloque de IP del conector)** requerido y entonces seleccione **Commit (Confirmar)** para confirmar y enviar dos veces. Se produce un error en la primera confirmación, pero se aprueba la segunda.



 ©2025 Palo Alto Networks, Inc.

Configurar el descubrimiento automático de aplicaciones mediante Cloud Identity Engine

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Para que ZTNA Connector pueda descubrir automáticamente las aplicaciones definidas en Azure Active Directory o Okta Directory, debe configurar lo siguiente:

❑ Active Cloud Identity Engine en el hub y cree su primer inquilino.

Debe seleccionar **Collect enterprise applications (Recopilar aplicaciones empresariales)** cuando configure su directorio basado en la nube en Azure u Okta.

❑ Seleccione el tipo de directorio al que desea que acceda Cloud Identity Engine.

❑ Configure un directorio basado en la nube, como Azure Active Directory (Azure AD) o Okta Directory para comunicarse con Cloud Identity Engine.

Los siguientes IdP son compatibles para su uso con el descubrimiento de aplicaciones:

- Azure AD
- Okta

 ©2025 Palo Alto Networks, Inc.

Detección de objetivos de aplicaciones privadas

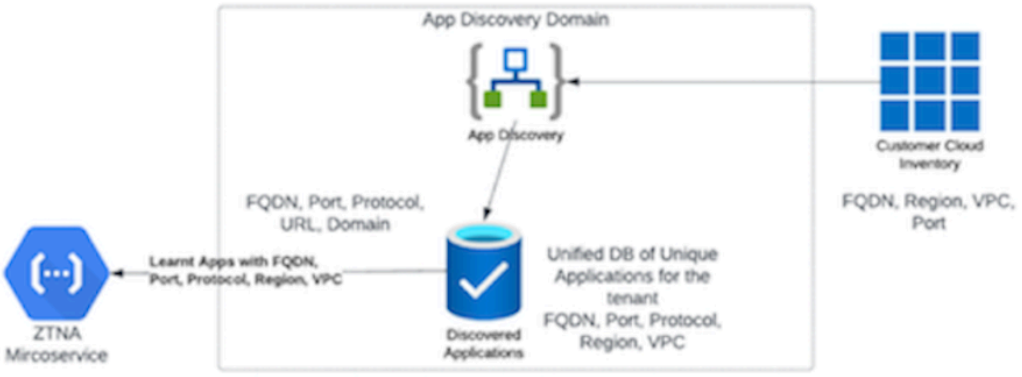
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

En una infraestructura de red moderna, se implementan miles de aplicaciones privadas en las instalaciones y en centros de datos multinube. Los equipos de redes no son conscientes de las aplicaciones que se ejecutan en su red o dentro de una subred concreta de la red, lo que provoca una falta de visibilidad de las aplicaciones.

Para proporcionar un acceso seguro a las aplicaciones, debe escribir manualmente el FQDN, el puerto y la aplicación, y tener en cuenta la dependencia que esta aplicación tiene de las demás aplicaciones.

La detección de objetivos de aplicaciones privadas proporciona una forma de detectar las aplicaciones alojadas en el entorno de la nube y permite que esas aplicaciones se incorporen en la solución ZTNA Connector. También se conecta a la red del proveedor de la nube, realiza la detección y la almacena en la base de datos. También proporciona las API a los diferentes servicios para obtener las aplicaciones detectadas. Si el usuario solo tiene una conexión de servicio en lugar de un ZTNA Connector, solo se detectan los destinos de la aplicación.

 ©2025 Palo Alto Networks, Inc.



La detección de objetivos de aplicaciones privadas identifica:

- FQDN
- Puerto de la aplicación
- Protocolo de aplicación

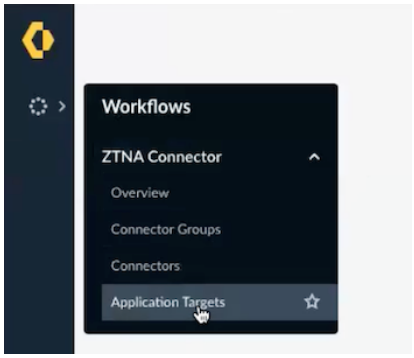
Asegúrese de activar cloud identity engine (CIE) antes de habilitar la función de detección de aplicaciones privadas.

Complete los siguientes pasos para añadir una cuenta en la nube, una función de IAM en AWS y descubra las aplicaciones de destino.

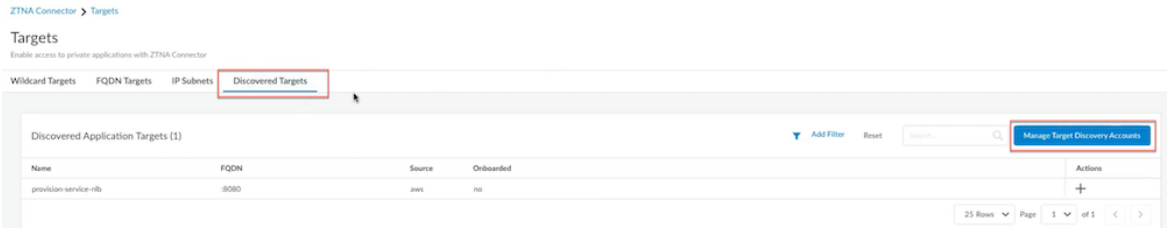
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenga la plantilla de CloudFormation (CFT) para añadir una cuenta en la nube.

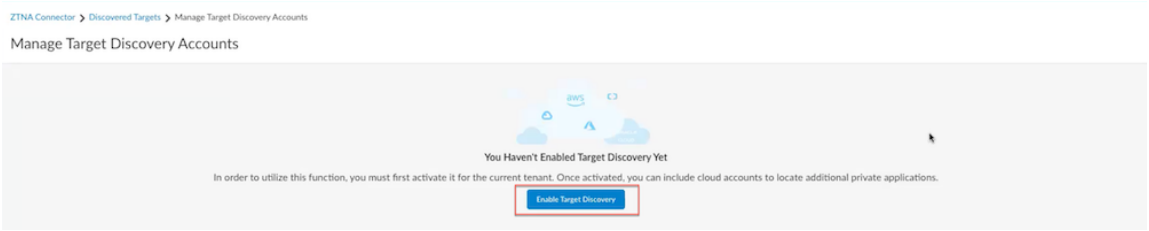
1. Vaya a **Application Targets (Objetivos de la aplicación)**[**Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)**].



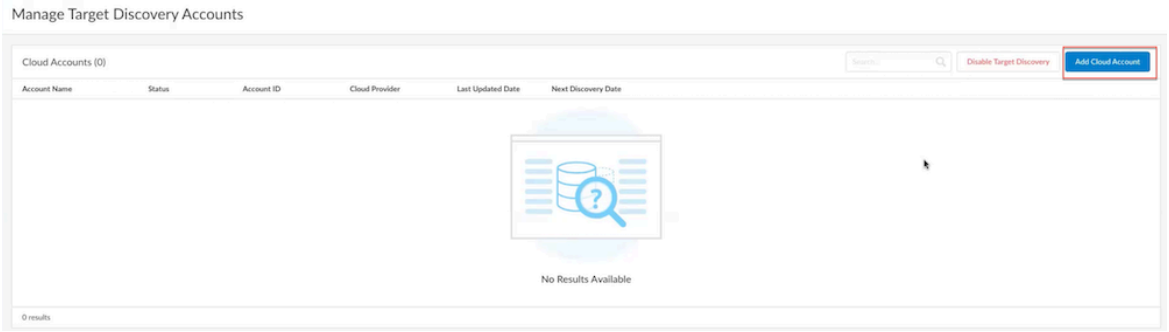
2. En la página **Application Targets (Objetivos de la aplicación)**, seleccione **Discovered Targets (Objetivos detectados)** y, a continuación, seleccione **Manage Target Discovery Accounts (Gestionar cuentas de detección de objetivos)**.



3. Seleccione **Enable Target Discovery (Habilitar la detección de objetivos)**y, a continuación, seleccione **Enable (Habilitar)**.



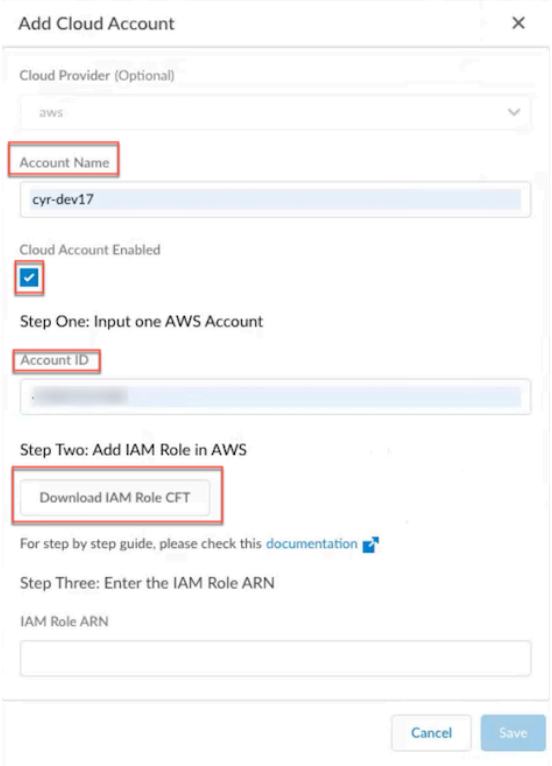
4. En la página **Manage Target Discovery Accounts (Gestionar cuentas de detección de objetivos)**, seleccione **Manage Target Discovery Accounts (Añadir cuenta en la nube)**.



5. Añada el **Account Name (Nombre de la cuenta)** y haga clic en la casilla de verificación situada en **Cloud Account Enabled (Cuenta en la nube habilitada)**. Añada el **Account**

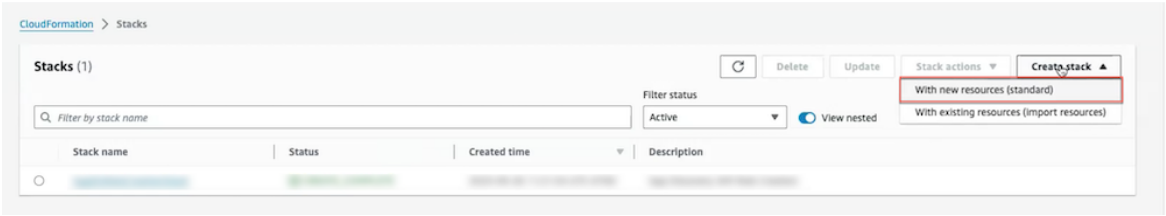
 ©2025 Palo Alto Networks, Inc.

ID (ID de cuenta) de AWS y haga clic en **Download IAM Role CFT (Descargar CFT de función de IAM)** para descargar el archivo.



STEP 2 | Cree la función de IAM en AWS.

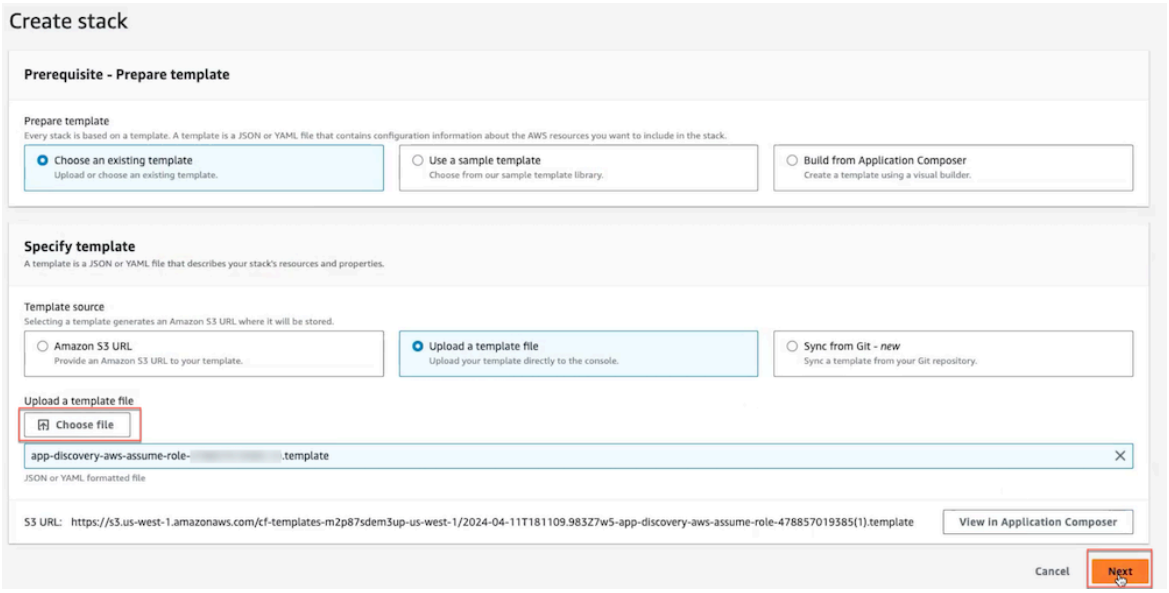
1. Vaya a la aplicación de AWS, seleccione su cuenta e **Sign in (Inicie sesión)**.
2. Vaya a **CloudFormation** > **Stacks (Pilas)** > **Create Stack (Crear pila)** > **With new resources (standard) [Con nuevos recursos (estándar)]** para crear la pila.



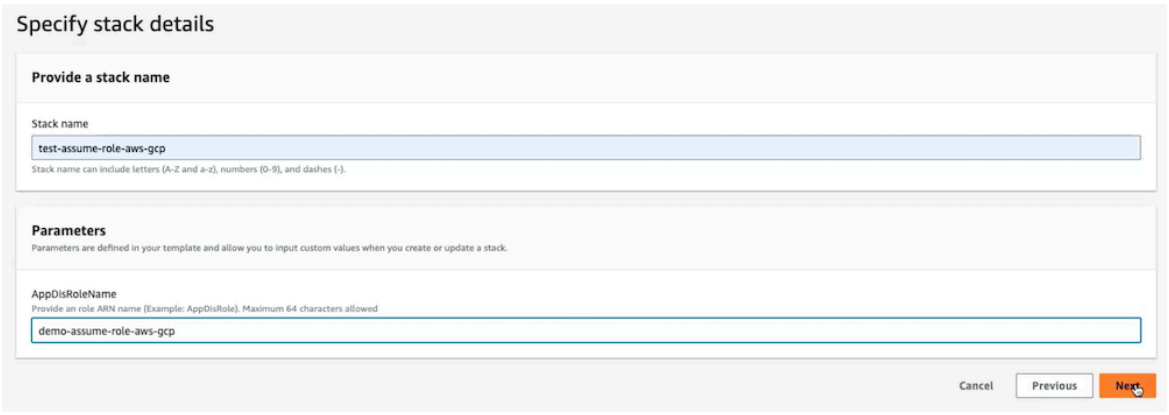
3. En la página **Create stack (Crear pila)**, en **Prerequisite-Prepare template**, seleccione **Choose an existing template (Seleccionar una plantilla existente)**. En **Specify template**

 ©2025 Palo Alto Networks, Inc.

(Especificar plantilla), seleccione **Upload a template file (Cargar un archivo de plantilla)**. Cargue el archivo descargado anteriormente en el Paso 1 y seleccione **Next (Siguiente)**.



4. Añada **Stack name (Nombre de la pila)**, **AppDisRoleName** y seleccione **Next (Siguiente)**.

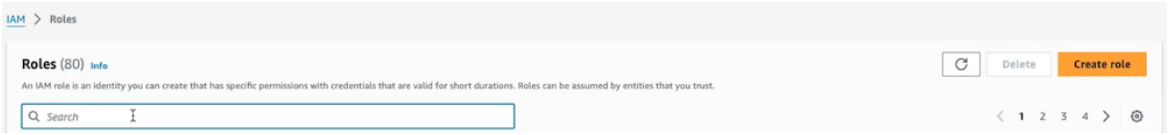


5. En la página **Configure stack options (Configurar opciones de pila)**, no realice ninguna actualización y seleccione **Next (Siguiente)**.
6. Revisar los cambios. Seleccione la casilla de verificación en **Capabilities (Capacidades)** para confirmar la creación de recursos de IAM con nombres personalizados y, a continuación, seleccione **Submit (Enviar)**.

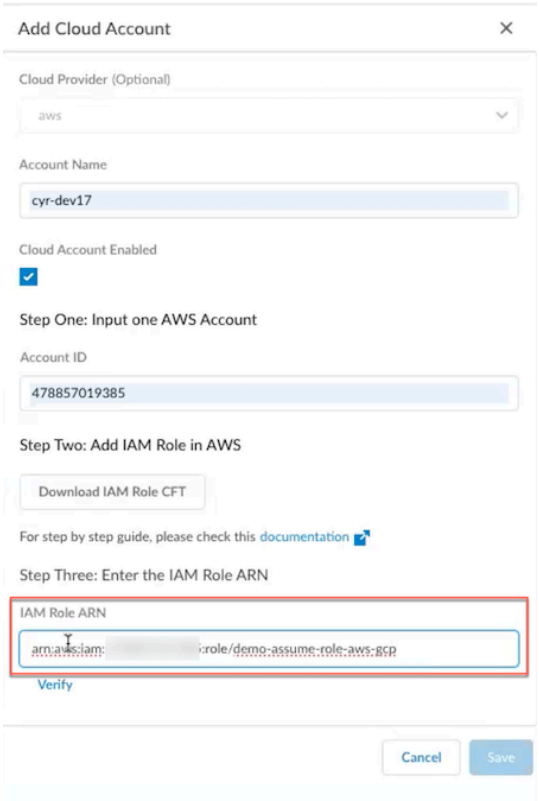


7. Vaya a **IAM** > **Roles (Funciones)** y busque el nombre de la función que definió. Seleccione el nombre de la función y copie el archivo **ARN** para la función.

 ©2025 Palo Alto Networks, Inc.



STEP 3 | Pegue el ARN en el campo de texto **IAM Role ARN (ARN de función de IAM)** y, a continuación, seleccione **Verify (Verificar)**. Cuando se verifique el ARN, seleccione **Save (Guardar)**.

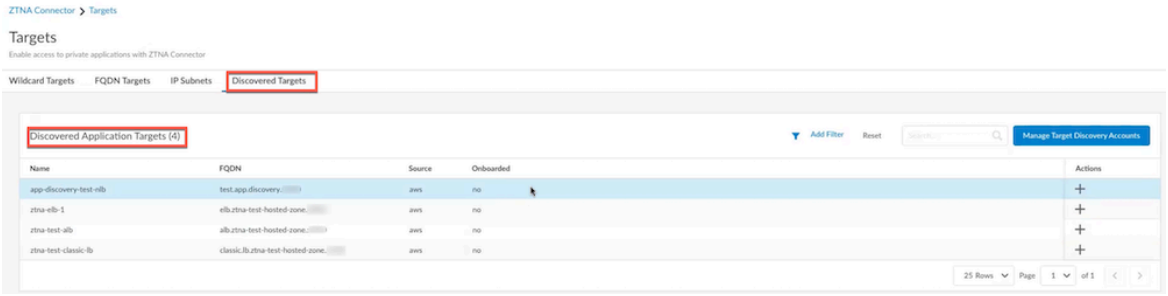


*Si añade un ARN incorrecto en el campo de texto **IAM Role ARN (ARN de función de IAM)**, se produce un error en la verificación y aparece un mensaje de error.*

Después de añadir la cuenta, puede ver el estado, el ID de la cuenta y otros detalles. El período de actualización para la detección es de 24 horas. También puede añadir varias cuentas al mismo inquilino.

©2025 Palo Alto Networks, Inc.

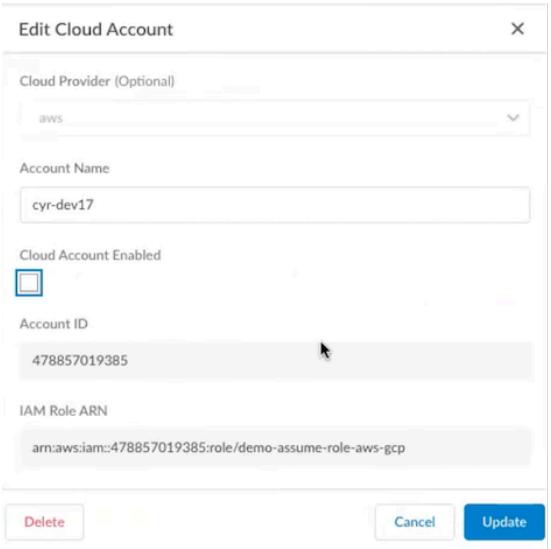
STEP 4 | Para identificar las aplicaciones detectadas, seleccione **Discovered Targets (Objetivos descubiertos)**. Puede encontrar la lista de aplicaciones identificadas en **Discovered Application Targets (Objetivos de aplicaciones detectados)**.



STEP 5 | (Opcional) Elimine la cuenta en la nube.

Para eliminar su cuenta en la nube y añadir una nueva sin deshabilitar la detección de destinos, siga este procedimiento. Sin embargo, estos pasos son obligatorios si desea deshabilitar la funcionalidad de detección de objetivos.

1. En **Manage Target Discovery Accounts (Gestionar cuentas de detección de objetivos)**, haga clic en el **Account Name (Nombre de la cuenta)** que desea eliminar.
2. Deshabilite la opción **Cloud Account Enabled (Cuenta en la nube habilitada)**y seleccione **Update (Actualizar)**. Cuando se actualice la cuenta, seleccione **Delete (Eliminar)**. La cuenta se elimina.

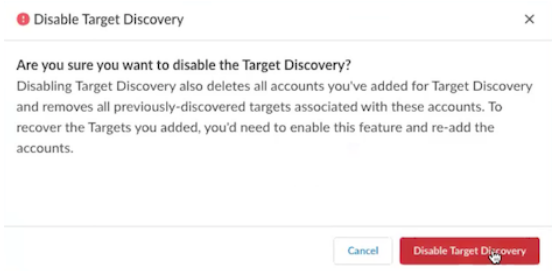


 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Deshabilite la detección de objetivos.

Asegúrese de que se hayan eliminado todas las cuentas en la nube antes de deshabilitar la detección de objetivos.

1. Seleccione **Disable Target Discovery (Deshabilitar la detección de objetivos)**y, a continuación, seleccione **Disable Target Discovery (Deshabilitar la detección de objetivos)**.



 ©2025 Palo Alto Networks, Inc.

Política de seguridad para aplicaciones habilitadas con ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

ZTNA Connector no aplica políticas; extiende sin problemas su política de seguridad de Prisma Access existente a las aplicaciones que habilita para Prisma Access. Esto significa que puede utilizar una política común en todas sus aplicaciones y centros de datos, y no necesita crear su política de seguridad por separado para las aplicaciones incorporadas a ZTNA Connector.

Sin embargo, como parte de la configuración de ZTNA Connector, debe asegurarse de que su política de seguridad:

Permite el tráfico entre Prisma Access y ZTNA Connector

Para ello, siga los Requisitos y directrices de ZTNA Connector para asegurarse de que ZTNA Connector pueda conectarse a Prisma Access.

Los usuarios pueden acceder a las aplicaciones detrás de ZTNA Connector

Para garantizar que sus usuarios puedan acceder a las aplicaciones de ZTNA Connector, siga los pasos aquí para la interfaz que esté usando para gestionar Prisma Access.

- Strata Cloud Manager

©2025 Palo Alto Networks, Inc.

- Panorama

Política de seguridad para aplicaciones habilitadas con ZTNA Connector (Strata Cloud Manager)

Después de incorporar aplicaciones a ZTNA Connector, debe configurar reglas de políticas para permitir y controlar el acceso a esas aplicaciones. El procedimiento para crear y aplicar políticas difiere según si sus aplicaciones están definidas por comodines, subredes de IPo FQDN.

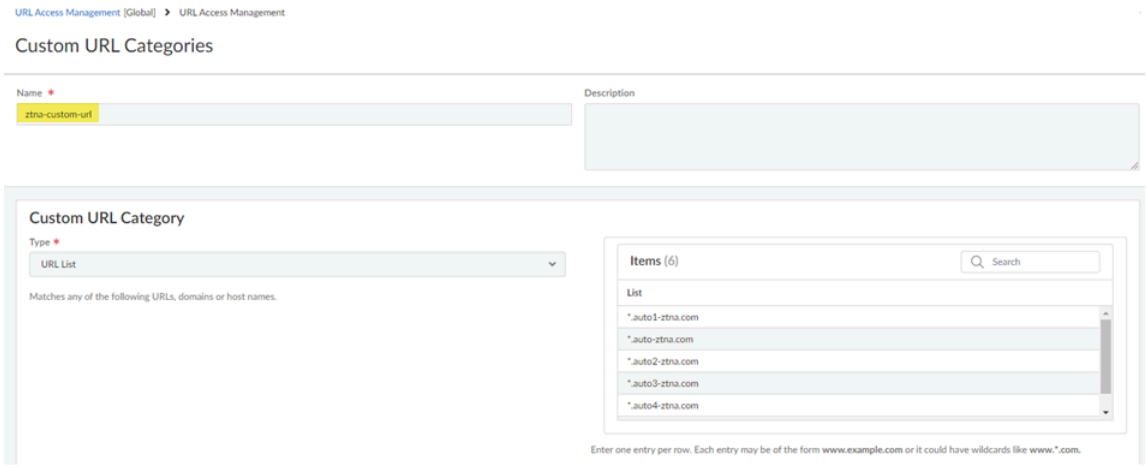
Política de seguridad para aplicaciones basadas en comodines

Las aplicaciones basadas en comodines [**Settings (Configuración)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **Wildcard Targets (Objetivos comodín)**] requieren que cree una categoría de URL personalizada; sin embargo, ese tipo de categoría solo aplica la política para el tráfico HTTP y HTTPS, y no se permite otro tipo de tráfico (como SSH). Por este motivo, es necesario permitir temporalmente el acceso a todas las aplicaciones permitiendo el tráfico a los bloques de IP de la aplicación ZTNA Connector.

Una vez que ZTNA Connector conoce los FQDN que se basan en los comodines, puede deshabilitar la política que permite el tráfico de bloqueo de IP de aplicación y aplicar la política en función de los FQDN conocidos.

STEP 1 | Cree una categoría de URL personalizada y añada las URL comodín a la categoría.

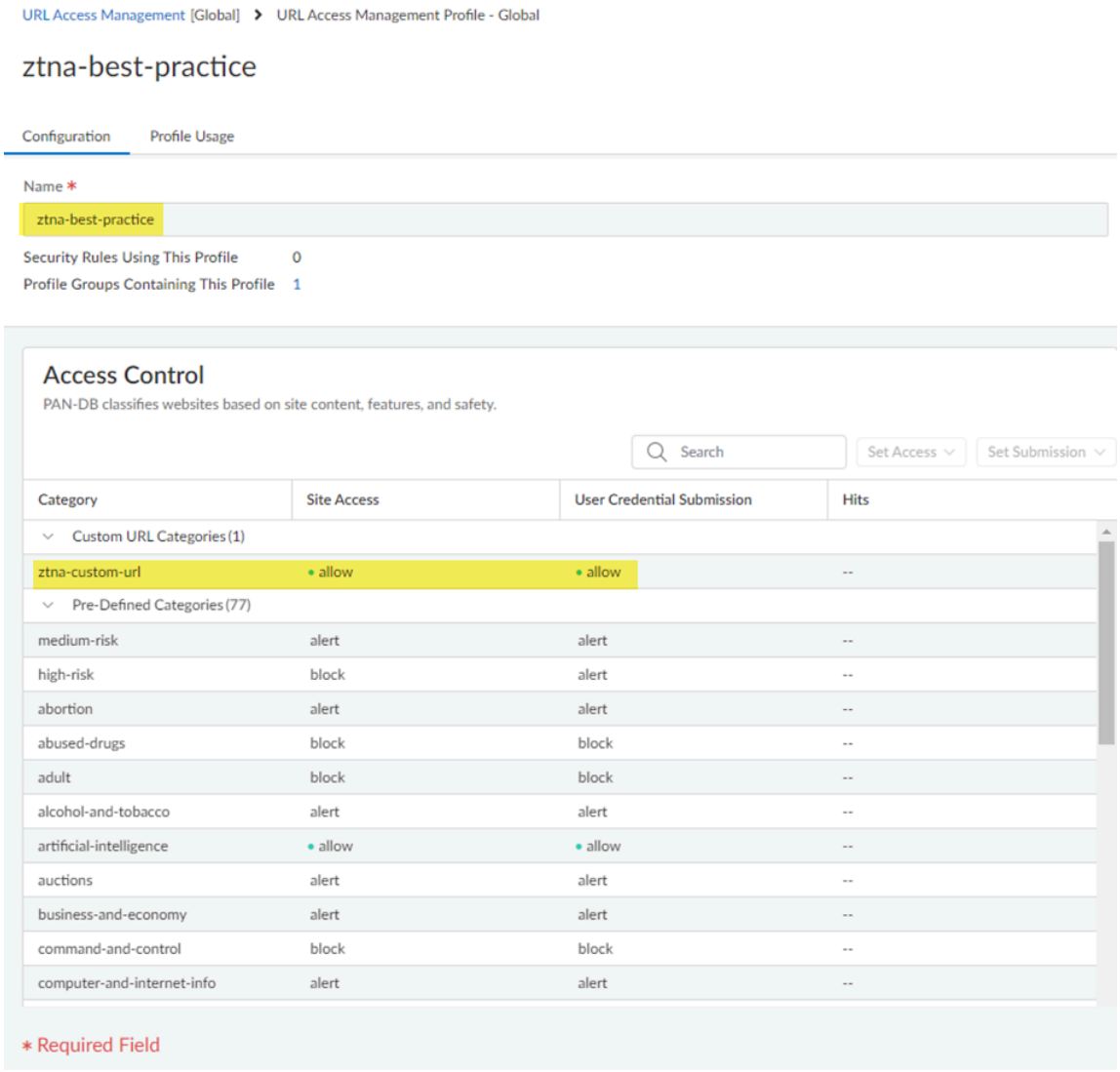
1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso de URL)**.
2. En Categorías de URL personalizadas, seleccione **Add Category (Añadir categoría)**.
3. Proporcione un **Name (Nombre)** descriptivo para la categoría de URL personalizada y seleccione un **Type (Tipo)** de **URL List (Lista de URL)**.
4. Añada las URL comodín que creó en ZTNA Connector a los **Items (Elementos)**.
5. Haga clic en **Save (Guardar)** para guardar sus cambios.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Cree un perfil de gestión de acceso URL y añádalo a la categoría de URL personalizada que creó.

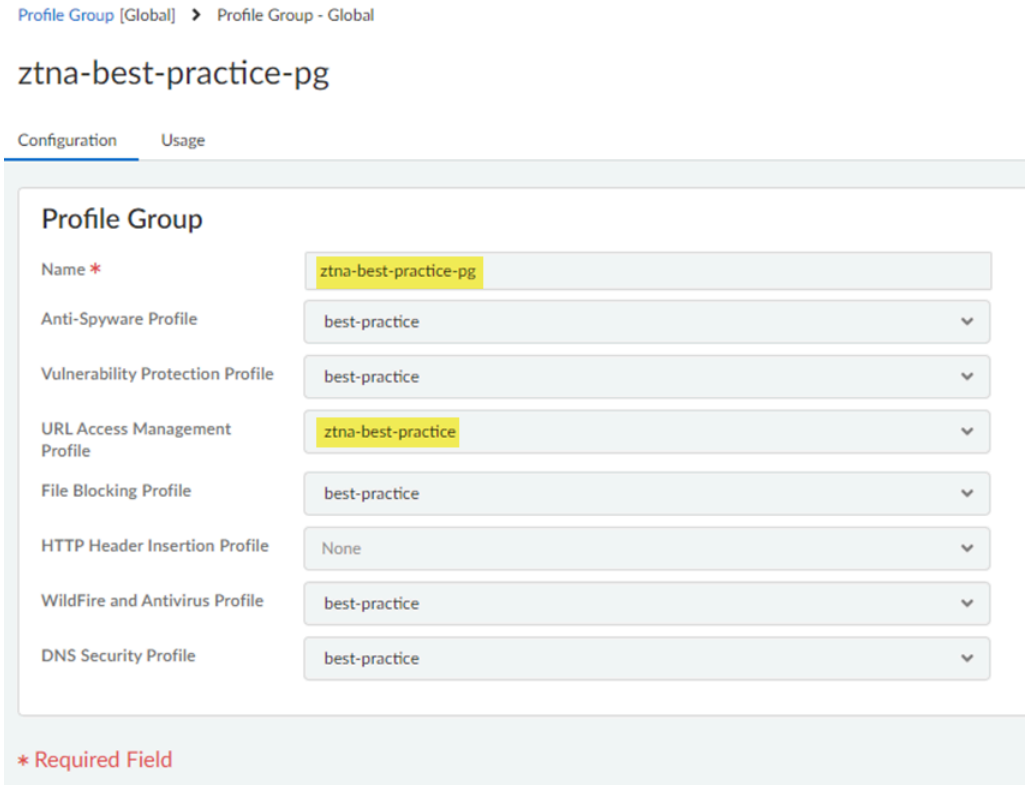
1. Mientras aún se encuentra en el área de **URL Access Management (Gestión de acceso a URL)**, seleccione **URL Access Management Profiles (Perfiles de gestión de acceso URL)**.
2. Seleccione un perfil existente para modificarlo o haga clic en **Add Profile (Añadir perfil)**.
3. Añada la categoría de URL personalizada que creó al perfil.
4. Seleccione los siguientes parámetros:
   - **Site Access (Acceso a sitio)**: Permitir
   - **User Credential Submission (Envío de credencial de usuario)**: Permitir
5. Haga clic en **Save (Guardar)** para guardar sus cambios.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cree un grupo de perfiles y adjunte el perfil de gestión de acceso URL al grupo.

1. Vaya a **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Profile Groups (Grupos de perfiles)**.
2. Elija **Add (Añadir)** un grupo de perfiles, especificando el perfil de gestión de acceso URL que creó.

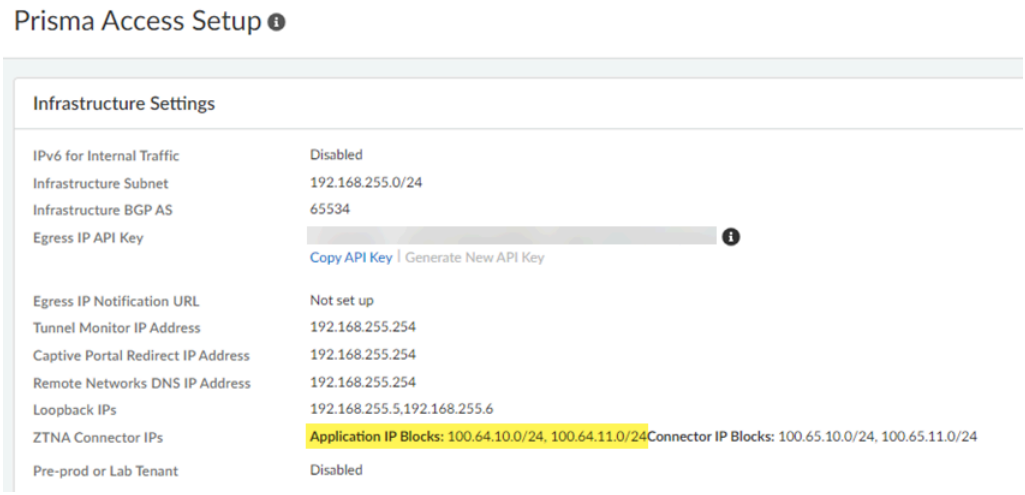


STEP 4 | Cree una política para permitir el grupo de perfiles y las direcciones IP para los bloques IP de la aplicación de ZTNA Connector.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Prisma Access Setup (Configuración de Prisma Access)** y

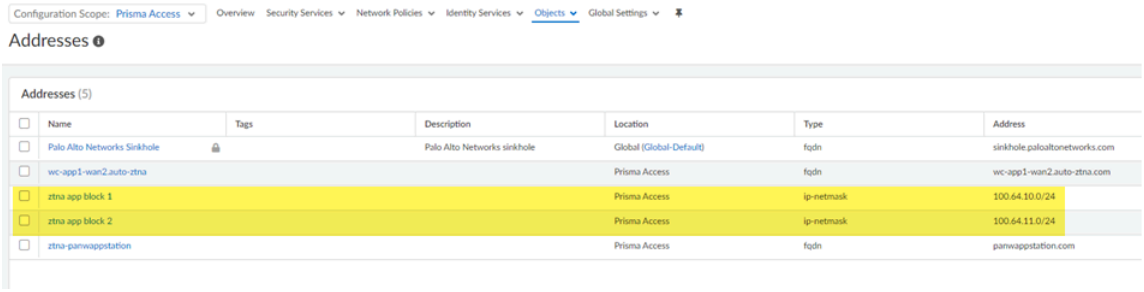
 ©2025 Palo Alto Networks, Inc.

tome nota de los **Application IP Blocks (Bloques de IP de la aplicación)** en las IP del ZTNA Connector.

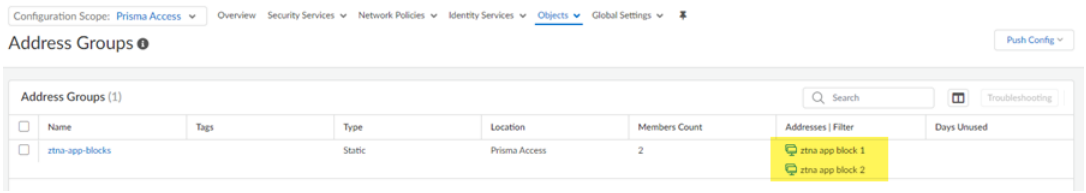


2. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Addresses (Direcciones)** y **Add (Añadir)** objetos de dirección en función de las direcciones IP que recuperó.

   Si tiene aplicaciones basadas en subredes IP, cree objetos de dirección también para esas subredes.



3. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Address Groups (Grupos de direcciones)** y luego **Add (Añadir)** para añadir los objetos de dirección que creó a un grupo de direcciones.



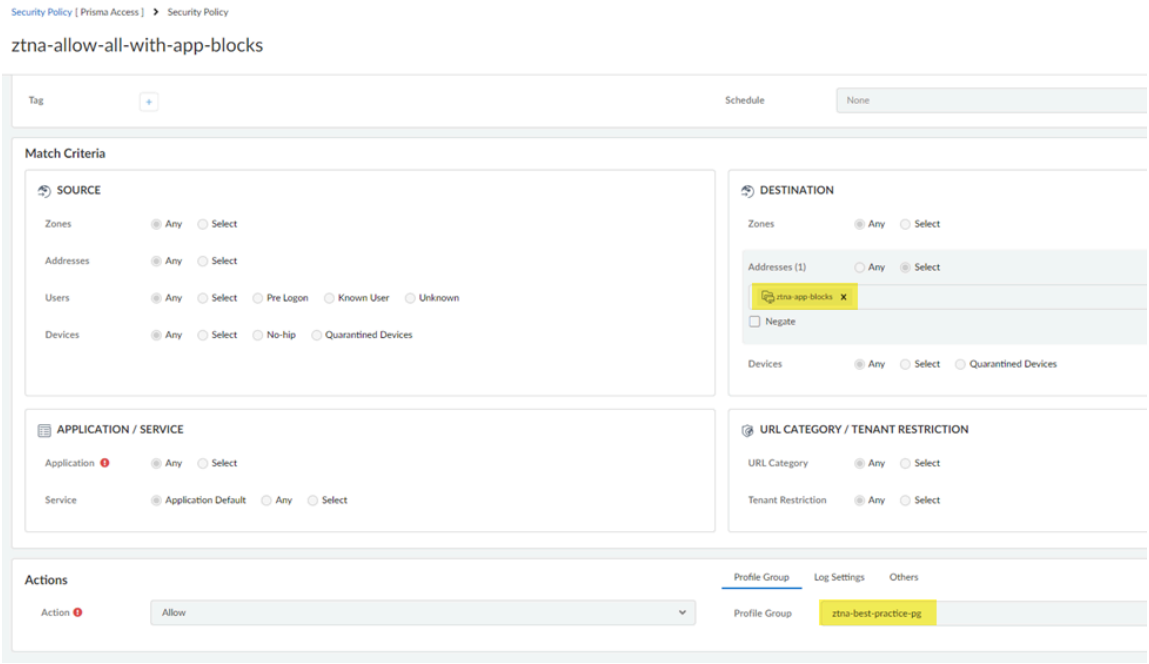
4. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **Pre Rules (Reglas previas)** y seleccione **Add (Añadir)** una política de seguridad para permitir el acceso a todos los bloques de direcciones IP de la

 ©2025 Palo Alto Networks, Inc.

aplicación, especificando el **Address Group (Grupo de direcciones)** y el **Profile Group (Grupo de perfiles)** que creó en un paso anterior.

Al añadir esta política de seguridad se permite que todo el tráfico de aplicaciones basadas en comodines pase mientras ZTNA Connector descubre las aplicaciones basadas en comodines. Sin la regla que permite los bloqueos de IP de aplicaciones, los usuarios no pueden acceder a aplicaciones basadas en comodines.

Puede dejar esta política vigente hasta que ZTNA Connector descubra las aplicaciones basadas en comodines. Luego, puede optar por deshabilitar esta política y añadir reglas de política de seguridad para cada una de las aplicaciones detectadas.



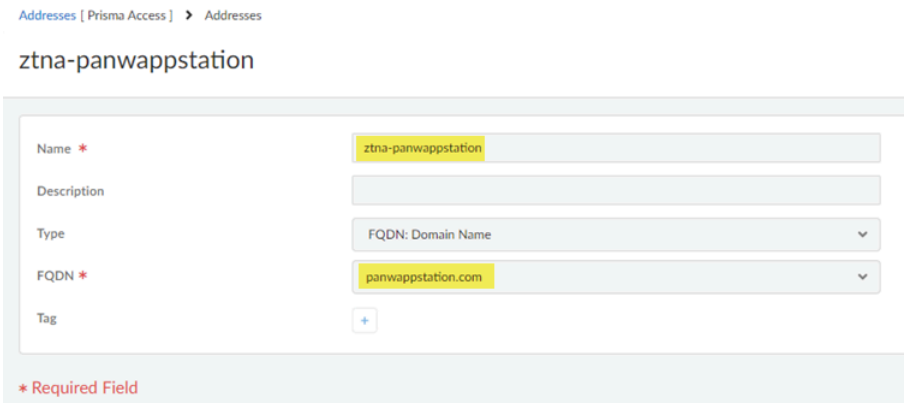
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Una vez que ZTNA Connector haya descubierto las aplicaciones basándose en comodines, configure una política de seguridad para las aplicaciones que añadió mediante FQDN.

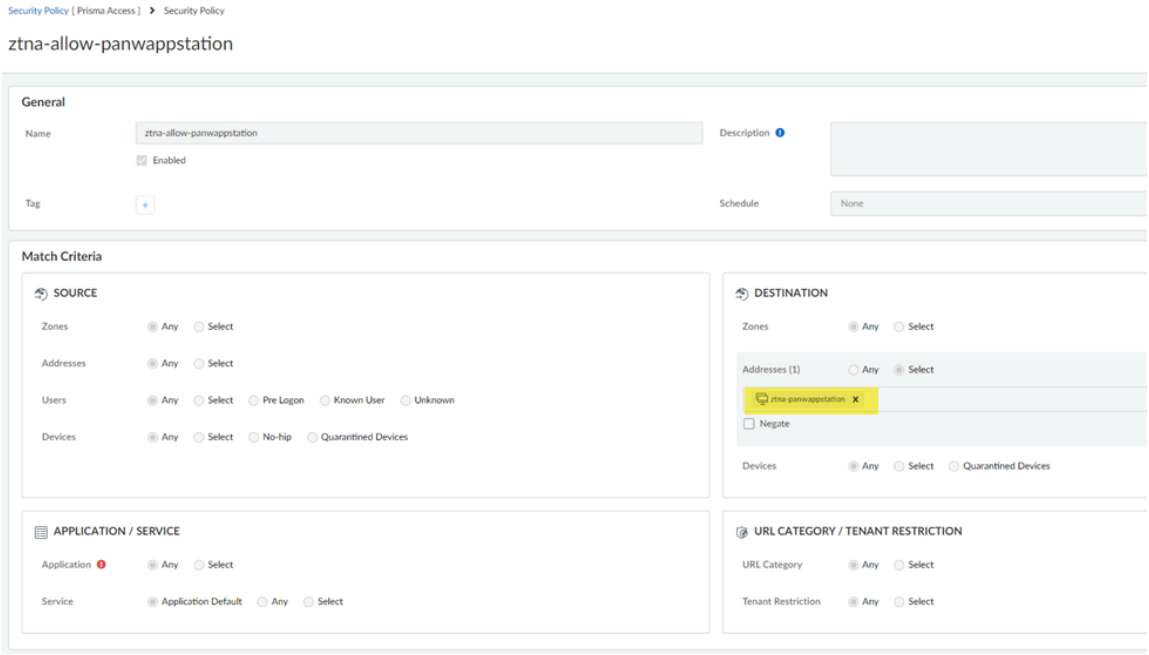
1. Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **FQDN Targets (Objetivos FQDN)** y tome nota de los FQDN utilizados por las aplicaciones.
2. Cree un objeto de dirección para el FQDN [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Addresses (Direcciones)**].

   Seleccione el ámbito de configuración de **Prisma Access**.
3. **Add (Añadir)** un objeto de dirección con el **Type (Tipo)** de **FQDN: Nombre de dominio** e introduzca el **FQDN** de la aplicación descubierta.

   Introduzca los FQDN para los objetivos FQDN.



4. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **Reglas previas** y seleccione **Add (Añadir)** para añadir una política de seguridad para permitir el acceso a las aplicaciones detectadas.



 ©2025 Palo Alto Networks, Inc.

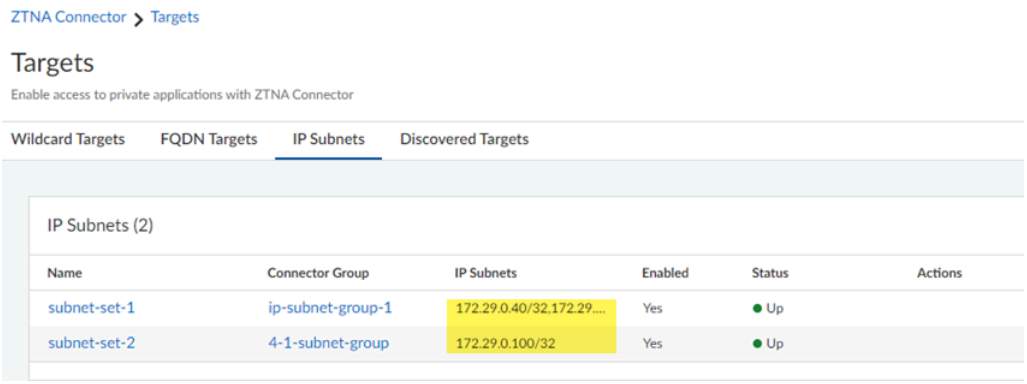
STEP 6 | Debe **Push Config (Enviar configuración)** para guardar y enviar sus cambios en la configuración.

STEP 7 | (Opcional) Después de haber creado la política de seguridad basada en FQDN, elimine la política basada en los bloques de aplicaciones IP.

Política de seguridad para aplicaciones basadas en subredes de IP

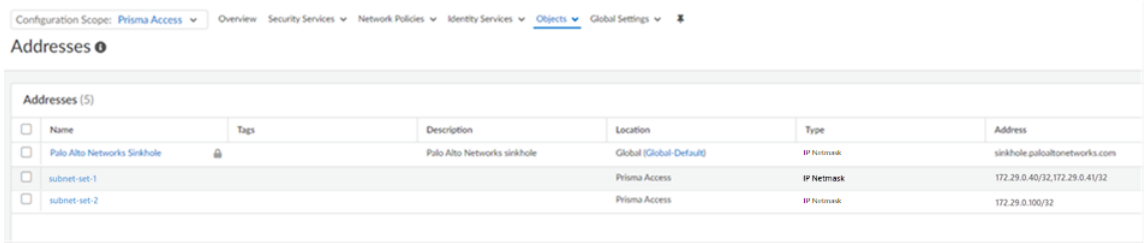
Si creó objetivos de aplicación de ZTNA Connector basados en subredes de IP (**Settings (Configuración)** > **ZTNA Connector** > **Connectors (Conectores)** > **Application Targets (Objetivos de aplicación)** > **IP Subnets (Subredes de IP)**], complete los siguientes pasos para permitir el acceso a las aplicaciones.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **IP Subnets (Subredes de IP)** y tome nota de las subredes de IP utilizadas por las aplicaciones.



STEP 2 | Cree una política para permitir las direcciones IP de las subredes de IP utilizadas para las aplicaciones.

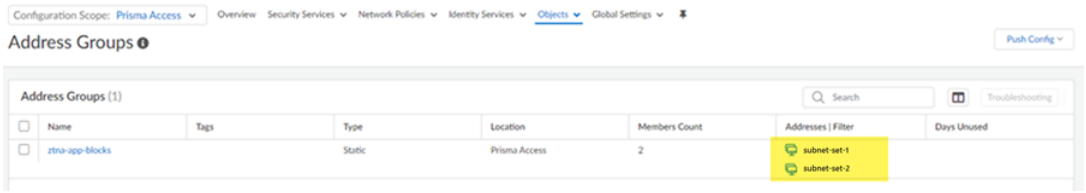
1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Addresses (Direcciones)** y **Add (Añadir)** objetos de dirección en función de las direcciones IP que recuperó.



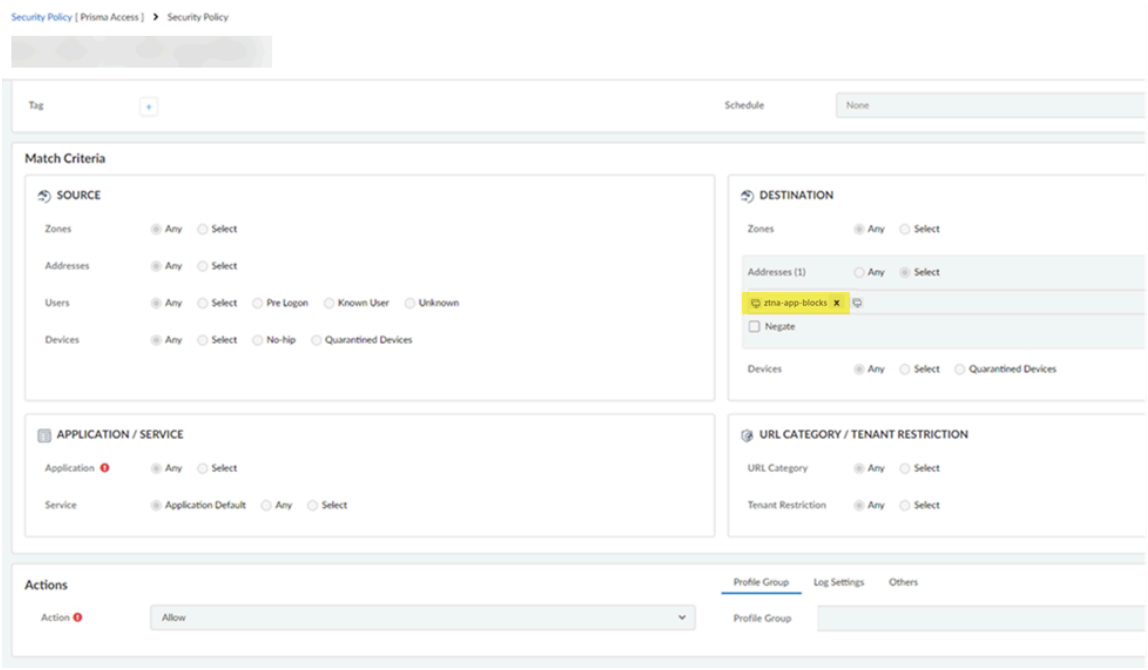
2. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Address Groups**

 ©2025 Palo Alto Networks, Inc.

(Grupos de direcciones) y elija **Add (Añadir)** para añadir las direcciones que creó a los grupos de direcciones.



3. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **Pre Rules (Reglas previas)** y **Add (Añadir)** para añadir una política de seguridad para permitir el acceso a las subredes IP para las aplicaciones, especificando las **Addresses (Direcciones)** que creó en un paso anterior.



STEP 3 | Debe **Push Config (Enviar configuración)** para guardar y enviar sus cambios en la configuración.

Política de seguridad para aplicaciones basadas en FQDN

Si ha añadido objetivos basados en FQDN (**Settings (Configuración)** > **ZTNA Connector** > **Connectors (Conectores)** > **Application Targets (Objetivos de aplicación)** > **FQDN Targets (Objetivos FQDN)**], cree un objeto de dirección y una política de seguridad para permitir el acceso a las aplicaciones completando los siguientes pasos.

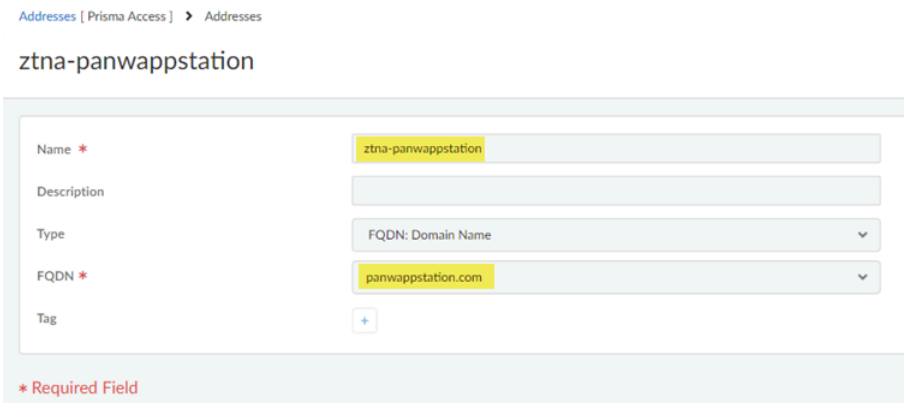
©2025 Palo Alto Networks, Inc.

STEP 1 | Configure una política de seguridad para las aplicaciones que añadió mediante FQDN.

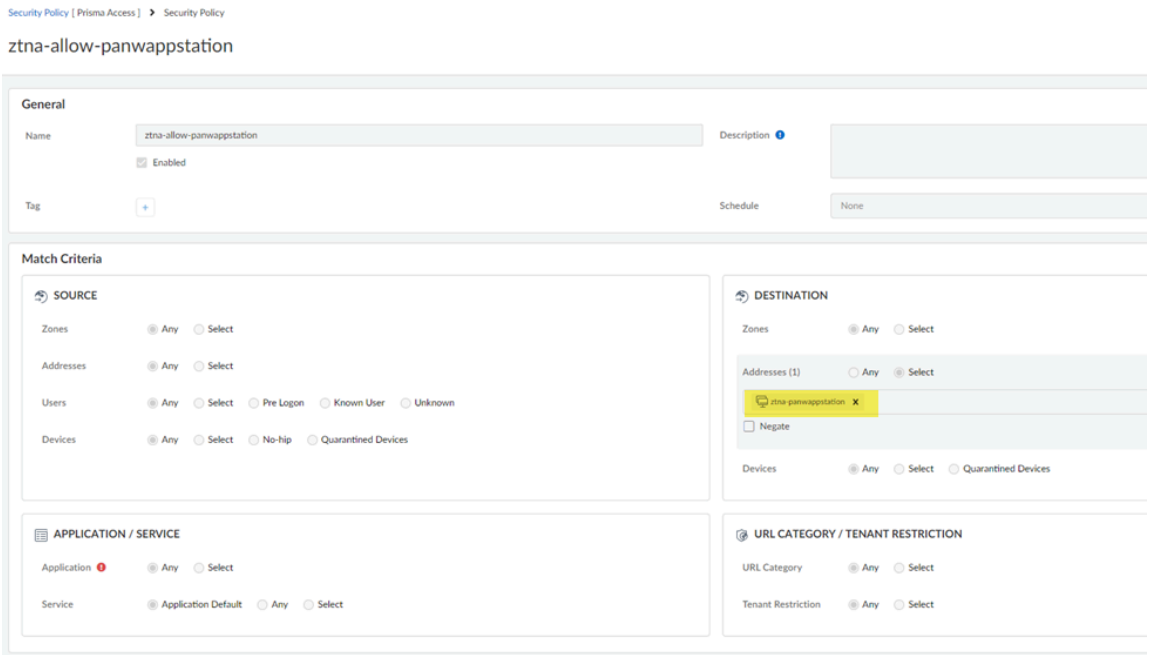
1. Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **FQDN Targets (Objetivos FQDN)** y tome nota de los FQDN utilizados por las aplicaciones.
2. Cree un objeto de dirección para el FQDN [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Addresses (Direcciones)**].

   Seleccione el ámbito de configuración de **Prisma Access**.
3. **Add (Añadir)** un objeto de dirección con el **Type (Tipo)** de **FQDN: Nombre de dominio** e introduzca el **FQDN** de la aplicación descubierta.

   Introduzca los FQDN de todas las aplicaciones detectadas.



4. Opcional: Vaya a **Manage (gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **Pre Rules (Reglas previas)** y **Add (Añadir)** para añadir una política de seguridad para permitir el acceso a las aplicaciones detectadas.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Debe **Push Config (Enviar configuración)** para guardar y enviar sus cambios en la configuración.

Política de seguridad para aplicaciones habilitadas con ZTNA Connector (Panorama)

Después de incorporar aplicaciones a ZTNA Connector, debe configurar reglas de políticas para permitir y controlar el acceso a esas aplicaciones. El procedimiento para crear y aplicar políticas difiere según si sus aplicaciones están definidas por comodines, subredes de IPo FQDN.

Política de seguridad para aplicaciones basadas en comodines

Las aplicaciones basadas en comodines [**Settings (Configuración)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **Wildcard Targets (Objetivos comodín)**] requieren que cree una categoría de URL personalizada; sin embargo, ese tipo de categoría solo aplica la política para el tráfico HTTP y HTTPS, y no se permite otro tipo de tráfico (como SSH). Por este motivo, es necesario permitir temporalmente el acceso a todas las aplicaciones permitiendo el tráfico a los bloques de IP de la aplicación ZTNA Connector.

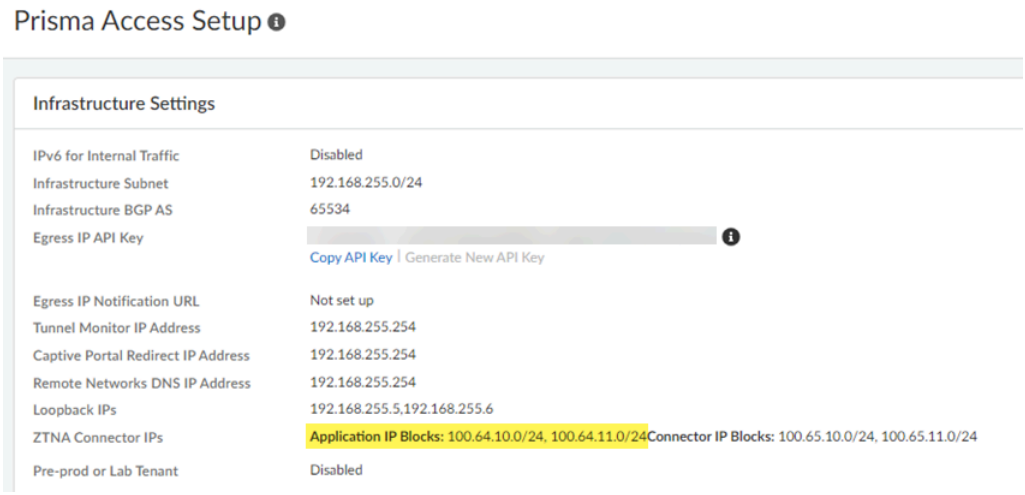
Una vez que ZTNA Connector conoce los FQDN que se basan en los comodines, puede deshabilitar la política que permite el tráfico de bloqueo de IP de aplicación y aplicar la política en función de los FQDN conocidos.

STEP 1 | Cree una política para permitir las direcciones IP para los bloques IP de la aplicación de ZTNA Connector.

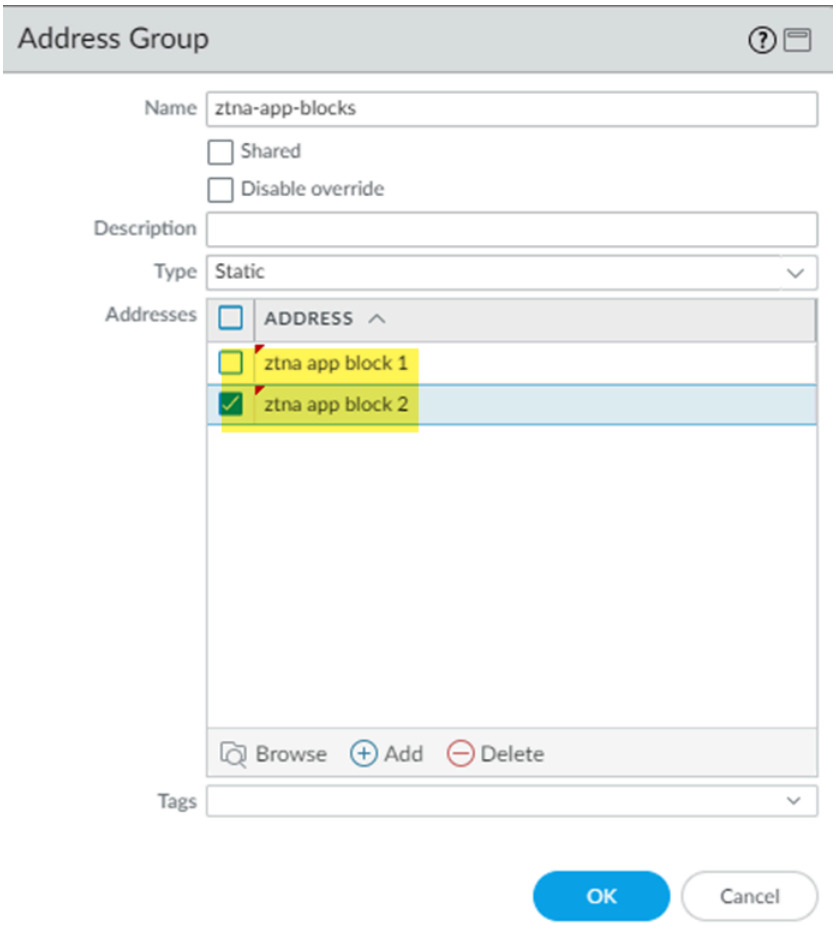
1. Desde la interfaz de usuario de ZTNA Connector, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Prisma**

 ©2025 Palo Alto Networks, Inc.

Access Setup (Configuración de Prisma Access) y tome nota de los **Application IP Blocks (Bloques de IP de aplicaciones)** en las IP del ZTNA Connector.



2. Vaya a **Objects (Objetos)** > **Addresses (Direcciones)** y seleccione **Add (Añadir)** objetos de dirección según las direcciones IP que recuperó.
3. Vaya a **Objetos** > **Address Groups (Grupos de direcciones)** y **Add (Añadir)** para añadir los objetos de dirección que creó a un grupo de direcciones.

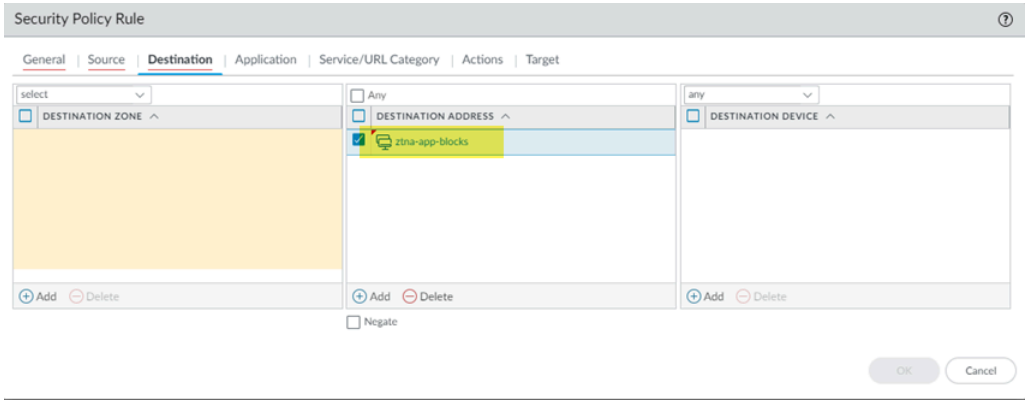


 ©2025 Palo Alto Networks, Inc.

4. Vaya a **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)** y seleccione **Add (Añadir)** para añadir una política de seguridad para permitir el acceso a todos los bloques de direcciones IP de la aplicación, especificando el **Address Group (Grupo de direcciones)** que creó en un paso anterior.

   Al añadir esta política de seguridad se permite que todo el tráfico de aplicaciones basadas en comodines pase mientras ZTNA Connector descubre las aplicaciones basadas en comodines. Sin la regla que permite los bloqueos de IP de aplicaciones, los usuarios no pueden acceder a aplicaciones basadas en comodines.

   Puede dejar esta política vigente hasta que ZTNA Connector descubra las aplicaciones basadas en comodines. Luego, puede optar por deshabilitar esta política y añadir reglas de política de seguridad para cada una de las aplicaciones detectadas.



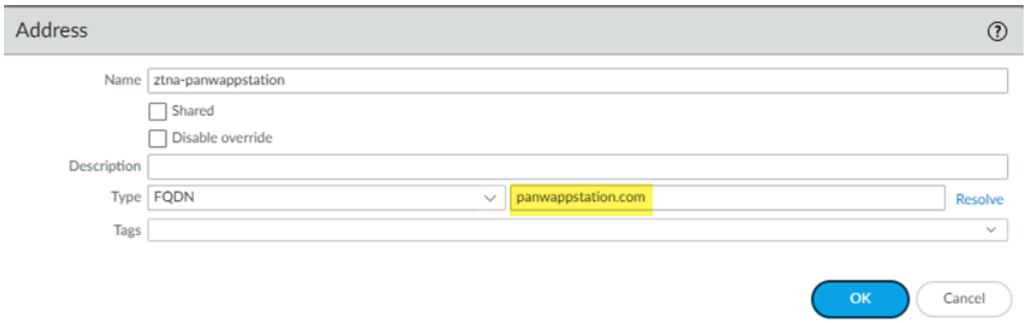
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Una vez que ZTNA Connector haya descubierto las aplicaciones basándose en comodines, configure una política de seguridad para las aplicaciones que añadió mediante FQDN.

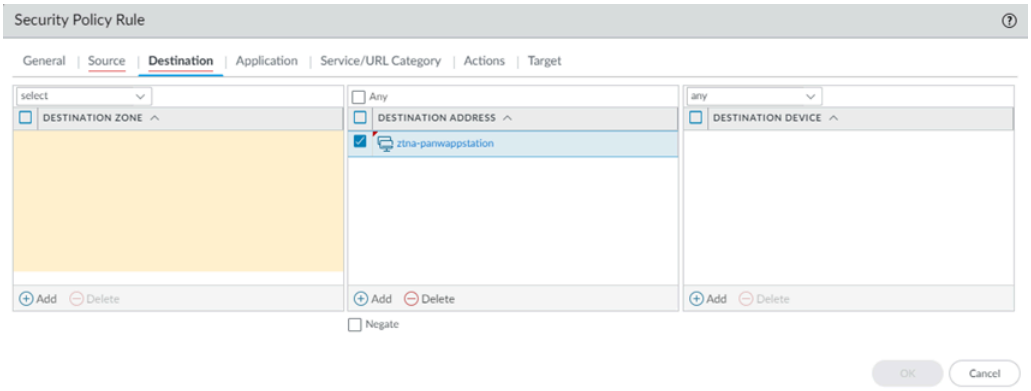
1. Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **FQDN Targets (Objetivos FQDN)** y tome nota de los FQDN utilizados por las aplicaciones.
2. Cree un objeto de dirección para el FQDN [**Objects (Objetos)** > **Addresses (Direcciones)**].

   Seleccione **Mobile_User_Device_Group** o **Remote_Network_Device_Group**, dependiendo de si los usuarios móviles o los usuarios en las sucursales accederán a las aplicaciones privadas detrás de ZTNA Connector.
3. Deberá **Add (Añadir)** un objeto de dirección con el **Type (Tipo)** de **FQDN** e introducir el **FQDN** de la aplicación detectada.

   Introduzca los FQDN para los objetivos FQDN.



4. Vaya a **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)** y luego **Add (Añadir)** para añadir una política de seguridad para permitir el acceso a las aplicaciones descubiertas.



STEP 3 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 4 | (Opcional) Después de haber creado la política de seguridad basada en FQDN, elimine la política basada en los bloques de aplicaciones IP.

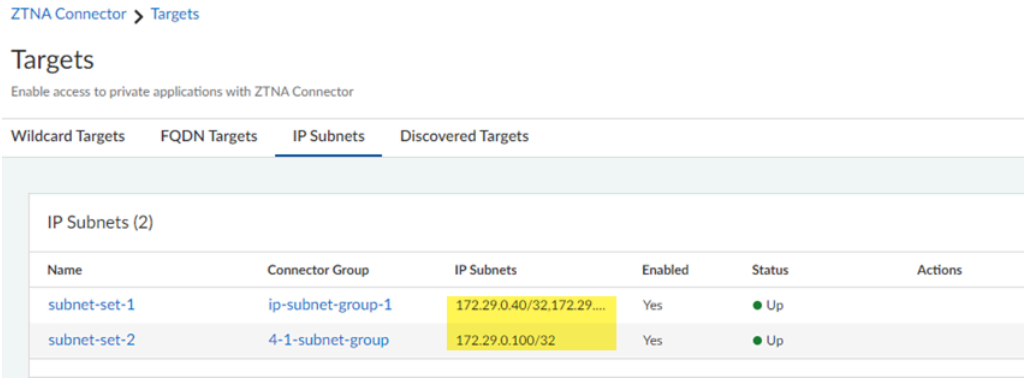
Política de seguridad para aplicaciones basadas en subredes de IP

Si creó objetivos de aplicación de ZTNA Connector basados en subredes de IP (**Settings (Configuración)** > **ZTNA Connector** > **Connectors (Conectores)** > **Application Targets (Objetivos**

 ©2025 Palo Alto Networks, Inc.

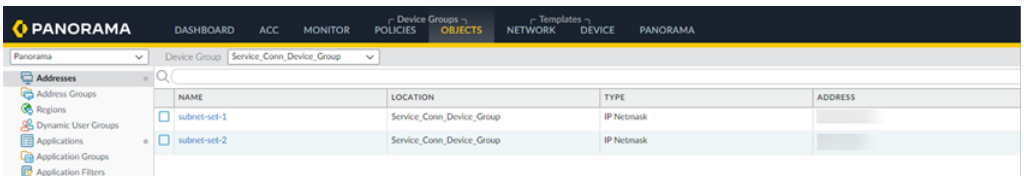
de aplicación) > **IP Subnets (Subredes de IP)**], complete los siguientes pasos para permitir el acceso a las aplicaciones.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **IP Subnets (Subredes de IP)** y tome nota de las subredes de IP utilizadas por las aplicaciones.

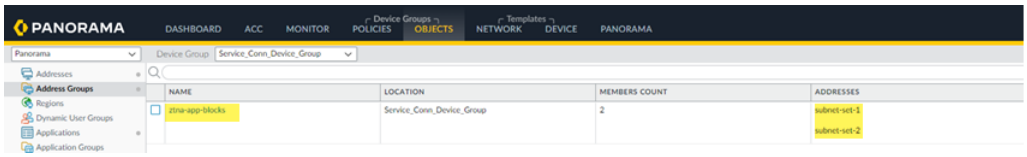


STEP 2 | Cree una política para permitir las direcciones IP de las subredes de IP utilizadas para las aplicaciones.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Address (Dirección)** > **Addresses (Direcciones)** y **Add (Añadir)** objetos de dirección en función de las direcciones IP que recuperó.



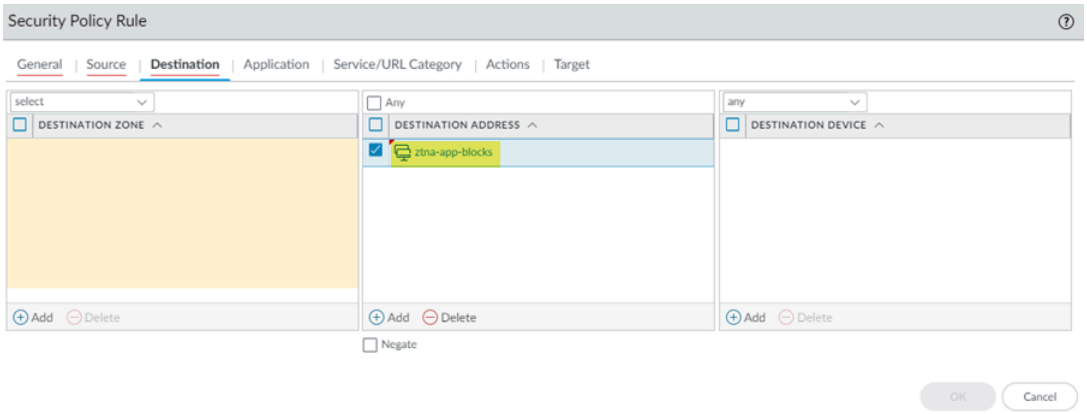
2. Vaya a **Objects (Objetos)** > **Address Groups (Grupos de direcciones)** y elija **Add (Añadir)** para añadir las direcciones que creó a los grupos de direcciones.



3. Vaya a **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)** y seleccione **Add (Añadir)** una política de seguridad para permitir el acceso a las subredes

 ©2025 Palo Alto Networks, Inc.

IP para las aplicaciones, especificando las **Addresses (Direcciones)** que creó en un paso anterior.



STEP 3 | Debe **Push Config (Enviar configuración)** para guardar y enviar sus cambios en la configuración.

Política de seguridad para aplicaciones basadas en FQDN

Si ha añadido objetivos basados en FQDN (**Settings (Configuración)** > **ZTNA Connector** > **Connectors (Conectores)** > **Application Targets (Objetivos de aplicación)** > **FQDN Targets (Objetivos FQDN)**], cree un objeto de dirección y una política de seguridad para permitir el acceso a las aplicaciones completando los siguientes pasos.

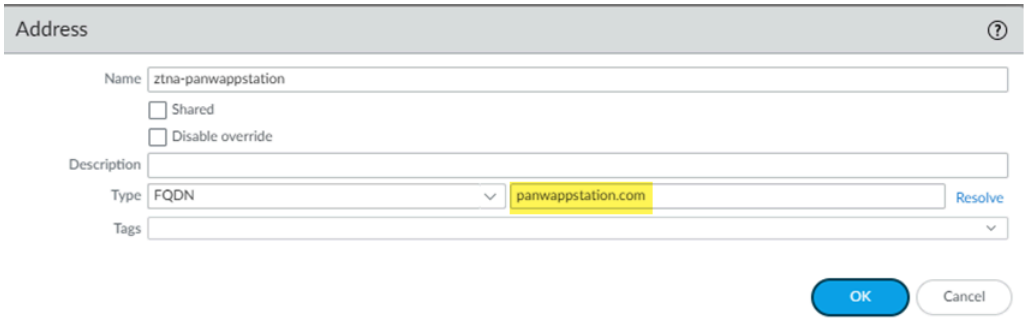
©2025 Palo Alto Networks, Inc.

STEP 1 | Configure una política de seguridad para las aplicaciones que añadió mediante FQDN.

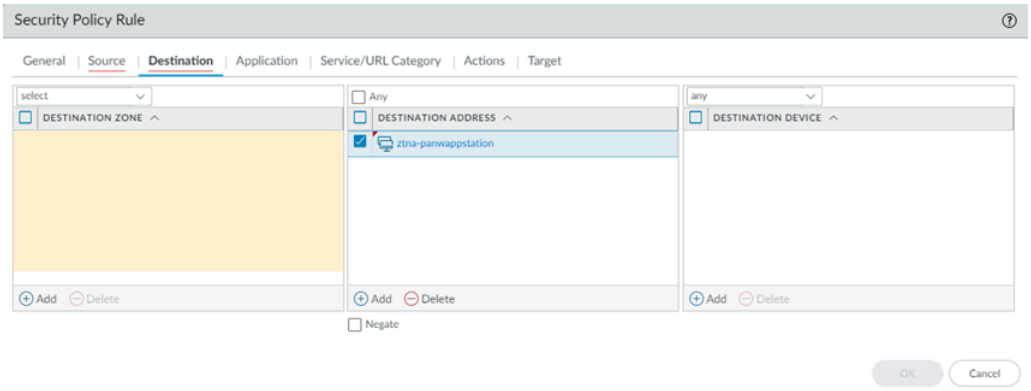
1. Vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Application Targets (Objetivos de la aplicación)** > **FQDN Targets (Objetivos FQDN)** y tome nota de los FQDN utilizados por las aplicaciones.
2. Cree un objeto de dirección para el FQDN [**Objects (Objetos)** > **Addresses (Direcciones)**].

   Seleccione **Mobile_User_Device_Group** o **Remote_Network_Device_Group**, dependiendo de si los usuarios móviles o los usuarios en las sucursales accederán a las aplicaciones privadas detrás de ZTNA Connector.
3. Deberá **Add (Añadir)** un objeto de dirección con el **Type (Tipo)** de **FQDN** e introducir el **FQDN** de la aplicación detectada.

   Introduzca los FQDN de todas las aplicaciones detectadas.



4. Opcional: Vaya a **Manage (gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **Pre Rules (Reglas previas)** y **Add (Añadir)** para añadir una política de seguridad para permitir el acceso a las aplicaciones detectadas.



STEP 2 | Debe **Push Config (Enviar configuración)** para guardar y enviar sus cambios en la configuración.

 ©2025 Palo Alto Networks, Inc.

Incorpore la máquina virtual de ZTNA Connector en su centro de datos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Después de configurar los grupos de conectores, los conectores y los destinos de aplicaciones dentro de Prisma Access, debe implementar la máquina virtual del conector en el centro de datos. Para simplificar la incorporación de conectores, las plantillas de implementación para cada entorno de centro de datos están disponibles en el portal de asistencia al cliente de Palo Alto Networks o en el marketplace de proveedores de nube. La plantilla que use depende de si planea usar una implementación de una interfaz de red o una implementación de dos interfaces de red.

Implementaciones de ZTNA Connector compatibles

El ZTNA Connector inicia la conexión a la dirección IP pública de Prisma Access en la nube y no es necesario definir ninguna regla de seguridad del cortafuegos de entrada. Sin embargo, dado que el conector ZTNA inicia la conexión, deberá añadir reglas de salida para permitir el acceso del ZTNA Connector al controlador en la nube y la conexión IPSec al plano de datos de Prisma Access. ZTNA Connector inicia la conexión con la dirección IP pública de Prisma Access en la nube. Por este motivo, necesita las siguientes reglas de salida para que el ZTNA Connector pueda crear un túnel IPSec para Prisma Access:

©2025 Palo Alto Networks, Inc.

- **Orientado a Internet**: permitir la salida para HTTPS (TCP 443) e IKE/IPSec (UDP 500 y 4500)
- **Orientado hacia el centro de datos**: permitir puertos de salida de la aplicación

  Por ejemplo, permitir los puertos de salida HTTP (80) y HTTPS (443) de la aplicación. Estos puertos de ejemplo son puertos TCP. Si su centro de datos utiliza diferentes puertos, permita esos puertos en su lugar.

Puede implementar la máquina virtual del conector en las siguientes topologías de implementación:

- **Implementación de una interfaz de red**

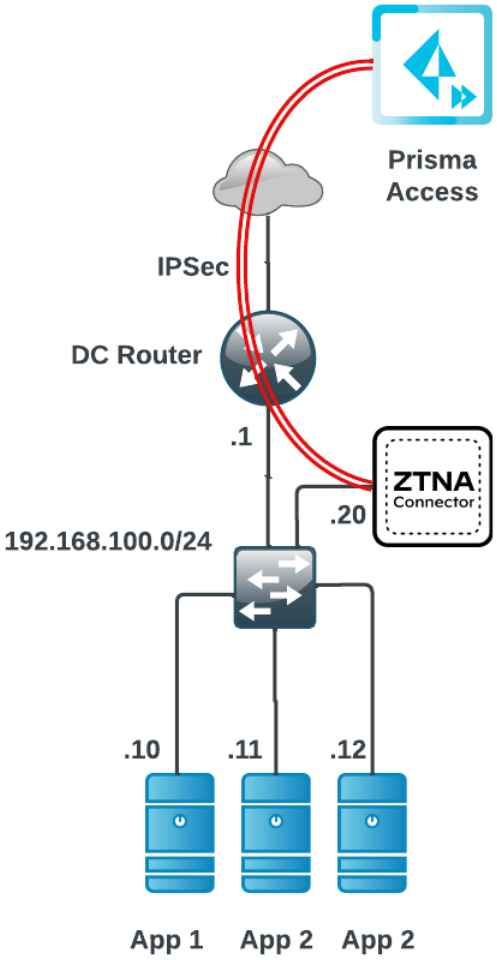
  Las implementaciones de una interfaz de red solo son compatibles con entornos nativos de la nube, como AWS, Azure o GCP. Para implementaciones locales como ESXi o una máquina virtual basada en kernel (KVM) o Microsoft Hyper-V, utilice la implementación de dos interfaces de red.

  En esta implementación, su ZTNA Connector se encuentra en una subred de centro de datos que es privada, con acceso a Internet a través de un enrutador de centro de datos. El acceso a

 ©2025 Palo Alto Networks, Inc.

las aplicaciones puede ser localmente en la misma subred o a través del enrutador del centro de datos.

En el diagrama siguiente se muestra un ejemplo de implementación de red del ZTNA Connector mediante una implementación de una interfaz de red.



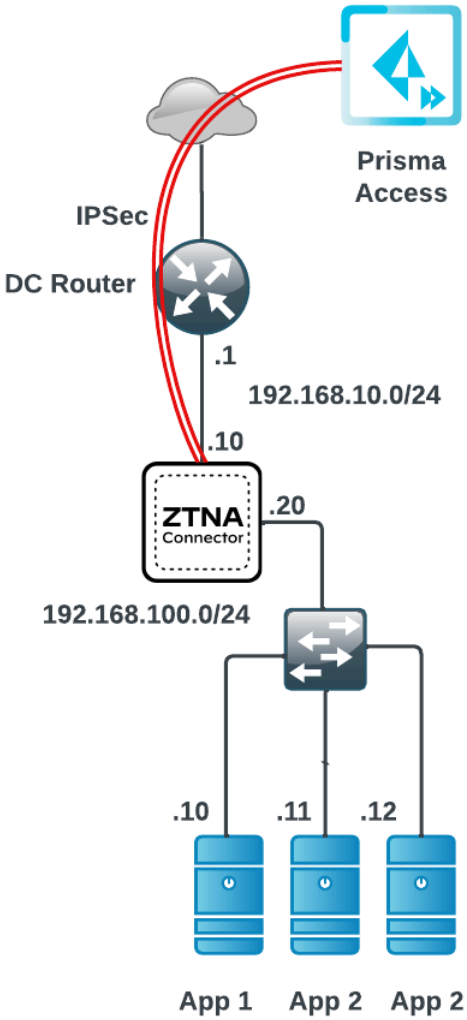
 ©2025 Palo Alto Networks, Inc.

- **Implementación de dos interfaces de red**

  Si desea tener más control sobre las reglas de seguridad de entrada y salida, o si tiene una implementación de máquina virtual local, puede usar una implementación de dos interfaces de red, donde una interfaz mira hacia Internet y otra hacia el centro de datos.

  > *Al configurar direcciones IP en un conector de dos interfaces de red, asegúrese de haber configurado correctamente las asignaciones de direcciones IP para ZTNA Connector antes de encender la máquina virtual. Por ejemplo, en el siguiente diagrama de ejemplo se usan las direcciones IP 192.168.10.10 y 192.168.10.20. Dadas estas direcciones de muestra, configure los puertos en el ZTNA Connector para 192.168.10.10 y 192.168.100.20, o Prisma Access no puede acceder a las aplicaciones en el centro de datos a través de ZTNA Connector. 192.168.10.10 y 192.168.100.20 son direcciones IP de ejemplo y no es necesario usar estas direcciones IP para que la implementación funcione.*

  En el diagrama siguiente se muestra un ejemplo de implementación de red del ZTNA Connector mediante una implementación de dos interfaces de red.

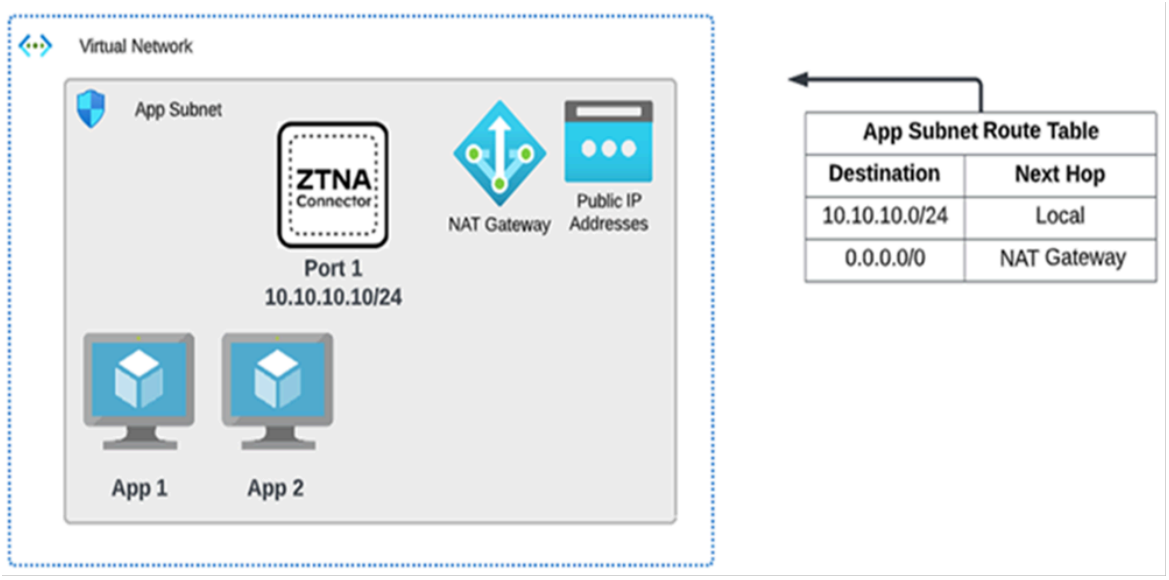


 ©2025 Palo Alto Networks, Inc.

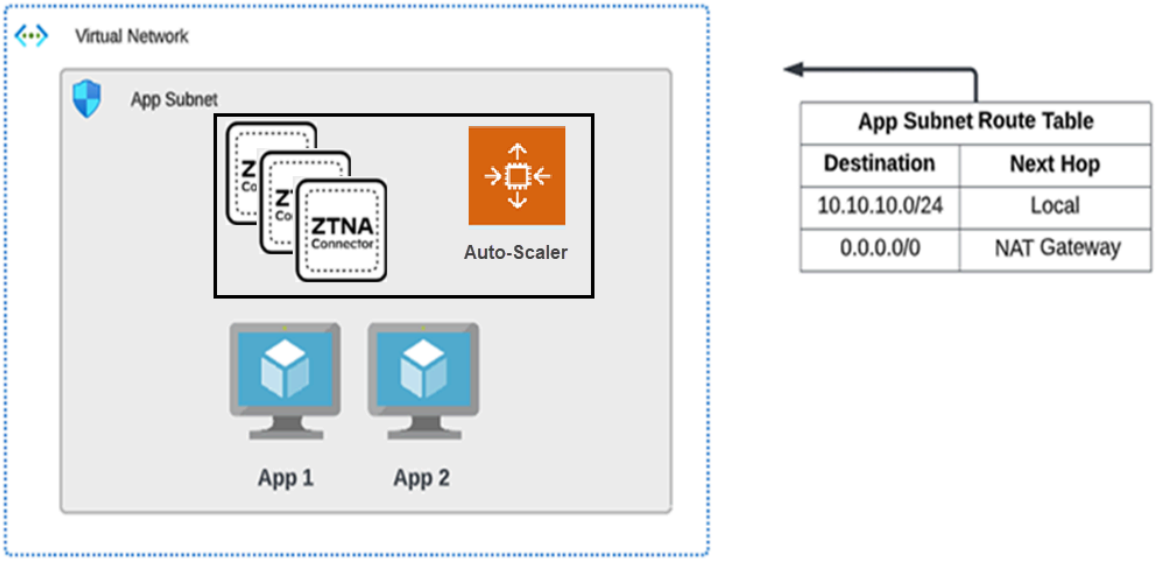
Implementaciones de Microsoft Azure compatibles con ZTNA Connector

La implementación de red del conector ZTNA de Prisma Access en Microsoft Azure admite dos implementaciones y una plantilla correspondiente para cada implementación.

El siguiente diagrama muestra una implementación de muestra de Prisma Access ZTNA Connector en Azure utilizando el modo de 1 brazo con una puerta de enlace NAT.

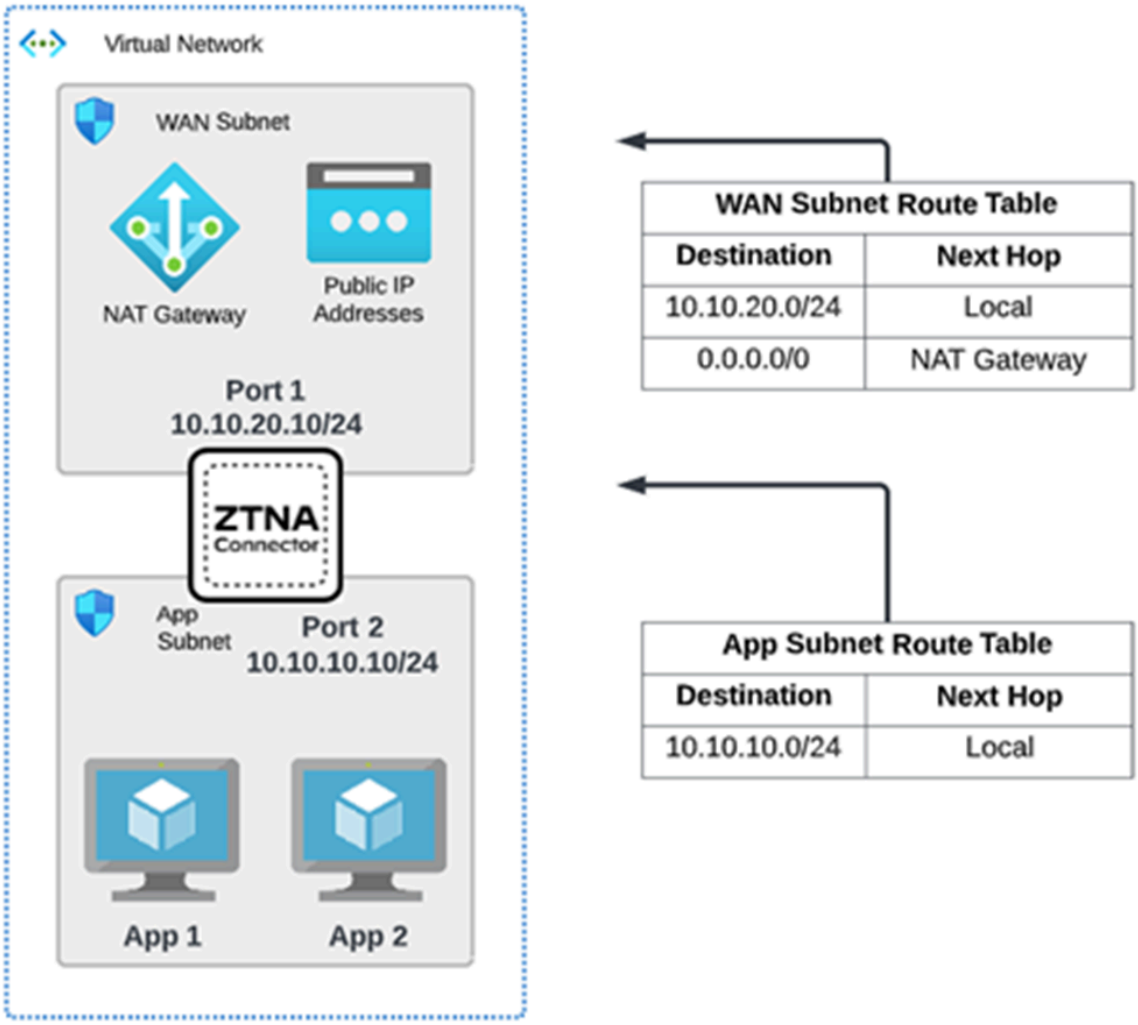


En el siguiente diagrama, se muestra un ejemplo de implementación del conector ZTNA en AWS mediante el escalado automático de un brazo con una puerta de enlace de NAT.



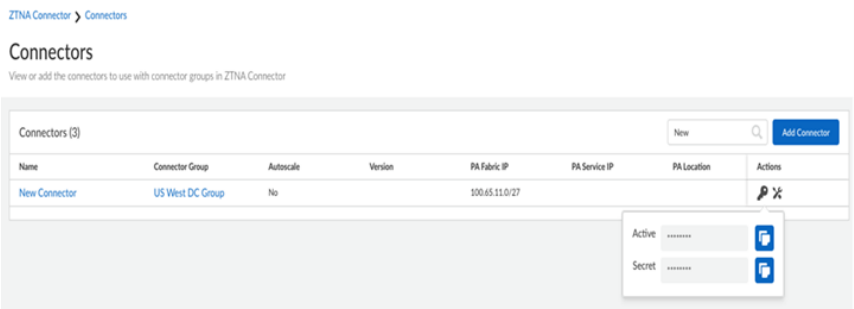
El siguiente diagrama muestra una implementación de muestra de Prisma Access ZTNA Connector en Azure utilizando el modo de dos brazos con una puerta de enlace NAT.

 ©2025 Palo Alto Networks, Inc.



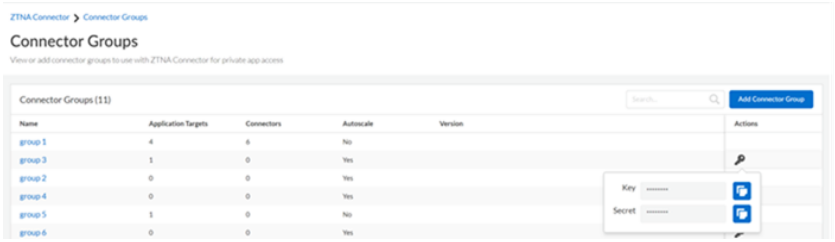
Integrar un ZTNA Connector en Microsoft Azure

- Revise los requisitos y directrices y los FQDN y puertos que necesita configurar para usar ZTNA Connector en Microsoft Azure.
- En la plataforma Prisma SASE, recupere y copie los valores clave y secreto del conector: **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Conectores**, busque el objeto Conector que creó en Prisma Access para asociar con esta VM, y seleccione **Copy Token (Copiar Token)**; luego, copie los valores de **Key (Clave)** y **Secret (Secreto)**.



 ©2025 Palo Alto Networks, Inc.

- Para la **Implementación de escalado automático de 1 interfaz de red de Prisma Access ZTNA Connector**, debe recuperar y copiar la clave y los valores Secreto y Clave del grupo de conectores: **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connector Groups (Grupos de conectores)**, busque el objeto Grupo de conectores que creó en Prisma Access para asociar con esta VM y seleccionar **Copy Token (Copiar Token)**; luego, copie la **Key (Clave)** y el **Secret (Secreto)**.



Una vez que haya cumplido con todos los requisitos previos, siga estos pasos para incorporar un conector ZTNA Connector en Microsoft Azure.

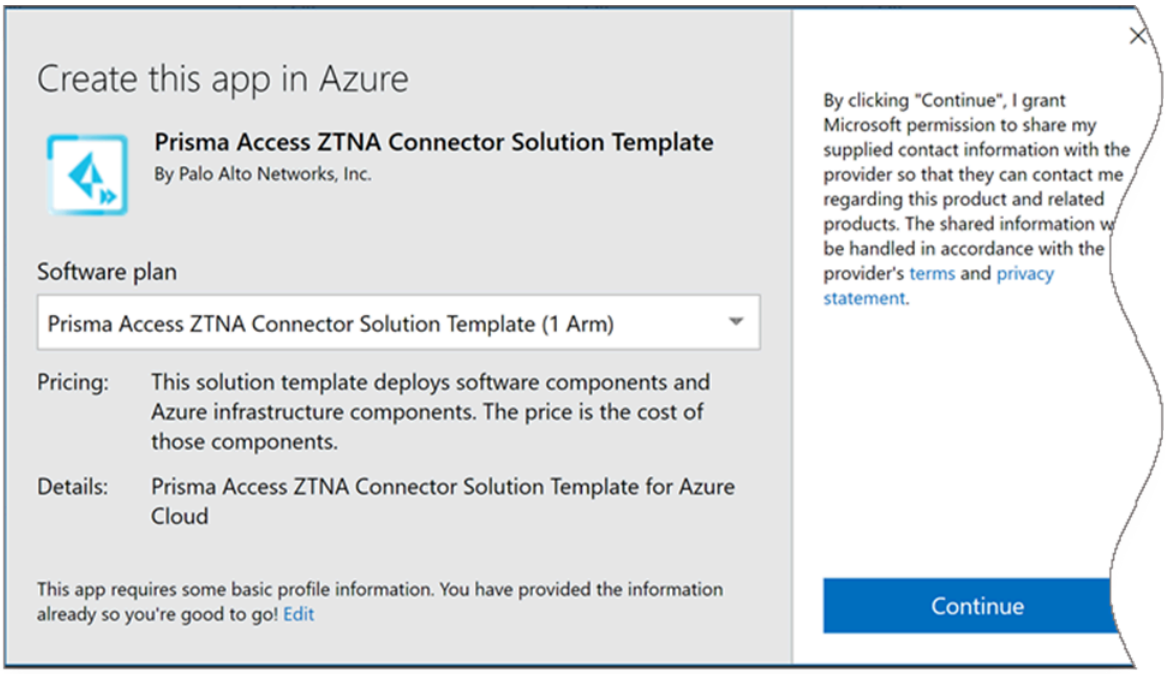
STEP 1 | Inicie sesión en Azure Marketplace y busque **Prisma Access ZTNA Connector**.

STEP 2 | Haga clic en **Get it Now (Obtenerlo ahora)**.



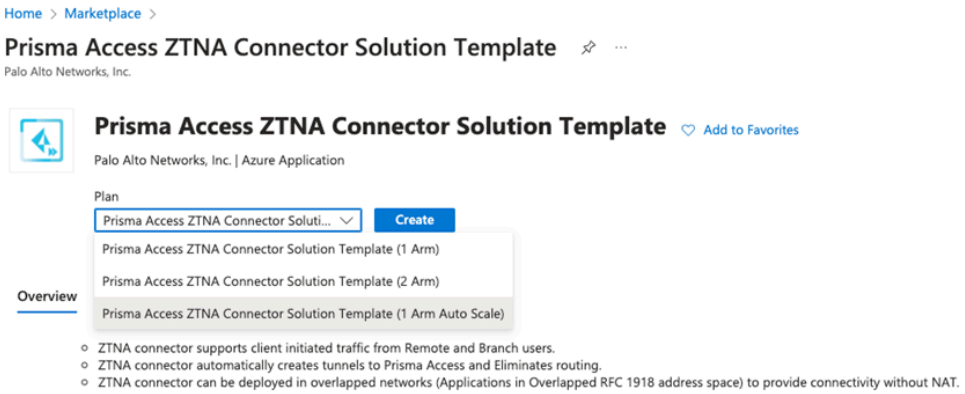
 ©2025 Palo Alto Networks, Inc.

STEP 3 | **Continue (Continuar)** el proceso de creación.



STEP 4 | Elija el plan de software y **cree** esta aplicación en Azure:

- Plantilla de la solución Prisma Access ZTNA Connector (1 interfaz)
- Implementar ZTNA Connector de una interfaz de red con escalado automático en Microsoft Azure
- Plantilla de la solución Prisma Access ZTNA Connector (2 interfaces)



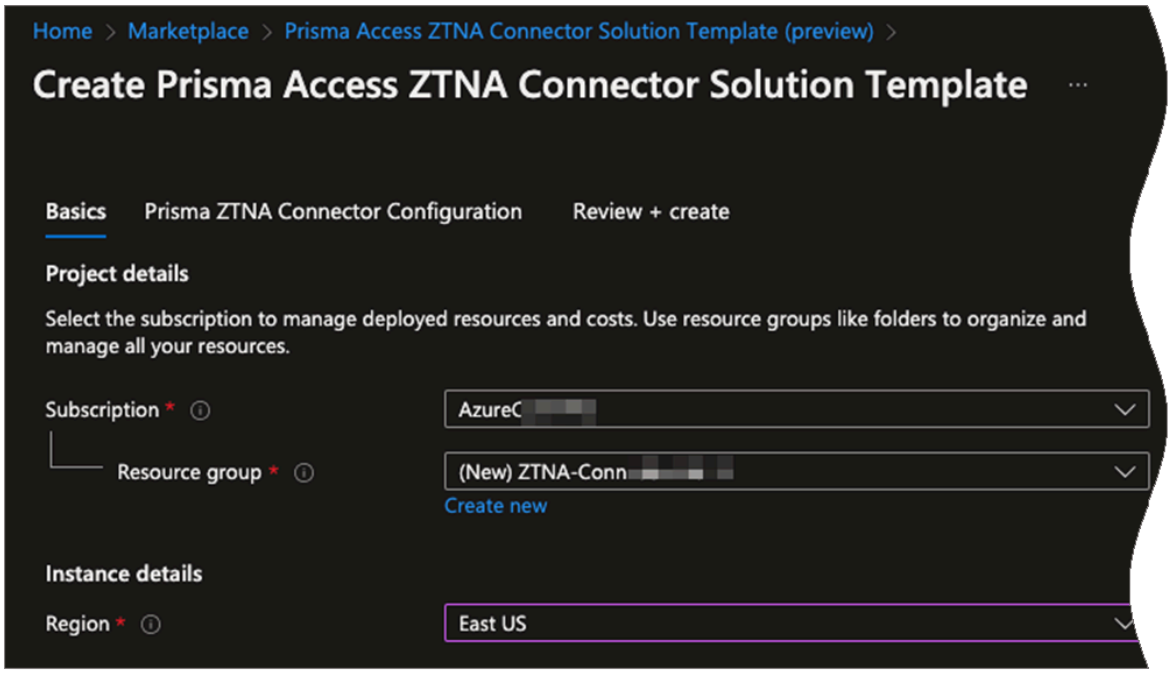
Implementar el ZTNA Connector de una interfaz de red en Microsoft Azure

Siga estos pasos para implementar el ZTNA Connector de 1 interfaz de red en Microsoft Azure:

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configure lo siguiente en la pestaña **Basics (Conceptos básicos)**:

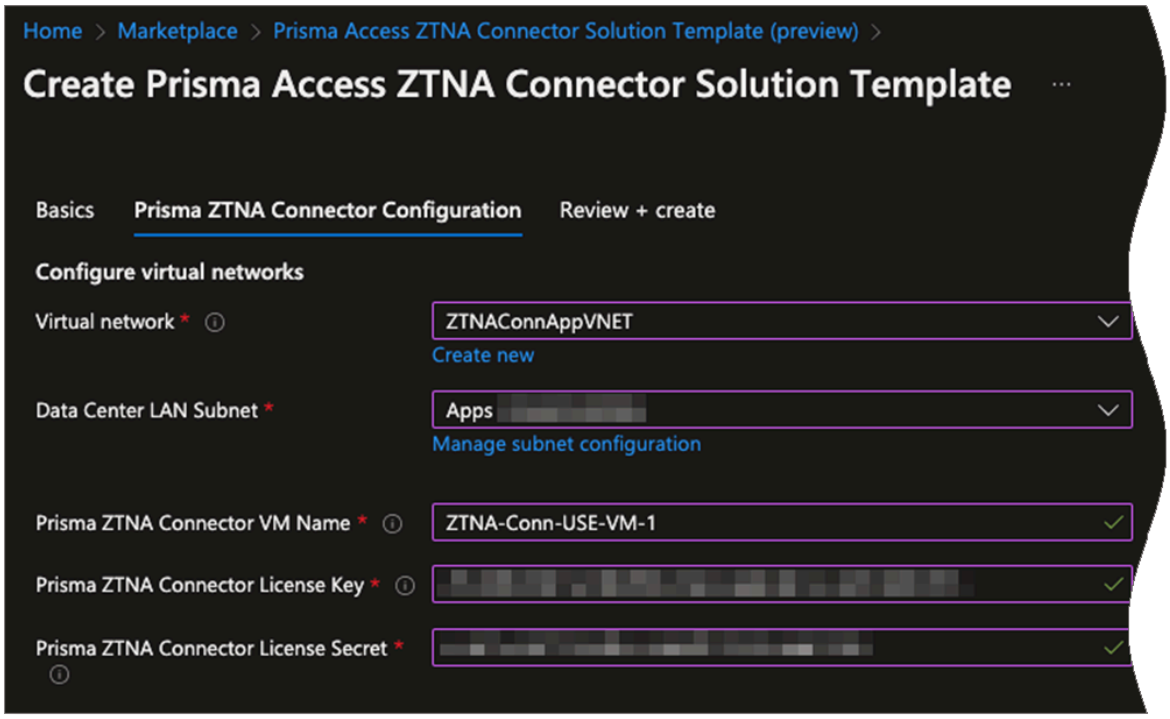
- Seleccione su **Subscription (Suscripción)** de Azure para administrar los recursos implementados.
- Seleccione un **Resource Group (Grupo de recursos)** existente o **Create new (Crear uno nuevo)**.
- Seleccione una **Region (Región)** de Azure relevante para su ubicación.
- Haga clic en **Next (Siguiente): Configuración de Prisma ZTNA Connector** .



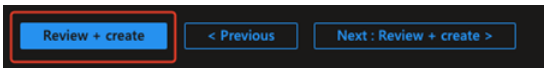
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configure una red virtual en la pestaña **Prisma ZTNA Connector Configuration (Configuración de Prisma ZTNA Connector)**:

- Cree una nueva red virtual o seleccione una **Virtual network (Red virtual)** existente.
- Seleccione la **Data Center LAN Subnet (Subred LAN del centro de datos)** donde ha aprovisionado aplicaciones para incorporarlas a este conector.
- Introduzca el **Prisma ZTNA Connector VM Name (Nombre de la máquina virtual de Prisma ZTNA Connector)**.
- Introduzca los valores **Prisma ZTNA Connector License Key (Clave de licencia de Prisma ZTNA Connector)** y **Prisma ZTNA Connector License Secret (Secreto de licencia de Prisma ZTNA Connector)** que recuperó del Portal SASE de Prisma.



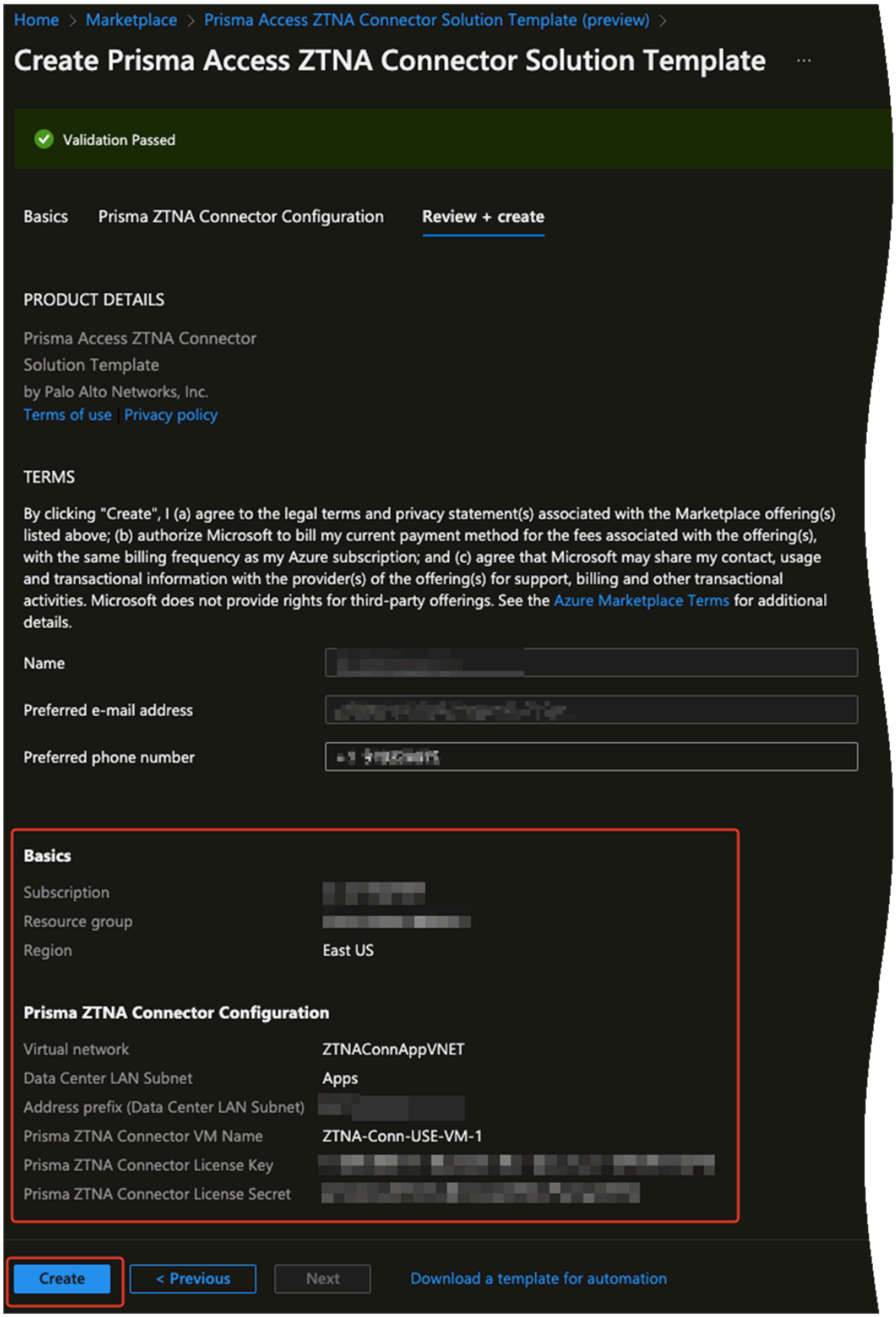
- **Review + create (Revisar + crear)** para revisar su configuración de Prisma ZTNA Connector gestionado.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirme los detalles que ha proporcionado y haga clic en **Create (Crear)** para iniciar la implementación de la máquina virtual.

 ©2025 Palo Alto Networks, Inc.



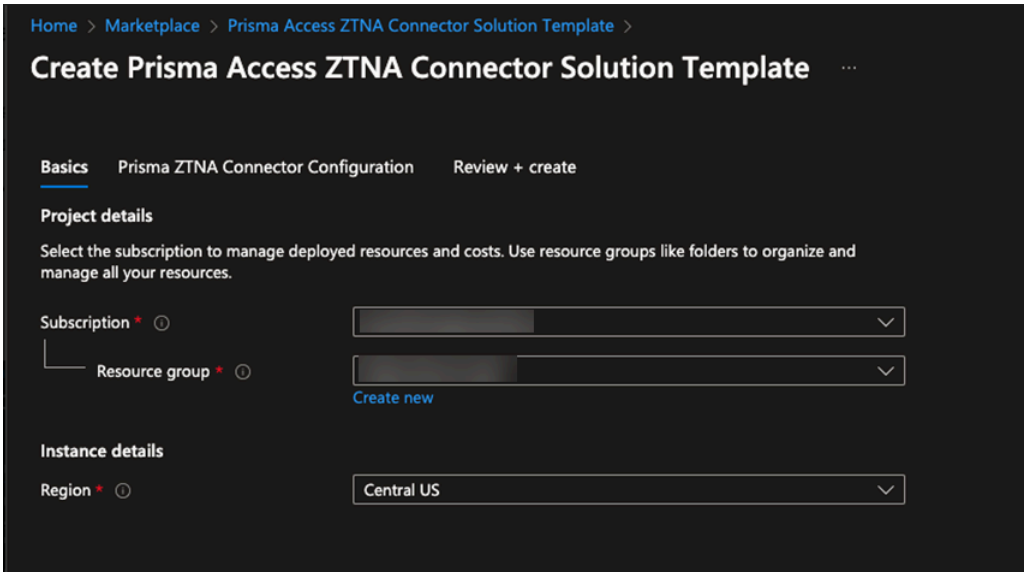
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Una vez completada la implementación, debe **Go to resource (Ir al recurso)**.

Implementar ZTNA Connector de una interfaz de red con escalado automático en Microsoft Azure

STEP 1 | Configure lo siguiente en la pestaña **Basics (Conceptos básicos)**:

- Seleccione su **Subscription (Suscripción)** de Azure para administrar los recursos implementados.
- Seleccione un **Resource Group (Grupo de recursos)** existente o **Create new (Crear uno nuevo)**.
- Seleccione una **Region (Región)** de Azure relevante para su ubicación.
- Haga clic en **Next (Siguiente): Configuración de Prisma ZTNA Connector** .



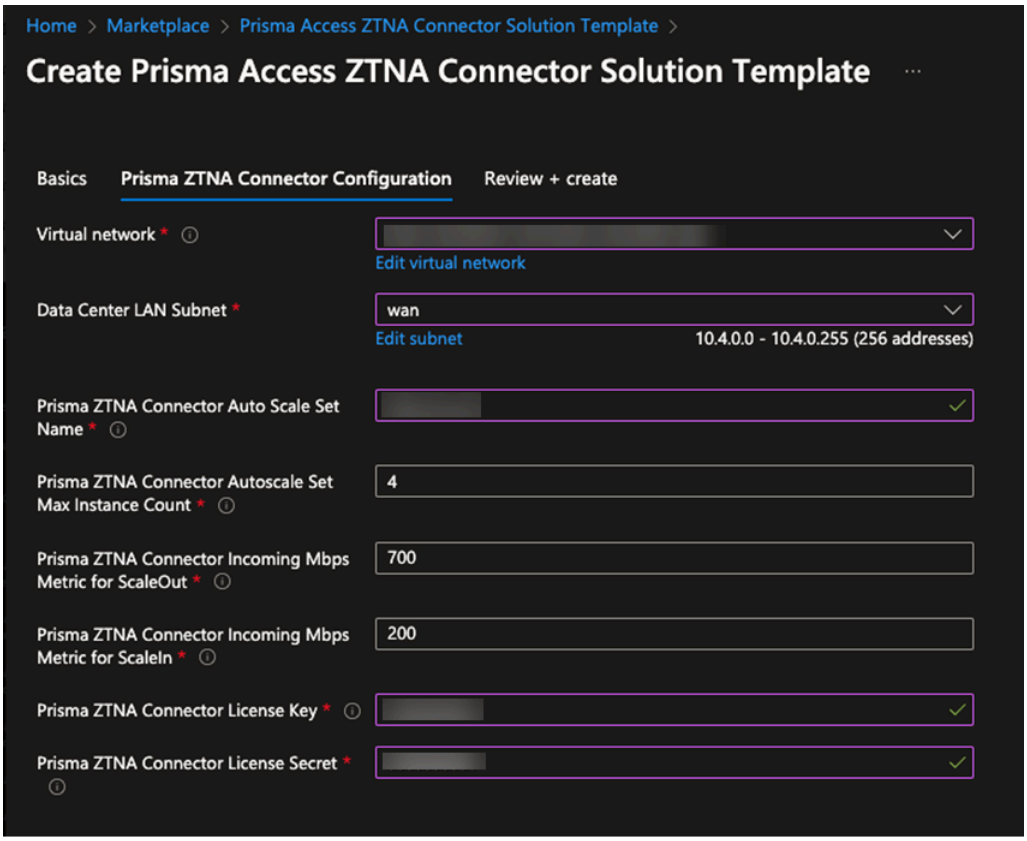
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurar una red virtual en la pestaña **Next (Siguiente): Pestaña de** Configuración de Prisma ZTNA Connector

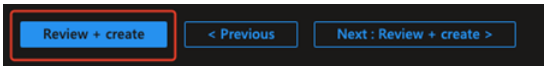
- Seleccione una **Virtual network (Red virtual)** nueva o seleccione una **Virtual network (Red virtual)** existente.
- Seleccione la **Data Center LAN Subnet (Subred LAN del centro de datos)** donde ha aprovisionado aplicaciones para incorporarlas a este conector.
- Introduzca el **Prisma ZTNA Connector Auto Scale Set Name (Nombre del conjunto de escalado automático de Prisma ZTNA Connector)** y especifique el nombre del conjunto de escalado creado en Azure.
- Introduzca el **Prisma ZTNA Connector Autoscale Set Max Instance Count (Recuento máximo de instancias de escalado automático de Prisma ZTNA Connector**. El número máximo de ZTNA Connectors permitidos en el grupo de conectores es 4.
- Introduzca la **Prisma ZTNA Connector Incoming Mbps Metric for ScaleOut (Métrica de Mbps entrantes de Prisma ZTNA Connector para ScaleOut**. Introduzca un valor entre 100 y 1000.
- Introduzca la **Prisma ZTNA Connector Incoming Mbps Metric for ScaleIn (Métrica de Mbps entrante de Prisma ZTNA Connector para ScaleIn**. Introduzca un valor entre 1 y 500.
- Introduzca la **Prisma ZTNA Connector License Key (Clave de licencia de Prisma ZTNA Connector)** y el **Prisma ZTNA Connector License Secret (Secreto de licencia de Prisma**

 ©2025 Palo Alto Networks, Inc.

ZTNA Connector) que recuperó del Portal SASE de Prisma para el grupo de conectores donde desea incorporar el conector.

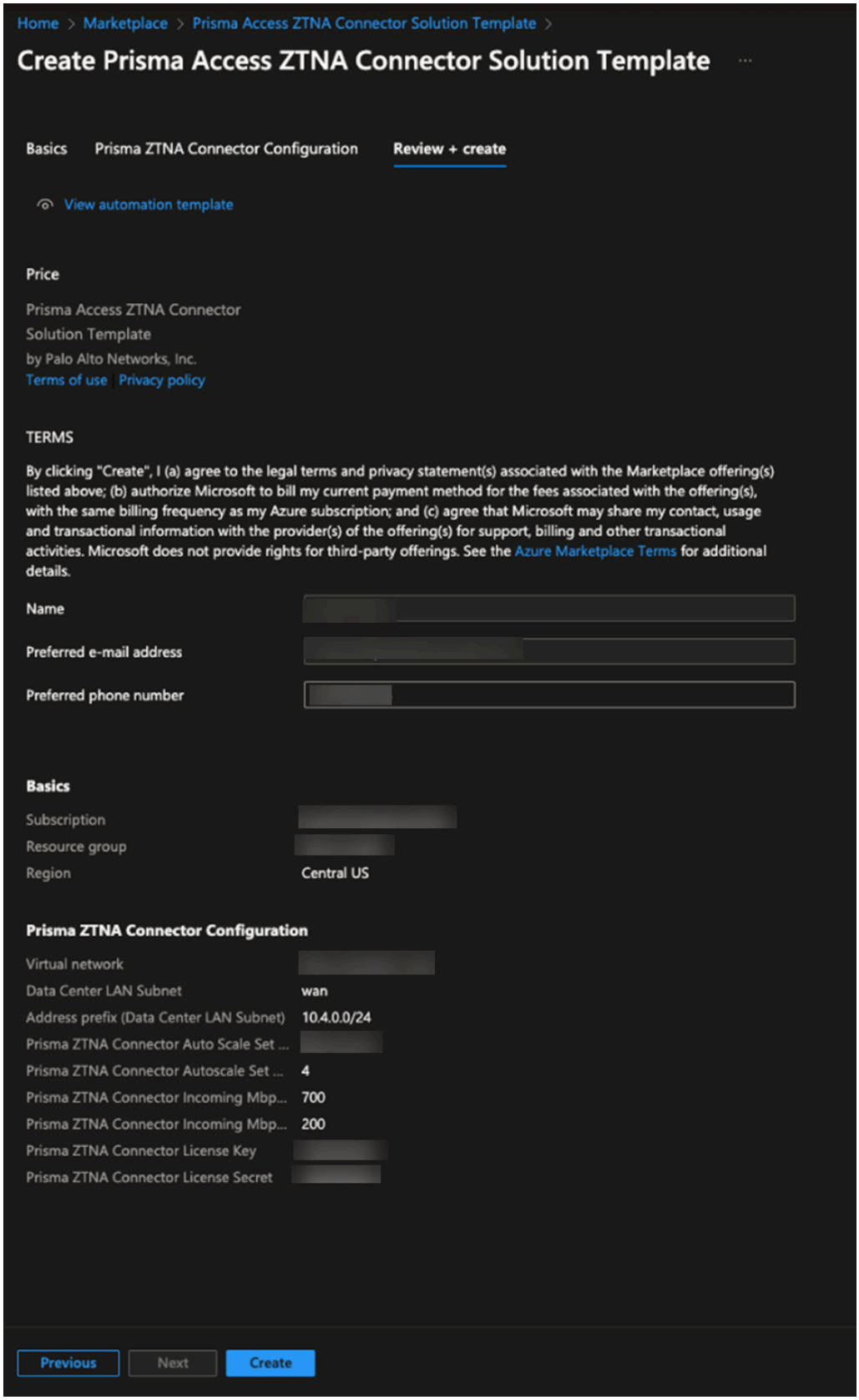


- **Review + create (Revisar + crear)** para revisar su configuración de Prisma ZTNA Connector gestionado.



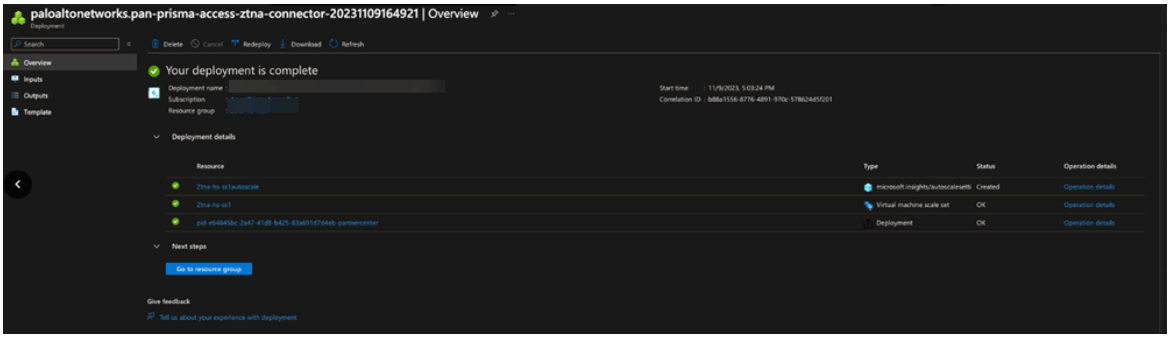
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirme los detalles que ha proporcionado y haga clic en **Create (Crear)** para iniciar la implementación de la máquina virtual.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Una vez completada la implementación, seleccione **Go to resource group (Ir al grupo de recursos)**.

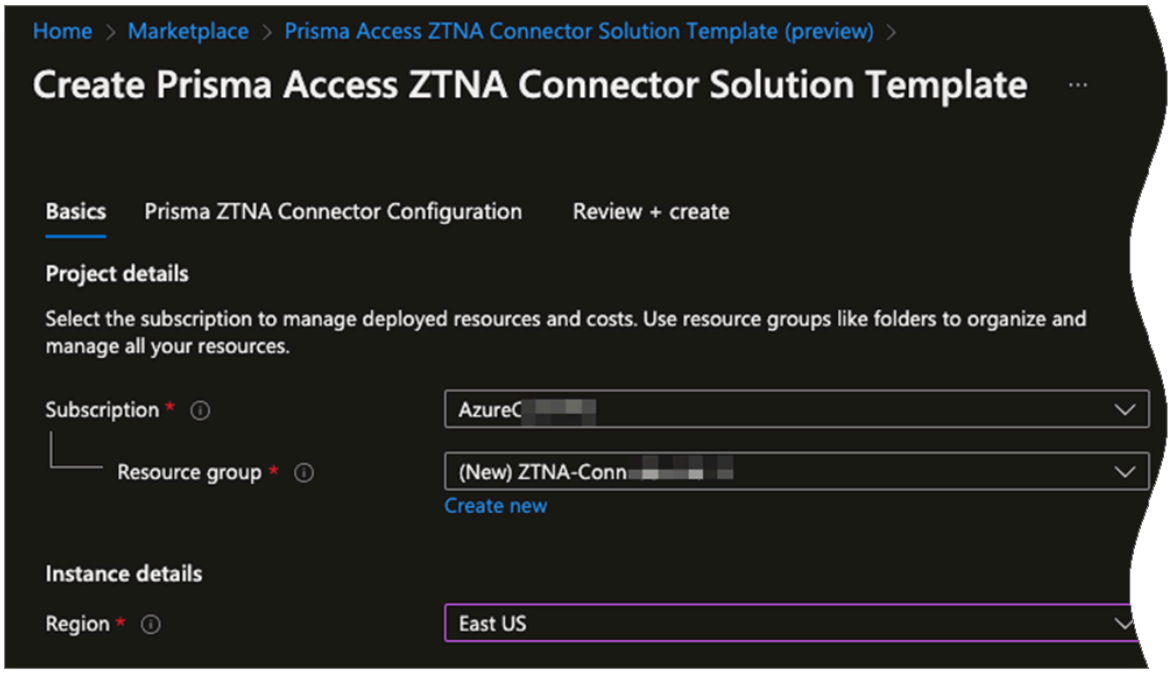


Implementar el ZTNA Connector de dos interfaces de red en Microsoft Azure

Siga estos pasos para implementar el ZTNA Connector de 2 interfaces de red en Microsoft Azure:

STEP 1 | Configure lo siguiente en la pestaña **Basics (Conceptos básicos)**:

- Seleccione su **Subscription (Suscripción)** de Azure para administrar los recursos implementados.
- Seleccione un **Resource Group (Grupo de recursos)** existente o **Create new (Crear uno nuevo)**.
- Seleccione una **Region (Región)** de Azure relevante para su ubicación.
- Haga clic en **Next (Siguiente): Configuración de Prisma ZTNA Connector**.

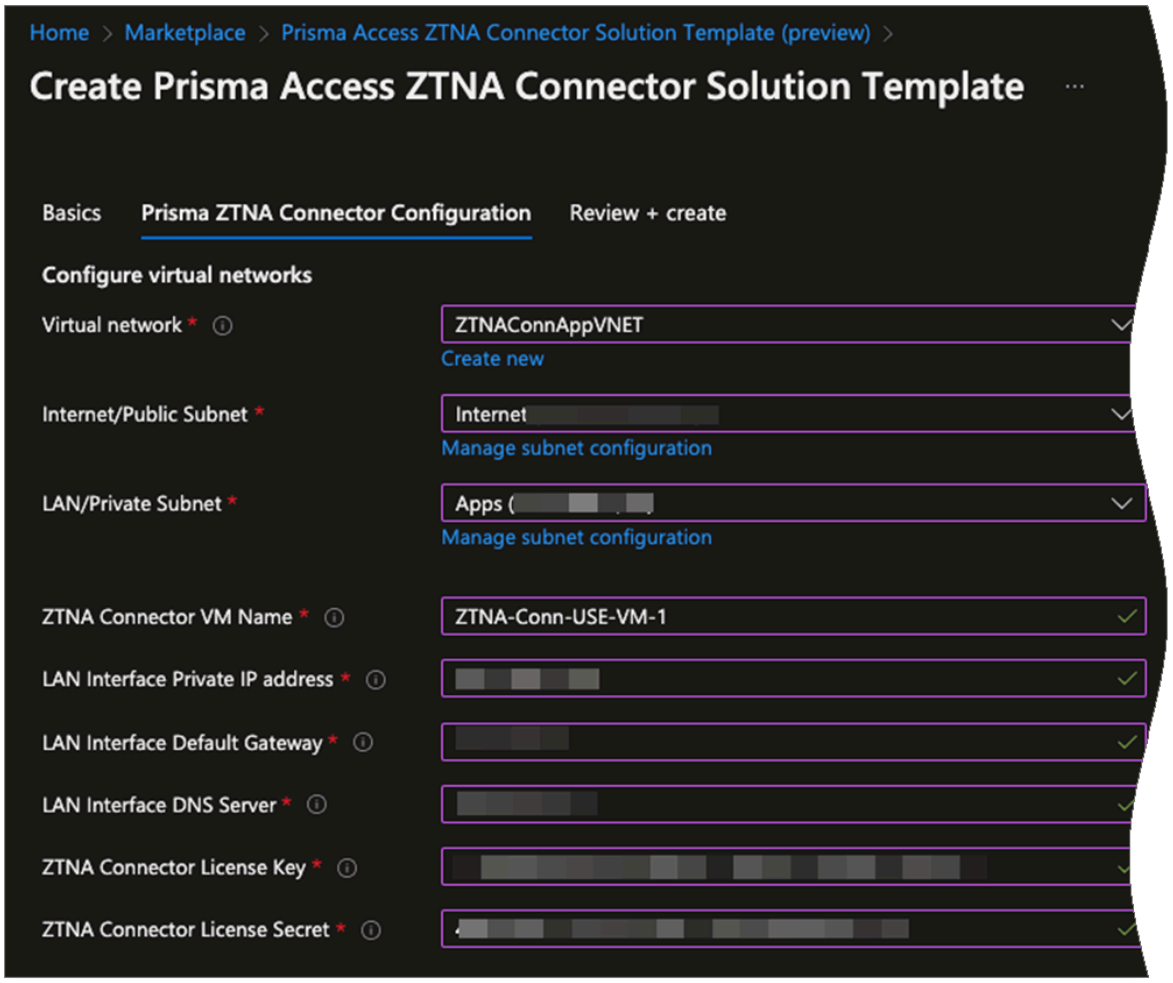


 ©2025 Palo Alto Networks, Inc.

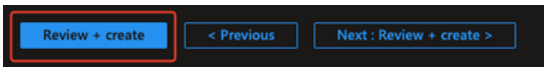
STEP 2 | Configurar una red virtual en la pestaña **Next (Siguiente): Pestaña de** Configuración de Prisma ZTNA Connector

- Cree una nueva **Virtual network (Red virtual** o utilice una **Virtual network (Red virtual)** existente.
- Seleccione **Internet/Public Subnet (Internet/subred pública)** para la conectividad WAN a IPSec. Es necesario tener la subred asociada con una puerta de enlace NAT para la conectividad a Internet.
- Seleccione la **Data Center LAN Subnet (Subred LAN del centro de datos)** donde ha aprovisionado las aplicaciones para incorporarlas a este conector.
- Introduzca el **Prisma ZTNA Connector VM Name (Nombre de la máquina virtual de Prisma ZTNA Connector)**.
- Introduzca la **LAN Interface Private IP address (Dirección IP privada de la interfaz LAN)**.
- Introduzca la dirección IP de la **LAN Interface Default Gateway (Puerta de enlace predeterminada de la interfaz LAN)**.
- Introduzca la dirección IP del **LAN Interface DNS Server (Servidor DNS de la interfaz LAN)**.
- Introduzca los valores **Prisma ZTNA Connector License Key (Clave de licencia de Prisma ZTNA Connector)** y **Prisma ZTNA Connector License Secret (Secreto de licencia de Prisma ZTNA Connector)** que recuperó del Portal SASE de Prisma.

 ©2025 Palo Alto Networks, Inc.



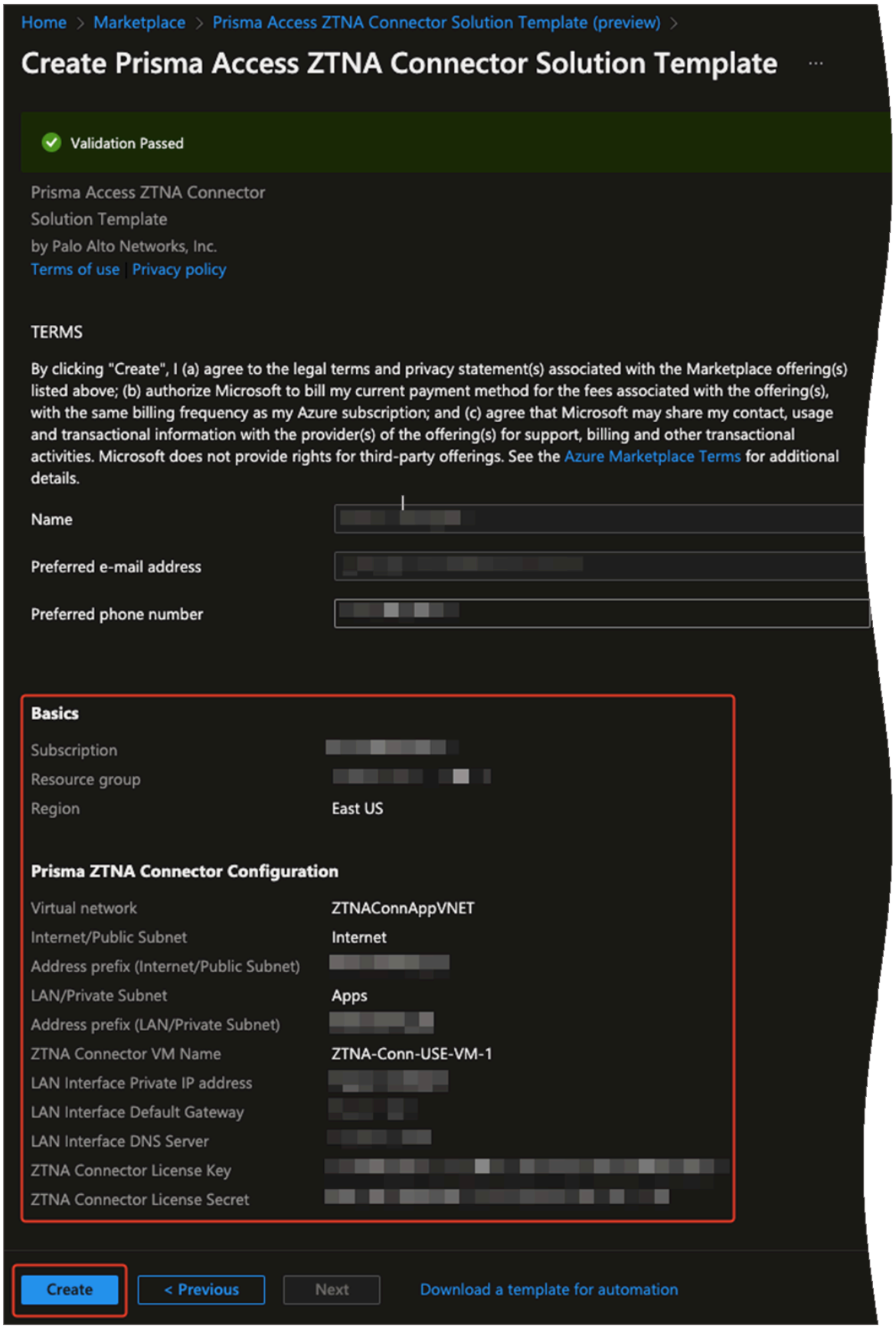
- **Review + create (Revisar + crear)** para revisar su configuración de Prisma ZTNA Connector gestionado.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirme los detalles que ha proporcionado y haga clic en **Create (Crear)** para iniciar la implementación de la máquina virtual.

 ©2025 Palo Alto Networks, Inc.



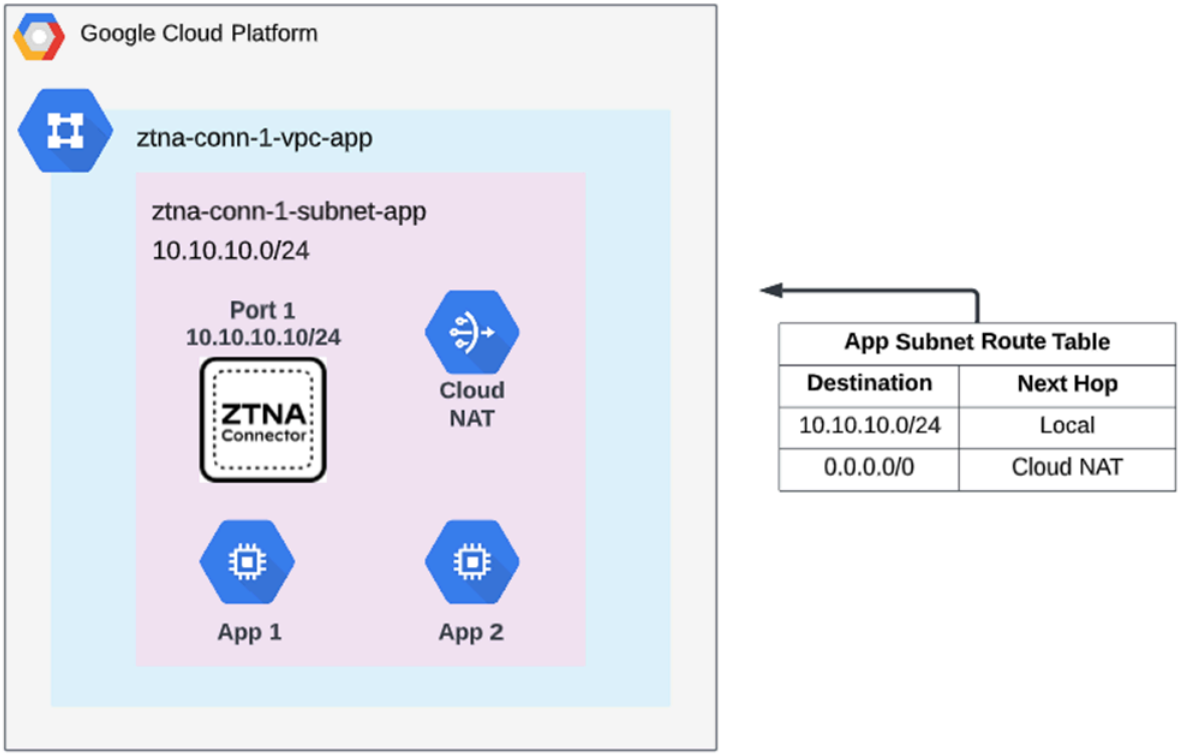
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Una vez completada la implementación, debe **Go to resource (Ir al recurso)**.

Implementaciones de plataforma en Google Cloud compatibles con ZTNA Connector

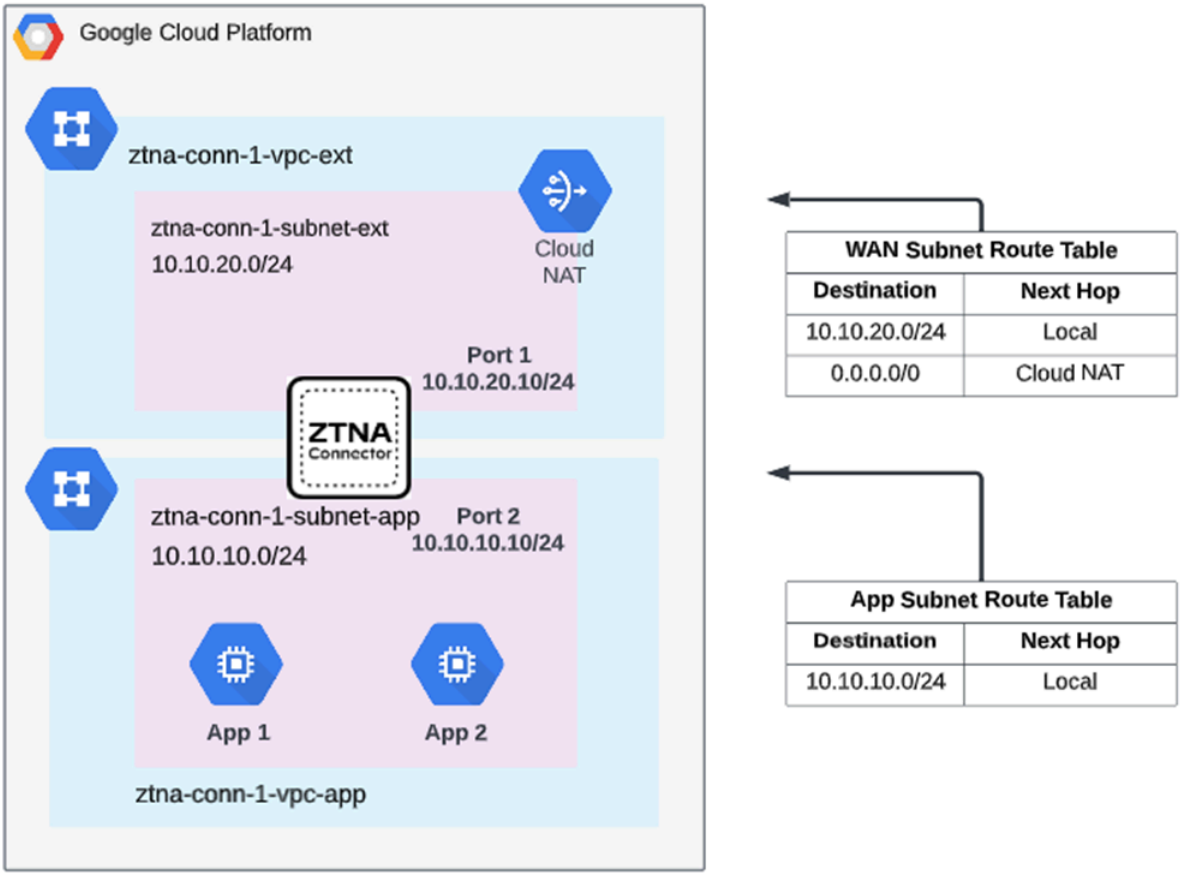
La implementación de red de ZTNA Connector de Prisma Access en Google Cloud Platform (GCP) admite dos implementaciones y una plantilla correspondiente para cada implementación.

En el diagrama siguiente se muestra un ejemplo de implementación del conector ZTNA de Prisma Access en GCP mediante el modo de un brazo con una puerta de enlace de NAT.



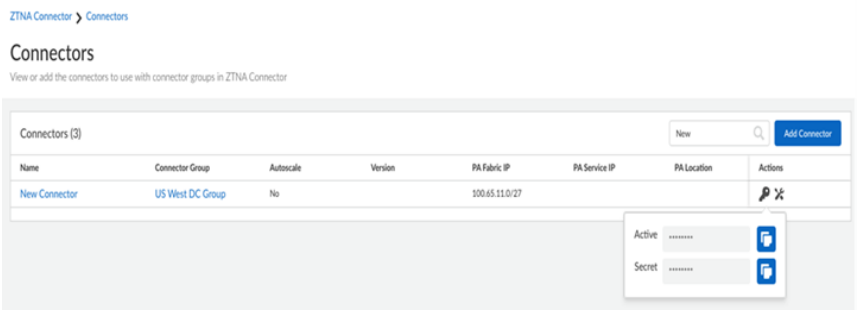
En el siguiente diagrama se muestra un ejemplo de implementación del conector ZTNA de Prisma Access en GCP mediante el modo de dos brazos con una puerta de enlace NAT.

 ©2025 Palo Alto Networks, Inc.



Incorporación de un ZTNA Connector en Google Cloud Platform

- Revise los requisitos y directrices y los FQDN y puertos que necesita configurar para usar Prisma Access ZTNA Connector en Google Cloud Platform (GCP).
- Recupere y copie la clave del conector y los valores clave y secreto en el portal Prisma SASE: **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Conectores**, busque el objeto Conector que creó en Prisma Access para asociar con esta VM, y seleccione **Copy Token (Copiar Token)**; luego, copie los valores de **Key (Clave)** y **Secret (Secreto)**.



Una vez que haya cumplido con todos los requisitos previos, siga estos pasos para incorporar un Prisma Access ZTNA Connector en GCP.

STEP 1 | Vaya a GCP Marketplace (Marketplace de GCP) y busque **Prisma Access ZTNA Connector**.

 ©2025 Palo Alto Networks, Inc.

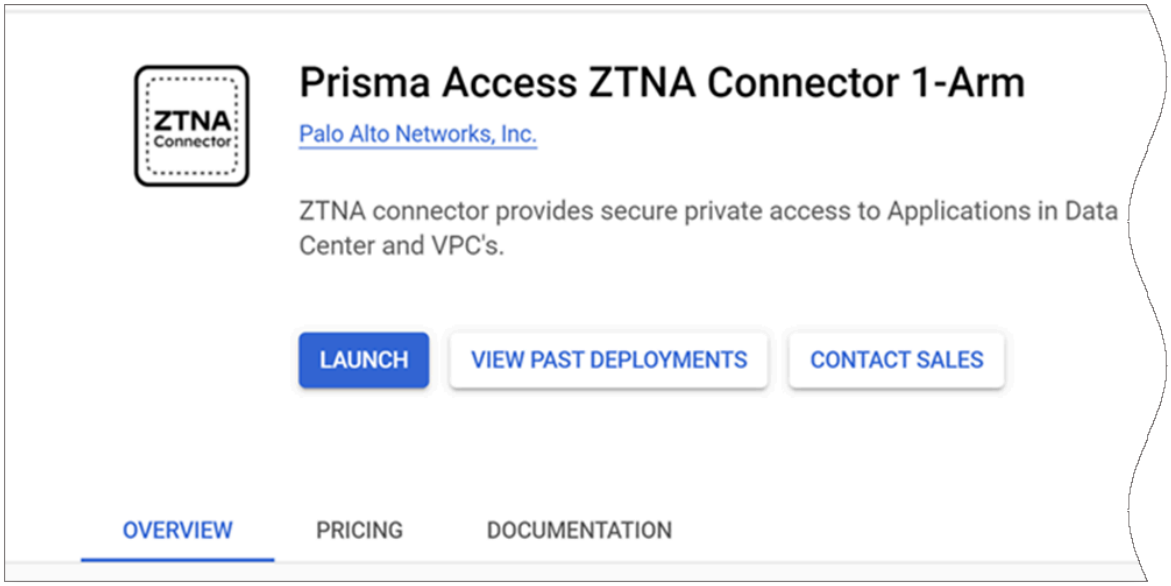
STEP 2 | Elija el plan de software que mejor se adapte a sus necesidades.

- Prisma Access ZTNA Connector de 1 interfaz
- Prisma Access ZTNA Connector 2 interfaces de red

Implementar ZTNA Connector de 1 interfaz en GCP

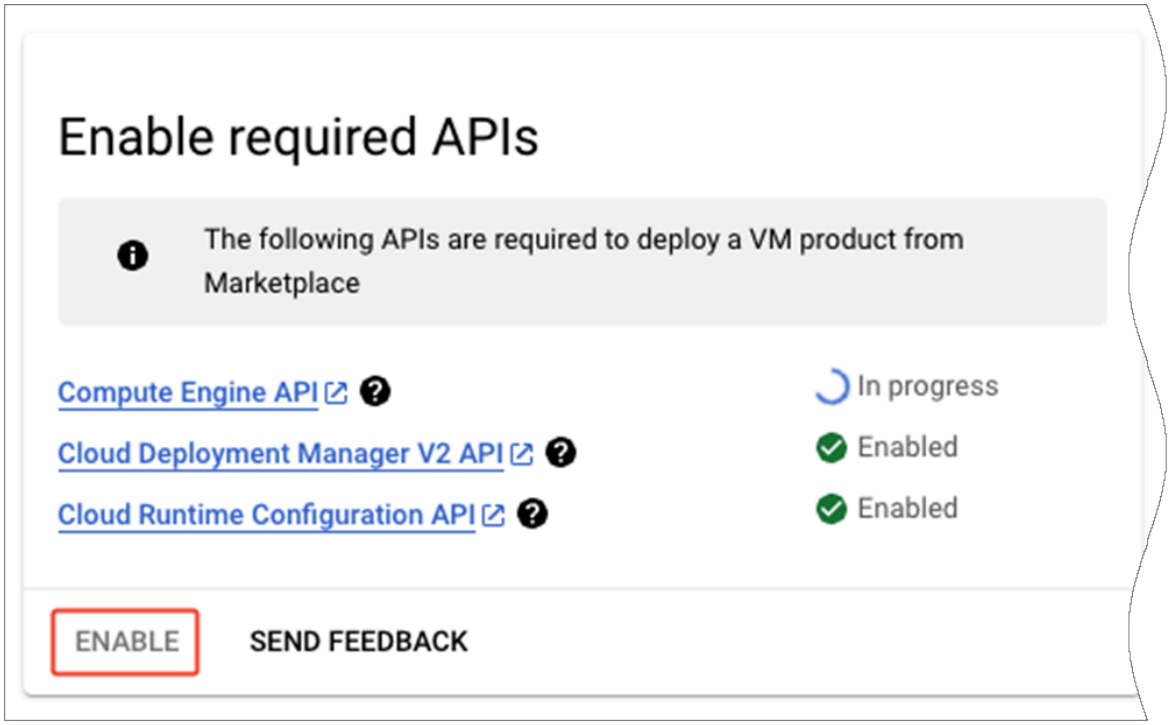
Siga estos pasos para implementar ZTNA Connector de dos interfaces de red en GCP:

STEP 1 | **LAUNCH (INICIAR)** para configurar el ZTNA Connector de 1 interfaz de red.



 ©2025 Palo Alto Networks, Inc.

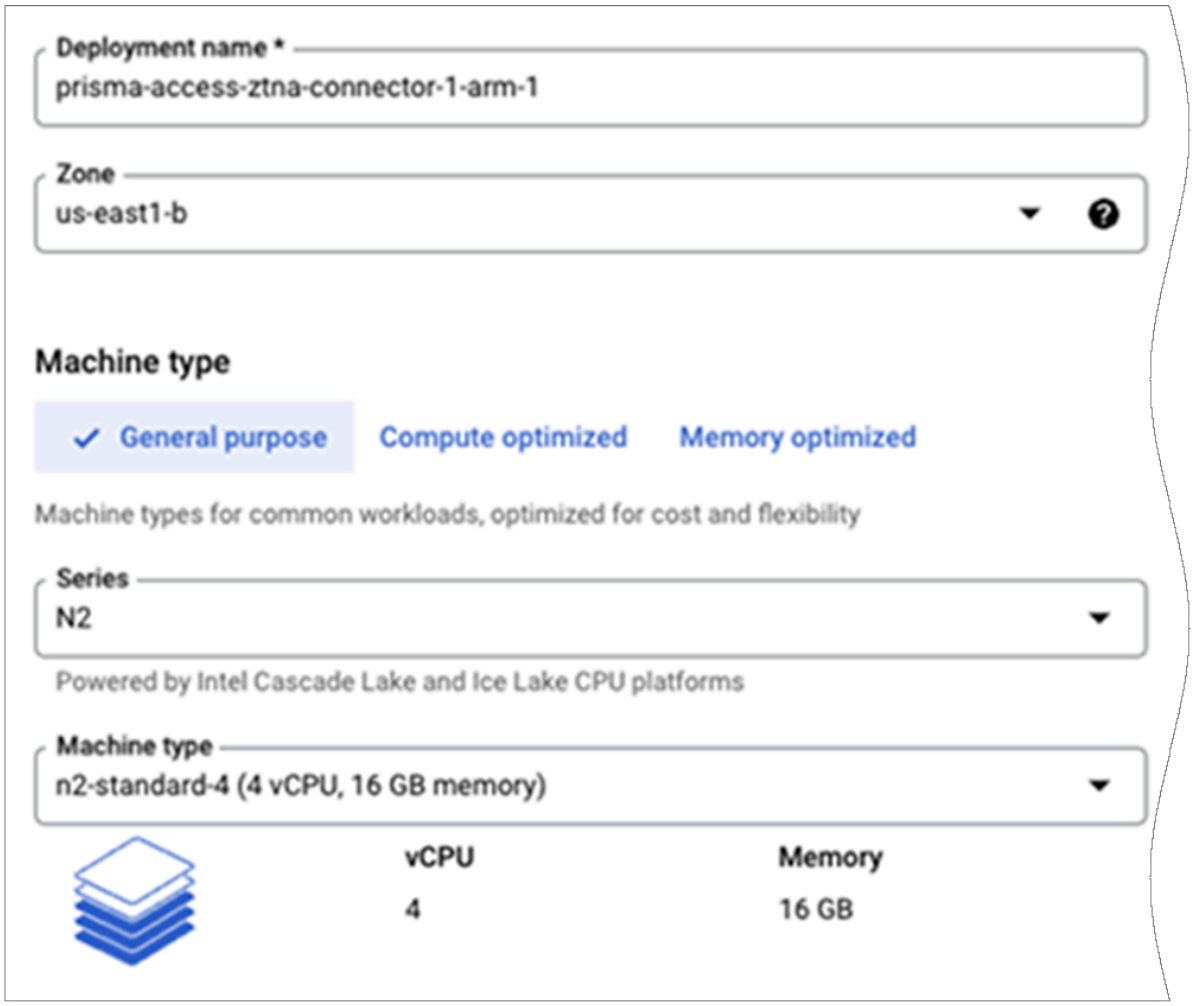
STEP 2 | (Opcional) **Enable (Habilitar)** las API de GCP necesarias para implementar una máquina virtual desde el marketplace.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure lo siguiente:

- Introduzca el **Deployment Name (Nombre de implementación)** que le permite identificar su máquina virtual.
- Seleccione la **Zone (Zona)** donde tiene ubicadas las aplicaciones para este Conector.
- Utilice el valor predeterminado para el **Machine type (Tipo de máquina)**. El tipo de máquina cualificado para este conector es **n2-standard-4**.



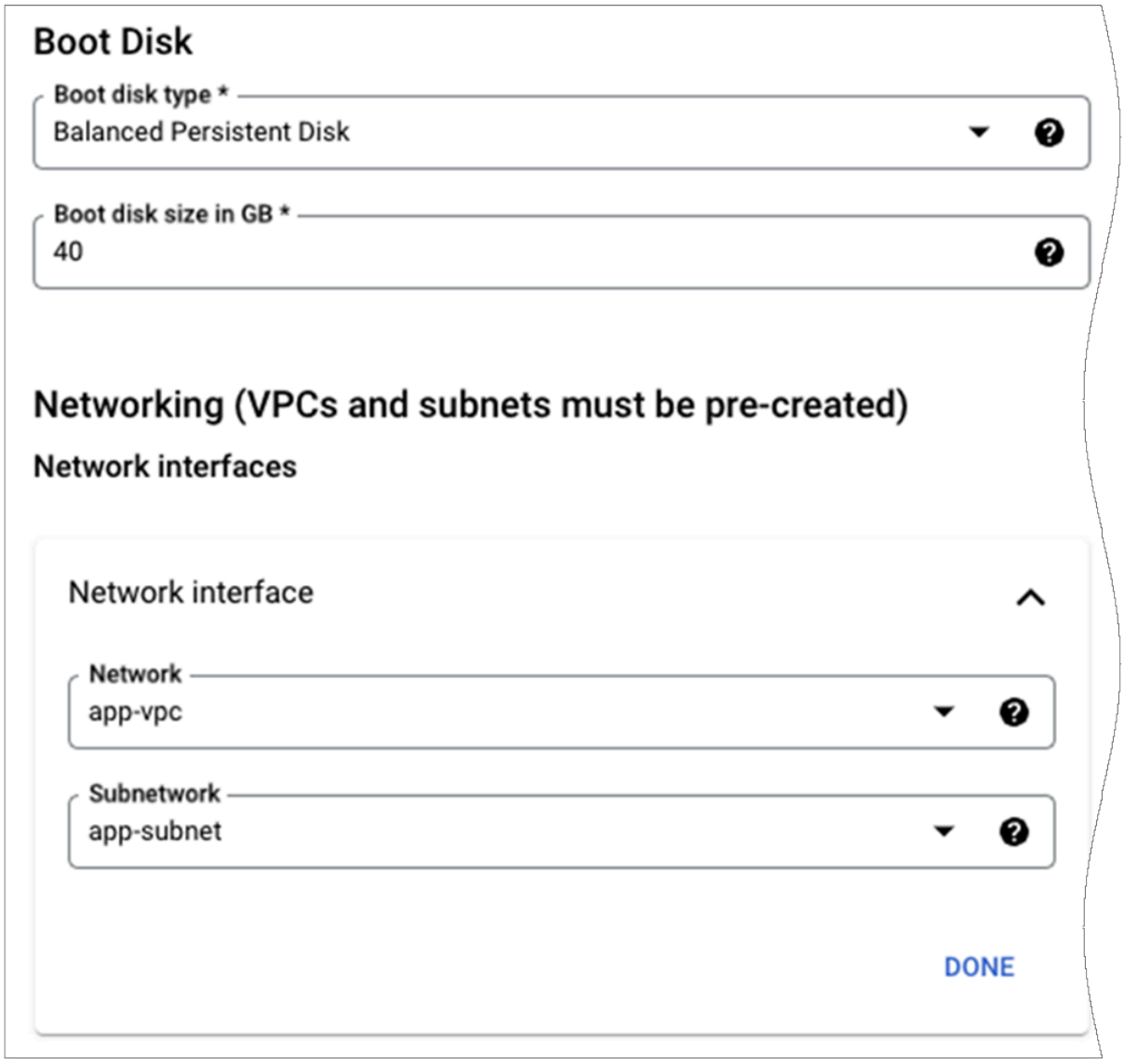
- Introduzca los valores **Prisma ZTNA Connector License Key (Clave de licencia de Prisma ZTNA Connector)** y **Prisma ZTNA Connector License Secret (Secreto de licencia de Prisma ZTNA Connector)** que recuperó del Portal SASE de Prisma.

 ©2025 Palo Alto Networks, Inc.



- Configure lo siguiente en la sección **Boot Disk (Disco de arranque)**:
  - Utilice el **Boot disk type (tipo de disco de arranque)** predeterminado.
  - Seleccione **40 GB** como **tamaño del disco de arranque en GB**.
- Expanda la sección **Networking (VPCs and subnets must be pre-created) [Redes (las VPC y las subredes deben crearse previamente)]** y seleccione los detalles de la **Network interface (Interfaz de red)**.
  - Seleccione la **Network (Red)** que contiene la subred que usted creó.
  - Seleccione la **Subnetwork (Subred)** que utilizará la máquina virtual.

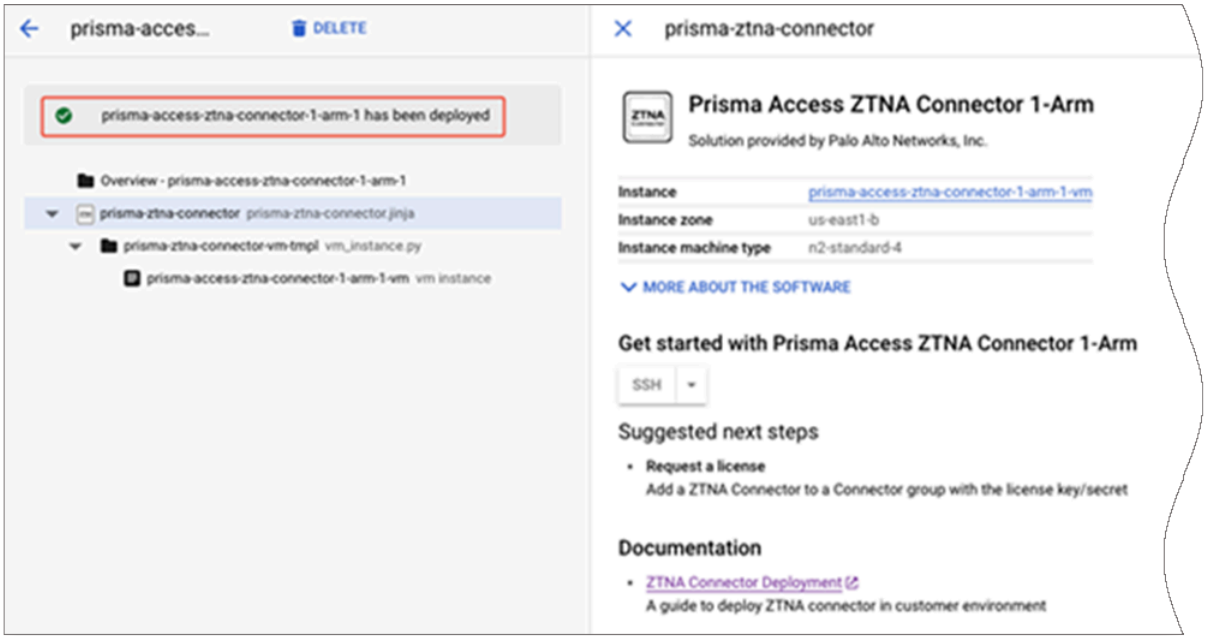
 ©2025 Palo Alto Networks, Inc.



STEP 4 | Haga clic en **Done (Listo)**.

 ©2025 Palo Alto Networks, Inc.

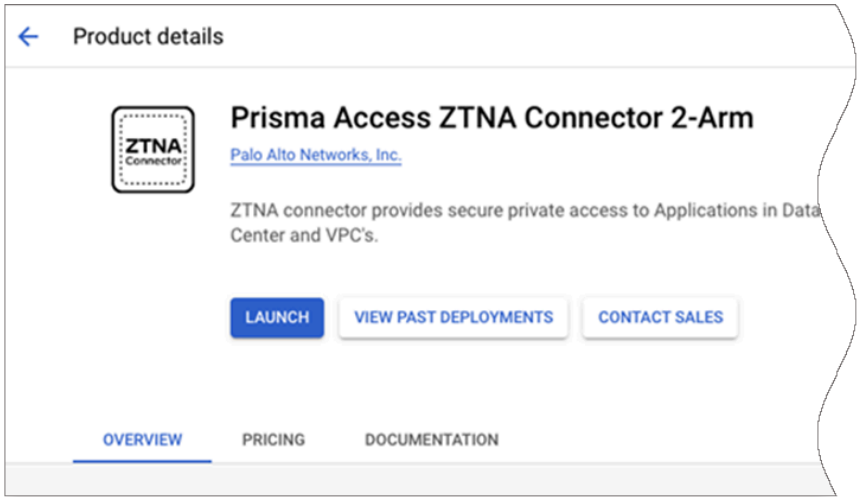
STEP 5 | Haga clic en **Deploy (Implementar)** para completar el proceso de incorporación.



Implementar ZTNA Connector de dos interfaces en GCP

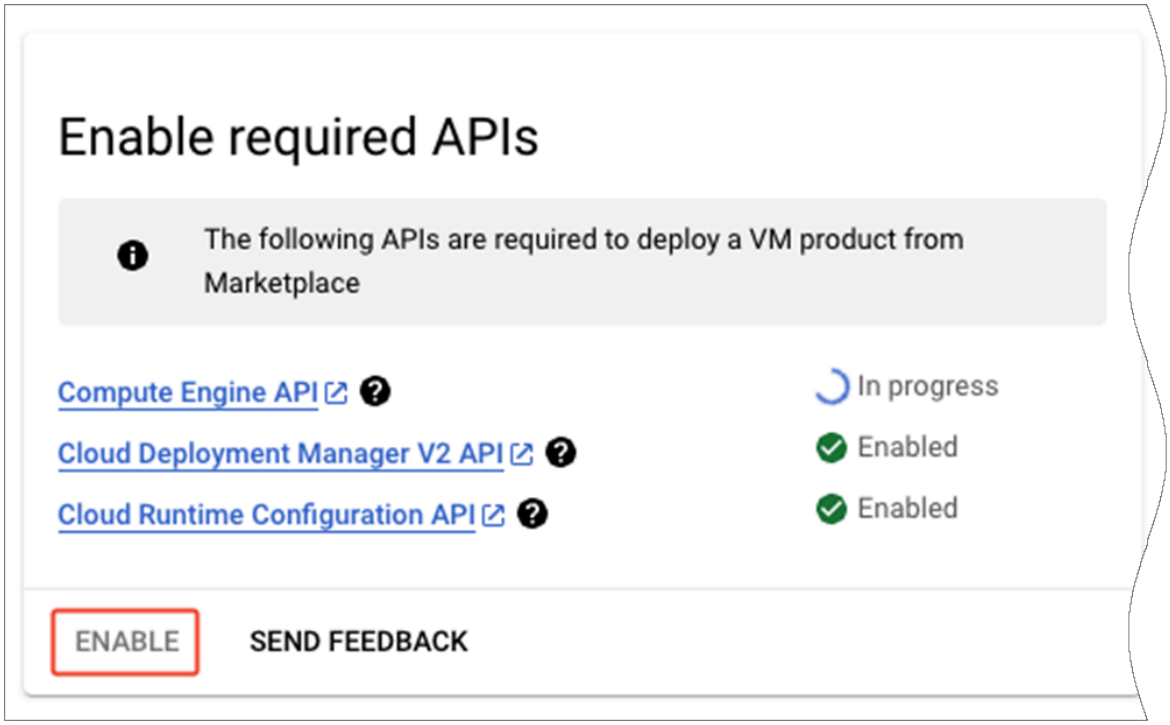
Siga estos pasos para implementar ZTNA Connector en GCP:

STEP 1 | **LAUNCH (INICIAR)** para configurar.



 ©2025 Palo Alto Networks, Inc.

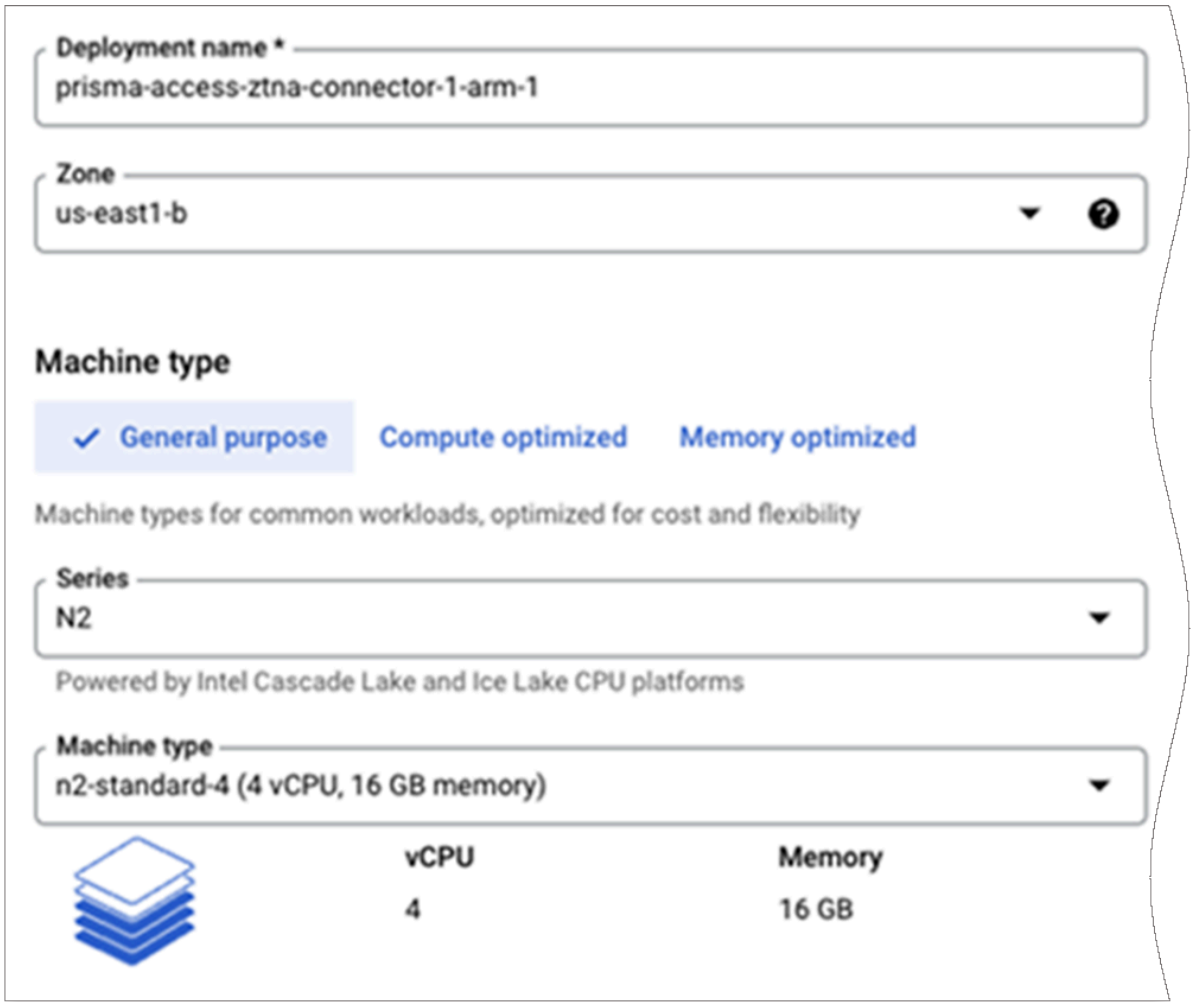
STEP 2 | (Opcional) **Enable (Habilitar)** las API necesarias para implementar una máquina virtual desde el marketplace.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure lo siguiente:

- Introduzca el **Deployment Name (Nombre de implementación)** que le permite identificar su máquina virtual.
- Seleccione la **Zone (Zona)** donde tiene ubicadas las aplicaciones para este Conector.
- Utilice el valor predeterminado para el **Machine type (Tipo de máquina)**. El tipo de máquina cualificado para este conector es **n2-standard-4**.



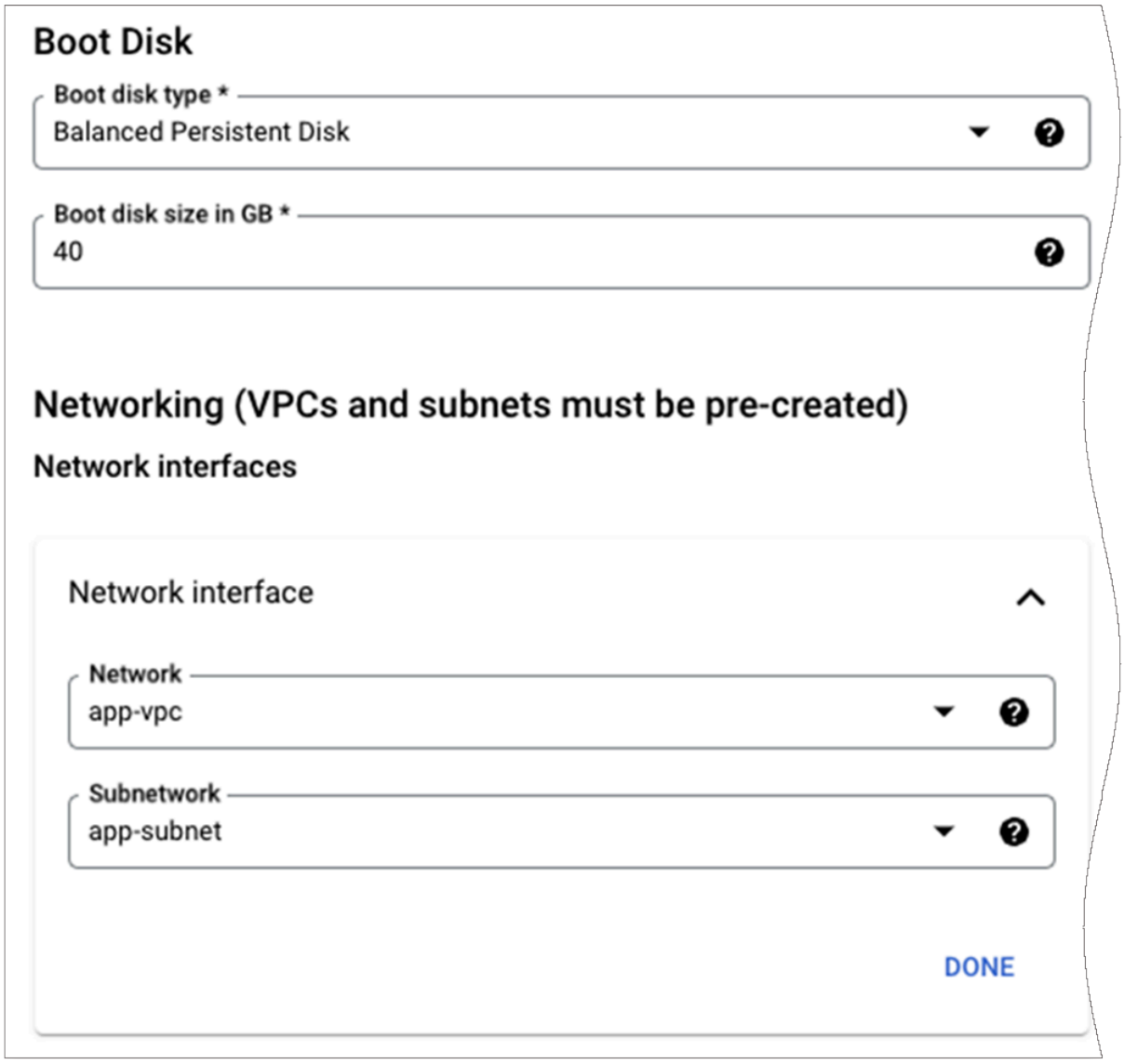
- Introduzca los valores **Prisma ZTNA Connector License Key (Clave de licencia de Prisma ZTNA Connector)** y **Prisma ZTNA Connector License Secret (Secreto de licencia de Prisma ZTNA Connector)** que recuperó del Portal SASE de Prisma.

 ©2025 Palo Alto Networks, Inc.

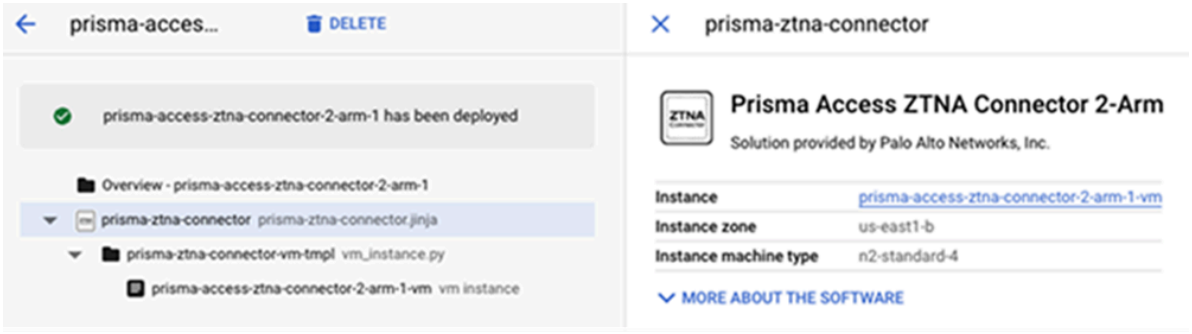


- En la sección **Boot Disk (Disco de arranque)**:
  - Utilice el **Boot disk type (tipo de disco de arranque)** predeterminado.
  - Seleccione **40 GB** como **tamaño del disco de arranque en GB**.
- Expanda la sección **Networking (VPCs and subnets must be pre-created) [Redes (las VPC y las subredes deben crearse previamente)]** y seleccione los detalles de la **Network interface (Interfaz de red)**.
  - Seleccione la **Network (Red)** que contiene la subred que usted creó.
  - Seleccione la **Subnetwork (Subred)** que utilizará la máquina virtual.

 ©2025 Palo Alto Networks, Inc.



STEP 4 | Haga clic en **Deploy (Implementar)** para completar el proceso de incorporación.

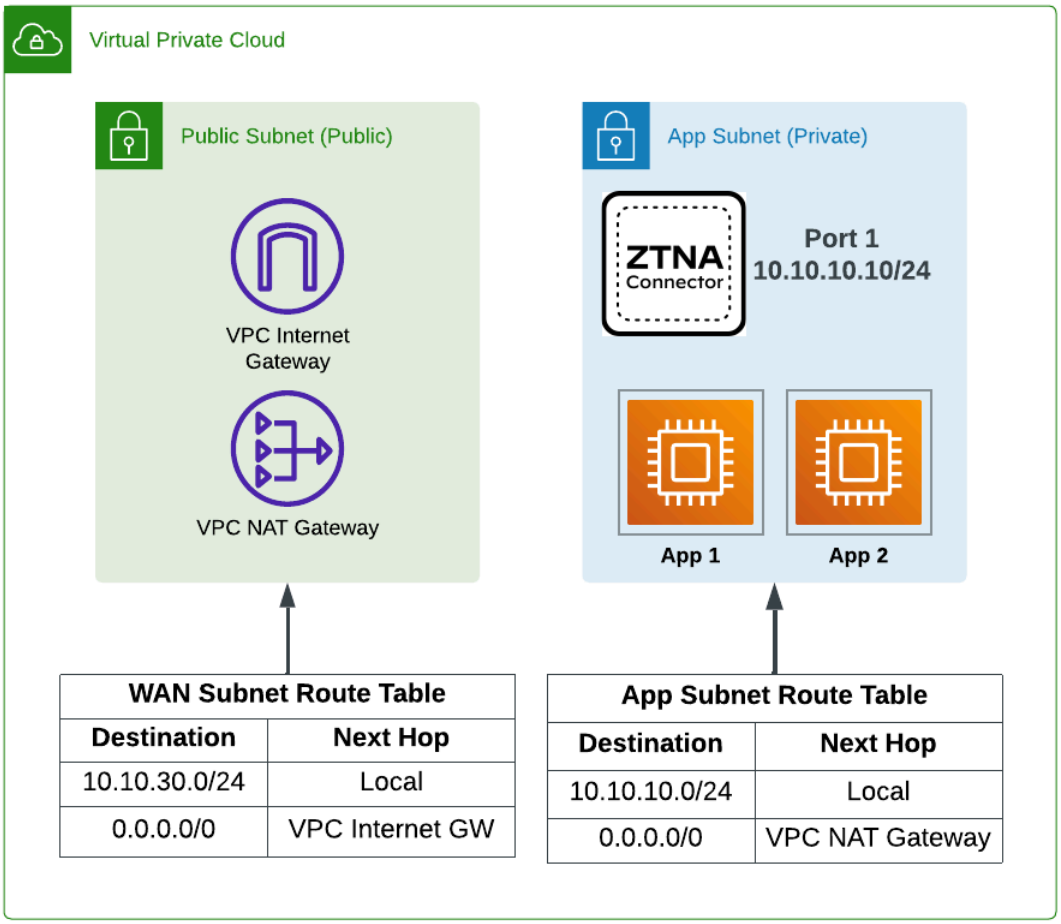


 ©2025 Palo Alto Networks, Inc.

Implementaciones de Amazon Web Services compatibles con el conector ZTNA

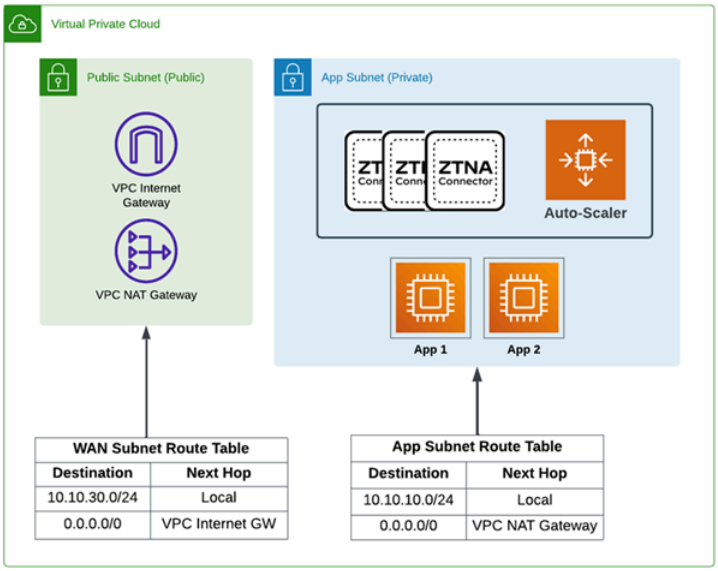
La implementación de red de Prisma Access ZTNA Connector en Amazon Web Services (AWS) admite tres implementaciones y una plantilla correspondiente para cada implementación.

En el diagrama siguiente se muestra un ejemplo de implementación del conector ZTNA en AWS de Prisma Access mediante el modo de un brazo con una puerta de enlace de NAT.

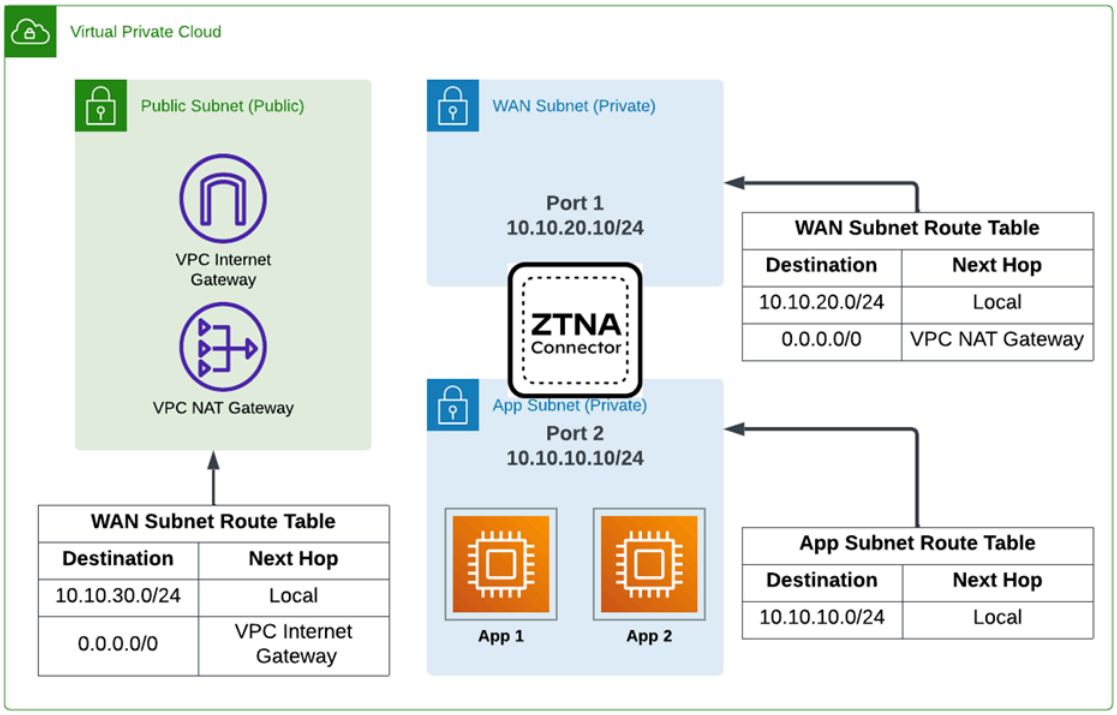


En el siguiente diagrama, se muestra un ejemplo de implementación del conector ZTNA en AWS mediante el escalado automático de un brazo con una puerta de enlace de NAT.

©2025 Palo Alto Networks, Inc.



En el siguiente diagrama se muestra un ejemplo de implementación del conector ZTNA en AWS mediante el modo de dos brazos con una puerta de enlace NAT.

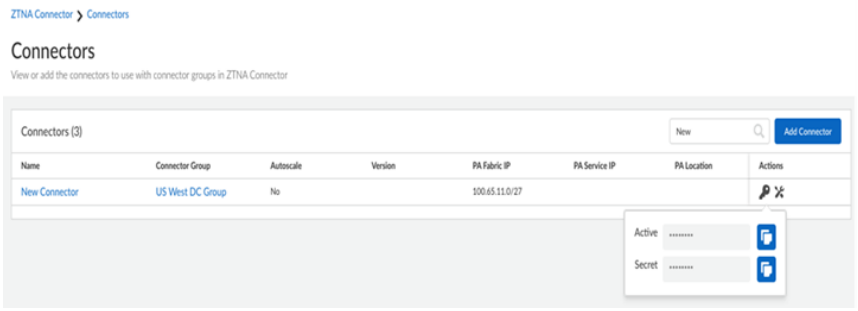


Incorpore un ZTNA Connector en Amazon Web Services

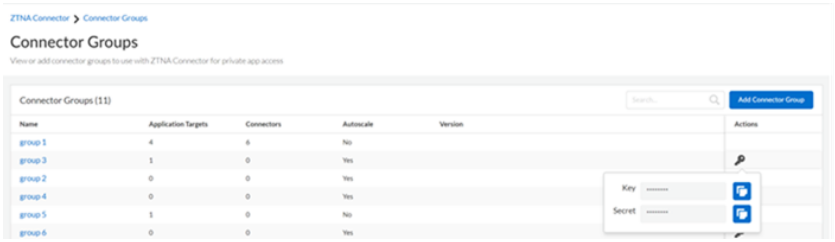
- Revise los requisitos y directrices y los FQDN y puertos que necesita configurar para usar ZTNA Connector en Amazon Web Services (AWS).

©2025 Palo Alto Networks, Inc.

- En la plataforma Prisma SASE, recupere y copie los valores clave y secreto del conector: **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Conectores**, busque el objeto Conector que creó en Prisma Access para asociar con esta VM, y seleccione **Copy Token (Copiar Token)**; luego, copie los valores de **Key (Clave)** y **Secret (Secreto)**.



- Para la **Implementación de escalado automático de 1 interfaz de red de Prisma Access ZTNA Connector**, debe recuperar y copiar la clave y los valores Secreto y Clave del grupo de conectores: **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connector Groups (Grupos de conectores)**, busque el objeto Grupo de conectores que creó en Prisma Access para asociar con esta VM y seleccionar **Copy Token (Copiar Token)**; luego, copie la **Key (Clave)** y el **Secret (Secreto)**.



Una vez que haya cumplido con todos los requisitos previos, siga estos pasos para incorporar un Prisma Access ZTNA Connector en AWS.

STEP 1 | Vaya a AWS Marketplace y busque **Prisma Access ZTNA Connector**.

STEP 2 | Elija el plan de software que mejor se adapte a sus necesidades.

- Prisma Access ZTNA Connector de 1 interfaz
- Prisma Access ZTNA Connector de 1 interfaz con escalado automático
- Prisma Access ZTNA Connector 2 interfaces de red

Implementar el ZTNA Connector de 1 interfaz en AWS

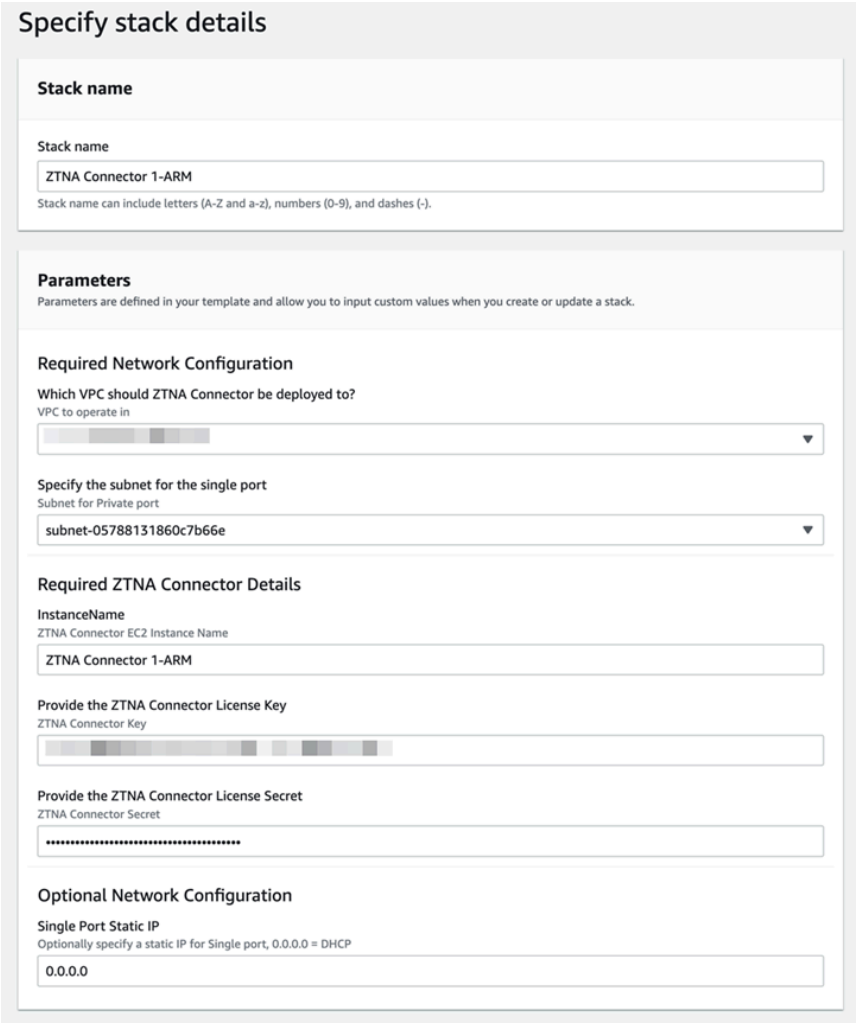
Siga estos pasos para implementar ZTNA Connector de una interfaz de red en AWS.

STEP 1 | Seleccione la plantilla de CloudFormation de **Prisma Access ZTNA Connector 1-Arm (Prisma Access ZTNA Connector de una interfaz de red)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configúrelos en la página **Specify stack details (Especificar detalles de la pila)**:

- Introduzca el **Stack name (Nombre de la pila)** para identificarla.
- En la sección **Parameters (Parámetros)**, especifique los parámetros definidos en la plantilla de pila.
  - Seleccione **Which VPC should ZTNA Connector be deployed to (En qué VPC se debe implementar ZTNA Connector)**.
  - **Specify the subnet for the single port (Especificar la subred para el puerto único)**, donde ha aprovisionado aplicaciones para incorporar a este conector. Debe tener acceso a Internet desde esta subred a través de una puerta de enlace NAT.
- Introduzca los valores **ZTNA Connector License Key (Clave de licencia de ZTNA Connector)** de Prisma y **ZTNA Connector License Secret (Secreto de licencia de Prisma ZTNA Connector)** de Prisma que recuperó del Portal SASE de Prisma.



Implementar ZTNA Connector de una interfaz de red con escalado automático en AWS

Siga estos pasos para implementar ZTNA Connector de 1 interfaz de red con escalado automático en AWS.

 ©2025 Palo Alto Networks, Inc.

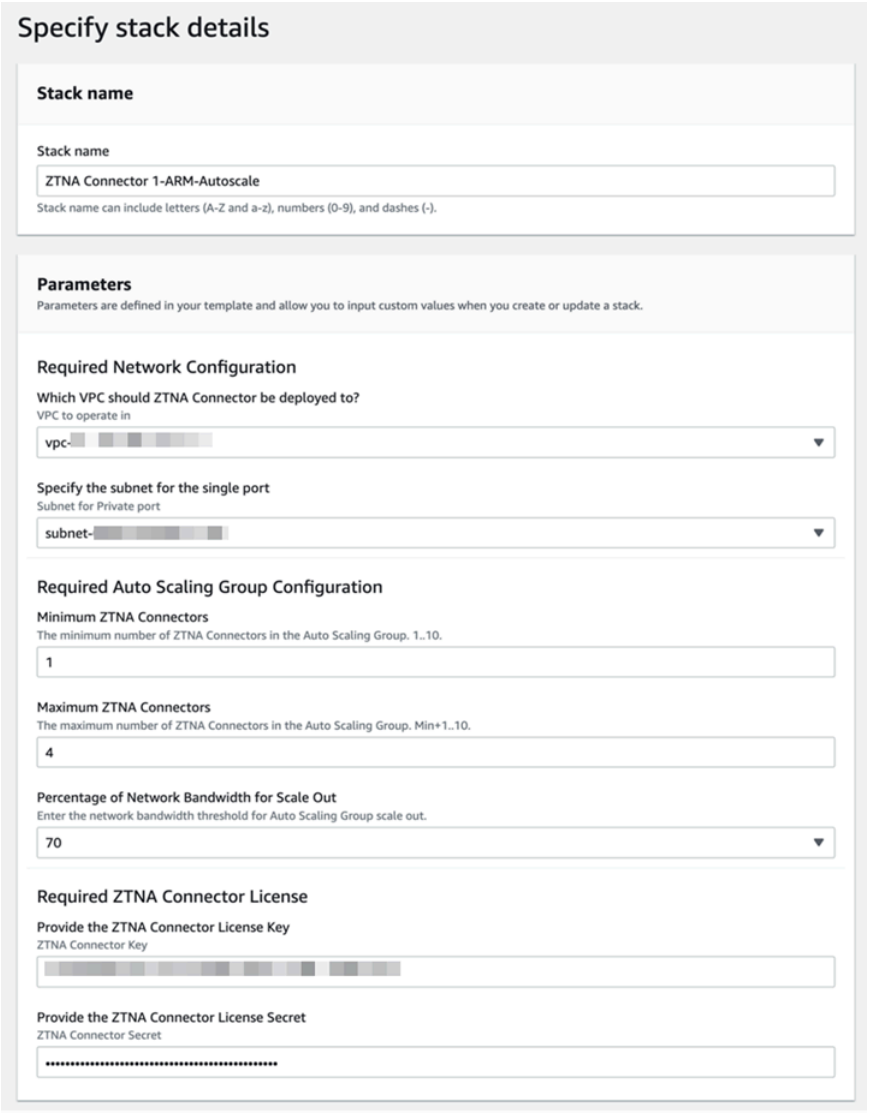
STEP 1 | Seleccione la plantilla de CloudFormation **Prisma Access ZTNA Connector 1-Arm Auto-Scaling (Prisma Access ZTNA Connector con escalado automático y una interfaz de red)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configure estos parámetros en la página **Specify stack details (Especificar detalles de la pila)**:

- Introduzca el **Stack name (Nombre de pila)** único para la implementación.
- Especifique los parámetros definidos en la plantilla de pila en la sección **Parameters (Parámetros)**:
  - Seleccione **Which VPC should ZTNA Connector be deployed to (En qué VPC se debe implementar ZTNA Connector)**.
  - **Specify the subnet for the single port (Especificar la subred para el puerto único)**, donde ha aprovisionado aplicaciones para incorporar a este conector. Debe tener acceso a Internet desde esta subred a través de una puerta de enlace NAT.
- En la **Required Auto Scaling Group Configuration (Configuración requerida del grupo de escalado automático)**:
  - Introduzca los **Minimum ZTNA Connectors (ZTNA Connectors mínimos)** requeridos en el grupo de escalado automático.
  - Introduzca los **Maximum ZTNA Connectors (ZTNA Connectors máximos)** requeridos en el grupo de escalado automático. El número máximo de ZTNA Connectors permitidos en el grupo de conectores es 4.
  - Establezca el **Percentage of Network Bandwidth for Scale Out (Porcentaje de ancho de banda de red para escalado horizontal)**. El valor predeterminado y recomendado es 70 %.
- Introduzca los valores **ZTNA Connector License Key (Clave de licencia de ZTNA Connector)** de Prisma y **ZTNA Connector License Secret (Secreto de licencia de ZTNA Connector)** de Prisma que recuperó del Portal SASE de Prisma.

 ©2025 Palo Alto Networks, Inc.



Implementar el ZTNA Connector de 2 interfaces en AWS

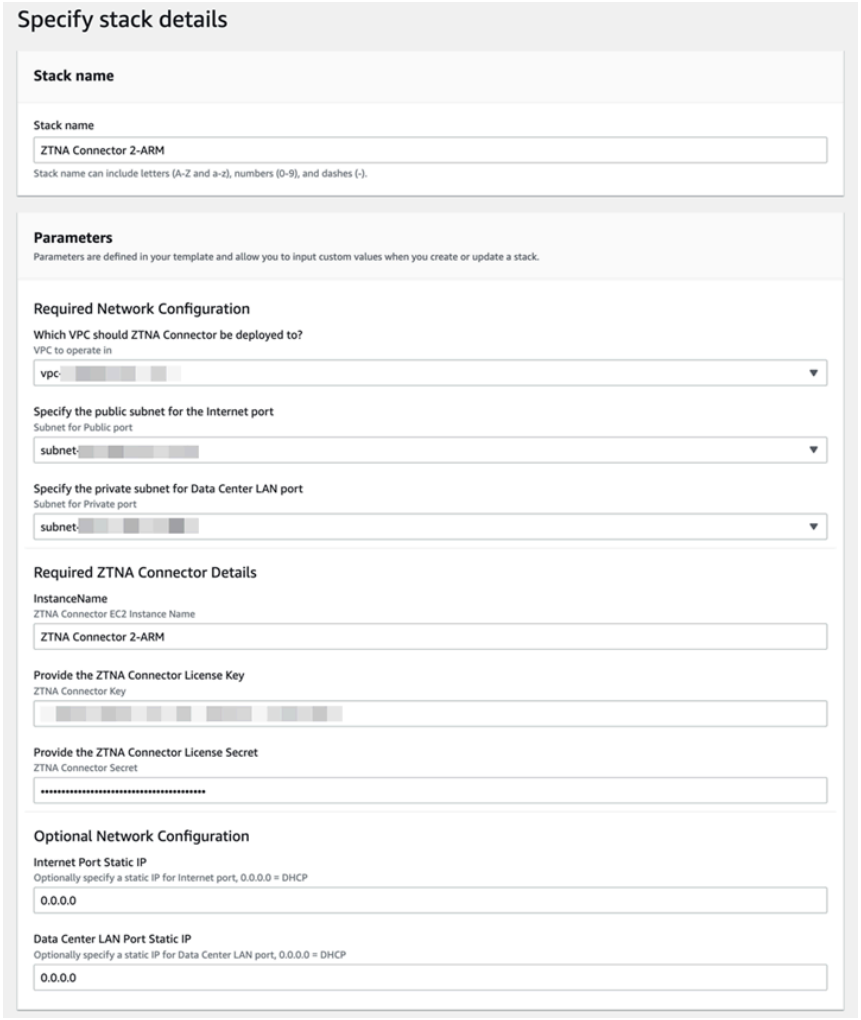
Siga estos pasos para implementar ZTNA Connector de dos interfaces de red en AWS.

STEP 1 | Seleccione la plantilla de CloudFormation de implementación de Prisma Access ZTNA Connector de una interfaz de red.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | En la página **Especificar detalles de la pila**:

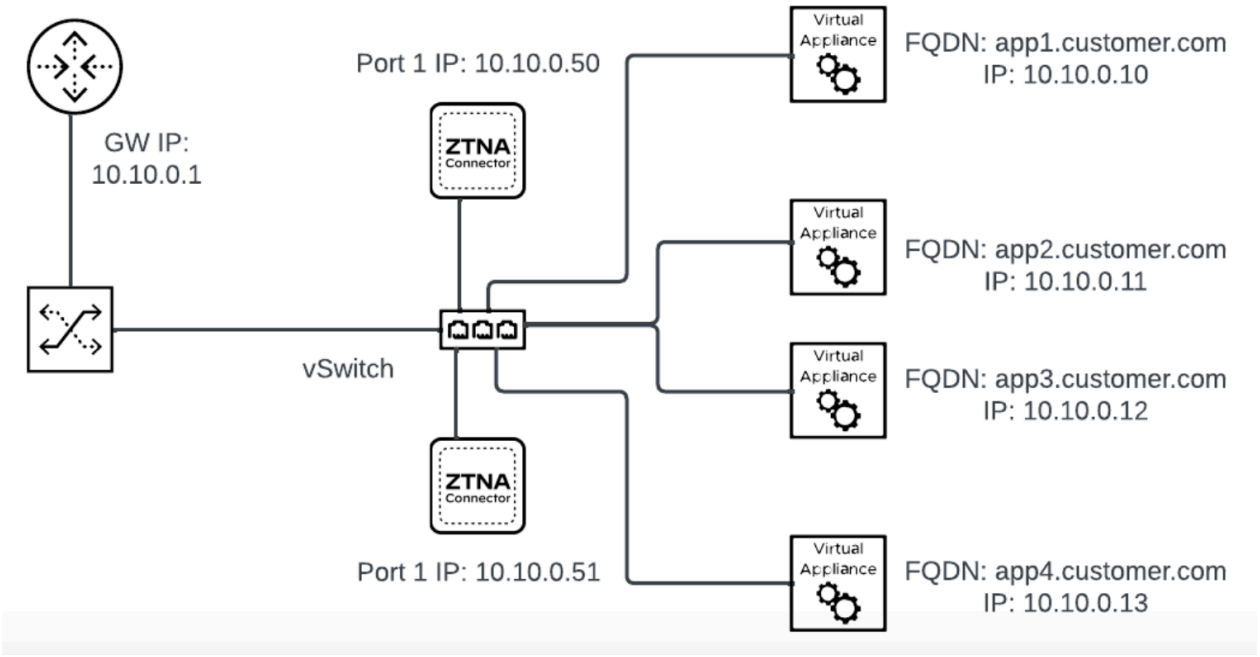
- Introduzca el **Stack name (Nombre de la pila)** para la implementación.
- Especifique los parámetros definidos en su plantilla de pila en la sección **Parameters (Parámetros)** .
  - Seleccione **Which VPC should ZTNA Connector be deployed to (En qué VPC se debe implementar ZTNA Connector)**.
  - **Specify the public subnet for the Internet port (Especifique la subred pública para el puerto de Internet)** para la conectividad WAN a IPSec. Esta subred debe estar asociada a una puerta de enlace NAT para poder conectarse a Internet.
  - **Specify the private subnet for Data Center LAN port (Especificar la subred privada para el puerto LAN del centro de datos**, donde ha aprovisionado aplicaciones para incorporar a este conector.
- Introduzca el **Instance Name (Nombre de la instancia)**
- Introduzca los valores **ZTNA Connector License Key (Clave de licencia de ZTNA Connector)** de Prisma y **ZTNA Connector License Secret (Secreto de licencia de Prisma ZTNA Connector)** de Prisma que recuperó del Portal SASE de Prisma.



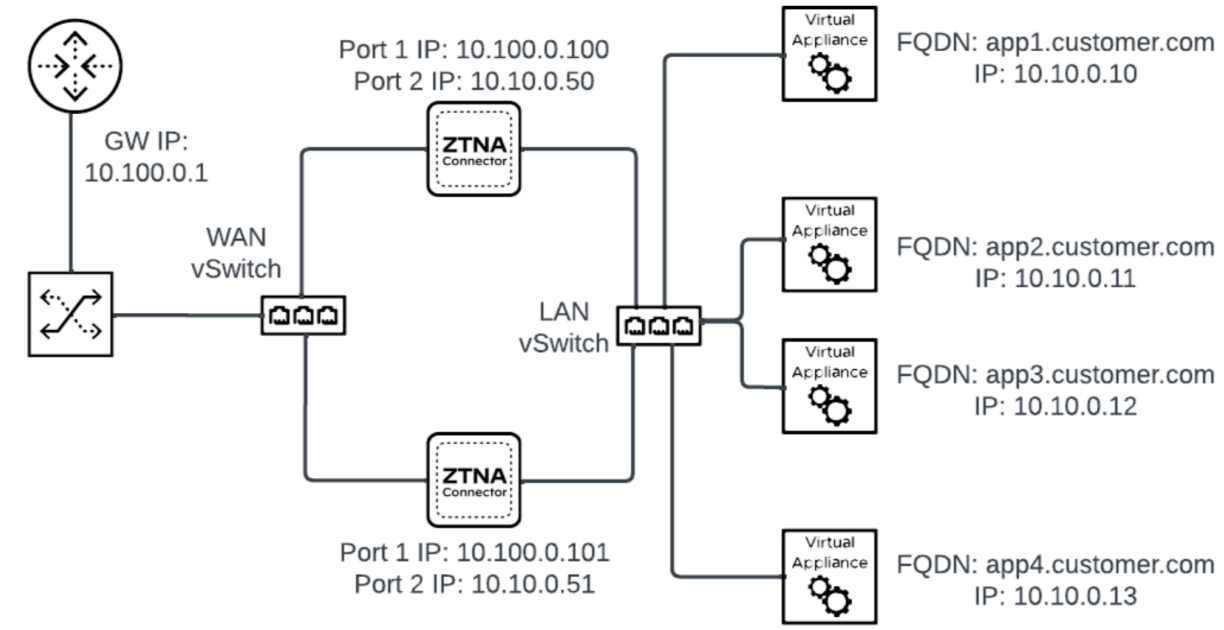
 ©2025 Palo Alto Networks, Inc.

Implementaciones de VMware ESXi compatibles con Prisma Access ZTNA Connector

El siguiente diagrama muestra una implementación de red de ZTNA Connector de ejemplo utilizando VMware ESXi en modo de una interfaz con una puerta de enlace NAT.



El siguiente diagrama muestra una implementación de red de ZTNA Connector de ejemplo utilizando VMware ESXi en modo de dos interfaces con una puerta de enlace NAT.



 ©2025 Palo Alto Networks, Inc.

Integrar un ZTNA Connector en VMware ESXi

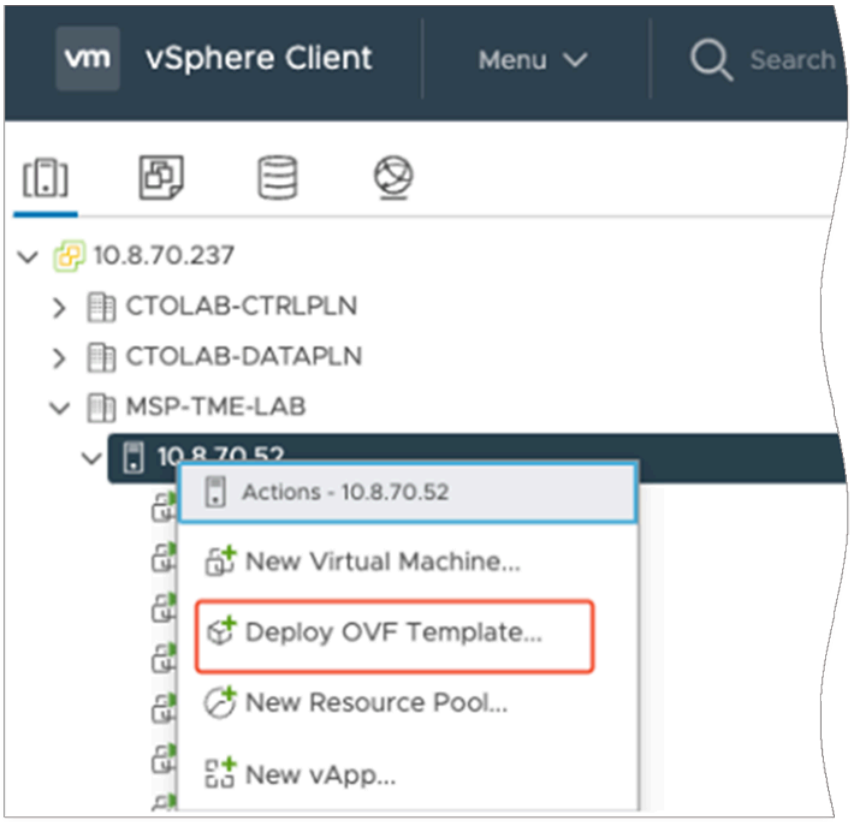
Para incorporar un ZTNA Connector en VMware ESXi, complete los siguientes pasos. Antes de comenzar, asegúrese de revisar los requisitos y directrices para ZTNA en general y las implementaciones de VMware ESXi en particular.

Antes de comenzar, revise los requisitos y directrices, así como los FQDN y los puertos que necesita configurar para usar ZTNA Connector con VMware ESXi.

STEP 1 | Descargue la imagen ZTNA Connector VMware ESXi desde el Portal de atención al cliente (CSP) en **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** > **Prisma Access ZTNA Connector for VMware (Prisma Access ZTNA Connector para VMware)**.

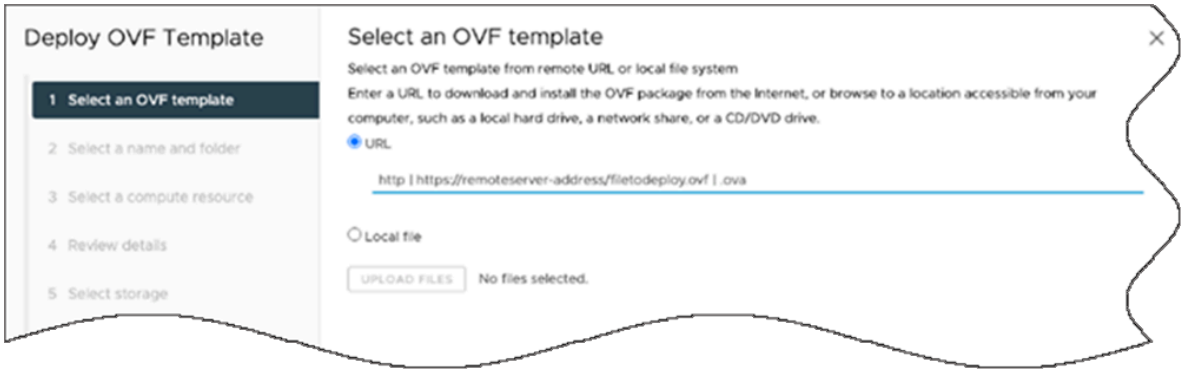
Descargue un archivo de versión 1-nic para implementación de una interfaz de red y un archivo de versión 2-nic para implementación de dos interfaces de red.

STEP 2 | Abra VMware vCenter, seleccione y haga clic con el botón derecho en el host y seleccione **Deploy OVF Template (Implementar plantilla OVF)**.

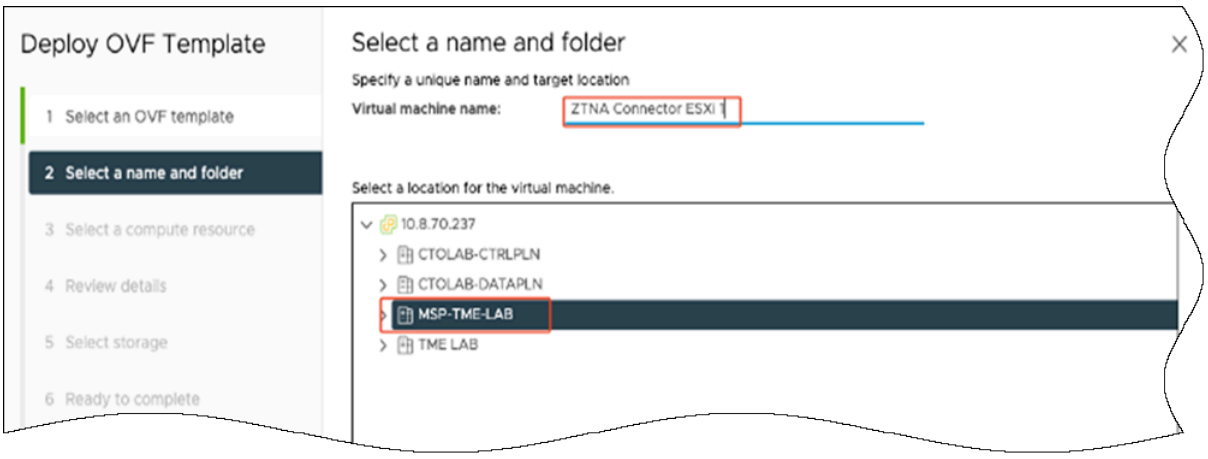


 ©2025 Palo Alto Networks, Inc.

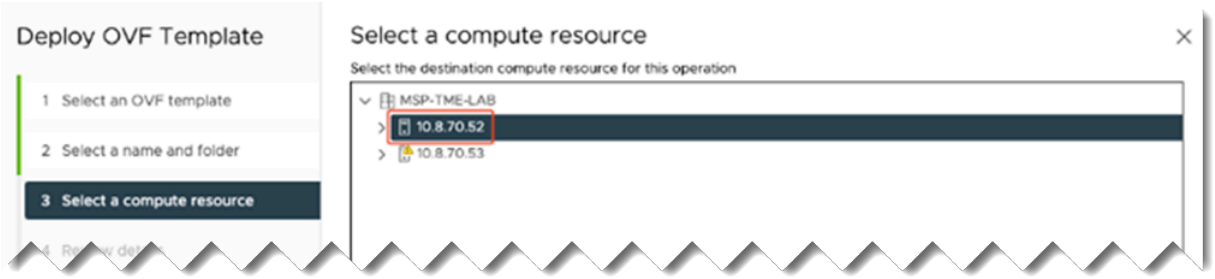
STEP 3 | Seleccione la ubicación de Connector OVA (ya sea una URL o un archivo local) y seleccione **Next (Siguiente)**.



STEP 4 | Introduzca un nombre de máquina virtual (VM) y una ubicación para la VM.

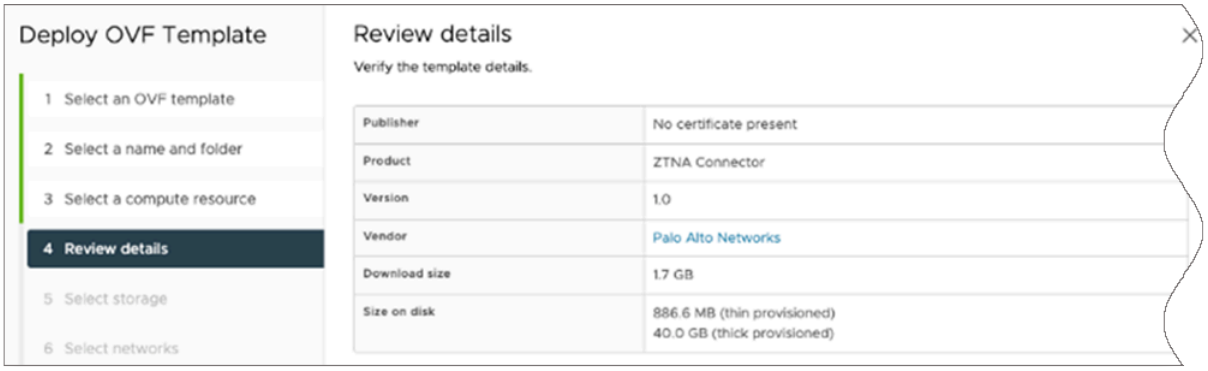


STEP 5 | Seleccione el recurso de cómputo para la VM.

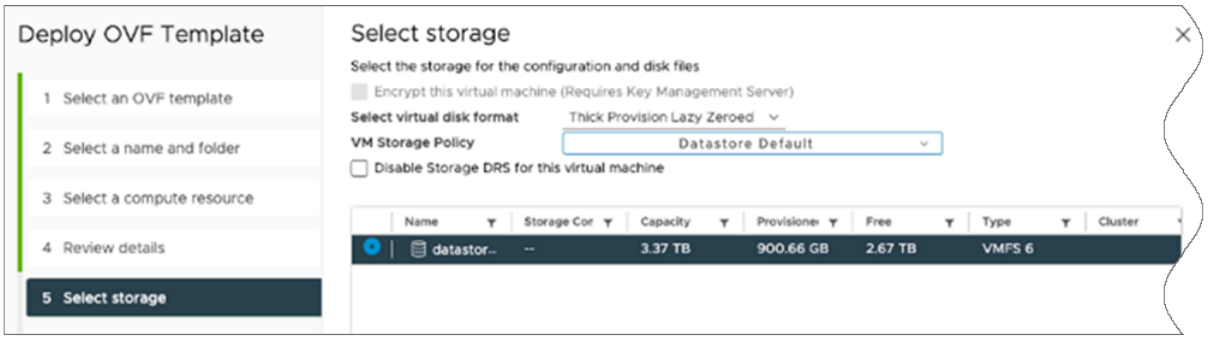


 ©2025 Palo Alto Networks, Inc.

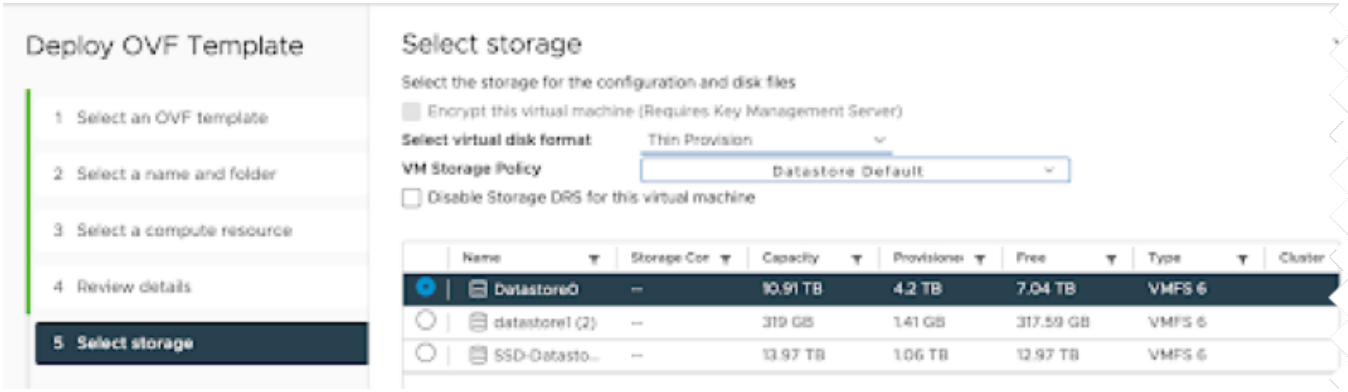
STEP 6 | Revise los detalles de la plantilla y seleccione **Next (Siguiente)**.



STEP 7 | Seleccione **Thick Provision Lazy Zeroed (Suministro estándar diferido a cero)** para el formato de disco virtual y el almacén de datos apropiado para la VM de ZTNA Connector.



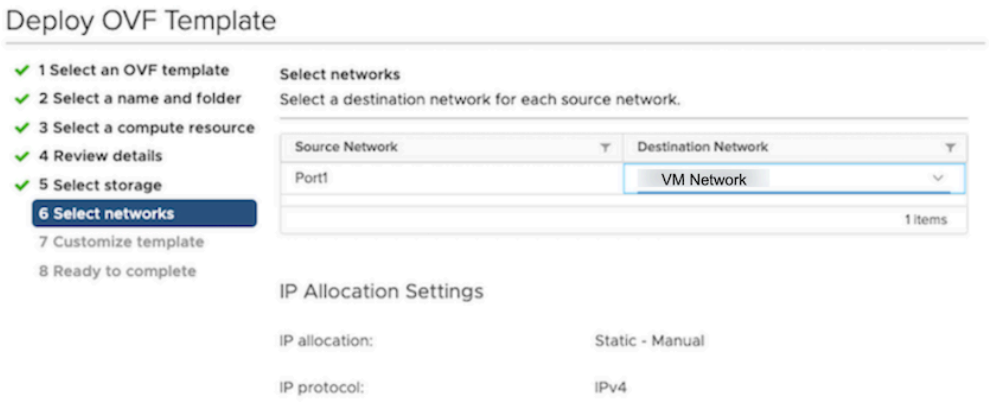
Opcional: Seleccione **Thin Provision (Aprovisionamiento fino)** para el formato de disco virtual y el almacén de datos apropiado para la máquina virtual del ZTNA Connector, donde, según el requisito, el servidor solo asigna el espacio que requiere el host.



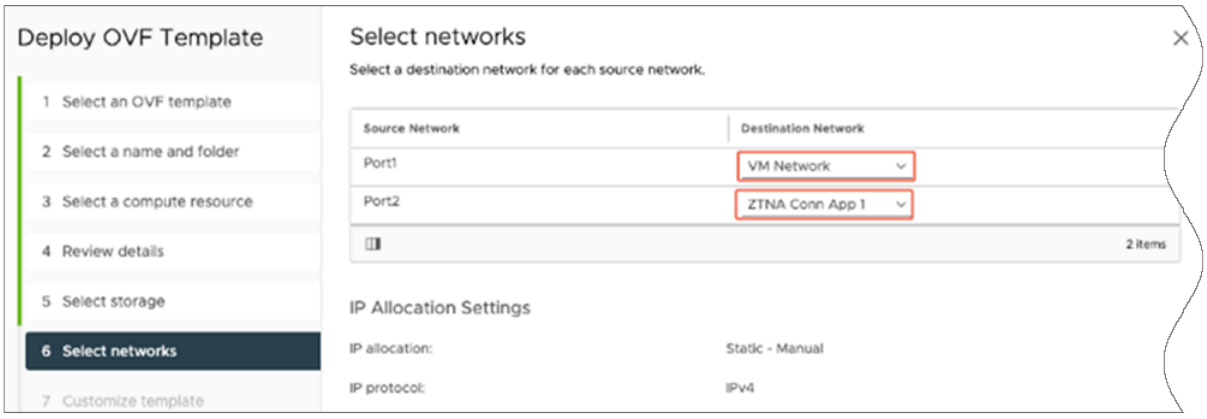
 ©2025 Palo Alto Networks, Inc.

STEP 8 | Seleccione las redes (para el puerto 1 y el puerto 2) para las interfaces que creó utilizando la plantilla de configuración OVA.

1. Si está implementando un conector de una sola interfaz de red, **Port 1 (Puerto 1)** es la red que puede llegar a los servidores de aplicaciones WAN y LAN. Seleccione la red WAN/LAN para el **Port 1 (Puerto 1)**.



2. Si está implementando un conector de dos interfaces de red, seleccione el puerto que da a Internet para el **Port 1 (Puerto 1)** y la red que da al servidor de aplicaciones para el **Port 2 (Puerto 2)**.
   - El puerto 1 es el puerto orientado a la WAN para la conectividad IPSec a Prisma Access.
   - El puerto 2 es el puerto orientado a la aplicación.



STEP 9 | Si aún no lo ha hecho, vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**, busque el objeto Conector que creó en Prisma Access para asociar

 ©2025 Palo Alto Networks, Inc.

con esta VM y seleccionar **Copy Token (Copiar token)** en la pestaña **Actions (Acciones)** (icono de llave); luego, copie los valores de **Key (Clave)** y **Secret (Secreto)**.



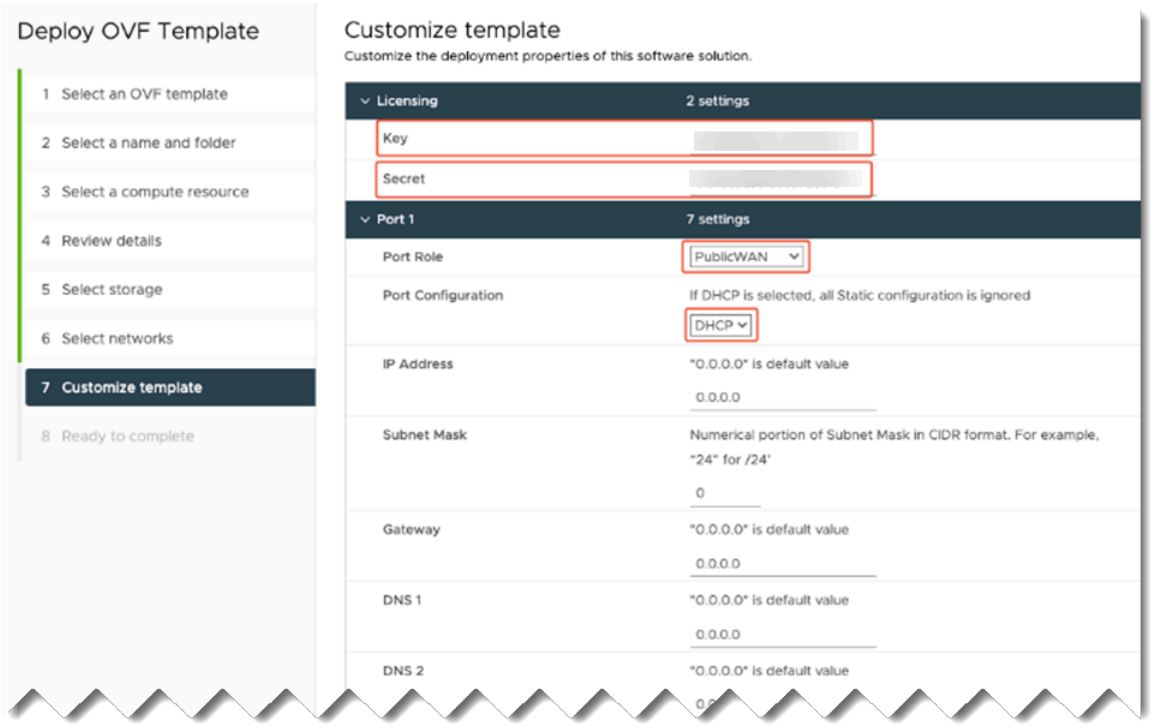
 ©2025 Palo Alto Networks, Inc.

STEP 10 | En la pantalla **Customize template (Personalizar plantilla)**, realice los siguientes cambios de configuración:

- Área de **Licensing (Licencias)**: introduzca los valores de **Key (Clave)** y **Secret (Secreto)** que recuperó del Portal SASE de Prisma.
- **Port 1 (Puerto 1)** (el área de Prisma Access orientada hacia el puerto): Realice los siguientes cambios:
  - **Role (Función)**: WAN pública.
  - **Port Configuration (Configuración del puerto)**: **DHCP** o **Static (Estática)**.

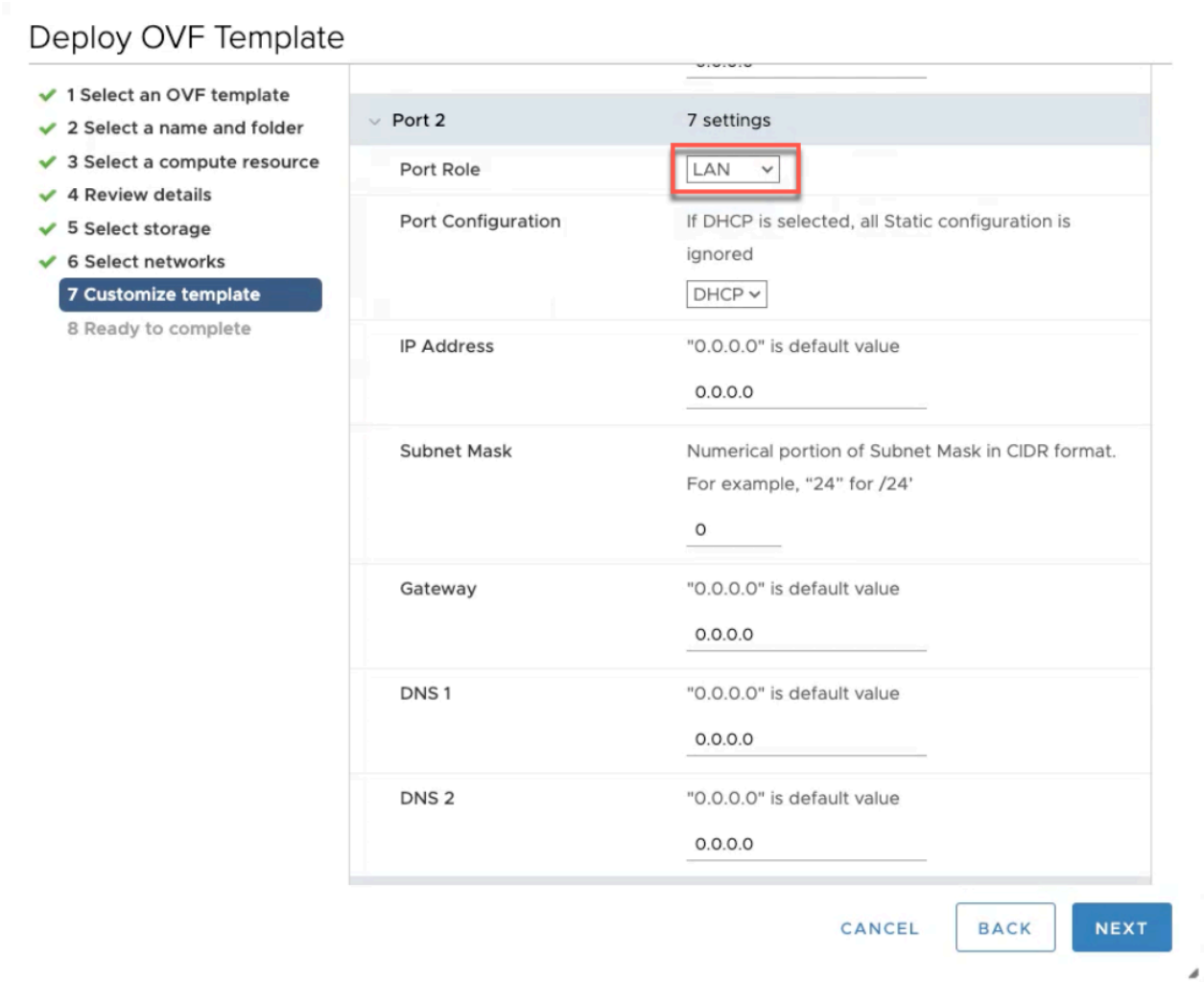
    Si selecciona **Static (Estática)**, introduzca la dirección IP, la máscara de subred, la puerta de enlace y uno o dos valores de servidor DNS.

    Si utiliza DHCP, deje los ceros predeterminados en los campos como se muestra en la siguiente captura de pantalla.



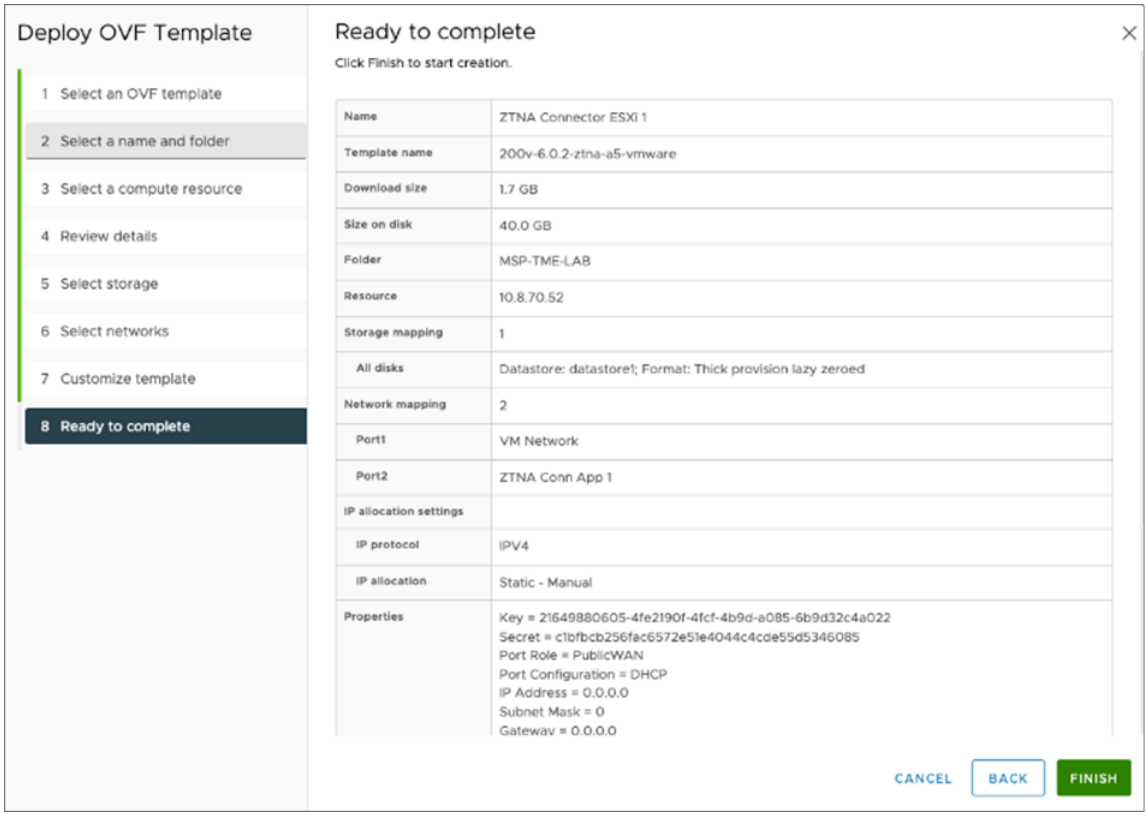
- Solo implementaciones de ESXi de dos interfaces de red Si tiene una implementación de dos interfaces de red, configure la interfaz IP de LAN del **Port 2 (Puerto 2)** con las mismas reglas que se aplicaron para el **Port 1 (Puerto 1)** en el Paso 10.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

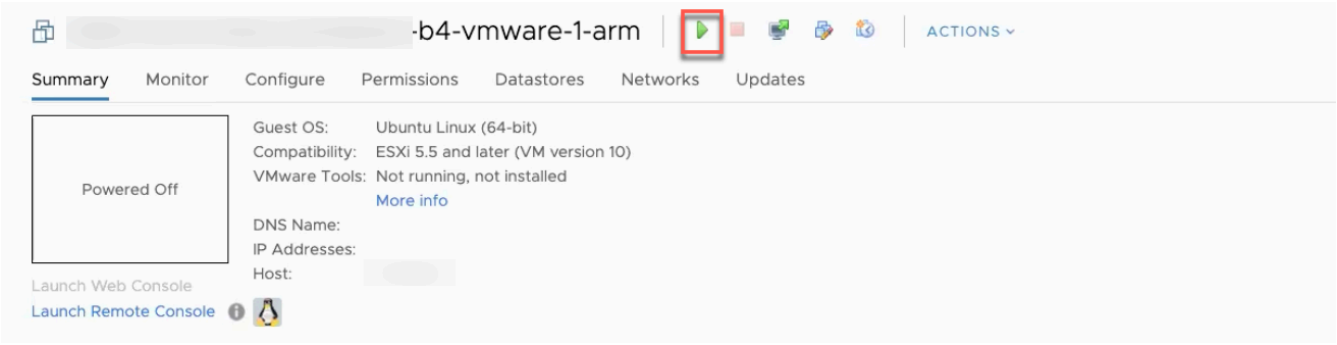
STEP 11 | Revise el resumen y luego seleccione **Finish (Finalizar)**.



 ©2025 Palo Alto Networks, Inc.

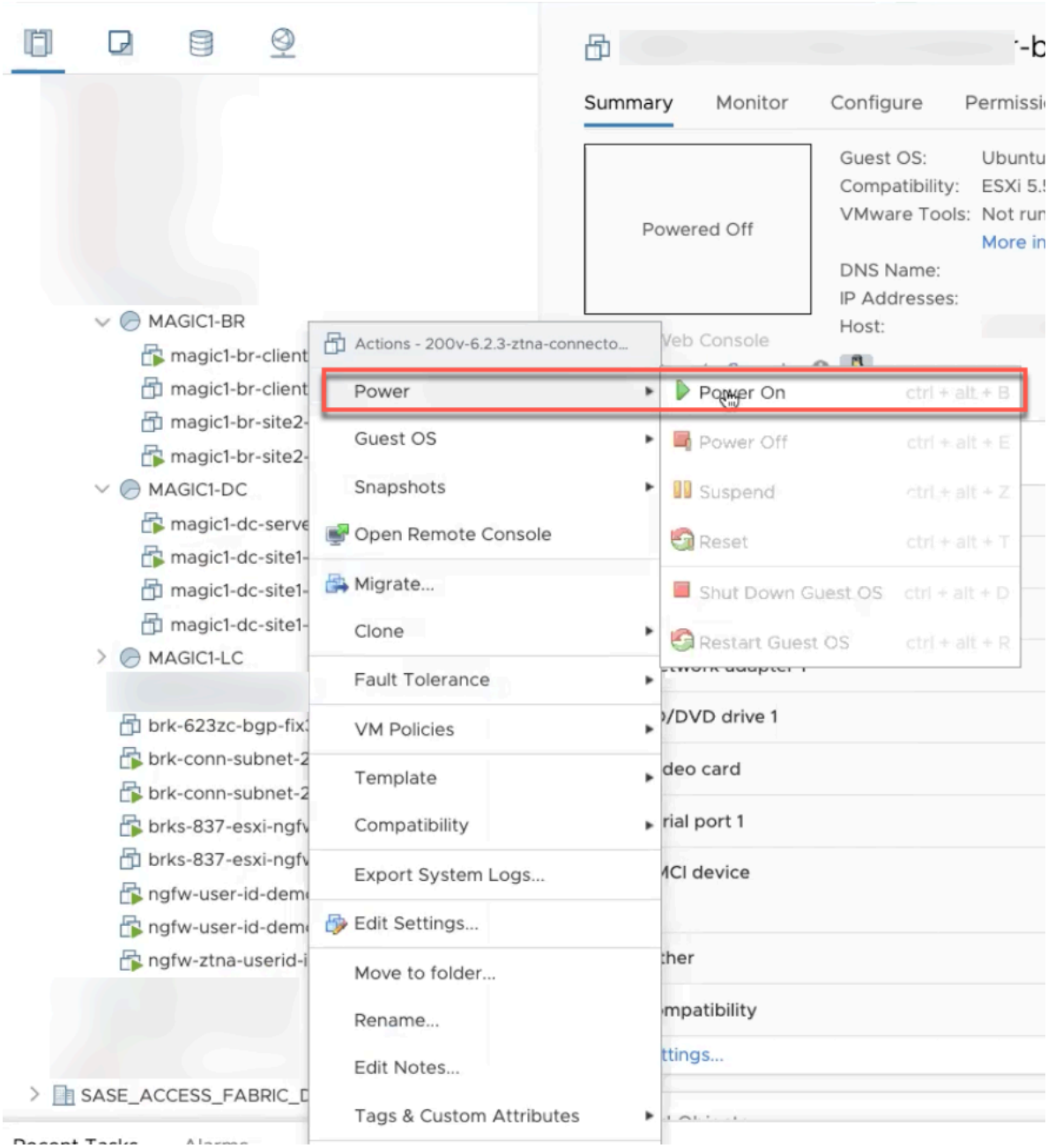
STEP 12 | Encienda la máquina virtual mediante uno de los siguientes métodos.

- Seleccione **Power On (Encender)** para iniciar el servidor virtual.



- Haga clic con el botón derecho en la interfaz y seleccione **Power On (Encender)** [**Power (Encender)** > **Power On (Encender)**].

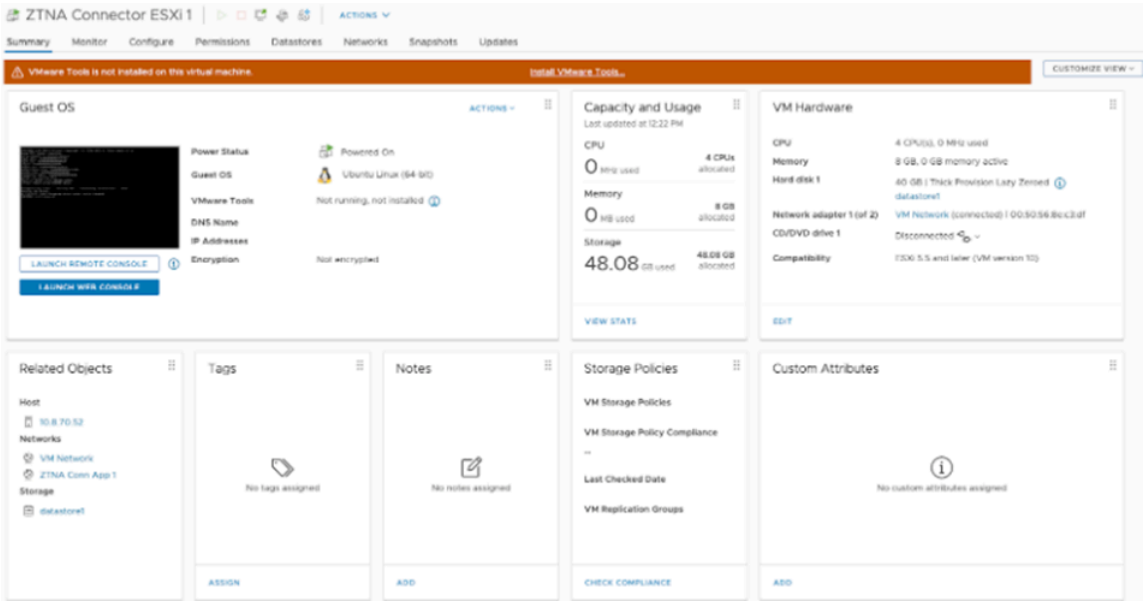
 ©2025 Palo Alto Networks, Inc.



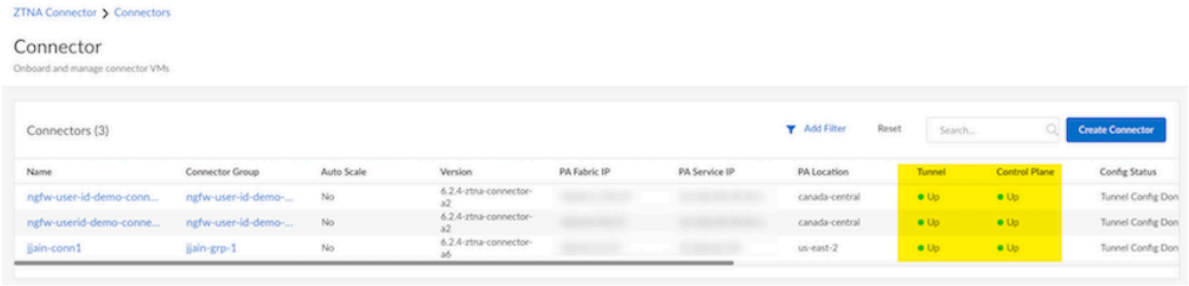
 ©2025 Palo Alto Networks, Inc.

STEP 13 | Después de implementar la máquina virtual, confirme que se haya activado.

Una vez que se activa el servidor virtual ESXi, Prisma Access completa la configuración del dispositivo que se utilizará como un ZTNA Connector.



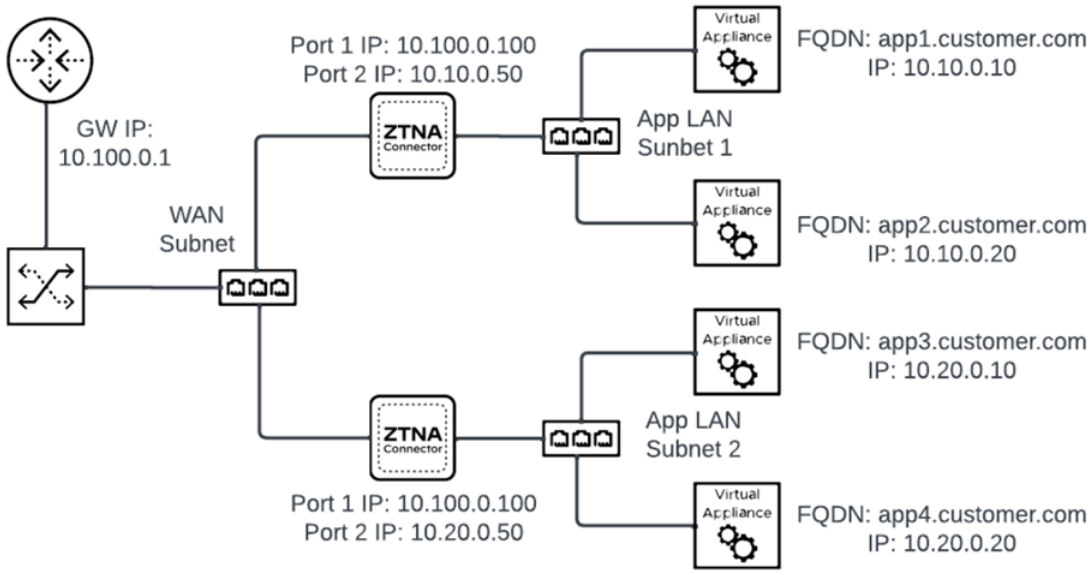
STEP 14 | En el portal Prisma SASE, vaya a **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)**, busque el Conector que desea usar y asegúrese de que muestre **Tunnel up (Túnel activo)**.



Implementaciones de KVM compatibles con Prisma Access ZTNA Connector

Implemente una máquina virtual basada en el núcleo (KVM) mediante una implementación de dos brazos. El siguiente diagrama muestra una implementación de red de ZTNA Connector de muestra utilizando KVM en modo de dos brazos con una puerta de enlace NAT.

 ©2025 Palo Alto Networks, Inc.



Integrar un ZTNA Connector mediante KVM

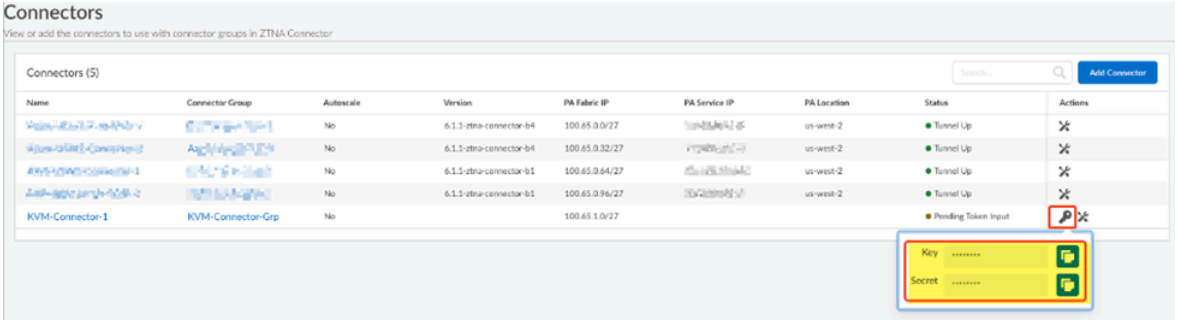
Para incorporar un ZTNA Connector mediante una máquina virtual basada en kernel (KVM), complete los siguientes pasos.

Antes de empezar, asegúrese de que cumple los siguientes requisitos previos:

- Descargue la imagen KVM de ZTNA Connector desde el Portal de atención al cliente (CSP) en **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** > **Prisma Access ZTNA Connector for KVM (ZTNA Connector para KVM)**.
- Asegúrese de que tiene un host KVM que cumpla con el mínimo de entornos de alojamiento para el ZTNA Connector.

STEP 1 | Cree un grupo de conectores y un conector para el host KVM.

STEP 2 | Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)** y busque el conector que creó para el host KVM, debe **Copy Token (Copiar token)** en el **Status (Estado)** y copiar los valores de **Key (Clave)** y **Secret (Secreto)**.



STEP 3 | Suba la imagen **qcow** que descargó del CSP al host KVM.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Si aún no lo ha hecho, cree y asocie las interfaces del puente virtual en el host KVM y prepare el host introduciendo los siguientes comandos:

- `brctl addbr virbr0`
- `brctl addbr virbr0`
- `brctl addbr virbr1`
- `brctl addif virbr1 ens192`

STEP 5 | Implemente la VM en el host KVM ejecutando el comando `virt-install` con las siguientes opciones configuradas:

- `-name` es el nombre de la máquina virtual.
- `-vcpu` es **4**.
- `-memory` is **16384** (16 GB).
- `-disk` es la ubicación y el nombre de la imagen **qcow** en el host KVM.
- `-network` hace referencia a las interfaces virtuales para conectarse a esta VM (es necesario implementar interfaces para un ZTNA Connector).

El siguiente es un comando de muestra utilizado para implementar el host KVM, donde <kvm-file-name> es el nombre del archivo qcow que descargó del CSP:

```
virt-install --name ztna-conn-1 --vcpus 4 --memory 16384 --disk ./
<kvm-file-name> --import --network bridge=virbr0,model=virtio --
network bridge=virbr1,model=virtio
```

STEP 6 | Conéctese a la consola de la máquina virtual introduciendo el siguiente comando:

```
virsh console ztna-conn-1
```

Se inicia un programa de instalación de la CLI interactivo.

STEP 7 | Configure el modelo ION, la clave y el secreto.

1. Seleccione **1** (un modelo ION de **ion 200v**) de las opciones que se muestran.

```
root@ubuntu-kvm-vm:/home/ubuntu-kvm/Desktop# virsh console
 ztna-conn-1 Connected to domain ztna-conn-1 Escape character
 is ^] Select an ION model: 1) ion 200v 2) ion 3102v 3) ion
 3104v 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8)
 ion 9100v Choose a Number or (Q)uit: 1 CPU: Passed (needed 4)
 Memory: Passed (needed 8.0G) Disk: No fue posible verificar
 (necesita 40.0 G) red: Aprobado (necesario 1) Seleccione
 un elemento para modificar o enviar la configuración: 1)
 Model : ion 200v 2) ION Key : 3) Secret Key : 4) Controller
 1 : Controller - DHCP 5) Port 1 : Disabled/Unused 6) Port
 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8) Port 4 :
 Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port 6 :
 Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

 ©2025 Palo Alto Networks, Inc.

2. Introduzca la clave desde el conector seleccionando la opción **2** e introduciendo la clave que guardó desde la interfaz de usuario de ZTNA Connector.

```
Choose a Number or (Q)uit: 2 Enter ION Key[None]: xxxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl Select an item to modify,
 or submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : 4)
 Controller 1 : Controller - DHCP 5) Port 1 : Disabled/Unused
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

3. Introduzca el secreto de conector ZTNA Connector seleccionando la opción **3** e introduciendo el secreto que guardó desde la interfaz de usuario del ZTNA Connector.

```
Choose a Number or (Q)uit: 3 Enter ION secret[None]: abcde12345
 Select an item to modify, or submit config: 1) Model :
 ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Secret Key : abcde12345 4) Controller 1 :
 Controller - DHCP 5) Port 1 : Disabled/Unused 6) Port 2 :
 Disabled/Unused 7) Port 3 : Disabled/Unused 8) Port 4 :
 Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port 6 :
 Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

STEP 8 | Configure puerto WAN opcional.

1. Seleccione la opción **5** (Puerto 1).

```
Choose a Number or (Q)uit: 5 Port 1: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Seleccione la opción **1** (Pública/WAN).

```
Choose a Number or (Q)uit: 1 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Opcional) Si necesita establecer una dirección IP estática, elija la opción **2** y establecer la dirección IP, la puerta de enlace y los parámetros del servidor DNS; de lo contrario, seleccione **1**.

```
Choose a Number or (Q)uit: 1 Port 1: 1) Role : PublicWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

 ©2025 Palo Alto Networks, Inc.

4. Seleccione opción **4** para volver al menú principal.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN
 - DHCP 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused
 14) Submit and restart Select an item to modify, or submit
 config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345 4)
 Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN - DHCP
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

STEP 9 | Configure las opciones del puerto LAN.

1. Seleccione la opción **6** (Puerto 2).

```
Choose a Number or (Q)uit: 6 Port 2: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Seleccionar opción **2** (WAN privada).

```
Choose a Number or (Q)uit: 2 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Opcional) Si necesita establecer una dirección IP estática, elija la opción **2** y establecer la dirección IP, la puerta de enlace y los parámetros del servidor DNS; de lo contrario, seleccione **1**.

```
Choose a Number or (Q)uit: 2 Port 2: 1) Role : PrivateWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

4. Seleccione opción **4** para volver al menú principal.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN -
 DHCP 6) Port 2 : PrivateWAN - DHCP 7) Puerto 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused 14)
 Submit and restart
```

 ©2025 Palo Alto Networks, Inc.

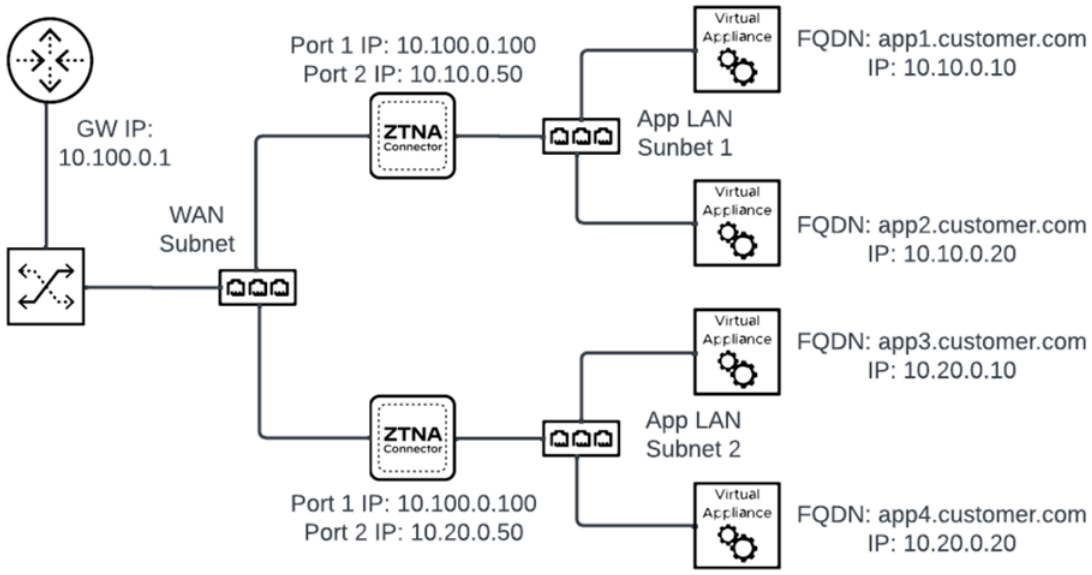
STEP 10 | Guarde y reinicie el conector.

```
Choose a Number or (Q)uit: 14 WARNING! Una vez enviada esta
 configuración, todo el hardware se firmará, registrará y vinculará
 permanentemente a la clave ION/clave secreta en el controlador
 de nube Prisma SDWAN. WHAT THIS MEANS is that hardware cannot
 be added/removed (disks, network cards) after this 'SUBMIT'
 function. If any hardware changes are required beyond this
 'SUBMIT', the ION will need to be re-deployed with a new ION
 Key and Secret Key. Si es necesario añadir o eliminar hardware,
 responda 'N' a continuación y apague el dispositivo ION y realice
 los cambios ahora. Submit these changes now?[N]: y Building
 configuration... [VFF:CFG] ZeroTouch Config Starting - config
 file parser [VFF:CFG] Attempting to load/parse as Config/INI
 file. [VFF:CFG] Successfully Loaded config style file. [VFF:CFG]
 Controller 1 successfully set to CONTROLLER/DHCP. [VFF:CFG] Port 1
 successfully set to PUBLICWAN/DHCP. [VFF:CFG] Port 2 successfully
 set to PRIVATEWAN/DHCP. [VFF:CFG] WARN: Port 3 had no config
 section. Defaulting to Disable. [VFF:CFG] WARN: Port 4 had no
 config section. Defaulting to Disable. [VFF:CFG] WARN: Port 5 had
 no config section. Defaulting to Disable. [VFF:CFG] WARN: Port 6
 had no config section. Defaulting to Disable. [VFF:CFG] WARN: Port
 7 had no config section. Defaulting to Disable. [VFF:CFG] WARN:
 Port 8 had no config section. Defaulting to Disable. [VFF:CFG]
 WARN: Port 9 had no config section. Defaulting to Disable.
 [VFF:CFG] Success with Config/INI file parser. [VFF:KVM] Menu
 config end, continuing normal boot... Reboot-reason: manufacture
```

Implementaciones de Hyper-V compatibles con Prisma Access ZTNA Connector

Implementa un hipervisor Microsoft Hyper-V utilizando una implementación de dos brazos. El siguiente diagrama muestra una implementación de red de ZTNA Connector de muestra utilizando Hyper-V en modo de dos brazos con una puerta de enlace NAT.

 ©2025 Palo Alto Networks, Inc.



Incorporar un ZTNA Connector mediante Hyper-V

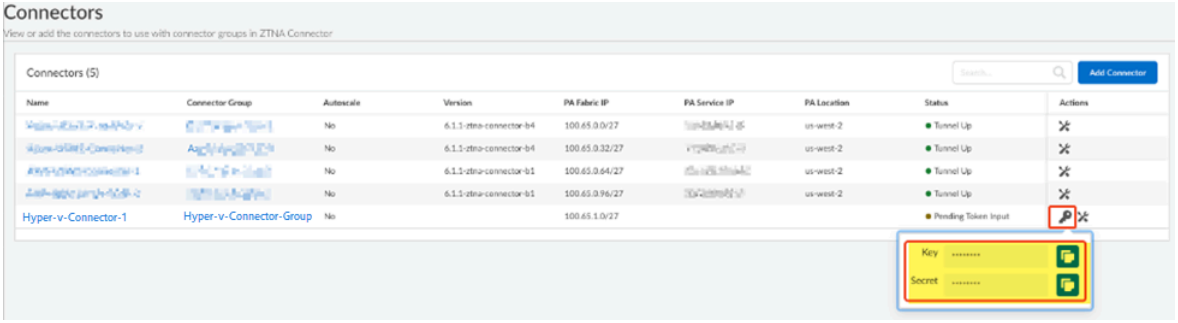
Para incorporar un ZTNA Connector mediante una máquina virtual (VM) de Microsoft Hyper-V, complete los siguientes pasos.

Antes de empezar, asegúrese de que cumple los siguientes requisitos previos:

- Descargue la imagen Hyper-V de ZTNA Connector del Portal de atención al cliente (CSP) en **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** > **Prisma Access ZTNA Connector for Hyper-V (Prisma Access ZTNA Connector para Hyper-V)**.
- Asegúrese de que tiene una máquina virtual de Hyper-V que cumpla con el mínimo de entornos de alojamiento para el ZTNA Connector.

STEP 1 | Crear un grupo de conectores y un conector para la máquina virtual de Hyper-V.

STEP 2 | Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)** y busque el conector que creó para la máquina virtual de Hyper-V, debe **Copy Token (Copiar token)** en el **Status (Estado)** y copiar los valores de **Key (Clave)** y **Secret (Secreto)**.



STEP 3 | Cargue la imagen **vhd** que descargó de la carpeta CSP a la máquina virtual de Hyper-V.

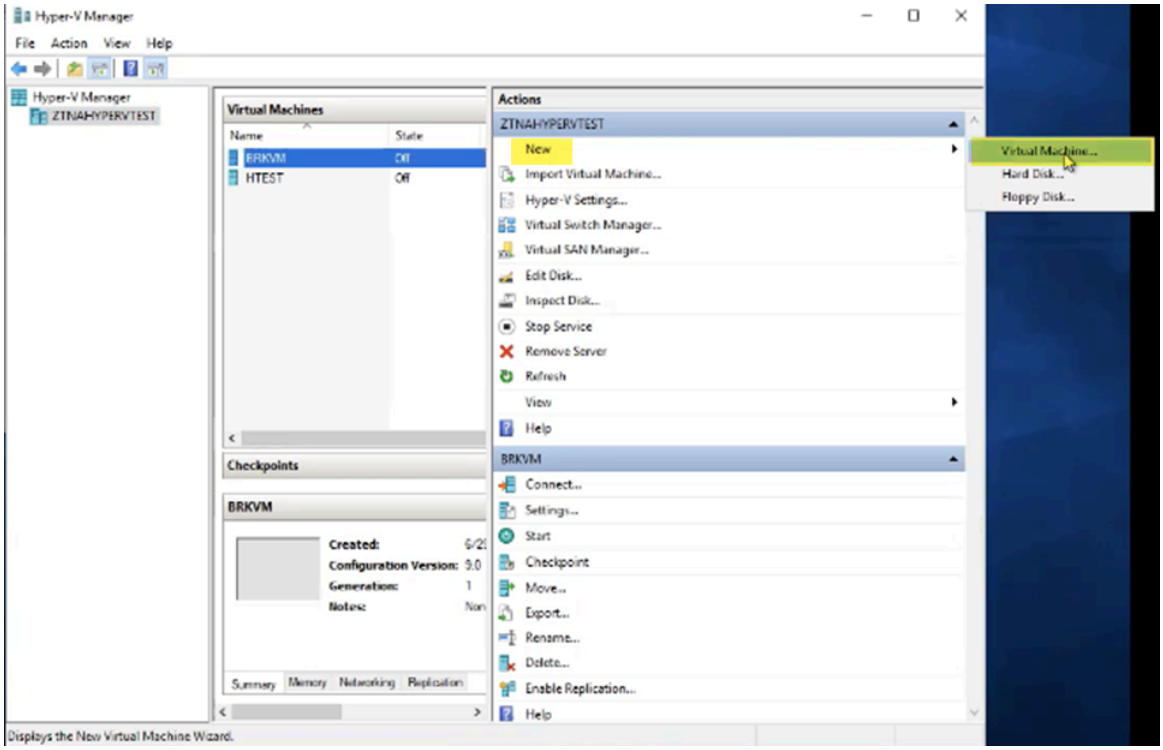
Asegúrese de que se pueda acceder a la ubicación que elija desde la máquina virtual de Hyper-V.

Se requiere un archivo (vhd) para cada máquina virtual de Hyper-V.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Vaya al Administrador de Hyper-V y cree una nueva máquina virtual seleccionando **Actions (Acciones)** > **New (Nuevo)** > **Virtual Machine (Máquina virtual)**.

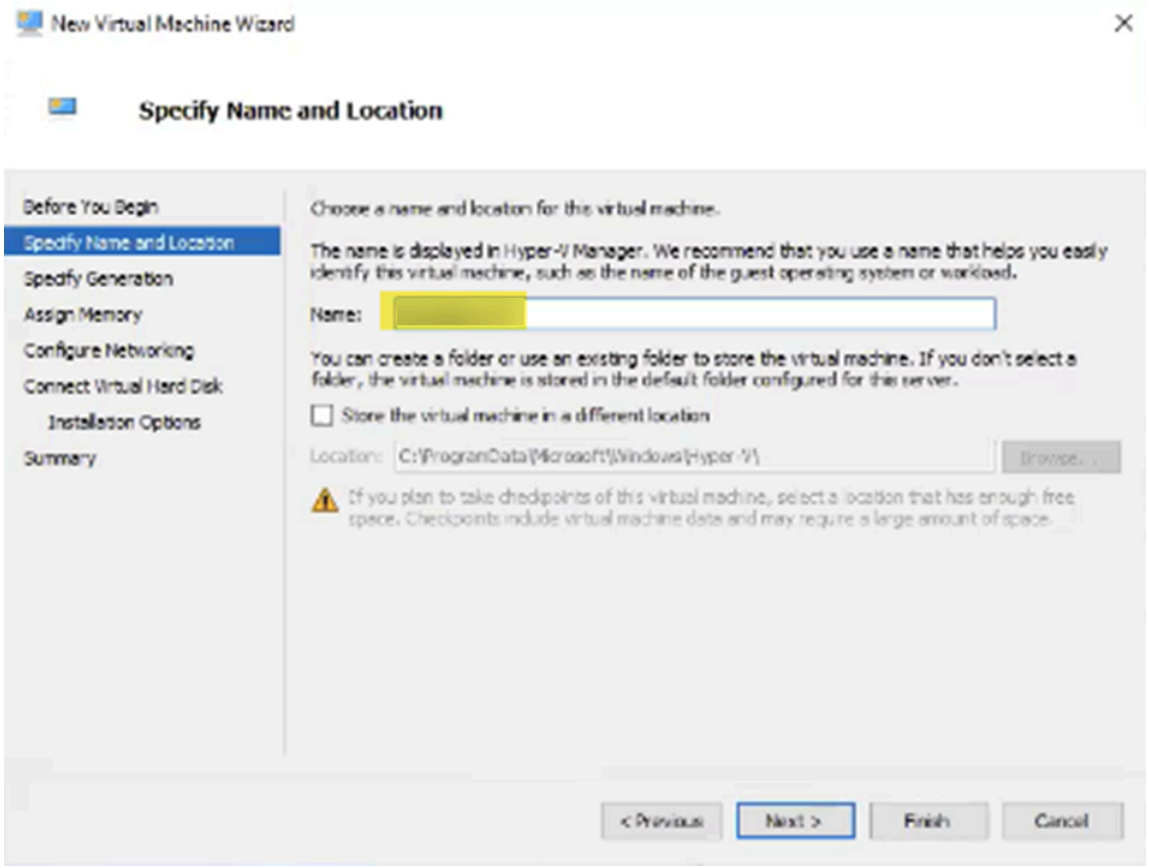
Este flujo de trabajo muestra los pasos que se realizan para implementar máquinas virtuales de Hyper-V en un servidor de Microsoft. La interfaz de usuario de Hyper-V puede tener un aspecto diferente en su entorno.



STEP 5 | Vaya a la pantalla **Next (Siguiente)** y escriba un nombre único para la máquina virtual y vaya a la página **Next (Siguiente)**.

 ©2025 Palo Alto Networks, Inc.

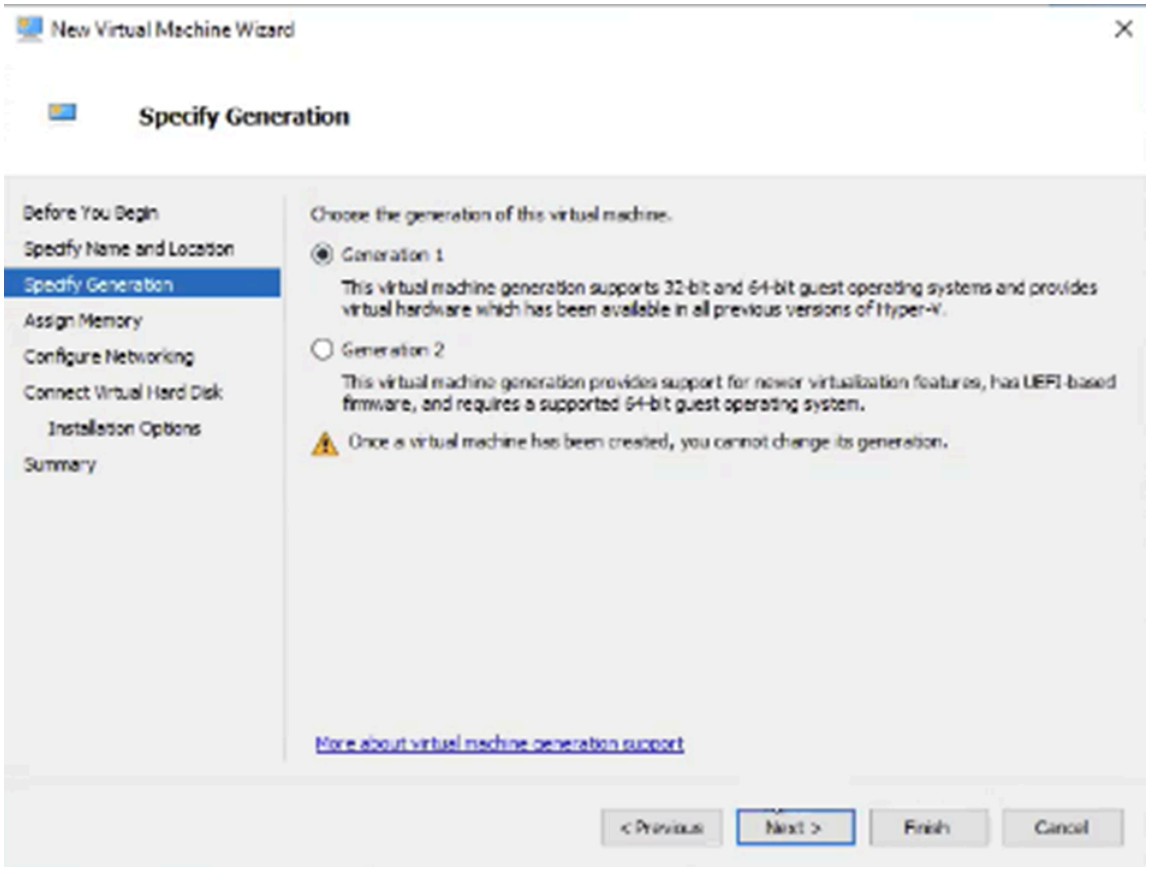
STEP 6 | (Opcional) Para cambiar la ubicación de la máquina virtual, seleccione **Store the virtual machine in a different location (Almacenar la máquina virtual en una ubicación diferente)** y seleccione la ubicación.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Seleccione **Generation 1 (Generación 1)** como la generación de VM y vaya a la **Next (Siguiente)** página.

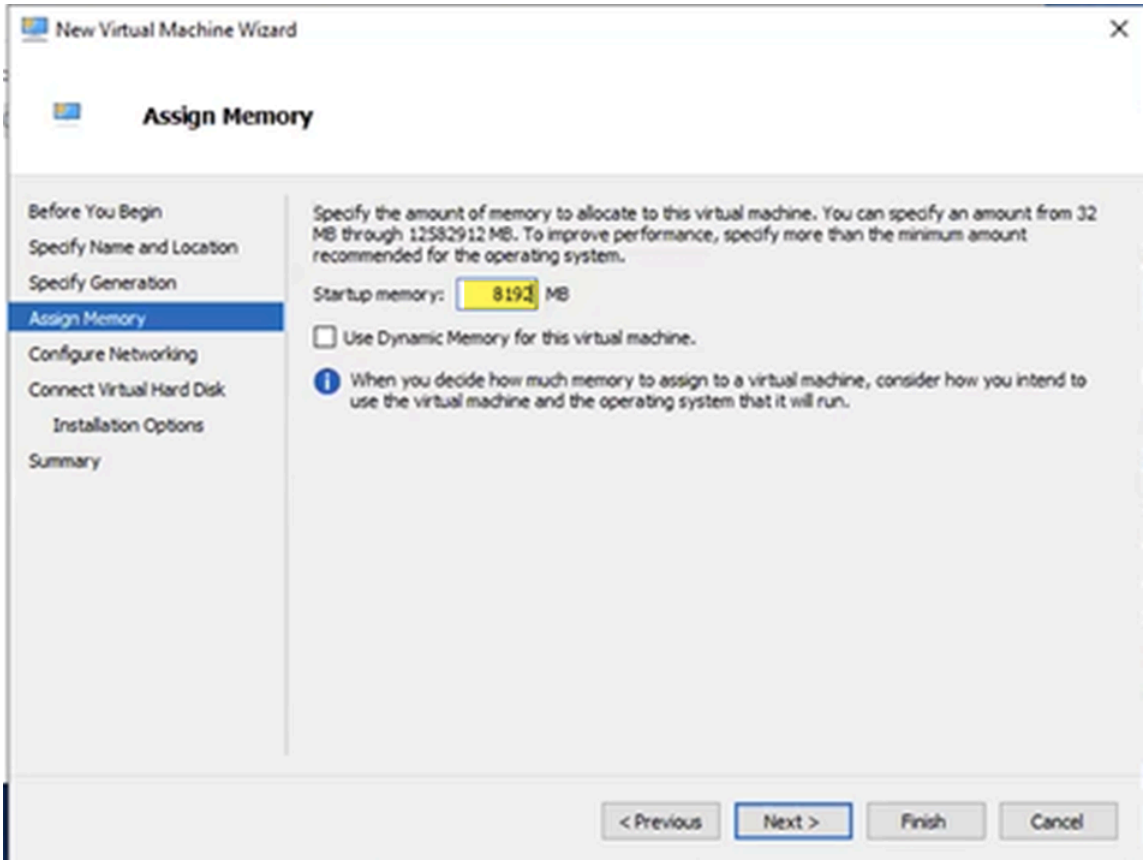
Esta es la generación que admite el archivo vhd de ZTNA Connector.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Asigne memoria a la máquina virtual.

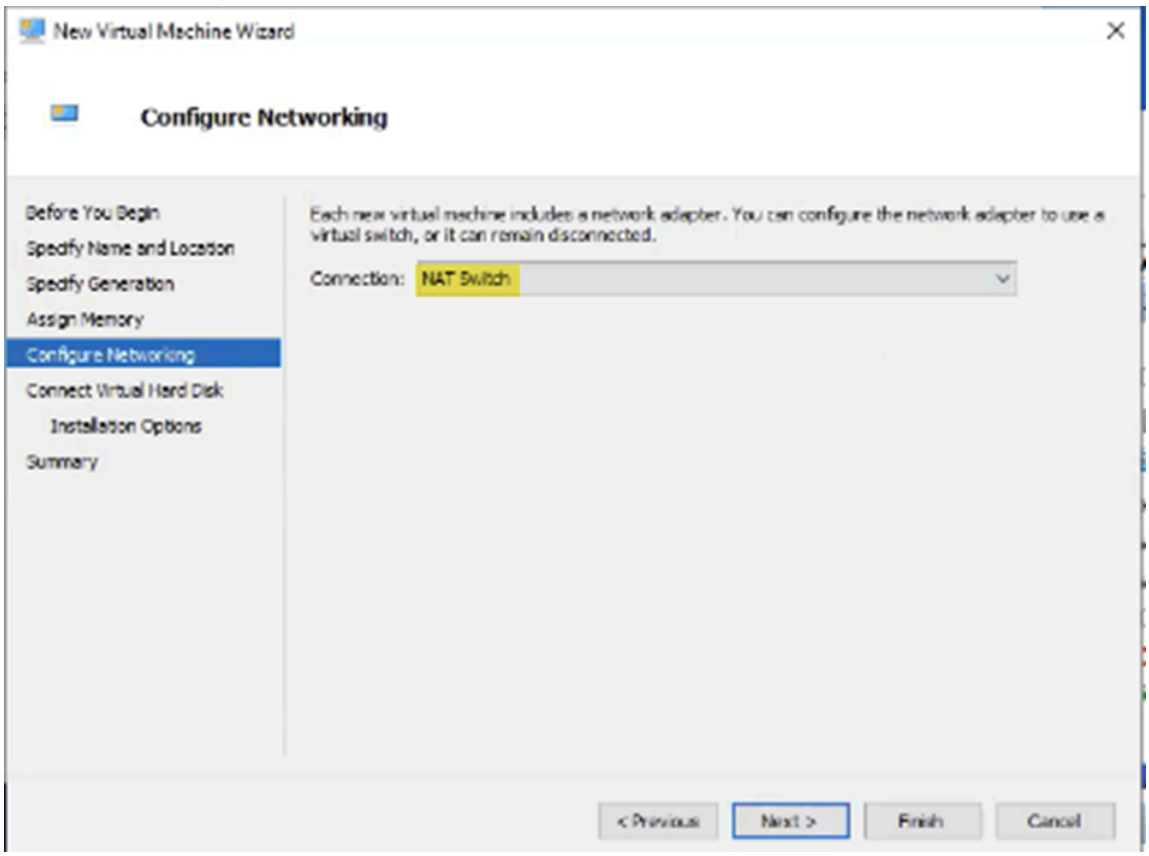
Asigne una memoria mínima de **8192** MB (8 GB), que cumple con los requisitos mínimos para una máquina virtual de Hyper-V y vaya a la página **Next (Siguiente)**.



 ©2025 Palo Alto Networks, Inc.

STEP 9 | Configure las redes para su máquina virtual; a continuación, vaya a la página **Next (Siguiente)**.

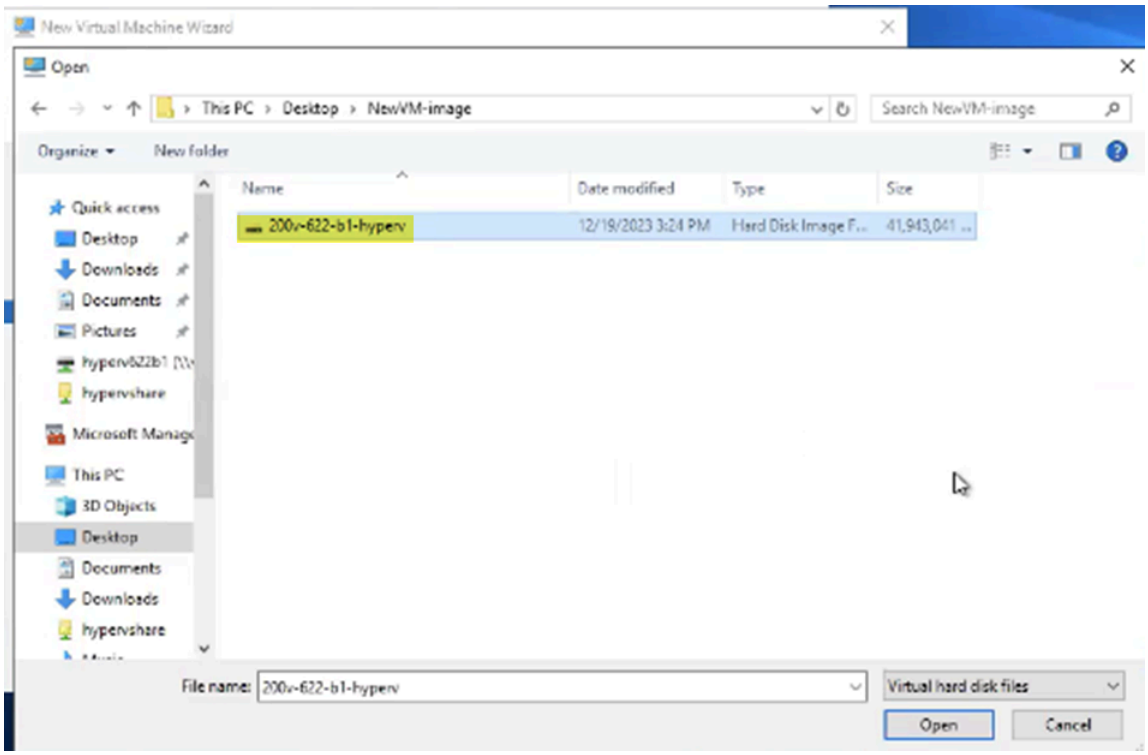
La red que utilice depende de su configuración. Este ejemplo utiliza un **NAT Switch (Conmutador NAT)** para las redes.



 ©2025 Palo Alto Networks, Inc.

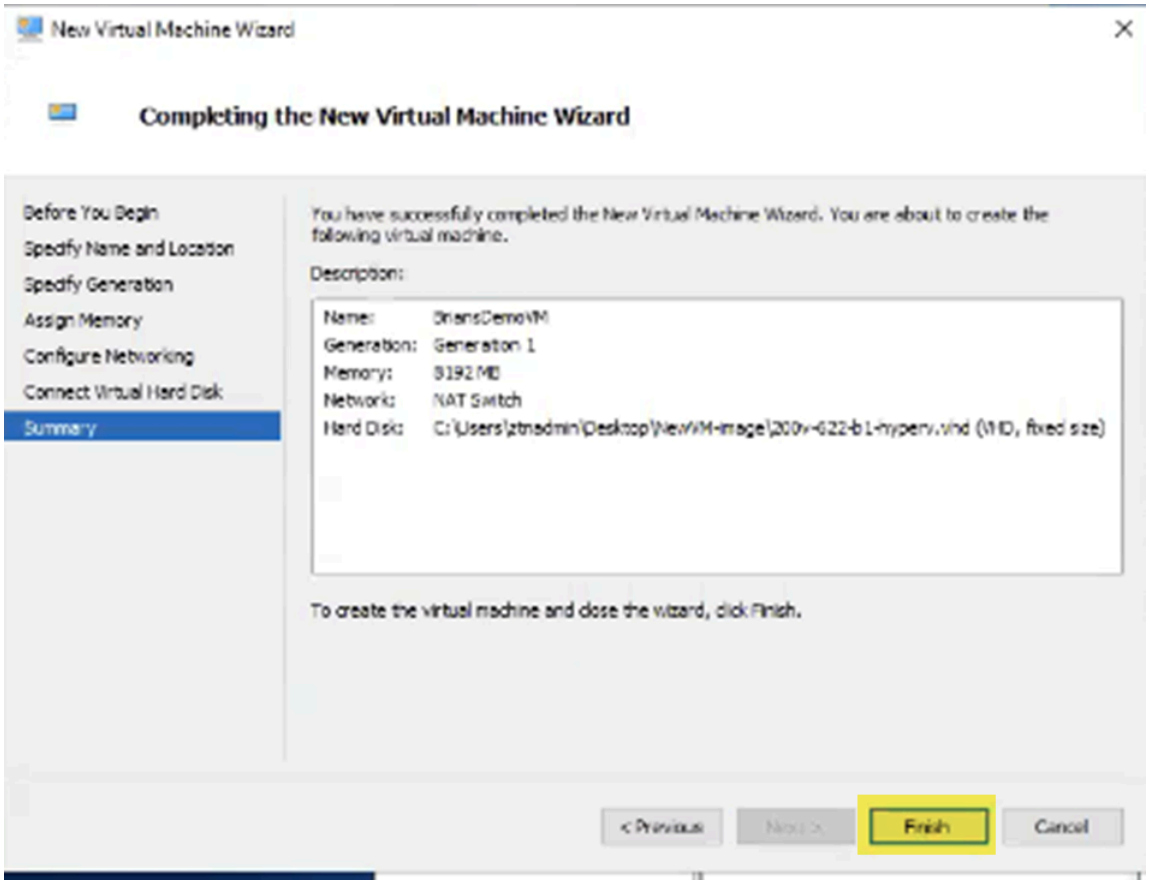
STEP 10 | Conecte el disco duro virtual.

1. Seleccione **Usar un disco duro virtual existente** y **Browse (Examinar)** en busca del archivo vhd que descargó
2. Seleccione el archivo vhd que descargó, a continuación seleccione **Open (Abrir)** para abrirlo y vaya a la página **Next (Siguiente)**.



 ©2025 Palo Alto Networks, Inc.

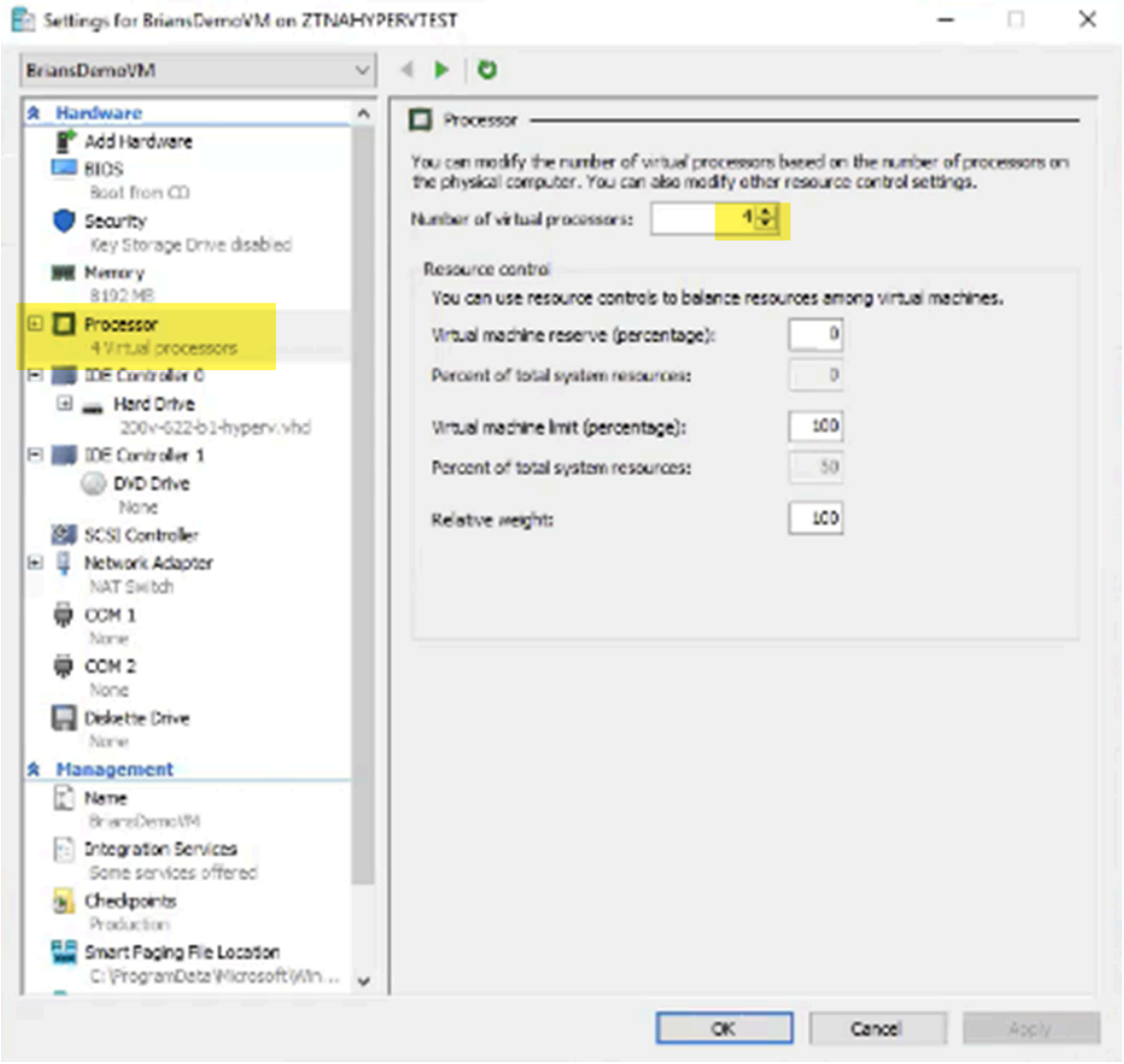
STEP 11 | Elija **Finish (Terminar)** el nuevo asistente de máquina virtual.



Hyper-V crea la máquina virtual.

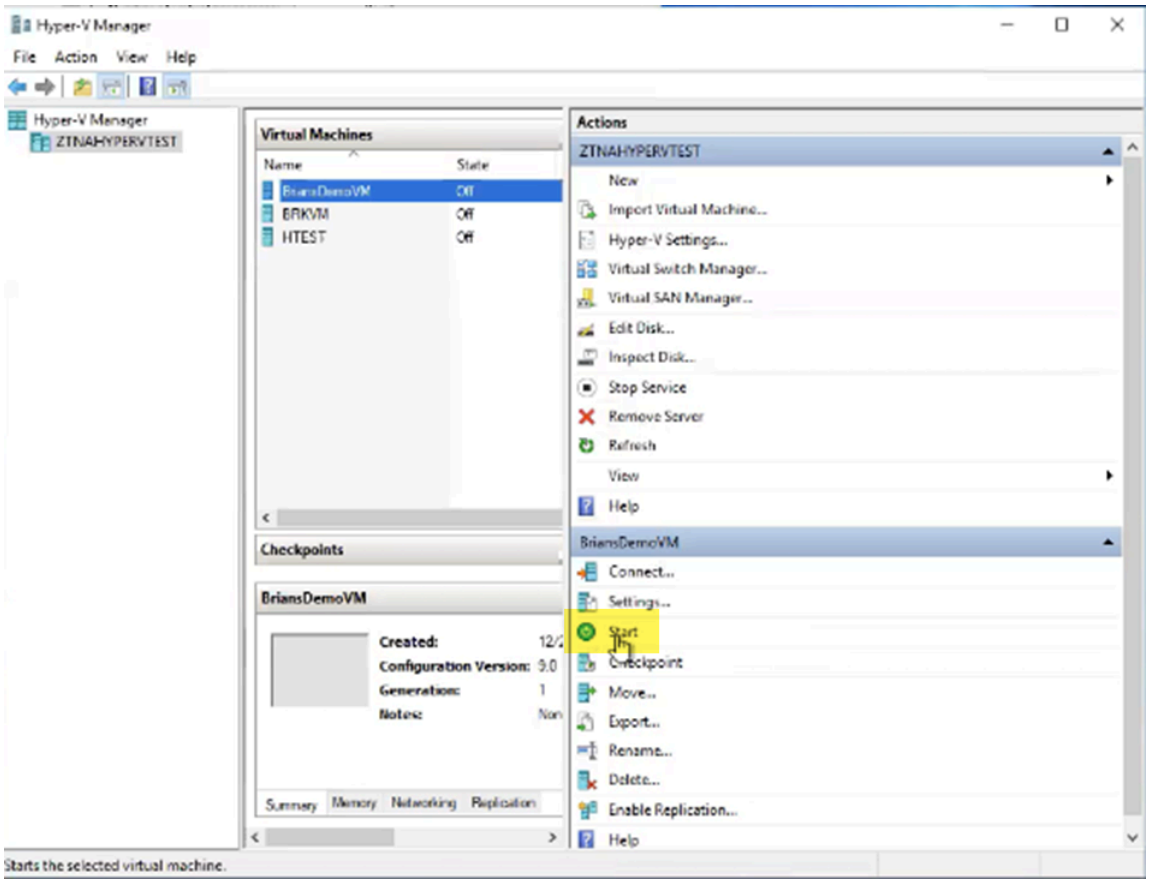
 ©2025 Palo Alto Networks, Inc.

STEP 12 | Para asegurarse de que la máquina virtual tenga al menos cuatro procesadores, vaya a la zona **Processor (Procesador)** y asegúrese de seleccionar al menos **4** procesadores virtuales.

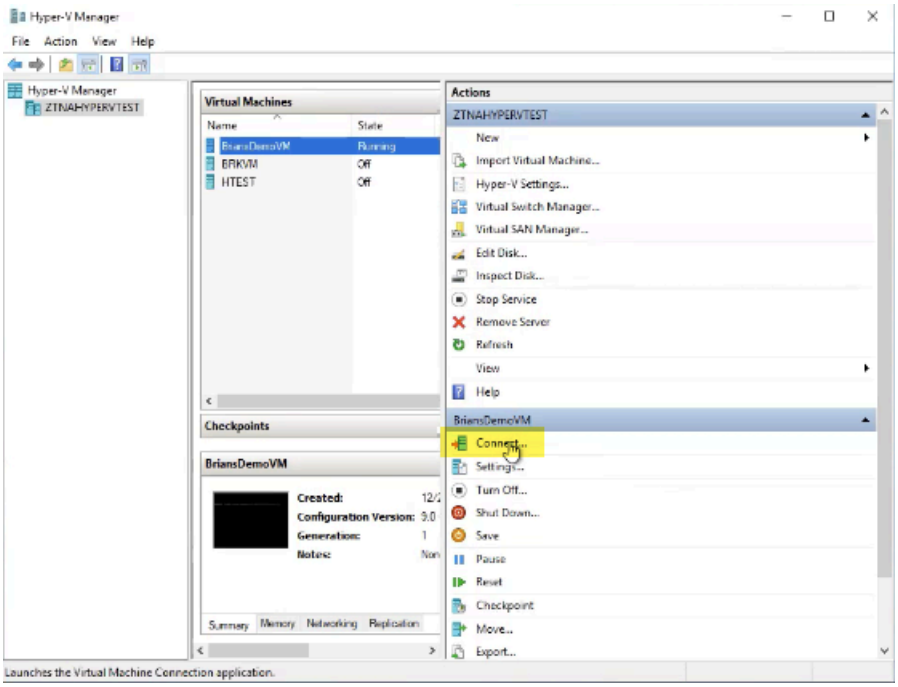


 ©2025 Palo Alto Networks, Inc.

STEP 13 | Debe **Start (Iniciar)** la máquina virtual.



STEP 14 | **Connect (Conectar)** a la consola serie.



 ©2025 Palo Alto Networks, Inc.

STEP 15 | Espere a que se inicialice el programa de instalación interactivo de la CLI y, a continuación, configure el modelo, la clave y el secreto de dispositivo ION.

1. Seleccione **1** (un modelo ION de **ion 200v**) de las opciones que se muestran.

```
Seleccione un modelo ION: 1) ion 200v 2) ion 3102v 3) ion
 3104v 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8)
 ion 9100v Choose a Number or (Q)uit: 1 CPU: Passed (needed 4)
 Memory: Passed (needed 8.0G) Disk: No fue posible verificar
 (necesita 40.0 G) red: Aprobado (necesario 1) Seleccione
 un elemento para modificar o enviar la configuración: 1)
 Model : ion 200v 2) ION Key : 3) Secret Key : 4) Controller
 1 : Controller - DHCP 5) Port 1 : Disabled/Unused 6) Port
 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8) Port 4 :
 Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port 6 :
 Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

2. Introduzca la clave desde el conector seleccionando la opción **2** e introduciendo la clave que guardó desde la interfaz de usuario de ZTNA Connector.

```
Choose a Number or (Q)uit: 2 Enter ION Key[None]: xxxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl Select an item to modify,
 or submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : 4)
 Controller 1 : Controller - DHCP 5) Port 1 : Disabled/Unused
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

3. Introduzca el secreto de conector ZTNA Connector seleccionando la opción **3** e introduciendo el secreto que guardó desde la interfaz de usuario del ZTNA Connector.

```
Choose a Number or (Q)uit: 3 Enter ION secret[None]: abcde12345
 Select an item to modify, or submit config: 1) Model :
 ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Secret Key : abcde12345 4) Controller 1 :
 Controller - DHCP 5) Port 1 : Disabled/Unused 6) Port 2 :
 Disabled/Unused 7) Port 3 : Disabled/Unused 8) Port 4 :
 Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port 6 :
 Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

 ©2025 Palo Alto Networks, Inc.

STEP 16 | Configure las opciones del puerto WAN.

1. Seleccione la opción **5** (Puerto 1).

```
Choose a Number or (Q)uit: 5 Port 1: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Seleccione la opción **1** (Pública/WAN).

```
Choose a Number or (Q)uit: 1 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Opcional) Si necesita establecer una dirección IP estática, elija la opción **2** y establecer la dirección IP, la puerta de enlace y los parámetros del servidor DNS; de lo contrario, seleccione **1**.

```
Choose a Number or (Q)uit: 1 Port 1: 1) Role : PublicWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

4. Seleccione opción **4** para volver al menú principal.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN
 - DHCP 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused
 14) Submit and restart Select an item to modify, or submit
 config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345 4)
 Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN - DHCP
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

STEP 17 | Configure las opciones del puerto LAN.

1. Seleccione la opción **6** (Puerto 2).

```
Choose a Number or (Q)uit: 6 Port 2: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Seleccionar opción **2** (WAN privada).

```
Choose a Number or (Q)uit: 2 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
```

 ©2025 Palo Alto Networks, Inc.

```
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Opcional) Si necesita establecer una dirección IP estática, elija la opción **2** y establecer la dirección IP, la puerta de enlace y los parámetros del servidor DNS; de lo contrario, seleccione **1**.

```
Choose a Number or (Q)uit: 2 Port 2: 1) Role : PrivateWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

4. Seleccione opción **4** para volver al menú principal.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN -
 DHCP 6) Port 2 : PrivateWAN - DHCP 7) Puerto 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused 14)
 Submit and restart
```

STEP 18 | Guarde y reinicie el conector.

```
Choose a Number or (Q)uit: 14 WARNING! Una vez enviada esta
 configuración, todo el hardware se firmará, registrará y vinculará
 permanentemente a la clave ION/clave secreta en el controlador
 de nube Prisma SDWAN. WHAT THIS MEANS is that hardware cannot
 be added/removed (disks, network cards) after this 'SUBMIT'
 function. If any hardware changes are required beyond this
 'SUBMIT', the ION will need to be re-deployed with a new ION
 Key and Secret Key. Si es necesario añadir o eliminar hardware,
 responda 'N' a continuación y apague el dispositivo ION y realice
 los cambios ahora. Submit these changes now?[N]: y Building
 configuration... [VFF:CFG] ZeroTouch Config Starting - config
 file parser [VFF:CFG] Attempting to load/parse as Config/INI
 file. [VFF:CFG] Successfully Loaded config style file. [VFF:CFG]
 Controller 1 successfully set to CONTROLLER/DHCP. [VFF:CFG] Port 1
 successfully set to PUBLICWAN/DHCP. [VFF:CFG] Port 2 successfully
 set to PRIVATEWAN/DHCP. [VFF:CFG] WARN: Port 3 had no config
 section. Defaulting to Disable. [VFF:CFG] WARN: Port 4 had no
 config section. Defaulting to Disable. [VFF:CFG] WARN: Port 5 had
 no config section. Defaulting to Disable. [VFF:CFG] WARN: Port 6
 had no config section. Defaulting to Disable. [VFF:CFG] WARN: Port
 7 had no config section. Defaulting to Disable. [VFF:CFG] WARN:
 Port 8 had no config section. Defaulting to Disable. [VFF:CFG]
 WARN: Port 9 had no config section. Defaulting to Disable.
 [VFF:CFG] Success with Config/INI file parser. [VFF:KVM] Menu
 config end, continuing normal boot... Reboot-reason: manufacture
```

 ©2025 Palo Alto Networks, Inc.

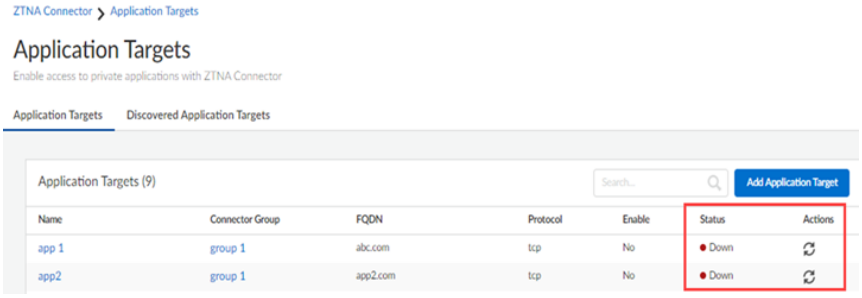
Supervisar ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Todos los componentes del ZTNA Connector proporcionan información de estado clara, logs y herramientas de diagnóstico para ayudarle a solucionar cualquier problema que surja. Utilice las siguientes herramientas para supervisar la implementación de su ZTNA Connector.

©2025 Palo Alto Networks, Inc.

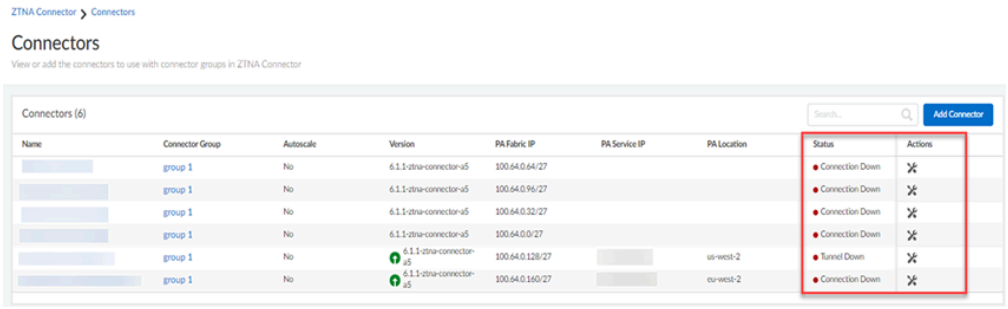
- Vea el estado de sus aplicaciones y conectores desde la plataforma Prisma SASE.
  - Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector)** > **Application Targets (Objetivos de la aplicación)** y verifique que el **Status (Estado)** de todos los objetivos de la aplicación sea **Up (Activo)**.



Si el estado muestra **Down (Inactivo)**, el Conector no puede comunicarse con su aplicación. Después de solucionar el problema con la aplicación, haga clic en el botón Actualizar estado en la columna **Action (Acción)** y verifique que el **Status (Estado)** cambie a **Up (Activo)** (el estado se actualiza automáticamente una vez por minuto).

El estado también es Activo si se puede acceder a la aplicación desde el conector ZTNA (utilizando el último resultado de resolución de DNS exitosa) pero la resolución de DNS del FQDN de la aplicación falla desde el conector ZTNA.

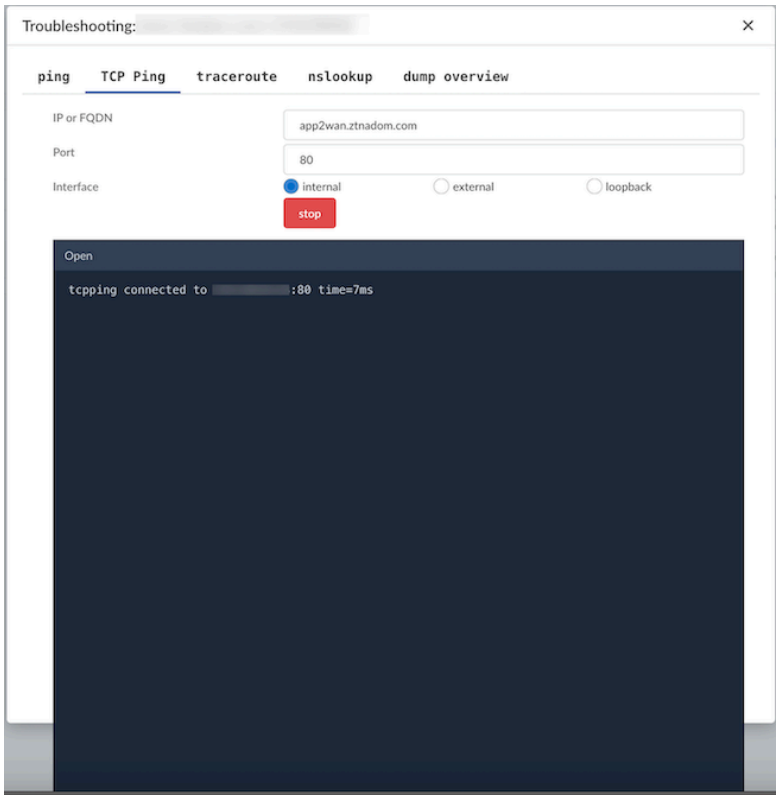
- Seleccione **Workflows (Flujos de trabajo)** > **ZTNA Connector** > **Connectors (Conectores)** y asegúrese de que el **Status (Estado)** de todos los conectores sea **Up (Activo)**.



Si el **Status (Estado)** muestra **Tunnel Down (Túnel inactivo)**, este indica que el túnel IPSec entre la máquina virtual del conector y Prisma Access esta inactivo. Si el **Status (Estado)** muestra **Connection Down (Conexión caída)**, esta indica que la máquina virtual del conector está inactiva. Haga clic en el icono de diagnóstico para iniciar una conexión de shell remota al Conector para solucionar el problema. Puede ejecutar un **`ping`**, **`ping TCP`**,

 ©2025 Palo Alto Networks, Inc.

`traceroute`, **`nslookup`**o **`dump overview`** para ayudarle a diagnosticar el problema de conectividad.



 ©2025 Palo Alto Networks, Inc.

Ver logs del ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licencia de complemento de ZTNA Connector La licencia Essential con la licencia complementaria incluye 8 conectores ZTNA, 100 FQDN y 4 funciones de subred IP. La licencia avanzada con la licencia complementaria incluye 40 conectores ZTNA, 300 FQDN y funcionalidad de subred de 1024 IP. La licencia Premium con la licencia complementaria incluye 200 conectores ZTNA, 4000 FQDN y funcionalidad de subred de 1024 IP. ❑ Si no compra la licencia complementaria de ZTNA Connector, Prisma Access proporciona licencias que incluyen cuatro conectores, 40 FQDN y cuatro subredes IP. Esta funcionalidad se proporciona con el propósito de probar los conectores ZTNA en su entorno.

Todo el tráfico del ZTNA Connector se registra en Strata Logging Service. Para almacenar logs de Prisma Access en el Strata Logging Service, debe estimar y comprar la cantidad adecuada de almacenamiento para logs en Strata Logging Service. Le recomendamos que aumente el porcentaje de su capacidad de almacenamiento total de Strata Logging Service en un 10 % para almacenar los logs de ZTNA Connector.

Asegúrese de haber configurado un perfil de Reenvío de logs que reenvíe los tipos de logs deseados a Strata Logging Service. Strata Logging Service enviará una notificación por correo electrónico para comprar más almacenamiento cuando la cuota de almacenamiento de logs alcance el 90 %. Si no compra más almacenamiento, se eliminarán los logs más antiguos.

Independientemente de la interfaz de gestión que esté utilizando, Prisma Access —Panorama o gestionada en la nube— puede ver sus logs en Prisma Access (Managed by Strata Cloud Manager) en **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.

ZTNA Connector proporciona los siguientes logs de red.

©2025 Palo Alto Networks, Inc.

- **Registros de auditoría** : están disponibles a través de la plataforma Prisma SASE y proporcionan registros de los cambios de configuración de los administradores en el ZTNA Connector. Puede utilizar estos logs para fines de cumplimiento y resolución de problemas.

  Puede filtrar los logs de auditoría por rango de tiempo, sitio, dispositivo y tipo. Los logs de auditoría proporcionan los siguientes detalles:

  - Número de intentos de inicio de sesión en un portal empresarial por parte de un usuario específico desde una dirección IP particular.
  - Si una aplicación o un conector de aplicaciones se incorpora o se elimina.
  - Cuando se programa una actualización del Conector.
  - Vista de todos los cambios del sistema y los accesos intentados.

  Los logs de auditoría de ZTNA Connector no están disponibles en la interfaz web de Prisma Access. Para ver los logs de auditoría, debe abrir un caso de asistencia con la asistencia técnica de Palo Alto Networks.
- **Traffic logs (Logs de tráfico)**: los logs de tráfico muestran una entrada para el inicio y el final de cada sesión. Todas las entradas incluyen la fecha y la hora, las zonas de origen y destino, las direcciones y los puertos, el nombre de la aplicación, el nombre de la regla de seguridad aplicada al flujo, la acción de la regla (permitir, denegar o descartar), la interfaz de entrada y salida, el número de bytes y la razón para finalizar la sesión.
  - La columna Type (Tipo) indica si la entrada es para el inicio o el final de la sesión.
  - La columna Action (Acción) indica si el cortafuegos permitió, denegó o descartó la sesión.
  - El descarte indica que la regla de seguridad que ha bloqueado el tráfico ha especificado una aplicación cualquiera, mientras que la denegación indica que la regla ha identificado una aplicación específica.
  - Si el cortafuegos descarta el tráfico antes de identificar la aplicación, como cuando una regla descarta todo el tráfico para un servicio específico, la columna Application muestra not-applicable.
  - El App-ID para un ZTNA Connector es el App-ID personalizado.
  - Si el tráfico llega a la puerta de enlace del Usuario móvil, la columna **Destination Address (Dirección de destino)** muestra la dirección IP RFC 6598.
- **Logs de configuración**: muestran entradas de los cambios en la configuración de ZTNA Connector. Cada entrada incluye la fecha y hora, el nombre de usuario del administrador, la dirección IP desde la cual se realizó el cambio, el tipo de cliente (Web, CLI o Panorama), el tipo de comando ejecutado, el estado del comando (si se ejecutó correctamente o falló), la ruta de configuración y los valores anteriores y posteriores al cambio.
- Strata Cloud Manager
- Panorama

Ver logs de ZTNA Connector (Panorama)

Utilice el siguiente flujo de trabajo para ver los logs del ZTNA Connector en Prisma Access (Managed by Panorama) Access.

STEP 1 | Inicie sesión en Prisma Access.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Monitor (Supervisar)** > **Logs**.

STEP 3 | Seleccione un tipo de log de la lista: Logs de **Audit (Auditoría)**, **Traffic (Tráfico)** y **Config (Configuración)**.

STEP 4 | Haga clic en la flecha a la derecha de cualquier encabezado de columna y seleccione **Columns**.

STEP 5 | Seleccione las columnas para mostrar las listas. El log se actualiza automáticamente para coincidir con sus selecciones.

STEP 6 | Haga clic en el icono de **lupa** para ver una entrada de log específica. La **Detailed Log View (Vista detallada de logs)** tiene más información sobre el origen y destino de la sesión, además de una lista de sesiones relacionadas con la entrada del log.

Ver logs de ZTNA Connector (Strata Cloud Manager)

Utilice el siguiente flujo de trabajo para ver los logs de ZTNA Connector en Cloud Managed Prisma Access.

STEP 1 | Inicie sesión en Prisma Access (Managed by Strata Cloud Manager).

STEP 2 | Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.

STEP 3 | Seleccione el tipo de log que desea ver: Logs de auditoría, cortafuegos/tráfico y Configuración.

STEP 4 | Seleccione un rango de tiempo para el cual desea ver los logs.

STEP 5 | Proporcione esta cadena de consulta para limitar la lista de logs del ZTNA Connector: **Subtype = 'netflow' AND Device Name = 'PA_CONN'** .

Los logs incluyen los siguientes detalles:

- Marca de tiempo
- Nombre del conector
- Dirección IP de origen original del cliente
- Puerto de origen original del cliente
- Dirección IP traducida del Conector
- Puerto traducido del Conector
- Dirección IP de destino traducida
- Puerto de destino traducido

 ©2025 Palo Alto Networks, Inc.

Preservar la asignación de User-ID para las conexiones de ZTNA Connector con NAT de origen

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.1.1

Puede usar ZTNA Connector en Prisma Access para proteger aplicaciones privadas. Para limitar el acceso a las aplicaciones en función del User-ID, puede implementar un Cortafuegos de nueva generación (NGFW) en el centro de datos o en la ubicación de la sede donde se encuentran las aplicaciones privadas; luego, configure las reglas de política en el NGFW basadas en la asignación de User-ID.

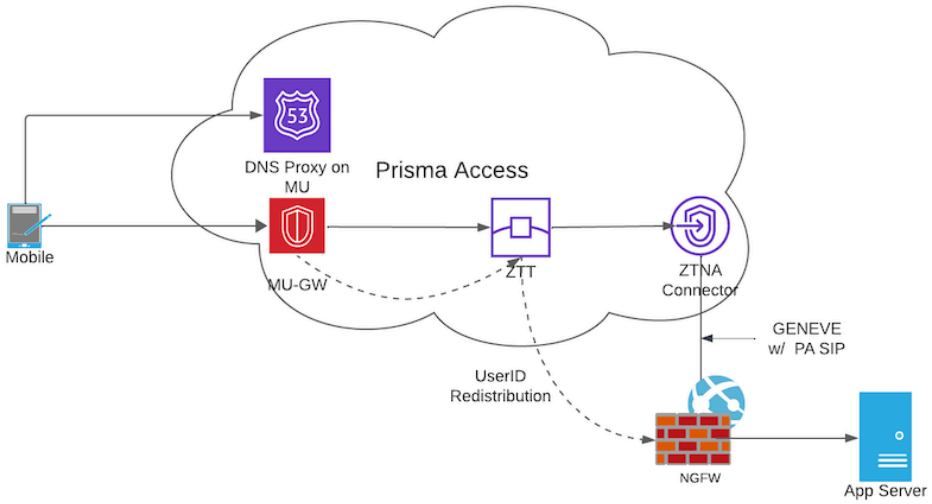
Si su implementación utiliza un cortafuegos de nueva generación (NGFW) en el centro de datos o en la ubicación de la sede donde se encuentran las aplicaciones privadas, y el ZTNA Connector realiza la NAT de origen, el NGFW no puede recuperar la asignación de User-ID. La NAT de origen en el ZTNA Connector impide que el NGFW obtenga la dirección IP del cliente, que es esencial para la asignación. Si el NGFW no puede recuperar esta dirección IP del cliente, no puede hacer cumplir las reglas de la política de seguridad basada en zonas que has creado en él, basado en la asignación de User-ID.

ZTNA Connector tiene las siguientes responsabilidades para habilitar User-ID dentro del centro de datos protegido por NGFW:

1. Proporcionar una conexión segura desde el NGFW a los Terminadores de túnel del ZTNA Connector regional (ZTT) para que el NGFW se conecte a su agente de redistribución de User-ID.
2. Para aplicaciones FQDN, con la sonda de salud configurada en tcpping, la sonda de la aplicación verifica las aplicaciones del centro de datos para determinar si la aplicación está activa y es accesible desde este conector individual.
3. Encapsular los paquetes IP post-NAT del espacio del centro de datos del usuario a la aplicación dentro de un paquete Geneve, incluyendo la dirección IP de origen original como una opción.

El siguiente diagrama ilustra los elementos de la red que proporcionan la dirección IP de origen para la asignación de User-ID al NGFW y entregan paquetes de datos encapsulados de Virtualización de Red Genérica (Geneve) que incluyen la opción de dirección IP de origen de Prisma Access al NGFW. Estos elementos permiten que el NGFW aplique de manera efectiva las reglas de política de seguridad basadas en User-ID.

©2025 Palo Alto Networks, Inc.



Restricciones

- La compatibilidad de User-ID con ZTNA Connector solo está disponible después de estas versiones:
  - Plano de datos de Prisma Access: Versión 10.2.4 y posteriores
  - Saas_agent: Versión 5.1.0 y versiones posteriores de
  - NGFW: Versión 11.2.0 y posterior
  - Versión del conector: Versión 6.2.4-ztna-connector-b3 y posteriores
- El sondeo ICMP no es compatible con objetivos FQDN, que están vinculados a grupos de conectores basados en User-ID.
- La configuración de la ruta del servicio de NGFW para un agente UID solo admite interfaces con direcciones IP estáticas. Si la interfaz del NGFW está configurada para estar en un modo dinámico (asignación de dirección IP a través de DHCP), el canal User-ID de NGFW a ZTT no puede establecer soporte para el User-ID del ZTNA Connector. Para resolver este problema, debe configurar la interfaz que se utilizará para el agente UID en NGFW con una dirección IP estática.
- Las herramientas de diagnóstico como ping y traceroute no son compatibles con los conectores basados en User-ID.

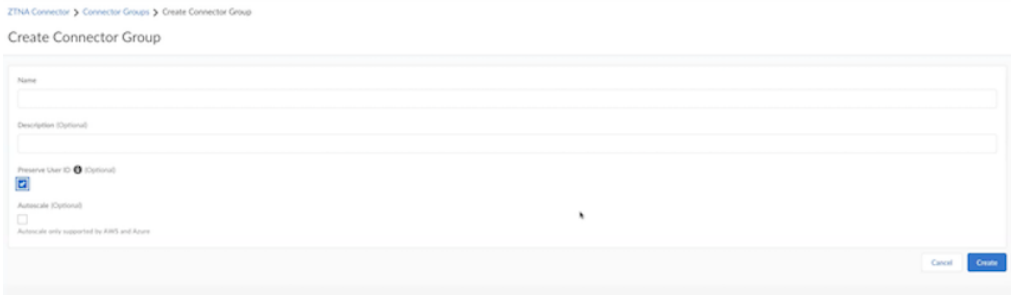
Este procedimiento asume que tiene las siguientes configuraciones de red en su lugar:

- Ha desplegado un NGFW en la sede o centro de datos donde se encuentran las aplicaciones privadas.
- Ha aplicado reglas de política de seguridad al cortafuegos NGFW basadas en las zonas (zona no fiable y zona fiable) que ha creado en el NGFW. Estas reglas de política de seguridad incluyen la aplicación de User-ID.

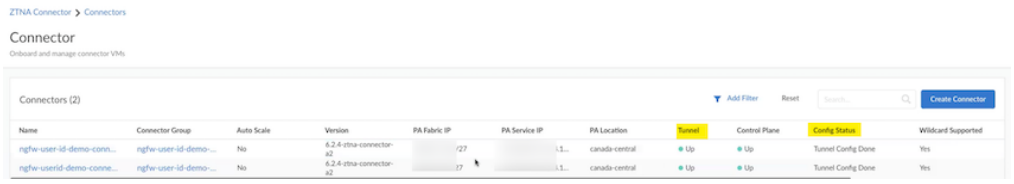
Para asegurarse de que su red distribuya la asignación de User-ID a la sede o al centro de datos, completa el procedimiento que se indica a continuación, que permite al NGFW hacer cumplir las reglas de la política de seguridad basadas en la asignación de User-ID que aprende de GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

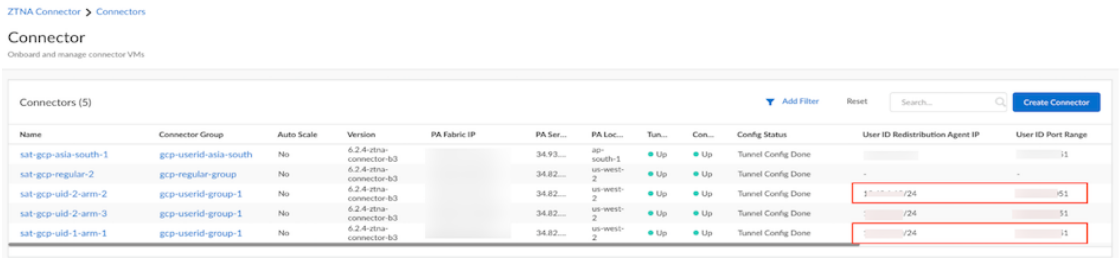
STEP 1 | Cree un Grupo de conectores, habilite la opción **Preserve User ID (Preservar ID de usuario)** y añada los Connectors (Conectores).



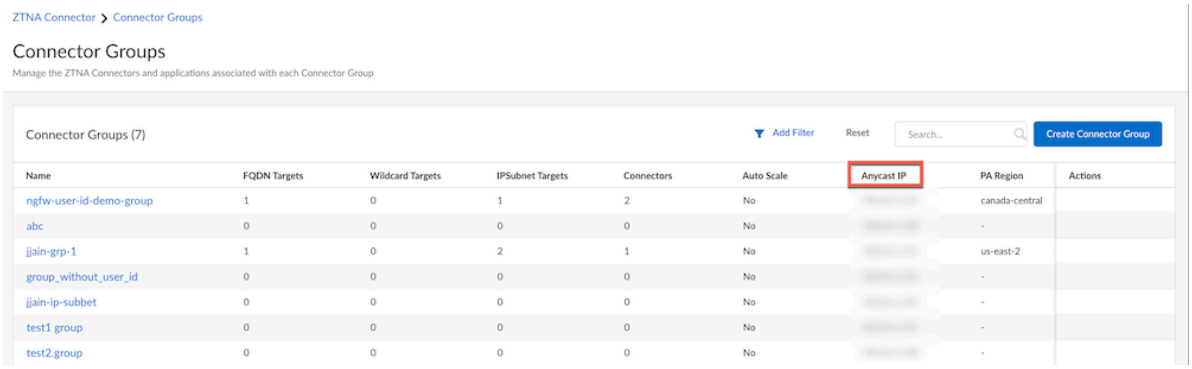
STEP 2 | Implementar e incorporar los conectores en su centro de datos y verificar si los túneles están activos y funcionando.



STEP 3 | Vaya a **Connector (Conector)** y toma nota de la **User ID Redistribution Agent IP (IP del agente de redistribución de ID de usuario)** y del **User ID Port Range (Rango de puertos de ID de usuario)** para su conector. Necesita estas direcciones IP y rangos de puertos para configurar los agentes de redistribución de User-ID en el NGFW.



Además, vaya a **Connector Groups (Grupos de conectores)** y toma nota de la **Anycast IP (IP de Anycast)**. Esta dirección de IP es necesaria para configurar las reglas de política de seguridad de NGFW para permitir la exploración de la aplicación TCP desde esta dirección IP de origen.



 ©2025 Palo Alto Networks, Inc.

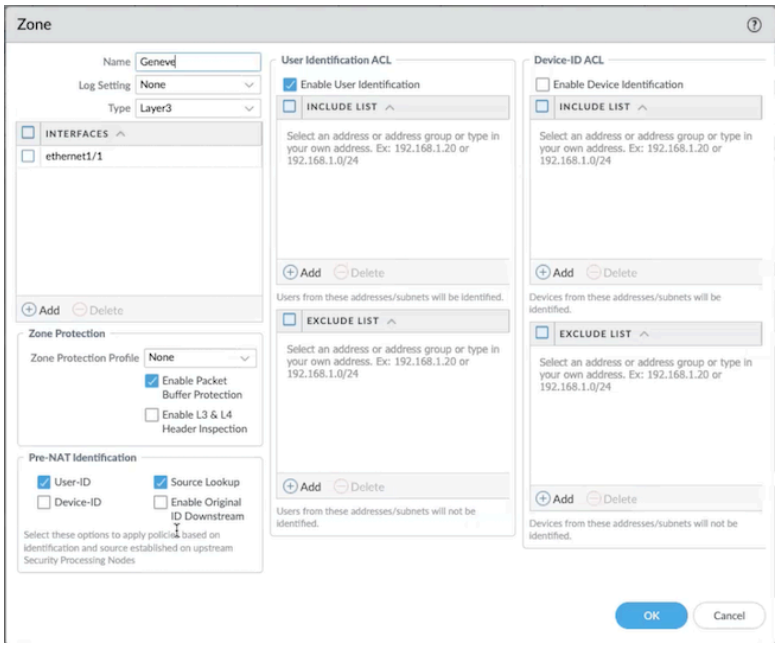
STEP 4 | Introduce parámetros de identificación pre-NAT en el NGFW.

1. Inicie sesión en la interfaz de usuario de NGFW, vaya a **Network (Red)** > **Zones (Zonas)**y seleccione **Add (Añadir)** para añadir 2 zonas (zona para la interfaz que conecta el ZTNA

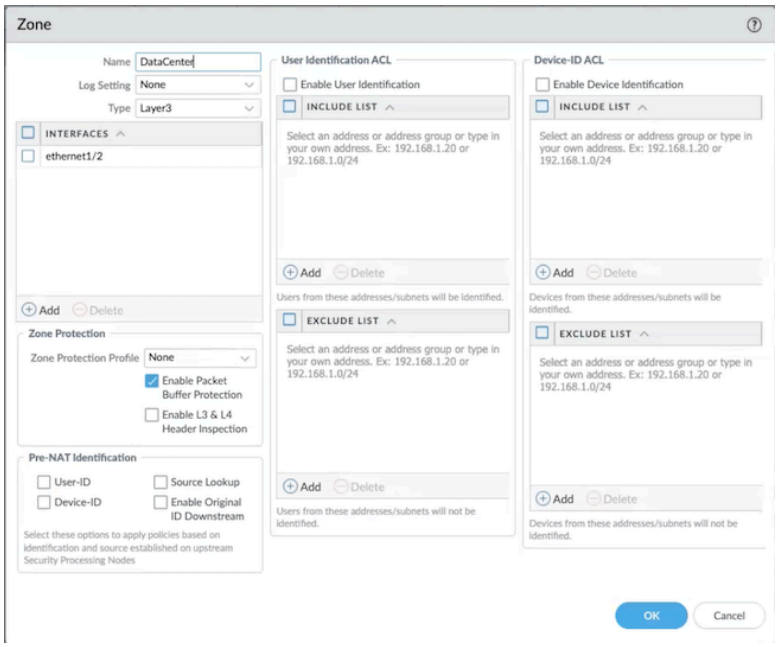
 ©2025 Palo Alto Networks, Inc.

Connector y zona para la interfaz que conecta el servidor de aplicaciones) o seleccione la existente.

1. Seleccione los siguientes parámetros de **Pre-NAT Identification (Identificación Pre-NAT)** para la zona con la interfaz que conecta a ZTNA Connector:
   - **User-ID**: preserva la asignación del User-ID móvil utilizado antes de que las direcciones IP sean asignadas por NAT. Habilite esto si está utilizando User-ID en las reglas de la política de seguridad.
   - **Búsqueda de fuente**: le permite hacer coincidir la dirección IP de origen original recibida de GlobalProtect.



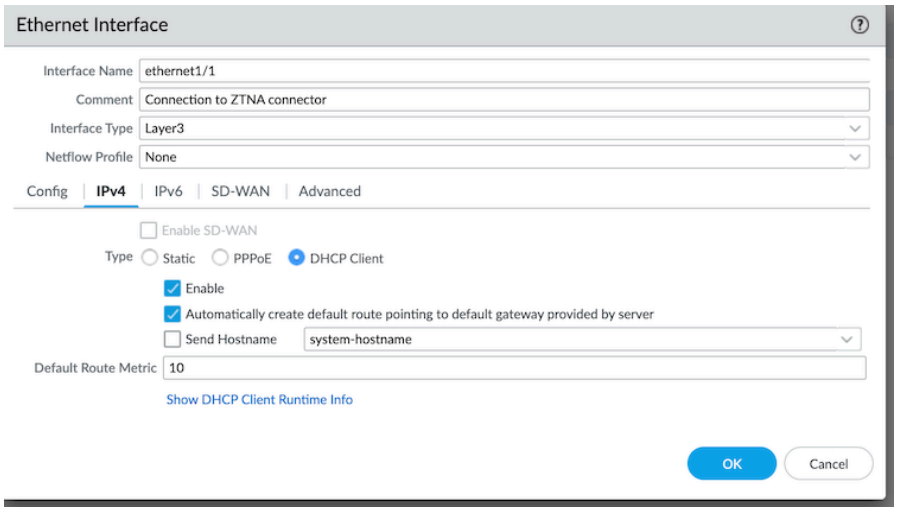
2. Para la interfaz que se conecta a la zona del servidor de aplicaciones, no es necesario seleccionar ningún parámetro de **identificación Pre-NAT**.



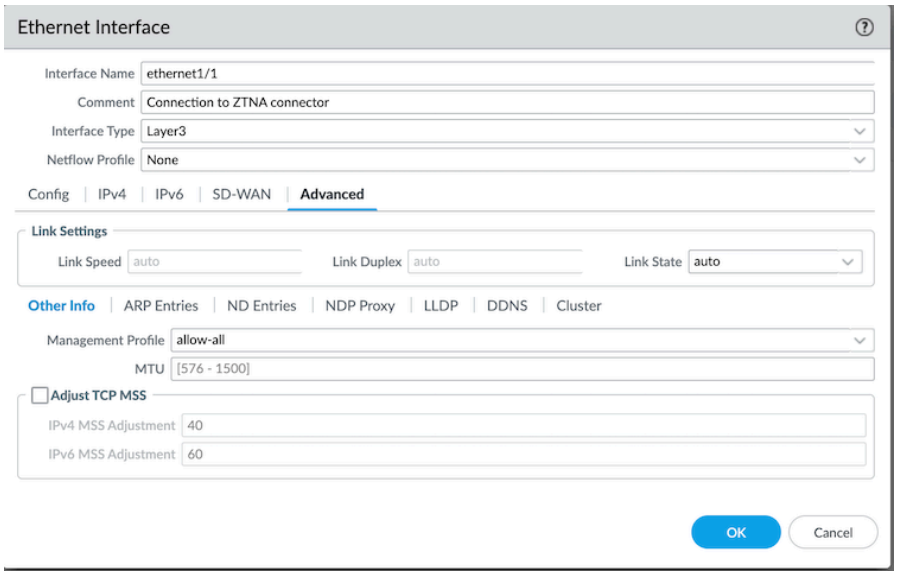
 ©2025 Palo Alto Networks, Inc.

3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

2. Añada las direcciones IP a las interfaces.
   1. Vaya a **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**.
   2. Seleccione la interfaz que se conecta a ZTNA Connector y al servidor de aplicaciones, y configúrelas. Añada el **Interface name (Nombre de la interfaz)** y el **Interface type (Tipo de interfaz)** a la **Layer 3 (Capa 3)**.



   3. Para la interfaz Ethernet conectada al servidor de aplicaciones, deseleccione la casilla de verificación **Crear automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor**.



3. Vaya a **Interfaces** y añada las direcciones IP estáticas a las interfaces. Añada la interfaz orientada al ZTNA Connector a la zona del ZTNA Connector (Ginebra) y la interfaz orientada al servidor de aplicaciones a la zona del servidor de aplicaciones (Centro de Datos).

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Cree una sesión de interfaz de línea de comandos (CLI) con el NGFW e introduzca el siguiente comando en el modo de configuración:

```
set deviceconfig setting preserve-prenat-feature yes
```

Si necesita deshabilitar esta función en el futuro, introduzca `set deviceconfig setting preserve-prenat-feature no`.

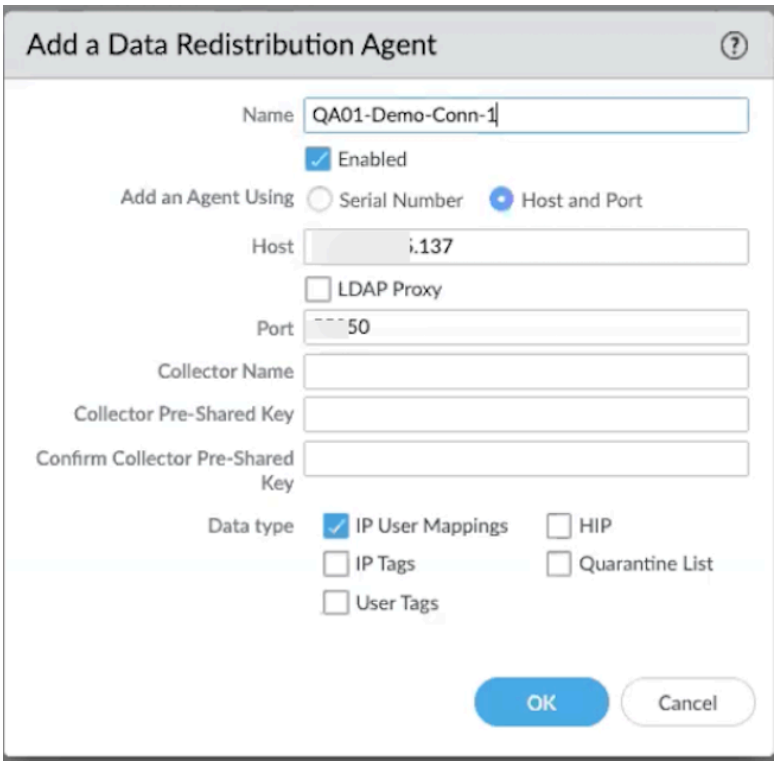
 ©2025 Palo Alto Networks, Inc.

STEP 6 | *Al configurar la redistribución de User-ID, debe añadir una entrada de agente de redistribución para cada puerto dentro del rango especificado en el paso 3**User ID Port Range (Rango de puertos de ID de usuario)**. Por ejemplo, si el rango es 55050-55055, tiene que configurar 6 entradas, alineándose con el número de regiones de ZTNA Connector que ha implementado.*

*Para cada puerto en el rango, seleccione una dirección IP de la **IP del agente de redistribución de ID de usuario** en el paso 3 para el campo **Host**. Si desea redundancia a nivel del ZTNA Connector, puede elegir dos direcciones de la **IP del agente de redistribución de ID de usuario** y aplicar el rango completo de puertos para ambas direcciones IP. Como alternativa, se pueden configurar todos los puertos en todas las direcciones **IP del agente de redistribución de ID de usuario**.*

Añada un agente de redistribución para cada uno de los puertos en el **User ID Port Range (Rango de ID de usuario)** con una o más de las direcciones en la **IP del agente de redistribución del ID de usuario**.

1. En la interfaz de NGFW, vaya a **Device (Dispositivo)** y luego seleccione **Data Redistribution (Redistribución de Datos)**.
2. Haga clic en **Add (Añadir)**, añada el **Name (Nombre)** y seleccione la casilla de verificación **Enabled (Habilitado)**.
3. Seleccione **Host and Port (Host y puerto)**, añada la **User ID Redistribution Agent IP (IP del agente de redistribución de ID de usuario)** del paso 3 en **Host** y añada el **User ID Port Range (Rango de puerto de ID de usuario)** copiado en el paso 3.
4. Habilite la casilla de verificación **IP User Mappings (Asignaciones de usuarios IP)** y haga clic en **OK (Aceptar)**.

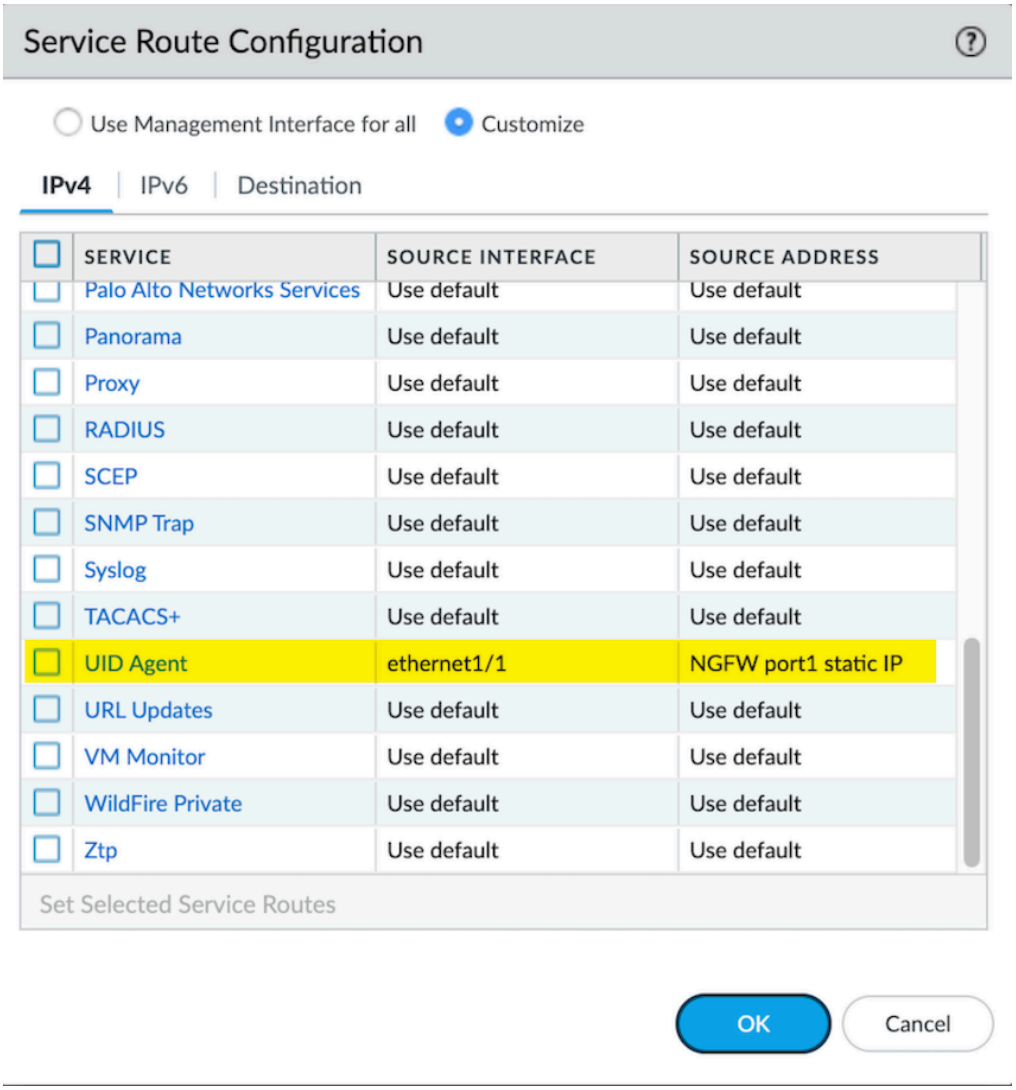


 ©2025 Palo Alto Networks, Inc.

5. Haga clic en **Commit (Confirmar)** para guardar la configuración.

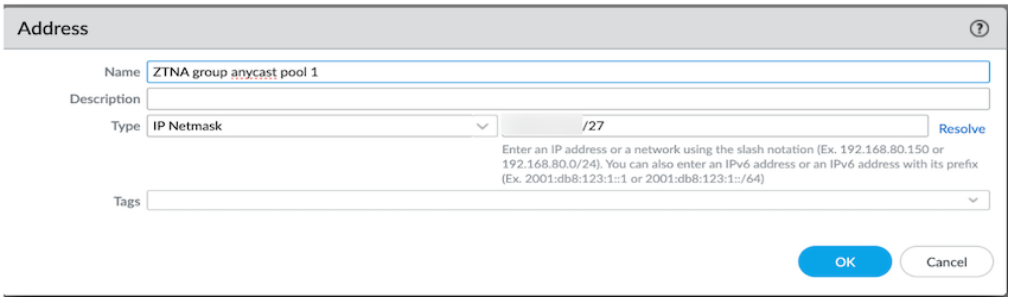
STEP 7 | En la interfaz de NGFW, vaya a **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Service Route Configuration (Configuración de ruta de servicio)** > **Customize (Personalizar)** > **UID agent (Agente de UID)**.

1. En **IPv4**, seleccione la **SOURCE INTERFACE (INTERFAZ DE ORIGEN)** como **Ethernet1/1** (interfaz orientada a ZTNA Connector), y añade la **DIRECCIÓN DE ORIGEN**.



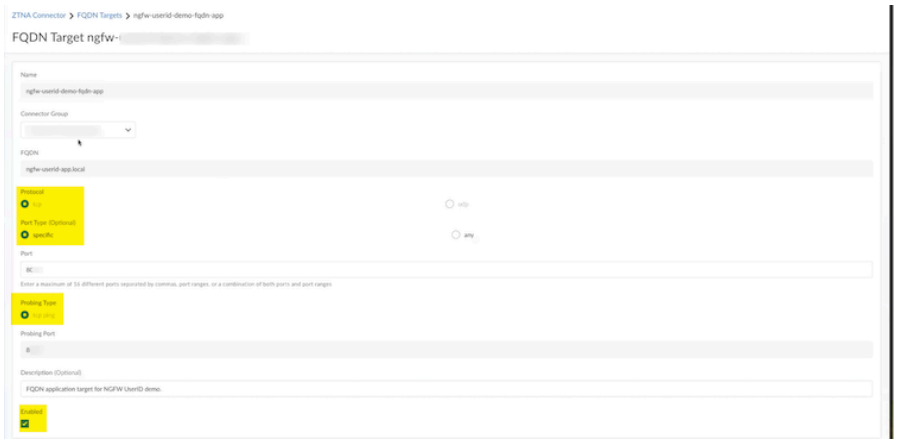
 ©2025 Palo Alto Networks, Inc.

STEP 8 | Añadir una regla de política de seguridad para permitir paquetes TCP con la dirección IP de origen. Añada la dirección IP de origen, que es la dirección IP Anycast copiada en el paso 3 y haga clic en **OK (Aceptar)**.

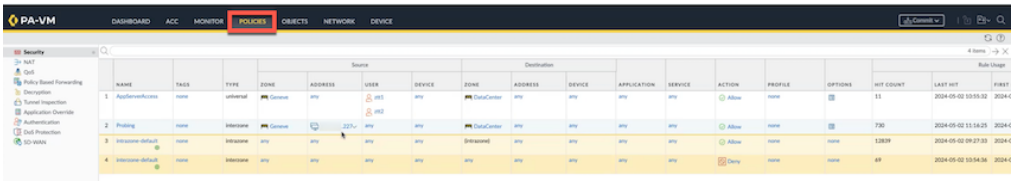


STEP 9 | (Opcional) Habilitar Sondeo de TCP.

1. Para crear un objetivo FQDN:
   1. Vaya a **Workflows (Flujos de trabajo)** > **Application Targets (Objetivos de aplicación)** > **FQDN Targets (Objetivos FQDN)** y haga clic en **Create FQDN Target (Crear Objetivo FQDN)**.
   2. Añada un **Name (Nombre)** y seleccione **Connector Group (Grupo de conectores)**.
   3. Habilite **tcp**, **specific (específico)**, **tcp ping (ping tcp)**y **Enabled (Habilitado)**. Añada el **Port (Puerto)** y haga clic en **Create (Crear)**.



STEP 10 | En la interfaz de NGFW, vaya a **Policies (Políticas)** y defina las políticas basadas en User-ID.



 ©2025 Palo Alto Networks, Inc.

Configurar la configuración de acceso a privilegios dinámicos

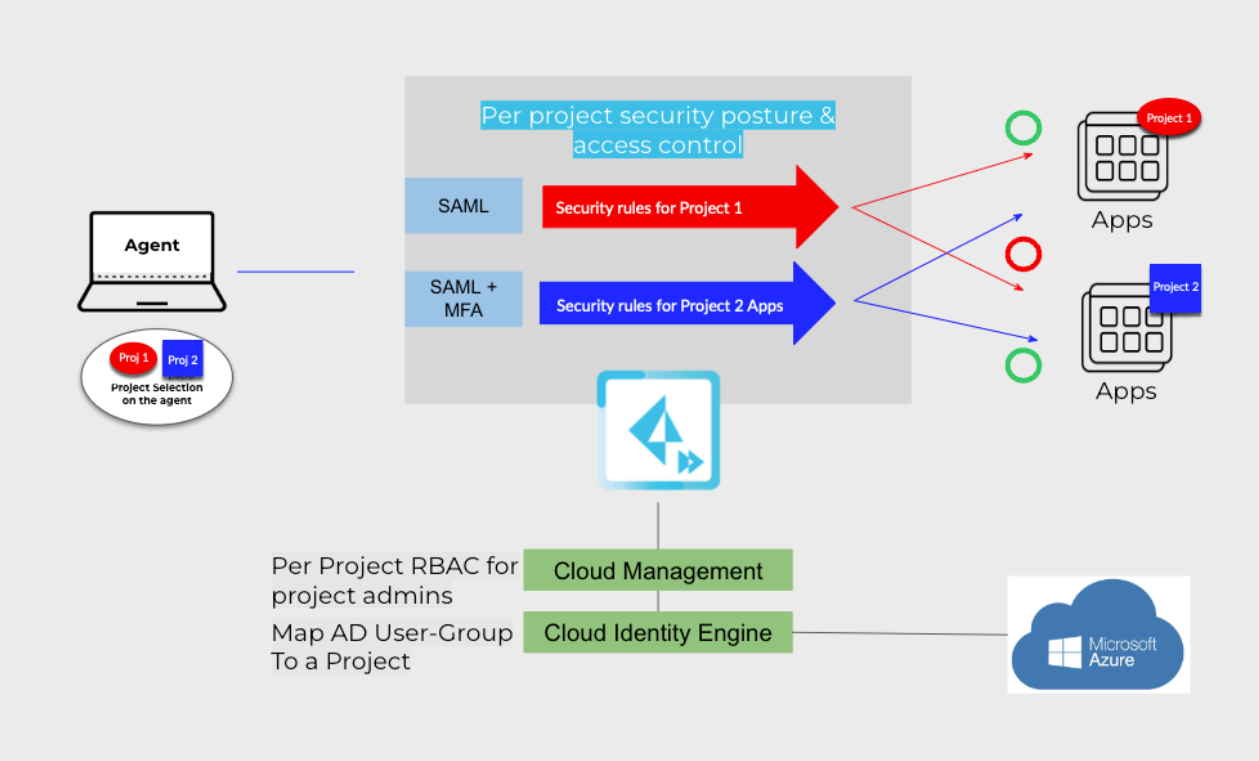
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access ❑ Prisma Access 5.1 ❑ Rol: Superusuario

Para las empresas de servicios de TI y servicios habilitados por TI (ITES) que necesitan controlar qué usuarios tienen acceso a sus proyectos de clientes, el *Acceso dinámico a privilegios* proporciona una forma fluida, segura y compartimentada para que sus usuarios accedan solo a aquellos proyectos a los que están asignados. Estas empresas suelen asignar varios proyectos de clientes a los empleados y proporcionar acceso aislado a estos proyectos para que un usuario autorizado solo pueda acceder a un proyecto de cliente a la vez.

¿Qué es Acceso dinámico a privilegios?

El Acceso dinámico a privilegios es una función en Prisma Access que proporciona privilegios dinámicos para sus usuarios en función del flujo de trabajo o proyecto que sus usuarios seleccionen en el Prisma Access Agent. Tus usuarios pueden tener privilegios dinámicos basados en la combinación del grupo de usuarios y el grupo de IP que se asigna a un proyecto. Esta combinación única define un proyecto. Con Acceso dinámico a privilegios, puede aislar recursos en su red para que solo sean accesibles para sus usuarios según los proyectos a los que estén asignados.

Un nuevo rol predefinido llamado **Project Admin (Administrador de proyecto)** está disponible en Prisma Access para permitir a los administradores de proyectos crear y gestionar definiciones de proyectos. Los administradores de proyectos tienen la capacidad de asignar proyectos a grupos de ubicación de Prisma Access seleccionados y crear asignaciones de direcciones IP utilizando DHCP en función del proyecto y del grupo de ubicación. Los administradores de proyectos solo pueden gestionar los proyectos a los que están asignados en Strata Cloud Manager.



Cuando sus usuarios finales inician sesión en un Prisma Access Agent que está habilitado para el Acceso dinámico a privilegios en sus dispositivos gestionados, se lleva a cabo el siguiente flujo de trabajo:

1. El usuario final selecciona un proyecto al que está asignado (por ejemplo, Proyecto 1).
2. Su identidad está autenticada en Cloud Identity Engine, que asigna el grupo de usuarios del usuario al proyecto.
3. Una vez que se haya autenticado correctamente y su grupo de usuarios coincida con los criterios del proyecto establecidos por el administrador del proyecto, el usuario tiene acceso a los recursos en la red a través de configuraciones específicas del proyecto para Project 1

 ©2025 Palo Alto Networks, Inc.

(Proyecto 1) y reglas de seguridad que proporcionan una postura de seguridad y control de acceso por proyecto. La infraestructura de seguridad aplica reglas de seguridad para restringir el acceso de los usuarios solo a los recursos y aplicaciones que pertenecen a ese proyecto. No se permite el acceso a recursos y aplicaciones de otros proyectos.

4. Cuando el usuario cambia a un proyecto diferente (por ejemplo, Proyecto 2), se cierra sesión en el proyecto anterior (Proyecto 1). A continuación, pueden acceder a los recursos del segundo proyecto basándose en la configuración específica del proyecto y las reglas de seguridad para ese proyecto.

Puede obtener visibilidad sobre su implementación de Prisma Access Agent utilizando Strata Cloud Manager para supervisar la actividad del proyecto de sus usuarios y ver el consumo de servicios y la postura de seguridad en su red.

 ©2025 Palo Alto Networks, Inc.

Habilite el acceso dinámico a privilegios para Prisma Access a través de Common Services

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access con suscripción de usuario móvil ❑ Enlace de activación ❑ Strata Logging Service ❑ Motor de identidad en la nube ❑ Prisma Access Agent ❑ Rol: Superusuario multiinquilino o Superusuario con acceso al Portal de atención al cliente

Con Acceso dinámico a privilegios, los administradores de TI pueden asignar usuarios finales a varios proyectos de clientes. Un usuario autorizado solo obtiene el acceso a un proyecto de cliente a la vez.

Dynamic Privilege Access (Acceso dinámico a privilegios) es una característica opcional durante la activación de un nuevo inquilino de Prisma Access. Una vez habilitada esta característica y activado el inquilino, el DPA se establece durante toda la vida útil del inquilino y no se puede deshabilitar.

La opción de habilitar DPA solo está disponible una vez durante la primera activación de un nuevo inquilino de Prisma Access. Una vez activado el inquilino, la opción se oculta para todas las activaciones siguientes, incluidos los complementos y las renovaciones. No está disponible para los inquilinos existentes.

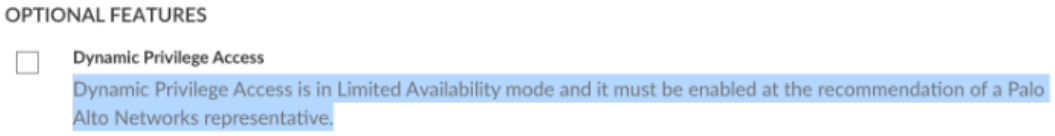
STEP 1 | Póngase en contacto con el representante de cuentas de Palo Alto Networks para activar esta funcionalidad para su inquilino.

STEP 2 | Activate (Activar) la licencia para su Prisma Access (Managed by Strata Cloud Manager).

STEP 3 | Asegúrese de asignar licencias, planificar sus conexiones de servicio y añadir ubicaciones adicionales en consecuencia.

STEP 4 | Habilitar los complementos disponibles.

STEP 5 | Seleccione la casilla de verificación para **Dynamic Privilege Access (Acceso dinámico a privilegios)**.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | Deberá **Agree to the Terms and Conditions (Aceptar las condiciones)**.

STEP 7 | **Activar ahora** Los productos y complementos que está activando (como Prisma Access o Strata Logging Service) ahora están aprovisionados. A medida que se activan las suscripciones, se mostrará el estado de progreso. Una vez finalizado el proceso, el estado del inquilino se muestra como `Up (Activo)`. Ahora tiene un inquilino aprovisionado con instancias de los productos que compró. El inquilino tiene un usuario: la cuenta que usó cuando comenzó este proceso.

STEP 8 | Para completar la configuración restante del producto, debe acceder a los productos que ha comprado y realizar cualquier configuración posterior a la instalación requerida. Para obtener información sobre sus productos, consulte:

- API abiertas
- Guía de introducción a Strata Logging Service
- Guía para los administradores de Prisma Access (Managed by Strata Cloud Manager)
- Guía de introducción de Cloud Identity Engine

STEP 9 | Añadir acceso de usuario y asignar funciones.

Proporcione acceso a los usuarios como **Project Admin (Administrador de proyectos)** basado en proyectos.

 ©2025 Palo Alto Networks, Inc.

Autoriza la asignación de grupos de usuarios en Cloud Identity Engine para el acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access ❑ Versión mínima de Prisma Access requerida: 5.1 ❑ Rol: Superusuario

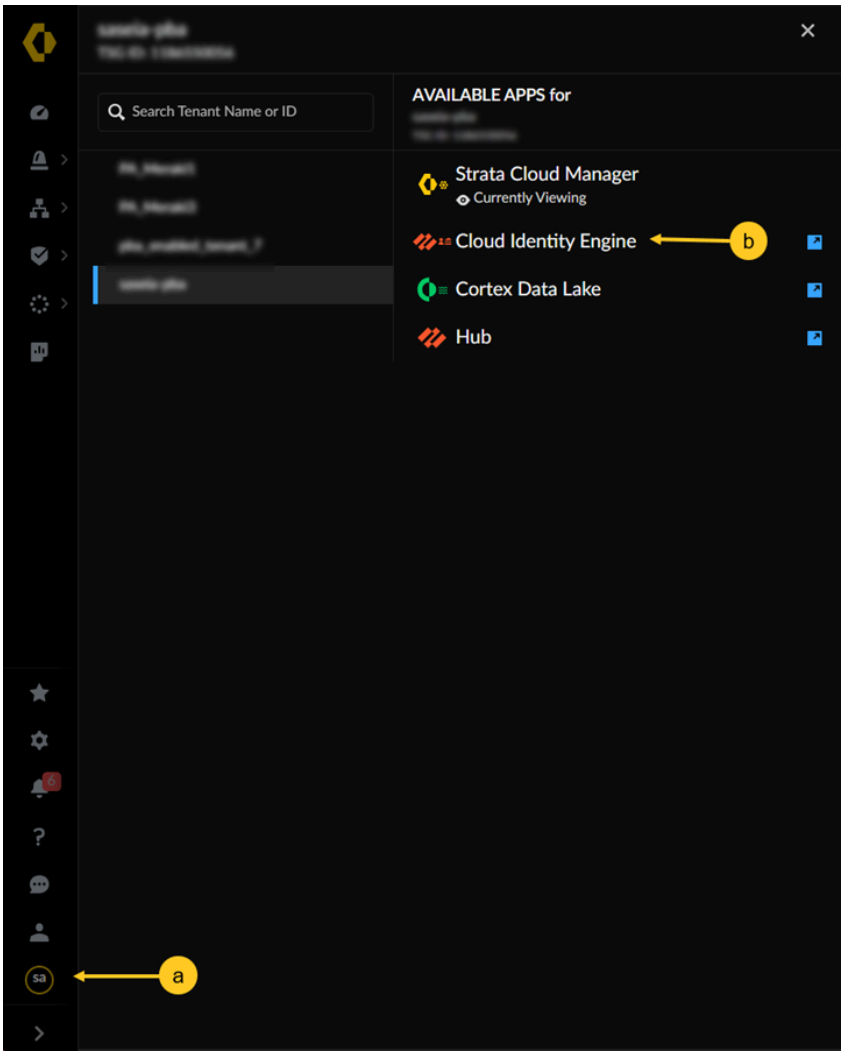
Antes de comenzar, asegúrese de haber completado los siguientes requisitos previos:

- Ponerse en contacto con su representante de cuentas de Palo Alto Networks para activar la funcionalidad de acceso dinámico a privilegios.
- Activar Cloud Identity Engine y crear su primer inquilino.
- Configurar Cloud Identity Engine.

En este flujo de trabajo, hemos usado Azure como IdP. También puede usar Okta como su IdP.

©2025 Palo Alto Networks, Inc.

STEP 1 | En Strata Cloud Manager, abra la aplicación Cloud Identity Engine asociada a su inquilino.



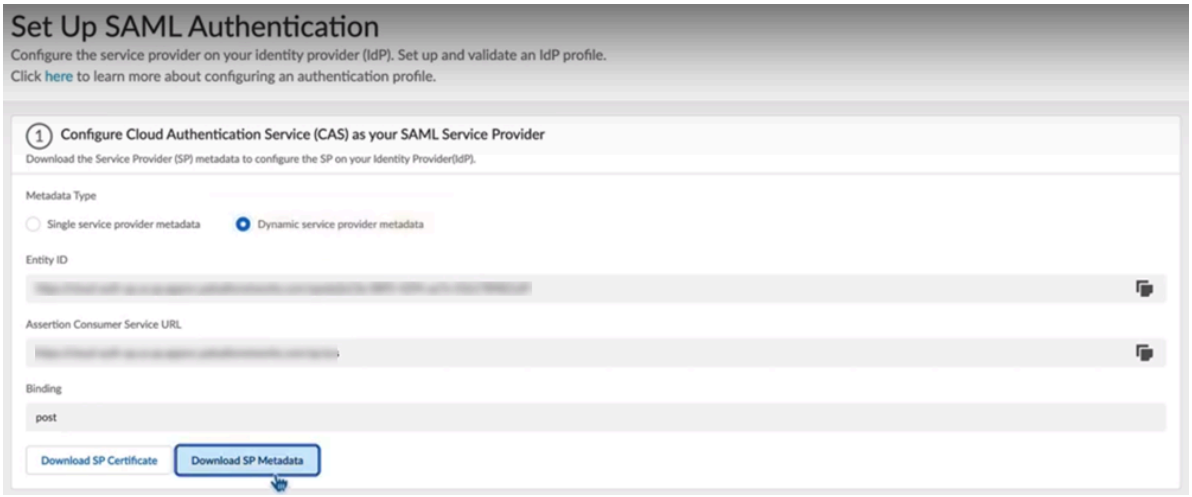
STEP 2 | Añada un directorio de Azure o un directorio de Okta como IdP para usuarios móviles.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Descargue los metadatos de SP en la aplicación de Cloud Identity Engine.

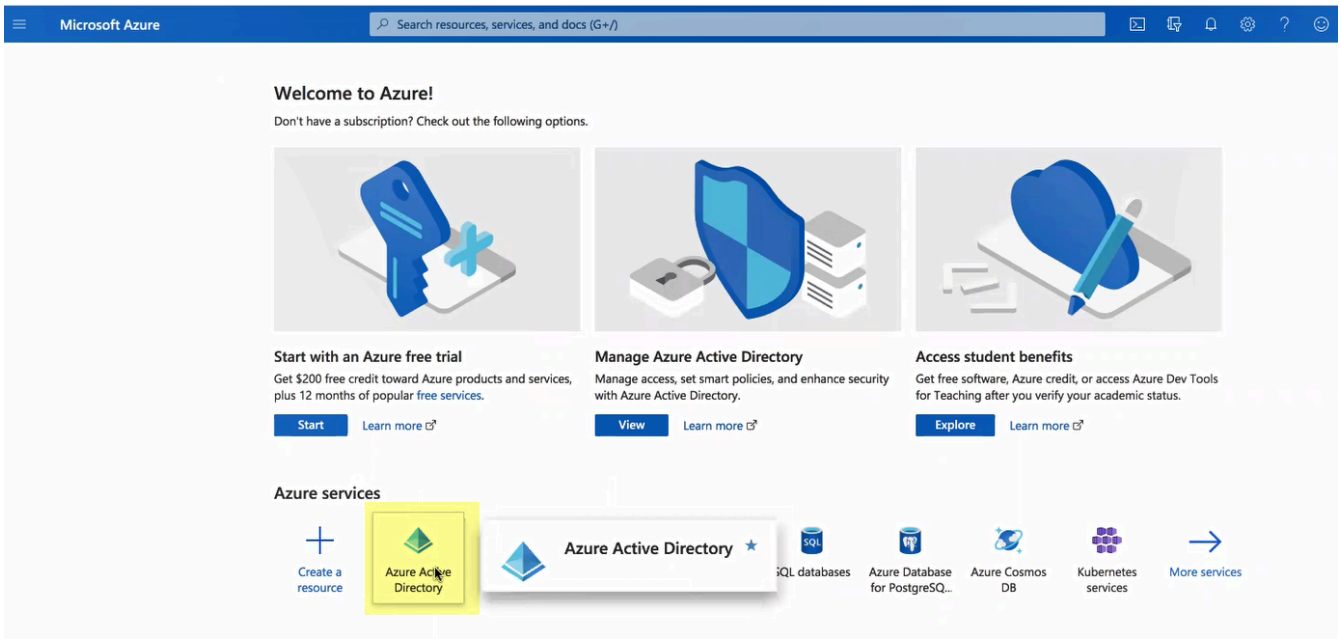
1. Vaya a **Authentication (Autenticación)** > **Authentication Types (Tipos de autenticación)** > **Add New Authentication Type (Añadir nuevo tipo de autenticación)**.
2. **Set Up (Configurar)** un tipo de autenticación SAML 2.0.

   Seleccione **Dynamic service provider metadata (Metadatos dinámicos del proveedor de servicios)**.
3. **Download SP Metadata (Descargar metadatos de SP)**.



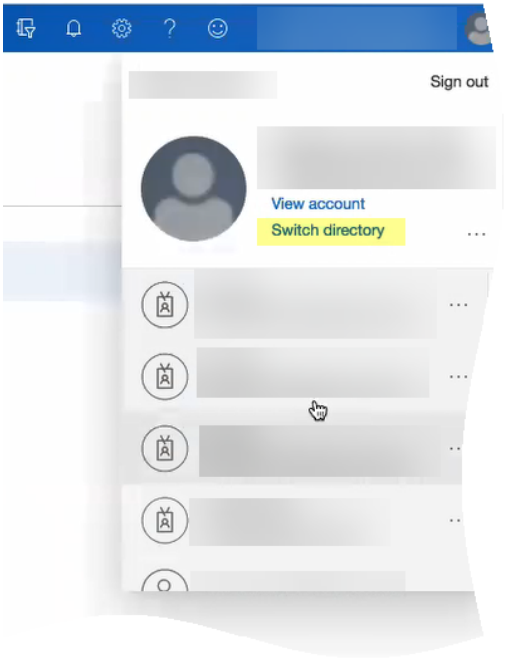
4. Inicie sesión en el Azure Portal y seleccione **Azure Active Directory**.

   ¡Asegúrese de completar todos los pasos necesarios en Azure Portal.

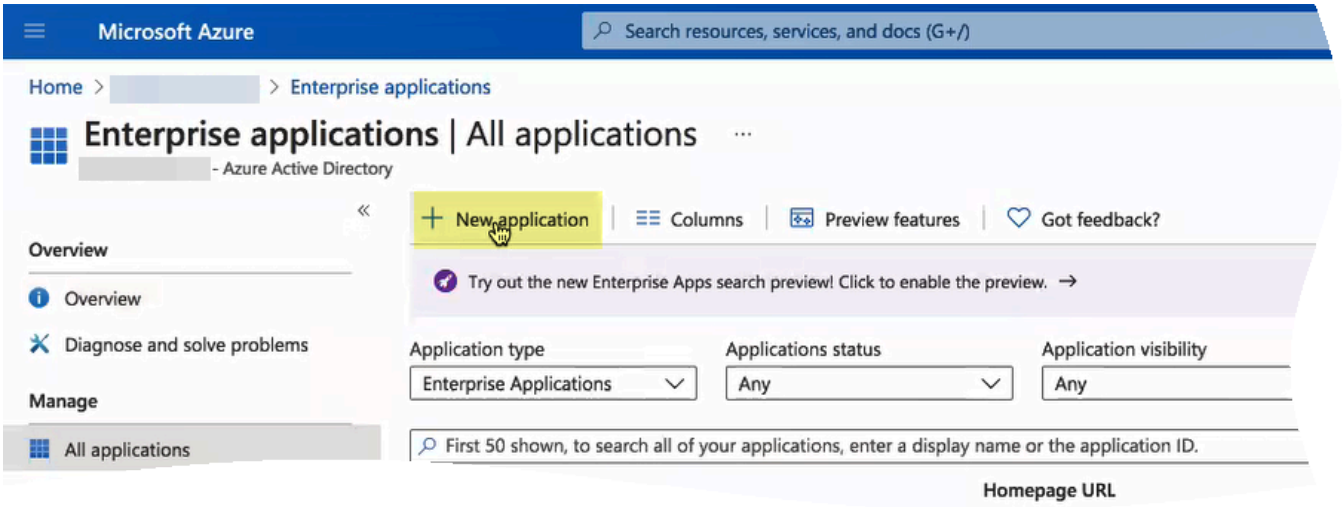


   Si tiene más de un directorio, seleccione **Switch directory (Cambiar directorio)** para seleccionar el directorio que desea usar con Cloud Identity Engine.

 ©2025 Palo Alto Networks, Inc.



5. Seleccione **Enterprise applications (Aplicaciones empresariales)** y haga clic en **New application (Nueva aplicación)**.



6. Busque **`Cloud Identity Engine de Palo Alto Networks: servicio de autenticación en la nube`** y seleccione crear la integración de inicio de sesión único de Azure Active Directory (AD).

   Personalice el nombre de la aplicación si es necesario al crear la aplicación.

7. Una vez cargada la aplicación, seleccione **Users and groups (Usuarios y grupos)** y luego **Add user/group (Añadir usuario/grupo)** para **Assign (Asignar)** a esta aplicación.

   Seleccione los usuarios y grupos que desea que usen el IdP de Azure en Cloud Identity Engine para la autenticación.

 ©2025 Palo Alto Networks, Inc.

> *Asegúrese de asignar la cuenta que está utilizando para que pueda probar la configuración cuando se complete. Es posible que deba actualizar la página después de añadir cuentas para completar correctamente la prueba.*

8. Deberá **Set up single sign-on (Configurar el inicio de sesión único)** y, a continuación, seleccione **SAML**.
9. Seleccione **Upload Metadata File (Cargar archivo de metadatos)**navegando hasta el archivo de metadatos que descargó de la aplicación de Cloud Identity Engine, en el paso 3.c y haga clic en **Add (Añadir)**.
10. Una vez cargados los metadatos, introduzca el endpoint regional como **Sign-on URL (URL de inicio de sesión)** utilizando el siguiente formato: https://<RegionUrl>.paloaltonetworks.com/sp/acs (donde <RegionUrl> es el endpoint regional).

    Como alternativa, copie la URL de respuesta en la URL de inicio de sesión.
11. Seleccione **Save (Guardar)** su configuración.

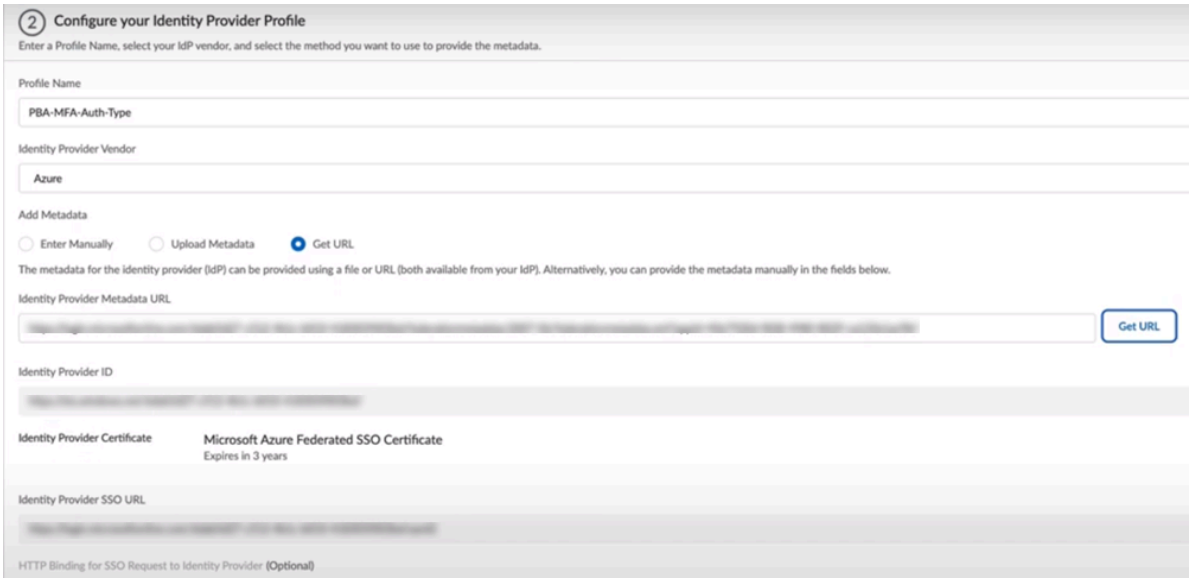
STEP 4 | Configure la política de acceso condicional para habilitar MFA en los grupos de usuarios seleccionados.

1. Vaya a la carpeta de su aplicación **Overview (Descripción general)** > **Conditional Access (Acceso condicional)** > **Create a policy (Crear una política)**.
2. Añada una nueva **Policy Rule (Regla de políticas)**.
3. Introduzca un nombre para la política.
4. En la sección **Users (Usuarios)**, incluya **Select users and groups (Seleccionar usuarios y grupos)** y seleccione sus grupos de proyecto en consecuencia.
5. Verifique el **Target resources (Recursos de destino)**.
6. Seleccione la opción **Conditions (Condiciones)** que desencadenan la política.
7. Acceso a **Grant (Subvención)** en **Access Controls (Controles de acceso)** usando **Require multifactor authentication (Requerir autenticación multifactor)**.
8. Habilite la política alternando el selector a **On (Activado)**, y seleccione **Create (Crear)** el acceso condicional.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Añada su proveedor de IdP como un tipo de autenticación.

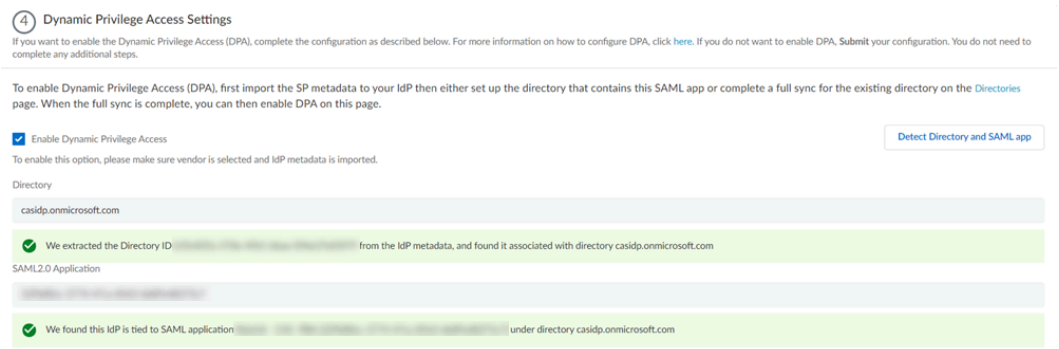
1. Seleccione **Single sign-on (Inicio de sesión único)** > **SAML Certificates (Certificados SAML)** y copie el archivo **App Federation Metadata URL (URL de metadatos de federación de aplicaciones)**.
2. En la aplicación de Cloud Identity Engine, seleccione **Authentication (Autenticación)** > **Authentication Types (Tipos de autenticación)** > **Add New Authentication Type (Añadir nuevo tipo de autenticación)**.
3. **Set Up (Configurar)** un tipo de autenticación SAML 2.0.
4. En **Configure your Identity Provider Profile (Configurar su perfil del proveedor de identidad)**, introduzca un **Profile Name (Nombre del perfil)**.
5. Seleccione **Azure** como su **IDP Vendor (Proveedor de IDP)**.
6. Seleccione **Get URL (Obtener URL)**, pegue la URL del paso 5.a y seleccione **Get URL (Obtener URL)** para obtener los metadatos.



7. Habilitar **Multi-factor Authentication is Enabled on the Identity Provider (La autenticación multifactor está habilitada en el proveedor de identidades)**.
8. **Test SAML Setup (Probar la configuración de SAML)** para verificar la configuración del perfil.
9. Seleccione los atributos SAML que desea que Prisma Access utilice para la autenticación.
10. Habilite **Dynamic Privilege Access (Acceso dinámico a privilegios)**

    Asegúrese de sincronizar el directorio que añadió en el paso 2 y la aplicación SAML.

 ©2025 Palo Alto Networks, Inc.



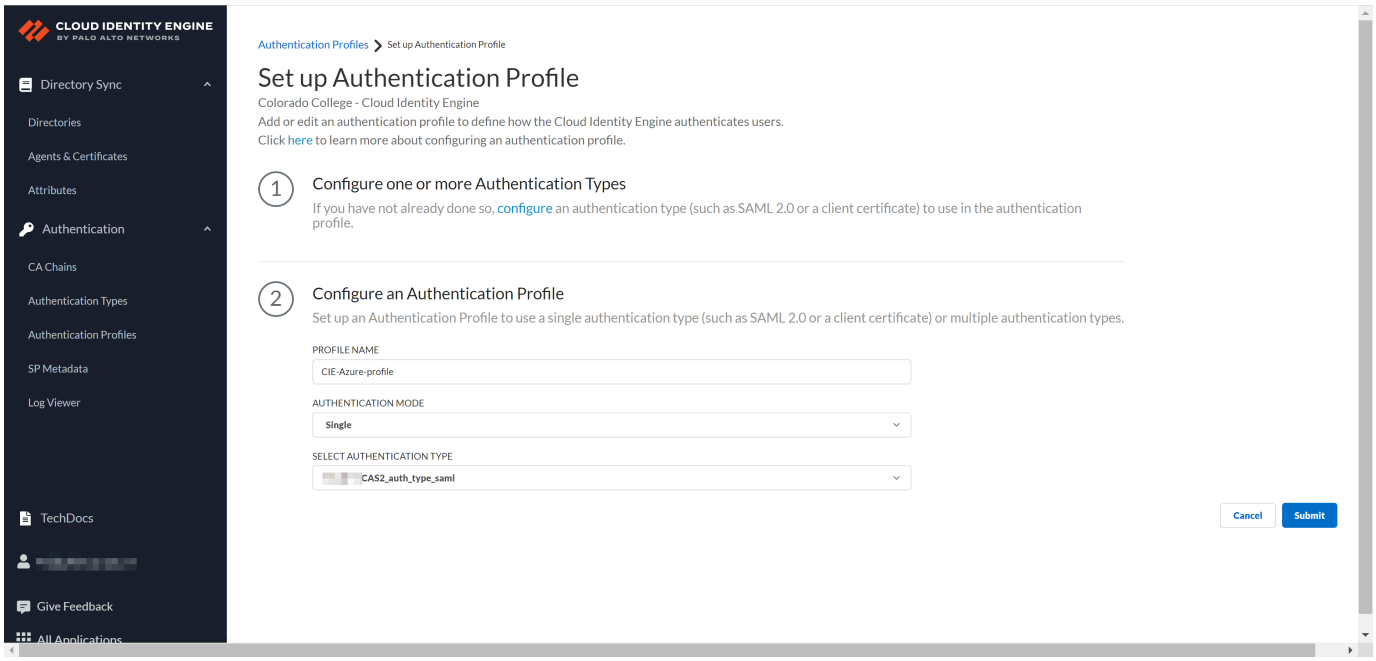
11. Deberá **Submit (Enviar)** el perfil del IdP.

STEP 6 | Repita los pasos de 3 a 5 para configurar la aplicación SAML para grupos de usuarios que no requieren MFA.

No habilite MFA en el paso 5.g para grupos de usuarios que no requieren MFA.

STEP 7 | Añada un perfil de autenticación para grupos de usuarios de MFA y grupos de usuarios que no son de MFA.

1. Seleccione **Authentication (Autenticación)** > **Authentication profiles (Perfiles de autenticación)** > **Add authentication profile (Añadir perfil de autenticación)**.
2. Introduzca un **PROFILE NAME (NOMBRE DE PERFIL)**.
3. Seleccione un **Authentication Mode (Modo de autenticación)**:
4. Seleccione **Authentication Type (Tipo de autenticación)** del paso 5 o 6, en función de los grupos de usuarios que requieren MFA, y luego **Submit (Enviar)**.

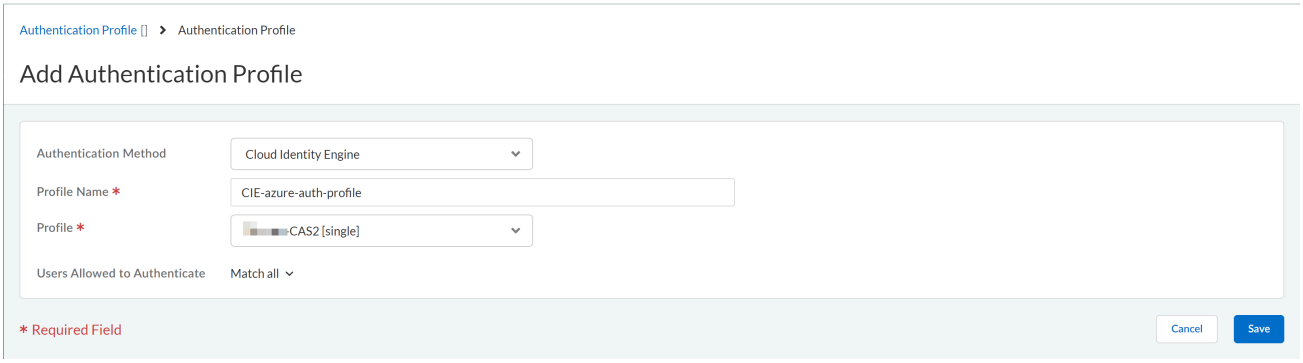


 ©2025 Palo Alto Networks, Inc.

STEP 8 | Añada el perfil de autenticación de Cloud Identity Engine a Prisma Access.

1. En Strata Cloud Manager, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)** > **Authentication Profiles (Perfiles de autenticación)**.

   Asegúrese de establecer el ámbito de configuración en el contenedor de usuarios móviles de **Access Agent (Agente de acceso)**.
2. **Add Profile (Añadir perfil)**.
3. Seleccione **Cloud Identity Engine** como su **Authentication Method (Método de autenticación)**.
4. Introduzca un **Profile Name (Nombre de perfil)**.
5. Seleccione el **Profile (Perfil)** que añadió en la aplicación de Cloud Identity Engine desde el paso 7.
6. **Save (Guardar)** los cambios.



STEP 9 | Adjunte la autenticación a los usuarios móviles.

1. Inicie Prisma Access desde su Strata Cloud Manager.
2. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**.
3. Establezca el ámbito en el fragmento de proyecto que creó y vaya a **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)**.
4. Cree una política para permitir el tráfico solo de un rango DHCP de proyecto determinado y ese grupo de usuarios basado en proyecto.

©2025 Palo Alto Networks, Inc.

Habilitar el agente de acceso.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Rol: Superusuario

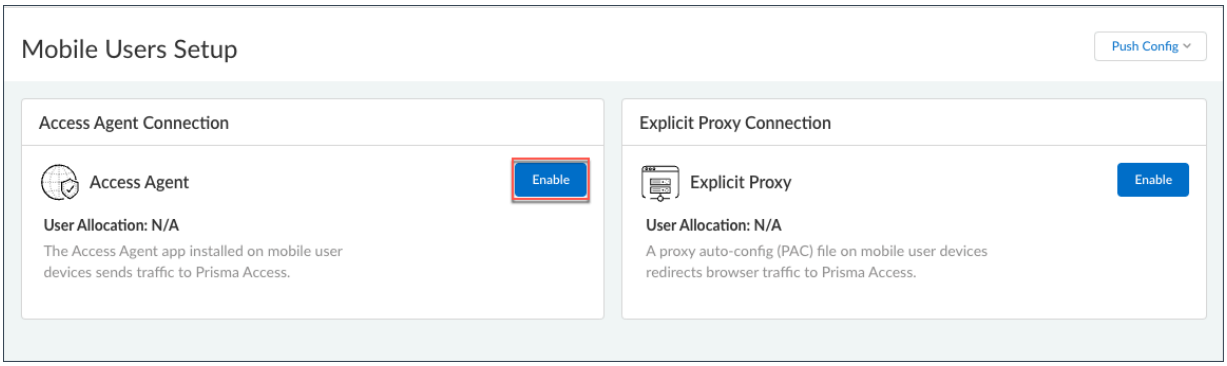
Para poder incorporar a los usuarios, debe habilitar **Access Agent (Agente de acceso)** como un tipo de conexión de usuario móvil mediante Strata Cloud Manager. Después de habilitar el tipo de conexión, los Prisma Access Agents instalados en los dispositivos móviles de los usuarios podrán enviar tráfico a Prisma Access.

Antes de comenzar a habilitar el Prisma Access Agent, asegúrese de que Autoriza la asignación de grupos de usuarios en Cloud Identity Engine para el acceso dinámico a privilegios.

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)**.

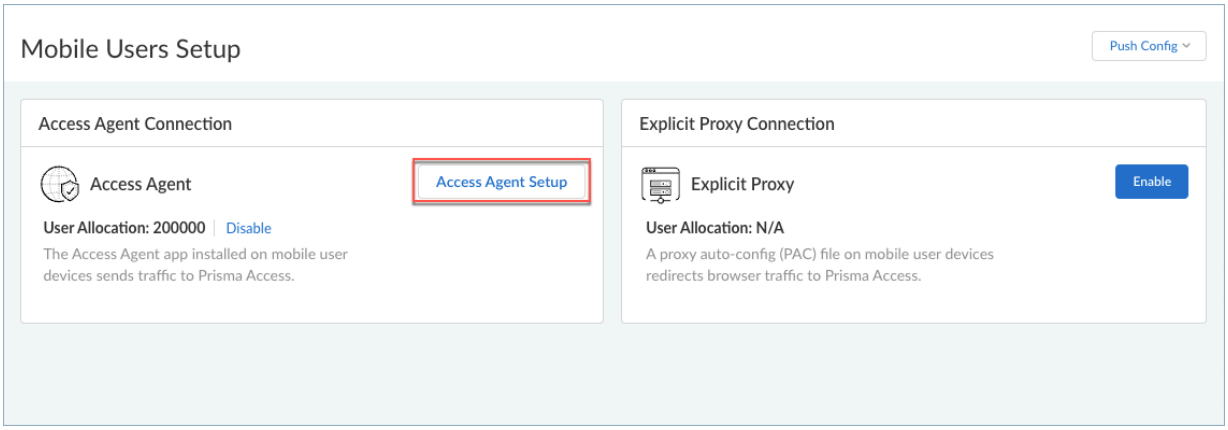
STEP 2 | Deberá **Enable (Habilitar)** el agente de acceso.

El proxy explícito no es compatible con el Agente de Prisma Access.

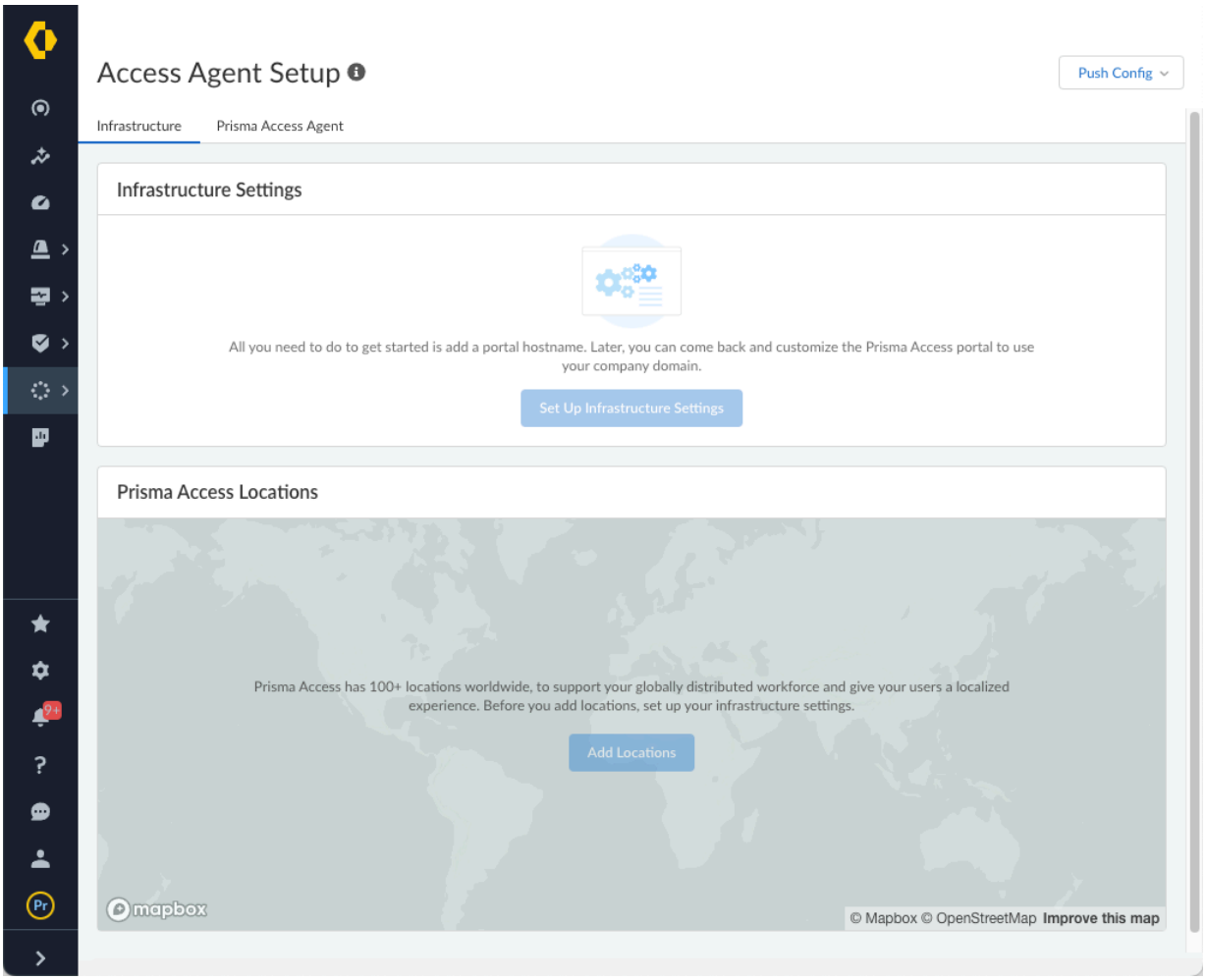


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Haga clic en **Access Agent Setup (Configuración del agente de acceso)** para comenzar a incorporar los usuarios móviles.



Aparece la página Configuración del agente de acceso.



 ©2025 Palo Alto Networks, Inc.

Configurar la infraestructura del agente para el acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Superusuario

Configure la configuración de infraestructura para Prisma Access Agent para que Prisma Access pueda aprovisionar su entorno de usuario móvil. Luego, seleccione las ubicaciones de Prisma Access donde sus usuarios de Prisma Access Agent se conectarán.

También puede opcionalmente habilitar el soporte SC-NAT para el Acceso dinámico a privilegios si ha creado conexiones de servicio para acceder a aplicaciones privadas en su centro de datos o ubicación de sede, o habilitar el resumen de rutas para el Acceso dinámico a privilegios para reducir el número de rutas que se envían a la red.

Configure la configuración de infraestructura

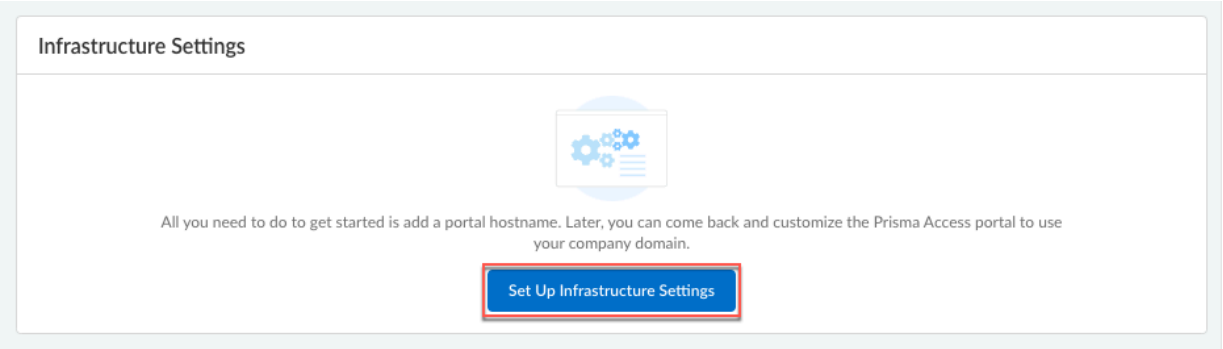
Para habilitar Prisma Access para el acceso a Internet solo para usuarios, Prisma Access proporciona un grupo de direcciones IP predeterminado y un servidor DNS predeterminado en la nube. Sin embargo, si desea que sus usuarios móviles accedan a recursos internos en su sede, centros de datos o en sitios de red remotos a los que se ha incorporado Prisma Access, debe asignar grupos de direcciones IP de cliente. Prisma Access utiliza los grupos de direcciones IP para asignar direcciones IP a sus usuarios móviles y configurar la infraestructura del servicio Prisma Access.

Antes de configurar los ajustes de infraestructura, asegúrese de configurar al menos un proyecto. De lo contrario, cuando intente confirmar y enviar la configuración de infraestructura, la confirmación fallará. Para obtener más información, consulte Crear un proyecto.

STEP 1 | En Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Infrastructure (Infraestructura)**.

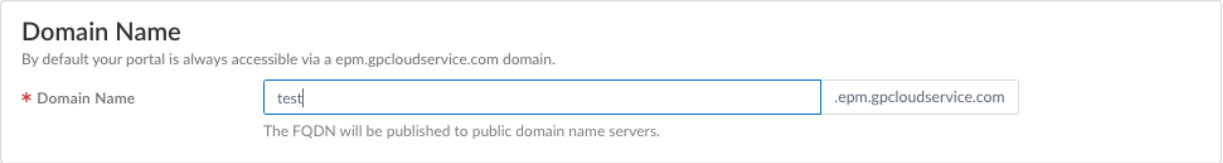
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Si va a configurar la infraestructura por primera vez, haga clic en **Set Up Infrastructure Settings (Configurar la configuración de la infraestructura)**. De lo contrario, edite la **Infrastructure Settings (Configuración de la infraestructura)**.



STEP 3 | Añada un nombre de host al **Domain Name (Nombre de dominio)** para el servicio al que se conectan los agentes de Prisma Access.

De forma predeterminada, los usuarios pueden acceder al servicio mediante un FQDN basado en su nombre de host y el dominio **`.epm.gpcloudservice.com`**.

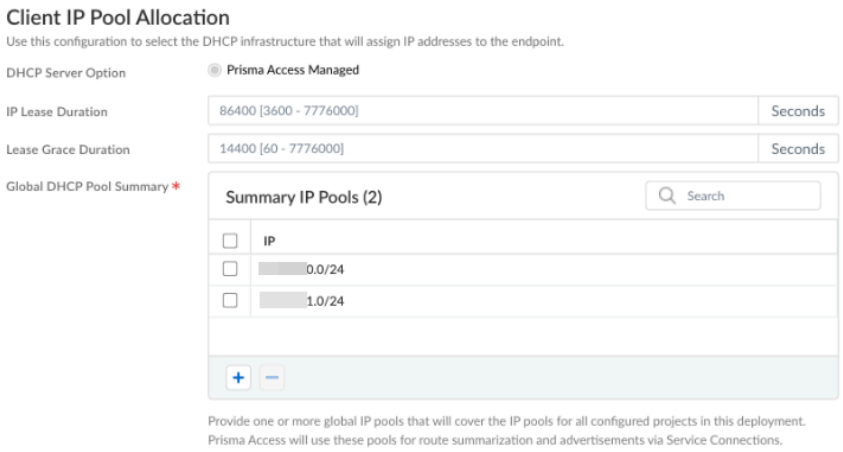


STEP 4 | En la **Client IP Pool Allocation (Asignación de grupo de direcciones IP de cliente)**, Prisma Access proporciona un servidor DHCP que gestionará la asignación de direcciones IP a sus endpoints para el acceso dinámico a privilegios.

El nombre del proyecto y el ID del grupo de ubicación de Prisma Access son parte de la solicitud DHCP. A cada Prisma Access Agent que se conecta a un proyecto específico se le asigna una dirección IP de la subred IP de ese proyecto. Cuando un usuario cambia a un

 ©2025 Palo Alto Networks, Inc.

proyecto diferente, se asigna una dirección IP diferente al Prisma Access Agent de la subred IP del proyecto.



Puede configurar las siguientes opciones:

- **IP Lease Duration (Duración de la concesión IP)**: Especifique el tiempo (en segundos) durante el cual el servidor DHCP asigna una dirección de red a un Prisma Access Agent. La duración predeterminada del arrendamiento de la dirección IP es de 86.400 segundos.
- **Lease Grace Duration (Periodo de gracia del arrendamiento)**: Especifique la cantidad de tiempo que puede continuar utilizando su alquiler de dirección IP después de que caduque el periodo de arrendamiento. El periodo de gracia del arrendamiento predeterminado es de 14.400 segundos.
- **Global DHCP Pool Summary (Resumen del grupo DHCP global)**: seleccione el grupo de direcciones IP en la que desea habilitar SC-NAT o configure y seleccione los grupos de IP del resumen global para el resumen de rutas.

STEP 5 | Deberá **Save (Guardar)** la configuración de la infraestructura.

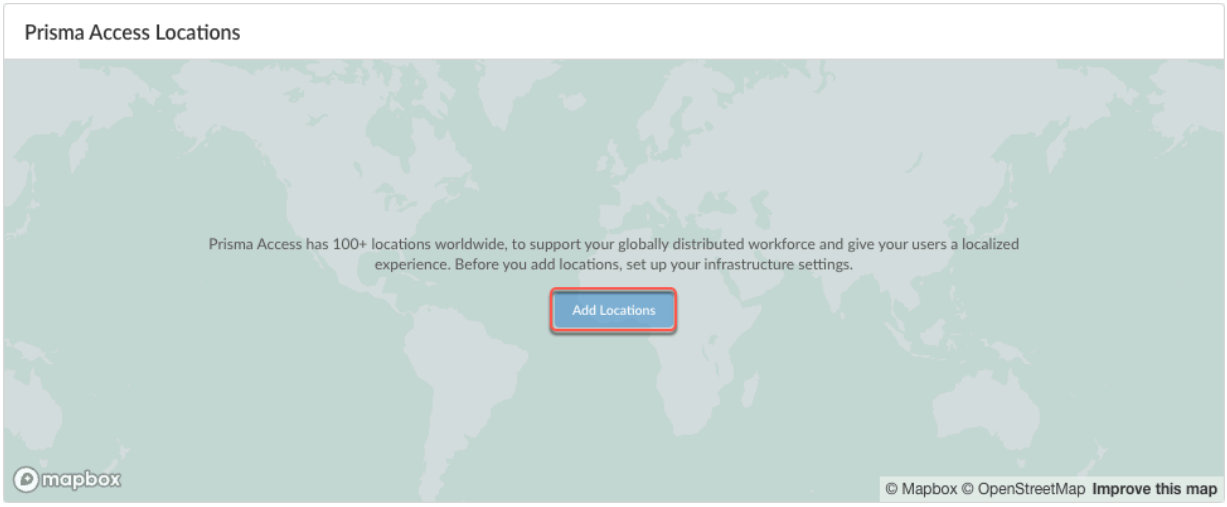
Seleccionar ubicaciones de Prisma Access

Seleccione las ubicaciones de Prisma Access en las que desea implementar usuarios de Prisma Access Agent Los grupos de ubicación se utilizan para el Acceso dinámico a privilegios.

STEP 1 | En Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Infrastructure (Infraestructura)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Si va a configurar la infraestructura por primera vez, seleccione **Add Locations (Añadir ubicaciones)**. De lo contrario, edite las **Prisma Access Locations (Ubicaciones de Prisma Access)**.



STEP 3 | Seleccione las ubicaciones de Prisma Access a las que se conectarán sus usuarios móviles.

Dependiendo de su acuerdo de licencia, puede seleccionar ubicaciones Locales o Mundiales. El mapa muestra las regiones donde puede implementar Prisma Access para los usuarios. Además, Prisma Access proporciona múltiples ubicaciones dentro de cada región para garantizar que sus usuarios puedan conectarse a una ubicación que proporciona una experiencia de usuario adaptada a la configuración regional de los usuarios. Para obtener el mejor rendimiento, deberá **Select All (Seleccionar todo)**. Alternativamente, seleccione ubicaciones específicas dentro de cada región seleccionada donde sus usuarios necesitarán acceso. Al limitar su implementación a una sola región, puede tener un control más granular sobre sus regiones implementadas y excluir las regiones requeridas por su política o regulaciones de la industria.

Para los agentes de Prisma Access, puede implementar Prisma Access en las siguientes regiones de Strata Logging Service:

- *Estados Unidos*
- *Alemania*
- *India*

Esta lista se actualizará a medida que haya más regiones disponibles.

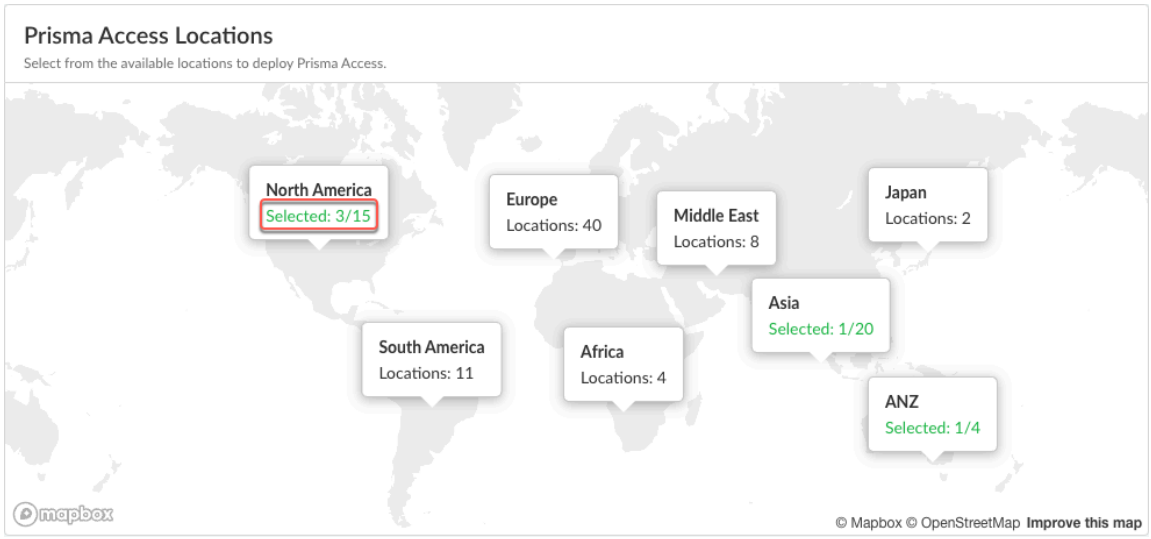
Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a sus usuarios o en el mismo país que sus usuarios. Si una ubicación

 ©2025 Palo Alto Networks, Inc.

no está disponible en el país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a sus usuarios para obtener el mejor rendimiento.

Las imágenes de esta sección se proporcionan solo con fines ilustrativos.

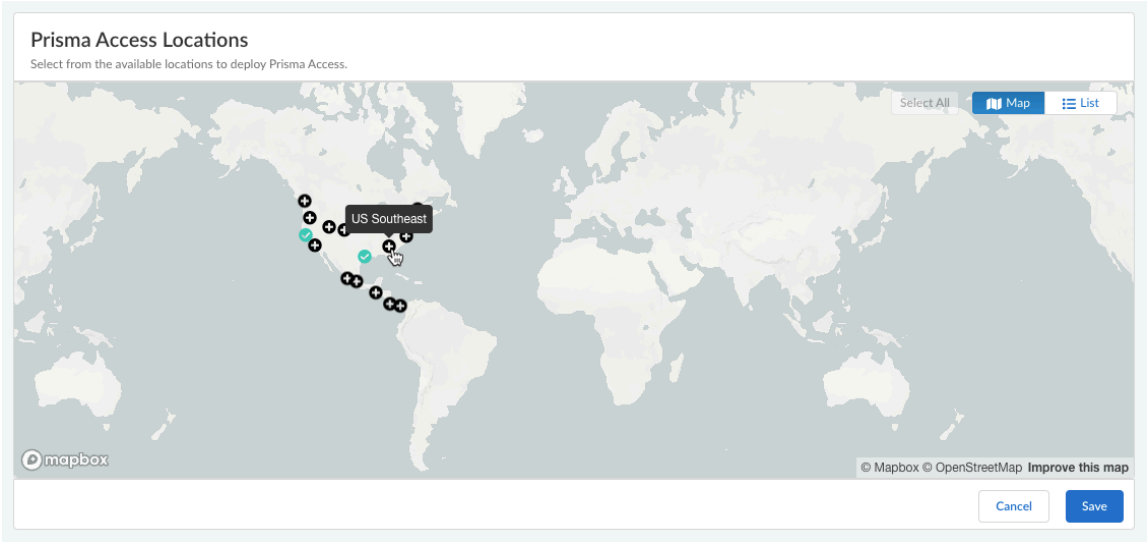
1. Seleccione una región disponible en el mapa.



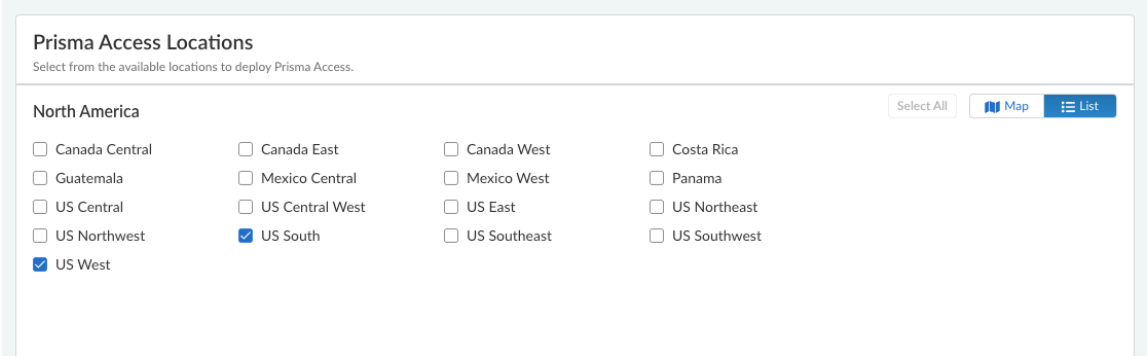
 ©2025 Palo Alto Networks, Inc.

2. Haga clic en el signo más **+** en las ubicaciones que desea añadir.

   Puede cambiar entre las vistas **Map (Mapa)** y **List (Lista)**. También puede **Select All (Seleccionar todas)** las ubicaciones.



   En la vista de lista, puede seleccionar de la lista de ubicaciones disponibles para implementar Prisma Access. Puede seleccionar **All (Todos)** los sitios dentro de una región.



3. Deberá **Save (Guardar)** la configuración de ubicación de Prisma Access.

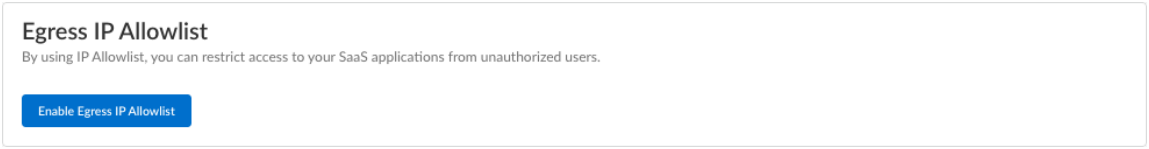
STEP 4 | (Opcional) Restringir el acceso a sus aplicaciones SaaS de usuarios no autorizados.

Puede habilitar las listas de permisos IP de salida para implementaciones de usuarios móviles existentes y durante la incorporación de nuevos usuarios. Si habilita las listas de permisos IP de salida para implementaciones de Prisma Access existentes, Prisma Access migra todas las direcciones IP de salida ya asignadas para sus ubicaciones a las listas de permisos IP de salida. Para las nuevas implementaciones de Prisma Access, habilite la lista de permisos IP de salida mientras se incorporan los usuarios móviles del Agente de Prisma Access. Cada vez que añade una ubicación o tenga un evento de escalado automático, debe recuperar las nuevas direcciones IP de salida que Prisma Access asigna y añadirlas para permitir listas en

 ©2025 Palo Alto Networks, Inc.

sus aplicaciones SaaS. A continuación, puede enviar la configuración a su implementación de Prisma Access para confirmar las listas de permisos IP de salida asignadas para sus ubicaciones.

1. Elija **Enable Egress IP Allowlist (Habilite la lista de permisos IP de salida)** para mostrar las direcciones IP de las ubicaciones de Prisma Access incorporadas.



2. Copie y añada las direcciones asignadas a las listas de permisos de sus aplicaciones SaaS.
3. Elija**Migrate (Migrar)** para confirmar las direcciones IP asignadas a las ubicaciones incorporadas en Prisma Access.
4. Recupere las direcciones IP de las nuevas ubicaciones incorporadas o durante un evento de escalado automático.
    1. Seleccione el nombre de la **Location (Ubicación)** para encontrar las nuevas direcciones IP de salida asignadas a la ubicación.
    2. Añada estas direcciones IP a las listas de permisos de sus aplicaciones SaaS antes de confirmarlas en Prisma Access.
    3. Deberá **Save (Guardar)** las direcciones IP de salida asignadas.

Habilitar compatibilidad con SC-NAT para el acceso dinámico con privilegios

Use Compatibilidad con SC-NAT para el Acceso con privilegios dinámicos (DPA) si utiliza DPA y ha creado conexiones de servicio para acceder a aplicaciones privadas en su centro de datos o sede central. Varios proyectos en su entorno de DPA pueden experimentar el agotamiento de direcciones IP si las direcciones IP de la subred de infraestructura se superponen. Para solucionar este problema, Prisma Access puede implementar NAT de origen (SNAT) para las direcciones IP, que:

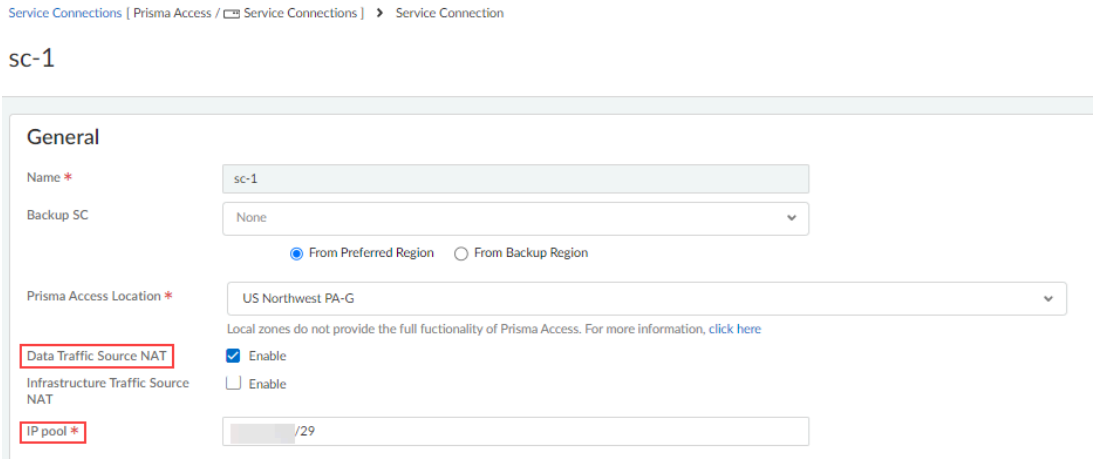
- Permite que Prisma Access asigne una sola dirección IP para un usuario móvil que accede a aplicaciones privadas mediante una conexión de servicio
- Le proporciona SNAT para facilitar el enrutamiento
- Elimina la superposición de grupos de IP
- Elimina el agotamiento de grupos de IP IPv4 entre Prisma Access y su centro de datos o sede central

Los clientes de DPA pueden incorporar ubicaciones de clientes a Prisma Access utilizando conexiones de servicio. Sin embargo, varios proyectos pueden tener grandes grupos de IP en múltiples centros de datos, lo que puede llevar al posible agotamiento de los grupos de IP privados. Para resolver este problema, el Acceso dinámico a privilegios en Prisma Access ofrece soporte para SC-NAT con grupos definidos. Los clientes tienen la opción de utilizar SC-NAT en lugar de la subred de infraestructura para dividir los grupos de IP. Si habilita SC-NAT para un nodo de acceso de conexión de servicio corporativo (SC-CAN), SC-NAT siempre será compatible con esa conexión de servicio.

Con DPA habilitado, puede activar SC-NAT (para usar SC-NAT) o desactivarlo (para usar la Subred de Infraestructura) por proyecto.

 ©2025 Palo Alto Networks, Inc.

1. En Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)**.
2. Seleccione una conexión de servicio de la tabla de **Service Connections (Conexiones de servicio)**.
3. Marque la casilla para la **Data Traffic Source NAT (Fuente NAT del tráfico de datos)**.
4. Después de hacer clic en la casilla de verificación **Data Traffic Source NAT (NAT de origen de tráfico de datos)**, verá el campo obligatorio de **IP Pool (grupo de direcciones IP)**. Introduzca las subredes para las que desea habilitar SC-NAT.
5. **Save (Guardar)** sus cambios.



Habilite Resumen de rutas para el Acceso dinámico con privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.2 Innovation ☐ Versión mínima de plano de datos de Prisma Access 11.2.3 ☐ Prisma Access Licencia con la suscripción de usuario móvil ☐ Rol: Superusuario

Para las empresas que tienen hardware local con capacidad limitada, como enrutadores en la nube simples que solo pueden acomodar unas pocas cientos de rutas, Prisma Access puede resumir las rutas de Usuario Móvil (MU) al anunciar las rutas a la red local. El resumen de rutas minimiza los requisitos en estos dispositivos al mantenerse dentro de la capacidad de ruta en el centro de datos.

Para habilitar el resumen de rutas, puede configurar grupos de resumen globales que consisten en listas de grupos de direcciones IP grandes que se pueden usar en múltiples proyectos. Cuando un usuario se conecta a un proyecto utilizando el agente de Prisma Access y se le asigna una dirección IP dentro del rango de un grupo de resumen global, la conexión del servicio de Prisma Access publicita el grupo de resumen global en lugar de la ruta agregada más pequeña.

Para ayudar a ilustrar el resumen de rutas para proyectos, considere el siguiente escenario:

 ©2025 Palo Alto Networks, Inc.

- Configura un grupo de resumen global de 10.10.0.0/16 y habilita la opción de resumen de rutas en la conexión de servicio **SC-A**.
- El **Usuario-A** se conecta al **Proyecto-A**, que tiene asignado el grupo de direcciones IP del proyecto 10.10.10.0/24. Al conectarse, el agente de Prisma Access adquiere la dirección IP 10.10.10.10/32.
- El **Usuario-B** se conecta al **Proyecto-B**, que tiene asignado el grupo de direcciones IP del proyecto 10.10.11.0/24. Al conectarse, el agente de Prisma Access adquiere la dirección IP 10.10.11.10/32.
- En este caso, la conexión de servicio anuncia solo una subred (el grupo de resumen global de 10.10.0.0/16) en lugar de las rutas agregadas /24 a la red local a través de eBGP.



- *Prisma Access no resumirá los grupos de IP que no forman parte de un proyecto.*
- *Los grupos de IP del proyecto dentro de un proyecto pueden superponerse, y los grupos de IP del resumen global también pueden superponerse.*
- *Los grupos de resumen global deben ser grandes grupos de IP que contengan los grupos de IP del proyecto que están asociados con varios proyectos.*

Para habilitar el resumen de rutas para proyectos en Strata Cloud Manager:

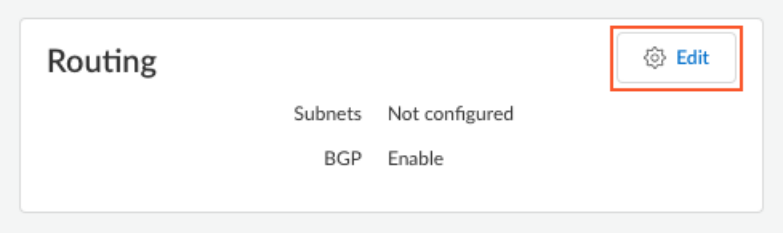
STEP 1 | Configure los grupos de IP del proyecto en la figuración del proyecto en **Manage (Gestionar)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **<Snippet>** > **Objects (Objetos)** > **Dynamic Privilege Access (Acceso dinámico a privilegios)** > **Projects (Proyectos)**.

STEP 2 | Configure los grupos de direcciones IP de resumen global en **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de Acceso)** > **Infrastructure Settings (Configuración de infraestructura)**.

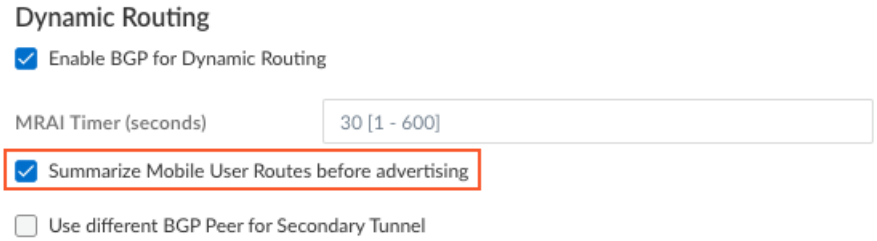
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Habilitar el resumen de rutas en la conexión de servicio.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connection (Conexión del servicio)**.
2. Seleccione una conexión de servicio de la tabla de **Service Connections (Conexiones de servicio)**.
3. **Edit (Editar)** la configuración de enrutamiento.



4. Seleccione **Summarize Mobile User Routes before advertising (Resumir las rutas de los usuarios móviles antes de anunciarse)**



STEP 4 | **Save (Guardar)** la configuración de enrutamiento.

STEP 5 | **Save (Guardar)** la configuración de conexión del servicio.

STEP 6 | Realice una configuración de envío para todos los administradores a Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Crear un fragmento

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia Prisma Access con la suscripción de usuario móvil ❑ Rol: Superusuario

Puede crear un fragmento para agrupar las configuraciones de Prisma Access Agents que pueda enviar rápidamente a sus implementaciones. Los fragmentos de código se utilizan para estandarizar una configuración de base común para un conjunto de implementaciones basadas en proyectos, lo que le permite incorporar rápidamente nuevos dispositivos con una configuración correcta conocida y reducir el tiempo necesario para incorporar un nuevo dispositivo.

Después de crear el fragmento de código, lo asociará a un ámbito, asignará un usuario al ámbito y le concederá la función de administrador del proyecto. A continuación, el usuario puede iniciar sesión como administrador del proyecto y utilizar el fragmento de código para gestionar la configuración del proyecto para el Prisma Access Agent. El administrador del proyecto solo puede cambiar el Prisma Access Agent para los fragmentos a los que están asignados.

Para crear un fragmento, siga estos pasos:

STEP 1 | Inicie sesión en Strata Cloud Manager como Superusuario.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**.

STEP 3 | Seleccione **Overview (Descripción general)** y expanda el ámbito de configuración para ver los **Snippets (Fragmentos)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Add Snippet (Añadir fragmento)** e introduzca los siguientes datos:

1. Introduzca un **Name (Nombre)** para el fragmento.
2. (Opcional) Introduzca una **Description (Descripción)** para el fragmento.
3. (Opcional) Asigne uno o más **Labels (Etiquetas)**.

   Puede seleccionar una etiqueta existente o crear una nueva escribiendo la etiqueta que desea crear.
4. Para asegurarse de que los nombres de los objetos sean únicos en un fragmento de código, **Add prefix to object names (Añadir prefijo a los nombres de los objetos)** está habilitado de forma predeterminada.

   Elija si desea generar de forma **Auto (Automática)** un prefijo aleatorio o seleccione **Manual** y añade el su **Prefix Value (Valor de prefijo)** propio. El valor del prefijo puede ser alfanumérico y tener un máximo de seis caracteres.

   El prefijo tendrá el formato **xxxxxx-**. Al añadir un objeto, Strata Cloud Manager rellenará previamente el nombre del objeto con el prefijo.
5. **Create (Crear)** el fragmento.

   Después de crear el fragmento de código, se encuentra en el Ámbito de configuración para el fragmento de código. Todas las configuraciones que cree en el ámbito del fragmento de código solo se producen para el fragmento de código.

STEP 5 | Asocie el fragmento de código a la carpeta **Access Agent (Agente de acceso)**.

1. En la página Descripción general del fragmento de código, seleccione la configuración **Snippet Associations (Asociaciones de fragmentos de código)**.
2. Seleccione **Access Agent (Agente de acceso)** de los **Config trees (Árboles de configuración)**.
3. Haga clic en el botón **X** para cerrar la ventana Asociaciones de fragmentos.

   Access Agent (Agente de acceso) aparece en la lista de Asociaciones de fragmentos.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Si aún no lo ha hecho, cree una identidad para el usuario que gestionará los proyectos y asigne al usuario la función de envío del administrador del proyecto.

1. En Strata Cloud Manager, seleccione **Settings (Configuración)** > **Identity & Access (Identidad y acceso)**.
2. Seleccione **Add Identity (Añadir identidad)**.
3. Introduzca la **Identity Address (Dirección de identidad)** para el usuario que será el administrador del proyecto y haga clic en **Next (Siguiente)**.
4. Seleccione **Add Access (Añadir acceso)** > **Prisma Access & NGFW Configuration (Prisma Access y configuración de NGFW)** y seleccione la función **Project Admin Push (Envío de administrador de proyectos)** para el usuario.
5. Haga clic en **Submit (Enviar)** para enviar.

STEP 7 | Cree un ámbito de gestión para el fragmento de código y asigne un usuario a ese ámbito.

1. Seleccione **Manage (Gestionar)** > **Access Control (Control de acceso)** > **Scope Management (Gestión del alcance)**.
2. **Crear nuevo alcance**.
3. Introduzca un **Name (Nombre)** para el ámbito y vea los **Snippets (Fragmentos)**.
4. Asocie el fragmento de código al ámbito. Seleccione el fragmento que ha creado y elija **Add (Añadir)** para añadirlo.
5. En los objetos de ámbito, deberá **Assign Users (Asignar usuarios)** al ámbito que creó para el fragmento de código.
6. Asigne un usuario al ámbito seleccionando un usuario de la lista y asignando al usuario la función de **Project Admin (Administrador de proyectos)**.
7. **Cierre** la ventana.
8. Envíe la configuración.
   1. Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Push Config (Configuración de envío)**.
   2. Seleccione el ámbito de administrador **All Admins (Todos los administradores)** y seleccione **Push Config (Enviar configuración)** > **Push (Enviar)**.

   Una vez completada la operación de configuración de envío, se crea el fragmento y las funciones se asocian al fragmento de código.

   El usuario asignado (administrador del proyecto) ahora puede iniciar sesión en Strata Cloud Manager y configurar ajustes específicos del proyecto de Prisma Access Agent usando el fragmento que creó. El usuario puede ver otros ámbitos a los que no está asignado pero no puede interactuar con ellos, como cambiar cualquier configuración.

 ©2025 Palo Alto Networks, Inc.

Configurar configuración de Prisma Access Agent específica de un proyecto

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Administrador de proyecto

Después de que el administrador de superusuario configura la infraestructura, crea un fragmento de código y le asigna el fragmento, puede iniciar sesión como administrador del proyecto para configurar una configuración específica del proyecto de Prisma Access Agents configuración, como la IP privada, el túnel dividido y la información de DNS que se asignará a los endpoints cuando inicien sesión en un proyecto mediante el Prisma Access Agent.

Puede crear ajustes específicos del proyecto para uno o varios Prisma Access Agents o utilice la configuración predeterminada del agente. Puede usar un agente diferente para cada proyecto que haya gestionado o compartir un agente con varios proyectos.

Configurar perfiles de reenvío para gestionar el tráfico de agentes para agentes con acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Administrador de proyecto

Los **Perfiles de reenvío** proporcionan un panel único para configurar y gestionar las reglas de reenvío de tráfico y la instauración de tráfico, como la configuración de parámetros de túnel dividido y la gestión del tráfico fuera de la conexión del túnel. Los perfiles de reenvío mejoran la configuración inconexa de las políticas de tráfico que se experimentan con otros agentes de acceso móvil y amplían en gran medida el límite del número de reglas y entradas que se pueden

 ©2025 Palo Alto Networks, Inc.

configurar. Al simplificar las configuraciones relacionadas y mejorar la claridad, puede centrarse en cómo desea que se enrute y aplique el tráfico del endpoint.

El perfil de reenvío es un tipo de perfil que contiene varias secciones lógicas y ordenadas. Estas secciones ilustran las distintas fases por las que pasa una conexión antes de que el agente determine cómo debe dirigirse la conexión. Esta estructura organizativa puede ayudarle a comprender por qué el tráfico se enruta de una manera determinada al presentar las entradas ordenadas en cada sección. Dentro de cada sección, puede añadir, editar, eliminar o reordenar entradas.

Una vez configurados los perfiles de reenvío, puede asignarlos a usuarios o grupos de usuarios en la página Configuración del agente.

Las reglas de reenvío de tráfico se aplican de arriba hacia abajo en el perfil de reenvío. Por lo tanto, configure el perfil de reenvío de arriba hacia abajo, es decir, configurando primero las reglas más específicas y al final las menos específicas.

Reglas de reenvío

Un perfil de reenvío consiste en un conjunto de reglas de reenvío de tráfico que especifican qué tráfico de la aplicación de origen o dominio de destino y dirección IP de destino deberá pasa a través del túnel o fuera del túnel, si se debe dividir el tráfico de DNS y qué medidas de instauración de tráfico están en vigor. El tráfico que coincide con una regla se reenvía a Prisma Access de acuerdo con las especificaciones de reenvío de tráfico. Las especificaciones de una regla de reenvío se organizan en las siguientes secciones:

- **Source Applications (Aplicaciones de origen)**: especifica las aplicaciones privadas o SaaS a las que se aplica la regla. Cuando el tráfico de un endpoint coincide con la aplicación de origen, el tráfico se enruta de acuerdo con la regla de reenvío.
- **Destinations (Destinos)**: especifica los dominios y las direcciones IP a los que se aplica la regla. Cuando el tráfico coincide con los destinos (especificados como FQDN o direcciones IP), el tráfico se enruta de acuerdo con la regla de reenvío.

Instauración de tráfico

Cada perfil de reenvío también contiene parámetros de aplicación del tráfico que le permiten:

- Bloquear todo el tráfico saliente que no coincida con ninguna regla de reenvío
- Bloquear el acceso a la LAN de salida cuando el agente esté conectado al túnel
- Bloquear el acceso entrante cuando el agente esté conectado al túnel

Para configurar un perfil de reenvío, complete los siguientes pasos:

STEP 1 | Inicia sesión en Strata Cloud Manager como Administrador del proyecto.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el Ámbito de configuración para ver los **Snippets (Fragmentos)**.

STEP 3 | Seleccione el fragmento que el administrador Superusuario le asignó.

También puede ver los fragmentos que no están asignados a usted, pero no puede interactuar con ellos, como para cambiar la configuración.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Objects (Objetos)** > **Dynamic Privilege Access (Acceso dinámico a privilegios)** para abrir la configuración de Acceso a privilegios dinámicos.

STEP 5 | Seleccione los **Forwarding Profiles (Perfiles de reenvío)** y edite la **Forwarding Profiles Setup (Configuración de perfiles de reenvío)**.

 ©2025 Palo Alto Networks, Inc.

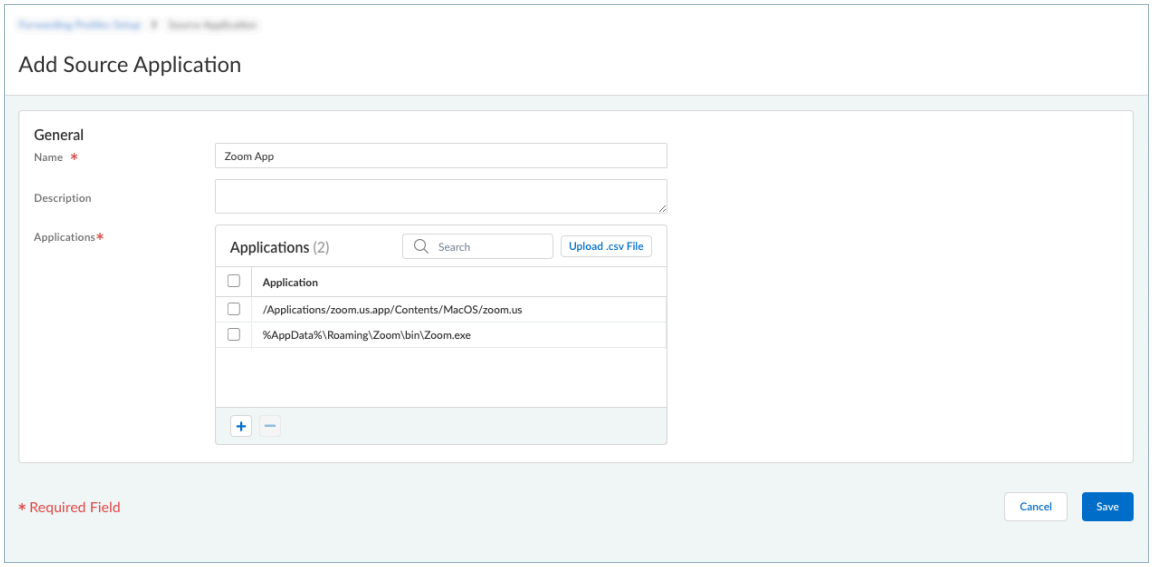
STEP 6 | Configure **Source Applications (Aplicaciones de origen)** si desea crear túneles divididos según el nombre de la aplicación de nube pública o SaaS.

1. En la página Configuración de perfiles de reenvío, seleccione **Source Applications (Aplicaciones de origen)** > **Add Source Application (Añadir aplicación de origen)**.

2. Introduzca un **Name (Nombre)** significativo para la aplicación que desea añadir.
3. Haga clic en **+** en la tabla **Applications (Aplicaciones)** e introduzca la ruta completa de la aplicación. Puede añadir una o más aplicaciones para gestionar si desea excluir o incluir el tráfico de aplicaciones en el túnel.

   Si elige excluir el tráfico de aplicaciones (seleccionando Conectividad **Direct (Directa)** en la regla de reenvío), el tráfico de estas aplicaciones se envía a través del adaptador físico en los endpoints en lugar del túnel (el adaptador virtual).

   Si elige incluir el tráfico de la aplicación (seleccionando Conectividad de **Tunnel (Túnel)** en la regla de reenvío), el tráfico de estas aplicaciones se enruta a Prisma Access, incluso si cumple con los criterios de exclusión de tráfico.



   Por ejemplo, para gestionar el tráfico desde la aplicación Zoom, añada las siguientes rutas completas:

   - Endpoints de Windows: **`%AppData%\Roaming\Zoom\bin\Zoom.exe`**
   - Endpoints de macOS: **`/Applications/zoom.us.app/Contents/MacOS/zoom.us`**

   Si tiene una lista de aplicaciones en un archivo de texto en formato de valores separados por comas (`.csv`), puede **Upload .csv File (Cargar un archivo .csv)**.
4. Elija **Save (Guardar)** la aplicación de origen.
5. Repita estos pasos para añadir más aplicaciones de origen.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Configure los **Destinations (Destinos)** si desea crear túneles divididos basados en el dominio de destino o las rutas de acceso.

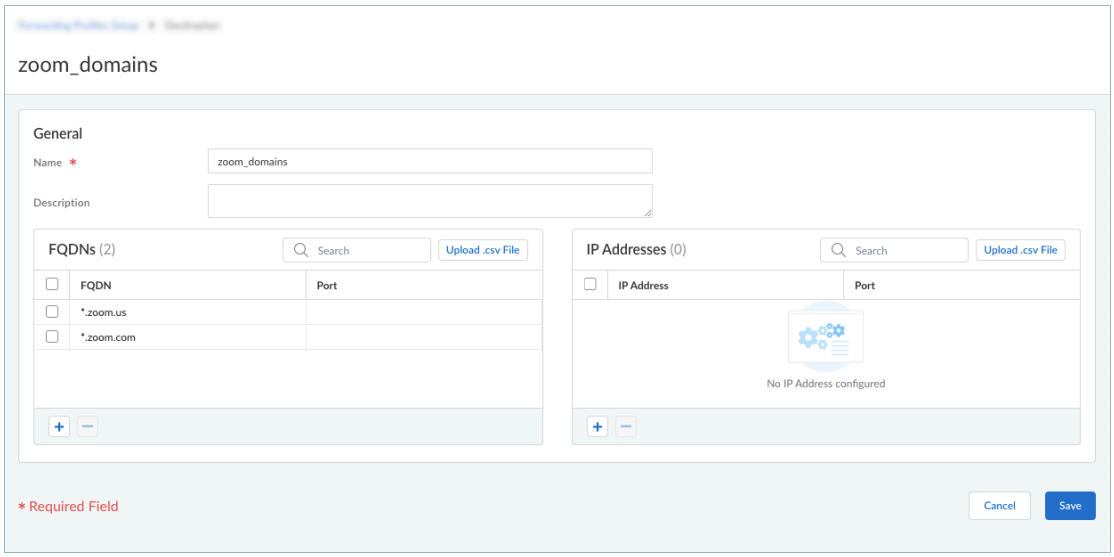
1. En la página Configuración de perfiles de reenvío, seleccione **Destinations (Destinos)** > **Add Destination (Añadir destino)**.

2. Introduzca un **Name (Nombre)** significativo para el destino que desea añadir.
3. Añada un destino especificando el nombre de dominio, la ruta de acceso o ambos.

   - Para añadir un dominio de destino, haga clic en **+** en la tabla **FQDN** e introduzca el FQDN para el dominio de destino. Opcionalmente, puede añadir un puerto. Si no especifica un puerto, todos los puertos del dominio especificado estarán sujetos a la regla de reenvío. Puede añadir uno o más dominios para la gestión del tráfico.

     Si elige excluir el tráfico en función del nombre de dominio (seleccionando Conectividad **Direct (Directa)** en la regla de reenvío), el tráfico del dominio se envía a través del adaptador físico en los endpoints en lugar del túnel (el adaptador virtual).

     Si elige incluir el tráfico en función del nombre de dominio (seleccionando Conectividad de **Tunnel (Túnel)** en la regla de reenvío), el tráfico del dominio se enruta a Prisma Access, incluso si cumple con los criterios de exclusión de tráfico.



   - Para añadir una ruta de acceso, haga clic en **+** en la tabla **IP Addresses (Direcciones IP)** e introduzca una subred de destino. Puede añadir una o más rutas de acceso para la gestión del tráfico.

     No incluya caracteres comodín en la dirección IP. Los comodines en direcciones IP no se admiten en los perfiles de reenvío.

     Si no incluye ni excluye rutas o aplicaciones, cada solicitud se enruta a través del túnel (sin un túnel dividido). Además, todo el tráfico se inspecciona y se somete a la aplicación de políticas cada vez que los usuarios se conectan a Prisma Access.

     Cuando se define el tráfico de túnel dividido para excluir rutas de acceso (seleccionando Conectividad **directa** en la regla de reenvío), estas rutas se envían a través del adaptador físico en el endpoint en lugar de enviarse a través del túnel

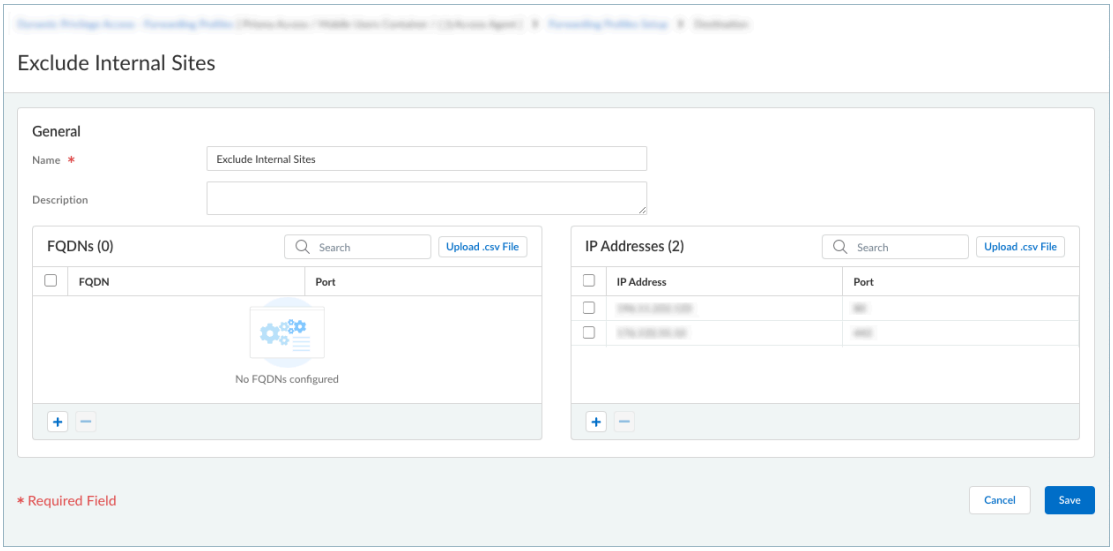
 ©2025 Palo Alto Networks, Inc.

mediante el adaptador virtual (el túnel). Al excluir el tráfico del túnel dividido por rutas de acceso, puede enviar tráfico sensible a la latencia o de alto ancho de banda fuera del túnel, mientras que el resto del tráfico se enruta a través del túnel para su inspección y aplicación de políticas por parte de la puerta de enlace de Prisma Access.

Cuando se define el tráfico de túnel dividido para incluir rutas de acceso (seleccionando Conectividad de **Tunnel (Túnel)** en la regla de reenvío), la puerta de enlace de Prisma Access envía estas rutas a los endpoints de los usuarios remotos para especificar qué tráfico pueden enviar estos endpoints a través del túnel.

Las rutas excluidas deben ser más específicas que las rutas incluidas para evitar excluir más tráfico del que se pretende.

Si tiene una lista de direcciones IP en un archivo de texto en formato `.csv`, puede **Upload .csv File (Cargar un archivo .csv)**.



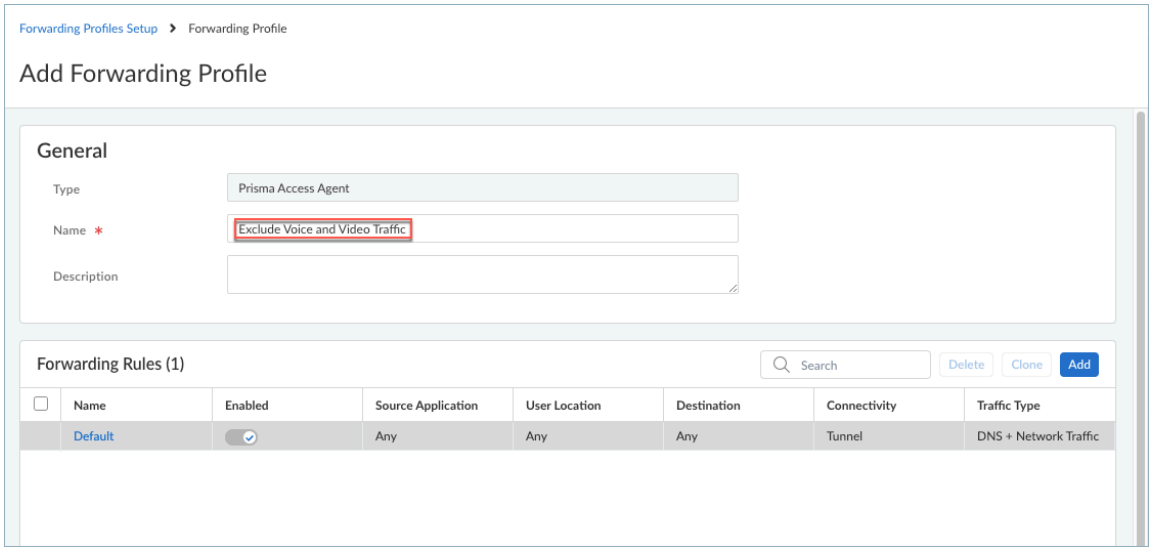
4. Deberá **Save (Guardar)** los destinos.
5. Repita estos pasos para añadir más destinos.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Cree un perfil de reenvío que permita o excluya el tráfico según las aplicaciones de origen o los destinos que haya configurado.

1. Para añadir un perfil de reenvío, seleccione **Forwarding Profiles (Perfiles de reenvío)** > **Add Forwarding Profile (Añadir perfil de reenvío)** > **Prisma Access Agent**.

   Para editar un perfil de reenvío, seleccione el nombre del perfil en la tabla Perfiles de reenvío.
2. Introduzca un **Name (Nombre)** significativo para el perfil de reenvío.
3. **Add (Añadir)** una regla de reenvío.

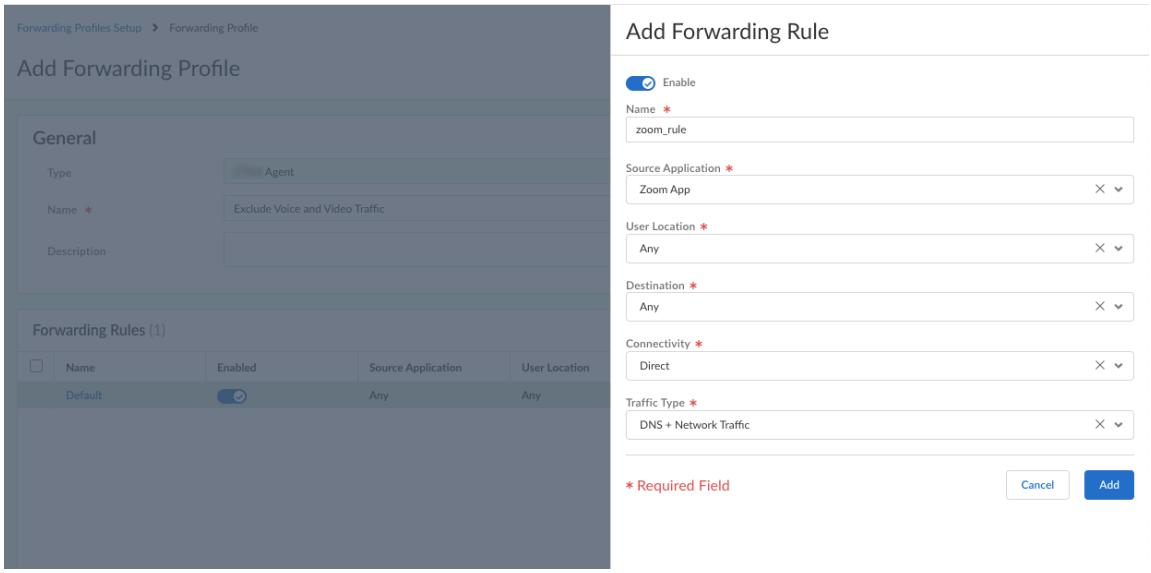


La tabla Reglas de reenvío muestra las reglas que componen el perfil de reenvío. Todos los perfiles de reenvío contienen la regla de reenvío **Default (Predeterminada)**, que envía todo el tráfico de DNS y de red a través del túnel. Cualquier regla nueva que añada se colocará encima de la regla predeterminada. No puede eliminar ni mover la

 ©2025 Palo Alto Networks, Inc.

regla de reenvío predeterminada, pero puede cambiar su parámetro de **Connectivity (Conectividad)**.

4. Introduzca las especificaciones para la regla de reenvío.



1. Seleccione **Enable (Habilitar)** para habilitar la regla.
2. Introduzca un **Name (Nombre)** para la regla.
3. Seleccione la **Source Application (Aplicación de origen)** que definió previamente. Si selecciona **Any (Cualquiera)**, la regla de reenvío se aplicará al tráfico de cualquier aplicación de origen.

   La regla solo coincidirá si la conexión la realiza la aplicación de origen especificada.
4. Seleccione una **User Location (Ubicación de usuario)**. Si no configuró una ubicación de usuario o si permite que la regla coincida con cualquier ubicación de usuario,

 ©2025 Palo Alto Networks, Inc.

seleccione **Any (Cualquiera)**. (No se aplica a agentes habilitados para el acceso con privilegios dinámicos).

La regla coincidirá solo si un endpoint está conectado a la ubicación del usuario que especifique.

5. Seleccione un **Destination (Destino)** que haya definido previamente. Si selecciona **Any (Cualquiera)**, la regla de reenvío se aplicará al tráfico de cualquier dominio de destino o dirección IP.

   La regla solo coincidirá si el destino de la conexión coincide con el dominio de destino o la dirección IP especificados.

6. Seleccione la **Connectivity (Conectividad)**:

   - **Direct (Directo)**: envía el tráfico fuera del túnel. Todo el tráfico de la aplicación o destino seleccionado se envía directamente al adaptador físico en el endpoint sin inspección.
   - **Tunnel (Túnel)**: envía el tráfico a través del túnel. Todo el tráfico que se dirige a la aplicación o destino seleccionado se envía a través del túnel a Prisma Access para su inspección y la aplicación de políticas.

7. Seleccionar el **Traffic Type (Tipo de tráfico)**:

   especifique si desea utilizar DNS dividido para permitir que los usuarios dirijan sus consultas DNS para aplicaciones y recursos a través del túnel o fuera del túnel, además del tráfico de red.

   - **DNS + Network Traffic (DNS + Tráfico de red)**: garantiza que 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.
   - **Network Traffic (Tráfico de red)**:incluye o excluye reglas que se aplican solo al tráfico de aplicaciones de red y no al tráfico de DNS. Todo el tráfico DNS pasa por

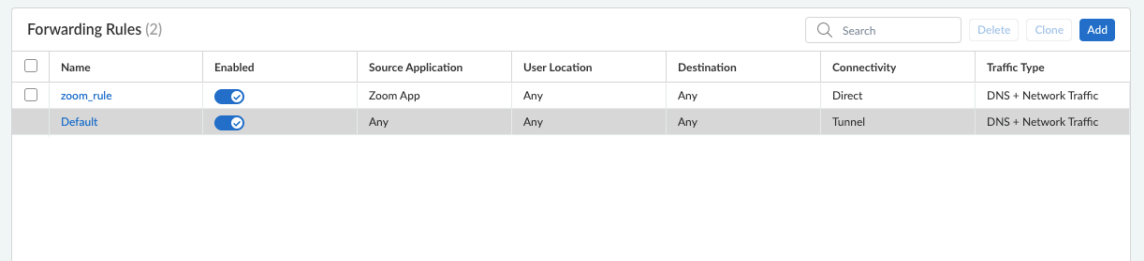
 ©2025 Palo Alto Networks, Inc.

el túnel independientemente del túnel dividido según el dominio de destino que especificó para las inclusiones o exclusiones.

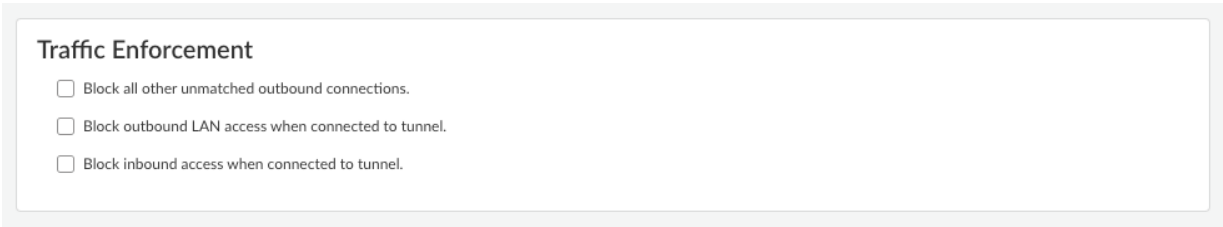
*Para los agentes de Windows, la opción de túnel dividido **DNS + Network Traffic (DNS + Tráfico de red)** no es compatible con las reglas de túnel dividido basadas en aplicaciones. Si configura la tunelización dividida para incluir o excluir tráfico del túnel basado en nombres de aplicaciones y selecciona **DNS + Network Traffic (DNS + Tráfico de red)**, los paquetes de consulta DNS para las aplicaciones excluidas e incluidas no respetarán la regla de túnel dividido.*

5. Deberá **Add (Añadir)** la regla de reenvío.

   La regla se añade a la tabla Reglas de reenvío. Puede añadir varias reglas al perfil de reenvío.



STEP 9 | Configure las opciones de **Traffic Enforcement (Instauración de tráfico)** para determinar cómo desea que se controle el tráfico.



*Asegúrese de **deseleccionar todas** estas opciones, ya que no se recomiendan para el Acceso dinámico a privilegios.*

- **Block all other unmatched outbound connections (Bloquear todas las demás conexiones salientes no coincidentes)**: cuando está habilitada, bloquea todas las conexiones que no coinciden con ninguna de las reglas de reenvío. El tráfico no se enviará a través del túnel.
- **Block outbound LAN access when connected to the tunnel (Bloquear el acceso a la LAN saliente cuando esté conectado al túnel)**: cuando está habilitada, bloquea el acceso directo a la red local cuando el agente está conectado al túnel.

  Bloquear el acceso a su red local impide que todo el tráfico se envíe al adaptador local. Además, sus usuarios no podrán acceder a los recursos de la subred local, como las

 ©2025 Palo Alto Networks, Inc.

impresoras. El tráfico de túnel dividido en función de la ruta de acceso, el dominio de destino y la aplicación todavía funciona como se esperaba.

Si deshabilita esta opción, los usuarios finales podrán acceder a los recursos locales sin necesidad de conectarse primero a Prisma Access utilizando el Agente de Prisma Access.

- **Block inbound access when connected to the tunnel (Bloquear el acceso entrante cuando esté conectado al túnel)**: cuando está habilitada, bloquea todas las conexiones entrantes desde el túnel.

STEP 10 | Seleccione **Save (Guardar)** su perfil de reenvío.

STEP 11 | Envíe la configuración seleccionando **Push Config (Enviar configuración)** > **Push (Enviar)**. Esta acción hará que su perfil de reenvío esté disponible para su selección en la página Configuración del agente.

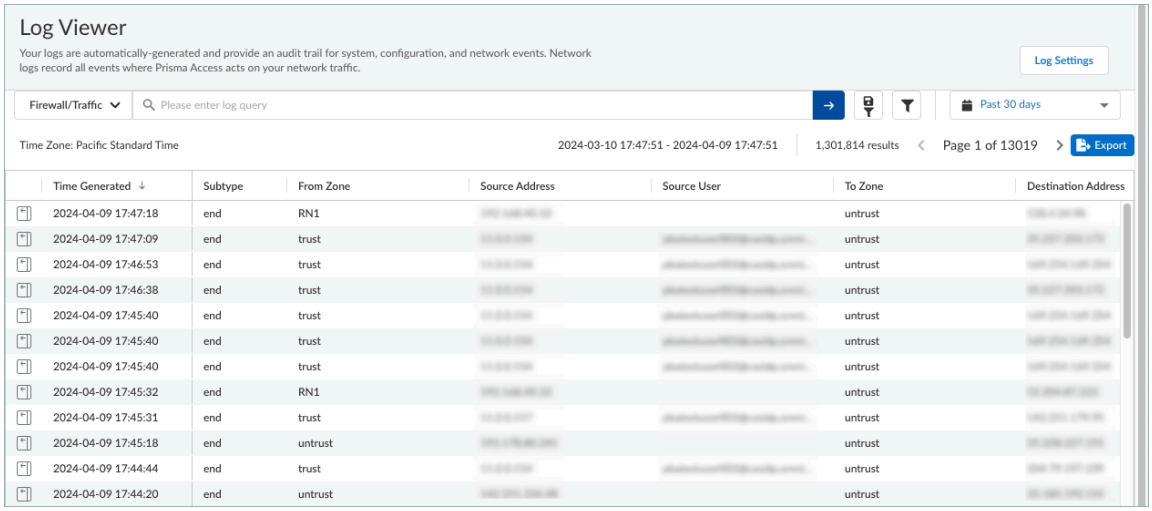
Verificar y solucionar problemas de configuraciones de perfil de reenvío para agentes de acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (gestionado por Strata Cloud Manager)	☐ Prisma Access 5.1 Preferred o Innovation ☐ Licencia Prisma Access con la suscripción de usuario móvil ☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Rol: Superusuario

Después de configurar un perfil de reenvío, puede verificar si el tráfico se está dirigiendo según lo previsto consultando los archivos de logs de tráfico. Puede ver los logs de tráfico en el visor de logs de Strata Cloud Manager o utilizando la herramienta de línea de comandos Prisma Access (PACli) en un endpoint.

 ©2025 Palo Alto Networks, Inc.

- Para ver los archivos de logs de tráfico desde el visor de logs de Strata Cloud Manager:
  1. Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
  2. Vea los logs de **Firewall/Traffic (Tráfico/cortafuegos)** para obtener más detalles.



 ©2025 Palo Alto Networks, Inc.

- Para ver los archivos de logs de tráfico en un endpoint:
  1. Inicie el shell remoto en **Manage (Gestionar)** > **Prisma Access Agent (Agente de Prisma Access)** o abra un símbolo del sistema de Windows o una ventana de terminal de macOS en el dispositivo de un usuario final.
  2. Para mostrar las reglas de reenvío en un perfil de reenvío, emita el siguiente comando:
     - En Windows:

       ```
       "C:\Program Files\Palo Alto Networks\Prisma Access Agent
       \pacli" traffic show
       ```

     - En macOS:

       ```
       /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
       pacli traffic show
       ```

       *Si configura una variable de entorno para la herramienta PACli (`pacli`), puede simplemente introducir **`pacli Traffic Show`**.*



El resultado de la línea de comandos de PACli de ejemplo muestra una tabla que contiene las reglas de reenvío que están vigentes en el perfil de reenvío, incluidas las prioridades de las reglas de reenvío. También se muestran las selecciones de instauración

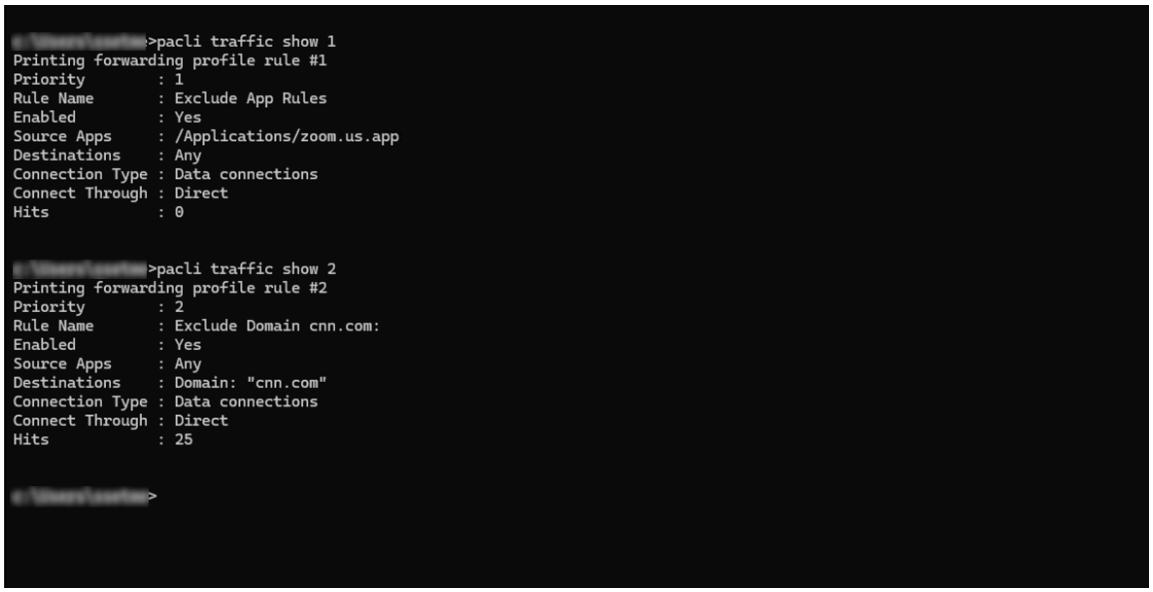
 ©2025 Palo Alto Networks, Inc.

de tráfico para el perfil de reenvío. Esta tabla corresponde a las reglas de reenvío que usted configura en su perfil de reenvío.

3. Para mostrar los detalles de una regla de reenvío, emita el siguiente comando:

```
pacli traffic show <number>
```

Dónde **<number>** es el número en la columna `Priority (Prioridad)`, por ejemplo:



4. Para solucionar problemas de túnel dividido, es posible que deba examinar qué tráfico del agente está dentro o fuera del túnel. Puede hacerlo mostrando el log de conexión de Agente de Prisma Access. Utilice el siguiente comando:

```
pacli traffic log
```

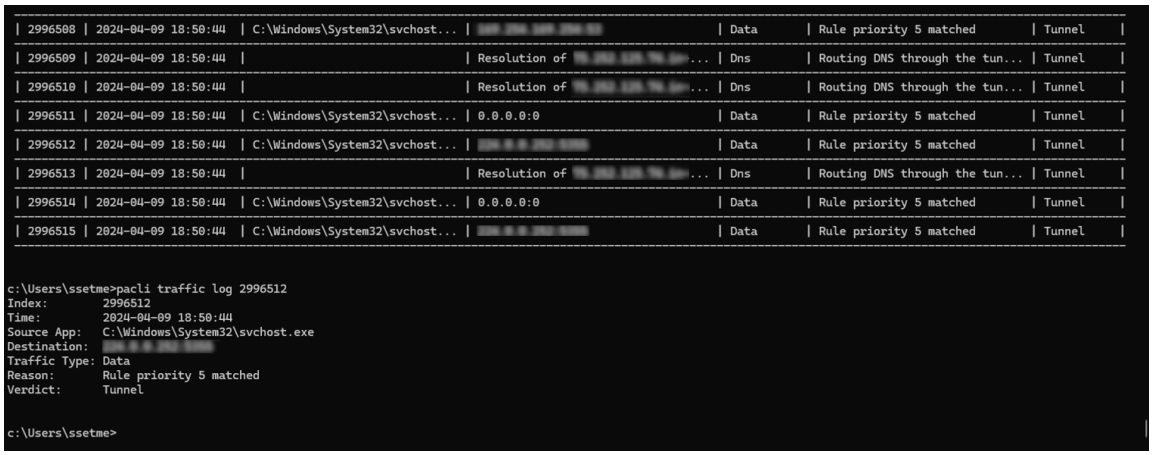


Para mostrar una entrada de log individual, emita el siguiente comando:

```
pacli traffic log <index>
```

 ©2025 Palo Alto Networks, Inc.

Dónde **<index>** corresponde al número de índice de la entrada. Por ejemplo:



También puede exportar el log de conexión a un archivo para su posterior análisis emitiendo lo siguiente:

```
pacli traffic log export <filename>
```

Configurar los ajustes de aplicación de Prisma Access Agent para el Acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ Licencia de Prisma Access con la suscripción de usuario móvil ☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Rol: Administrador de proyecto

Strata Cloud Manager proporciona las configuraciones de aplicación de Prisma Access Agent predeterminadas que se aplican a todos los grupos de usuarios en todos los proyectos. Puede añadir una configuración de aplicación para personalizar cómo interactúan sus usuarios finales en un proyecto con el Prisma Access Agent.

STEP 1 | Inicia sesión en Strata Cloud Manager como Administrador del proyecto.

STEP 2 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el Ámbito de configuración para ver los **Snippets (Fragmentos)**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Seleccione el fragmento que el administrador Superusuario le asignó.

También puede ver los fragmentos que no están asignados a usted, pero no puede interactuar con ellos, como para cambiar la configuración.

STEP 4 | Seleccione **Objects (Objetos)** > **Dynamic Privilege Access (Acceso dinámico a privilegios)** para abrir la configuración de Acceso a privilegios dinámicos.

STEP 5 | Seleccione la pestaña **Agent Settings (Configuración del agente)**.

STEP 6 | Strata Cloud Manager le proporciona la configuración predeterminada del agente. Si no desea usar la configuración predeterminada. Seleccione **Add Agent Settings (Añadir configuración de agente)**.

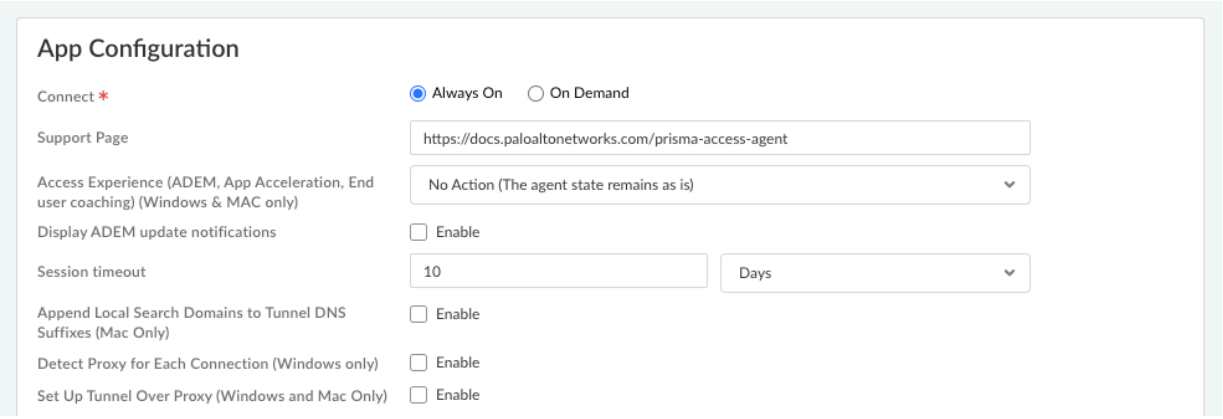
Para editar la configuración de un agente, seleccione un nombre de agente de la tabla.

STEP 7 | Cree una regla de configuración de la aplicación. La regla de configuración asocia uno o más proyectos con ciertos parámetros que son específicos de dichos proyectos.

1. Introduzca un **Name (Nombre)** para la regla.
2. Especifique los **Match Criteria (Criterios de coincidencia)** al añadir **Projects (Proyectos)**. Los usuarios y grupos que cumplan con los criterios del **Project (Proyecto)** recibirán la configuración de la aplicación cuando inicien sesión en el proyecto utilizando el Prisma Access Agent.
   - Para implementar la configuración a todos los usuarios, establezca **Projects (Proyectos)** en **Any (Cualquiera)**.
   - Para implementar la configuración a los usuarios que inician sesión en proyectos específicos, establezca **Projects (Proyectos)** para **Add Projects (Añadir Proyectos)** y seleccione de la lista de proyectos.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Configure los ajustes de la aplicación para el Agente de Prisma Access.



- **Connect (Conectar)**: especifique cómo se conecta el Agente de Prisma Access a Prisma Access. Esta configuración es obligatoria.
  - Seleccione **Always on (Siempre activo)** para establecer automáticamente una conexión con el Agente de Prisma Access cada vez que el usuario inicia sesión en un terminal.
  - Seleccione **On Demand (Bajo demanda)** para conectarse al Agente de Prisma Access solo cuando el usuario inicia sesión en el Agente de Prisma Access haciendo clic en el botón de bloqueo.
- **Support Page (Página de asistencia)**: entre en el sitio web al que los usuarios pueden acceder para obtener ayuda cuando hacen clic en **Support Resources (Recursos de apoyo)** en el Agente de Prisma Access.

  La página de asistencia predeterminada es el sitio web de la documentación del Agente de Prisma Access.
- **Access Experience (ADEM, App Acceleration, End user coaching) (Windows & MAC only) [Experiencia de acceso (ADEM, aceleración de aplicaciones, entrenamiento de usuarios finales) (solo Windows y MAC)]**: especifique si desea instalar el agente de endpoint Autonomous DEM (ADEM) durante la instalación de la aplicación del Agente de Prisma Access y permitir que los usuarios finales habiliten o deshabiliten las pruebas de experiencia de usuario desde la aplicación.
  - **Instale el agente**
  - **Desinstale el agente**
  - **Sin acción (el estado del agente permanece como está)** (Este es el valor predeterminado)

  Para obtener más información sobre cómo comenzar a usar ADEM en Cloud Managed Prisma Access, consulte Get Started with Autonomous DEM (Introducción a Autonomous DEM).
- **Display ADEM update notifications (Mostrar notificaciones de actualización de ADEM)**: deberá**Enable (Habilitar)** esta configuración para mostrar notificaciones de ADEM cuando haya una actualización disponible en el terminal.
- **Session timeout (Tiempo de espera de sesión)**: las sesiones de usuario del Agente de Prisma Access se crean cuando un usuario se conecta a la puerta de enlace de Prisma Access (ubicación) y se autentica correctamente. A continuación, la sesión se asigna a una puerta de enlace específica que determina qué tráfico se va a tunelizar en función de las reglas de

 ©2025 Palo Alto Networks, Inc.

túnel dividido definidas. La versión mínima del plano de datos para Prisma Access debe ser 11.2.

Especifique el tiempo que debe transcurrir antes de que se agote el tiempo de espera de la sesión debido a inactividad. Esta configuración es obligatoria.

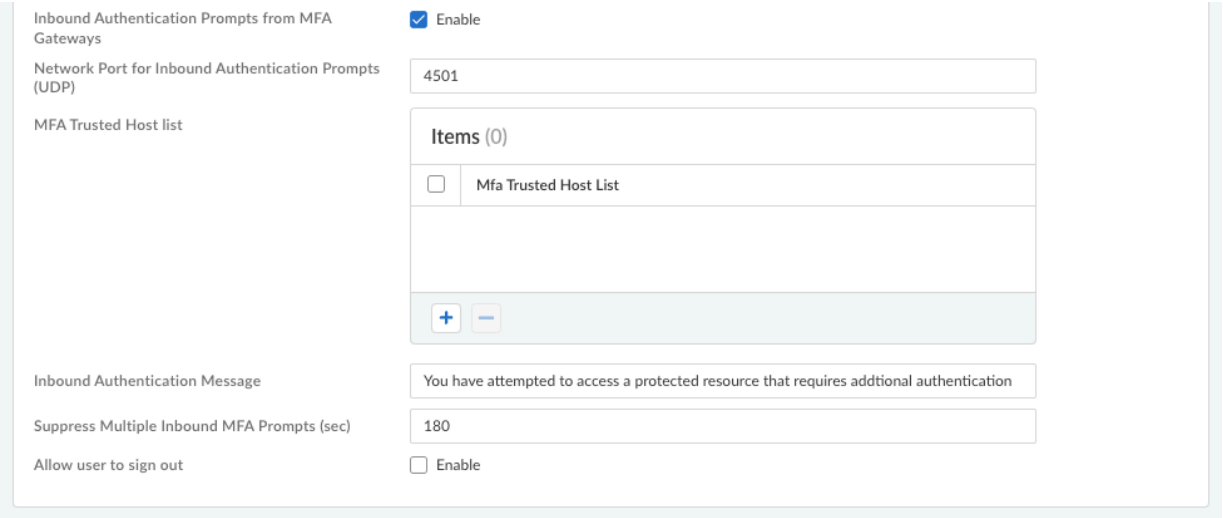
> *Si está utilizando el plano de datos Nebula (10.2) en Prisma Access, el valor del **Session timeout (Tiempo de espera de la sesión)** no es configurable y, de forma predeterminada, es de 7 días.*

- **Append Local Search Domains to Tunnel DNS Suffixes (Mac only) [Anexar dominios de búsqueda local a los sufijos DNS del túnel (solo Mac)]**: deberá **Enable (Habilitar)** esta configuración para anexar dominios de búsqueda DNS de túnel a dominios de búsqueda DNS locales en endpoints de macOS. La anexión de dominios de búsqueda de túnel a los dominios de búsqueda DNS locales de un endpoint permite a los usuarios acceder rápidamente a sitios web y servidores corporativos locales y remotos que visitan con frecuencia sin tener que introducir la dirección completa.
- **Detect Proxy for Each Connection (Windows only) [Detectar proxy para cada conexión (solo Windows)]**: Deberá **Enable (Habilitar)** esta configuración para detectar automáticamente el proxy en cada conexión. Deshabilite esta configuración si desea detectar automáticamente el proxy para la conexión de puerta de enlace y usar ese proxy para conexiones posteriores a Prisma Access.
- **Set Up Tunnel Over Proxy (Windows and Mac Only) [Configurar el túnel a través de proxy (solo Windows y Mac)]**: deberá **Enable (Habilitar)** este parámetro para configurar el comportamiento del tráfico de red en función del uso del proxy del Agente de Prisma Access. Seleccione **Enable (Habilitar)** para solicitar que el Agente de Prisma Access use proxies. Deshabilite este parámetro si desea que el Agente de Prisma Access omita los proxies. En función del uso del proxy de GlobalProtect, el SO del endpoint y el tipo de túnel, el tráfico de red se comportará de diferente manera.

  Si deshabilita esta opción, el Agente de Prisma Access omitirá los proxies. Todo el tráfico HTTP o HTTPS que coincida con las reglas de archivo proxy o PAC debe atravesar el túnel del Agente de Prisma Access antes de llegar al destino previsto. Al omitir los proxies, puede

 ©2025 Palo Alto Networks, Inc.

evitar que los usuarios configuren un proxy personal para acceder a los recursos web sin pasar por el túnel para la inspección y la aplicación de políticas.



- **Optimized MTU (MTU optimizada)**: la unidad máxima de transmisión (MTU) es el tamaño de paquete más grande que se puede enviar en un paquete durante una transmisión. Deberá **Enable (Habilitar)** esta opción para determinar automáticamente la mejor MTU que se utilizará para las transmisiones de paquetes.

  Las conexiones del Agente de Prisma Access pueden atravesar múltiples ISP y saltos de red con valores de MTU inferiores a los 1500 bytes estándar. Cuando el valor de la MTU del agente estático es inferior al que ofrece un ISP, se produce una fragmentación excesiva y una sobrecarga adicional, lo que da como resultado un rendimiento inferior. Los paquetes descartados en la ruta de red del ISP también desencadenan retransmisiones que contribuyen a un rendimiento por deficiente.

  Habilitar la **Optimized MTU (MTU optimizada)** puede ayudarle a evitar la tediosa determinación y configuración manual del valor óptimo de MTU, y evitar que los usuarios experimenten un rendimiento deficiente que afecte a su productividad.

  Optimized MTU (MTU optimizada) está habilitada de forma predeterminada. Si la deshabilita, puede configurar manualmente la MTU. El rango de la **Configurable MTU (bytes) [MTU configurable (bytes)]** es de 256-1420 bytes. El valor predeterminado es de 1400 horas.
- **Inbound Authentication Prompts from MFA Gateways (Solicitudes de autenticación entrantes desde las puertas de enlace de MFA)**: para admitir la autenticación multifactor (MFA), un terminal del Agente de Prisma Access debe recibir y reconocer los mensajes UDP entrantes desde la puerta de enlace. Debe **Enable (Habilitar)** esta configuración para permitir que un endpoint del Agente de Prisma Access reciba y reconozca las solicitudes UDP. Este parámetro está habilitado de forma predeterminada. Deshabilite este parámetro para bloquear las solicitudes UDP de la puerta de enlace.
- **Network Port for Inbound Authentication Prompts (UDP) [Puerto de red para solicitudes de autenticación entrante (UDP)]**: especifica el número de puerto que utiliza un endpoint de Agente de Prisma Access para recibir solicitudes de autenticación entrantes de puertas de enlace de MFA. El puerto predeterminado es 4501. Para cambiar el puerto, especifique un número de 1 a 65535.

 ©2025 Palo Alto Networks, Inc.

- **MFA Trusted Host list (Lista de hosts de confianza de MFA)**: debe **Add (Añadir)** los hosts de cortafuegos o puertas de enlace de autenticación en los que un endpoint de Agente de Prisma Access puede confiar para la autenticación multifactor. Cuando un endpoint de GlobalProtect recibe un mensaje UDP en el puerto de red especificado, GlobalProtect muestra un mensaje de autenticación sólo si el mensaje UDP proviene de una puerta de enlace de confianza.
- **Inbound Authentication Messages (Mensajes de autenticación entrantes)**: personalice un mensaje de notificación para mostrar cuando los usuarios intentan acceder a un recurso que requiere autenticación adicional.

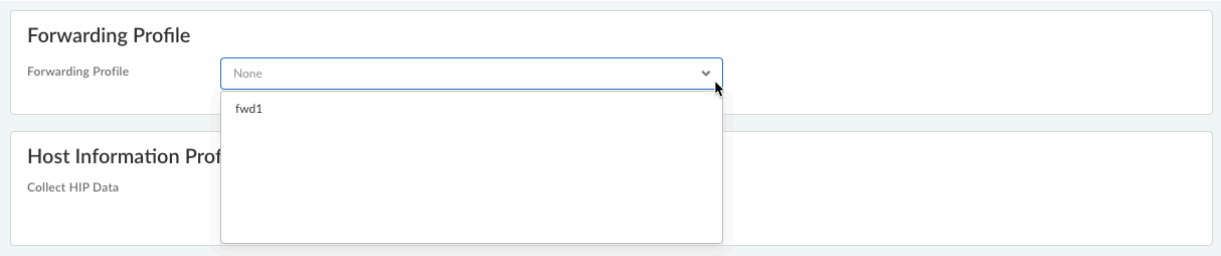
  Cuando los usuarios intentan acceder a un recurso que requiere autenticación adicional, GlobalProtect recibe un paquete UDP que contiene la solicitud de autenticación de entrada y muestra este mensaje. El paquete UDP también contiene la URL para la página del portal de autenticación que especificó cuando realizó la configuración de autenticación de múltiples factores. El Agente de Prisma Access adjunta automáticamente la URL al mensaje.

  Por ejemplo:

  ```
  Ha intentado acceder a un recurso protegido que requiere
   autenticación adicional. Proceda a autenticarse en
  ```

  El mensaje puede tener 255 caracteres o menos.
- **Suppress Multiple Inbound MFA Prompts (sec) [Ocultar varios mensajes de MFA entrantes (s)]**: especifique el número de segundos que se deben esperar antes de que Agente de Prisma Access pueda suprimir varios mensajes UDP entrantes. El valor predeterminado es 180 segundos.
- **Allow user to sign out (Permitir que el usuario cierre sesión)**: debe **Enable (Habilitar)** esta configuración para permitir que los usuarios cierren sesión en el Agente de Prisma Access. Este parámetro está deshabilitado de forma predeterminada.

STEP 9 | Seleccione un **Forwarding Profile (Perfil de reenvío)** que usted haya configurado previamente para gestionar cómo fluye el tráfico entre el agente y Prisma Access.



STEP 10 | Configurar la configuración de DNS para el Acceso dinámico a privilegios.

STEP 11 | Configure los ajustes del perfil de información del host

STEP 12 | Cuando haya terminado de configurar los ajustes, haga clic en **Save (Guardar)**.

 ©2025 Palo Alto Networks, Inc.

Configurar los configuración DNS para el Acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Administrador de proyecto

Puede configurar los servidores DNS para habilitar Prisma Access para resolver sus dominios internos.

STEP 1 | Desde Strata Cloud Manager Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el Alcance de la configuración para ver los **Snippets (Fragmentos)**.

STEP 2 | Seleccione el fragmento que el administrador Superusuario le asignó.

STEP 3 | Seleccione **Objects (Objetos)** > **Dynamic Privilege Access (Acceso dinámico a privilegios)** para abrir la configuración de Acceso a privilegios dinámicos.

STEP 4 | Seleccione la pestaña **Agent Settings (Configuración del agente)**.

STEP 5 | Deberá **Add Agent Settings (Añadir configuración de agente)** o seleccionar una configuración existente de la tabla Configuración del agente.

STEP 6 | Introduzca el servidor **Primary DNS (DNS primario)** y el servidor **Secondary DNS (DNS secundario)** que Prisma Access debe usar para resolver nombres de dominio internos.

STEP 7 | Puede añadir una **Client DNS Suffix List (Lista de sufijos DNS de cliente)** para especificar el sufijo que el cliente debe usar localmente cuando se introduce un nombre de host no cualificado que no puede resolver, por ejemplo, **`acme.local`**.

No introduzca un carácter comodín (*) antes del sufijo de dominio (por ejemplo, acme.com). Puede añadir varios sufijos.

©2025 Palo Alto Networks, Inc.

Configurar los ajustes de recopilación de datos HIP para el Acceso dinámico con privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Rol: Administrador de proyecto

El Agente de Prisma Access recopila información sobre el host en el que se está ejecutando y envía esta información de host a la ubicación de Prisma Access (puerta de enlace) tras una conexión realizada correctamente. La puerta de enlace compara esta información de host sin procesar que envía el Agente de Prisma Access con todos los objetos de perfil de información de host (HIP) y perfiles 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.

En la pestaña **HIP Notifications (Notificaciones HIP)** de la página Editar configuración global del agente, puede crear notificaciones HIP, crear y gestionar objetos HIP, y crear y gestionar perfiles HIP que se aplican al Agente de Prisma Access en todos los endpoints.

Aquí puede definir datos de HIP personalizados que desea que el Agente de Prisma Access recopile o excluya. Cuando esta opción está activada, el Agente de Prisma Access recopila datos de dispositivos que ejecutan sistemas operativos macOS o Windows.

Por ejemplo, una verificación personalizada podría permitirle saber si una determinada aplicación está instalada o se ejecuta en un endpoint. Los datos que define para que se recopilen en una comprobación personalizada se incluyen en los datos de información de host sin procesar que el Agente de Prisma Access recopila y, a continuación, envía a Prisma Access cuando el Agente de Prisma Access se conecta.

STEP 1 | Desde Strata Cloud Manager Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Visión general)** y expanda el Alcance de la configuración para ver los **Snippets (Fragmentos)**.

STEP 2 | Seleccione el fragmento que el administrador Superusuario le asignó.

STEP 3 | Seleccione **Objects (Objetos)** > **Dynamic Privilege Access (Acceso dinámico a privilegios)** para abrir la configuración de Acceso a privilegios dinámicos.

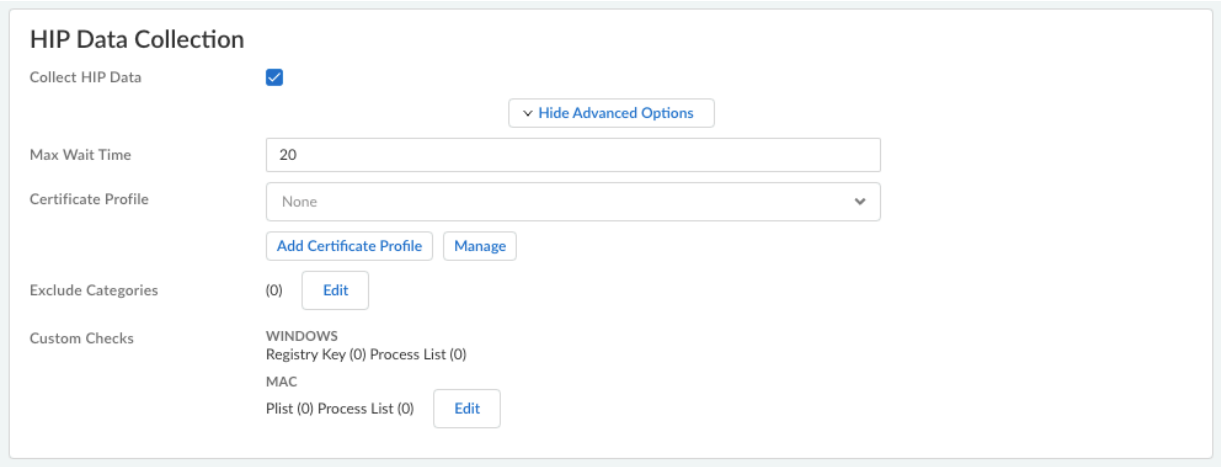
STEP 4 | Seleccione la pestaña **Agent Settings (Configuración del agente)**.

STEP 5 | **Add Agent Settings (Añadir configuración de agente)** o seleccione una configuración existente de la tabla Configuraciones de agente.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | En la sección Perfil de información de host (HIP), seleccione **Collect HIP Data (Recopilar datos HIP)** para habilitar la recopilación de datos HIP en los endpoints que iniciaron sesión con un proyecto.

STEP 7 | Seleccione **Show Advanced Options (Mostrar opciones avanzadas)**.



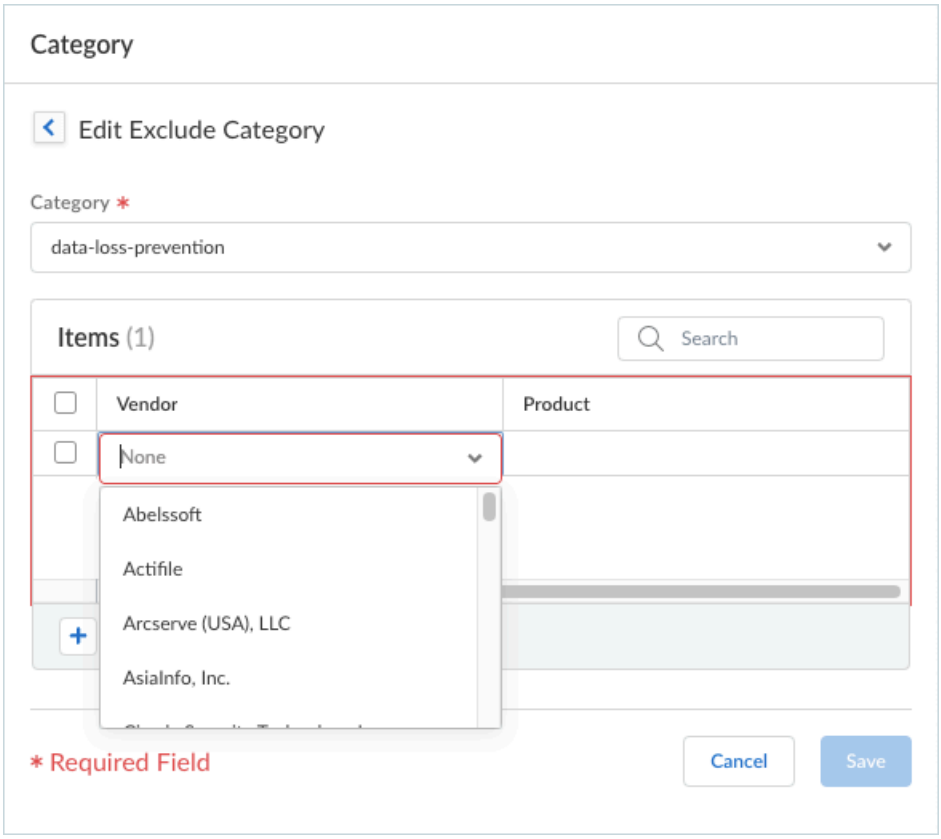
STEP 8 | Especifique el **Max Wait Time (Tiempo máximo de espera)** (en segundos) que el Agente de Prisma Access tiene para buscar los datos HIP antes de enviar los datos disponibles. El rango es de 10 a 60 segundos, siendo 20 segundos el valor predeterminado.

STEP 9 | Deberá **Edit (Editar)** Excluir categorías para excluir categorías específicas, o proveedores, aplicaciones o versiones dentro de una categoría de Recopilación de datos HIP.

Seleccione **Category (Categoría)** (como prevención de pérdida de datos) para excluir de la recopilación HIP. Después de seleccionar una categoría, puede hacer clic en **Add (Añadir)** para añadir un **Vendor (Proveedor)** particular y luego puede seleccionar **Add (Añadir)** para añadir un **Product (Producto)** específico del proveedor para ajustar más la exclusión, según fuera

 ©2025 Palo Alto Networks, Inc.

necesario. Puede añadir a varios proveedores y productos a la lista de exclusión. Deberá **Save (Guardar)** la configuración en cada diálogo.



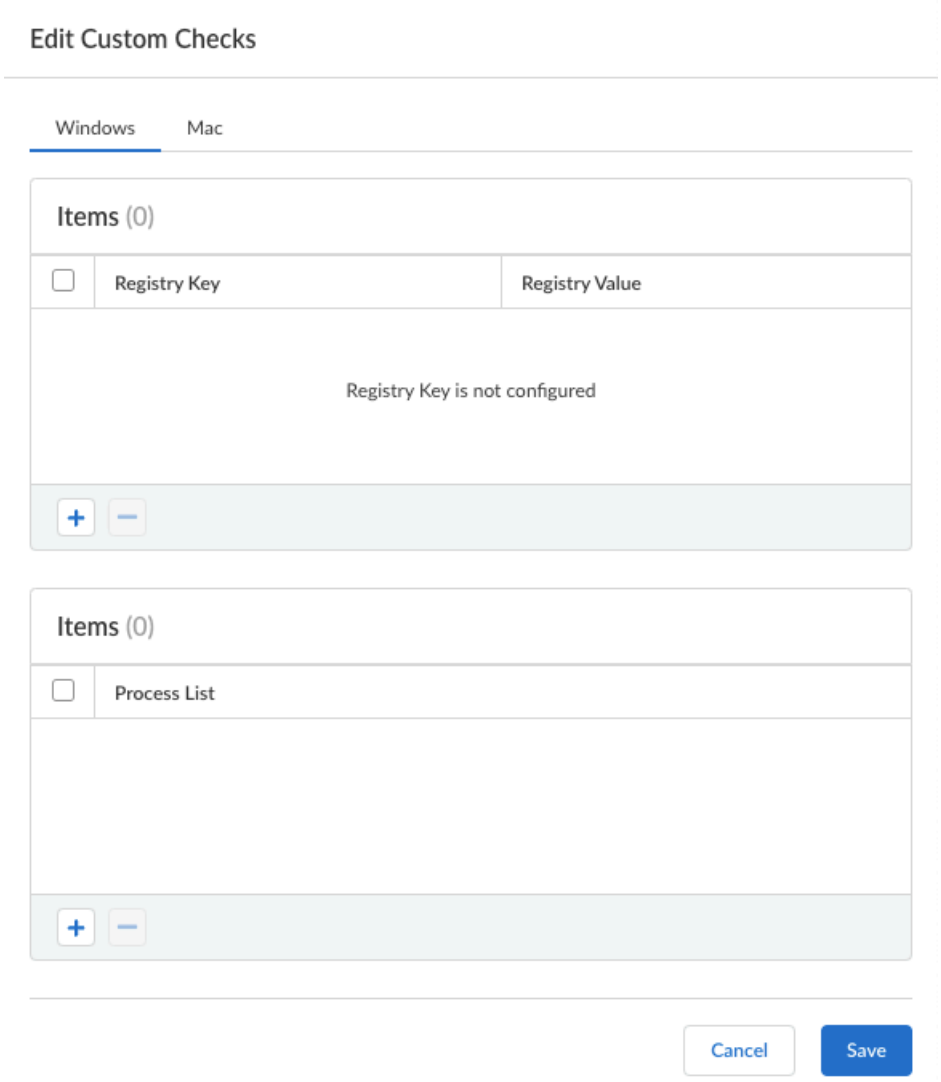
Si no quiere excluir a un proveedor completo, puede excluir parches específicos de un proveedor. Después de añadir el proveedor, puede especificar el nombre o número de parche y, opcionalmente, una fecha hasta la que desea excluir las actualizaciones de parche del informe de HIP utilizando el siguiente formato:

```
Exclude: [kb-article-id1: MM/DD/AAAA], [kb-article-id2: MM/DD/AAAA]
```

Dónde **<kb-article-id>** es el nombre o el número del atributo (por ejemplo **<kb-article-id>2267602</kb-article-id>**) y el **MM/DD/AAAA** especifica la fecha hasta la cual el parche se excluye del informe HIP. Si no establece una fecha, el parche se excluirá del informe de HIP indefinidamente. Si elige establecer una fecha, el parche se excluirá hasta la fecha especificada.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | **Edit (Editar)** las comprobaciones personalizadas para definir los datos personalizados que desea recopilar de los hosts que ejecutan esta configuración.



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 para determinar si se ha instalado esa aplicación (tiene un registro de Windows o clave plist de Mac que corresponde) o se está ejecutando actualmente (tiene un proceso en ejecución que corresponde).

- **Windows**: haga clic en **Add (Añadir)** para añadir una comprobación de una clave de registro determinada o un valor de clave. 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.
- **Mac**: deberá **Add (Añadir)** una comprobación para una clave de **Plist** determinada o un valor **Key (Clave)**. Para limitar la recopilación de datos a valores de clave específicos, haga clic en **Add (Añadir)** para añadir valores de clave. Haga clic en OK (Aceptar) para guardar los parámetros.

©2025 Palo Alto Networks, Inc.

- **Process List (Lista de procesos)**: haga clic en **Add (Añadir)** para añadir los procesos que desea comprobar en los endpoints de usuario para ver si se están ejecutando. Por ejemplo, para determinar si una aplicación de software se está ejecutando, agregue el nombre del archivo ejecutable a la lista de procesos. Puede añadir un proceso a la pestaña **Windows** o **Mac** o a ambas.

Deberá **Save (Guardar)** la configuración de comprobación personalizada cuando haya terminado.

STEP 11 | Cuando haya terminado de configurar los parámetros del Prisma Access Agent específico del proyecto, deberá **Save (Guardar)** la configuración.

 ©2025 Palo Alto Networks, Inc.

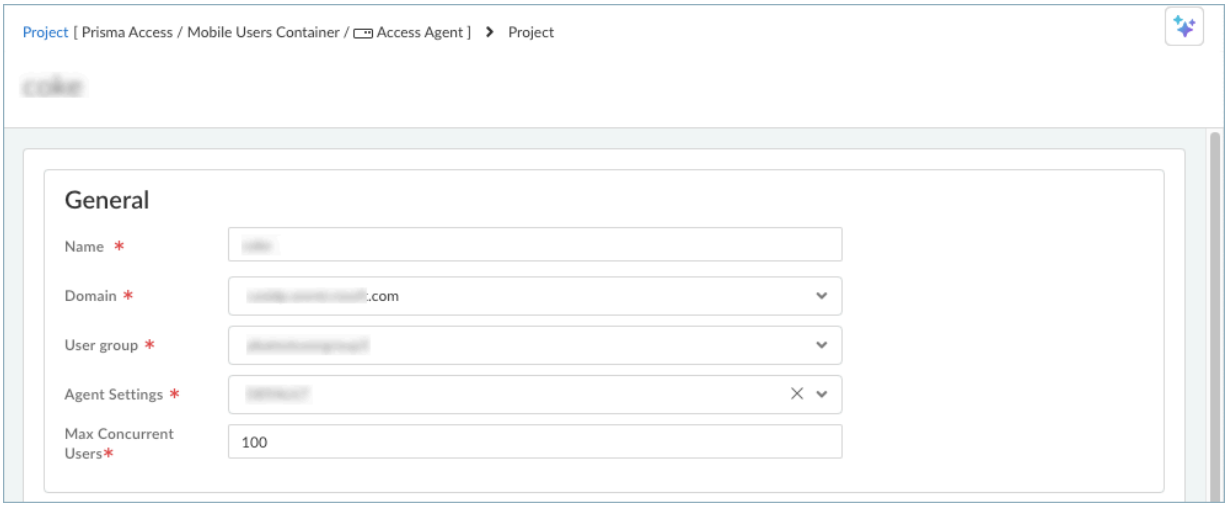
Crear un proyecto

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access ❑ Versión mínima de Prisma Access requerida: 5.1 ❑ Rol: Superusuario

Añada proyectos a los que desea que los usuarios accedan mediante el Prisma Access Agent. Sólo un administrador de proyectos puede crear y gestionar las definiciones del proyecto.

STEP 1 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**.

STEP 2 | Establezca el alcance en el fragmento de proyecto que creó y vaya a **Objects (Objetos)** > **Dynamic Privilege Access (Acceso dinámico a privilegios)** > **Projects (Proyectos)** > **Add Project (Añadir proyecto)**.

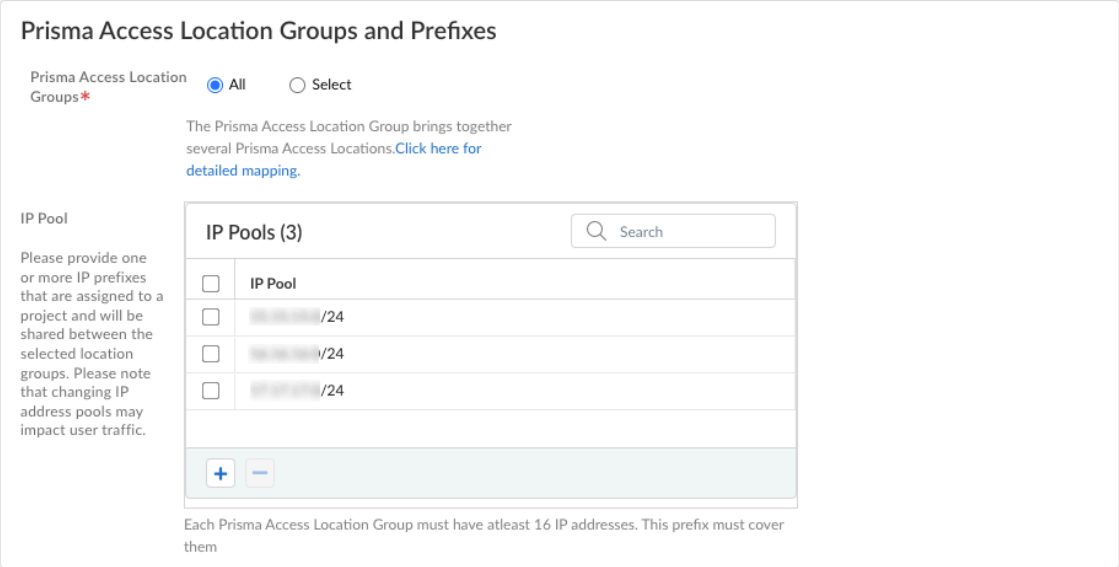


1. Introduzca un **Name (Nombre)** para el proyecto.
2. Seleccione el **Domain (Dominio)** que añadió en Cloud Identity Engine y el **User Group (Grupo de usuarios)** asignado al directorio.
3. Seleccione la **Agent Settings (Configuración del agente)** que añadió anteriormente y el **Max Concurrent Users (Número máximo de usuarios simultáneos)** para el proyecto.
4. Seleccione **Prisma Access Location Groups (Grupos de ubicaciones de Prisma Access)**. La lista de grupos de ubicaciones se completa según las ubicaciones donde añade las puertas de enlace de GlobalProtect.

   El proyecto que está creando está asociado a grupos de IP y grupos de ubicaciones. Los usuarios adquirirán las direcciones IP en función del proyecto y la ubicación de cómputo de Prisma Access a los que se conecten mediante el Prisma Access Agent. Un proyecto solo puede conectarse a la ubicación dentro del grupo de ubicaciones asociado con el proyecto. Puede seleccionar **Click here for detailed mapping (Haga clic aquí para**

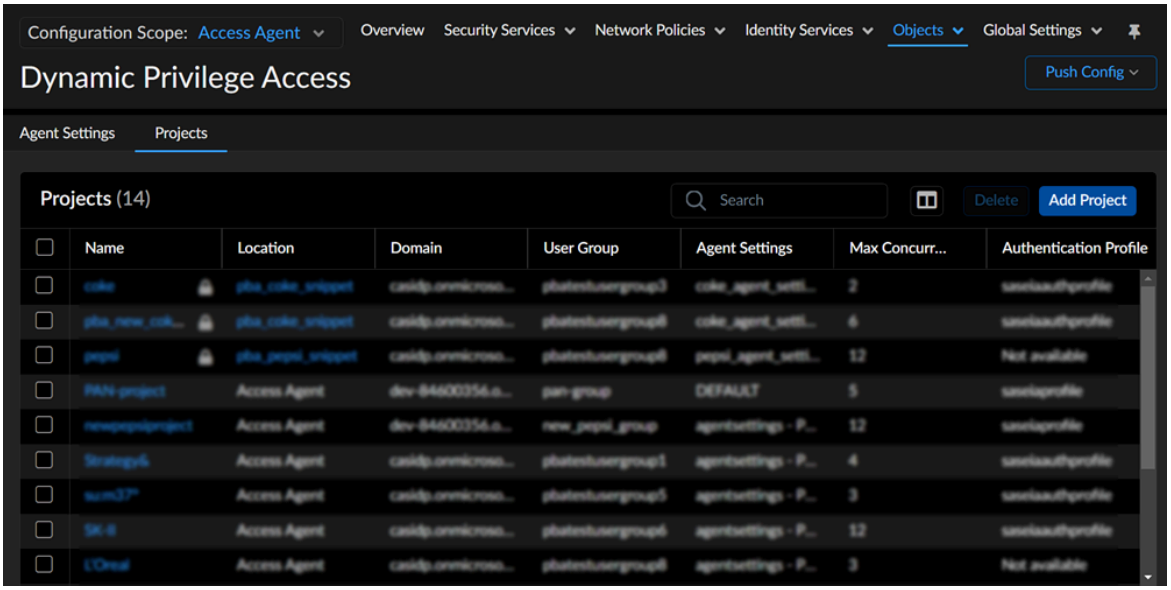
©2025 Palo Alto Networks, Inc.

obtener una asignación detallada) para ver la asignación entre los grupos de ubicaciones de Prisma Access y las ubicaciones de cómputo de Prisma Access.



5. Añada o seleccione los **IP Pools (Grupos de IP)** para su proyecto. Los prefijos de IP se asignan a su proyecto y se compartirán entre los grupos de ubicación de Prisma Access que seleccionó.

   Estos grupos de IP del proyecto se pueden resumir para reducir la cantidad de rutas que se envían a la red.
6. Deberá **Save (Guardar)** la configuración del proyecto.



 ©2025 Palo Alto Networks, Inc.

- *Cuando selecciona un fragmento de proyecto en su ámbito de configuración, puede acceder solo a las configuraciones y detalles relacionados con ese proyecto en particular.*
- *Cuando inicia sesión en Strata Cloud Manager como administrador de proyecto o administrador de envío de proyecto, solo puede ver los detalles del proyecto a los que tiene acceso. Si selecciona el alcance de configuración de otro fragmento de proyecto, no podrá acceder a la configuración y los detalles de otro proyecto.*
- *Para cambiar entre proyectos, debe volver a iniciar sesión en Strata Cloud Manager como un administrador de proyecto diferente o un administrador de envío de proyecto utilizando las credenciales de diferentes proyectos.*

STEP 3 | Seleccione **Push (Enviar)** sus cambios.

Después de crear un proyecto en Prisma Access, pueden pasar hasta 15 minutos antes de que el usuario pueda autenticarse en ese proyecto usando el Prisma Access Agent.

 ©2025 Palo Alto Networks, Inc.

Dirección de tráfico para el acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licencia de Prisma Access ☐ Versión mínima de Prisma Access requerida: 5.1 ☐ Rol: Administrador del proyecto

Utilice la dirección de tráfico para reenviar el tráfico de un proyecto a una conexión de servicio y a rutas específicas del proyecto.

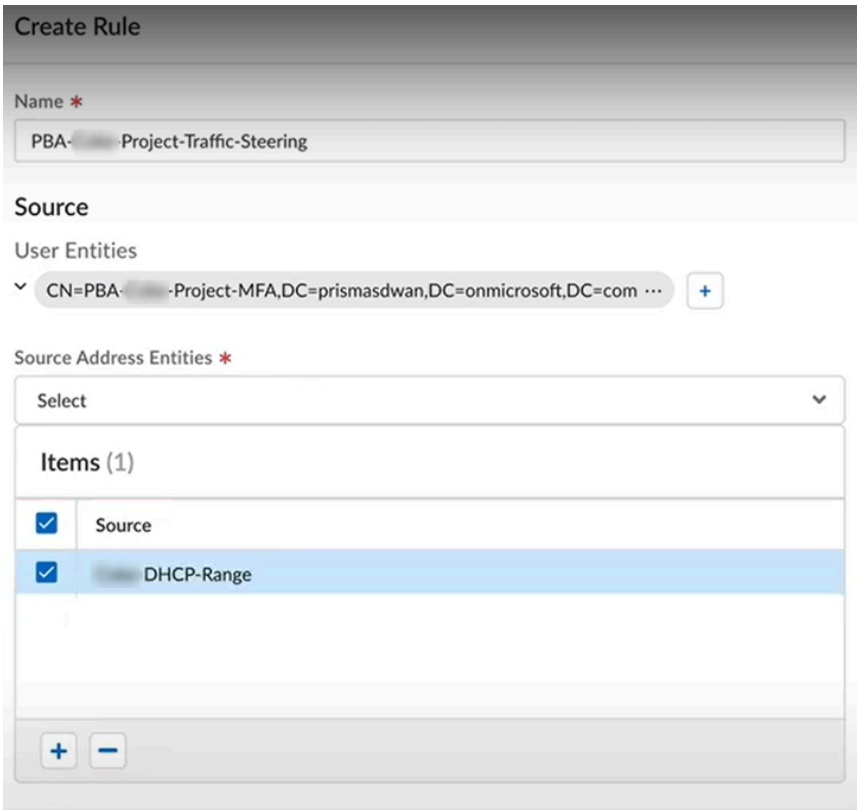
STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)**.

STEP 2 | Crear una conexión de servicio.

STEP 3 | Edite la **Advanced Settings (Configuración avanzada)** para enrutar el tráfico.

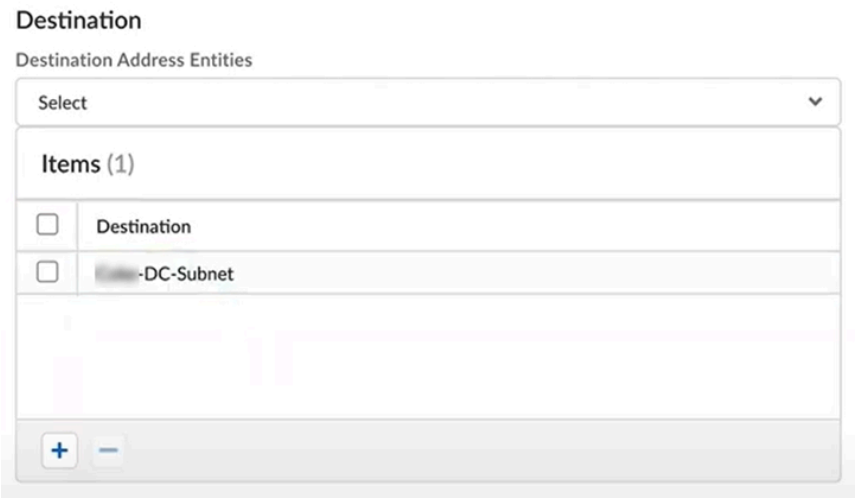
STEP 4 | **Add Rule (Añadir regla)** en **Traffic Steering (Dirección de tráfico)** para sus proyectos.

STEP 5 | Haga coincidir el **Source (Origen)** con los usuarios y añada el rango DHCP del proyecto como **Source Address Entities (Entidades de dirección de origen)**.

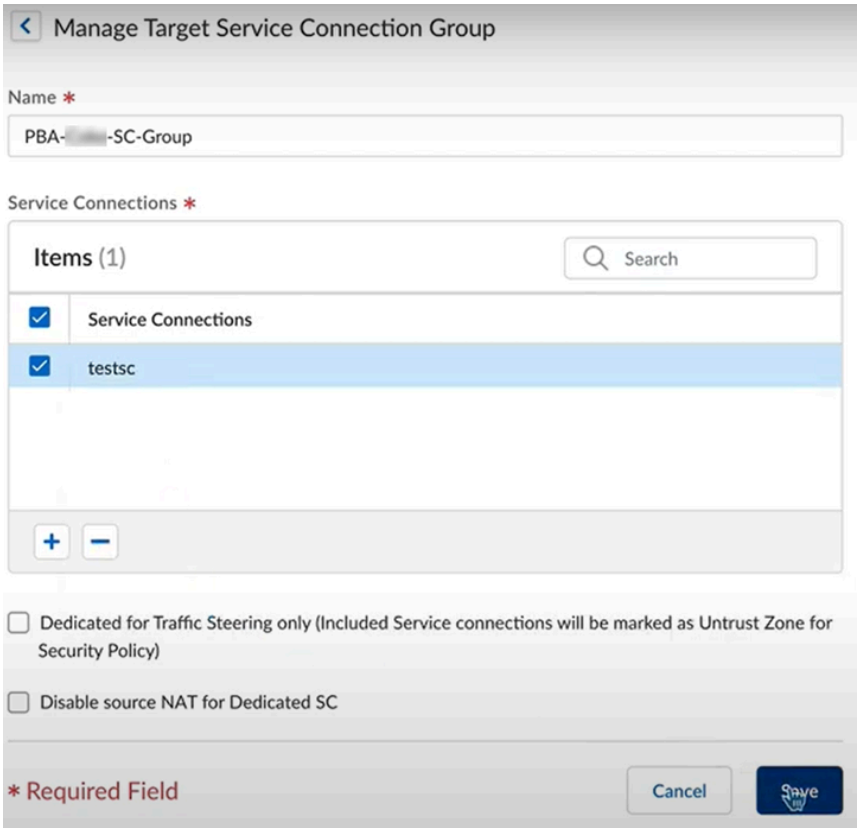


 ©2025 Palo Alto Networks, Inc.

STEP 6 | Haga coincidir las entidades de dirección de **Destination (Destino)**.



STEP 7 | Seleccione los servicios y acciones.



STEP 8 | Guardar y confirmar los cambios.

 ©2025 Palo Alto Networks, Inc.

Configurar el Prisma Access Agent para el Acceso dinámico con privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ Licencia Prisma Access con la suscripción de usuario móvil ☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Rol: Superusuario

Sus usuarios finales utilizarán el Prisma Access Agent para acceder a la red de su organización en función de los proyectos de clientes a los que están asignados sus usuarios.

Después de configurar los ajustes del agente específicos del proyecto y crear los proyectos, puede configurar otras configuraciones de Prisma Access Agent como implementaciones por etapas y configuraciones de agentes globales.

Puede configurar los siguientes ajustes de Prisma Access Agent:

- Configurar implementaciones por etapas para el agente de Prisma Access
- Configurar los parámetros globales generales para el agente de Prisma Access
- Configurar notificaciones HIP para el agente de Prisma Access

Configurar implementaciones por etapas para el Prisma Access Agent

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (gestionado por Strata Cloud Manager)	☐ Prisma Access 5.1 Preferred o Innovation ☐ Licencia Prisma Access con la suscripción de usuario móvil ☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Rol: Superusuario

La funcionalidad de implementación de actualizaciones del Agente de Prisma Access proporciona a los administradores una forma de actualizar grupos de dispositivos en un orden específico. Con

 ©2025 Palo Alto Networks, Inc.

las implementaciones de actualizaciones, ya no se tiene que depender del software de gestión de dispositivos móviles (MDM), como Jamf Pro y Microsoft Intune, para actualizar el Agente de Prisma Access.

Las implementaciones de actualización por etapas solo se pueden producir después de la implementación inicial o instalación del Agente de Prisma Access en los dispositivos de sus usuarios finales.

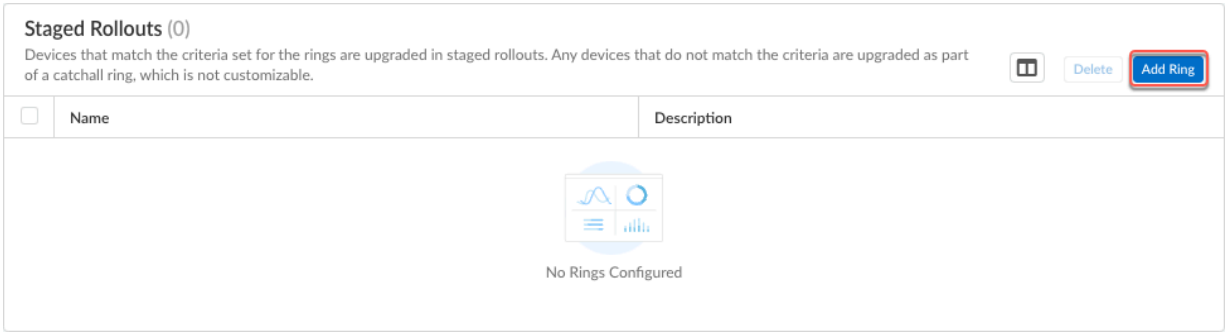
Para preparar la implementación de las actualizaciones del Agente de Prisma Access, puede configurar anillos de actualización con criterios de coincidencia basados en usuarios, grupos y sistemas operativos. Los dispositivos que coinciden con los criterios se actualizan en el orden de los anillos de actualización (anillo 0 a anillo 4, anillo predeterminado).

Opcionalmente, puede definir anillos de actualización al incorporar usuarios móviles mediante la página Configuración del agente de acceso para el Agente de Prisma Access. Si decide no definir anillos de actualización durante la configuración inicial del agente, todos los dispositivos se colocan en el anillo predeterminado. Puede volver a la página de configuración del Agente de Prisma Access más adelante para definir los anillos de actualización y enviar la configuración a Prisma Access. Estos cambios surtirán efecto durante la siguiente implementación por etapas o después de detener e iniciar una implementación por etapas.

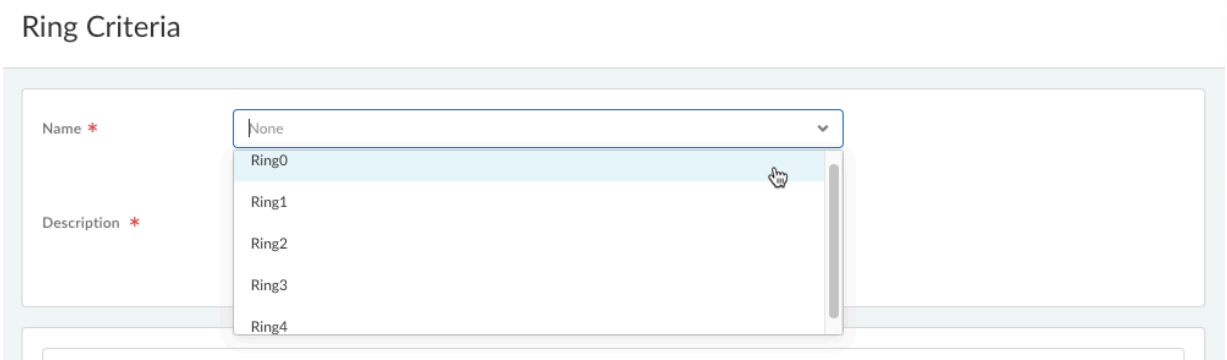
Para configurar un anillo de actualización:

STEP 1 | En Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Prisma Access Agent (Agente de Prisma Access)**.

STEP 2 | En **Staged Rollouts (Implementaciones por etapas)**, haga clic en **Add Ring (Añadir anillo)**.



STEP 3 | Seleccione un **Name (Nombre)** predefinido para el anillo. Puede seleccionar de **Anillo0** a **Anillo4**. El primer anillo que añadirá es **Ring0 (Anillo0)**.

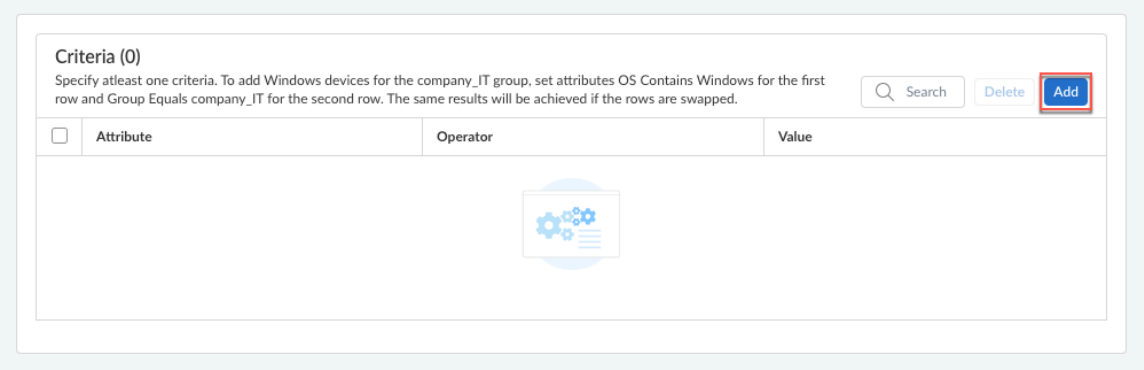


 ©2025 Palo Alto Networks, Inc.

STEP 4 | Introduzca un **Description (Descripción)** para el anillo.

STEP 5 | Especifique los criterios para el anillo en función de los atributos **User (Usuario)**, **Groups (Grupos)** o **Device OS (SO del dispositivo)**.

1. Elija **Add (Añadir)** un criterio.



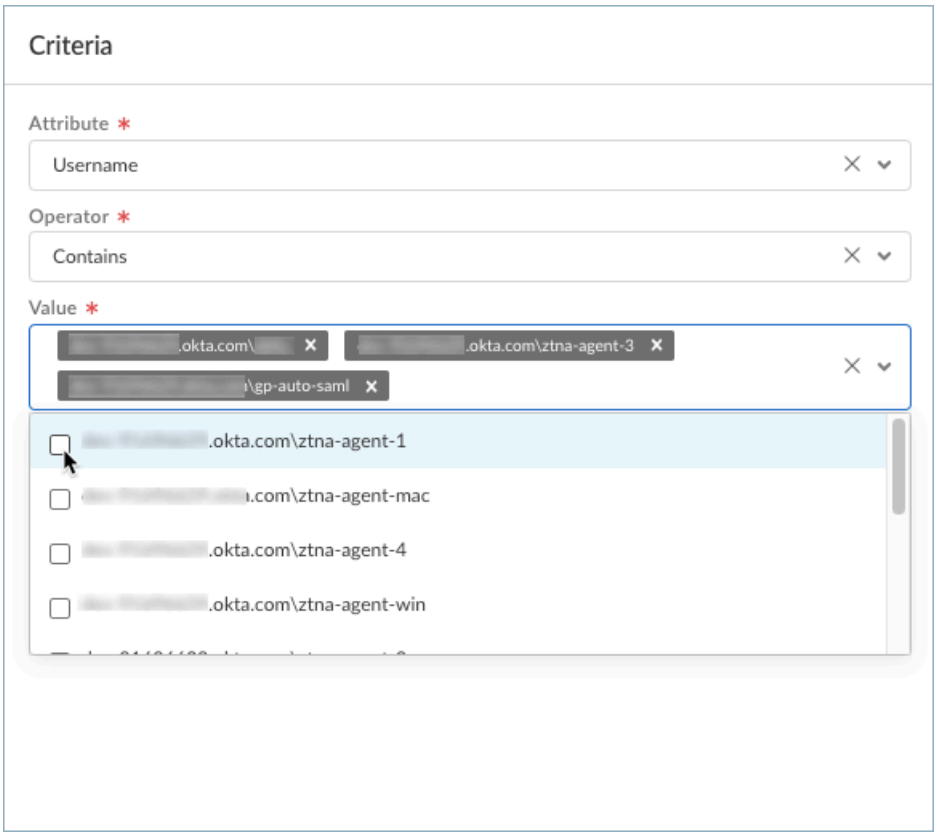
2. Para cada criterio, seleccione un **Attribute (Atributo)**, **Operator (Operador)**, **Value (Valor)**y, a continuación, haga clic en **Add (Añadir)**.

   Solo puede seleccionar un atributo y un operador por criterio. El valor depende de lo que haya seleccionado para el atributo y el operador:

   - En el caso del atributo **Username (Nombre de usuario)**:
     - Si selecciona **Operator (Operador)** > **Contains (Contiene)**, seleccione o busque un nombre de usuario de la lista **Value (Valor)**. Para iniciar una búsqueda, comience a

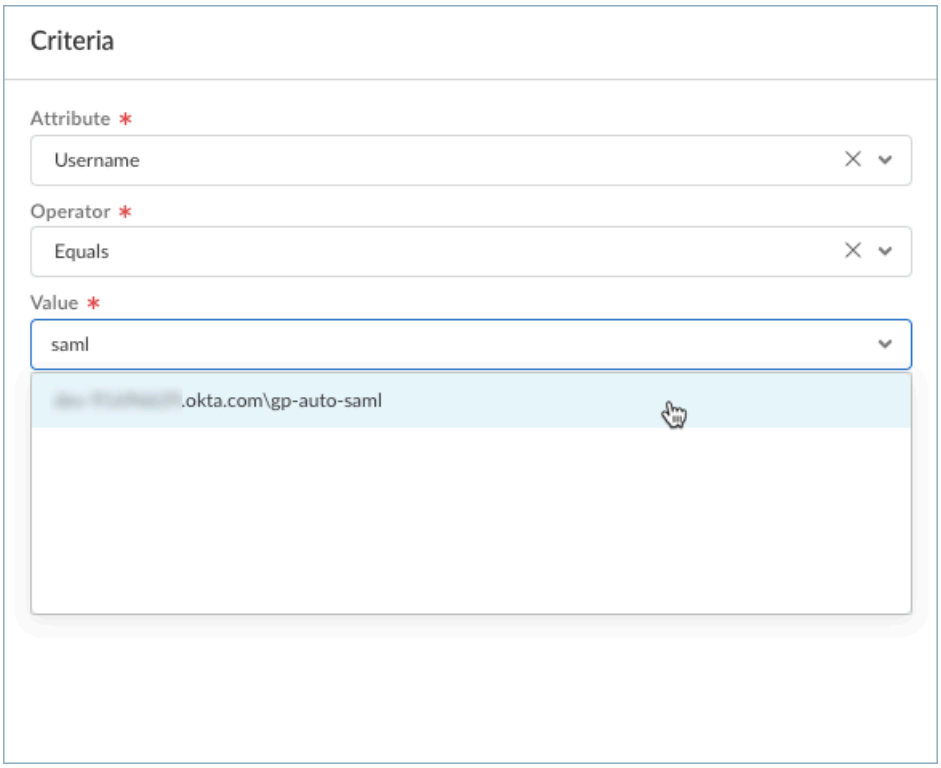
©2025 Palo Alto Networks, Inc.

escribir el nombre de usuario. Puede seleccionar uno o más nombres de usuario de la lista.

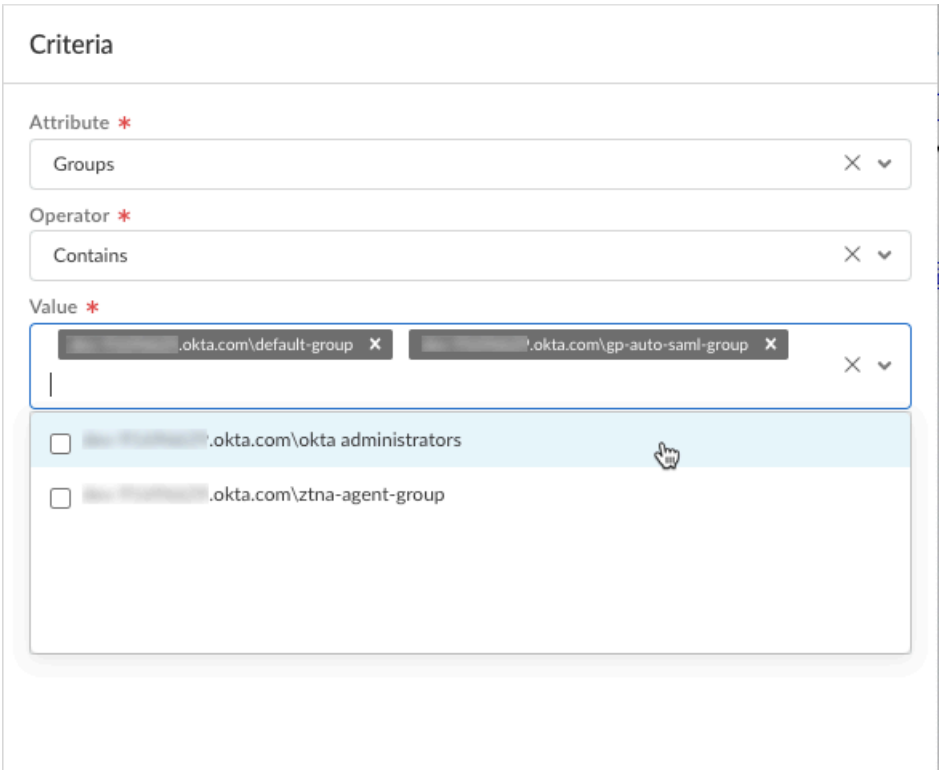


- Si selecciona **Operator (Operador)** > **Equals (Iguales)**, seleccione o busque un nombre de usuario en la lista **Value (Valor)**. Para iniciar una búsqueda, comience a escribir el nombre de usuario. Puede seleccionar un nombre de usuario de la lista.

©2025 Palo Alto Networks, Inc.

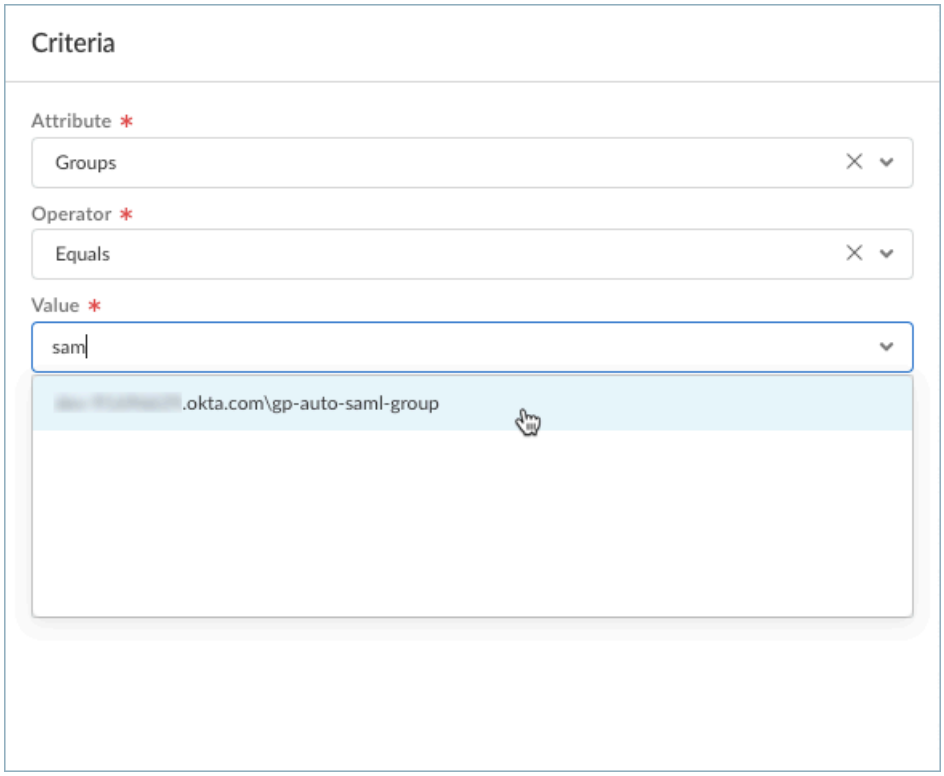


- En el caso del atributo **Groups (Grupos)**:
  - Si selecciona **Operator (Operador)** > **Contains (Contiene)**, seleccione o busque un grupo de la lista **Value (Valor)**. Para iniciar una búsqueda, comience a escribir el nombre del grupo. Puede seleccionar uno o más grupos de la lista.



 ©2025 Palo Alto Networks, Inc.

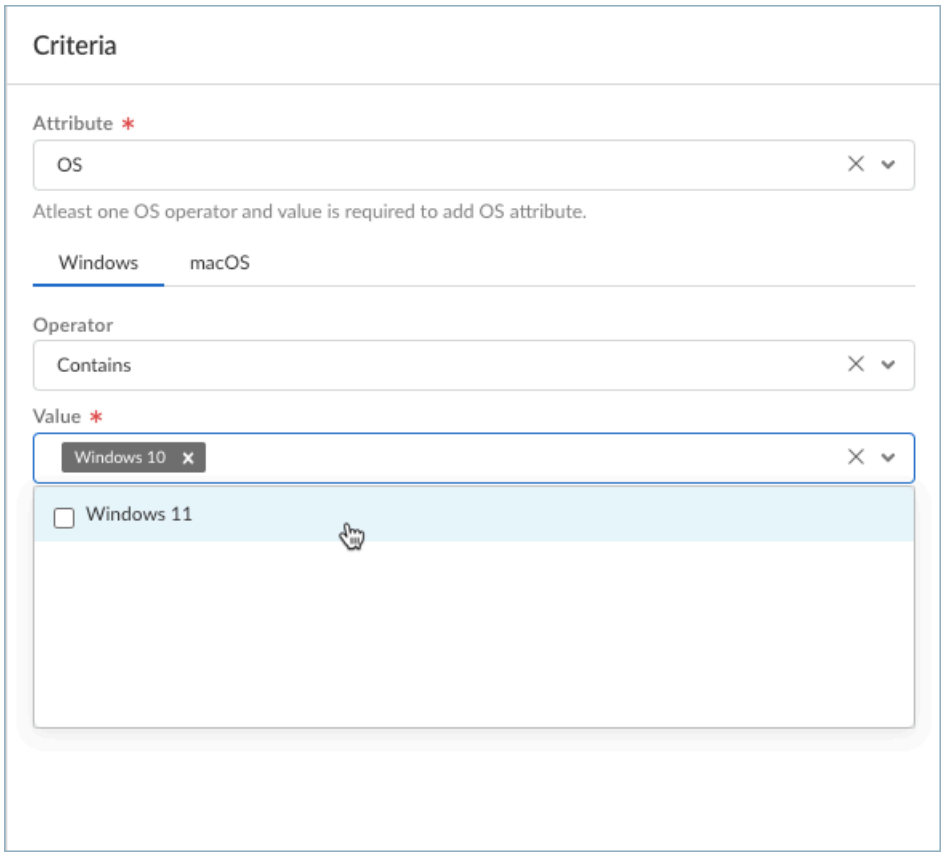
- Si selecciona **Operator (Operador)** > **Equals (Igual)**, seleccione o busque un grupo de la lista **Value (Valor)**. Para iniciar una búsqueda, comience a escribir el nombre del grupo. Puede elegir un grupo de la lista.



- En el caso del atributo **OS (SO)**, seleccione un tipo de sistema operativo (**Windows** o **macOS**). A continuación:
  - Si selecciona **Operator (Operador)** > **Contains (Contiene)**, busque o seleccione una o más versiones del sistema operativo de la lista **Value (Valor)**. Para iniciar una

©2025 Palo Alto Networks, Inc.

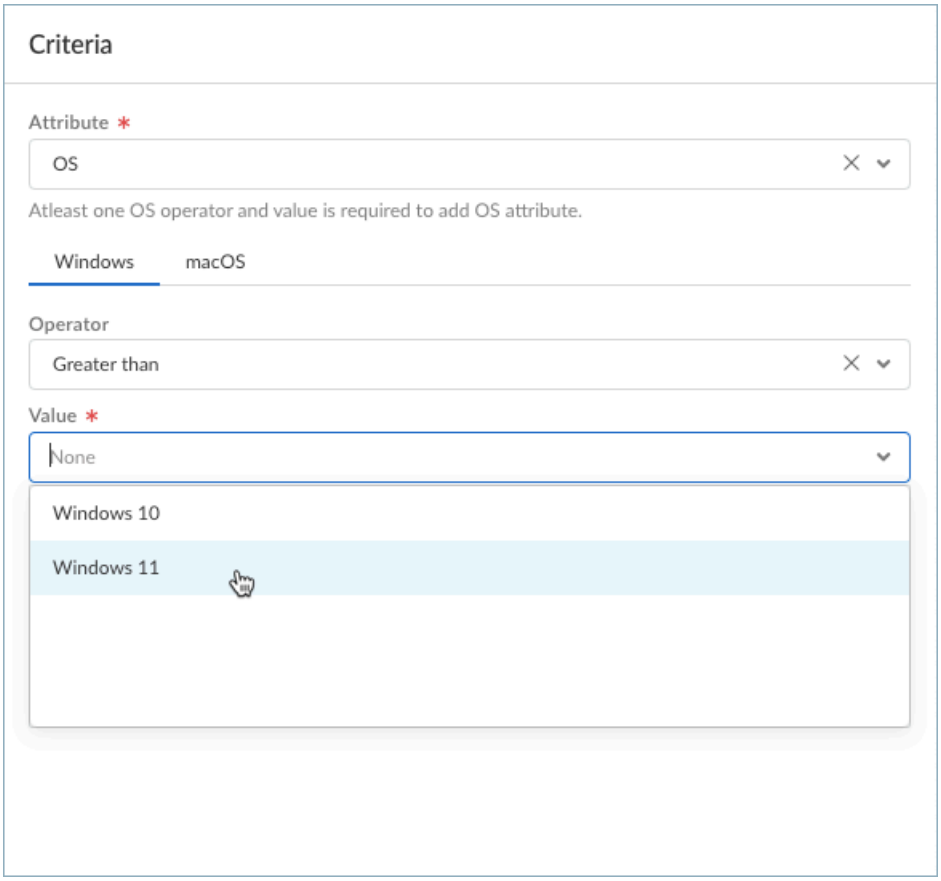
búsqueda, comience a escribir el sistema operativo y la versión. Puede seleccionar una o más versiones del sistema operativo de la lista.



- Si selecciona el operador **Greater than (Mayor que)** o **Less than (Menor que)**, busque o seleccione una versión del sistema operativo en el lista **Value (Valor)**.

 ©2025 Palo Alto Networks, Inc.

Para iniciar una búsqueda, comience a escribir el sistema operativo y la versión. Puede seleccionar una versión del sistema operativo de la lista.



3. Si es necesario, deberá **Add (Añadir)** más criterios. Puede especificar hasta tres criterios por anillo.

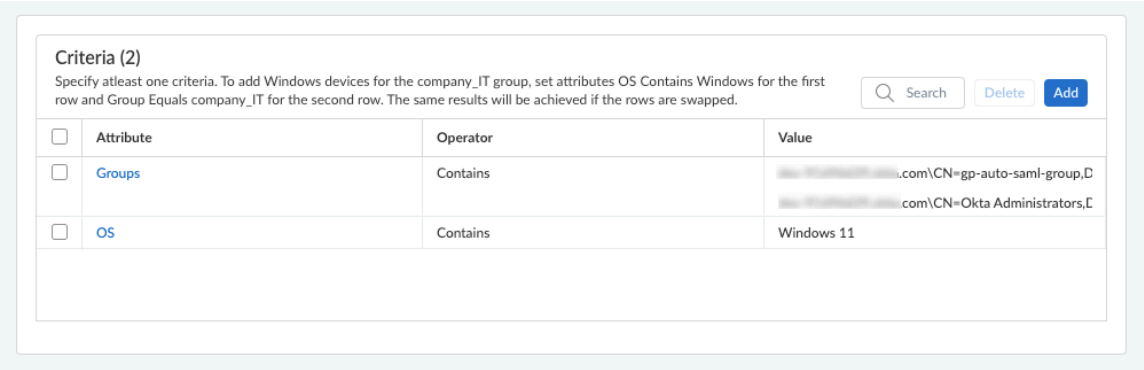
   Solo puede utilizar un atributo una vez por anillo. Después de añadir un criterio mediante un atributo, ese atributo ya no aparecerá en el archivo menú desplegable **Attribute (Atributo)**.

   Después de añadir los criterios, los criterios se muestran en el archivo **Criteria (Criterios)** en la página Criterios de anillo. Cuando Prisma Access evalúa los criterios, los valores

 ©2025 Palo Alto Networks, Inc.

enumerados en la misma celda se evalúan mediante el operador lógico OR, mientras que los atributos y valores entre las filas se evalúan mediante el operador lógico AND.

Por ejemplo, los criterios de la siguiente imagen harán coincidir los dispositivos que pertenecen al grupo **`gp-auto-saml-group`** o **`Administradores de Okta`** y ejecutará el sistema operativo Windows 11.



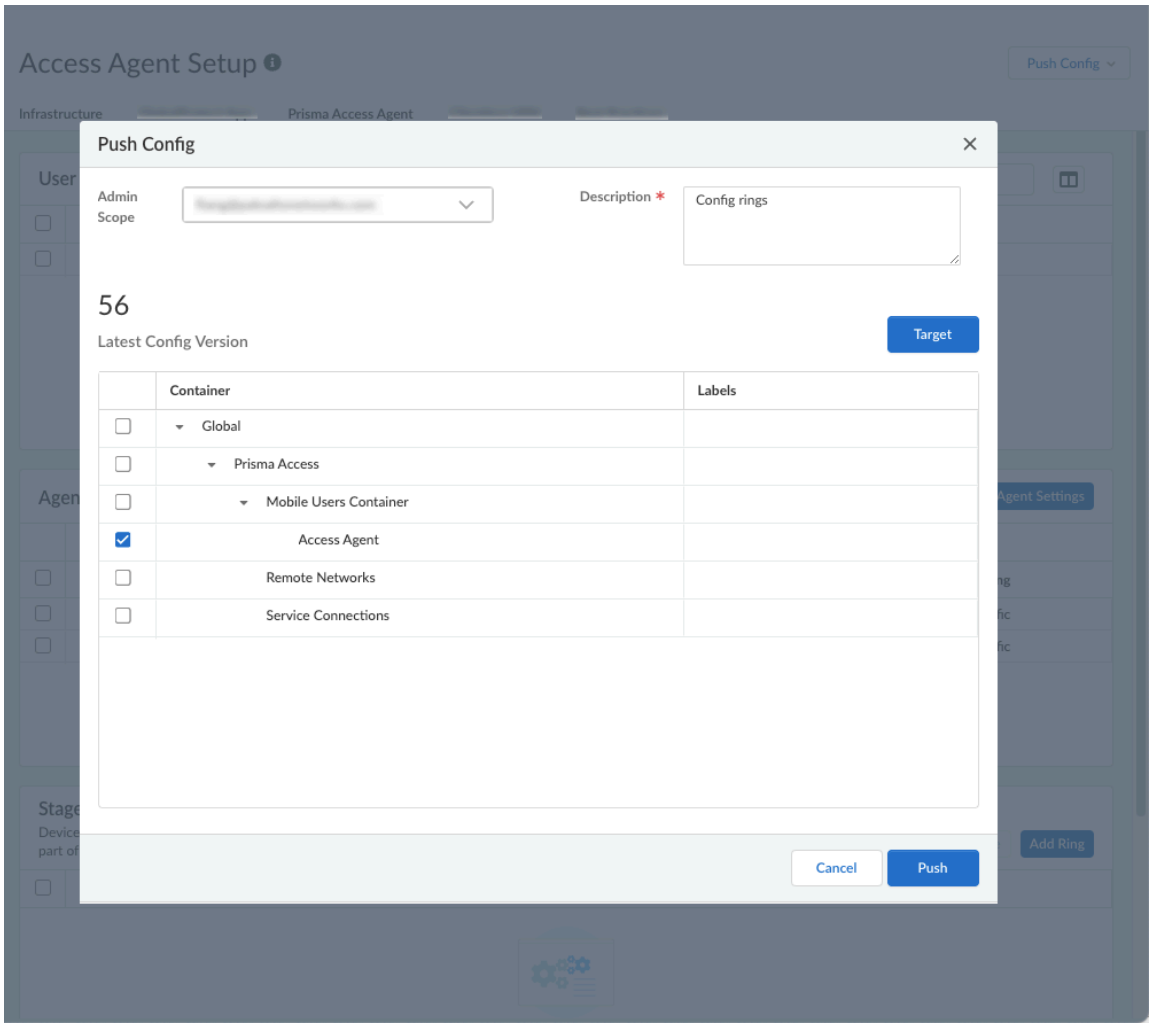
4. Deberá **Save (Guardar)** los criterios de anillo.

STEP 6 | Para crear más anillos, repita los pasos 2 a 5. Puede crear un total de cinco anillos (Anillo 0 a Anillo 4).

 ©2025 Palo Alto Networks, Inc.

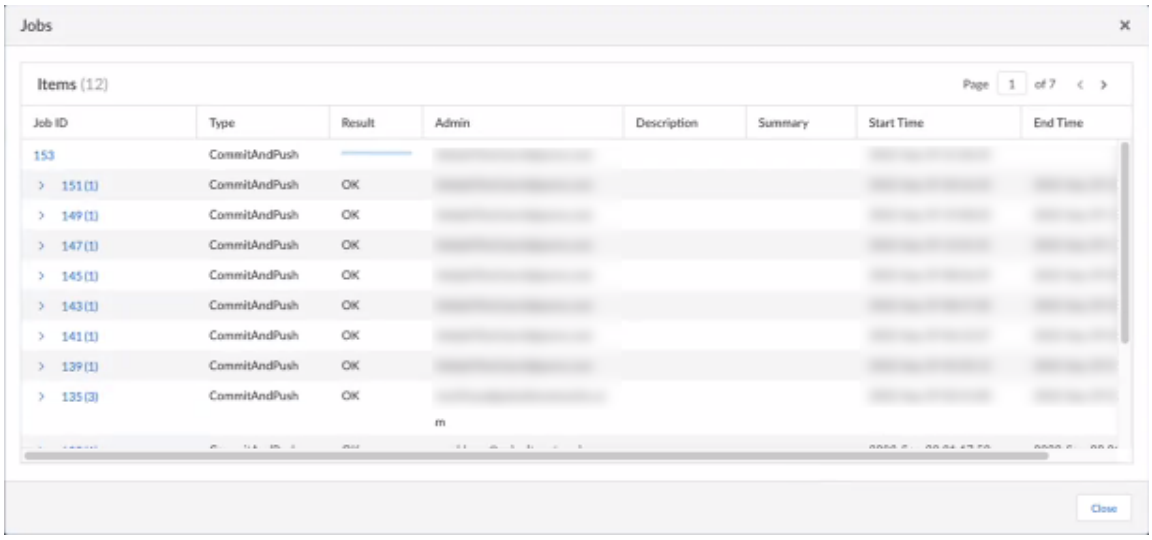
STEP 7 | Envíe la configuración a Prisma Access.

1. Seleccione **Push Config (Enviar configuración)** > **Push (Enviar)**.
2. Introduzca una **Description (Descripción)** para la pila.
3. Seleccione el contenedor **Global** > **Prisma Access** > **Mobile Users (Usuarios móviles)** > **Access Agent (Agente de acceso)** y haga clic en **Push (Enviar)**.



4. Espere a que finalice el trabajo y seleccione **Close (Cerrar)** el cuadro de diálogo de Tareas.

 ©2025 Palo Alto Networks, Inc.



STEP 8 | Puede supervisar la implementación por etapas en **Manage (Gestionar)** > **Prisma Access Agent (Agente de Prisma Access)** en Strata Cloud Manager.

Configure los ajustes globales generales para Prisma Access Agents

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ Licencia de Prisma Access con la suscripción de usuario móvil ☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Rol: Superusuario

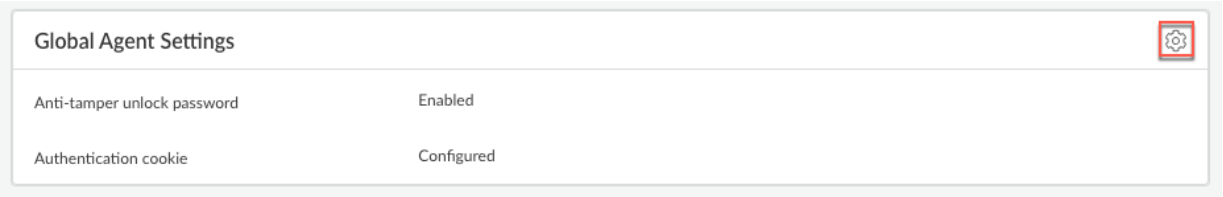
Puede personalizar la configuración global del agente que se aplica a los agentes de Prisma Access en todos los endpoints.

La configuración global del agente general incluye la configuración de la función antimanipulación que evita que los usuarios manipulen el Agente de Prisma Access, como desinstalarlo del dispositivo de un usuario final. Además, puede configurar los parámetros de anulación de autenticación, el parámetro del tiempo de espera por inactividad y bloquear el inicio de sesión de dispositivos en cuarentena.

STEP 1 | Desde Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Prisma Access Agent (Agente de Prisma Access)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Edite la **Global Agent Settings (Configuración de agente global)**



STEP 3 | Seleccione **General**.

STEP 4 | Configure una contraseña de desbloqueo antimanipulación.

Puede proteger el Agente de Prisma Access habilitando la función antimanipulación, que evita que cualquier usuario no autorizado manipule el Agente de Prisma Access. La función antimanipulación puede proteger los siguientes recursos del Agente de Prisma Access en sus endpoints:

- Carpetas y archivos del Agente de Prisma Access: los usuarios no autorizados no pueden eliminar ni cambiar el nombre de ningún archivo o carpeta relacionado con el Agente de Prisma Access.
- Servicios de Agente de Prisma Access y procesos de perfil de información de host (HIP): los usuarios no autorizados no pueden detener ningún servicio relacionado con el Agente de Prisma Access ni ningún proceso HIP. Los procesos HIP recopilan información sobre el host en el que se ejecuta el Agente de Prisma Access y envían la información del host a Prisma Access para su inspección. Si un usuario intenta detener un proceso, debe proporcionar la contraseña de desbloqueo antimanipulación.
- Claves de registro de Agente de Prisma Access (en Windows) o archivo `.plist` (en macOS): los usuarios no autorizados no pueden eliminar ni actualizar las claves de registro de Windows ni el archivo `.plist` de Agente de Prisma Access.
- La interfaz de línea de comandos de PACli: los usuarios no autorizados no pueden deshabilitar el Agente de Prisma Access ni la función antimanipulación mediante la interfaz de línea de comandos de PACli. Los administradores y usuarios autorizados que necesitan realizar determinadas acciones para solucionar problemas en la línea de comandos deben proporcionar la contraseña de desbloqueo antimanipulación (supervisor) cuando se les solicite.

Para desbloquear la función antimanipulación para solucionar problemas del Agente de Prisma Access, debe configurar una contraseña de desbloqueo de la antimanipulación (también conocida como contraseña de supervisor).

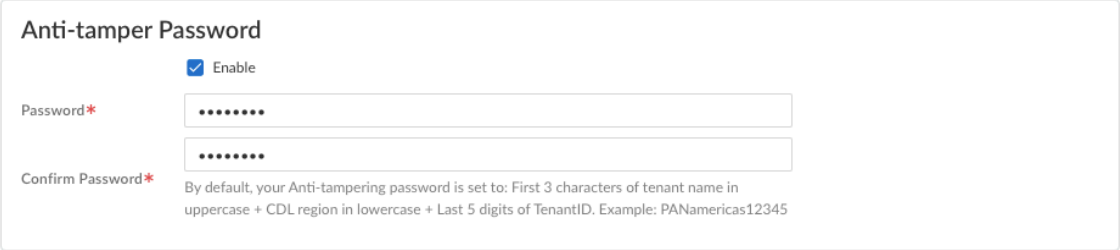
1. Deberá **Enable (Habilitar)** la contraseña antimanipulación.

   Si no habilita la contraseña antimanipulación, no se asigna ninguna contraseña y el usuario puede introducir cualquier contraseña (incluida una contraseña vacía) cuando se le solicite en la línea de comandos del Agente de Prisma Access.

   Si deshabilita la contraseña antimanipulación después de habilitarla, los usuarios pueden ejecutar ciertos comandos PACli en el agente, como los comandos **`pacli disable`**, **`pacli hip status`**, **`pacli protect disable`**y **`pacli switchto GlobalProtect`**, sin proporcionar la contraseña de supervisor. Sólo necesitan pulsar **Enter (Intro)** cuando se les solicite la contraseña.

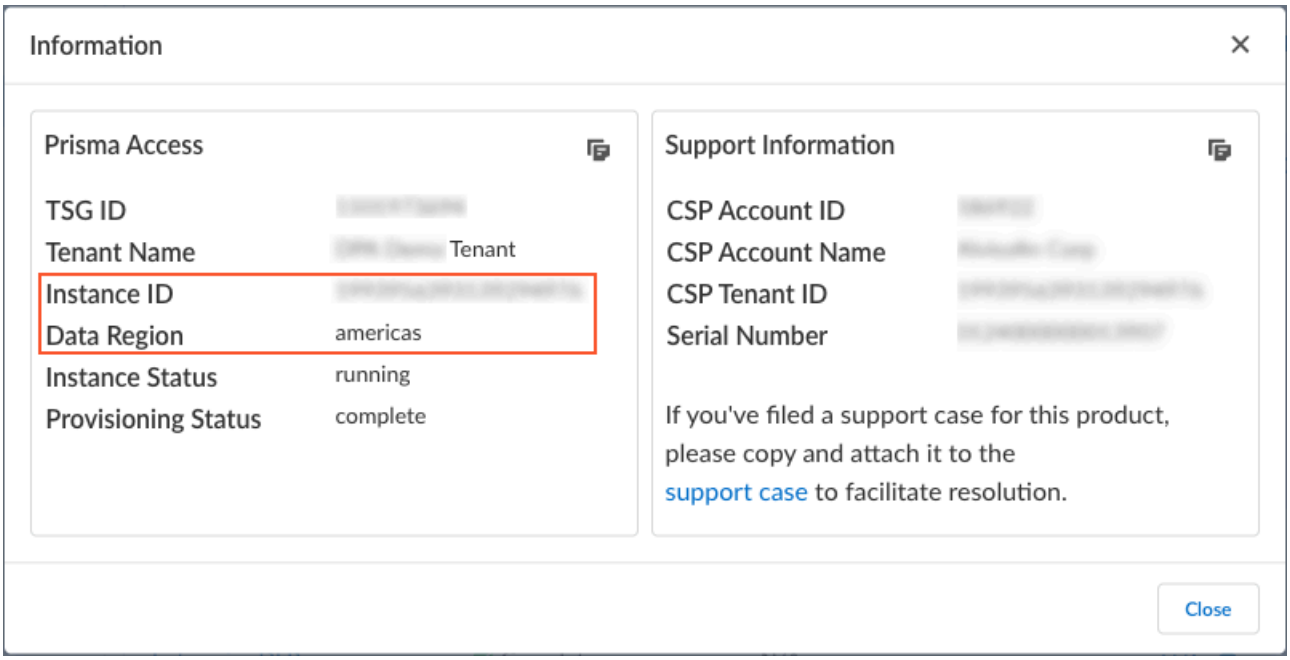
 ©2025 Palo Alto Networks, Inc.

2. Introduzca la **Password (Contraseña)** y luego vuelva a introducirla para **Confirm Password (Confirmar contraseña)**. La contraseña debe tener un mínimo de ocho caracteres alfanuméricos.



Si no proporciona una contraseña, se utilizará la contraseña predeterminada. De manera predeterminada, la contraseña antimanipulación se establece con los primeros tres caracteres del nombre del inquilino de Prisma Access en mayúsculas, más la **Data Region (Región de datos)** de Prisma Access en minúsculas, más los últimos cinco dígitos del **Instance ID (ID de instancia)** de Prisma Access, por ejemplo: **PANamericas56789**.

Puede obtener el **Instance ID (ID de instancia)** de Prisma Access y la **Data Region (Región de datos)** seleccionando **Settings (Configuración)** > **Tenants (Inquilinos)** > **<your_tenant>** y seleccionando la información sobre herramientas **View Support Info (Ver información de asistencia)** junto al número de serie de Prisma Access.

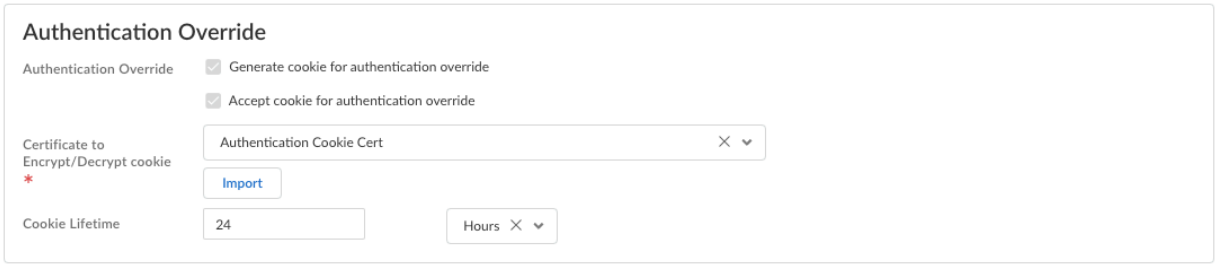


Para proporcionar un mayor nivel de seguridad a sus agentes, configure una nueva contraseña de desbloqueo antimanipulación para anular la contraseña predeterminada, ya que esta podría no ser la más segura.

STEP 5 | Configure los parámetros de la **Authentication Override (Anulación de autenticación)** para permitir que la puerta de enlace genere y acepte cookies seguras y cifradas para la autenticación del usuario. La anulación de la autenticación permite al usuario proporcionar

 ©2025 Palo Alto Networks, Inc.

credenciales de inicio de sesión solo una vez durante la **Cookie Lifetime (Vida útil de la cookie)**especificada.



- **Generate cookie for authentication override (Generar cookie para la anulación de la autenticación)**: permite que Prisma Access genere cookies cifradas y específicas del endpoint y emite cookies de autenticación al endpoint.
- **Accept cookie for authentication override (Aceptar cookie para la anulación de autenticación)**: permite que Prisma Access autentique usuarios con una cookie válida y cifrada. Cuando la aplicación presenta una cookie válida, Prisma Access verifica que Prisma Access cifraron la cookie, descifra la cookie y, luego, autentica el usuario.
- **Certificate to Encrypt/Decrypt Cookie (Certificado para cifrar/descifrar la cookie)**: selecciona el certificado que se debe usar para cifrar o descifrar la cookie.
- **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 rango de horas es de 1 a 72; el rango de semanas es de 1 a 52; y el rango de días es de 1 a 365. Una vez que la cookie caduca, el usuario debe volver a introducir sus credenciales de inicio de sesión. Luego, Prisma Access cifra una nueva cookie para enviarla al agente. Este valor puede ser el mismo o diferente a la vida útil de la cookie que configuró para el portal.

STEP 6 | Introduzca el número de minutos para el **Inactivity Logout (Cierre de sesión por inactividad)** para especificar el tiempo después del cual los usuarios inactivos cierran la sesión del Agente de Prisma Access.

Puede utilizar el período de cierre de sesión por inactividad para aplicar una política de seguridad para supervisar el tráfico desde los endpoints mientras está conectado a Prisma Access y para cerrar rápidamente las sesiones inactivas del Agente de Prisma Access. Puede aplicar un período de cierre de sesión de inactividad más corto. Los sesión se desconectan si el Agente de Prisma Access no ha enrutado tráfico a través del túnel VPN o si la puerta de enlace no recibe una comprobación HIP del endpoint en el período establecido.

STEP 7 | **Bloquear el inicio de sesión para dispositivos en cuarentena** para evitar que los usuarios del Agente de Prisma Access inicien sesión desde dispositivos en cuarentena.

Si un usuario intenta iniciar sesión desde un dispositivo en cuarentena cuando esta configuración está habilitada, el Agente de Prisma Access notifica al usuario que el dispositivo está en cuarentena y el usuario no puede iniciar sesión desde dicho dispositivo. Si esta configuración no está habilitada, el usuario recibe la notificación pero puede iniciar sesión desde ese dispositivo.

STEP 8 | Seleccione **Save (Guardar)** su configuración.

©2025 Palo Alto Networks, Inc.

Configurar notificaciones HIP para el acceso dinámico a privilegios de Prisma Access Agent

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Superusuario

En la pestaña **HIP Notifications (Notificaciones HIP)** de la página Editar configuración global del agente, puede crear notificaciones de perfil de información de host, crear y gestionar objetos HIP, y crear y gestionar perfiles HIP que se aplican al Agente de Prisma Access en todos los endpoints.

El Agente de Prisma Access recopila información sobre el host en el que se está ejecutando y envía esta información de host a la ubicación de Prisma Access (puerta de enlace) tras una conexión realizada correctamente. La puerta de enlace compara esta información del host sin procesar que envía el Agente de Prisma Access frente a 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 Prisma Access está conectado. El Agente de Prisma Access 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, para los endpoints que no cumplan esta regla, puede crear un mensaje de notificación que alerte a los usuarios de por qué se les ha denegado el acceso. También puede proporcionar un enlace a la ubicación donde pueden acceder al programa de instalación del software de cifrado que falta. Para permitir que el usuario acceda a ese recurso compartido de archivos, tendrá que crear una regla de seguridad correspondiente que permita el acceso al recurso compartido particular para los hosts con esa coincidencia de perfil HIP específica.

Puede completar las siguientes tareas:

 ©2025 Palo Alto Networks, Inc.

- Crear una notificación HIP para el acceso dinámico a privilegios de Prisma Access Agent
- Crear y gestionar objetos HIP para el acceso dinámico a privilegios de Prisma Access Agent
- Crear y gestiona perfiles HIP para el acceso dinámico a privilegios de Prisma Access Agent

Crear una notificación HIP para el acceso dinámico a privilegios de Prisma Access Agent

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Superusuario

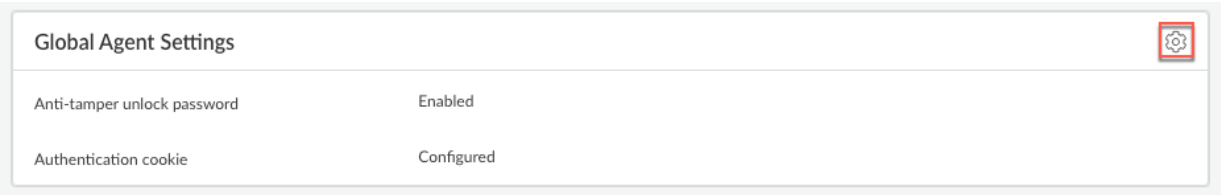
Puede definir los mensajes de notificaciones que ven los usuarios finales cuando se aplica una regla de seguridad con un perfil HIP.

La decisión de mostrar un mensaje de notificación cuando la configuración del usuario coincide o no coincide con un perfil HIP en la política depende en gran medida de su política, y de lo que significa una coincidencia (o no coincidencia) de HIP para el usuario. Es decir, ¿una coincidencia significa que se les concede acceso completo a los recursos de su red o significa que tienen 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. Podría 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.

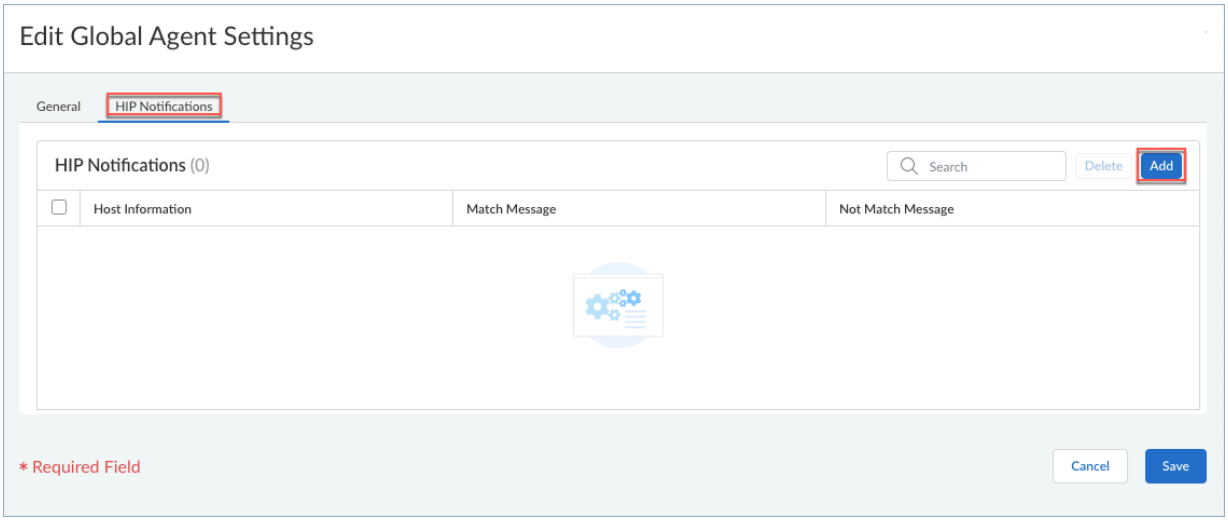
STEP 1 | Desde Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Prisma Access Agent (Agente de Prisma Access)**.

STEP 2 | Deberá **Edit (Editar)** la **Global Agent Settings (Configuración global del agente)**.

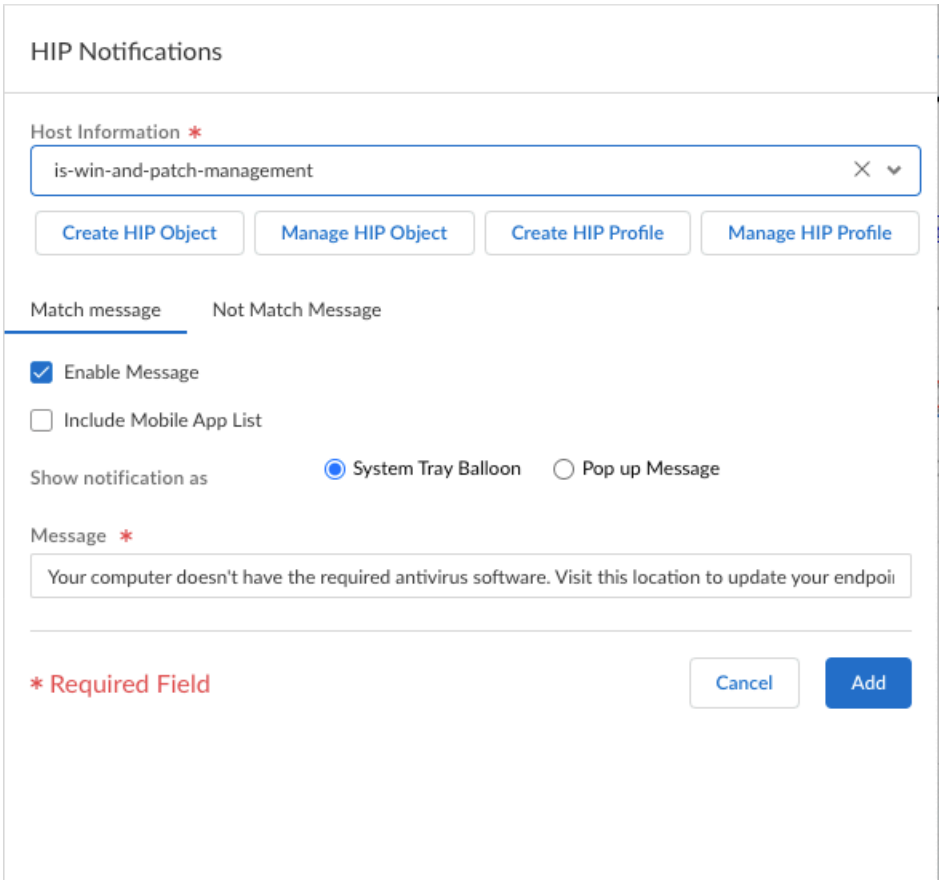


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Seleccione **HIP Notifications (Notificaciones HIP)** y haga clic en **Add (Añadir)**.



STEP 4 | Seleccione el perfil HIP al que se aplica este mensaje en el menú desplegable **Host Information (Información de host)**.



Si no hay perfiles HIP, deberá crear un perfil HIP.

STEP 5 | Dependiendo de 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 desee crear

 ©2025 Palo Alto Networks, Inc.

mensajes tanto para una coincidencia como para una no coincidencia, según los objetos que esté haciendo coincidir y cuáles sean sus objetivos para la política.

STEP 6 | Seleccione **Enable Message (Habilitar mensaje)** y luego seleccione si desea mostrar el mensaje como un **System Tray Balloon (Globo de la bandeja del sistema)** o como **Pop Up Message (Mensaje emergente)**.

STEP 7 | Introduzca el texto de su **Message (Mensaje)** y luego haga clic en **Add (añadir)**.

STEP 8 | Repita este procedimiento para cada mensaje que quiera definir.

Crear y gestionar objetos HIP para el acceso dinámico a privilegios de Prisma Access Agent

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Superusuario

Puede definir qué atributos de host le interesa supervisar o utilizar para la aplicación de políticas creando objetos HIP y perfiles HIP en la puerta de enlace de Prisma Access.

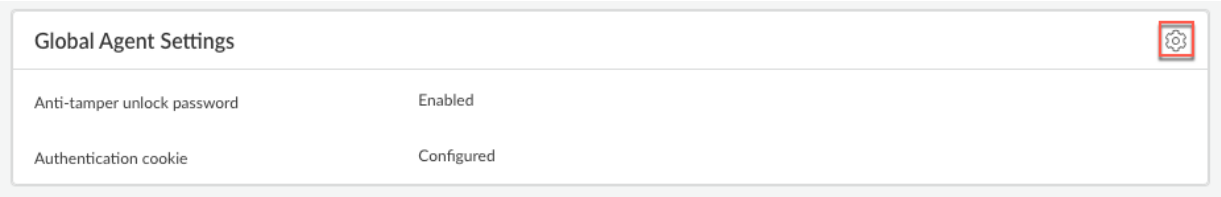
Los objetos HIP consisten en los criterios de coincidencia utilizados para filtrar la información de host que está interesado en usar para aplicar la política a partir de los datos sin formato indicados por el Agente de Prisma Access. Por ejemplo, aunque los datos sin procesar del host pueden incluir información sobre varios paquetes de antivirus instalados en el endpoint, puede que solo esté interesado en una aplicación concreta. 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, intente 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 un sistema operativo determinado. De este modo, tendrá la flexibilidad de crear una política aumentada HIP granular (y muy potente).

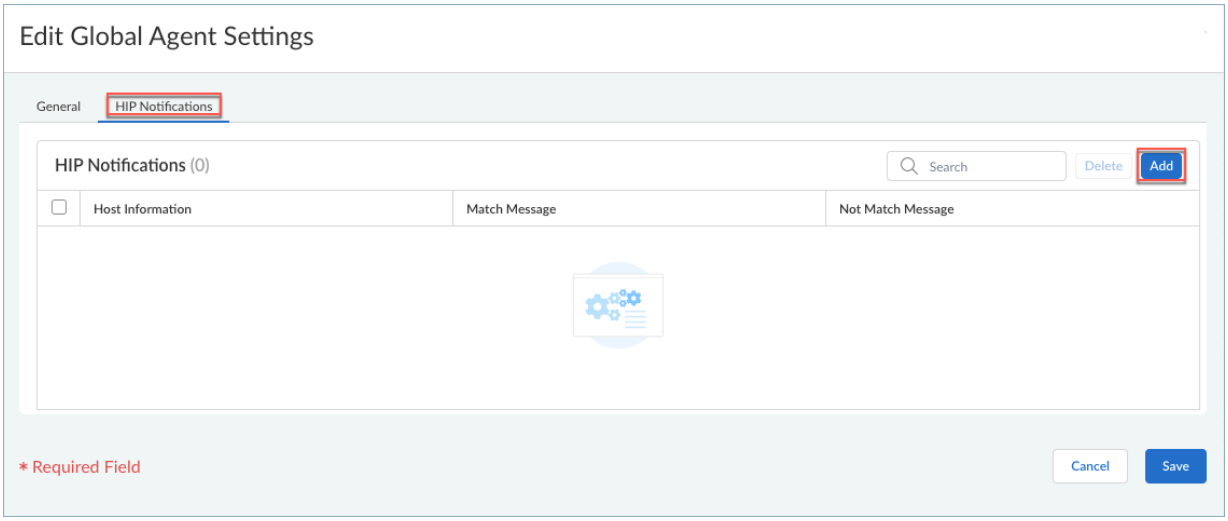
STEP 1 | Desde Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Prisma Access Agent (Agente de Prisma Access)**.

 ©2025 Palo Alto Networks, Inc.

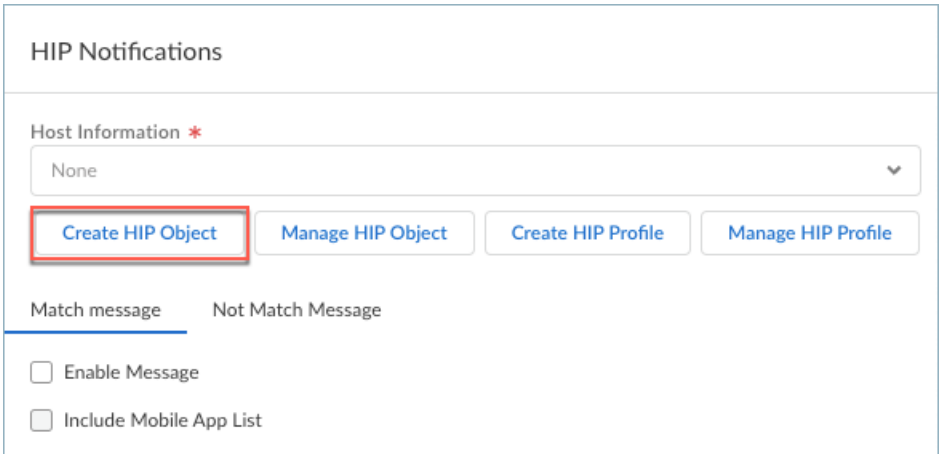
STEP 2 | Deberá **Edit (Editar)** la **Global Agent Settings (Configuración global del agente)**.



STEP 3 | Seleccione **HIP Notifications (Notificaciones HIP)** y haga clic en **Add (Añadir)**.



STEP 4 | Haga clic en **Create HIP Object (Crear objeto HIP)**.



STEP 5 | Introduzca un **Name (Nombre)** y una **Description (Descripción)** para el objeto.

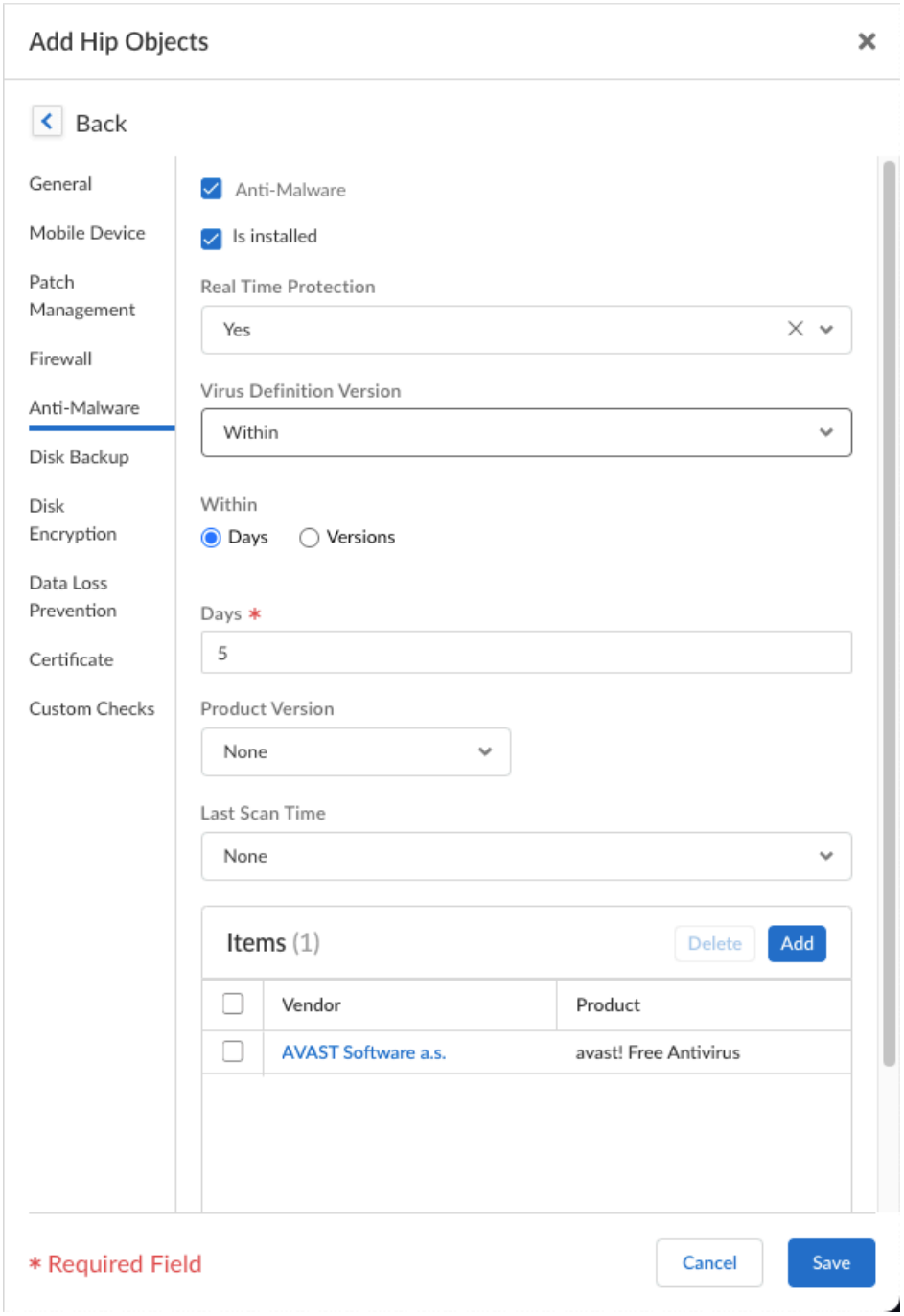
STEP 6 | Seleccione la pestaña que corresponde a la categoría de información del host que le interesa comparar y seleccione la casilla de verificación para habilitar la comparación del objeto con esta categoría.

Por ejemplo, para crear un objeto que busque información acerca de software antivirus o antispyware, seleccione la pestaña **Anti-Malware (Antimalware)** y, a continuación, seleccione la casilla de verificación **Anti-Malware (Antimalware)** para habilitar los campos

©2025 Palo Alto Networks, Inc.

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 malware en los 5 últimos días.



Repita este paso para cada categoría que quiera comparar con este objeto. Para obtener más información, consulte la Tabla: Categorías de recopilación de datos.

©2025 Palo Alto Networks, Inc.

STEP 7 | Deberá **Save (Guardar)** y **Add (Añadir)** su objeto HIP.

STEP 8 | Para gestionar los objetos HIP, puede seleccionar un objeto existente en la tabla de notificaciones HIP o hacer clic en **Añadir** en la página Editar configuración global del agente para abrir la ventana de notificaciones HIP.

Desde allí, haga clic en **Manage HIP Object (Gestionar objeto HIP)** para ver la lista de objetos HIP que configuró. Puede seleccionar un objeto HIP y **Delete (Eliminar)**, **Clone (Duplicar)** o **Move (Mover)**.

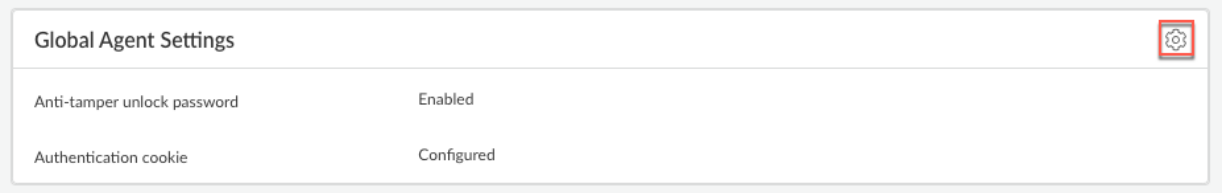
Crear y gestiona perfiles HIP para el acceso dinámico a privilegios de Prisma Access Agent

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia Prisma Access con la suscripción de usuario móvil ❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Rol: Superusuario

Un perfil HIP es una colección de objetos de perfiles de información de host (HIP) que deben evaluarse en conjunto para la supervisión o para la aplicación de políticas de seguridad. Cuando crea sus perfiles de HIP, puede combinar los objetos HIP y los perfiles HIP que haya creado previamente utilizando lógica booleana, de modo que cuando se evalúe un flujo de tráfico con el perfil de HIP resultante, este coincida o no. 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.

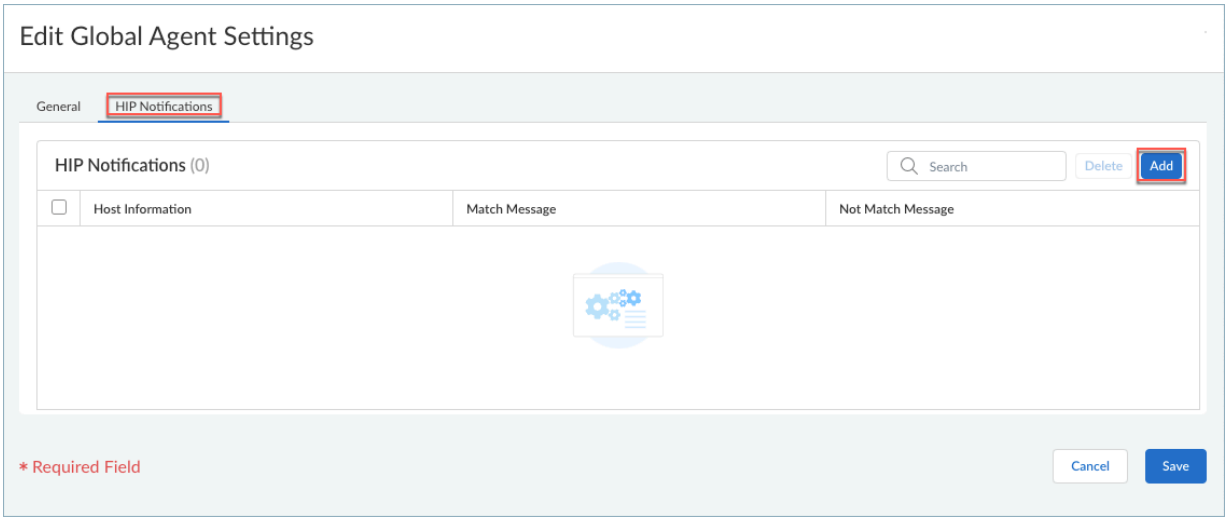
STEP 1 | Desde Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Access Agent (Agente de acceso)** > **Prisma Access Agent (Agente de Prisma Access)**.

STEP 2 | Deberá **Edit (Editar)** la **Global Agent Settings (Configuración global del agente)**.

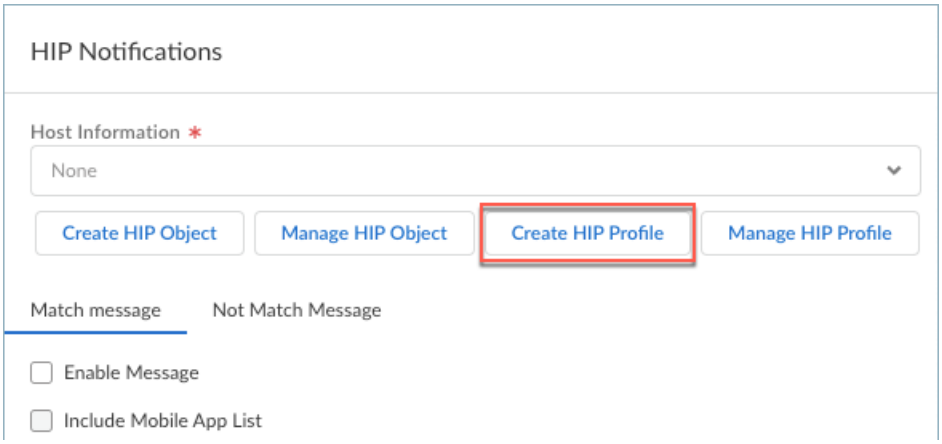


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Seleccione **HIP Notifications (Notificaciones HIP)** y haga clic en **Add (Añadir)**.



STEP 4 | Haga clic en **Create HIP Profile (Crear perfil de HIP)**.



STEP 5 | Introduzca un **Name (Nombre)** y una **Description (Descripción)** para identificar el perfil.

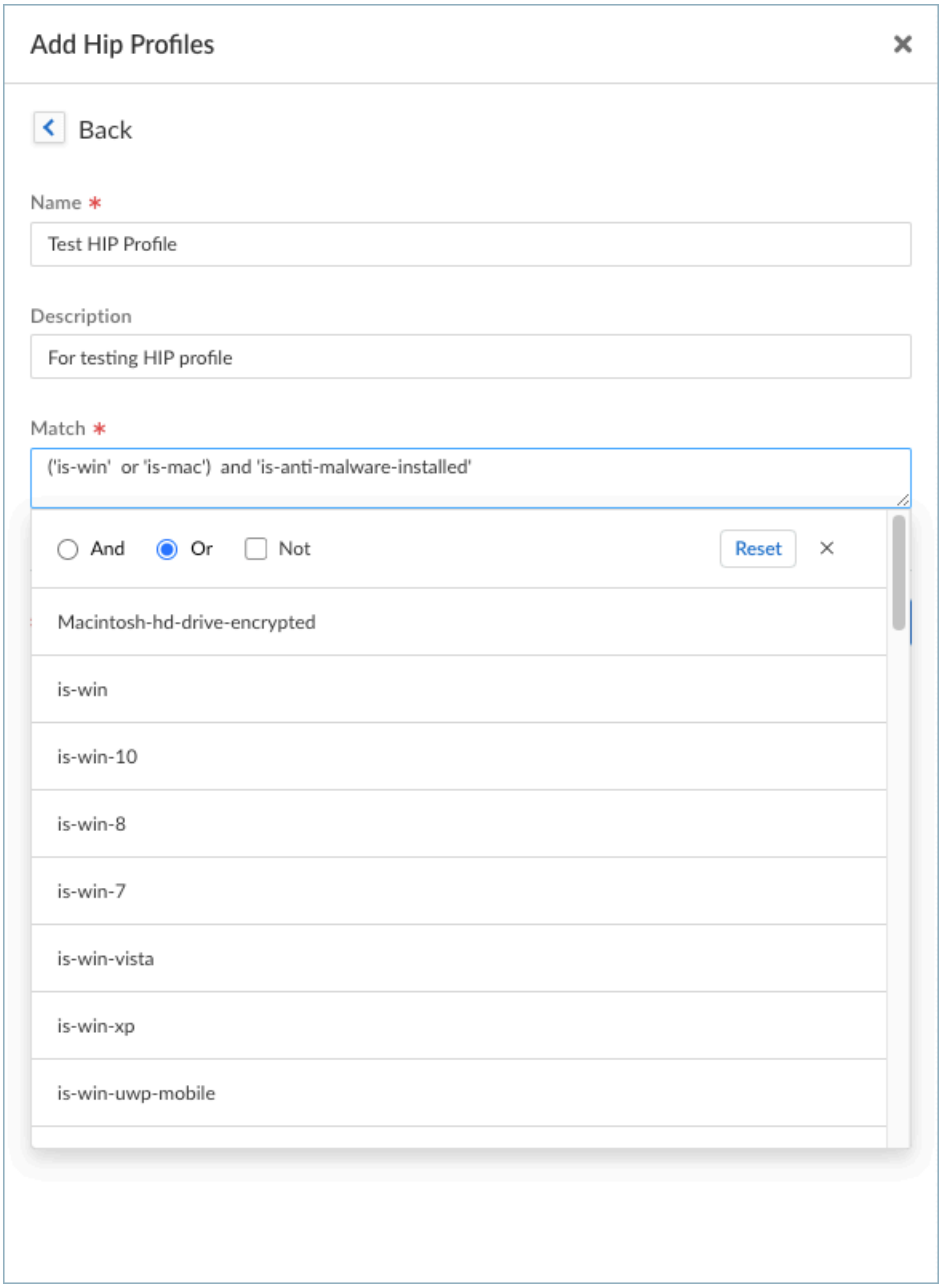
STEP 6 | Haga clic en el icono **Match (Coincidencia)** para abrir el generador de perfiles de HIP.

1. Seleccione el perfil u objeto HIP que desea utilizar como criterio de coincidencia de la lista.
2. Seleccione un operador booleano (**And**, **And**). 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.
3. Seleccione otro objeto o perfil HIP para evaluarlo con el primer objeto HIP.

STEP 7 | Continúe añadiendo criterios de coincidencia para el perfil que está creando. Para ello, seleccione el botón de opción del operador booleano apropiado (**And** o **And**) cada vez que añada un elemento y, de nuevo, use la casilla de verificación **NOT [NO]** cuando corresponda. El perfil HIP puede contener hasta 2.048 caracteres.

©2025 Palo Alto Networks, Inc.

STEP 8 | Cuando 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 usando la lógica que desea.



STEP 9 | Deberá **Save (Guardar)** y **Add (Añadir)** su perfil de HIP.

STEP 10 | Para gestionar sus perfiles de HIP, puede seleccionar un perfil existente en la tabla Notificaciones de HIP o hacer clic en **Add (Añadir)** en la página Editar configuración global del agente para abrir la ventana de Notificaciones de HIP.

Desde allí, haga clic en **Manage HIP Profile (Gestionar perfil de HIP)** para ver la lista de perfiles de HIP que ha configurado. Puede seleccionar un perfil de HIP y luego **Delete (Eliminar)**, **Clone (Duplicar)**o **Mover (Mover)** el perfil. También puede hacer lo siguiente: **Add (Añadir)** un perfil de HIP desde aquí.

 ©2025 Palo Alto Networks, Inc.

Envíe la configuración de Prisma Access Agent.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ Licencia Prisma Access con la suscripción de usuario móvil ☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Rol: Superusuario

Después de completar la configuración de Prisma Access Agent o actualizar la configuración, debe enviar la configuración a Prisma Access.

Cree al menos un proyecto antes de poder enviar la confirmación; de lo contrario, la confirmación fallará.

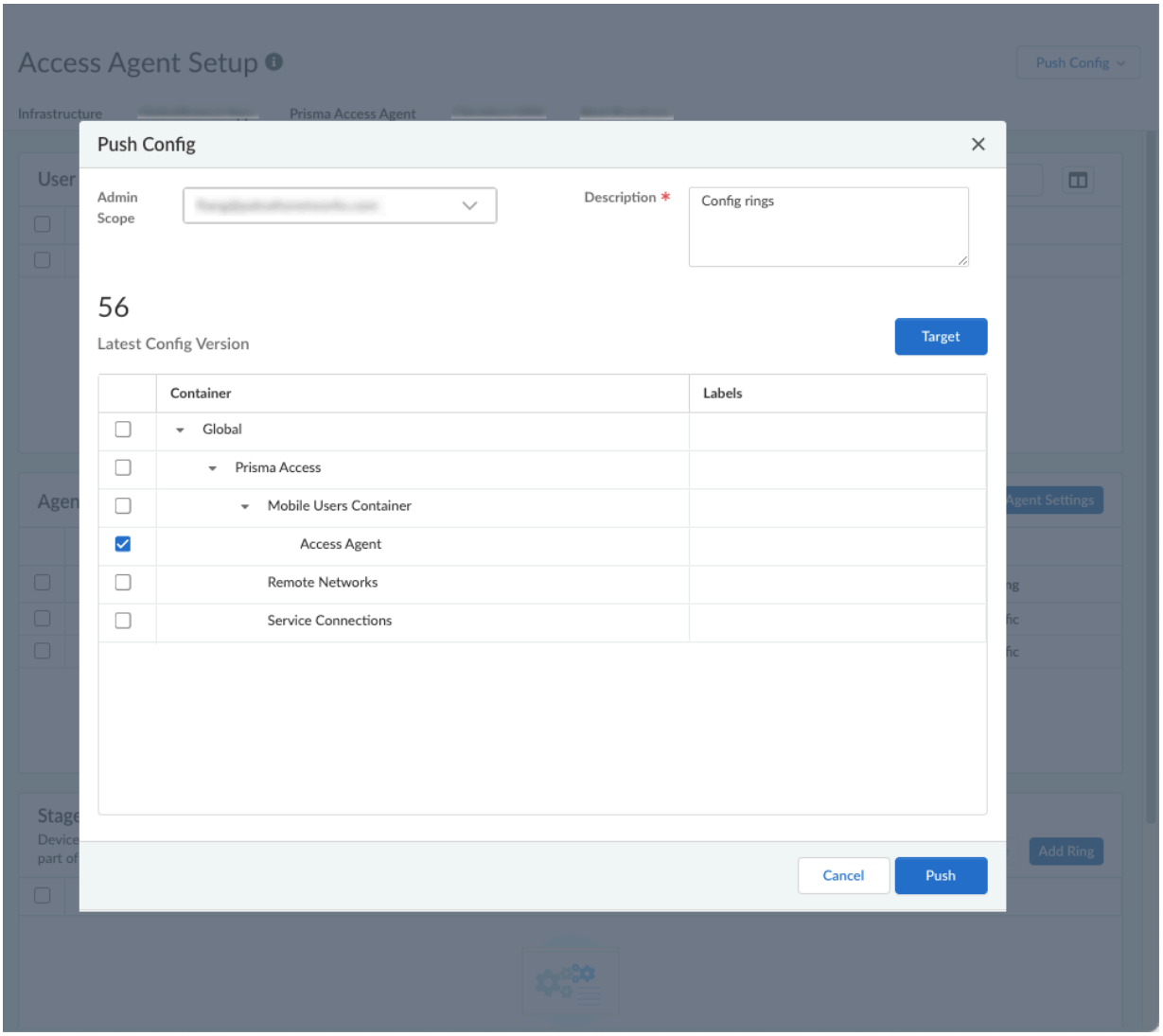
STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configurar Prisma Access)** > **Access Agent (Agente de Access)**.

STEP 2 | Seleccione **Push Config (Enviar configuración)** > **Push (Enviar)**.

STEP 3 | Introduzca una **Description (Descripción)** para la pila.

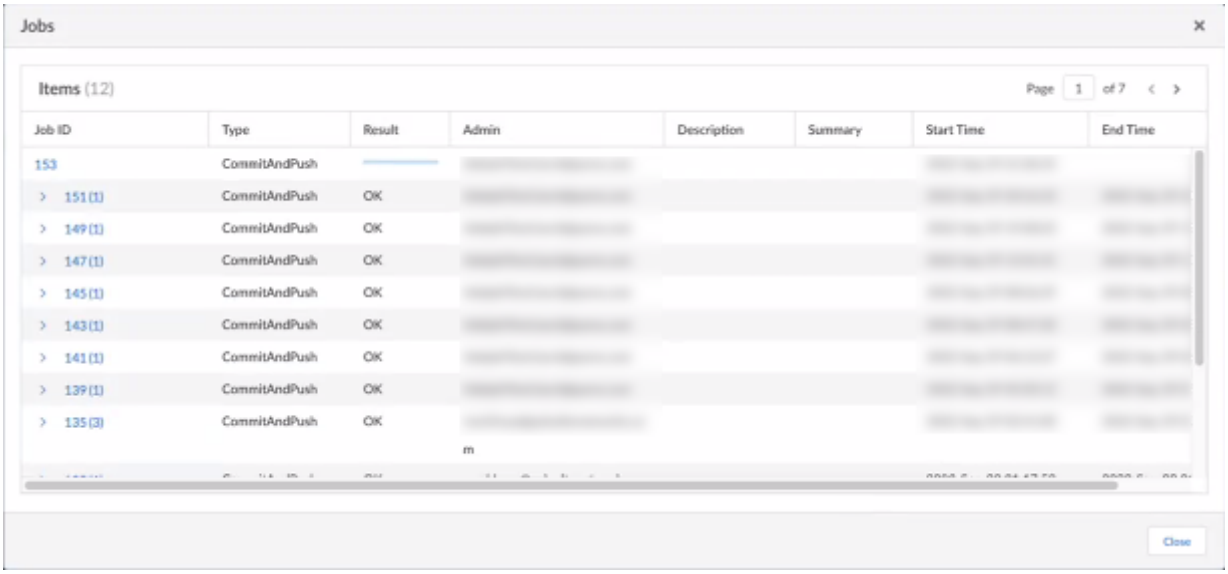
©2025 Palo Alto Networks, Inc.

STEP 4 | Seleccione el contenedor **Global** > **Prisma Access** > **Mobile Users (Usuarios móviles)** > **Access Agent (Agente de Access)** y haga clic en **Push (Enviar)**.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Espere a que finalice el trabajo y seleccione **Close (Cerrar)** el cuadro de diálogo de Tareas.



 ©2025 Palo Alto Networks, Inc.

Descargue el paquete de Prisma Access Agent habilitado por acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licencia de Prisma Access con la suscripción de usuario móvil ❑ Rol: Superusuario

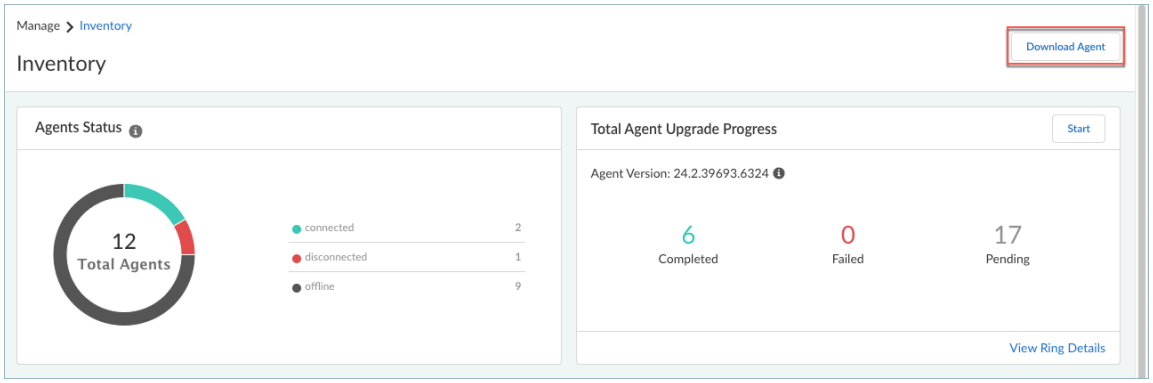
Después de haber configurado Prisma Access Agent y la configuración específica de proyecto de Prisma Access Agent, puede descargar el paquete de Prisma Access Agent para que pueda estar disponible para su descarga e instalación por parte de sus usuarios finales.

Además, asegúrese de descargar el archivo de configuración. Su agente y las configuraciones de agente específicas del proyecto, junto con el ID de inquilino de Prisma Access y el dominio del servidor, se guardan en el archivo de configuración de Prisma Access Agent. El archivo de configuración se utilizará durante la instalación y el registro del Prisma Access Agent.

©2025 Palo Alto Networks, Inc.

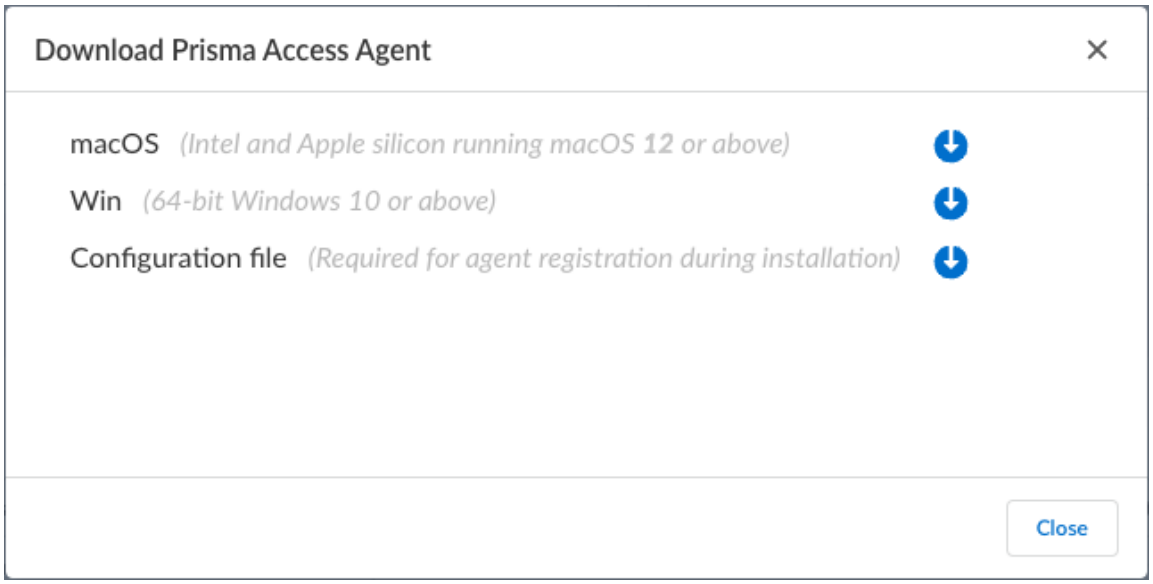
STEP 1 | Descargar el paquete y archivo de configuración de Prisma Access Agent.

1. Seleccione **Manage (Gestionar)** > **Prisma Access Agent** > **Inventory (Inventario)**.
2. Haga clic en el **Download Agent (Agente de descarga)**



3. Haga clic en la flecha hacia abajo correspondiente a los elementos que desea descargar.

   Asegúrese de descargar el **Configuration file (Archivo de configuración)** porque se utilizará durante la instalación y el registro del Prisma Access Agent.



4. Guarde el paquete en una ubicación de su sistema y elija **Close (Cerrar)** para cerrar el cuadro de diálogo Agente de descarga.

STEP 2 | Cargue el paquete en una ubicación central en la red de su organización o distribuya el paquete para que sus usuarios finales puedan descargar e instalar el Prisma Access Agent.

 ©2025 Palo Alto Networks, Inc.

Utilice el Prisma Access Agent para acceder a sus proyectos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Acceso a Internet

Si su organización es una empresa de TI o de servicios habilitados por TI (ITES) que necesita controlar qué usuarios tienen acceso a los proyectos de sus clientes, el acceso dinámico con privilegios proporciona una forma fluida, segura y compartimentada para que usted pueda acceder solo a aquellos proyectos que le están asignados.

Si su administrador ha configurado Prisma Access y el Prisma Access Agent para el Acceso dinámico a privilegios, puede utilizar el Prisma Access Agent para acceder y trabajar en los proyectos que le sean asignados.

Después de iniciar sesión en su proyecto, podrá acceder a la red de su organización, a los recursos de la red o a las aplicaciones de software como servicio que sean específicas del proyecto. Aprenda cómo:

- Iniciar sesión en el agente de Prisma Access habilitado con acceso dinámico a privilegios
- Ver el estado de su conexión
- Cambiar las preferencias del agente de Prisma Access habilitado con Acceso dinámico a privilegios
- Conectarse a una ubicación de Prisma Access diferente
- Ver notificaciones de la aplicación

Además, si se le asigna trabajar en diferentes proyectos, puede cambiar a un proyecto diferente o conectar el agente de Prisma Access a un servidor diferente.

Instalar el Prisma Access Agent.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 con privilegios de administrador ❑ Acceso a Internet

©2025 Palo Alto Networks, Inc.

Si su administrador no envió el Prisma Access Agent a su dispositivo, puede instalar manualmente el Prisma Access Agent en su dispositivo macOS o Windows.

> *El Prisma Access Agent y la aplicación GlobalProtect pueden coexistir en el mismo dispositivo, pero solo una de ellas puede conectarse a Prisma Access. Si la aplicación GlobalProtect también está instalada y habilitada en su dispositivo, la instalación de Prisma Access Agent deshabilitará automáticamente la aplicación GlobalProtect. Para utilizar la aplicación GlobalProtect después de instalar el Prisma Access Agent, necesitará* cambiar a la aplicación GlobalProtect.

- macOS
- Windows

Instalar el Prisma Access Agent (macOS)

Para instalar manualmente el Agente de Prisma Access en su dispositivo macOS:

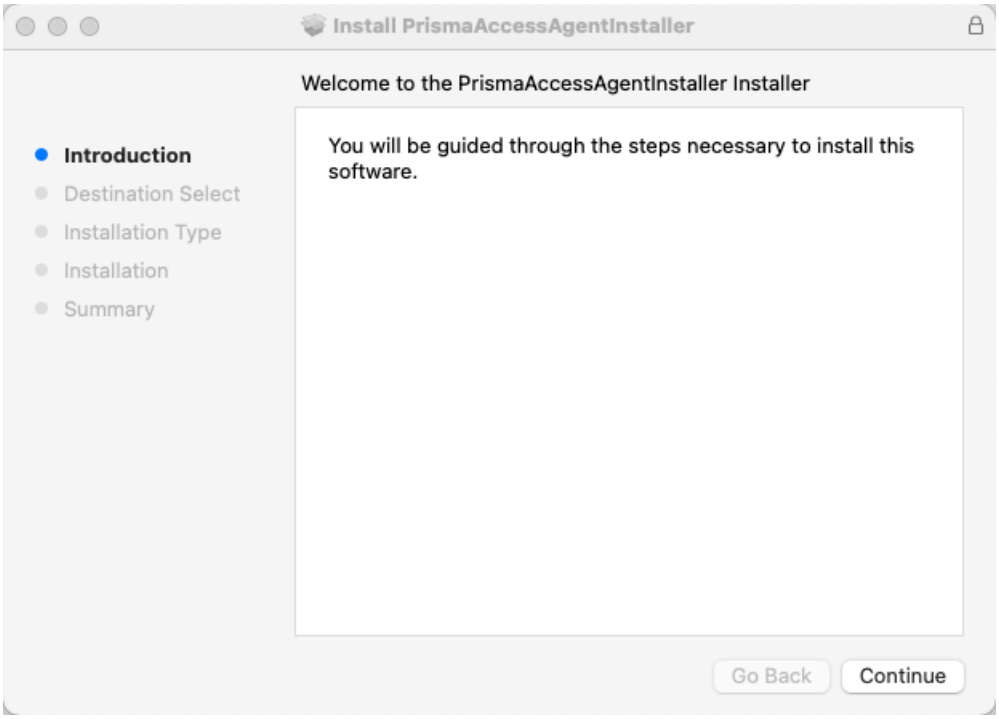
STEP 1 | Obtenga el paquete del Agente de Prisma Access que le proporcionó su administrador. El nombre del paquete tiene el siguiente formato:

`PrismaAccessAgentInstaller_<version>.Pkg`

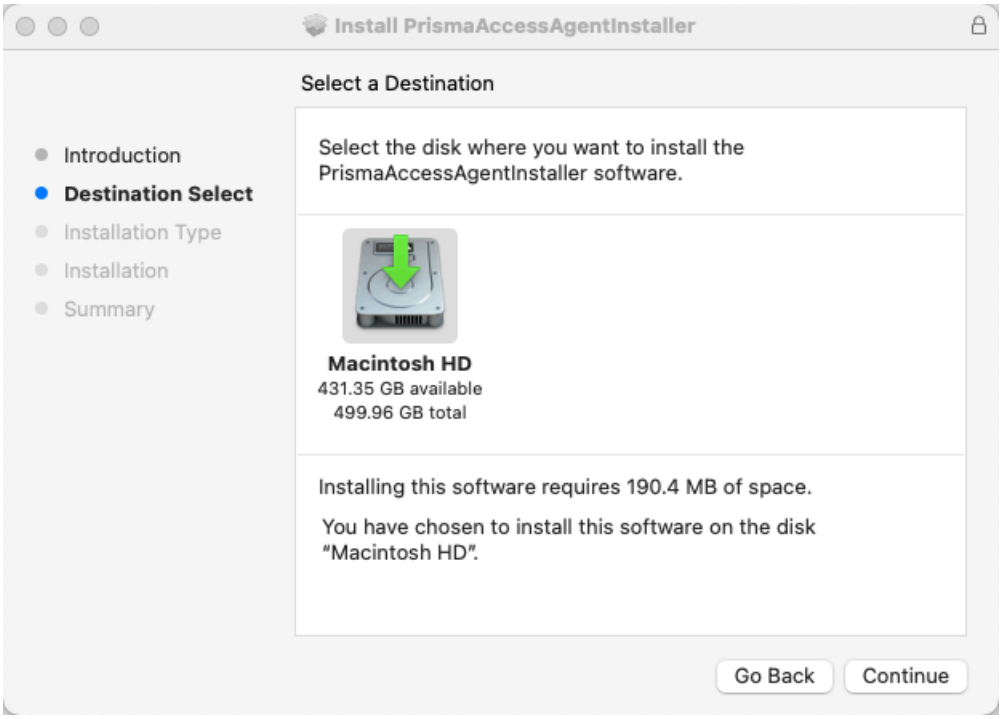
 ©2025 Palo Alto Networks, Inc.

STEP 2 | En la carpeta Descargas (o donde sea que haya colocado el paquete de instalación), abra el paquete de instalación y siga las instrucciones para instalar el Agente de Prisma Access.

1. En el instalador, haga clic en **Continue (Continuar).**

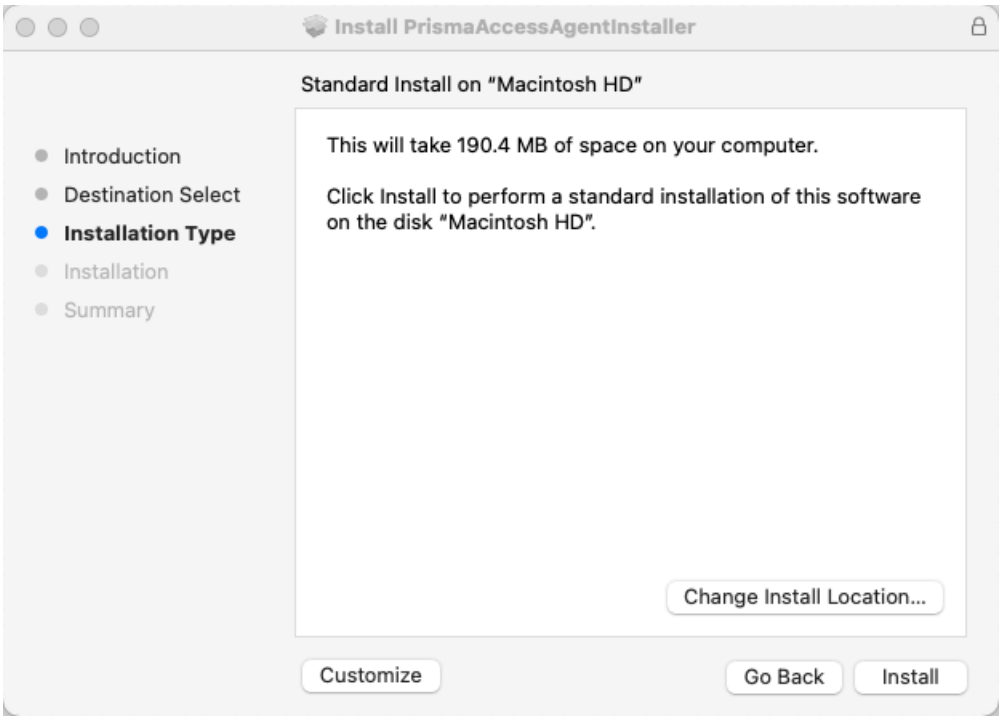


2. Seleccione la carpeta para la instalación de Agente de Prisma Access y haga clic en **Continue (Continuar)**.



3. Revise la información de la página Tipo de instalación y haga clic en **Install (Instalar)**.

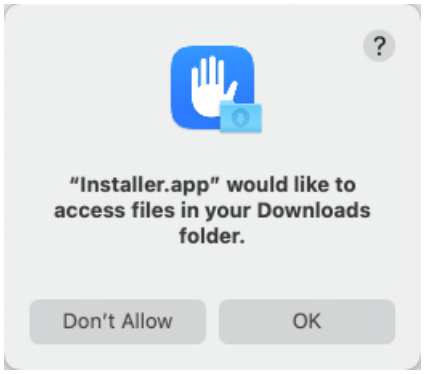
 ©2025 Palo Alto Networks, Inc.



4. Cuando se le solicite, introduzca su **User Name (Nombre de usuario)** y **Password (Contraseña)**y, a continuación, haga clic en **Install Software (Instalar software)** para comenzar la instalación.

   Como alternativa, puede usar Touch ID (si está habilitado) para completar este paso.

5. Cuando se le solicite que permita que el instalador acceda a los archivos de la carpeta donde descargó el paquete de instalación, haga clic en **OK (Aceptar)**.



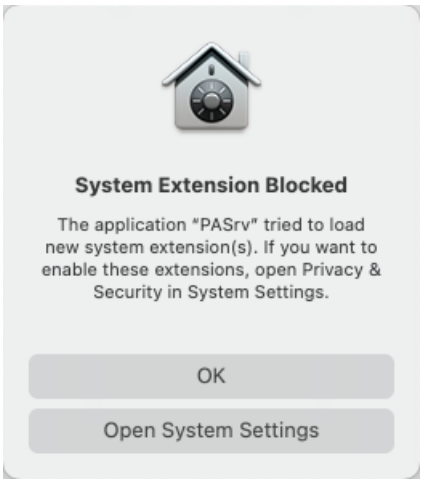
6. De forma predeterminada, macOS bloquea las extensiones del sistema del Agente de Prisma Access. Las extensiones del sistema o de la red aparecen si el administrador ha configurado el Agente de Prisma Access con reglas de reenvío de tráfico para:

   - Tunelización dividida: dirige el tráfico de red a través o fuera de la conexión de Prisma Access.
   - DNS dividido: dirige las consultas de DNS para aplicaciones y recursos a través de Prisma Access o fuera de Prisma Access, además del tráfico de red.

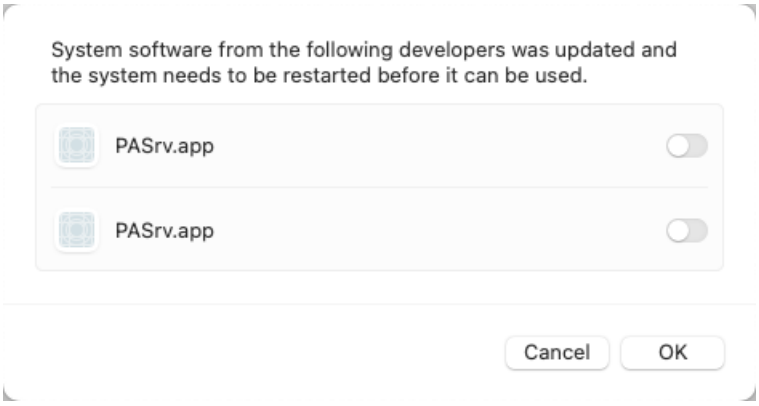
   Para que el Agente de Prisma Access funcione, debe habilitar las extensiones del sistema:

   1. Haga clic en **Open System Settings (Abrir configuración del sistema)**.

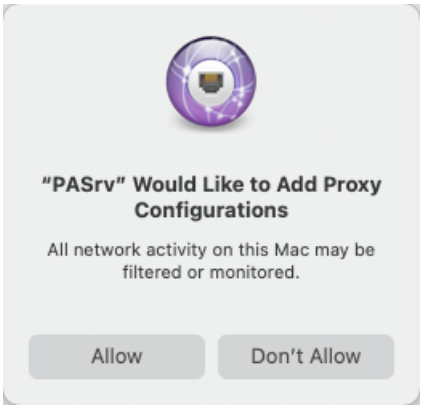
 ©2025 Palo Alto Networks, Inc.



2. En la ventana Privacidad y seguridad, haga clic en **Details (Detalles)** para **Some system software requires your attention before it can be used. (Algunos programas del sistema requieren su atención antes de poder utilizarlos.**
3. Habilite ambos aplicaciones de **PASrv.app** y haga clic en **OK (Aceptar)**.



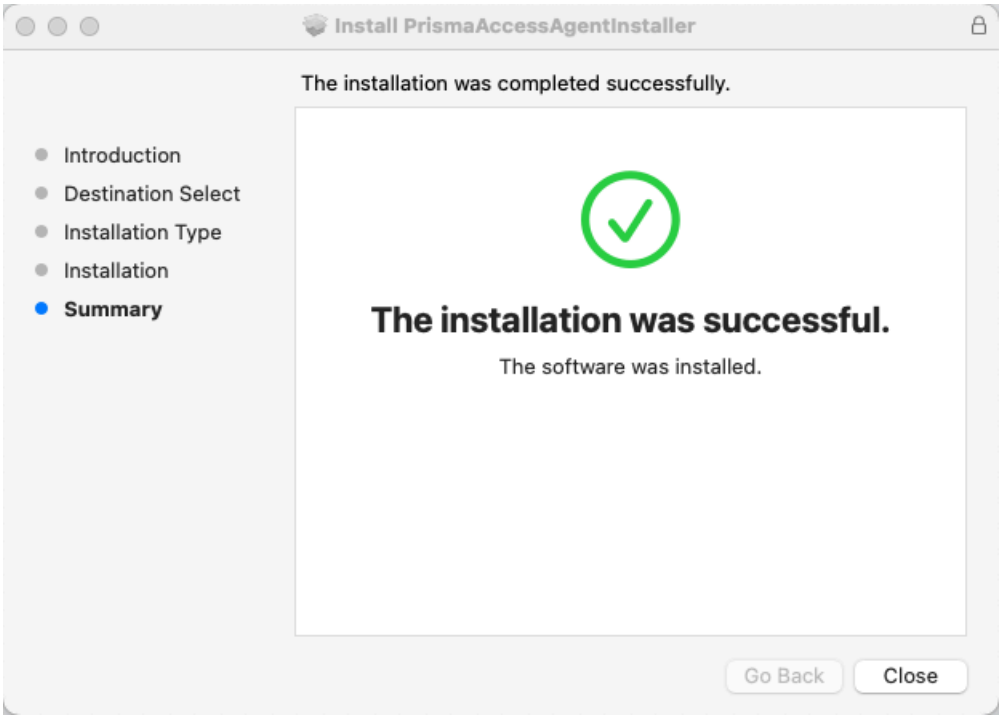
7. Si su administrador habilitó la función para aplicar conexiones de Prisma Access para el acceso a la red, se le pedirá que añada una configuración para filtrar el contenido de la red. Para continuar, haga clic en **Allow (Permitir)**.



Al hacer esto, sus conexiones de red se filtrarán y supervisarán por motivos de seguridad.

 ©2025 Palo Alto Networks, Inc.

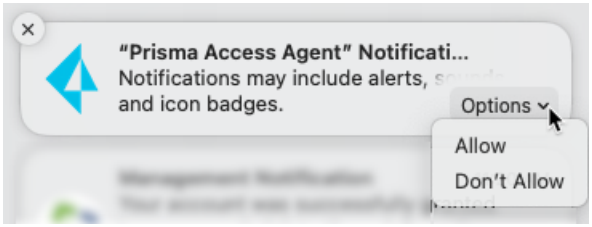
8. Cuando la instalación se haya completado, haga clic en **Close (Cerrar)** para cerrar el asistente de instalación.



9. Si el administrador configuró el agente para instalar el agente de Autonomous DEM junto con el Agente de Prisma Access, haga clic en **OK (Aceptar)** para que no se le vuelva a preguntar.
10. Haga clic en la ventana emergente Notificaciones del Agente de Prisma Access para abrir la ventana de preferencias de notificaciones.

STEP 3 | Si se le solicita, habilite las notificaciones de Agente de Prisma Access.

Cuando aparezca la ventana emergente de notificaciones de Agente de Prisma Access en su escritorio, pase el cursor sobre la ventana emergente y seleccione **Options (Opciones)** > **Allow (Permitir)**.

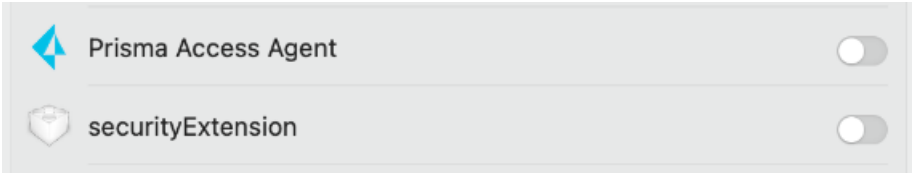


STEP 4 | Para que el Agente de Prisma Access acceda a los datos en el navegador Safari, debe otorgar acceso completo al disco a la Extensión de seguridad y al Agente de Prisma Access.

1. En macOS, seleccione **System Settings (Configuración del sistema)** > **Privacy & Security (Privacidad y seguridad)** > **Full Disk Access (Acceso completo al disco)**. Habilite **Prisma**

 ©2025 Palo Alto Networks, Inc.

Access Agent (Agente de Prisma Access) y **securityExtension (Extensión de seguridad)** de la lista de aplicaciones.



2. Cuando se le solicite, deberá **Quit & Reopen (Salir y volver a abrir)** el Agente de Prisma Access para que los cambios surtan efecto.

Instalar el Prisma Access Agent (Windows)

Para instalar manualmente el Agente de Prisma Access en su dispositivo Windows.

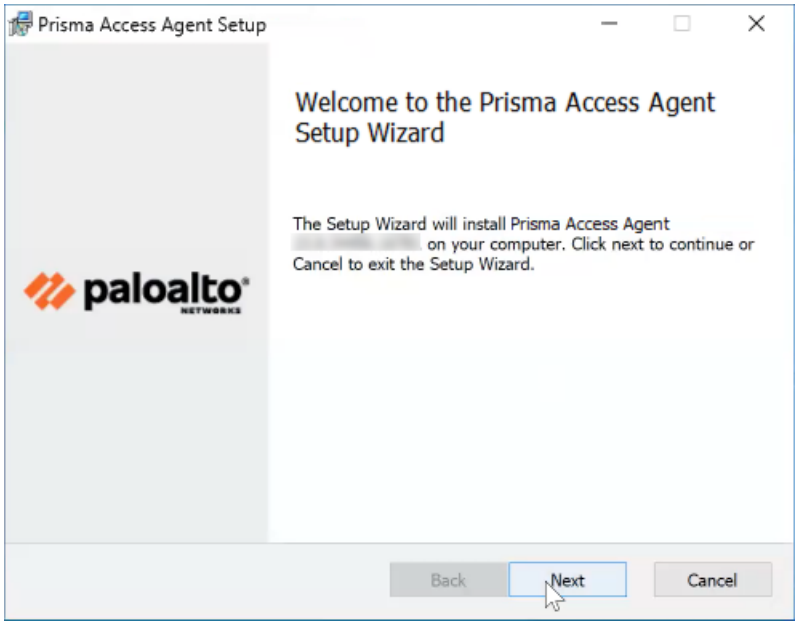
STEP 1 | Obtenga el paquete del Agente de Prisma Access que le proporcionó su administrador. El nombre del paquete tiene el siguiente formato:

`PrismaAccessAgent_x64_<version>.msi`

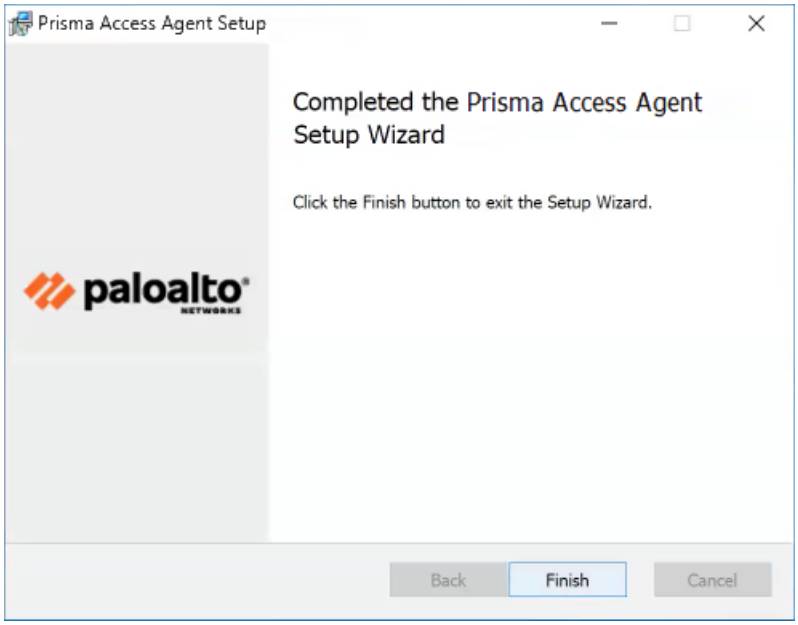
 ©2025 Palo Alto Networks, Inc.

STEP 2 | En la carpeta Descargas (o donde sea que haya colocado el paquete de instalación), haga doble clic en el icono del paquete de instalación y siga las instrucciones para instalar el Agente de Prisma Access.

1. Cuando aparezca el asistente de configuración, haga clic en **Next (Siguiente)** para continuar.



2. Revise el contrato de licencia de usuario final, seleccione **I accept the terms in the License Agreement (Acepto los términos del contrato de licencia)** y haga clic en **Next (Siguiente)**.
3. Haga clic en **Install (Instalar)** para iniciar la instalación.
4. Cuando se le solicite que **allow this app to make changes to your device (permita que esta aplicación realice cambios en su dispositivo)**, haga clic en **Yes (Sí)**.
5. Cuando se complete la instalación, haga clic en **Finish (Finalizar)**.



 ©2025 Palo Alto Networks, Inc.

6. Si el administrador configuró el agente para instalar el agente de Autonomous DEM junto con el Agente de Prisma Access, haga clic en **OK (Aceptar)** para que no se le vuelva a preguntar.

Inicie sesión en Prisma Access Agent habilitado por acceso dinámico a privilegios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Acceso a Internet

Para acceder a la red, los recursos, las aplicaciones SaaS o Internet de su organización, inicie sesión en el Agente de Prisma Access con sus credenciales de inicio de sesión.

Después de iniciar sesión en el Agente de Prisma Access, se conecta automáticamente a su red utilizando la mejor ubicación de Prisma Access (a veces llamada puerta de enlace). La mejor ubicación se elige automáticamente para proporcionarle el mejor rendimiento para permitir una mejor experiencia, como ver sitios web en su idioma local. Cuando su dispositivo se encuentra fuera de la red de su organización, el agente encuentra la mejor ubicación para ofrecerle el mejor rendimiento al conectarse a la red corporativa.

Antes de comenzar, el Agente de Prisma Access debe estar instalado en su dispositivo. Por lo general, el administrador implementará el Agente de Prisma Access en el dispositivo que utiliza para acceder a la red, los recursos y las aplicaciones de su organización. El agente está configurado de acuerdo con las reglas de políticas definidas por el administrador e implementadas en el dispositivo. Sin embargo, si su administrador no implementó el Agente de Prisma Access en su dispositivo, deberá instalarlo manualmente.

Dependiendo de cómo se configure Prisma Access en su organización, su administrador debe proporcionarle la siguiente información de inicio de sesión:

- El nombre del servidor de Prisma Access que aloja el servicio que gestiona su Prisma Access Agent. Puede haber varios servidores dependiendo de la configuración de Prisma Access.
- El nombre de los proyectos en los que trabaja si su organización utiliza el *Acceso dinámico a privilegios*. Acceso dinámico a privilegios le permite acceder a la red y los recursos de su organización en función del proyecto al que está asignado, de modo que no acceda accidentalmente a los recursos de otro proyecto. Si se le ha asignado a trabajar en más de un proyecto, puede cambiar de proyecto fácilmente.



Según la configuración de su sistema operativo, los iconos de la aplicación y la interfaz de usuario de la aplicación pueden aparecer en modo oscuro o en modo claro.

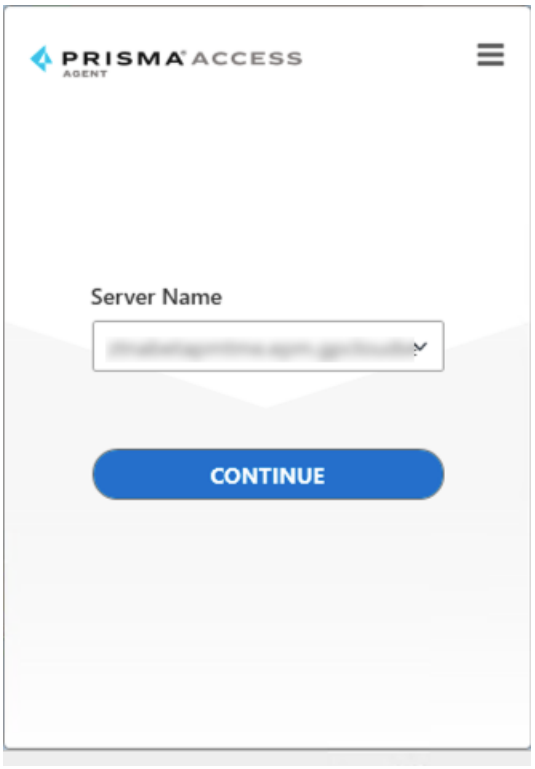
Inicie sesión en el Agente de Prisma Access siguiendo los siguientes pasos:

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Inicie el archivo el Prisma Access Agent haciendo clic en el icono Prisma Access Agent desde la barra de menús de macOS o la barra de tareas de Windows.

STEP 2 | Si se le solicita, introduzca o seleccione el **Server Name (Nombre del servidor)** para el servidor de Prisma Access que su administrador proporcionó y luego **Continue (Continuar)**.

El formato del nombre del servidor es **<example.domain.com>** sin el protocolo **https://**. La longitud máxima de un nombre de clúster es de 256 caracteres.



STEP 3 | Introduzca el nombre del proyecto que le envió su administrador y elija **Continue (Continuar)**.

La longitud máxima del nombre del proyecto es de 32 caracteres.

STEP 4 | En la página de inicio de sesión que aparece en el navegador web predeterminado, inicie sesión en la aplicación de inicio de sesión único (SSO) de su organización, como Okta o Azure Active Directory (AD), introduciendo sus credenciales de inicio de sesión para su organización.

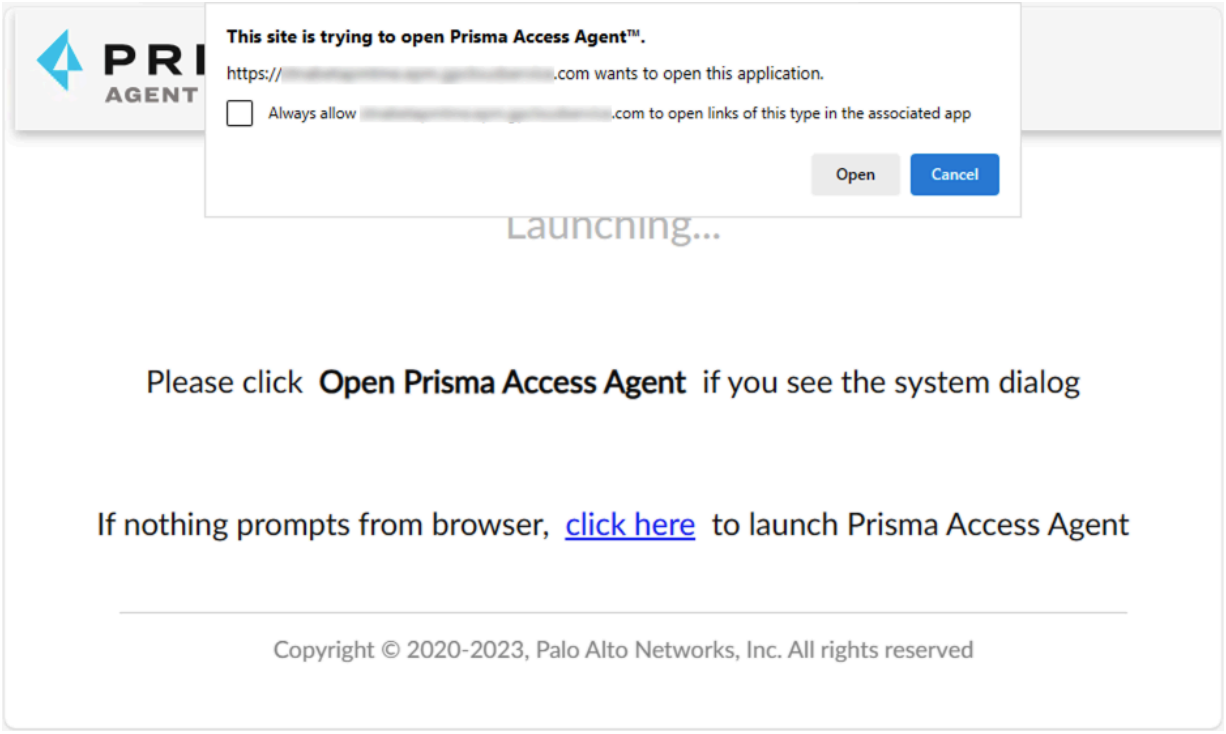
Si el administrador habilitó la autenticación multifactor (MFA), deberá completar la verificación adicional en el navegador cuando inicie sesión.

STEP 5 | Cuando su navegador web le solicite, haga clic en **Open (Abrir)**.

Si no desea que el navegador le solicite la próxima vez que inicie sesión, seleccione **Always allow (Permitir siempre que) <site> to open these types of links in the associated app (abra**

 ©2025 Palo Alto Networks, Inc.

este tipo de enlaces en la aplicación asociada) y, a continuación, haga clic en **Open (Abrir)** (si es compatible con su navegador web predeterminado).



STEP 6 | Espere mientras el Agente de Prisma Access se conecta a Prisma Access.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Después de iniciar sesión correctamente, se conecta automáticamente a la mejor ubicación de Prisma Access disponible. Si inició sesión con un proyecto, está conectado a la mejor ubicación disponible para su proyecto.

Ahora puede acceder a los recursos de su organización y a las aplicaciones SaaS, junto con un acceso seguro a Internet.

*Si el administrador habilitó el modo **Always On (Siempre activado)** para Prisma Access Agent, no puede desconectarse de Prisma Access debido a la política de su organización. Sin embargo, todavía puede cambiar las ubicaciones de Prisma Access.*

*Si el administrador habilitó el modo **On Demand (Bajo demanda)** para Prisma Access Agent, debe hacer clic en el icono de candado para conectarse a Prisma Access.*

Cambiar las preferencias para el acceso privilegiado dinámicamente habilitado de Prisma Access Agent

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Acceso a Internet

Utilice la ventana de preferencias de Prisma Access Agent para ver información sobre su dispositivo y cambiar opciones para su agente, como por ejemplo habilitar notificaciones de escritorio.

STEP 1 | Inicie el archivo el Prisma Access Agent haciendo clic en el icono Prisma Access Agent desde la barra de menús de macOS o la barra de tareas de Windows.

STEP 2 | Haga clic en el menú de tres barras para abrir la ventana de preferencias.

STEP 3 | En la ventana de preferencias, puede ver la siguiente información:

Icono	Descripción
	Su ID de usuario.
	La ubicación de Prisma Access a la que está conectado el dispositivo.
	La dirección IP de la ubicación de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Icono	Descripción
	El nombre de host o la dirección IP de la interfaz administrativa (servidor) a la que está conectado. Puede hacer clic en el botón más (+) para conectarse a un servidor diferente.
	El proyecto en el que ha iniciado sesión.

STEP 4 | Para recibir notificaciones de Prisma Access Agent en la barra de menú (en macOS) o en la barra de tareas (en Windows), seleccione **Allow desktop notifications (Permitir notificaciones de escritorio)**. Este parámetro está habilitado de forma predeterminada.

Las notificaciones de escritorio se adherirán a cualquier configuración de no molestar que establezca en el momento de la instalación. El sistema operativo le pedirá que permita las notificaciones de Prisma Access Agent en el momento de la instalación.

STEP 5 | Para comprender qué datos Prisma Access Agent recopila y cómo se utiliza la información, consulte **Our Privacy Policy (Nuestra política de privacidad)**.

STEP 6 | Haga clic en para obtener asistencia sobre los problemas que pueda encontrar con el Prisma Access Agent, haga clic en **Support Resources (Recursos de apoyo)**.

STEP 7 | Si su administrador lo permite, puede **Sign Out (Cerrar sesión)** de Prisma Access Agent.

STEP 8 | Si el administrador habilitó la función, puede **Disable (Deshabilitar)** el Prisma Access Agent para que pueda cambiar a la aplicación GlobalProtect (si está instalado en su dispositivo).

STEP 9 | Ver la versión de su Prisma Access Agent.

STEP 10 | Para cerrar la ventana, haga clic en el botón **X**.

Conecte el Prisma Access Agent habilitado por el Acceso dinámico a privilegios a una Ubicación diferente

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Acceso a Internet

Después de iniciar sesión en Prisma Access Agent, está automáticamente conectado a la mejor ubicación disponible de Prisma Access. Si desea cambiar de ubicación, puede hacerlo utilizando el menú desplegable **Location (Ubicación)**.

STEP 1 | Inicie el archivo el Prisma Access Agent haciendo clic en el icono Prisma Access Agent desde la barra de menús de macOS o la barra de tareas de Windows.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione una **Location (Ubicación)** diferente. Puede **Search (Buscar)** una ubicación o elegir una ubicación de la lista.

La lista de ubicaciones disponibles se ordena según la mejor experiencia en función del tiempo de respuesta, la disponibilidad y otros factores. La ubicación que ofrece la mejor experiencia se enumera como **Best Location (Mejor ubicación)**.

STEP 3 | Si su administrador habilitó el modo **On Demand (Bajo demanda)** para el Prisma Access Agent, haga clic en el icono de candado para conectarse a la nueva ubicación seleccionada. De lo contrario, Prisma Access Agent procede a cambiar de ubicación.

Cambiar a un inquilino diferente

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	❑ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ❑ Acceso a Internet

Si está asignado a varios proyectos en su organización, puede cambiar a otro proyecto para acceder a la red y los recursos asociados con ese proyecto.

Si el proyecto al que intenta cambiar es accesible desde un servidor diferente, primero deberá cambiar a ese servidor.

STEP 1 | Inicie el Prisma Access Agent haciendo clic en el icono Prisma Access Agent desde la barra de menú macOS y la barra de tareas de Windows.

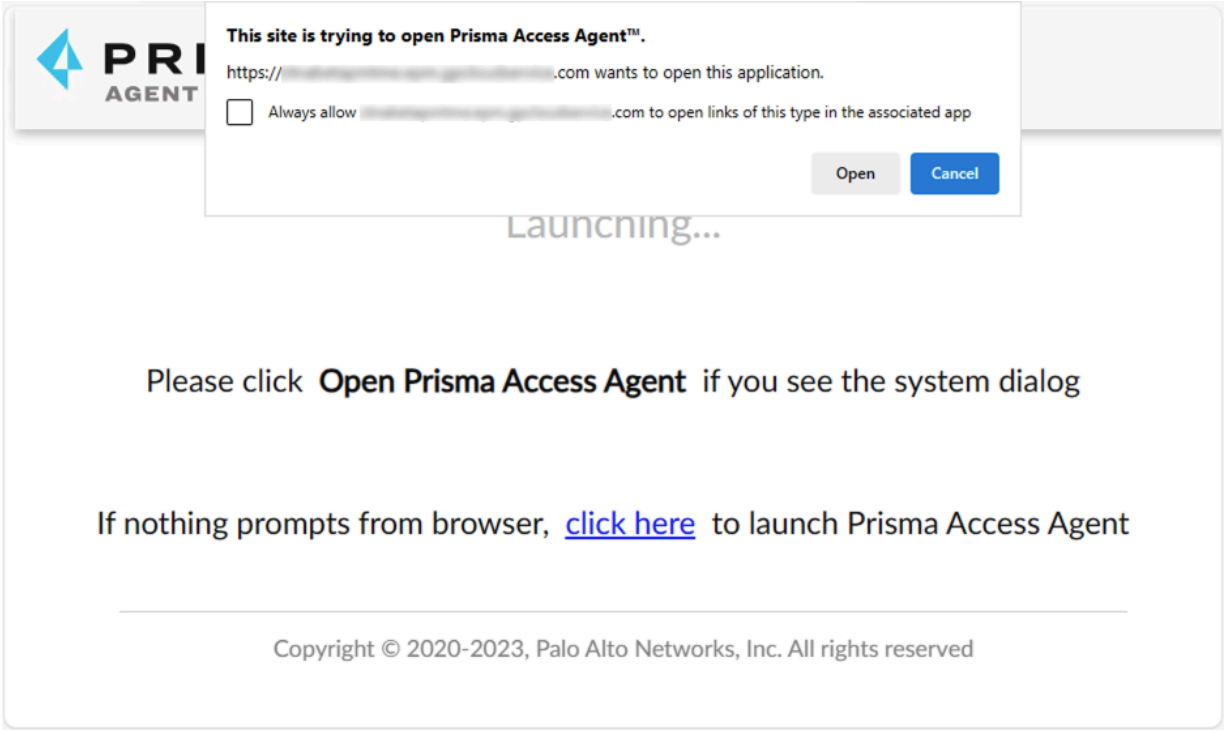
STEP 2 | Seleccione un **Project (Proyecto)** diferente. Puede **Search (Buscar)** una ubicación o elegir una ubicación de la lista.

Debe estar asignado al proyecto al que está cambiando.

STEP 3 | Si su administrador habilitó el modo **On Demand (Bajo demanda)** para el Prisma Access Agent, haga clic en el icono de candado para cambiar de proyecto. De lo contrario, Prisma Access Agent procede a cambiar de proyectos.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Cada vez que cambia de proyecto, Prisma Access Agent se desconecta del proyecto actual y se conecta al proyecto recién seleccionado. Es posible que se le solicite que **Abra** el Prisma Access Agent de nuevo.



Conecte el Prisma Access Agent habilitado por el Acceso dinámico a privilegios a un servidor diferente

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Acceso a Internet

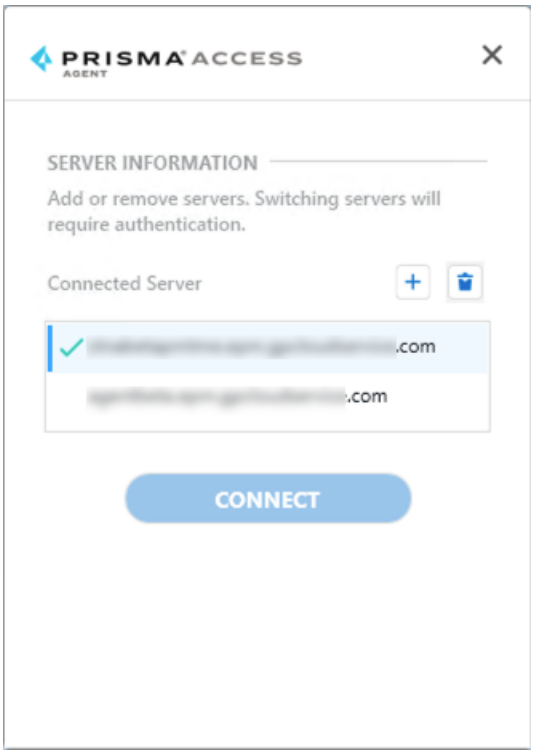
Una instancia del servidor Prisma Access también se conoce como *inquilino*. Si sus administradores configuran varios servidores de Prisma Access, puede conectarse a un servidor diferente para acceder a la red o a los recursos a través de dicho servidor.

Por ejemplo, necesita trabajar en un proyecto diferente, pero solo se puede acceder a ese proyecto en un servidor diferente. Deberá conectarse a ese servidor antes de poder cambiar a ese proyecto.

STEP 1 | Inicie el archivo el Prisma Access Agent haciendo clic en el icono Prisma Access Agent desde la barra de menús de macOS o la barra de tareas de Windows.

STEP 2 | Edite la configuración del servidor seleccionando el icono de gestión del servidor.

STEP 3 | La ventana de información del servidor muestra el servidor al que está conectado. Si otros servidores se enumeran, puede seleccionar uno y luego **Connect (Conectar)**.

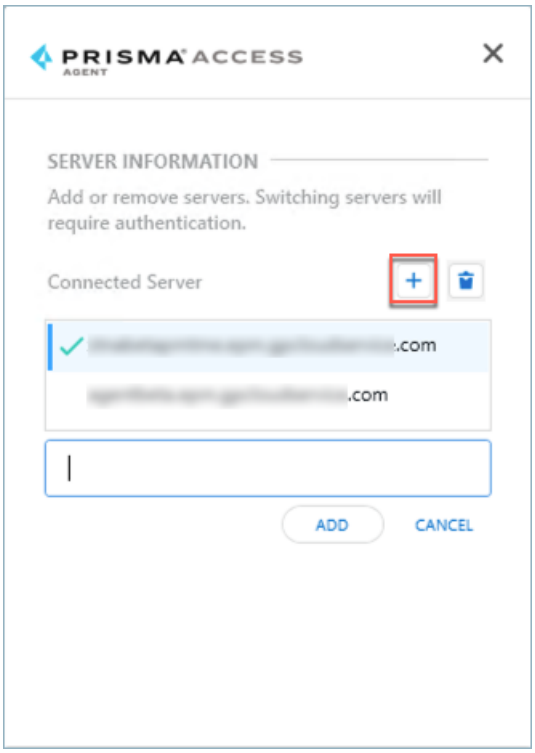


 ©2025 Palo Alto Networks, Inc.

STEP 4 | Si necesita añadir un servidor, complete los siguientes pasos:

1. Haga clic en el signo **+**.
2. Introduzca el nuevo nombre del servidor (proporcionado por su administrador) y luego **Add (Añadir)**.

   El formato del nombre del servidor es **<example.domain.com>** sin **https://**. La longitud máxima de un nombre de clúster es de 256 caracteres. El número máximo de servidores permitidos en esta página es 20.



3. Después de añadir el servidor, selecciónelo y haga clic en **Connect (Conectar)**.

STEP 5 | Cuando aparezca la ventana Confirmación, haga clic en **Yes (Sí)** para desconectarse del servidor actual y conectarse al otro servidor. Tendrá que proporcionar sus credenciales de inicio de sesión único de nuevo.

STEP 6 | Cuando se le solicite, inicie sesión en el nuevo servidor proporcionando el nombre del proyecto (si corresponde).

Cambie entre Prisma Access Agent y la aplicación GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access Agent	☐ Dispositivos de escritorio macOS 12 o posteriores o Windows 10 versión 2024 o posterior, o dispositivos de escritorio con Windows 11 ☐ Acceso a Internet

 ©2025 Palo Alto Networks, Inc.

En algunas organizaciones, el Prisma Access Agent se instala en dispositivos de usuario que ya tienen instalada la aplicación GlobalProtect. Después de instalar el Prisma Access Agent, puede cambiar entre el Prisma Access Agent y la aplicación GlobalProtect según sea necesario.

Después de cambiar a la aplicación GlobalProtect, el agente de Prisma Access está en el estado deshabilitado. En el estado deshabilitado:

- Todo el tráfico a las ubicaciones de Prisma Access está deshabilitado y la autenticación multifactor (MFA) está deshabilitada.

  Tanto el agente de Prisma Access como GlobalProtect utilizan el mismo puerto GlobalProtect para escuchar solicitudes MFA (para autenticación adicional para ciertas aplicaciones), pero solo un agente puede utilizar el puerto a la vez. Cuando deshabilite el agente de Prisma Access, el puerto se liberará para su uso por GlobalProtect.
- La comunicación con el servidor persiste para que el agente pueda continuar recibiendo actualizaciones de implementación por etapas, notificaciones ADEM, solicitudes de shell remotas del administrador y realizar comprobaciones HIP.
- Si está configurada por el administrador, la función antimanipulación continuará funcionando para proteger al agente de manipulaciones no autorizadas.
- En los dispositivos macOS, el sistema y las extensiones de red para el agente de Prisma Access continuarán activos, y el filtro de contenido también continuará activo.
- Si cambia a otro servidor, el agente de Prisma Access se volverá a habilitar automáticamente. Si intenta conectarse a una ubicación de Prisma Access mientras el agente está deshabilitado, el agente se conectará a la mejor ubicación.

Puede utilizar la aplicación Prisma Access Agent o la herramienta de línea de comandos Prisma Access (PACli) para cambiar entre las dos aplicaciones.

- Aplicación de agente de Prisma Access
- Línea de comandos Prisma Access (PACli)

Cambiar entre el Prisma Access Agent y la aplicación GlobalProtect (mediante la aplicación de agente de Prisma Access)

Cambie entre Prisma Access Agent y la aplicación GlobalProtect (utilizando la herramienta PACli)

 ©2025 Palo Alto Networks, Inc.

Ver y supervisar usuarios con acceso dinámico a privilegios

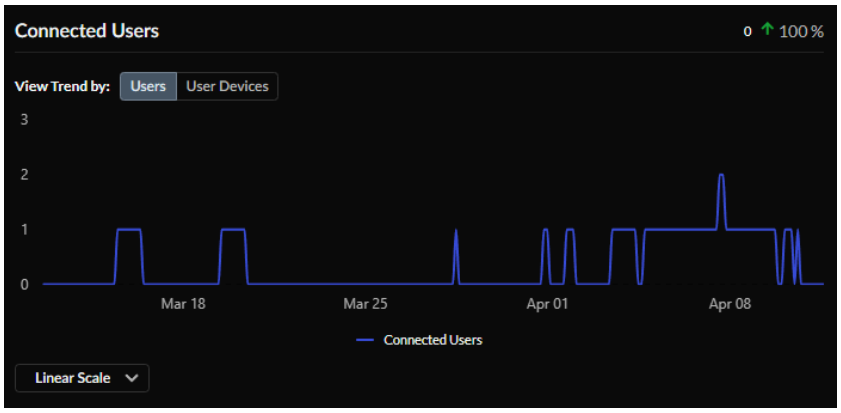
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

El acceso dinámico con privilegios permite que Prisma Access aplique diferentes reglas de políticas de seguridad y de red a los flujos de usuarios móviles en función del proyecto en el que estén trabajando sus usuarios. Vaya a **Insights** > **Users (Usuarios)** en el Centro de control de Strata Cloud Manager para ver la información de acceso basada en usuarios en su entorno.

Usuarios conectados

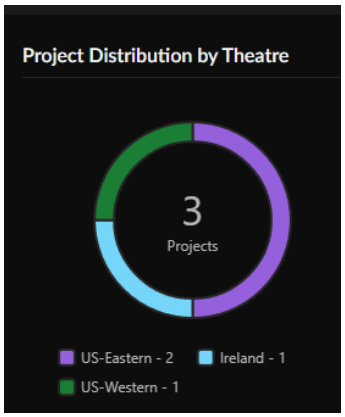
Vea los **Connected Users (Usuarios conectados)** para ver los usuarios conectados actuales o los dispositivos de usuarios conectados. La flecha Arriba o Abajo compara este intervalo de tiempo con un intervalo de tiempo anterior para determinar la diferencia, en porcentaje, del número de dispositivos conectados.

Seleccione **View Trend by Users (Ver tendencia por usuarios)** para ver la cantidad de usuarios actualmente conectados al agente de Prisma Access, y haga clic en **View Trend by User Devices (Ver tendencia por dispositivos de usuario)** para ver la cantidad de dispositivos de usuario actualmente conectados al agente de Prisma Access.

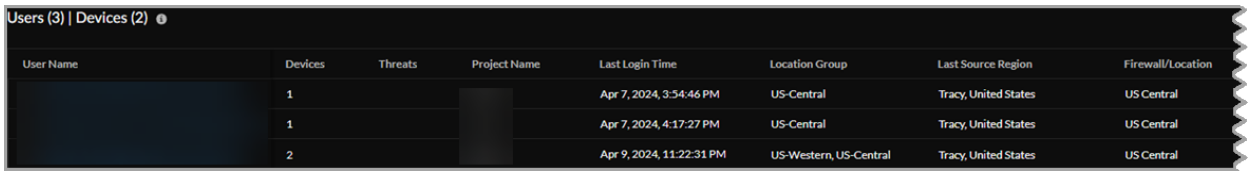


Vea **Project Distribution by Theatre (Distribución de Proyectos por teatro)** para ver la cantidad de proyectos por ubicación o teatro.

 ©2025 Palo Alto Networks, Inc.



La tabla **Usuarios | Dispositivos** muestra el **Project Name (Nombre del proyecto)** asociado con cada usuario y dispositivo. También puede ver cuántos dispositivos están conectados por usuario, la última hora de inicio de sesión, la última ubicación de origen, la última ubicación de Prisma Access conectada, el protocolo de Internet de origen y la familia y versión del sistema operativo.

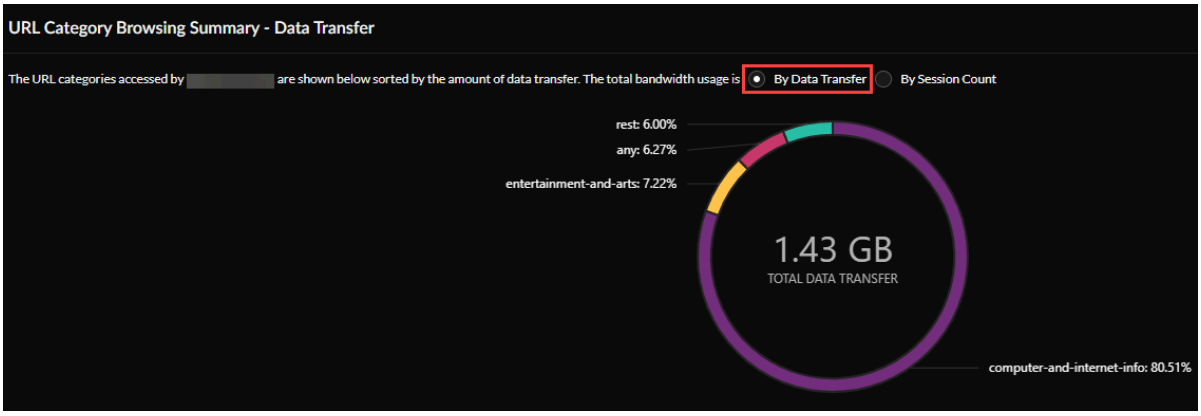


Seleccione cualquier **Project Name (Nombre de proyecto)** para ir a la página **Projects (Proyectos)**.

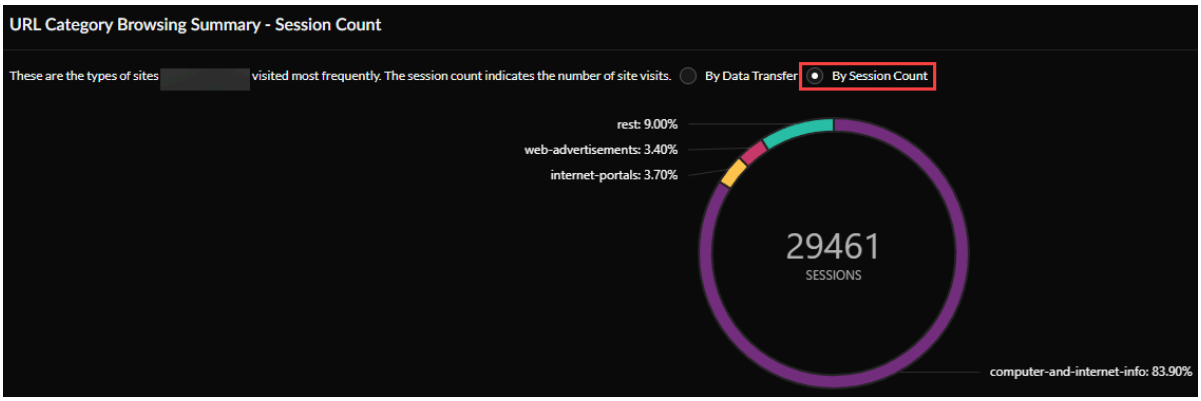
Seleccione cualquier **User Name (Nombre de usuario)** para ver los detalles del usuario, como **Activity (Actividad)** y **Connectivity (Conectividad)**.

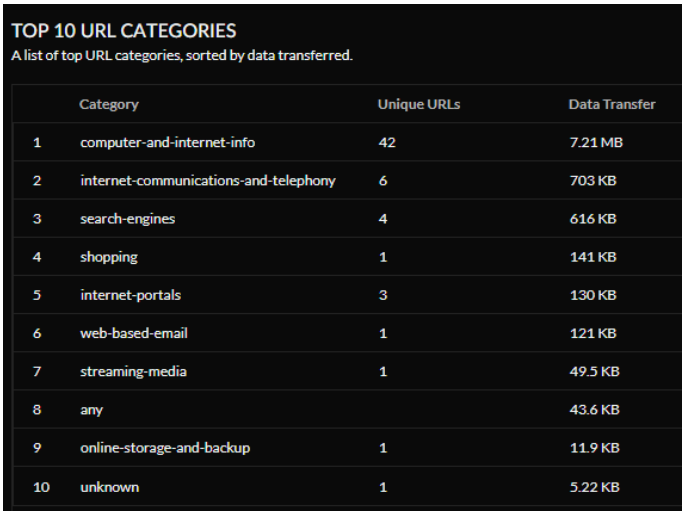
Actividad

URL Browsing Category Summary- Data Transfer (Resumen de categoría de navegación de URL: Transferencia de datos): vea el resumen de transferencia de datos de su categoría de navegación **By Data Transfer (Por transferencia de datos)** o **By Session Count (Por recuento de sesiones)**. También puede ver una lista de las **Top 10 URL Categories((10 principales categorías de URL)**, ordenadas por los datos transferidos.



 ©2025 Palo Alto Networks, Inc.





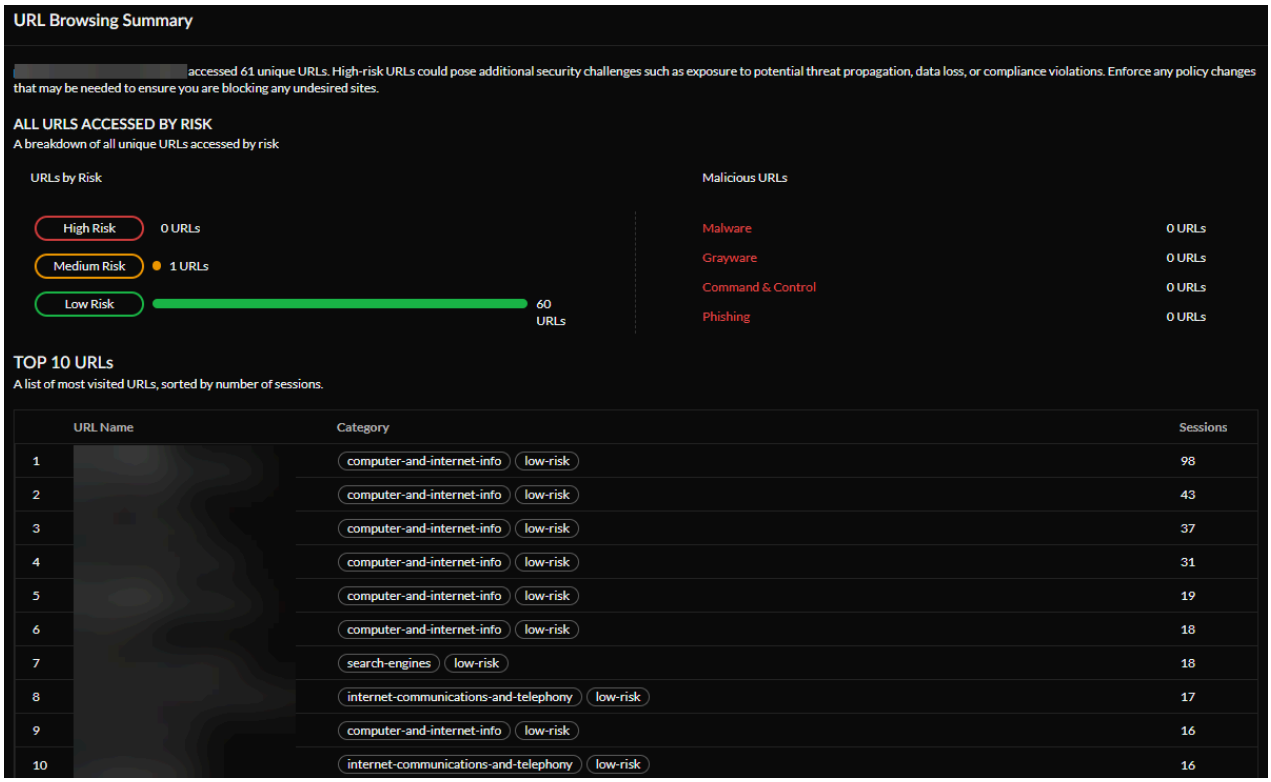
TOP 10 URL CATEGORIES

A list of top URL categories, sorted by data transferred.

	Category	Unique URLs	Data Transfer
1	computer-and-internet-info	42	7.21 MB
2	internet-communications-and-telephony	6	703 KB
3	search-engines	4	616 KB
4	shopping	1	141 KB
5	internet-portals	3	130 KB
6	web-based-email	1	121 KB
7	streaming-media	1	49.5 KB
8	any		43.6 KB
9	online-storage-and-backup	1	11.9 KB
10	unknown	1	5.22 KB

URL Browsing Summary (Resumen de navegación de URL): vea su resumen de navegación de URL, incluidas todas las URL a las que accedió por riesgo. Puede ver un desglose de las URL por riesgo (alto, medio o bajo) y ver a cuántas URL maliciosas accedió. También puede ver una lista de las **Top 10 URLs (10 URL más)** visitadas y cuántas veces visitó cada URL.

©2025 Palo Alto Networks, Inc.

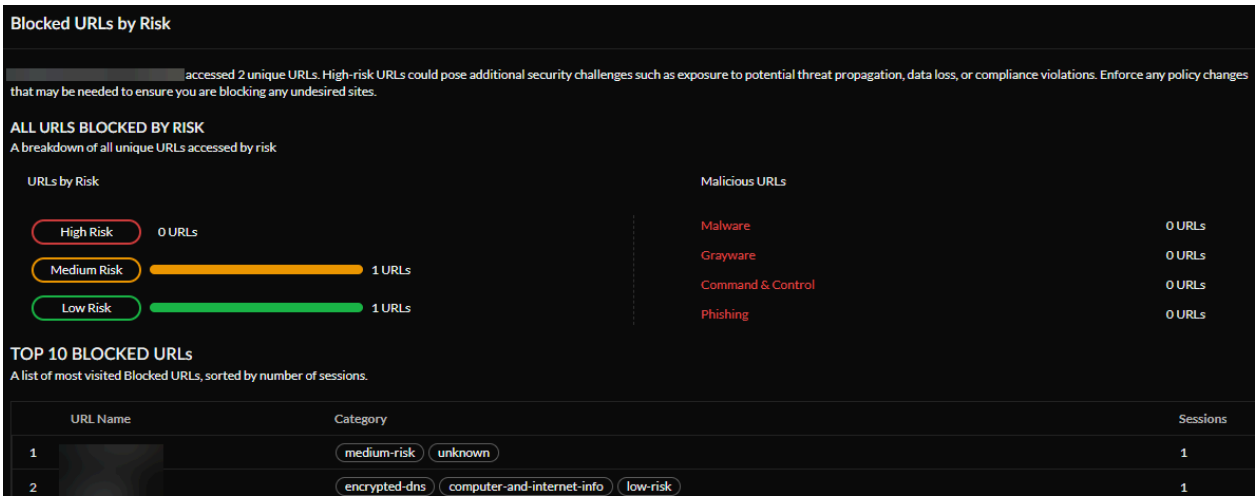


Ver logs de filtrado de URL: seleccione **View URL Filtering Logs (Ver logs de filtrado de URL)** para ver detalles sobre la cantidad total de datos transferidos. Los logs proporcionan una pista de auditoría para eventos de sistema, configuración y red. Los logs de red registran todos los eventos en los que Prisma Access actúa sobre la red.

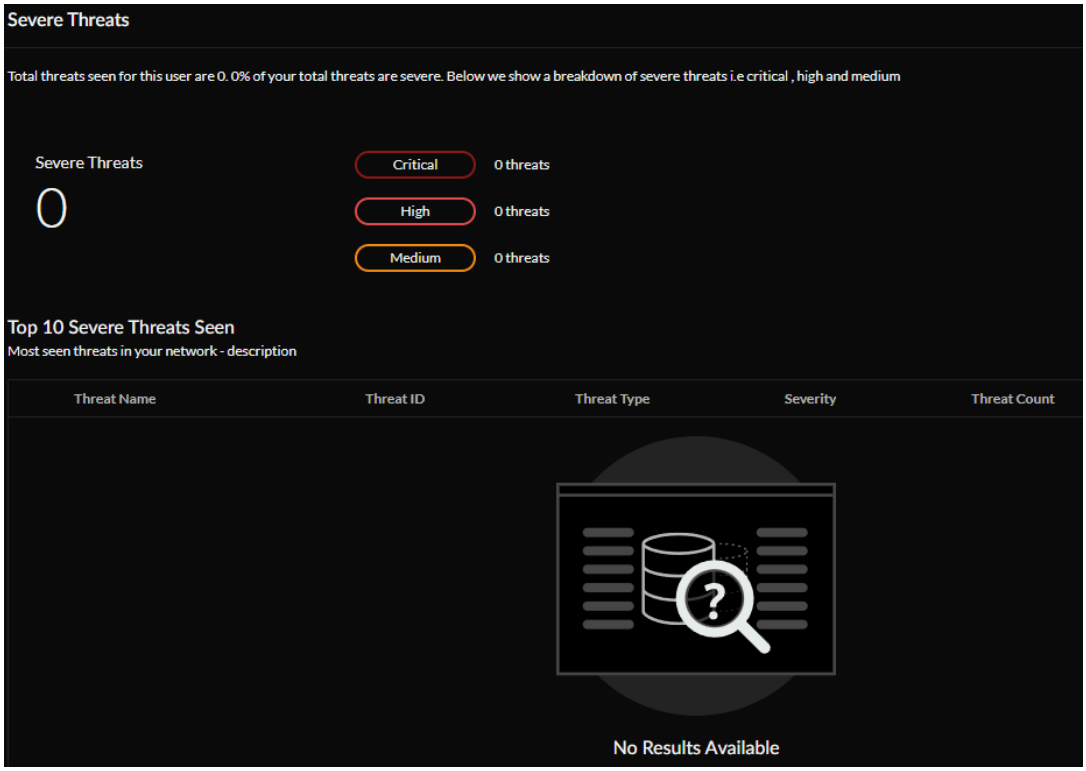
- Vea todos los datos de registro o utilice el menú desplegable para filtrar por **Firewall/URL (Cortafuegos/URL)**, **Common (Común)**o **Endpoint**. Cada uno de estos filtros también tiene varios subfiltros para elegir.
- Introduzca una consulta de log. Haga clic en este campo para ver una selección de consultas con las que puede comenzar y crear su consulta.
- Seleccione un intervalo de tiempo. El valor predeterminado es después de 60 minutos.
- Seleccione **Log Settings (Configuración de logs)** para ver el panel de Strata Logging Service. El servicio Strata Logging Service gestiona el mecanismo de entrega de logs.

Blocked URLs by Risk (URL bloqueadas por riesgo): vea si ha accedido o intentado acceder a alguna URL bloqueada por riesgo. Las URL de alto riesgo podrían crear desafíos de seguridad adicionales, como la exposición a posibles propagaciones de amenazas, pérdida de datos o violaciones de cumplimiento. Aplique cualquier cambio de política necesario para bloquear cualquier sitio no deseado. También puede ver una lista de las **10 URL principales bloqueadas** que más visitó, ordenadas por la cantidad de sesiones.

 ©2025 Palo Alto Networks, Inc.



Severe Threats (Amenazas graves): vea cuántas de sus amenazas son graves. Las amenazas graves se dividen en amenazas críticas, altas y medias. También puede ver una lista de las **Top 10 Severe Threats Seen(Las 10 amenazas más graves detectadas)** en su entorno.



Conectividad

Seleccione cualquier nombre de **User (Usuario)** para ver información sobre la **Connectivity (Conectividad)** del usuario durante el **Time Range (Intervalo de tiempo)** seleccionado.

Proyectos activos: puede ver qué proyectos estuvieron activos durante el intervalo de tiempo que seleccionó y la fecha en que cada proyecto se activó.

Tendencia de dispositivos de usuarios conectados y dispositivos de usuarios conectados: en la página principal de Usuarios, puede ver todos los usuarios conectados y sus proyectos. En la

 ©2025 Palo Alto Networks, Inc.

página **Conectividad**, vea la tendencia individual **de los dispositivos de su usuario conectado** durante el intervalo de tiempo seleccionado y detalles sobre **los dispositivos de su usuario conectado**, como el nombre del dispositivo, la última dirección IP de origen del usuario, la última dirección IP privada, la última ubicación del usuario, la última hora de inicio de sesión, la última hora de cierre de sesión y la duración de la última sesión.



Connected User's Devices (5)

Device Name	Last User Source IP Addre...	Last Private IP	Last User Location	Last Login Time	Last Logout Time	Last Session Duration
MANAN-PBA-WINDO	[redacted]	[redacted]	The Dalles, United States	Mar 19, 2024, 4:42:45 PM	-	-
W-CND1105545			Watford, United Kingdom	Apr 16, 2024, 12:50:32 PM	-	-
DESKTOP-N6D822E			Watford, United Kingdom	Apr 16, 2024, 12:21:15 PM	-	-
DESKTOP-HBF679O			Santa Clara, United States	Apr 15, 2024, 9:00:41 PM	-	-
Automation-Windows-10			Tracy, United States	Apr 16, 2024, 11:48:07 AM	-	-

10 Rows Page 1 of 1

Actividad del proyecto: vea la actividad del proyecto de un usuario por sesión. Puede ver el estado actual de una sesión, cuándo el usuario inició sesión en cada proyecto, cuándo cerró la sesión y cuánto duró cada sesión.

Project Activity

Project Name	Status	Location Group	Last Login time	Last Logout time	Session Duration
[redacted]	DISCONNECTED	US-Central	Apr 12, 2024, 2:53:34 PM	Apr 13, 2024, 6:07:24 AM	15 h 13 min
	DISCONNECTED	US-Central	Apr 15, 2024, 6:27:36 PM	Apr 15, 2024, 9:02:14 PM	2 h 34 min
snippet1project	DISCONNECTED		Apr 4, 2024, 6:28:48 PM	Apr 4, 2024, 9:48:15 PM	3 h 19 min
[redacted]	DISCONNECTED		Mar 28, 2024, 12:09:19 PM	Mar 28, 2024, 12:21:42 PM	12 min 23 sec
	DISCONNECTED	US-Western	Apr 15, 2024, 11:14:37 AM	-	-
	DISCONNECTED	US-Western	Apr 15, 2024, 11:14:37 AM	Apr 15, 2024, 2:20:48 PM	3 h 6 min
	DISCONNECTED	US-Eastern	Apr 14, 2024, 6:48:57 PM	Apr 14, 2024, 7:05:08 PM	16 min 11 sec
	DISCONNECTED		Apr 1, 2024, 5:24:57 PM	Apr 1, 2024, 10:44:35 PM	5 h 19 min
	DISCONNECTED	US-Eastern	Apr 15, 2024, 10:50:17 AM	-	-
	DISCONNECTED	US-Western	Apr 15, 2024, 6:01:35 PM	Apr 15, 2024, 6:13:58 PM	12 min 23 sec

Actividad total del usuario por proyecto: vea el tiempo que un usuario pasó en cada proyecto durante el intervalo de tiempo seleccionado.

©2025 Palo Alto Networks, Inc.

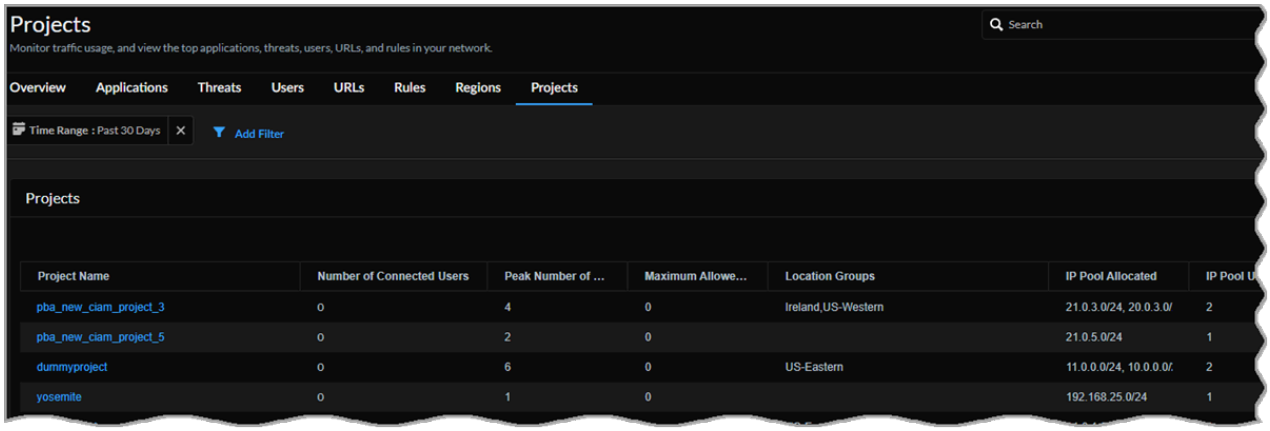
Ver y supervisar proyectos de acceso con privilegios dinámicos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Obtenga visibilidad de su implementación del agente de Prisma Access mediante el uso de Strata Cloud Manager para supervisar la actividad de su proyecto. Vaya a **Activity Insights** > **Projects (Proyectos)** en el Centro de control de Strata Cloud Manager para ver información de acceso basada en proyectos en su entorno.

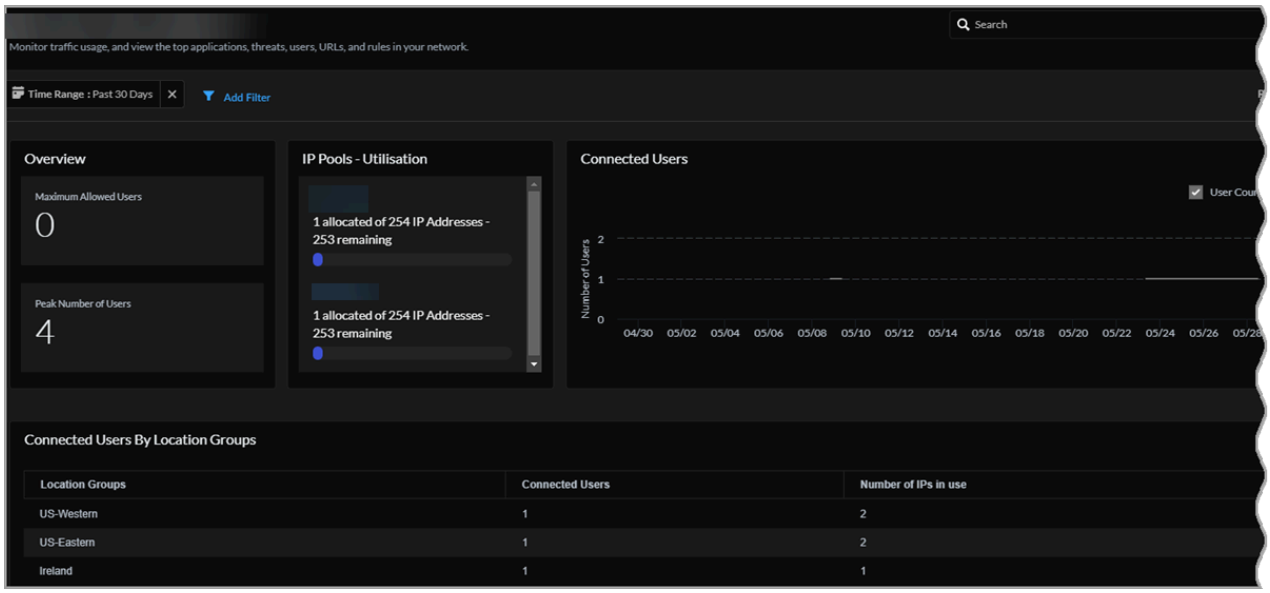
Proyectos

La tabla **Projects (Proyectos)** proporciona una vista general de los proyectos a los que acceden sus usuarios mediante Prisma Access durante el intervalo de tiempo seleccionado. Puede ver el número de usuarios conectados de cada proyecto, el número máximo de usuarios, el máximo de usuarios permitidos, los grupos de ubicaciones de Prisma Access, el grupo de direcciones IP asignado, el grupo de IP utilizado, la cantidad de direcciones IP disponibles y la última ubicación de Prisma Access conectada.



Seleccione un **Project Name (Nombre de proyecto)** para ir a la página de detalles de ese proyecto. El nombre del proyecto (borroso en la siguiente imagen) aparece en la esquina superior izquierda de la página.

 ©2025 Palo Alto Networks, Inc.

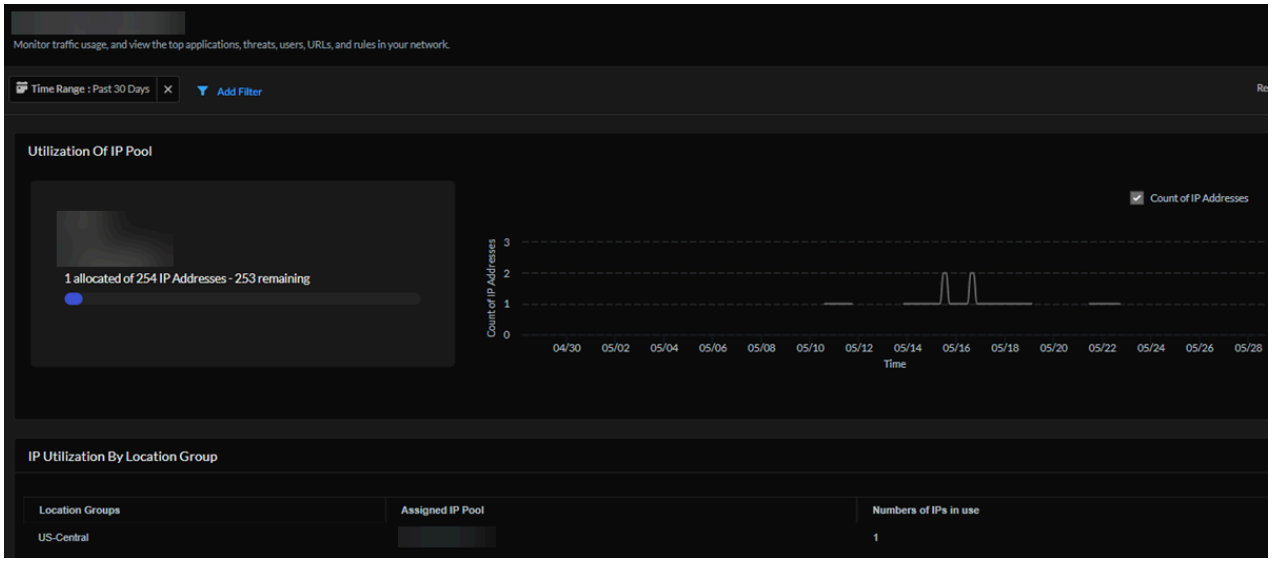


Descripción general

En la página de detalles del proyecto, el **Overview (Descripción general)** muestra el máximo de usuarios permitidos para este proyecto y la cantidad máxima de usuarios durante el intervalo de tiempo seleccionado.

Grupos de IP: Utilización

Vea el número de direcciones IP en uso y el número de direcciones IP que aún están disponibles para los grupos de este proyecto. Seleccione un grupo de IP específico para ir a su página de detalles (ver la siguiente imagen), donde puede ver la utilización de este grupo de IP, el número de direcciones IP utilizadas y la utilización de direcciones IP por grupo de ubicación de Prisma Access.



Usuarios conectados

Vea un gráfico de los usuarios conectados durante el intervalo de tiempo seleccionado. Coloque el cursor sobre cualquier punto del gráfico para ver el número de usuarios en ese punto.

 ©2025 Palo Alto Networks, Inc.

Usuarios conectados por grupos de ubicación

Vea la cantidad de usuarios por el **Location Group (Grupo de ubicación** de Prisma Access en el que se encuentran. También puede ver el número de direcciones IP en uso para cada **Location Group (Grupo de ubicación)**.

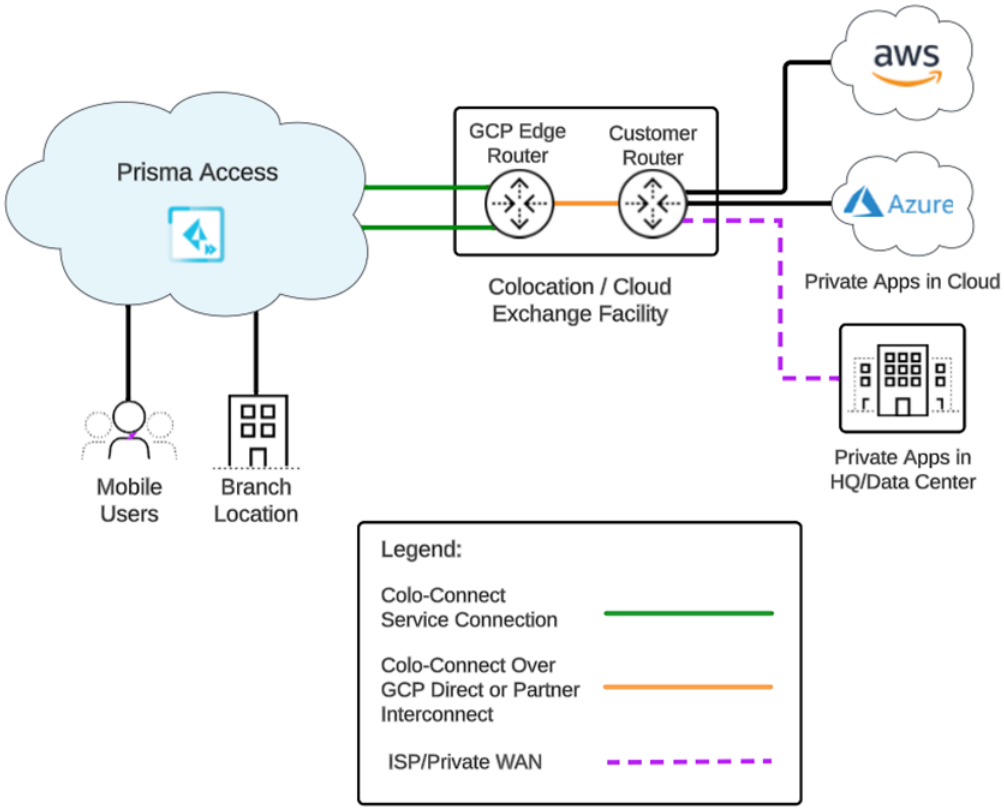
©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Una implementación de Prisma Access (Managed by Panorama) que ejecute una versión mínima del complemento Cloud Services 4.1 y una Versión del plano de datos mínima de 10.2.4 ❑ Una licencia de complemento de Colo-Connect

Hoy en día, las grandes empresas están construyendo centros de rendimiento basados en Colo para llegar a aplicaciones privadas en arquitecturas híbridas y multinube debido a los requisitos de alto ancho de banda y baja latencia. Normalmente, estos centros incluyen interconexiones a uno o varios proveedores de nube y conexiones a los centros de datos locales a través de una WAN privada o alquilada. Los centros de rendimiento pueden enrutar el tráfico entre la nube pública y la infraestructura local a alta velocidad, y son resistentes debido a la infraestructura de interconexión subyacente.

Colo-Connect se basa en el concepto de hub, o centro, de rendimiento basado en Colo, proporcionando conexiones privadas de gran ancho de banda (hasta 20 Gbps) junto con conectividad de Capa 2/3 a Prisma Access desde centros de rendimiento existentes. La siguiente figura muestra la incorporación de Prisma Access en una instancia de GCP mediante conexiones de servicio e interconexiones directas o de socios. Esta configuración limita la exposición a Internet y permite el uso de conexiones privadas para la conectividad de aplicaciones privadas.



Prisma AccessPrisma Access Colo-Connect aprovecha la tecnología de interconexión GCP nativa de la nube para proporcionar conexiones de servicio de gran ancho de banda a sus aplicaciones privadas.

- Alto rendimiento de ancho de banda (hasta 20 Gbps) por región para el acceso a aplicaciones privadas
- Compatibilidad con ambas Interconexiones dedicadas y de socios usando Google Cloud Platform (GCP)
- Compatibilidad con múltiples adjuntos de VLAN por enlace de interconexión.
- Redundancia regional

 ©2025 Palo Alto Networks, Inc.

Casos de uso de Colo-Connect

Prisma Access Colo-Connect proporciona conectividad bidireccional de gran ancho de banda para proteger las aplicaciones privadas, como se muestra en los siguientes casos de uso.

Acceso de gran ancho de banda a aplicaciones privadas

Si su organización tiene presencia de red en un Colo y está aprovechando las instalaciones de Colo para crear conectividad privada con las aplicaciones que están alojadas en las instalaciones, en la nube pública o ambas, Prisma Access puede convertirse en parte de esa infraestructura de Colo a través de Colo-Connect. Puede configurar Colo-Connect con una interconexión dedicada o de socios proporcionado por GCP para obtener un rendimiento de hasta 20 Gbps por región para el acceso a aplicaciones privadas.

Por ejemplo, tiene uno o más centros de datos o ubicaciones de oficinas centrales que tienen conectividad directa con el Colo y desea conectarse a Prisma Access para un acceso seguro y de gran ancho de banda a aplicaciones privadas. En este caso, podría usar una interconexión de socio con Prisma Access Colo-Connect para proporcionar a los usuarios un acceso seguro a las aplicaciones. Dado que el equipo del Colo está emparejado con la nube pública, así como con su centro de datos, también puede proporcionar acceso a cualquier aplicación privada que esté alojada en la nube pública.

Colo-Connect coexiste con las conexiones de servicio basadas en túneles IPSec existentes, por lo que si necesita proporcionar acceso a aplicaciones privadas a centros de datos más pequeños que no requieran un rendimiento de varios gigabits y ancho de banda alto, también puede usar conexiones de servicio a esos centros de datos. Puede configurar las conexiones de servicio mediante el enrutamiento BGP para que su red sea compatible con las conexiones de servicio y las conexiones Colo-Connect.

Conectividad privada para aplicaciones privadas

Colo-Connect puede aprovechar una red privada para que los usuarios accedan a aplicaciones privadas en lugar de acceder a ellas a través de Internet, lo que añade un nivel adicional de control y seguridad para las aplicaciones privadas.

Uso de un proveedor de NaaS de terceros

En este caso de uso, está aprovechando proveedores de red como servicio (NaaS) de terceros, como Megaport y PacketFabric, para conectarse entre Colo y sus aplicaciones que se ejecutan en nubes públicas o con proveedores de SaaS, como salesforce.com o Box. Desea establecer la conectividad de red entre las redes de terceros y Prisma Access para proporcionar acceso de gran ancho de banda a los servicios, nubes y aplicaciones conectados. Usted puede:

- Utilice el equipo de red de un proveedor de NaaS como centro para proporcionar conectividad entre los usuarios y las aplicaciones que se ejecutan en VPC de nube pública o proveedores de SaaS públicos en una región determinada.
- Establecer una sesión BGP entre el equipo de red del proveedor de NaaS y Prisma Access.

©2025 Palo Alto Networks, Inc.

Palo Alto Networks no ha validado el uso de soluciones NaaS de terceros con Prisma Access Colo-Connect. Se recomienda evaluar las capacidades compatibles con el proveedor externo, incluida la configuración de una interconexión a GCP y la creación de túneles GRE a Prisma Access para las conexiones de servicio Colo-Connect.

©2025 Palo Alto Networks, Inc.

¿En qué se diferencia Colo-Connect de las conexiones de servicio y el conector ZTNA?

Palo Alto Networks ofrece tres formas de proteger el acceso a aplicaciones privadas: Conexiones de servicio, Conector ZTNA y Colo-Connect. Las conexiones de servicio y el conector ZTNA protegen el acceso a aplicaciones privadas a través de Internet, mientras que Colo-Connect establece una conexión privada con su centro de datos. Consulte la tabla a continuación para obtener una comparación del ancho de banda y los factores diferenciadores.

Tipo de implementación			
Funcionalidad	**Colo-Connect**	**Conector ZTNA**	**Conexiones de servicio**
Ancho de banda máximo por región de cómputo	20 Gbps	10 Gbps	5 Gbps
Throughput (Rendimiento)	Conectividad privada bidireccional de 20 Gbps al centro de datos	Hasta 10 Gbps por centro de datos	1 Gbps por conexión
Compatible con proveedores de SDN/NaaS como Equinix Cross-Connect y Megaport	Sí	No	No
Redes superpuestas en los centros de datos	No	Sí	No
Otros beneficios	Incorporación sencilla a implementaciones existentes que son híbridas y multinube a través de Colo	Incorporación simplificada de aplicaciones privadas en implementaciones híbridas y multinube	Compatible con Active Directory local.
¿Requiere implementación local?	No	Sí	No

©2025 Palo Alto Networks, Inc.

Características y funcionalidades no compatibles de Colo-Connect

Las siguientes características y funcionalidades no son compatibles con Colo-Connect:

- Configuración de una conexión de servicio Colo-Connect como una conexión de servicio de destino cuando se utiliza Dirección de tráfico
- Compatibilidad con IPv6 para el acceso a aplicaciones privadas
- Emparejamiento de eBGP a través de IPv6

©2025 Palo Alto Networks, Inc.

Requisitos y requisitos previos para Prisma Access Colo-Connect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Una implementación de Prisma Access (Managed by Panorama) que ejecuta una versión mínima del complemento Cloud Services de 4.1 y una versión mínima del plano de datos de 10.2.4 ❑ Una licencia de complemento de Colo-Connect

Antes de iniciar la incorporación y configuración de Colo-Connect, tenga en cuenta la información y los requisitos necesarios siguiendo esta lista de verificación.

- ❑ Asegúrese de tener acceso al proveedor de servicios de Colo (por ejemplo, tiene acceso al portal del cliente de Equinix).
- ❑ Asegúrese de que su CPE pueda admitir GRE y BGP.

  Las conexiones de servicio Colo-Connect utilizan túneles GRE.
- ❑ Decida qué tipo de interconexión utilizará para Colo-Connect (un socio o una interconexión dedicada).
  - **Interconexión de socios**: se requiere una clave de emparejamiento de Prisma Access para las interconexiones de socios. Usted recibe esta clave durante la incorporación de Prisma Access.

    Si crea una interconexión de socio, asegúrese de que el proveedor de servicios (SP) es un SP aprobado con GCP y la conectividad entre el SP y GCP ya está establecida.
  - **Interconexión dedicada**:
    - Determine la ubicación de Colo donde se conectará el cable de conexión cruzada antes de comenzar a incorporarlo en Prisma Access. La ubicación de Colo es necesaria para que Palo Alto Networks ordene el enlace dedicado
    - Familiarícese con las interconexiones de red básicas para que pueda configurar los circuitos.
    - Después de aprovisionar la interconexión dedicada, debe probarla.
- ❑ **Requisitos de subredes**: determine las subredes IPv4 RFC-1918 que utilizará para cada conexión Colo-Connect por región. Prisma Access utiliza estas subredes para la comunicación interna y la creación de redes.

  Haga que las subredes sean únicas entre todas las regiones de Colo-Connect en un inquilino determinado. La subred Colo-Connect no se puede superponer con la subred de infra de Prisma Access y el grupo de usuarios móviles. Utilice un tamaño mínimo de subred de /28.

©2025 Palo Alto Networks, Inc.

- **Requisitos de enlace (interconectar)**: siga estas directrices al configurar los enlaces:
  - Cada licencia adicional de Colo-Connect incluye un enlace de 10 Gbps de capacidad. Necesita un mínimo de dos enlaces, lo que significa que necesita comprar un mínimo de dos licencias en una implementación de Colo-Connect.
  - Incorpore dos enlaces en cada región.

    Ambos enlaces deben estar en diferentes zonas de disponibilidad (dominios periféricos).
  - (Implementaciones de interconexión dedicadas únicamente) Si desea incorporar más de seis enlaces en un inquilino, póngase en contacto con su representante de cuenta o socio de Palo Alto Networks, quien se comunicará con el equipo de Ingeniería de fiabilidad del sitio (SRE), y envíe una solicitud para aumentar la cuota de un inquilino determinado.

- **Requisitos de conexión**:
  - Incorpore dos conexiones en cada región.

    Ambas conexiones deben estar en diferentes dominios de extremo.
  - Las conexiones en modo activo/copia de seguridad o modo activo/activo deben tener el mismo ancho de banda.
  - Decida si desea configurar sus conexiones en una configuración activa/activa o activa/copia de seguridad.
- **Requisitos de conexión de servicio de Colo-Connect**:
  - cada conexión de servicio requiere dos conexiones.
  - Cada conexión para una conexión de servicio dada debe estar en un enlace diferente y un dominio de borde diferente.
  - Tenga en cuenta las direcciones que utilizará como dirección IP BGP con colo-router y las direcciones IP locales del túnel GRE. Utilice estas direcciones durante la creación de la conexión de servicio.
  - Las conexiones de servicio deben estar en el mismo tipo de enlace (enlaces de interconexión de socios o enlaces de interconexión dedicada).
- **Interoperabilidad con conexiones de servicio basadas en IPSec existentes**: Palo Alto Networks recomienda encarecidamente que implemente conexiones de servicio basadas en túneles Colo-Connect e IPSec en diferentes regiones. Además, si migra de una conexión de servicio basada en túnel IPSec a una conexión de servicio Colo-Connect, debe programar una ventana de mantenimiento. Después de migrar de una conexión de servicio basada en túnel IPSec a una conexión de servicio Colo-Connect, quite la conexión de servicio basada en IPSec después de que la conexión de servicio Colo-Connect esté en funcionamiento y antes de que caduque la ventana de mantenimiento.

 ©2025 Palo Alto Networks, Inc.

Configurar Prisma Access Colo-Connect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Una implementación de Prisma Access (Managed by Panorama) que ejecute una versión mínima del complemento Cloud Services 4.1 y una Versión del plano de datos mínima de 10.2.4 ❑ Una licencia de complemento de Colo-Connect

Prisma Access Colo-Connect consta de los siguientes componentes:

- **Colo**: la instalación de colocación que proporciona espacio en rack, energía y conectividad para alojar redes, infraestructura de nube privada y pública, como Equinix.
- **Interconexión dedicada**: la conexión física dedicada de Capa 2 o Capa 3 entre su enrutador y un enrutador de borde de GCP en una región de cómputo de GCP. Una interconexión dedicada proporciona una conexión física directa entre su red local y la red de Google.

  Las interconexiones se llaman *Links (Enlaces)* en la UI de Prisma Access.
- **GCP VLAN Attachment (Adjunto de VLAN de GCP)**: la conexión lógica de Capa 2 sobre el enlace que separa el tráfico de cualquier otra conexión lógica que comparta el mismo enlace.

  Las conexiones de VLAN se llaman *Conexiones* en la interfaz de usuario de Prisma Access.
- **Interconexión de Socios**: la conexión física de Capa 3 entre un enrutador propiedad de un proveedor de servicios y un enrutador de borde de GCP en una región de cómputo de GCP dada. Un socio de Interconexión proporciona conectividad entre sus redes locales y VPC a través de un proveedor de servicios compatible.

  Colo-Connect admite tanto interconexiones dedicadas como de socios.
- **Enrutador Colo (cliente)**: el dispositivo de enrutamiento en la instalación de Colo que establece eBGP con el enrutador de la nube GCP a través de la interconexión en la instalación de Colo, así como eBGP con la conexión de servicio Colo-Connect a través del túnel GRE. Es un enrutador de cliente para una interconexión dedicada, o si el proveedor de servicios tiene conectividad de Capa 2 con GCP a través de la interconexión de socios. El proveedor de servicios posee el enrutador Colo cuando tiene conectividad de Capa 3 con el enrutador de la nube GCP.
- **Enrutador de borde de GCP**: equipo de red de borde de GCP para proporcionar conectividad física entre GCP y la red de cliente/socio a través de Colo.
- **Enrutador en la Nube**: la creación de software de GCP en la nube que establece sesiones BGP con el dispositivo de red (por ejemplo, enrutador o cortafuegos de Capa 3) en el Colo y enruta el tráfico entre Prisma Access y su red. No es necesario configurar este componente; Prisma Access lo hace automáticamente.

Para configurar Colo-Connect, primero debe recopilar información sobre su entorno de red existente y asegurarse de tener todos los componentes de red necesarios. Asegúrese de tener

 ©2025 Palo Alto Networks, Inc.

todos los requisitos previos; luego, implemente Colo-Connect en la red de su organización utilizando una interconexión dedicada o de socios.

- Strata Cloud Manager
- Panorama

Configurar Prisma Access Colo-Connect (Strata Cloud Manager)

Para configurar Colo-Connect, primero debe recopilar información sobre su entorno de red existente y asegurarse de tener todos los componentes de red necesarios. Asegúrese de tener todos los requisitos previos; luego, implemente Colo-Connect en la red de su organización utilizando una interconexión dedicada o de socios.

Configure Prisma Access Colo-Connect: implementaciones que utilizan interconexiones de socios

Para configurar Prisma Access Colo-Connect mediante una interconexión de socio, complete estos pasos.

STEP 1 | Cree subredes para sus conexiones Colo-Connect.

Las subredes que se crean aquí se utilizan en las conexiones y conexiones de servicio que se crean en los pasos posteriores.

1. Desde Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect**.
2. Deberá **Add Prefix (Añadir un prefijo)** y añadir una subred Colo-Connect a una ubicación Prisma Access para ello.

   Consulte la lista de ubicaciones de colo-connect compatibles aquí. Introduzca una subred mínima de /28.
3. (Opcional) Si planifica crear instancias de Colo-Connect para más de una ubicación, añada más subredes por ubicación.

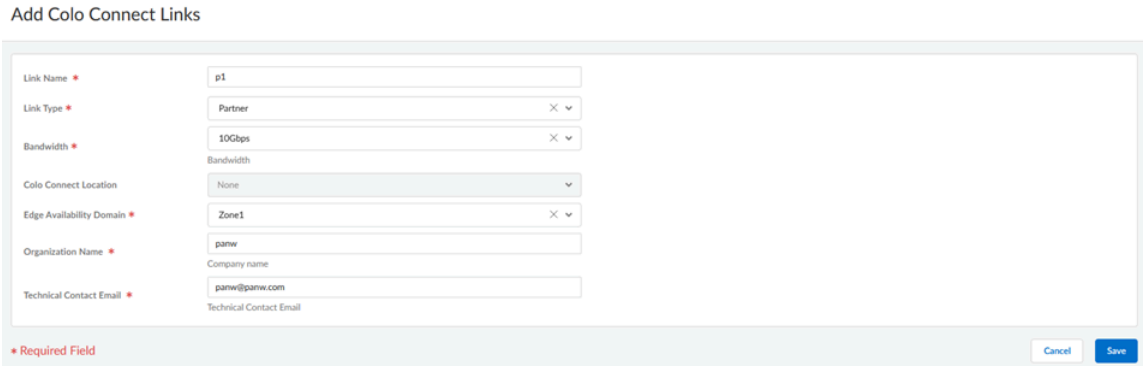
   Puede configurar una subred por ubicación.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada un nuevo enlace Colo-Connect (también conocido como *interconexión*).

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** y **Add Link (Añadir enlace)**.
2. Dé al enlace un **Link Name (Nombre de enlace)** único.
3. Seleccione Interconexión de **Partner (Socios)** como el **Link Type (Tipo de enlace)**.
4. Especifique los parámetros restantes del enlace Colo-Connect.
   - Seleccione una de las siguientes opciones: **10 Gbps** o **20 Gbps** para el **Bandwidth (Ancho de banda)**.
   - Seleccione **Zone1 (Zona1)** o **Zone2 (Zona2)** para el **Edge Availability Domain (Dominio de disponibilidad de borde)**. Tome este valor de la GCP zone (Zona de GCP) utilizada para su dominio de disponibilidad de borde.
   - Introduzca el **Organization Name (Nombre de la organización)** que se utilizará para este enlace.
   - Introduzca el **Email (Correo electrónico)** a utilizar para este enlace. Cualquier dirección de correo electrónico es aceptable.



5. Repita los pasos 2.a a 2.d y cree otro enlace con un **Edge Availability Domain (Dominio de disponibilidad de borde)** diferente.

STEP 3 | Cree las conexiones [también conocidas como *VLAN attachments (Adjuntos VLAN)*] para Colo-Connect.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** y **Add Connection (Añadir conexión)**.
2. Configure la configuración de conexión.
   - Introduzca un **Connection Name (Nombre de conexión)**único.
   - Seleccione un **Link Name (Nombre de enlace)** de los enlaces que configuró en un paso anterior.

     No necesita introducir un **VLAN ID (ID de VLAN)**; no se puede configurar para las VLAN creadas en interconexiones de socios.
   - Seleccione un **Bandwidth (Ancho de banda)** para la conexión.

     Puede seleccionar entre **1 Gbps**, **2 Gbps**, **5 Gbps**, **10 Gbps**o **20 Gbps**.

     Si configura varias conexiones para una interconexión, asegúrese de que el ancho de banda total de las conexiones no exceda el ancho de banda de la interconexión.

 ©2025 Palo Alto Networks, Inc.

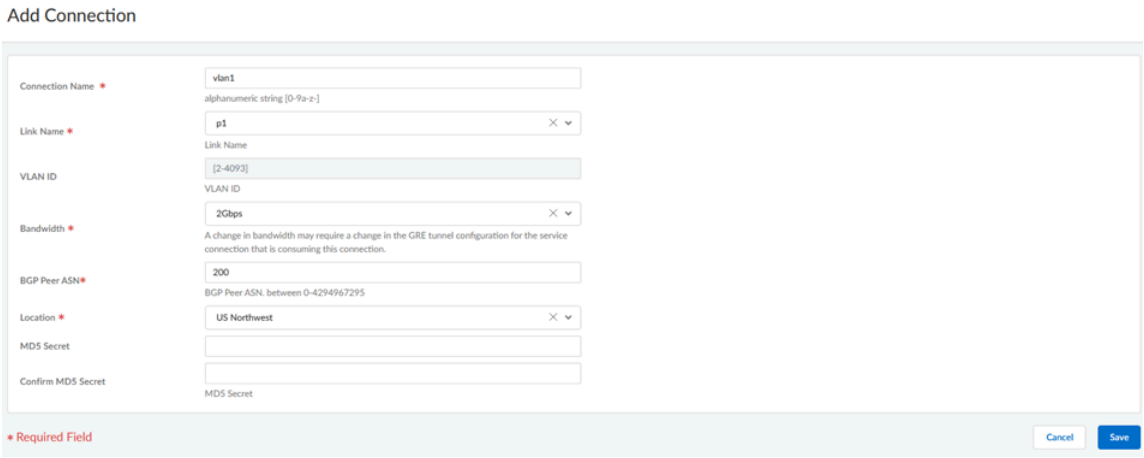
Por ejemplo, dada una interconexión de socio de 10 Gbps, puede configurar 10 conexiones de 1 Gbps cada una, pero no supere los 10 Gbps en total para todas las conexiones.

Si su implementación requiere más de 16 conexiones, comuníquese con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de SRE para atender la solicitud.

- Introduzca un **BGP Peer ASN (ASN de peer BGP)**.

  Introduzca el número de Sistema Autónomo (AS) para el enrutador local del cliente en el Colo. El rango está entre 1 y 4294967295.
- Seleccione la **Location (Ubicación)** de los nombres de conexión que creó en un paso anterior.

  Ya debe haber añadido una subred para cualquier ubicación que especifique.
- (Opcional) Introduzca el **MD5 Secret (Secreto MD5)**de BGP.



3. Continúe creando conexiones hasta completar.

   Crea dos conexiones. Ambas conexiones deben estar en la misma región y cada conexión debe estar en una zona separada. Estas conexiones se utilizan en las conexiones de servicio que se crean en un paso posterior.

STEP 4 | **Push Config (Enviar configuración)**.

Actualice el navegador una vez completado el trabajo de confirmación para ver las claves de emparejamiento en **Connections (Conexiones)**.

STEP 5 | Recupere la **Pairing Key (Clave de emparejamiento)** y complete la configuración de interconexión de su socio en GCP.

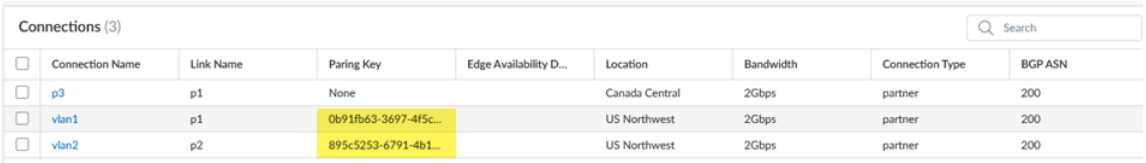
Utilice esta clave de emparejamiento cuando configure la interconexión de socios en el Colo.

Cuando se incorpora por primera vez una nueva conexión, el **Status (Estado)** en el área **Connections (Conexiones)** muestra un **Status (Estado)** de **PENDING_PARTNER** y un **BGP**

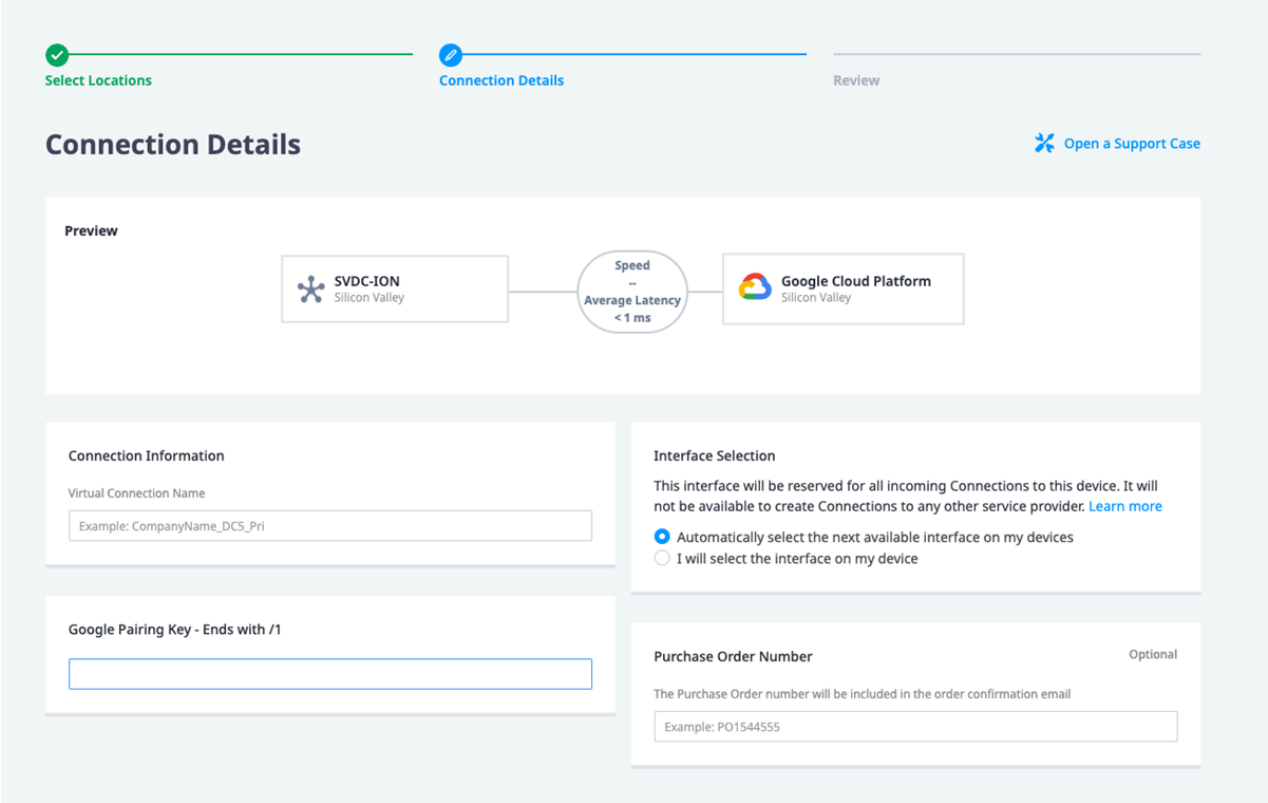
 ©2025 Palo Alto Networks, Inc.

Status (Estado de BGP) de **DOWN (CAÍDO)**. Para cambiar el estado de la conexión a **ACTIVE (ACTIVO)**, recupere la clave de emparejamiento e introduzca la conexión en el Colo.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** > **Connections (Conexiones)** y copie la **Pairing Key (Clave de emparejamiento)**.



2. Cree una nueva conexión VLAN en el Colo.



3. Pegue la clave de emparejamiento en la VLAN Colo.

   GCP detecta cuando se consume la clave de emparejamiento, cambia el estado de la VLAN a **ACTIVE (ACTIVA)** y genera la dirección IP BGP para que la configure en su enrutador local en el Colo. Prisma Access utiliza estas IP para iniciar la adyacencia eBGP sobre cada VLAN asociada entre el enrutador Colo y el enrutador en la nube GCP.

STEP 6 | Creación de enrutamiento eBGP en el enrutador del cliente (Colo) para la conexión Colo-Connect.

Debe configurar el emparejamiento BGP para garantizar la conectividad entre el enrutador del cliente y el enrutador en la nube.

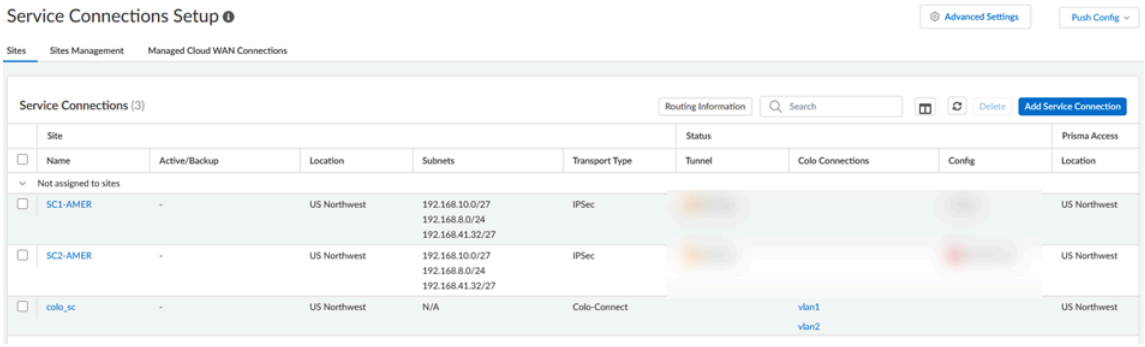
STEP 7 | Configurar las conexiones de servicio para utilizar con Colo-Connect.

STEP 8 | **Push Config (Enviar configuración)**.

 ©2025 Palo Alto Networks, Inc.

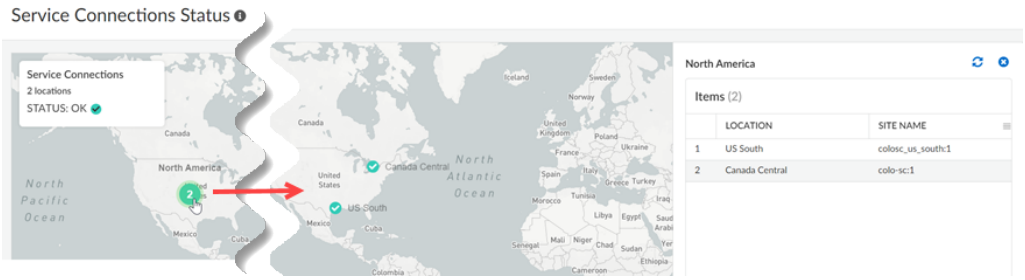
STEP 9 | Verifique el estado de las conexiones Colo-Connect.

1. Para comprobar el estado de una conexión de servicio utilizada por una conexión Colo-Connect, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connection (Conexión de servicio)**.



2. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**. Establezca el **Configuration Scope (Ámbito de configuración)** en **Prisma Access**. Seleccione el estado **In sync (Sincronizado)** de las **Service Connections (Conexiones de servicios)** en el estado de sincronización de Prisma Access. Seleccione la región que tiene una conexión Colo-Connect implementada.

   - Si la conexión Colo-Connect y el enrutamiento BGP están activos, el Estado muestra **OK (Aceptar)**.
   - Si la conexión Colo-Connect está activa pero el enrutamiento BGP no está activo, se muestra el estado **Warning (Advertencia)**.
   - Si la conexión Colo-Connect y el enrutamiento BGP están inactivos, el Estado muestra **Down (Inactivo)**.
   - Si la conexión Colo-Connect está inactiva pero el enrutamiento BGP está activo, el Estado muestra **Error**.



3. Para obtener más información, haga clic en el cuadro de la región y vea la información en la pestaña **Status (Estado)**.

STEP 10 | Para verificar los detalles de conexión, incluida la clave de emparejamiento, de las conexiones Colo-Connect vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo Connect**.

Configurar Prisma Access Colo-Connect: implementaciones que utilizan interconexiones dedicadas

Para configurar Prisma Access Colo-Connect usando una interconexión dedicada, complete estos pasos.

©2025 Palo Alto Networks, Inc.

STEP 1 | Cree subredes para sus conexiones Colo-Connect.

Las subredes que se crean aquí se utilizan en las conexiones y conexiones de servicio que se crean en los pasos posteriores.

1. Desde Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** y haga clic en el icono de engranaje para editar la configuración.
2. Deberá **Add Prefix (Añadir un prefijo)** para la **Colo-Connect Subnet (Subred Colo-Connect)** y seleccionar una ubicación de Prisma Access [**PA Location (ubicación de PA)**] para ello.

   Introduzca una subred mínima de /28.
3. (Opcional) Si planifica crear instancias de Colo-Connect para más de una ubicación, añada más subredes por ubicación.

   Puede configurar solo una subred por ubicación.

STEP 2 | Añada un nuevo enlace Colo-Connect (también conocido como *interconexión*).

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** y **Add Link (Añadir enlace)**.
2. Dé al enlace un **Link Name (Nombre de enlace)** único.
3. Seleccione una interconexión **Dedicated (Dedicada)** como **Link Type (Tipo de enlace)**.
4. Especifique los parámetros restantes del enlace Colo-Connect.
   - Seleccione una de las siguientes opciones: **10 Gbps** o **20 Gbps** para el **Bandwidth (Ancho de banda)**.

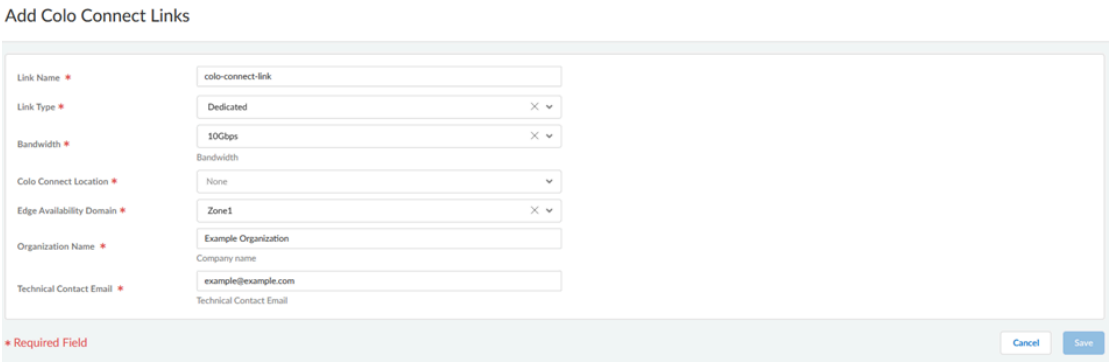
     Si selecciona 20 Gbps, debe añadir el enlace de interconexión dedicada en dos enlaces de 10 Gbps utilizando LACP.

     No puede cambiar el ancho de banda de un enlace de interconexión dedicado después de especificarlo y confirmar y enviar los cambios.
   - Seleccione una **Colo-Connect Location (Ubicación de Colo-Connect)** de la lista desplegable.

     Asegúrese de seleccionar la misma ubicación que utilizó para la interconexión dedicada.
   - Seleccione **Zone1 (Zona1)** o **Zone2 (Zona2)** para el **Edge Availability Domain (Dominio de disponibilidad de borde)**. Tome este valor de la GCP zone (Zona de GCP) utilizada para su dominio de disponibilidad de borde.
   - Introduzca el **Organization Name (Nombre de la organización)** que se utilizará para este enlace.
   - Introduzca el **Email (Correo electrónico)** donde desea recibir los detalles del LOA-CFA del proveedor de la nube.
     - GCP utiliza este correo electrónico para enviar la Carta de autorización y Asignación de facilidad de conexión (LOA-CFA). Asegúrese de que el LOA-

 ©2025 Palo Alto Networks, Inc.

CFA se envíe a su proveedor de Colo, para que puedan comenzar a instalar sus conexiones.



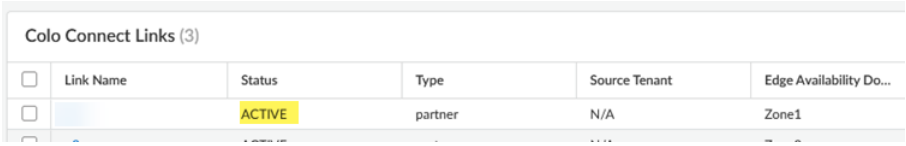
STEP 3 | Una vez creada la conexión dedicada, la instalación de Colo prueba sus conexiones y le informa de que han sido probadas y están listas para usar.

No se requiere configuración de Prisma Access para este paso. No cree las conexiones Colo-Connect en Prisma Access hasta que las instalaciones de Colo le informen que se han sometido a pruebas.

STEP 4 | Cree las conexiones [también conocidas como *VLAN attachments (Adjuntos VLAN)*] para Colo-Connect.

1. Para asegurarse de que el estado del enlace dedicado sea Activo, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** > **Colo Connect links (Enlaces de Colo Connect)**.

   Hasta que el estado del enlace dedicado esté Activo, no puede crear enlaces Colo-Connect.

2. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** y **Add Connection (Añadir conexión)**.
3. Configure la configuración de conexión.
   - Introduzca un **Name (Nombre)** único para la conexión.
   - Seleccione un **Link Name (Nombre de enlace)** de los enlaces que configuró en un paso anterior.
   - (Opcional) Introduzca una **ID VLAND (ID de VLAN)** para la conexión.

     Los ID de VLAN las genera el proveedor de interconexión (GCP) si no introduce un valor manualmente.
   - Seleccione un **Bandwidth (Ancho de banda)** para la conexión.

     Puede seleccionar entre **1 Gbps**, **2 Gbps**, **5 Gbps**, **10 Gbps**o **20 Gbps**.

     Si configura varias conexiones para una interconexión, asegúrese de que el ancho de banda total de las conexiones no exceda el ancho de banda de la interconexión. Por ejemplo, dada una interconexión dedicada de 20 Gbps, puede configurar 10

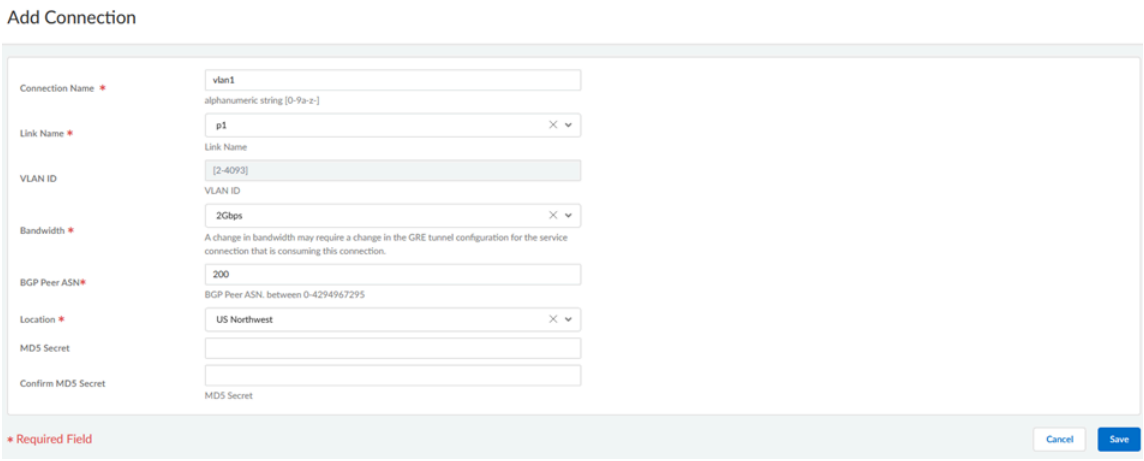
 ©2025 Palo Alto Networks, Inc.

conexiones de 2 Gbps cada una, pero no supere los 20 Gbps en total para todas las conexiones.

- Introduzca un **BGP Peer ASN (ASN de peer BGP)**.

  Introduzca el número de Sistema Autónomo (AS) para el enrutador local del cliente en el Colo. El rango está entre 1 y 4294967295.
- Seleccione la **Location (Ubicación)** de los nombres de conexión que creó en un paso anterior.

  Ya debe haber añadido una subred para cualquier ubicación que especifique.
- (Opcional) Introduzca el **MD5 Secret (Secreto MD5)**de BGP.



4. Continúe creando conexiones hasta completar.

   Crea dos conexiones. Ambas conexiones deben estar en la misma región y cada conexión debe estar en una zona separada. Estas conexiones se utilizan en las conexiones de servicio que se crean en un paso posterior.

STEP 5 | **Push Config (Enviar configuración)**.

STEP 6 | Configure el enrutamiento eBGP en el enrutador del cliente.

Debe configurar el emparejamiento BGP para garantizar la conectividad entre los enrutadores del cliente.

STEP 7 | Configurar las conexiones de servicio para utilizar con Colo-Connect.

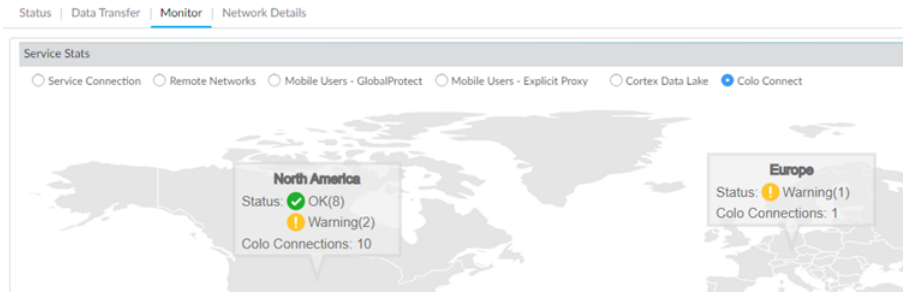
STEP 8 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios de configuración, asegurándose de que **Colo-Connect** esté seleccionado en el **Push Scope (Ámbito de envío)**.

STEP 9 | Verifique el estado de las conexiones Colo-Connect.

1. Para verificar el estado de una conexión de servicio utilizada por una conexión Colo-Connect, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**. Establezca el **Configuration Scope (Ámbito de configuración)** en **Prisma Access**.

 ©2025 Palo Alto Networks, Inc.

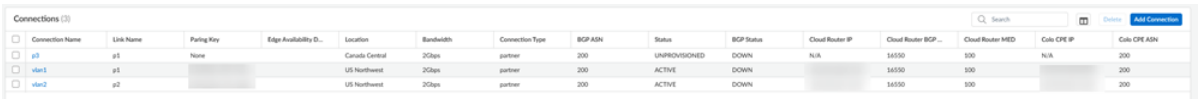
2. Coloque el cursor sobre una región que tenga una conexión Colo-Connect implementada.
   - Si la conexión Colo-Connect y el enrutamiento BGP están activos, el Estado muestra **OK (Aceptar)**.
   - Si la conexión Colo-Connect está activa pero el enrutamiento BGP no está activo, se muestra el estado **Warning (Advertencia)**.
   - Si la conexión Colo-Connect y el enrutamiento BGP están inactivos, el Estado muestra **Down (Inactivo)**.
   - Si la conexión Colo-Connect está inactiva pero el enrutamiento BGP está activo, el Estado muestra **Error**.



3. Para obtener más información, haga clic en el cuadro de la región y vea la información en la pestaña **Status (Estado)**.

STEP 10 | Para verificar los detalles de la red de las conexiones de Colo-Connect, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** > **Connections (Conexiones)** y vea los detalles.

En el caso de los enlaces dedicados, la **Pairing Key (Clave de emparejamiento)** se muestra como **N/A (N/D)**.



Configurar el enrutamiento eBGP de VLAN en el enrutador del cliente

GCP crea direcciones IP para el enrutador del cliente (Colo) y el enrutador en la nube durante estas etapas de su implementación:

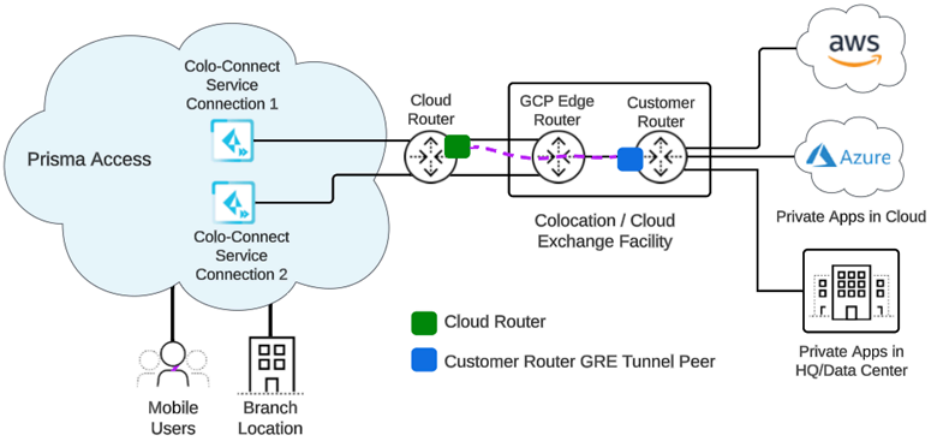
- Para las interconexiones de socios, GCP crea las direcciones IP después de que su Colo consume la clave de emparejamiento (por ejemplo, Equinix).
- Para las interconexiones dedicadas, GCP crea las direcciones IP después de que usted incorpora sus conexiones Colo-Connect (archivos adjuntos de VLAN) y confirma y envía sus cambios.

Para garantizar un enrutamiento correcto, debe:

- Configure la dirección IP del enrutador Colo (la **Colo CPE IP** en Prisma Access) como la dirección IP eBGP local
- Configure la dirección IP del enrutador en la nube [**Cloud Router IP (IP del enrutador en la nube)**] como la dirección del par eBGP en su router Colo.

 ©2025 Palo Alto Networks, Inc.

Una vez completado, eBGP estará configurado para la conexión (conexión VLAN) entre el enrutador Colo y el enrutador en la nube.



La creación de esta ruta es el primer paso para configurar el enrutamiento del túnel GRE. Complete el enrutamiento del túnel GRE cuando configure túneles GRE durante la configuración de la conexión del servicio.

Utilice los siguientes pasos para configurar el enrutamiento entre Colo y el enrutador en la nube.

STEP 1 | Desde Strata Cloud Manager, cree las subredes, los enlaces y las conexiones y proceda a **Push Config (Enviar configuración)**.

Utilice el flujo de trabajo específico para su tipo de interconexión (ya sea de Socio o Dedicada). Para las interconexiones de socio, asegúrese de pegar la clave de emparejamiento en la VLAN de Colo.

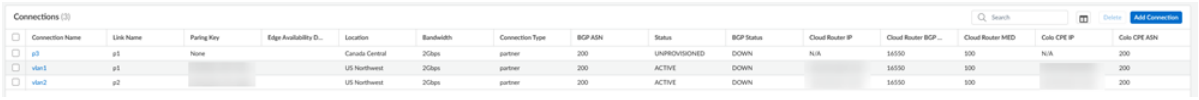
STEP 2 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** > **Connections (Conexiones)**.

STEP 3 | Tome nota de los siguientes elementos de conexión:

- **Colo CPE IP**
- **IP del enrutador en la nube**
- **Cloud Router ASN BGP**

En el siguiente ejemplo:

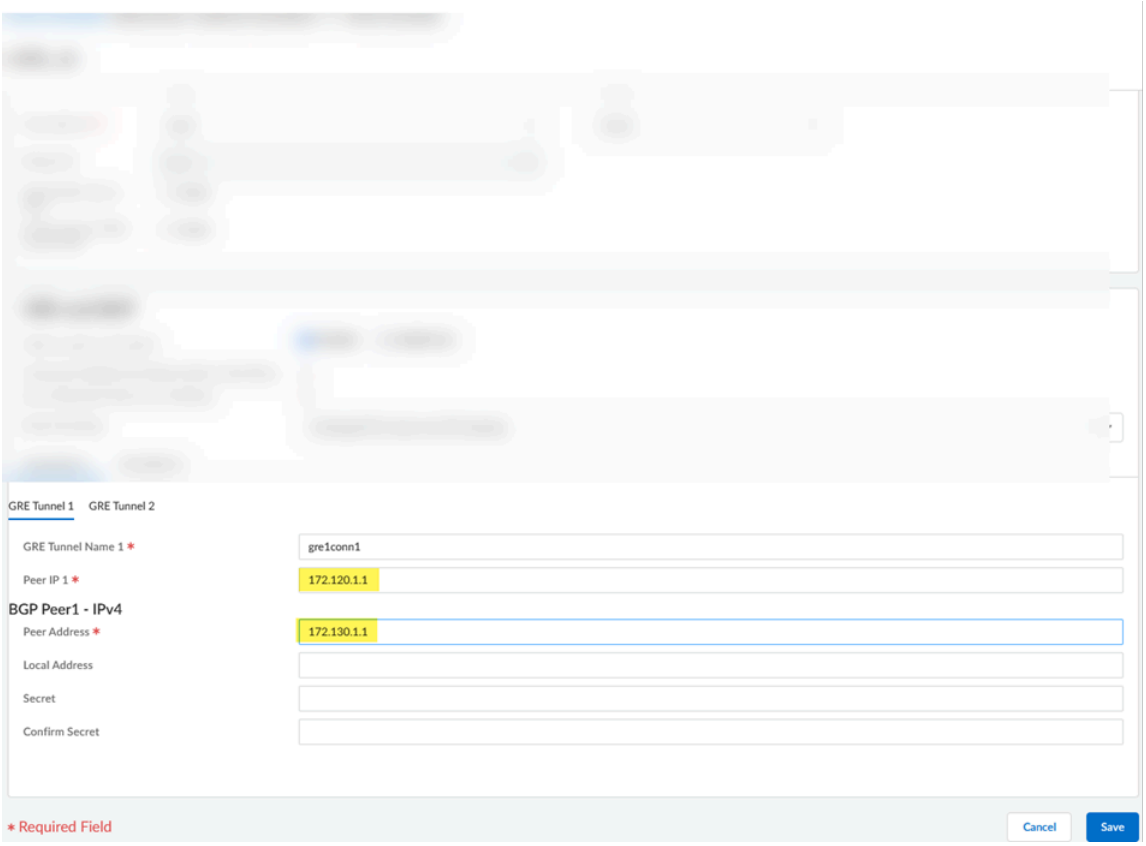
- Para la conexión vlan-central-1, la **Colo CPE IP (IP de Colo CPE)** es 169.254.24.170/29, la **Cloud Router IP (IP del enrutador en la nube)** es 169.254.24.169/29 y el **Cloud Router BGP ASN (ASN BGP del enrutador en la nube)** es 16550.
- Para la conexión vlan-central-2, la **Colo CPE IP (IP de Colo CPE)** es 169.254.120.74/29, la **Cloud Router IP (IP del enrutador en la nube)** es 169.254.120.73/29 y el **Cloud Router BGP ASN (ASN BGP del enrutador en la nube)** es 16550
- .



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Determine las direcciones IP que utilizará para las direcciones IP GRE locales cuando configure las conexiones del servicio Colo-Connect.

Configúrelas cuando configure una conexión de servicio Colo-Connect (**Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)**]. En las áreas **Peer IP 1 (IP del peer 1)** y, si es necesario, **Peer IP 2 (IP del peer 2)**.



Si está configurando una conexión de servicio para admitir hasta 10 Gbps de rendimiento, coloque un túnel en cada **Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**, para un total de dos túneles en cada conexión de servicio.

Si está configurando una conexión de servicio para que admita más de 10 Gbps de rendimiento (hasta 20 Gbps), coloque dos túneles en cada **Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**, para un total de cuatro túneles en cada conexión de servicio.

Los siguientes ejemplos muestran un túnel configurado para un rendimiento de más de 10 Gbps, por lo que se utilizan dos túneles por conexión y utilizan las siguientes direcciones IP de peers:

- 172.120.1.1 para Conexión 1
- 172.130.1.1 para Conexión 1
- 172.121.1.1 para Conexión 2
- 172.131.1.1 para Conexión 2

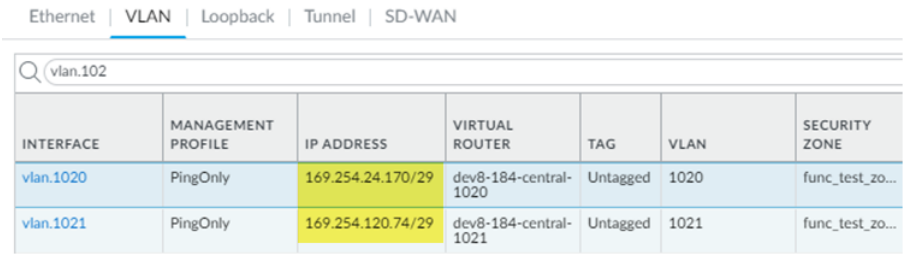
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Inicie sesión en el enrutador Colo.

Las siguientes capturas de pantalla de configuración utilizan un cortafuegos de nueva generación de Palo Alto Networks como enrutador Colo.

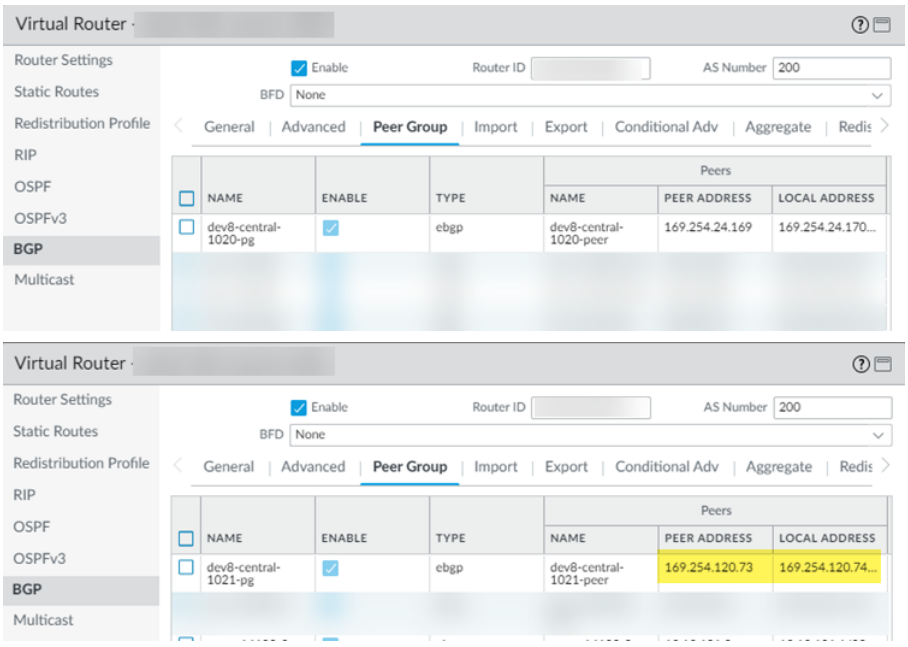
STEP 6 | Añada una interfaz VLAN, especificando la dirección **Colo CPE IP** como dirección IP.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (red)** > **Interfaces** > **VLAN** y **Add (Añadir)** la interfaz VLAN, especificando el nombre del **Virtual router (Enrutador virtual)** y



STEP 7 | Configure la dirección IP del enrutador Colo [**Colo CPE IP (Colo CPE IP**] como la dirección IP eBGP local y configure la dirección IP del enrutador en la nube [**Cloud Router IP (IP del enrutador en la nube)**] como la dirección de peer eBGP en su enrutador Colo.

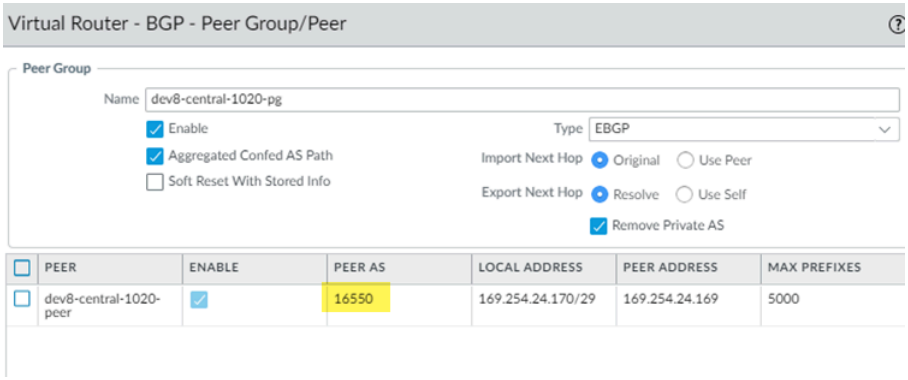
Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Peer Group (Grupo de peers)** y introduzca la **Colo CPE IP (IP de Colo CPE)** como la **Peer Address (Dirección del peer)** y la **Cloud Router IP (IP del enrutador en la nube)** como la **Local Address (Dirección local)**.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Configure el **Cloud Router BGP ASN** como el número de sistema autónomo (ASN) del peer de eBGP.

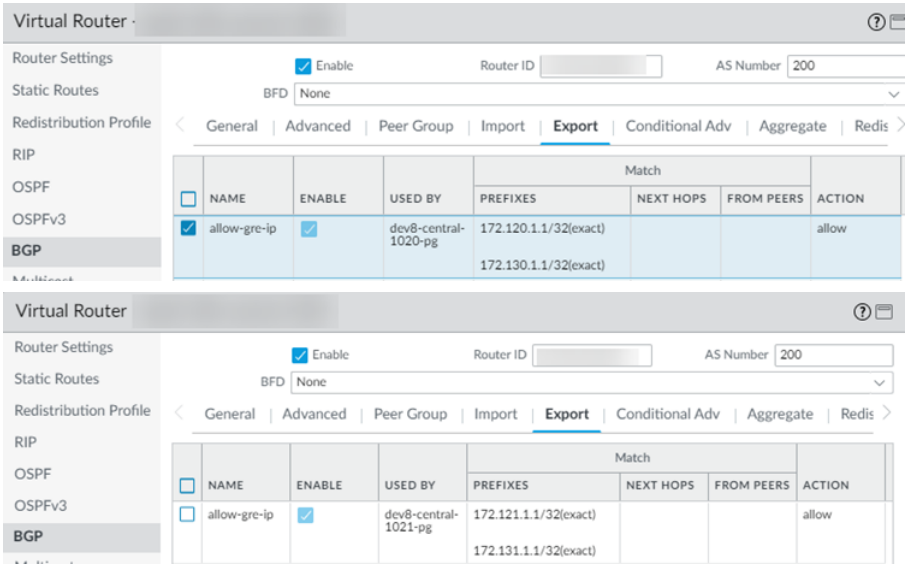
Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Peer Group (Grupo de peers)**, **Add (Añadir)** un grupo de peers y seleccione un **Peer AS (AS de peer)** de **16500**.



STEP 9 | Cree una política de exportación BGP que permita que solo la dirección IP GRE local se anuncie a la dirección IP del par del enrutador en la nube.

Debido a que los enrutadores en la nube solo pueden recibir un número limitada de rutas, es necesario crear políticas para que solo el enrutamiento entre las direcciones IP para los túneles GRE de conexión de servicio se envíe al enrutador en la nube.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Export (Exportar)**, **Add (Añadir)** una norma de exportación, **Match (Hacer coincidir)** las direcciones IP utilizadas como la dirección IP del peer y crear una **Action (Acción)** de **Allow (Permitir)**.



STEP 10 | Cree las conexiones del servicio de Colo-Connect.

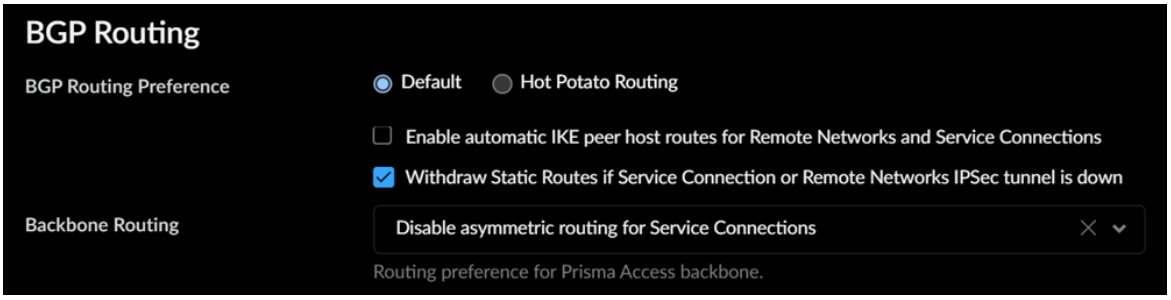
 ©2025 Palo Alto Networks, Inc.

Crear conexiones de servicio de Colo-Connect

Colo-Connect utiliza conexiones de servicio, pero difieren de Prisma Access Service Connections (Conexiones de servicio de Prisma Access) porque utilizan túneles GRE en lugar de túneles IPSec y siempre utilizan BGP para el enrutamiento. Para configurar las conexiones de servicio Colo-Connect, complete los siguientes pasos.

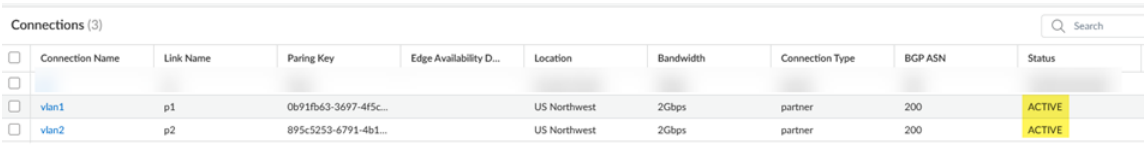
STEP 1 | Asegúrese de que Prisma Access retira rutas estáticas yendo a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)** > **Advanced Settings (Configuración avanzada)** y seleccionando **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Retirar rutas estáticas si el túnel IPSec de Conexión de servicio o Redes remotas está inactivo)**.

Seleccionar esta opción garantiza que, si el túnel GRE deja de funcionar, se retire la ruta estática utilizada por el túnel GRE.



STEP 2 | Vaya a los **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** > **Connections (Conexiones)** y asegúrese de que las conexiones estén en estado **Active (Activo)** mediante la comprobación de sus **Status (Estados)**.

Hasta que el **Status (Estado)** de la conexión no esté **Active (Activo)**, no se puede configurar conexiones de servicio.



STEP 3 | Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **(NGFW and Prisma Access (NGFW y Prisma Access)** y establezca el ámbito de la configuración en **Prisma Access**.

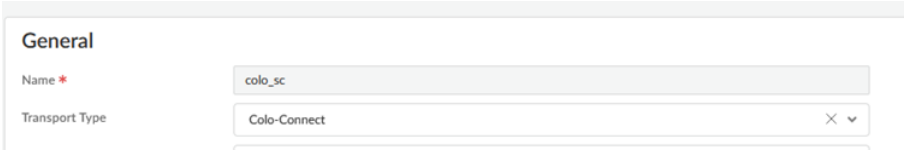
STEP 4 | Actualice el **Prisma Access Sync Status (Estado de sincronización de Prisma Access)** para que la configuración de Colo-Connect se aprovisione en el área de conexiones de servicio.

STEP 5 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Prisma Access Configuración)** > **Service Connection (Conexión de servicio)Add Service Connection (Añadir conexión**

 ©2025 Palo Alto Networks, Inc.

de servicio), asígnele un **Name (Nombre)** único y seleccione un **Transport Type (Tipo de transporte)** de **Colo-Connect**.

Asegúrese de que el nombre que introduzca tenga 31 caracteres o menos; la introducción de un nombre de 32 caracteres o más hace que el túnel se asigne incorrectamente en la infraestructura de Prisma Access.



STEP 6 | Seleccione dos conexiones para utilizar con las conexiones de servicio [**Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**).

Estas conexiones deben estar en dos zonas diferentes.



STEP 7 | Seleccione **Active (Activo)** o **Backup (Copia de seguridad)** para la **Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**

Utilice estas directrices al configurar conexiones de servicio:

- Puede configurar conexiones en estos modos:
  - **Active (Activo)/Active (Activo)**
  - **Active (Activo)/Backup (Copia de seguridad)**
  - **Backup (Copia de seguridad)/Active (Activo)**

  Configurar ambas conexiones en modo **Backup (Copia de seguridad)/Backup (Copia de seguridad)** no es válido y no es compatible.
- El ancho de banda de las conexiones debe ser el mismo para todos los modos.
- Las conexiones deben estar en zonas diferentes.
- El ancho de banda máximo que puede especificar para una conexión de servicio es 20 Gbps. Si especifica un **Bandwidth (Ancho de banda)** de **20 Gbps** para una conexión, no podrá usar esa conexión en una configuración **Active (Activa)/Active (Activa)** [debe configurarse como **Active (Activa)/Backup (Respaldo)**].
- No mezcle interconexiones dedicadas y de socios en la misma conexión de servicio y asegúrese de que las conexiones de servicio utilicen zonas diferentes. Esta tabla muestra las configuraciones permitidas y no permitidas para las conexiones de servicio, asumiendo

 ©2025 Palo Alto Networks, Inc.

que las zonas, las ubicaciones, el ancho de banda y las funciones siguen las pautas y los requisitos de conexión de servicio:

La conexión 1 pertenece a	La conexión 2 pertenece a	¿Configuración válida de la conexión de servicio Colo-Connect?
Conexión de socios 1	Conexión de socios 2	Sí
Conexión dedicada 1	Conexión dedicada 2	Sí
Conexión de socios 1	Conexión de socios 1	No
Conexión dedicada 1	Conexión dedicada 1	No
Conexión de socios	Conexión dedicada	No

STEP 8 | (Opcional y solo para implementaciones de enrutamiento de hot potato) Seleccione una conexión de servicio para usar como respaldo preferido, que es el **Backup SC (SC de respaldo)**, en la configuración de enrutamiento de hot potato.

Solo puede seleccionar una conexión de servicio que se haya configurado como conexión de servicio Colo-Connect. Prisma Access utiliza el Backup SC que usted seleccione como la conexión de servicio preferida en caso de un fallo de conexión. La selección de una conexión de servicio de respaldo puede evitar problemas de enrutamiento asimétrico si ha creado más de dos conexiones de servicio.

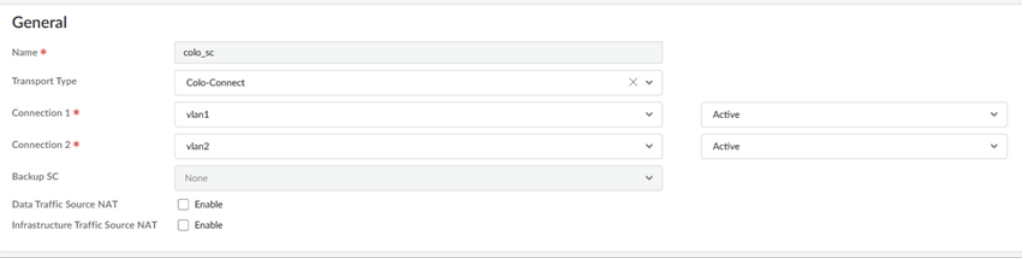
STEP 9 | (Opcional) Habilite NAT de origen para usuarios móviles: direcciones IP del grupo de GlobalProtect, direcciones IP en la subred de infraestructura o ambas.

Puede especificar una subred en una o más conexiones de servicio que se utilizan para el tráfico NAT entre Prisma Access Usuarios móviles y aplicaciones y recursos privados de GlobalProtect en un centro de datos.

- **Habilitar NAT de Origen de tráfico de datos**: realiza NAT en las direcciones del grupo de direcciones IP del usuario móvil para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncien y enruten en el centro de datos.
- **Habilitar NAT de origen de tráfico de infraestructura**: realiza NAT en las direcciones de la subred de infraestructura para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncian y enrutan en el centro de datos.
- **Grupo IP**: especifique el grupo de direcciones IP utilizado para realizar la NAT en el grupo de direcciones IP del usuario móvil, la subred de infraestructura o ambos. Utilice una subred IP privada (RFC 1918) o una subred adecuada que sea enrutable en su dominio de

 ©2025 Palo Alto Networks, Inc.

enrutamiento y que no se superponga con el grupo de direcciones IP de Usuarios móviles—GlobalProtect o la Subred de infraestructura. Introduzca una subred entre /25 y /32.



STEP 10 | En el área **GRE and BGP (GRE y BGP)**, configure el túnel GRE y la configuración BGP para la conexión del servicio.

BGP siempre está configurado en **Enable (Habilitar)**.

1. (Opcional) Seleccione una de las siguientes opciones:

   - Para añadir una comunidad **no-export (sin exportación)** para nodos de acceso corporativo (conexiones de servicio) a los prefijos salientes de los pares eBGP en el equipo de las instalaciones del cliente (CPE), configure **Add no-export community (Añadir comunidad sin exportación)** en **Enabled Out (Habilitado de salida)**. Esta capacidad está **Disabled (Deshabilitada)** de manera predeterminada.

     No utilice esta capacidad en el modo de enrutamiento hot potato.

   - Para reducir el número de anuncios de subred IP de usuarios móviles a través de BGP a los equipos de las instalaciones del cliente (CPE) resumiéndolos, seleccione **Summarize Mobile User Routes before advertising (Resumir rutas de usuarios móviles antes de anunciar)**.

     Por defecto, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de subredes /24; si los resume, Prisma Access anuncia el grupo en función de la subred que especificó. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

     Si tiene habilitado el enrutamiento de hot potato y habilita el resumen de rutas, Prisma Access ya no se antepone a los AS-PATH, lo que podría provocar un enrutamiento asimétrico. Asegúrese de que el tráfico de retorno desde el centro de datos o la sede central haya garantizado un retorno simétrico antes de habilitar el resumen de rutas con el enrutamiento de hot potato.

   - Para evitar que el peer de BGP de Prisma Access reenvíe rutas a la red de su organización. **Don't Advertise Prisma Access Routes (No anuncie las rutas de Prisma Access)**

     Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de

 ©2025 Palo Alto Networks, Inc.

servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.

- ¿Qué es el ajuste "Intercambio de ruta"?

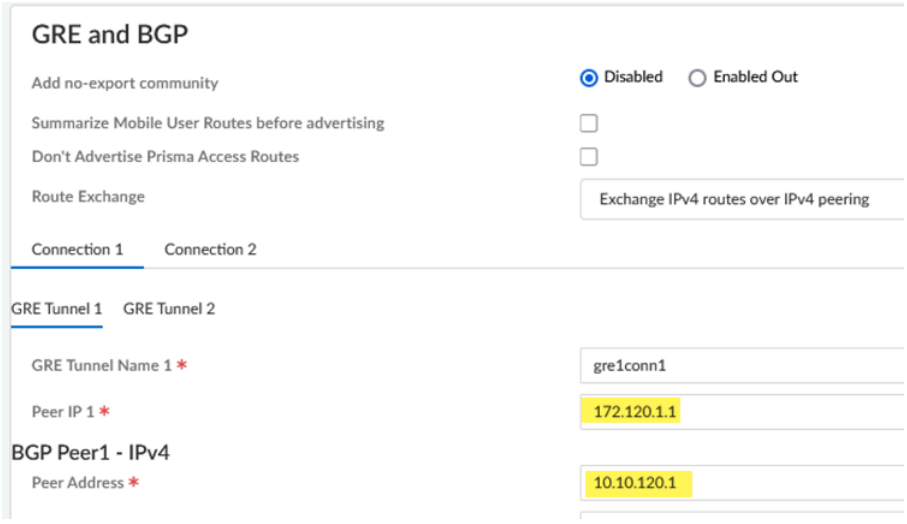
2. Configure el enrutamiento para la conexión de servicio utilizando túneles GRE.
3. Desde Strata Cloud Manager, vuelva a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connection (Conexión de servicio)** un túnel GRE para la **Connection 1 (Conexión 1)** introduciendo un **GRE Tunnel Name 1 (Nombre de túnel GRE 1)** y una **Peer IP 1 (IP de peer 1)** para la **Connection 1 (Conexión 1)** y, si se requieren más de 10 Gbps de ancho de banda, introduciendo el **GRE Tunnel Name 2 (Nombre de túnel GRE 2)** y la **Peer IP 2 (IP de peer 2)** para el segundo túnel para la Conexión 1; luego, cree un túnel GRE para la **Connection 2 (Conexión 2)** repitiendo estos mismos pasos.

   Cada par de túneles GRE en una conexión admite un máximo de 10 Gbps de ancho de banda. Si necesita más de 10 Gbps de ancho de banda, configure dos túneles por conexión. Por ejemplo:

   Para la IP del peer, introduzca la dirección IP GRE del enrutador local en el Colo.

   Utilice direcciones IPv4 para los valores BGP; no se admite IPv6.
4. Introduzca la **Peer Address (Dirección del peer)** y la **Local Address (Dirección local)** para el peer de BGP 1 y, si se requiere una segunda para la conexión 1, para el peer de BGP 2.

   Para **Peer Address (Dirección de pares)**, introduzca la dirección IP del peer BGP del enrutador Colo; para **Local Address (Dirección local)**, introduzca la dirección que se utilizará para el establecimiento de la red BGP a través del túnel GRE.
5. (Opcional) Para configurar un secreto BGP, introduzca los valores **Secret (Secreto)** y **Confirm Secret (Confirmar secreto)**.

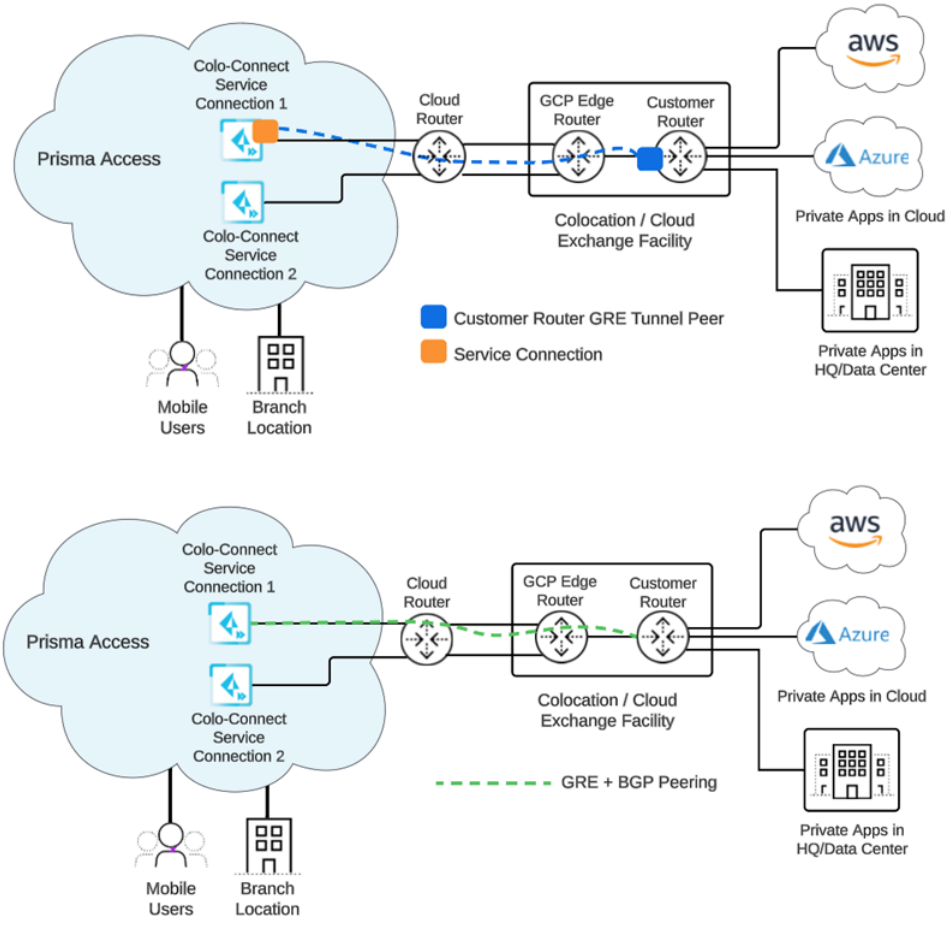


 ©2025 Palo Alto Networks, Inc.

STEP 11 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios de configuración, asegurándose de que **Colo-Connect** esté seleccionado en el **Push Scope (Ámbito de envío)**.

Configurar el enrutamiento para la conexión de servicio mediante túneles GRE

El enrutador Colo anuncia la dirección IP de su peer del túnel GRE al enrutador en la nube y obtiene la subred para el túnel GRE del enrutador en la nube. Cuando configuró por primera vez el enrutamiento eBGP a través de la VLAN en el enrutador de cliente, anunció la accesibilidad local para los túneles GRE. Una vez que el enrutador en la nube y el enrutador Colo se anuncian y aprenden las rutas para la subred Colo y las direcciones IP GRE locales entre sí, los túneles GRE utilizados por la conexión de servicio se vuelven activos.



Para configurar el enrutamiento y añadir túneles GRE a las conexiones de servicio, complete los siguientes pasos.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Tome nota de las direcciones IP que utilizará para la **Peer Address (Dirección del peer)** y la **Local Address (Dirección local)** para el peer de BGP 1 y, si se requiere un segundo para la conexión 1, el peer de BGP 2.

Los siguientes ejemplos utilizan las siguientes direcciones locales y de peer:

- **Peer Address (Dirección del peer)**: 10.10.120.0 y 10.10.130.1 para la conexión 1, 10.10.120.2 y 10.10.130.2 para la conexión 2
- **Local Address (Dirección local)**: 10.10.120.2 y 10.10.130.2 para la conexión 1, 10.10.121.2 y 10.10.131.2 para la conexión 2

STEP 2 | Tome nota de las direcciones IP que utilizará para la **Peer IP 1 (dirección IP de peer 1)** y, si es necesario, la dirección **IP Peer 2 (dirección IP de peer 2)** en las conexiones de servicio.

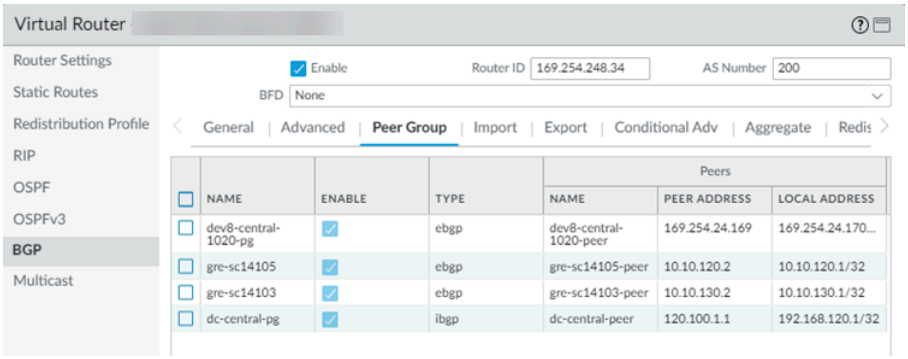
Utilice estas direcciones IP para crear una política de denegación que impida que la dirección IP GRE local se anuncie a la conexión del servicio Colo-Connect.

Todos los ejemplos de este documento utilizan estas direcciones IP:

- 172.120.1.1 para Conexión 1
- 172.121.1.1 para Conexión 2

STEP 3 | Configurar grupos de peers para los pares y las direcciones IP locales.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Peer Group (Grupo de peers)** y escriba la dirección del peer como la **Peer Address (Dirección del peer)** y la **Local Address (Dirección local)** como la **Local Address (Dirección local)**.



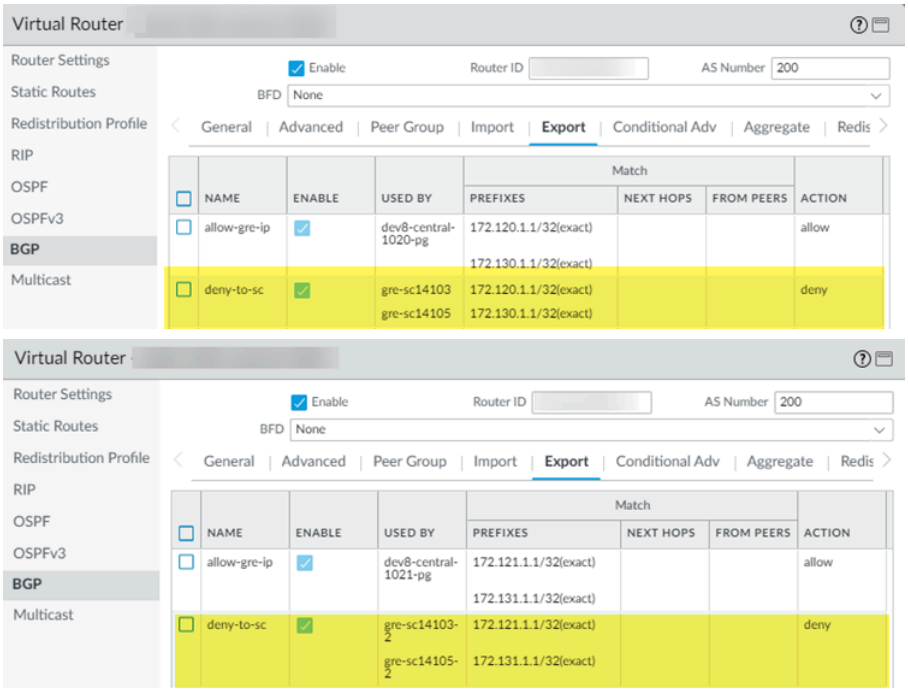
STEP 4 | Cree una política de exportación BGP para denegar las direcciones IP de los peers que configuró (172.120.1.1, 172.130.1.1, 172.121.1.1 y 172.131.1.1) y aplicarlas a los grupos de peers que creó.

Esta política de exportación coloca una regla DENY (DENEGAR) en las direcciones IP de los peers del túnel GRE local y permite que todas las demás rutas se anuncien a la conexión de servicio.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Export (Exportar)**, **Add (Añadir)** una norma de exportación, **Match (Hacer coincidir)** las

 ©2025 Palo Alto Networks, Inc.

direcciones IP utilizadas como la dirección IP del peer y crear una **Action (Acción)** de **Deny (Denegar)**.



Incrementar o disminuir el ancho de banda de una conexión de servicio Colo-Connect

Cuando configura conexiones de servicio, configura el ancho de banda en función de las conexiones (adjuntos de VLAN) asociadas a él. Asigna dos conexiones por conexión de servicio y luego asigna uno o dos túneles GRE por conexión.

Si bien cada conexión de servicio Colo-Connect admite un máximo de 20 Gbps, cada túnel GRE en la conexión de servicio admite 10 Gbps. Por este motivo, es posible que tenga que añadir o eliminar los túneles GRE en la conexión del servicio Colo-Connect para cambiar el ancho de banda total en un enlace y hacer que el ancho de banda de la conexión del servicio supere o deje de ser de 10 Gbps.

Aumentar el ancho de banda de una conexión de servicio Colo-Connect

Para aumentar el ancho de banda de una conexión de servicio existente por encima de 10 Gbps, complete los siguientes pasos:

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect**.

STEP 2 | Seleccione la opción **Link Name (Nombre del enlace)** asociado a la conexión de servicio.

STEP 3 | Aumenta el **Bandwidth (Ancho de banda)** del enlace (interconexión).

STEP 4 | **Push Config (Enviar configuración)**.

STEP 5 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connection (Conexión del servicio)**.

STEP 6 | Añada el túnel GRE adicional a la conexión del servicio Colo-Connect.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | **Push Config (Enviar configuración)**.

STEP 8 | Añada las direcciones IP locales (pares) de GRE a sus políticas de exportación para el enrutamiento eBGP de VLAN y el enrutamiento de conexión de servicio para los túneles GRE.

Reducir el ancho de banda de una conexión de servicio Colo-Connect

Para reducir el ancho de banda de una conexión de servicio existente por encima de 10 Gbps, complete los siguientes pasos:

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect** .

STEP 2 | Seleccione la opción **Link Name (Nombre del enlace)** asociado a la conexión de servicio.

STEP 3 | Disminuya el **Bandwidth (Ancho de banda)** del enlace (interconexión).

STEP 4 | **Push Config (Enviar configuración)**.

No es necesario volver a configurar la conexión de servicio para eliminar el túnel GRE adicional; Prisma Access detecta y reduce el ancho de banda del vínculo y quita el túnel adicional cuando se confirman y envían los cambios en el ámbito de inserción de la conexión de servicio.

Eliminar una conexión de Colo-Connect

Para eliminar una conexión de Colo-Connect, siga el orden inverso de su configuración completando los siguientes pasos:

STEP 1 | Para eliminar las conexiones de servicio asociadas con la conexión, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)**, seleccione la conexión de servicio y **Delete (Eliminar)** para eliminarla.

STEP 2 | **Push Config (Enviar configuración)**.

STEP 3 | Elimine las conexiones de Colo-Connect asociadas con la conexión yendo a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Colo-Connect**, seleccionando el **Connection Name (Nombre de conexión)** en la sección **Onboarding (Incorporación)** y elija **Delete (Eliminar)** para eliminarla.

STEP 4 | Elimine el enlace Colo-Connect seleccionando el **Link Name (Nombre del enlace)** y **Delete (Eliminar)**.

STEP 5 | Elimine las direcciones IP locales (peers) de GRE a sus políticas de exportación para el enrutamiento eBGP de VLAN y el enrutamiento de conexión de servicio para los túneles GRE.

Configurar Prisma Access Colo-Connect (Panorama)

 ©2025 Palo Alto Networks, Inc.

Configure Prisma Access Colo-Connect: implementaciones que utilizan interconexiones de socios

Para configurar Prisma Access Colo-Connect mediante una interconexión de socio, complete estos pasos.

STEP 1 | Cree subredes para sus conexiones Colo-Connect.

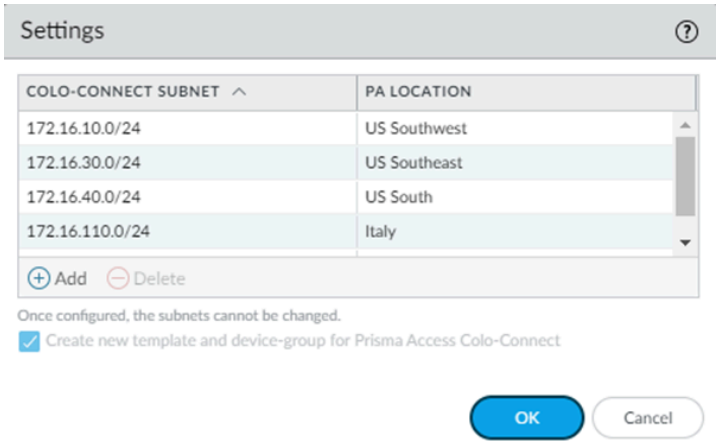
Las subredes que se crean aquí se utilizan en las conexiones y conexiones de servicio que se crean en los pasos posteriores.

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** y haga clic en el icono de engranaje para editar la configuración.
2. **Add (Añadir)** un **Colo-Connect Subnet (Subred Colo-Connect)** y seleccione una ubicación de Prisma Access (**PA Location (Ubicación de PA)**) para ello.

   Introduzca una subred mínima de /28.
3. (Opcional) Si planifica crear instancias de Colo-Connect para más de una ubicación, añada más subredes por ubicación.

   Puede configurar una subred por ubicación.
4. Seleccione **Create new templates and device-group for Prisma Access Colo-Connect (Crear nuevas plantillas y grupos de dispositivos para Prisma Access Colo-Connect)**.

   La primera vez que configure una implementación de Colo-Connect, active esta casilla de verificación para que se creen plantillas y grupos de dispositivos (Colo_Connect_Template y Colo_Connect_Device_Group, respectivamente) para Colo-Connect. Después de crear estas plantillas y grupos de dispositivos, esta casilla de verificación aparece atenuada.



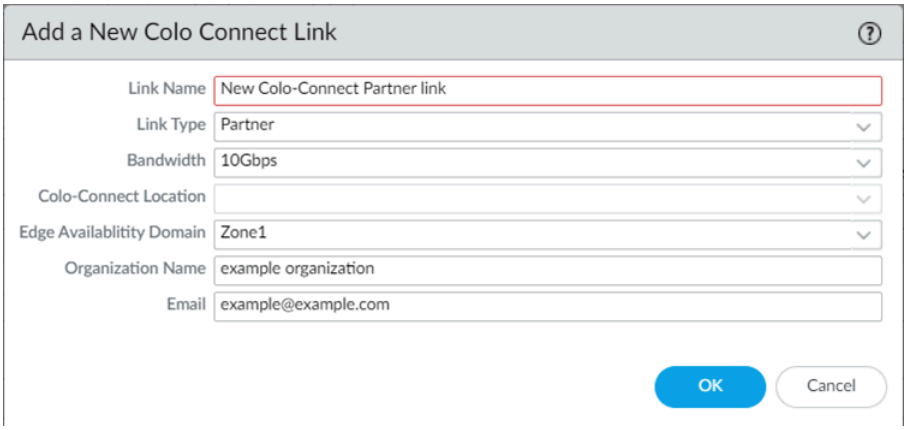
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada un nuevo enlace Colo-Connect (también conocido como *interconexión*).

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** > **Colo-Connect Link (Enlace Colo Connect)** y seleccione **Add (Añadir)** un enlace Colo-Connect.
2. Dé al enlace un **Link Name (Nombre de enlace)** único.
3. Seleccione una interconexión de **Partner (Socio)**.

   No es necesario que introduzca un **VLAN ID (ID de VLAN)**, su Colo proporciona uno cuando utiliza la clave de emparejamiento para completar la configuración de su conexión VLAN.
4. Especifique los parámetros restantes del enlace Colo-Connect.
   - Seleccione una de las siguientes opciones: **10 Gbps** o **20 Gbps** para el **Bandwidth (Ancho de banda)**.

     No puede cambiar el ancho de banda de un enlace de interconexión dedicado después de especificarlo y confirmar e insertar los cambios.
   - Seleccione **Zone1 (Zona1)** o **Zone2 (Zona2)** para el **Edge Availability Domain (Dominio de disponibilidad de borde)**. Tome este valor de la GCP zone (Zona de GCP) utilizada para su dominio de disponibilidad de borde.
   - Introduzca el **Organization Name (Nombre de la organización)** que se utilizará para este enlace.
   - Introduzca el **Email (Correo electrónico)** a utilizar para este enlace. Cualquier dirección de correo electrónico es aceptable.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cree las conexiones [también conocidas como *VLAN attachments (Adjuntos VLAN)*] para Colo-Connect.

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** > **Onboarding (Incorporación)** y **Add (Añadir)** para añadir una nueva conexión.
2. Configure la configuración de conexión.
   - Introduzca un **Name (Nombre)** único para la conexión.
   - Seleccione un **Link Name (Nombre de enlace)** de los enlaces que configuró en un paso anterior.
   - Seleccione un **Bandwidth (Ancho de banda)** para la conexión.

     Puede seleccionar entre **1 Gbps**, **2 Gbps**, **5 Gbps**, **10 Gbps**o **20 Gbps**.

     Si configura varias conexiones para una interconexión, asegúrese de que el ancho de banda total de las conexiones no exceda el ancho de banda de la interconexión. Por ejemplo, dada una interconexión de socio de 10 Gbps, puede configurar 10

 ©2025 Palo Alto Networks, Inc.

conexiones de 1 Gbps cada una, pero no supere los 10 Gbps en total para todas las conexiones.

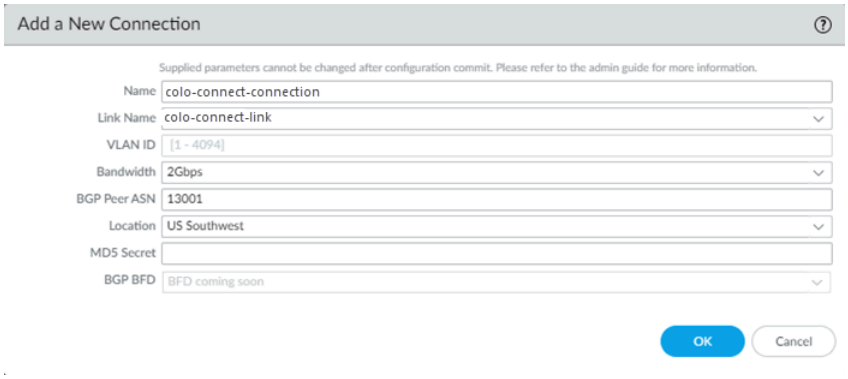
Si su implementación requiere más de 16 conexiones, comuníquese con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de SRE para atender la solicitud.

- Introduzca un **BGP Peer ASN (ASN de peer BGP)**.

  Introduzca el número de Sistema Autónomo (AS) para el enrutador local del cliente en el Colo. El rango está entre 1 y 4294967295.
- Seleccione la **Location (Ubicación)** de los nombres de conexión que creó en un paso anterior.

  Ya debe haber añadido una subred para cualquier ubicación que especifique.
- (Opcional) Introduzca el **MD5 Secret (Secreto MD5)**de BGP.

*Ignore el campo **BGP BFD**; está reservado para una futura versión de Colo-Connect.*



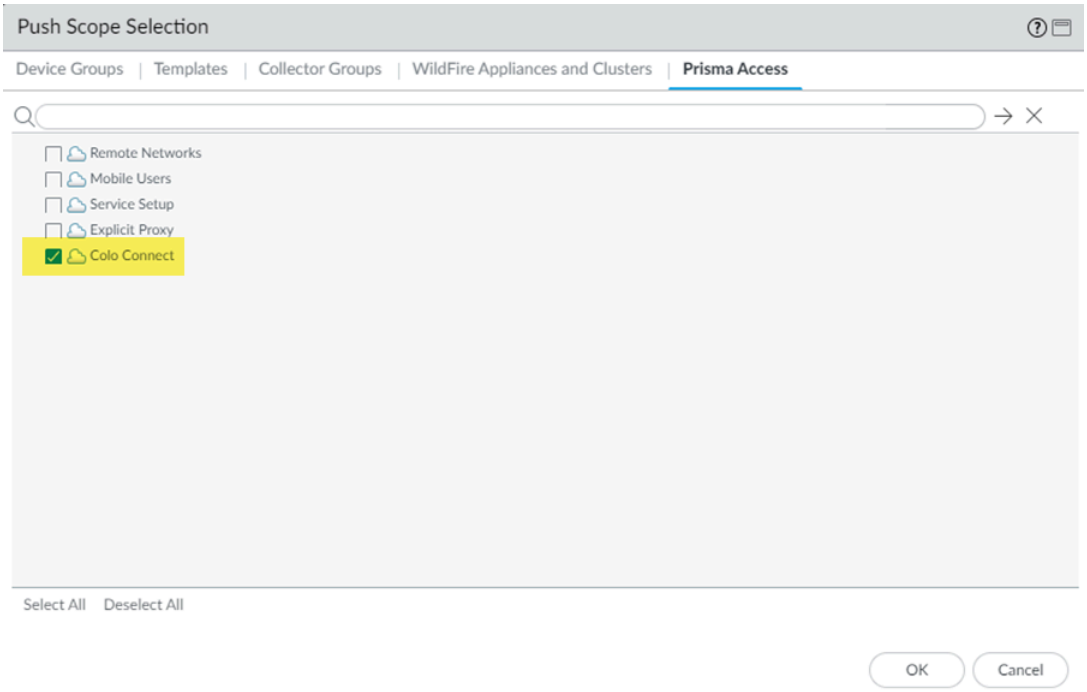
3. Continúe creando conexiones hasta completar.

   Debe crear dos conexiones. Ambas conexiones deben estar en la misma región y cada conexión debe estar en una zona separada. Estas conexiones se utilizan en las conexiones de servicio que se crean en un paso posterior.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Confirme y envíe sus cambios.

1. Vaya a **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Seleccione **Edit Selections (Editar selecciones)** y asegúrese de que Colo-Connect esté seleccionado en el ámbito de inserción.



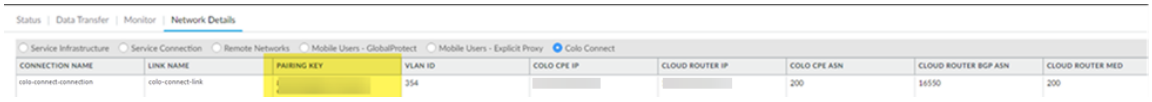
3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 5 | Recupere la **Pairing Key (Clave de emparejamiento)** y complete la configuración de interconexión de su socio en GCP.

Utilice esta clave de emparejamiento cuando configure la interconexión de socios en el Colo.

Cuando se incorpora por primera vez a una nueva conexión, el estado en el área de incorporación de Colo-Connect muestra un **Status (Estado)** de **PENDING_PARTNER** y un **BGP Status (Estado de BGP)** de **DOWN (CAÍDO)**. Para llevar el estado de la conexión a **ACTIVE (ACTIVO)**, recupere la clave de emparejamiento e introduzca en la conexión en el Colo.

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Colo Connect** y copie el archivo **Pairing Key (Clave de emparejamiento)**.



2. Cree una nueva conexión VLAN en el Colo (por ejemplo, Equinix).
3. Pegue la clave de emparejamiento en la VLAN Colo.

   GCP detecta cuando se consume la clave de emparejamiento, cambia el estado de la VLAN a **ACTIVE (ACTIVA)** y genera la dirección IP BGP para que la configure en su enrutador local en el Colo. Estas acciones inician el enrutamiento eBGP a través de la VLAN entre el enrutador Colo y el enrutador en la nube de GCP.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Creación de enrutamiento eBGP en el enrutador del cliente (Colo) para la conexión Colo-Connect.

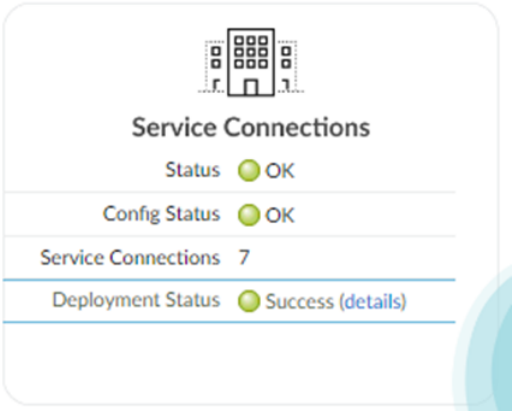
Debe configurar el emparejamiento BGP para garantizar la conectividad entre el enrutador del cliente. y el enrutador en la nube.

STEP 7 | Configurar las conexiones de servicio para utilizar con Colo-Connect.

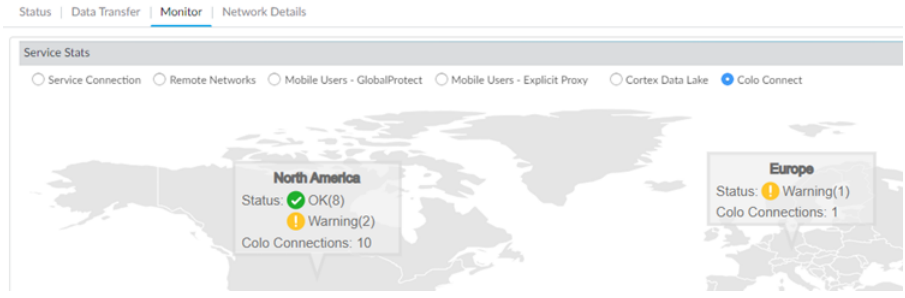
STEP 8 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios de configuración, asegurándose de que **Colo-Connect** esté seleccionado en el **Push Scope (Ámbito de envío)**.

STEP 9 | Verifique el estado de las conexiones Colo-Connect.

1. Para verificar el estado de una conexión de servicio utilizada por una conexión Colo-Connect, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > > **Colo Connect** > **Monitor (Supervisar)**



2. Coloque el cursor sobre una región que tenga una conexión Colo-Connect implementada.
   - Si la conexión Colo-Connect y el enrutamiento BGP están activos, el Estado muestra **OK (Aceptar)**.
   - Si la conexión Colo-Connect está activa pero el enrutamiento BGP no está activo, se muestra el estado **Warning (Advertencia)**.
   - Si la conexión Colo-Connect y el enrutamiento BGP están inactivos, el Estado muestra **Down (Inactivo)**.
   - Si la conexión Colo-Connect está inactiva pero el enrutamiento BGP está activo, el Estado muestra **Error**.



3. Para obtener más información, haga clic en el cuadro de la región y vea la información en la pestaña **Status (Estado)**.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Verifique los detalles de la red, incluida la clave de emparejamiento, de las conexiones Colo-Connect yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Colo Connect** y visualizando la información en los siguientes campos.

Configurar Prisma Access Colo-Connect: implementaciones que utilizan interconexiones dedicadas

Para configurar Prisma Access Colo-Connect usando una interconexión dedicada, complete estos pasos.

STEP 1 | Cree subredes para sus conexiones Colo-Connect.

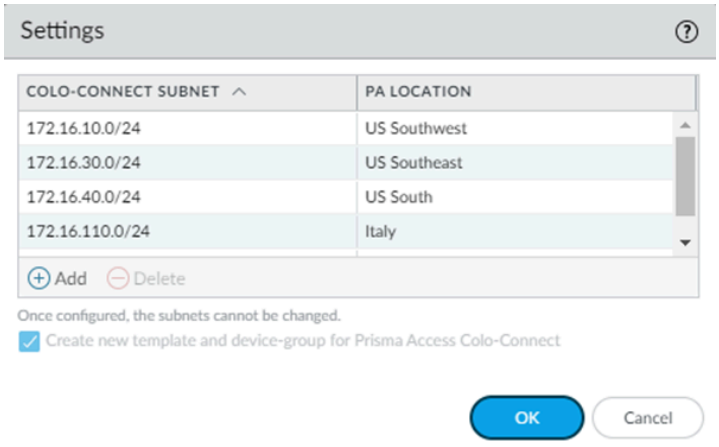
Las subredes que se crean aquí se utilizan en las conexiones y conexiones de servicio que se crean en los pasos posteriores.

1. Desde el Panorama que gestiona Prisma Access, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** y haga clic en el icono de engranaje para editar la configuración.
2. **Add (Añadir)** un **Colo-Connect Subnet (Subred Colo-Connect)** y seleccione una ubicación de Prisma Access (**PA Location (Ubicación de PA)**) para ello.

   Introduzca una subred mínima de /28.
3. (Opcional) Si planifica crear instancias de Colo-Connect para más de una ubicación, añada más subredes por ubicación.

   Puede configurar solo una subred por ubicación.
4. Seleccione **Create new templates and device-group for Prisma Access Colo-Connect (Crear nuevas plantillas y grupos de dispositivos para Prisma Access Colo-Connect)**.

   La primera vez que configure una implementación de Colo-Connect, active esta casilla de verificación para que se creen plantillas y grupos de dispositivos (Colo_Connect_Template y Colo_Connect_Device_Group, respectivamente) para Colo-Connect. Después de crear estas plantillas y grupos de dispositivos, esta casilla de verificación aparece atenuada.



 ©2025 Palo Alto Networks, Inc.

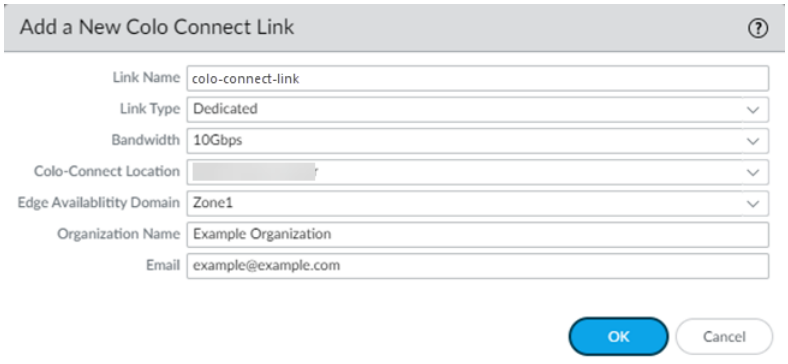
STEP 2 | Añada un nuevo enlace Colo-Connect (también conocido como *interconexión*).

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** > **Colo-Connect Link (Enlace Colo Connect)** y seleccione **Add (Añadir)** un enlace Colo-Connect.
2. Dé al enlace un **Link Name (Nombre de enlace)** único.
3. Seleccione una interconexión **Dedicated (Dedicada)**.
4. Especifique los parámetros restantes del enlace Colo-Connect.
   - Seleccione una de las siguientes opciones: **10 Gbps** o **20 Gbps** para el **Bandwidth (Ancho de banda)**.

     Si selecciona 20 Gbps, debe añadir el enlace de interconexión dedicada en dos enlaces de 10 Gbps utilizando LACP.

     No puede cambiar el ancho de banda de un enlace de interconexión dedicado después de especificarlo y confirmar e insertar los cambios.
   - Seleccione una **Colo-Connect Location (Ubicación de Colo-Connect)** de la lista desplegable.

     Asegúrese de seleccionar la misma ubicación que utilizó para la interconexión dedicada.
   - Seleccione **Zone1 (Zona1)** o **Zone2 (Zona2)** para el **Edge Availability Domain (Dominio de disponibilidad de borde)**. Tome este valor de la GCP zone (Zona de GCP) utilizada para su dominio de disponibilidad de borde.
   - Introduzca el **Organization Name (Nombre de la organización)** que se utilizará para este enlace.
   - Introduzca el **Email (Correo electrónico)** donde desea recibir los detalles del LOA-CFA del proveedor de la nube.
     - GCP utiliza este correo electrónico para enviar la Carta de autorización y Asignación de facilidad de conexión (LOA-CFA). Asegúrese de que el LOA-CFA se envíe a su proveedor de Colo, para que puedan comenzar a instalar sus conexiones.



 ©2025 Palo Alto Networks, Inc.

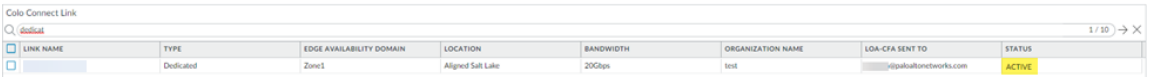
STEP 3 | Una vez creada la conexión dedicada, la instalación de Colo prueba sus conexiones y le informa de que han sido probadas y están listas para usar.

No se requiere configuración de Prisma Access para este paso. No cree las conexiones Colo-Connect en Prisma Access hasta que las instalaciones de Colo le informen que se han sometido a pruebas.

STEP 4 | Cree las conexiones [también conocidas como *VLAN attachments (Adjuntos VLAN)*] para Colo-Connect.

1. Asegúrese de que el estado del enlace dedicado sea Activo yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** > **Colo Connect Link (Enlace Colo Connect)**.

   Hasta que el estado del enlace dedicado esté Activo, no puede crear enlaces Colo-Connect.

2. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect** > **Onboarding (Incorporación)** y **Add (Añadir)** para añadir una nueva conexión.
3. Configure la configuración de conexión.
   - Introduzca un **Name (Nombre)** único para la conexión.
   - Seleccione un **Link Name (Nombre de enlace)** de los enlaces que configuró en un paso anterior.
   - (Opcional) Introduzca una **ID VLAND (ID de VLAN)** para la conexión.

     Los ID de VLAN las genera el proveedor de interconexión (GCP) si no introduce un valor manualmente.
   - Seleccione un **Bandwidth (Ancho de banda)** para la conexión.

     Puede seleccionar entre **1 Gbps**, **2 Gbps**, **5 Gbps**, **10 Gbps**o **20 Gbps**.

     Si configura varias conexiones para una interconexión, asegúrese de que el ancho de banda total de las conexiones no exceda el ancho de banda de la interconexión. Por ejemplo, dada una interconexión dedicada de 20 Gbps, puede configurar 10

 ©2025 Palo Alto Networks, Inc.

conexiones de 2 Gbps cada una, pero no supere los 20 Gbps en total para todas las conexiones.

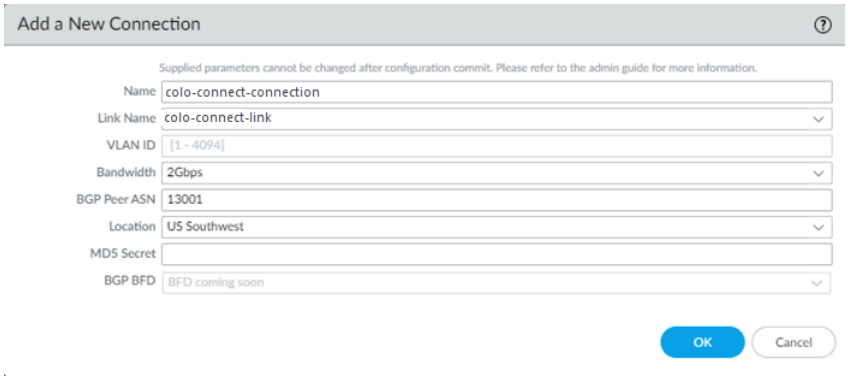
- Introduzca un **BGP Peer ASN (ASN de peer BGP)**.

  Introduzca el número de Sistema Autónomo (AS) para el enrutador local del cliente en el Colo. El rango está entre 1 y 4294967295.

- Seleccione la **Location (Ubicación)** de los nombres de conexión que creó en un paso anterior.

  Ya debe haber añadido una subred para cualquier ubicación que especifique.

- (Opcional) Introduzca el **MD5 Secret (Secreto MD5)**de BGP.



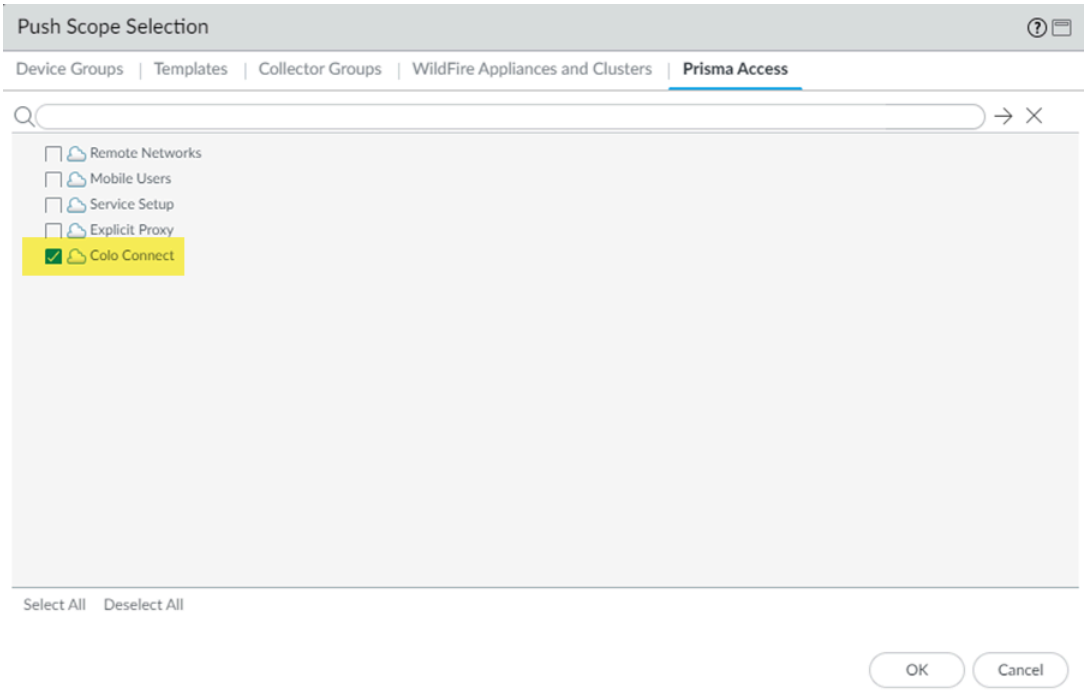
4. Continúe creando conexiones hasta completar.

   Debe crear dos conexiones. Ambas conexiones deben estar en la misma región y cada conexión debe estar en una zona separada. Estas conexiones se utilizan en las conexiones de servicio que se crean en un paso posterior.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Confirme y envíe sus cambios.

1. Vaya a **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Seleccione **Edit Selections (Editar selecciones)** y asegúrese de que Colo-Connect esté seleccionado en el ámbito de inserción.



3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 6 | Configure el enrutamiento eBGP en el enrutador de cliente.

Debe configurar el emparejamiento BGP para garantizar la conectividad entre el enrutador del cliente,

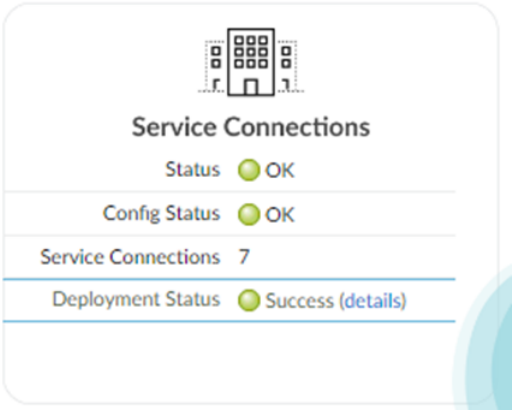
STEP 7 | Configurar las conexiones de servicio para utilizar con Colo-Connect.

STEP 8 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios de configuración, asegurándose de que **Colo-Connect** esté seleccionado en el **Push Scope (Ámbito de envío)**.

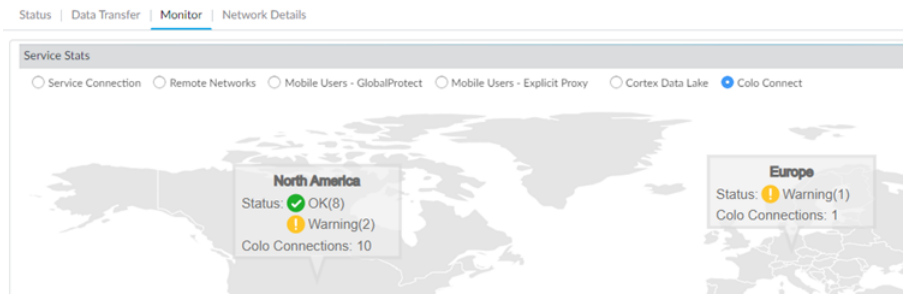
©2025 Palo Alto Networks, Inc.

STEP 9 | Verifique el estado de las conexiones Colo-Connect.

1. Para verificar el estado de una conexión de servicio utilizada por una conexión Colo-Connect, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > > **Colo Connect** > **Monitor (Supervisar)**.



2. Coloque el cursor sobre una región que tenga una conexión Colo-Connect implementada.
   - Si la conexión Colo-Connect y el enrutamiento BGP están activos, el Estado muestra **OK (Aceptar)**.
   - Si la conexión Colo-Connect está activa pero el enrutamiento BGP no está activo, se muestra el estado **Warning (Advertencia)**.
   - Si la conexión Colo-Connect y el enrutamiento BGP están inactivos, el Estado muestra **Down (Inactivo)**.
   - Si la conexión Colo-Connect está inactiva pero el enrutamiento BGP está activo, el Estado muestra **Error**.

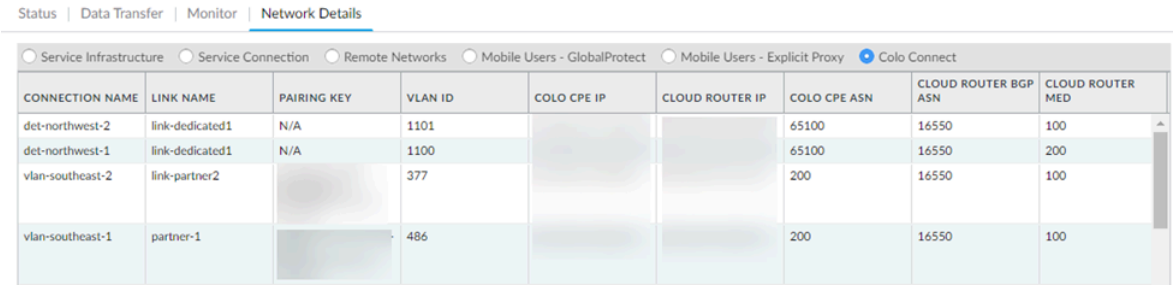


3. Para obtener más información, haga clic en el cuadro de la región y vea la información en la pestaña **Status (Estado)**.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Para verificar los detalles de red de las conexiones Colo-Connect, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Colo Connect** y vea los detalles.

En el caso de los enlaces dedicados, la **Pairing Key (Clave de emparejamiento)** se muestra como **N/A (N/D)**.



Configurar el enrutamiento eBGP de VLAN en el enrutador del cliente

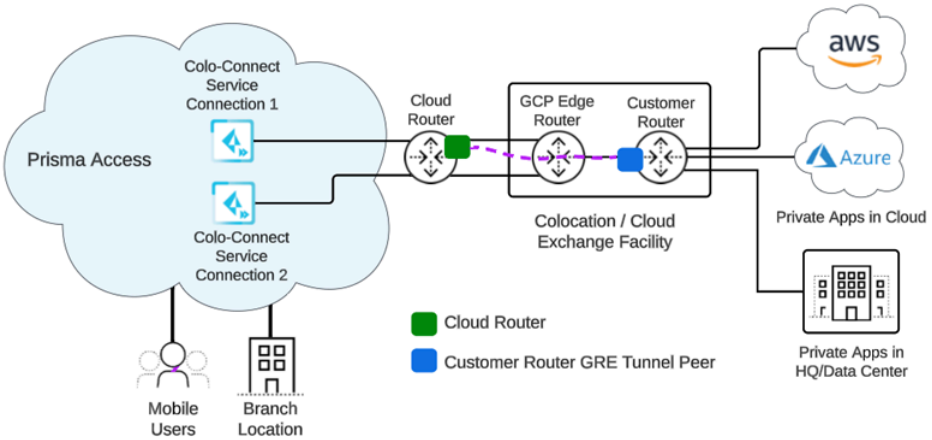
GCP crea direcciones IP para el enrutador del cliente (Colo) y el enrutador en la nube durante estas etapas de su implementación:

- Para las interconexiones de socios, GCP crea las direcciones IP después de que su Colo consume la clave de emparejamiento (por ejemplo, Equinix).
- Para las interconexiones dedicadas, GCP crea las direcciones IP después de que usted incorpora sus conexiones Colo-Connect (archivos adjuntos de VLAN) y confirma y envía sus cambios.

Para garantizar un enrutamiento correcto, debe:

- Configure la dirección IP del enrutador Colo (la **Colo CPE IP** en la UI de Prisma Access) como la dirección IP de VLAN local y la dirección IP eBGP local
- Configure la dirección IP del enrutador en la nube [**Cloud Router IP (IP del enrutador en la nube)**] como la dirección del par eBGP en su router Colo.

Una vez completado, eBGP estará configurado para la conexión (conexión VLAN) entre el enrutador Colo y el enrutador en la nube.



 ©2025 Palo Alto Networks, Inc.

La creación de esta ruta es el primer paso para configurar el enrutamiento del túnel GRE. El enrutamiento del túnel GRE se completa cuando se configuran túneles GRE durante la configuración de la conexión de servicio.

Utilice los siguientes pasos para configurar el enrutamiento entre Colo y el enrutador en la nube.

STEP 1 | Desde el Panorama que gestiona Prisma Access, cree las subredes, los vínculos y las conexiones y seleccione **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios.

Utilice el flujo de trabajo específico para su tipo de interconexión (ya sea de Socio o Dedicada). Para las interconexiones de socio, asegúrese de pegar la clave de emparejamiento en la VLAN de Colo.

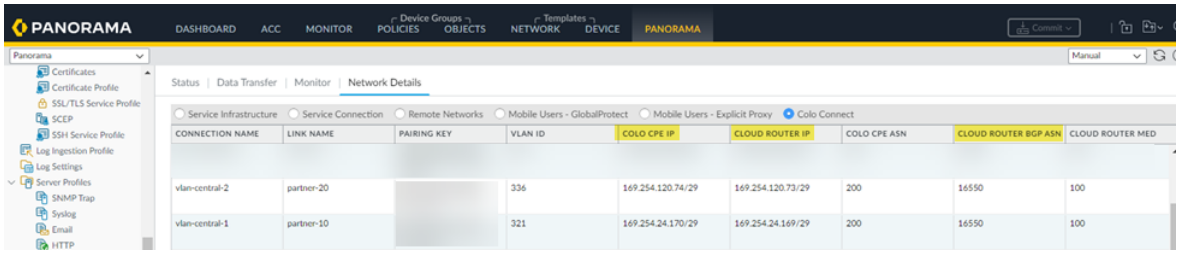
STEP 2 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Colo Connect**.

STEP 3 | Tome nota de los siguientes elementos de conexión:

- **Colo CPE IP**
- **IP del enrutador en la nube**
- **Cloud Router ASN BGP**

En el siguiente ejemplo:

- Para la conexión vlan-central-1, la **Colo CPE IP (IP de Colo CPE)** es 169.254.24.170/29, la **Cloud Router IP (IP del enrutador en la nube)** es 169.254.24.169/29 y el **Cloud Router BGP ASN (ASN BGP del enrutador en la nube)** es 16550.
- Para la conexión vlan-central-2, la **Colo CPE IP (IP de Colo CPE)** es 169.254.120.74/29, la **Cloud Router IP (IP del enrutador en la nube)** es 169.254.120.73/29 y el **Cloud Router BGP ASN (ASN BGP del enrutador en la nube)** es 16550
- .

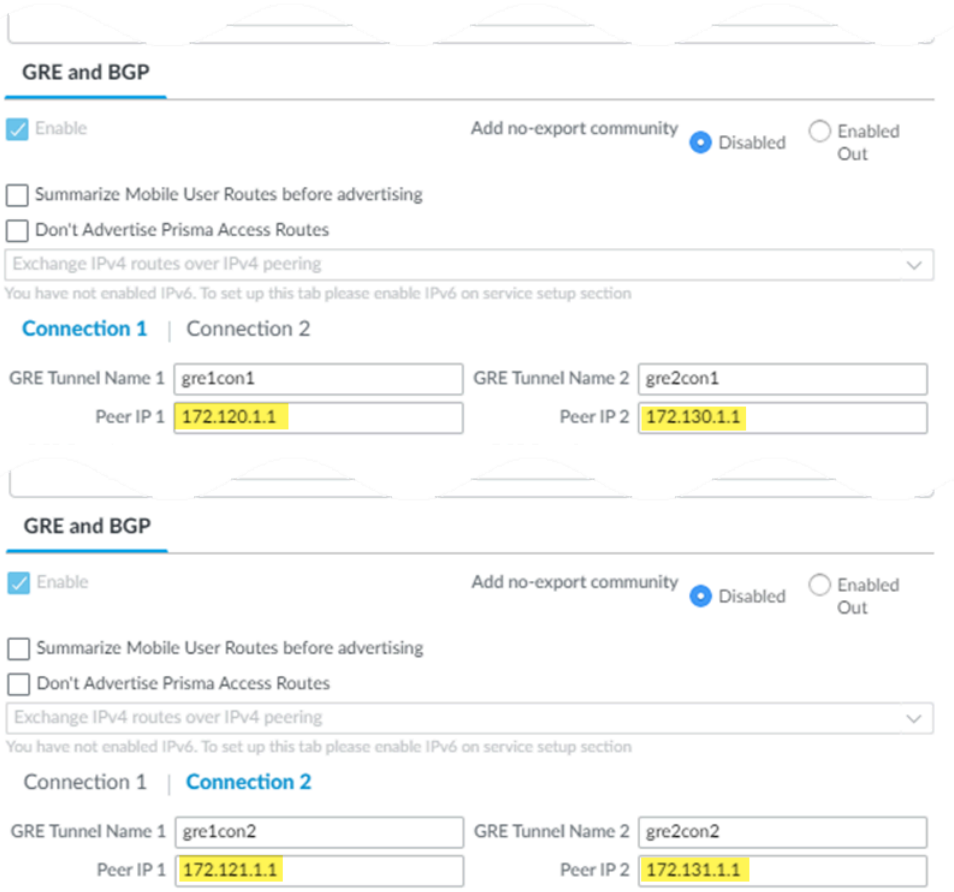


STEP 4 | Determine las direcciones IP que utilizará para las direcciones IP GRE locales cuando configure las conexiones del servicio Colo-Connect.

Estos se configuran cuando se configura una conexión de servicio Colo-Connect [**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection**

 ©2025 Palo Alto Networks, Inc.

(Conexión de servicio)]. En las áreas **Peer IP 1 (IP del mismo nivel 1)** y **Peer IP 2 (IP del mismo nivel 2)**.



Si está configurando una conexión de servicio para admitir hasta 10 Gbps de rendimiento, coloque un túnel en cada **Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**, para un total de dos túneles en cada conexión de servicio.

Si está configurando una conexión de servicio para que admita más de 10 Gbps de rendimiento (hasta 20 Gbps), coloque dos túneles en cada **Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**, para un total de cuatro túneles en cada conexión de servicio.

Los siguientes ejemplos muestran un túnel configurado para un rendimiento de más de 10 Gbps, por lo que se utilizan dos túneles por conexión y utilizan las siguientes direcciones IP de peers:

- 172.120.1.1 para Conexión 1
- 172.130.1.1 para Conexión 1
- 172.121.1.1 para Conexión 2
- 172.131.1.1 para Conexión 2

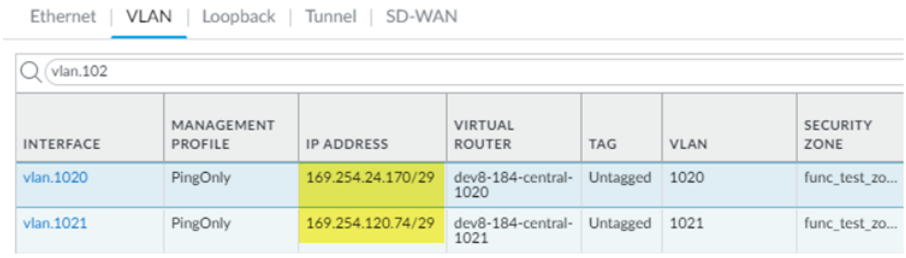
STEP 5 | Inicie sesión en el enrutador Colo.

Las siguientes capturas de pantalla de configuración utilizan un cortafuegos de nueva generación de Palo Alto Networks como enrutador Colo.

 ©2025 Palo Alto Networks, Inc.

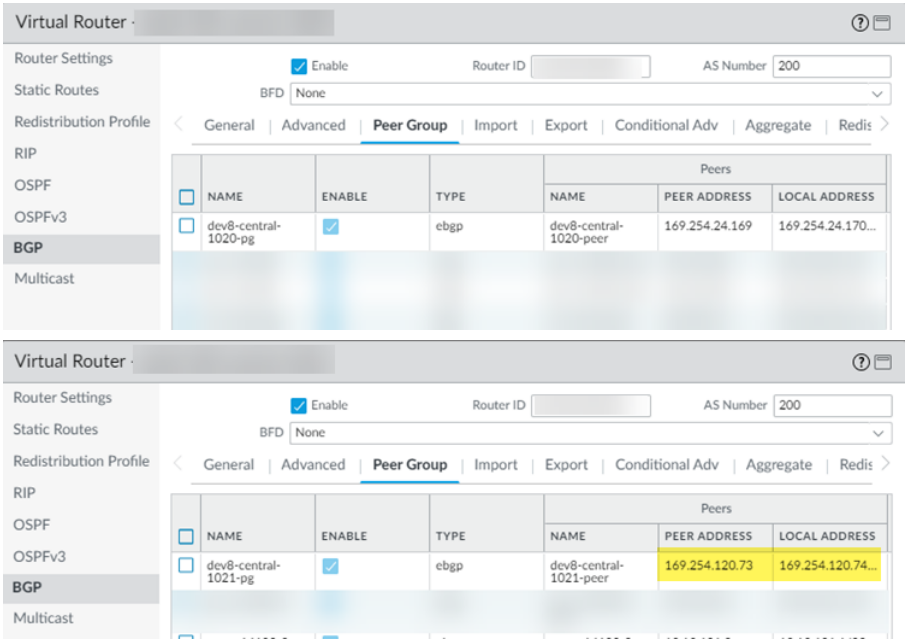
STEP 6 | Añada una interfaz VLAN, especificando la dirección **Colo CPE IP** como dirección IP.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (red)** > **Interfaces** > **VLAN** y **Add (Añadir)** la interfaz VLAN, especificando el nombre del **Virtual router (Enrutador virtual)** y



STEP 7 | Configure la dirección IP del enrutador Colo [**Colo CPE IP (Colo CPE IP**] como la dirección IP eBGP local y configure la dirección IP del enrutador en la nube [**Cloud Router IP (IP del enrutador en la nube)**] como la dirección de peer eBGP en su enrutador Colo.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Peer Group (Grupo de peers)** y introduzca la **Colo CPE IP (IP de Colo CPE)** como la **Peer Address (Dirección de peer)** y la **Cloud Router IP (IP del enrutador en la nube)** como la **Local Address (Dirección local)**.

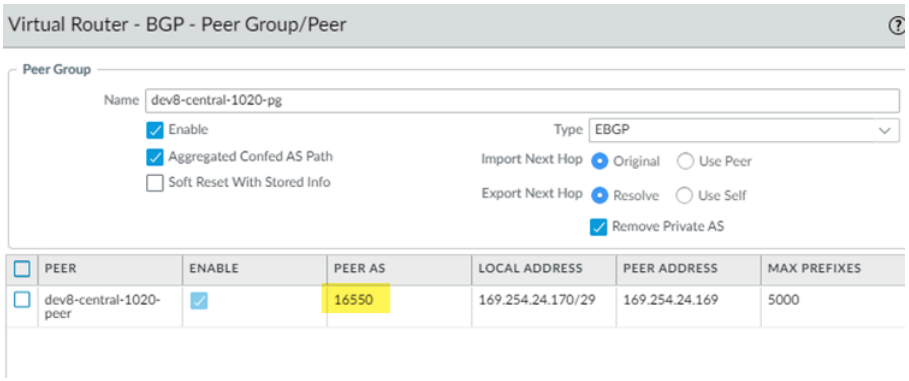


STEP 8 | Configure el **Cloud Router BGP ASN** como el número de sistema autónomo (ASN) del peer de eBGP.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP**

 ©2025 Palo Alto Networks, Inc.

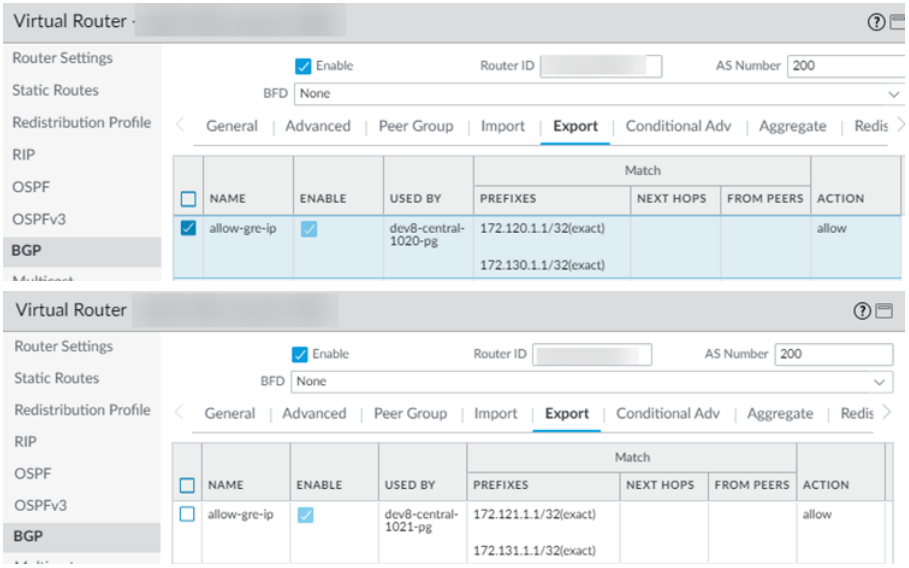
> **Peer Group (Grupo de peers)**, **Add (Añadir)** un grupo de peers y seleccione un **Peer AS (AS de peer)** de **16500**.



STEP 9 | Cree una política de exportación BGP que permita que solo la dirección IP GRE local se anuncie a la dirección IP del par del enrutador en la nube.

Dado que los enrutadores en la nube solo pueden recibir un número limitado de rutas, debe crear políticas para que solo se envíe al enrutador en la nube el enrutamiento entre las direcciones IP para los túneles GRE de conexión de servicio.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Export (Exportar)**, **Add (Añadir)** una norma de exportación, **Match (Hacer coincidir)** las direcciones IP utilizadas como la dirección IP del peer y crear una **Action (Acción)** de **Allow (Permitir)**.



STEP 10 | Cree de las conexiones de servicio de Colo-Connect.

Crear conexiones de servicio de Colo-Connect

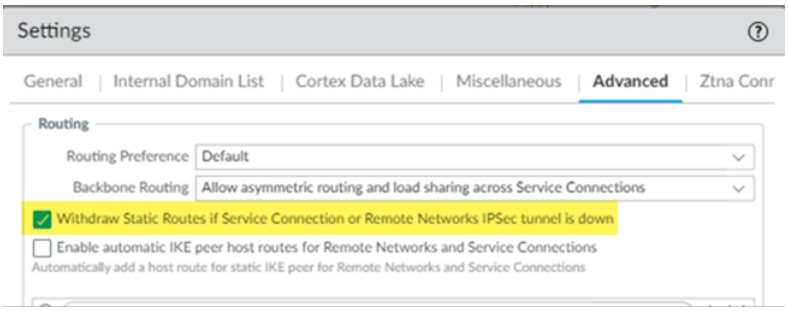
Colo-Connect utiliza conexiones de servicio, pero difieren de Prisma Access Service Connections (Conexiones de servicio de Prisma Access) porque utilizan túneles GRE en lugar de túneles IPSec

 ©2025 Palo Alto Networks, Inc.

y siempre utilizan BGP para el enrutamiento. Para configurar las conexiones de servicio Colo-Connect, complete los siguientes pasos.

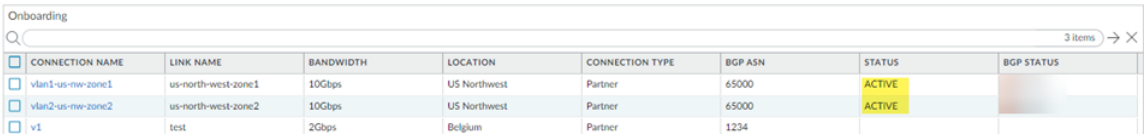
STEP 1 | Del Panorama que gestiona Prisma Access, asegúrese de que Prisma Access retira las rutas estáticas yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**, haciendo clic en el icono de engranaje para editar la **Settings (Configuración)** y seleccionando **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Retirar rutas estáticas si el túnel IPSec de Conexión de servicio o Redes remotas está inactivo)**.

Seleccionar esta opción garantiza que, si el túnel GRE deja de funcionar, se retire la ruta estática utilizada por el túnel GRE.



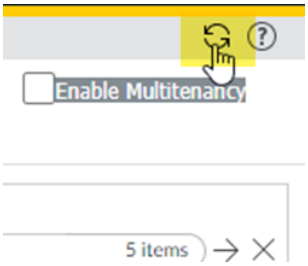
STEP 2 | Vaya a la pestaña **Colo-Connect** y asegúrese de que las conexiones estén en un estado **Active (Activo)** comprobando el **Status (Estado)** en el área de incorporación.

Hasta que el **Status (Estado)** de la conexión es **Active (Activo)**, no se pueden configurar las conexiones de servicio.



STEP 3 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)**.

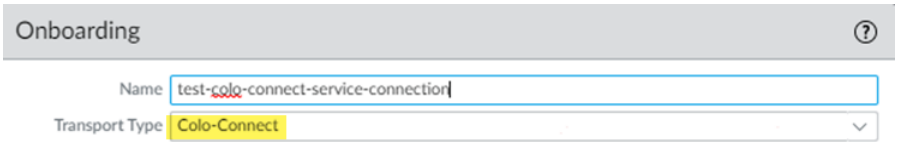
STEP 4 | Haga clic en **Refresh (Actualizar)** en la parte superior derecha de la interfaz de usuario de Panorama para que la configuración de Colo-Connect se aprovisione en el área de conexiones de servicio.



 ©2025 Palo Alto Networks, Inc.

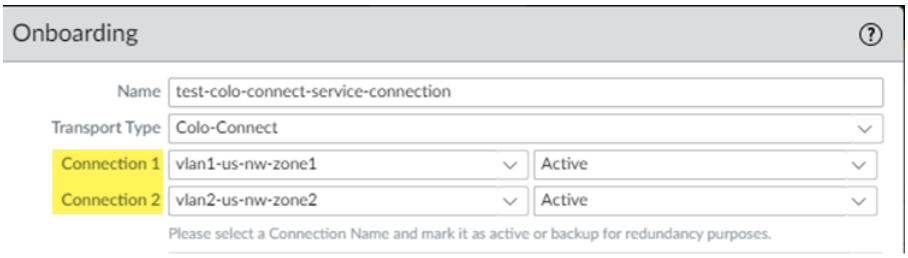
STEP 5 | **Add (Añadir)** una conexión de servicio, darle un carácter único **Name (Nombre)** y seleccione un **Transport Type (Tipo de transporte)** de **Colo-Connect**.

> *Asegúrese de que el nombre que introduzca tenga 31 caracteres o menos; la introducción de un nombre de 32 caracteres o más hace que el túnel se asigne incorrectamente en la infraestructura de Prisma Access.*



STEP 6 | Seleccione dos conexiones para utilizar con las conexiones de servicio [**Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**).

Estas conexiones deben estar en dos zonas diferentes.



STEP 7 | Seleccione **Active (Activo)** o **Backup (Copia de seguridad)** para la **Connection 1 (Conexión 1)** y **Connection 2 (Conexión 2)**

Utilice estas directrices al configurar conexiones de servicio:

- Puede configurar conexiones en estos modos:
  - **Active (Activo)/Active (Activo)**
  - **Active (Activo)/Backup (Copia de seguridad)**
  - **Backup (Copia de seguridad)/Active (Activo)**

  Configurar ambas conexiones en modo **Backup (Copia de seguridad)/Backup (Copia de seguridad)** no es válido y no es compatible.
- El ancho de banda de las conexiones debe ser el mismo para todos los modos.
- Las conexiones deben estar en zonas diferentes.
- El ancho de banda máximo que puede especificar para una conexión de servicio es 20 Gbps. Si especifica un **Bandwidth (Ancho de banda)** de **20 Gbps** para una conexión, no podrá usar esa conexión en una configuración **Active (Activa)/Active (Activa)** [debe configurarse como **Active (Activa)/Backup (Respaldo)**].
- No mezcle interconexiones dedicadas y de socios en la misma conexión de servicio y asegúrese de que las conexiones de servicio utilicen zonas diferentes. Esta tabla muestra las configuraciones permitidas y no permitidas para las conexiones de servicio, asumiendo

 ©2025 Palo Alto Networks, Inc.

que las zonas, las ubicaciones, el ancho de banda y las funciones siguen las pautas y los requisitos de conexión de servicio:

La conexión 1 pertenece a	La conexión 2 pertenece a	¿Configuración válida de la conexión de servicio Colo-Connect?
Conexión de socios 1	Conexión de socios 2	Sí
Conexión dedicada 1	Conexión dedicada 2	Sí
Conexión de socios 1	Conexión de socios 1	No
Conexión dedicada 1	Conexión dedicada 1	No
Conexión de socios	Conexión dedicada	No

STEP 8 | (Opcional, solo implementaciones de enrutamiento de BGP y hot potato) Seleccione una conexión de servicio para usar como copia de seguridad preferida (SC de copia de seguridad).

Solo puede seleccionar una conexión de servicio que se haya configurado como conexión de servicio Colo-Connect. Prisma Access utiliza la SC de copia de seguridad que seleccione como conexión de servicio preferida en caso de que se produzca un error de conexión. La selección de una conexión de servicio de respaldo puede evitar problemas de enrutamiento asimétrico si ha creado más de dos conexiones de servicio.

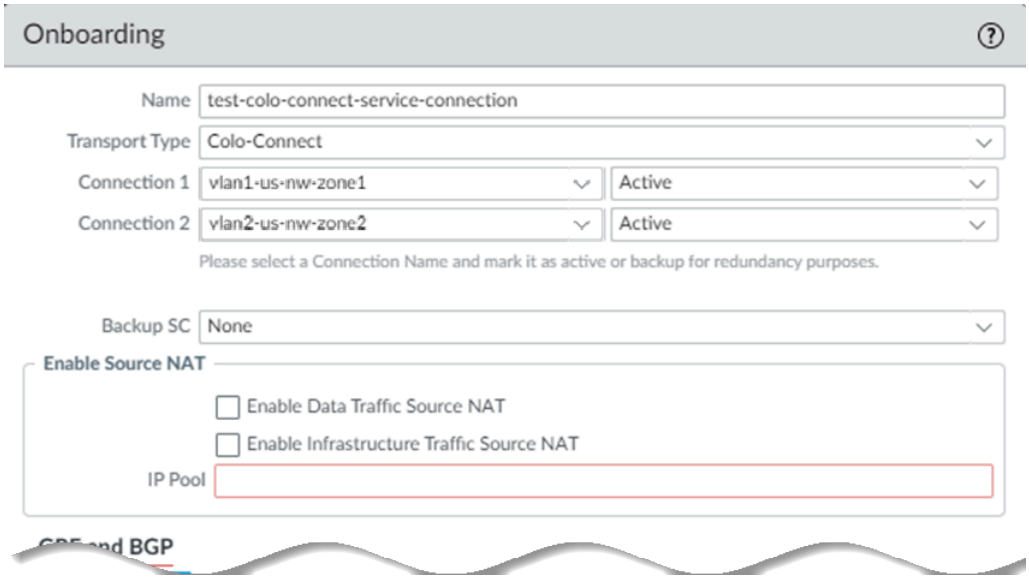
STEP 9 | (Opcional) Habilite la NAT de origen para Usuarios móviles: Direcciones de grupo de IP de GlobalProtect, direcciones IP en la subred de infraestructura o ambas.

Puede especificar una subred en una o más conexiones de servicio que se utilizan para el tráfico NAT entre Prisma Access Usuarios móviles y aplicaciones y recursos privados de GlobalProtect en un centro de datos.

- **Habilitar NAT de Origen de tráfico de datos**: realiza NAT en las direcciones del grupo de direcciones IP del usuario móvil para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncien y enruten en el centro de datos.
- **Habilitar NAT de origen de tráfico de infraestructura**: realiza NAT en las direcciones de la subred de infraestructura para que no se anuncien en el centro de datos, y solo las subredes que especifique en las conexiones de servicio se anuncian y enrutan en el centro de datos.
- **Grupo IP**: especifique el grupo de direcciones IP utilizado para realizar la NAT en el grupo de direcciones IP del usuario móvil, la Subred de infraestructura o ambos. Utilice una subred de IP privada (RFC 1918) o una subred adecuada que se pueda enrutar en su dominio de

 ©2025 Palo Alto Networks, Inc.

enrutamiento y que no se superponga con el grupo de direcciones IP de Usuarios móviles—GlobalProtect o la subred de infraestructura. Introduzca una subred entre /25 y /32.



STEP 10 | En el área **GRE and BGP (GRE y BGP)**, configure el túnel GRE y la configuración BGP para la conexión del servicio.

BGP siempre está configurado en **Enable (Habilitar)**.

1. (Opcional) Seleccione una de las siguientes opciones:

   - Para añadir una comunidad **no-export (sin exportación)** para nodos de acceso corporativo (conexiones de servicio) a los prefijos salientes de los pares eBGP en el equipo de las instalaciones del cliente (CPE), configure **Add no-export community (Añadir comunidad sin exportación)** en **Enabled Out (Habilitado de salida)**. Esta capacidad está **Disabled (Deshabilitada)** de manera predeterminada.

     No utilice esta capacidad en el modo de enrutamiento hot potato.

   - Para evitar que el peer de BGP de Prisma Access reenvíe rutas a la red de su organización. **Don't Advertise Prisma Access Routes (No anuncie las rutas de Prisma Access)**

     Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

     Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.

   - Para reducir el número de anuncios de subred IP de usuarios móviles a través de BGP a los equipos de las instalaciones del cliente (CPE) resumiéndolos, seleccione

 ©2025 Palo Alto Networks, Inc.

Summarize Mobile User Routes before advertising (Resumir rutas de usuarios móviles antes de anunciar).

Por defecto, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de subredes /24; si los resume, Prisma Access anuncia el grupo en función de la subred que especificó. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

Si tiene habilitado el enrutamiento de hot potato y habilita el resumen de rutas, Prisma Access ya no se antepone a los AS-PATH, lo que podría provocar un enrutamiento asimétrico. Asegúrese de que el tráfico de retorno desde el centro de datos o la sede central haya garantizado un retorno simétrico antes de habilitar el resumen de rutas con el enrutamiento de hot potato.

2. Configurar enrutamiento para la conexión de servicio mediante túneles GRE.
3. Desde el Panorama que gestiona Prisma Access, vuelva a **Panorama** > **Cloud Service (Servicio en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)** un túnel GRE para **Connection 1 (Conexión 1)** al introducir un archivo **GRE Tunnel Name 1 (Nombre del túnel GRE 1)** y un **Peer IP 1 (IP de peer 1)** para **Connection 1 (Conexión 1)** y, si se requiere más de 10 Gbps de ancho de banda, introduciendo **GRE Tunnel Name 2 (Nombre del túnel GRE 2)** y **Peer IP 2 (IP de peer 2)** para el segundo túnel para la conexión 1; a continuación, cree un túnel GRE para **Connection 2 (Conexión 2)** repitiendo estos mismos pasos.

   Cada par de túneles GRE en una conexión admite un máximo de 10 Gbps de ancho de banda. Si necesita más de 10 Gbps de ancho de banda, configure dos túneles por conexión. Por ejemplo:

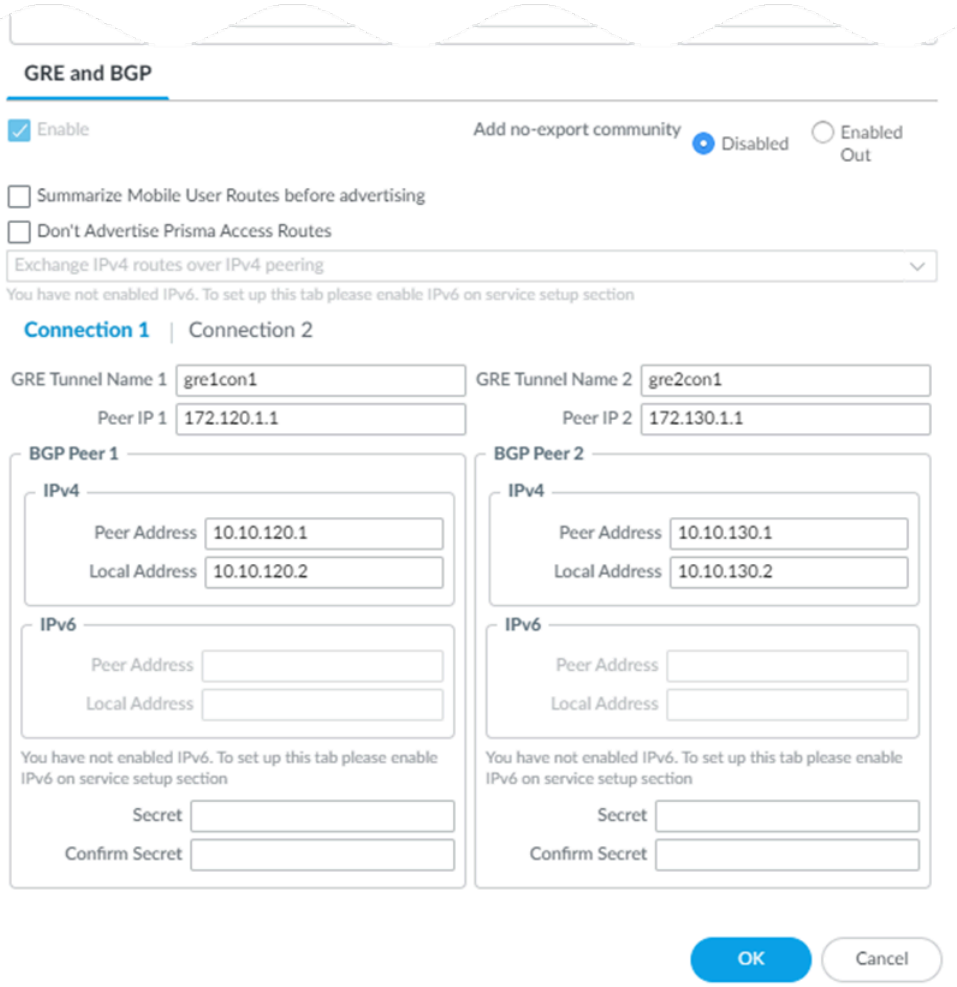
   Para la IP del peer, introduzca la dirección IP GRE del enrutador local en el Colo.

   Utilice direcciones IPv4 para los valores de BGP; IPv6 no es compatible.
4. Introduzca la **Peer Address (Dirección del peer)** y la **Local Address (Dirección local)** para el par BGP 1 y, si se requiere un segundo túnel para la conexión 1, el par BGP 2.

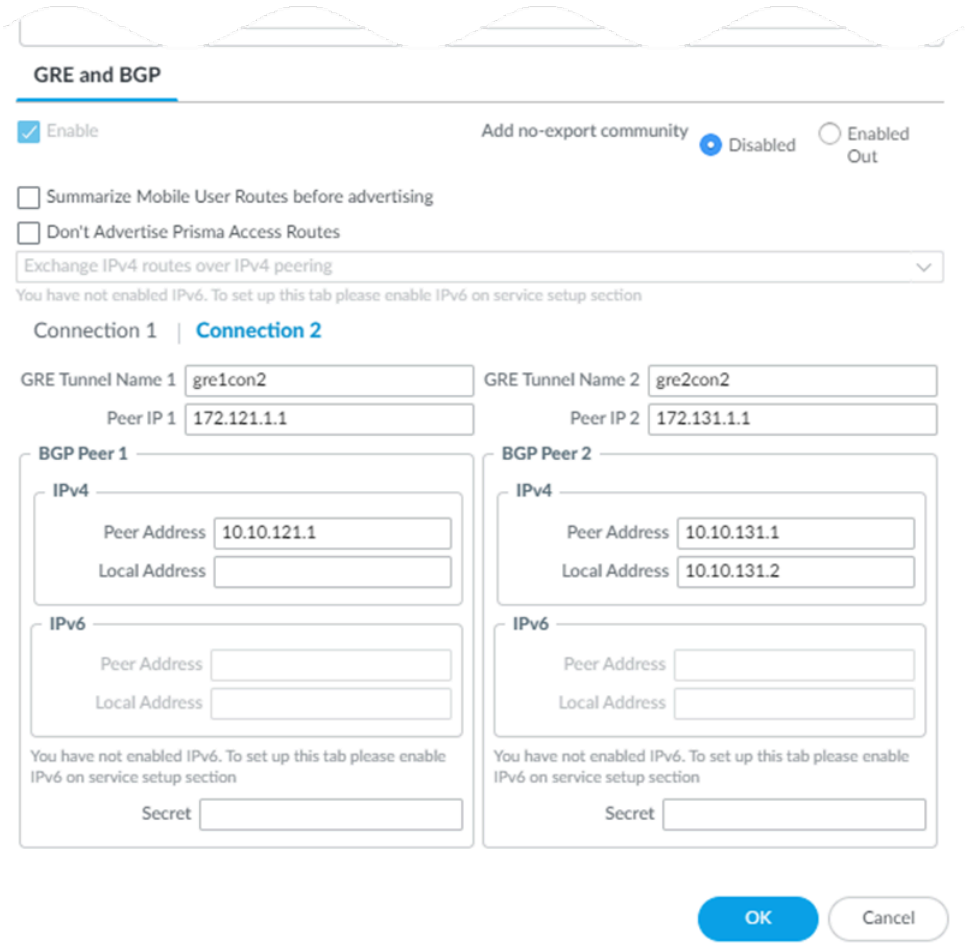
   Para **Peer Address (Dirección de pares)**, introduzca la dirección IP del peer BGP del enrutador Colo; para **Local Address (Dirección local)**, introduzca la dirección que se utilizará para el establecimiento de la red BGP a través del túnel GRE.

 ©2025 Palo Alto Networks, Inc.

5. (Opcional) Para configurar un secreto BGP, introduzca los valores **Secret (Secreto)** y **Confirm Secret (Confirmar secreto)**.



 ©2025 Palo Alto Networks, Inc.

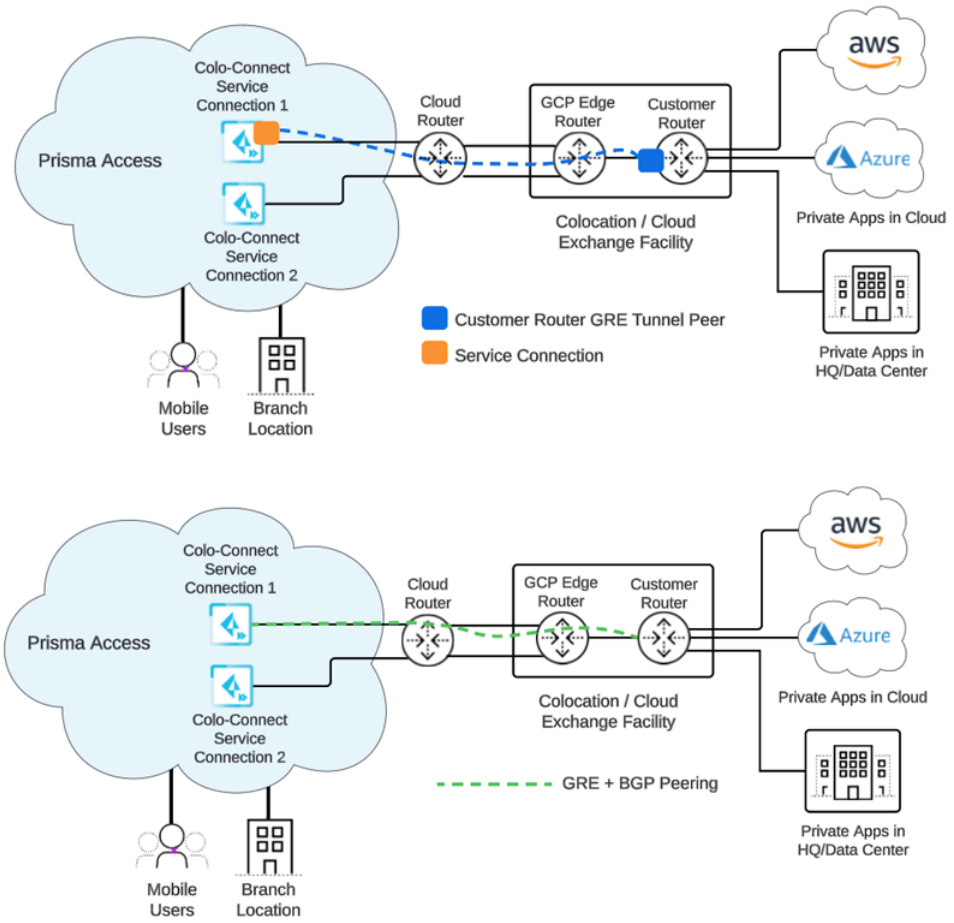


STEP 11 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios de configuración, asegurándose de que **Colo-Connect** esté seleccionado en el **Push Scope (Ámbito de envío)**.

Configurar el enrutamiento para la conexión de servicio mediante túneles GRE

El enrutador Colo anuncia la dirección IP de su peer del túnel GRE al enrutador en la nube y obtiene la subred para el túnel GRE del enrutador en la nube. Cuando configuró por primera vez el enrutamiento eBGP a través de la VLAN en el enrutador de cliente, anunció la accesibilidad local para los túneles GRE. Una vez que el enrutador en la nube y el enrutador Colo se anuncian y aprenden las rutas para la subred Colo y las direcciones IP GRE locales entre sí, los túneles GRE utilizados por la conexión de servicio se vuelven activos.

 ©2025 Palo Alto Networks, Inc.



Para configurar el enrutamiento y añadir túneles GRE a las conexiones de servicio, complete los siguientes pasos.

STEP 1 | Tome nota de las direcciones IP que utilizará para la **Peer Address (Dirección del peer)** y la **Local Address (Dirección local)** para el par BGP 1 y, si se requiere un segundo túnel para la conexión 1, el par BGP 2.

Los siguientes ejemplos utilizan las siguientes direcciones locales y de peer:

- **Peer Address (Dirección del peer)**: 10.10.120.0 y 10.10.130.1 para la conexión 1, 10.10.120.2 y 10.10.130.2 para la conexión 2
- **Local Address (Dirección local)**: 10.10.120.2 y 10.10.130.2 para la conexión 1, 10.10.121.2 y 10.10.131.2 para la conexión 2

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Tome nota de las direcciones IP que utilizará para la **Peer IP 1 (dirección IP de peer 1)** y, si es necesario, la dirección **IP Peer 2 (dirección IP de peer 2)** en las conexiones de servicio.

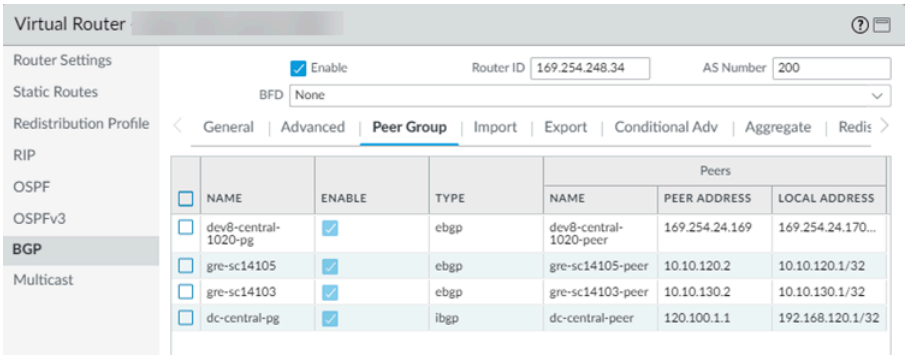
Utilice estas direcciones IP para crear una política de denegación que impida que la dirección IP GRE local se anuncie a la conexión del servicio Colo-Connect.

Todos los ejemplos de este documento utilizan estas direcciones IP:

- 172.120.1.1 para Conexión 1
- 172.130.1.1 para Conexión 1
- 172.121.1.1 para Conexión 2
- 172.131.1.1 para Conexión 2

STEP 3 | Configurar grupos de peers para los pares y las direcciones IP locales.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Peer Group (Grupo de peers)** y escriba la dirección del peer como la **Peer Address (Dirección del peer)** y la **Local Address (Dirección local)** como la **Local Address (Dirección local)**.



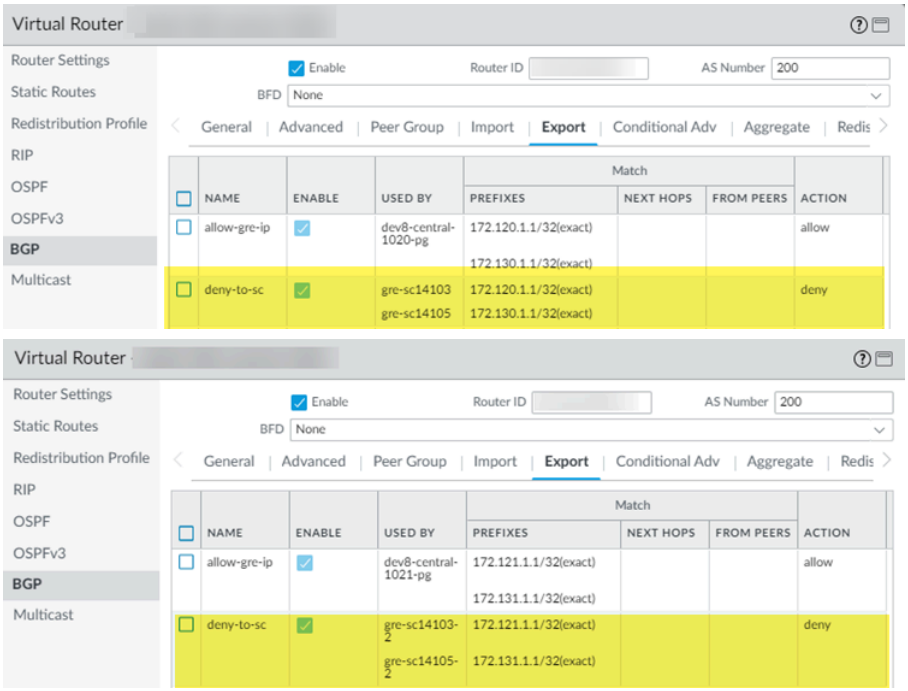
STEP 4 | Cree una política de exportación BGP para denegar las direcciones IP de los peers que configuró (172.120.1.1, 172.130.1.1, 172.121.1.1 y 172.131.1.1) y aplicarlas a los grupos de peers que creó.

Esta política de exportación coloca una regla DENY (DENEGAR) en las direcciones IP de los peers del túnel GRE local y permite que todas las demás rutas se anuncien a la conexión de servicio.

Si está utilizando un cortafuegos de nueva generación como enrutador Colo, vaya a **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** un enrutador virtual, vaya a **BGP** > **Export (Exportar)**, **Add (Añadir)** una norma de exportación, **Match (Hacer coincidir)** las

 ©2025 Palo Alto Networks, Inc.

direcciones IP utilizadas como la dirección IP del peer y crear una **Action (Acción)** de **Deny (Denegar)**.



Incrementar o disminuir el ancho de banda de una conexión de servicio Colo-Connect

Cuando configura conexiones de servicio, configura el ancho de banda en función de las conexiones (adjuntos de VLAN) asociadas a él. Asigna dos conexiones por conexión de servicio y luego asigna uno o dos túneles GRE por conexión.

Si bien cada conexión de servicio Colo-Connect admite un máximo de 20 Gbps, cada túnel GRE en la conexión de servicio admite 10 Gbps. Por este motivo, es posible que tenga que añadir o eliminar los túneles GRE en la conexión del servicio Colo-Connect para cambiar el ancho de banda total en un enlace y hacer que el ancho de banda de la conexión del servicio supere o deje de ser de 10 Gbps.

Aumentar el ancho de banda de una conexión de servicio Colo-Connect

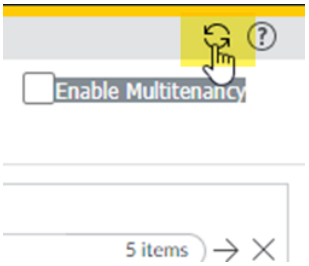
Para aumentar el ancho de banda de una conexión de servicio existente por encima de 10 Gbps, complete los siguientes pasos:

STEP 1 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect**.

STEP 2 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)** y haga clic en **Refresh (Actualizar)** en la parte

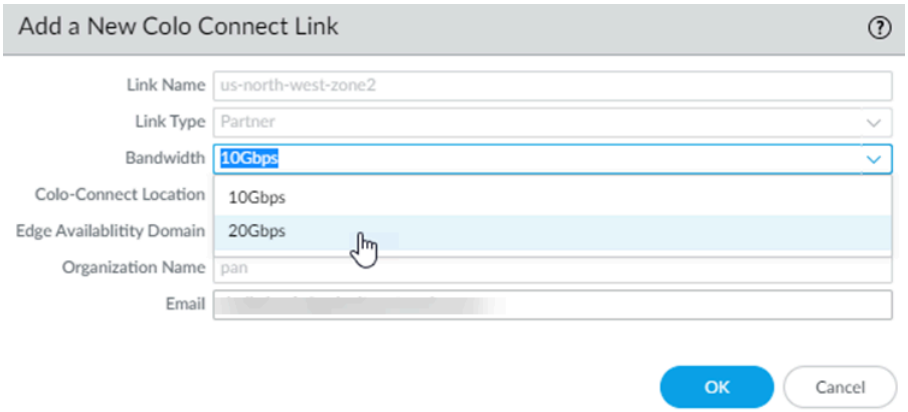
 ©2025 Palo Alto Networks, Inc.

superior derecha de la interfaz de usuario de Panorama para que la configuración de Colo-Connect se aprovisione en el área de conexiones de servicio.



STEP 3 | Seleccione la opción **Link Name (Nombre del enlace)** asociado a la conexión de servicio.

STEP 4 | Aumenta el **Bandwidth (Ancho de banda)** del enlace (interconexión).

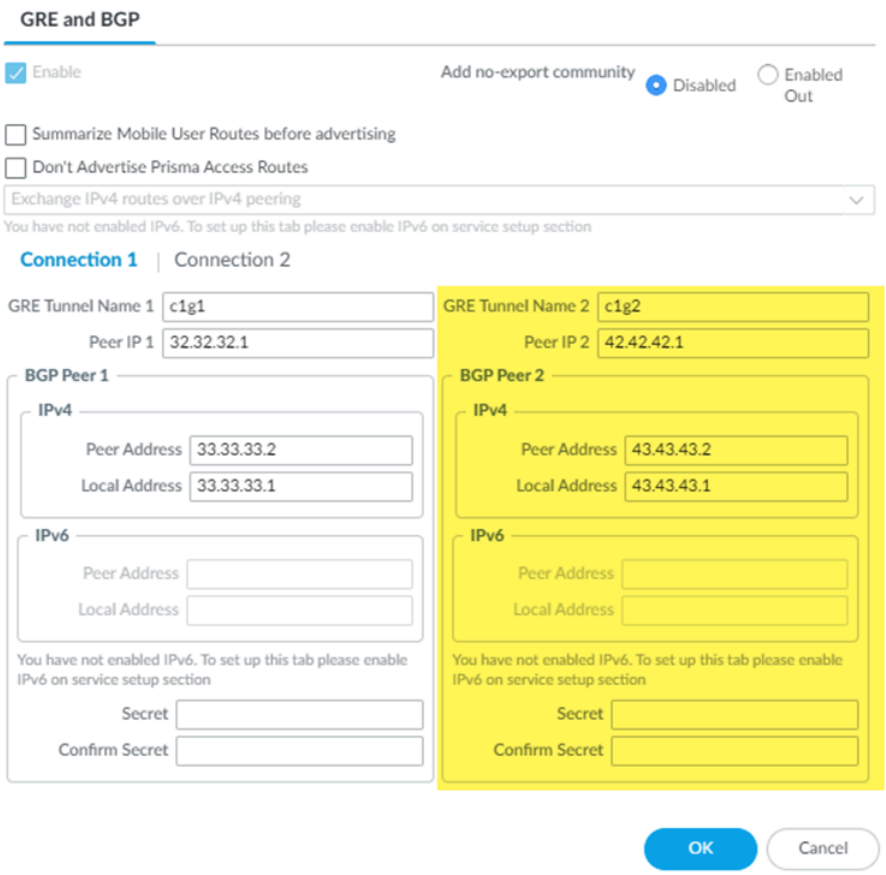


STEP 5 | Deberá **Commit and Push (Confirmar y enviar)** los cambios, seleccionando solo **Colo-Connect** en el **Push Scope (Ámbito de envío)**.

STEP 6 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)** > ***<service-connection-name>*** > **Onboarding (Incorporación)**.

©2025 Palo Alto Networks, Inc.

STEP 7 | Añada el túnel GRE adicional a la conexión del servicio Colo-Connect.



STEP 8 | Deberá **Commit and Push (Confirmar y enviar)** los cambios, seleccionando **Service Connections (Conexiones de servicio)** en el **Push Scope (Ámbito de envío)**.

STEP 9 | Añada las direcciones IP locales (del mismo nivel) de GRE a sus políticas de exportación para el VLAN eBGP routing (Enrutamiento eBGP de VLAN) y el enrutamiento de la conexión de servicio para los túneles GRE.

Reducir el ancho de banda de una conexión de servicio Colo-Connect

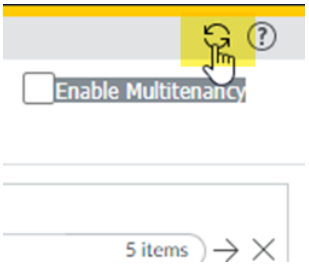
Para reducir el ancho de banda de una conexión de servicio existente por encima de 10 Gbps, complete los siguientes pasos:

STEP 1 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect**

STEP 2 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)** y haga clic en **Refresh (Actualizar)** en la parte

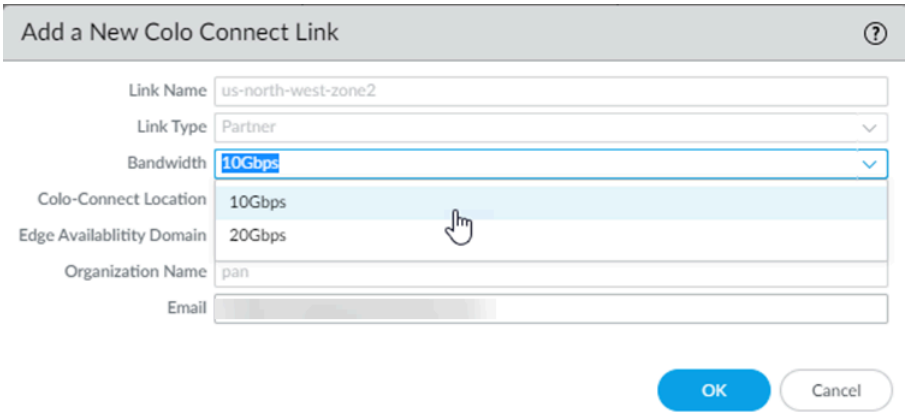
©2025 Palo Alto Networks, Inc.

superior derecha de la interfaz de usuario de Panorama para que la configuración de Colo-Connect se aprovisione en el área de conexiones de servicio.



STEP 3 | Seleccione la opción **Link Name (Nombre del enlace)** asociado a la conexión de servicio.

STEP 4 | Disminuya el **Bandwidth (Ancho de banda)** del enlace (interconexión).



STEP 5 | Deberá **Commit and Push (Confirmar y enviar)** los cambios, seleccionando solo **Colo-Connect** en el **Push Scope (Ámbito de envío)**.

STEP 6 | Deberá **Commit and Push (Confirmar y enviar)** los cambios, seleccionando **Service Connections (Conexiones de servicio)** en el **Push Scope (Ámbito de envío)**.

No es necesario volver a configurar la conexión de servicio para eliminar el túnel GRE adicional; Prisma Access detecta y reduce el ancho de banda del vínculo y quita el túnel adicional cuando se confirman y envían los cambios en el ámbito de inserción de la conexión de servicio.

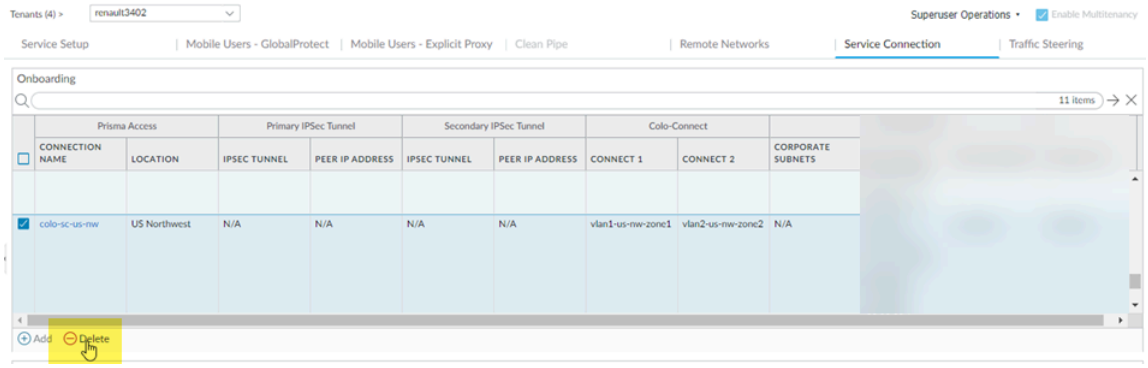
Eliminar una conexión de Colo-Connect

Para eliminar una conexión de Colo-Connect, siga el orden inverso de su configuración completando los siguientes pasos:

STEP 1 | Elimine las conexiones de servicio asociadas con la conexión yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection**

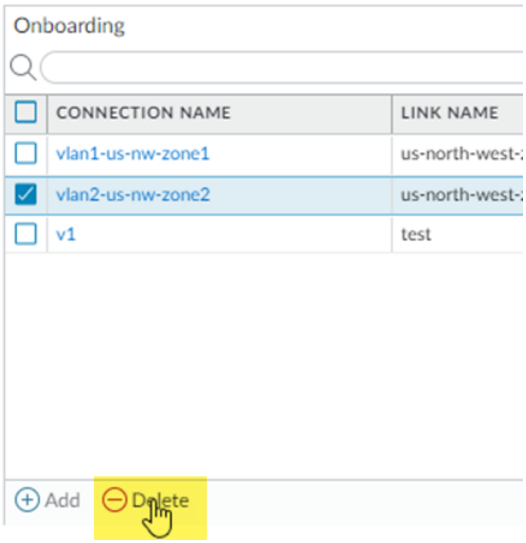
 ©2025 Palo Alto Networks, Inc.

(Conexión de servicio), seleccionando la conexión de servicio, y seleccionando **Delete (Eliminar)** para borrarla.



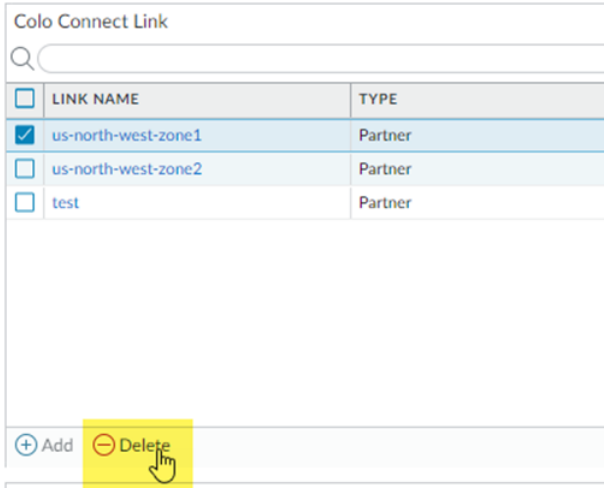
STEP 2 | Deberá **Commit and Push (Confirmar y enviar)** los cambios, seleccionando **Service Connections (Conexiones de servicio)** en el **Push Scope (Ámbito de envío)**.

STEP 3 | Elimine las conexiones de Colo-Connect asociadas con la conexión yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Colo-Connect**, seleccionando la opción **Connection Name (Nombre de conexión)** el la sección **Onboarding (Incorporación)** y seleccione **Delete (Borrar)** eso.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Elimine el enlace Colo-Connect seleccionando el **Link Name (Nombre del enlace)** y **Delete (Eliminar)**.



STEP 5 | Elimine las direcciones IP locales (peers) de GRE a sus políticas de exportación para el enrutamiento eBGP de VLAN y el enrutamiento de conexión de servicio para los túneles GRE.

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Aceleración de aplicaciones en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Una versión mínima Prisma Access de 5.0 Innovación ❑ Licencia de Prisma Access ❑ La aceleración de aplicaciones requiere una versión de plano de datos de Prisma Access de 10.2.10. ❑ Licencia de complemento de aceleración de aplicaciones La licencia de aceleración de aplicaciones incluye una licencia de evaluación de 30 días para Autonomous DEM (ADEM) para que pueda recuperar métricas de rendimiento de aceleración de aplicaciones de ADEM.

La Aceleración de aplicaciones aborda directamente las causas del mal rendimiento de las aplicaciones y actúa en tiempo real para mitigarlas, mejorando drásticamente la experiencia del usuario para los usuarios de Prisma Access GlobalProtect y Red remota.

Las principales causas de una mala experiencia del usuario al acceder a aplicaciones son el contenido dinámico (contenido que se debe procesar para cada usuario de forma individual, bajo demanda) y los problemas de conectividad de red.

La aceleración de aplicaciones le proporciona la siguiente funcionalidad:

Aceleración para las principales aplicaciones SaaS: la Aceleración de aplicaciones para Prisma SASE acelera el contenido dinámico para mejorar el tiempo de respuesta de las principales aplicaciones SaaS. Prepara de forma segura e inteligente el contenido dinámico que cada usuario necesita, antes de que el usuario lo solicite.

Como resultado, la Aceleración de aplicaciones reduce drásticamente el tiempo de respuesta de las aplicaciones y las API que las impulsan para mejorar la experiencia del usuario y aumentar la productividad.

Las aplicaciones aceleradas se enumeran en la sección de Aplicaciones compatibles.

Aceleración de red: cuando sus usuarios acceden a aplicaciones, pueden experimentar un rendimiento deficiente de la aplicación causado por una disminución del rendimiento, que podría ser el resultado de una pérdida de paquetes, conectividad inalámbrica degradada, congestión de red y otros factores. Estos problemas de red pueden afectar negativamente la experiencia del empleado y reducir su productividad.

Cuando se concibió internet, las redes eran homogéneas y la conectividad inalámbrica estaba en su infancia. Los protocolos fundamentales como TCP fueron creados de forma original para estas redes. Hoy en día, las redes ya no son homogéneas y la conectividad inalámbrica crea una experiencia de usuario altamente variable. Cuando los usuarios experimentan condiciones de red degradadas, TCP no puede diferenciar si el problema ocurrió debido a limitaciones del dispositivo, limitaciones de la red o restricciones físicas.

Sin requerir cambios en la configuración de su cliente o aplicaciones, la Aceleración de aplicaciones construye de manera segura una comprensión de los:

- **Capacidad del dispositivo**: el tipo de endpoint del cliente
- **Capacidad de red**: el tipo de red
- **Contexto de la aplicación**: el tipo de aplicación que se está utilizando

Usando su comprensión del contexto del dispositivo, la red y la aplicación, la Aceleración de aplicaciones maximiza el rendimiento y se ajusta en tiempo real para tener en cuenta las condiciones cambiantes de la red.

Cuando se compara con el acceso directo a Internet, la Aceleración de aplicaciones ofrece una mejora notable en el rendimiento del tráfico TCP al conectarse a través de Prisma Access.

Puede ver las mejoras de rendimiento de la Aceleración de aplicaciones en Incidentes y alertas de Prisma SASE. Autonomous DEM impulsado por IA (ADEM) se integra con la Aceleración de aplicaciones y le proporciona métricas como el número de aplicaciones que fueron aceleradas y el aumento de rendimiento obtenido en general.

 ©2025 Palo Alto Networks, Inc.

Requisitos y directrices para la aceleración de aplicaciones

Al configurar la Aceleración de aplicaciones, tenga en cuenta las siguientes pautas y requisitos:

- **Aplicaciones compatibles**: la aceleración de aplicaciones admite las siguientes aplicaciones:
  - Amazon S3
  - Azure Storage
  - Box
  - Google Drive
  - Microsoft 365:
    - My Content (Mi contenido)
  - Microsoft OneDrive
  - Salesforce
  - SAP Ariba
  - ServiceNow
  - Slack (*descargas de archivos*)
  - Zoom:
    - Descargas de archivos desde el chat
    - Descargas de grabaciones en la nube
    - Chat de equipo de Zoom
- **Ubicaciones compatibles**: la aceleración de la aplicación está disponible para todas las ubicaciones de Prisma Access excepto para las siguientes ubicaciones:
  - Todas Zonas Locales
  - Baréin
  - China
  - Irlanda
  - Sudáfrica Oeste
  - Suecia
  - Emiratos Árabes Unidos
- **Carga de CA raíz de confianza**: necesita configurar una CA raíz de confianza y realizar una operación de confirmar y enviar, y luego seleccionarla durante la configuración de Aceleración de aplicaciones, como se muestra en los siguientes procedimientos. Si utiliza Strata Cloud Manager para configurar la Aceleración de aplicaciones, configure la CA raíz en el alcance Prisma Access. Si cambia el certificado que utiliza, también debe confirmar y enviar el certificado cambiado antes de seleccionarlo.
- **Certificado de reenvío fiable y CA raíz de confianza:** habilite la CA/certificado que subió como un certificado de reenvío fiable y CA raíz de confianza, como se muestra en los siguientes

 ©2025 Palo Alto Networks, Inc.

procedimientos. Si se aplica el descifrado SSL a cualquier aplicación acelerada, debe marcar el certificado como un certificado de reenvío fiable y CA raíz de confianza, o los usuarios encontrarán errores SSL al intentar acceder a esas aplicaciones.

- **Funcionalidad de Prisma Access no compatible**: la siguiente funcionalidad no es compatible con la Aceleración de aplicaciones y Prisma Access las implementaciones con estas características habilitadas no serán aceleradas. La aceleración de aplicaciones de
  - IPv6

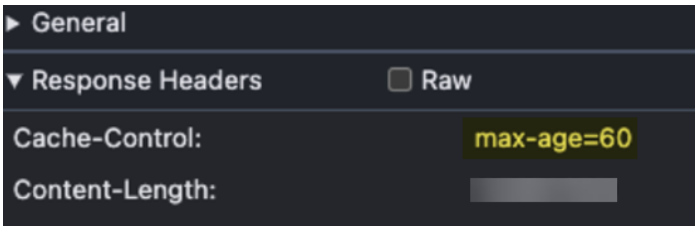
    coexiste con la red IPv6 cuando se configura IPv6; sin embargo, solo se acelera el tráfico TCP de IPv4. El tráfico de IPv6 no está acelerado, pero funciona con normalidad.
  - Redes remotas que utilizan subredes superpuestas (soportadas por defecto en implementaciones Prisma Access (Managed by Strata Cloud Manager), configurables en implementaciones de Prisma Access (Managed by Panorama).
- **Directrices de Aceleración de aplicaciones**:
  - **Compatibilidad con el protocolo QUIC**: Algunos navegadores (como Google Chrome) pueden utilizar el protocolo de conexiones rápidas de UDP por defecto. La aceleración de aplicaciones de la Capa 7 no se puede utilizar en el tráfico que utiliza QUIC. Como solución alternativa, desactive el protocolo QUIC cuando configure la Aceleración de aplicaciones.
  - **Aplicaciones SaaS y encabezados de respuesta Zy-***: los usuarios que se conectan a las implementaciones de Prisma Access que tienen habilitada la Aceleración de aplicaciones para las principales aplicaciones SaaS pueden esperar ver encabezados de respuesta con un nombre de Zy-*, como Zy-Server y Zy-Accelerated, y una cookie de sesión zy_sid.

    Si el encabezado de respuesta es Zy-Accelerated, un valor de **1** indica que la respuesta fue acelerada y un valor de **0** indica que la respuesta no fue acelerada.
  - **Localización de Contenido**: Si una aplicación SaaS acelerada localiza contenido únicamente en función de la dirección IP del usuario o del ID del usuario, cuando la aceleración está habilitada para esa aplicación, su contenido no se localizará.
  - **Cambiar al Comportamiento predeterminado para las reglas de política de seguridad con una Acción configurada en Denegar**: si tiene una regla de política de seguridad con una acción configurada en **Deny (Denegar)** que se aplica al tráfico que pasa a través de la Aceleración de Aplicaciones utilizando una regla basada en la dirección de origen o destino, aplicación o servicio, el tráfico completará una negociación en tres pasos pero Prisma Access lo bloqueará y la política de **Deny (Denegar)** funcionará como se configuró.
  - **Amazon S3 y Azure Blob Storage `control de caché`**: los buckets y archivos de Amazon S3 y Azure Blob Storage tienen una serie de encabezados de respuesta HTTP asociados. Uno de estos valores es `cache-control.` Los archivos no se aceleran si el valor de `control de caché` es:
    - Desactivar
    - Establecer a un valor de `max-age=0`

 ©2025 Palo Alto Networks, Inc.

- Establecer a un valor de `max-age=no-cache`

  Para obtener el beneficio de la Aceleración de aplicaciones para Amazon S3 y Azure Blob Storage, establezca el valor de `max-age` de `control de caché` a uno que sea mayor que cero.



- **Aplicaciones con dominio compartido en Activity Insights**: al utilizar la aceleración de aplicaciones, la aceleración de la capa 7 se basa en el dominio. En ciertas condiciones, si dos aplicaciones comparten el mismo dominio, la aplicación que informa en Activity Insights podría atribuir el tráfico de Capa 7 de una aplicación a otra aplicación. Por ejemplo, si algún tráfico de la aplicación MS Teams y OneDrive comparte el mismo dominio, el informe de la aplicación MS Teams se mostrará en OneDrive.
- **Conexiones de larga duración y logs del sistema**: la aceleración de aplicaciones escribe logs de Capa 4 cuando finaliza una conexión TCP individual. Para conexiones de corta duración, este comportamiento es transparente, porque las conexiones de corta duración son creadas frecuentemente por las aplicaciones. La

  aceleración de aplicación recopila métricas durante todo el período en que la conexión está activa. Para conexiones de larga duración, como las utilizadas por las unidades de red SMB montadas, este comportamiento puede hacer que parezca que las métricas se recopilan solo al final de la conexión.

 ©2025 Palo Alto Networks, Inc.

Configurar la aceleración de aplicaciones

Para configurar la Aceleración de Aplicaciones en Prisma Access, seleccione una de las siguientes pestañas según su implementación (Prisma Access (Managed by Strata Cloud Manager) o Prisma Access (Managed by Panorama)).

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Configurar la aceleración de aplicaciones en Prisma Access (Strata Cloud Manager)

Para configurar la aceleración de aplicaciones en una implementación de Prisma Access (Managed by Strata Cloud Manager), complete esta tarea.

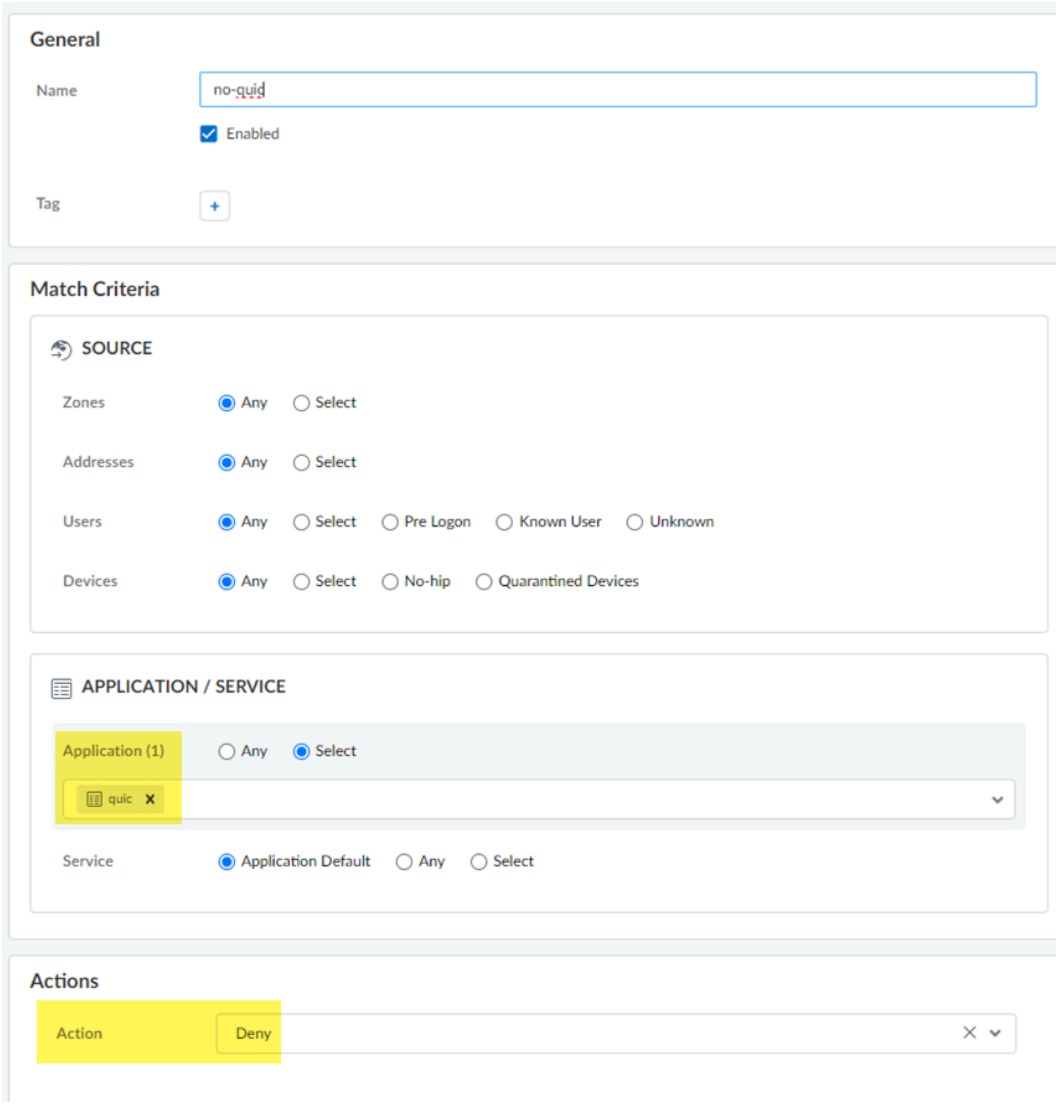
©2025 Palo Alto Networks, Inc.

STEP 1 | (Opcional) Deshabilite el protocolo de Conexiones UDP rápidas en Internet (QUIC).

La aceleración de aplicaciones no puede acelerar las aplicaciones en Capa 7 sin deshabilitar QUIC.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** y **Add Rule (Añadir regla)** > **Pre Rules (Reglas previas)**.

   Cree esta regla de política de seguridad en el ámbito de configuración **Global**.
2. Seleccione una **Application / Service (Aplicación / servicio)** de **quic** y una **Action (Acción)** de **Deny (Denegar)**.

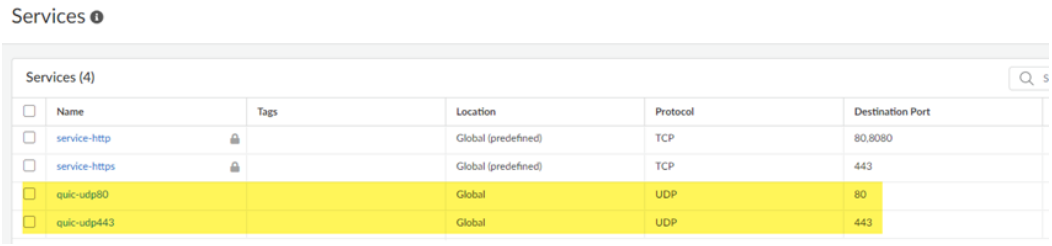


3. Haga clic en **Save (Guardar)** para guardar sus cambios.
4. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW & Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Services (Servicios)** > **Service (Servicio)** y seleccione **Add (Añadir)** servicios para el puerto UDP 80 y el puerto UDP 443.

   Palo Alto Networks recomienda añadir servicios para el puerto UDP 80 y el puerto UDP 443, y crear una política de seguridad adicional para bloquear el tráfico UDP en esos

 ©2025 Palo Alto Networks, Inc.

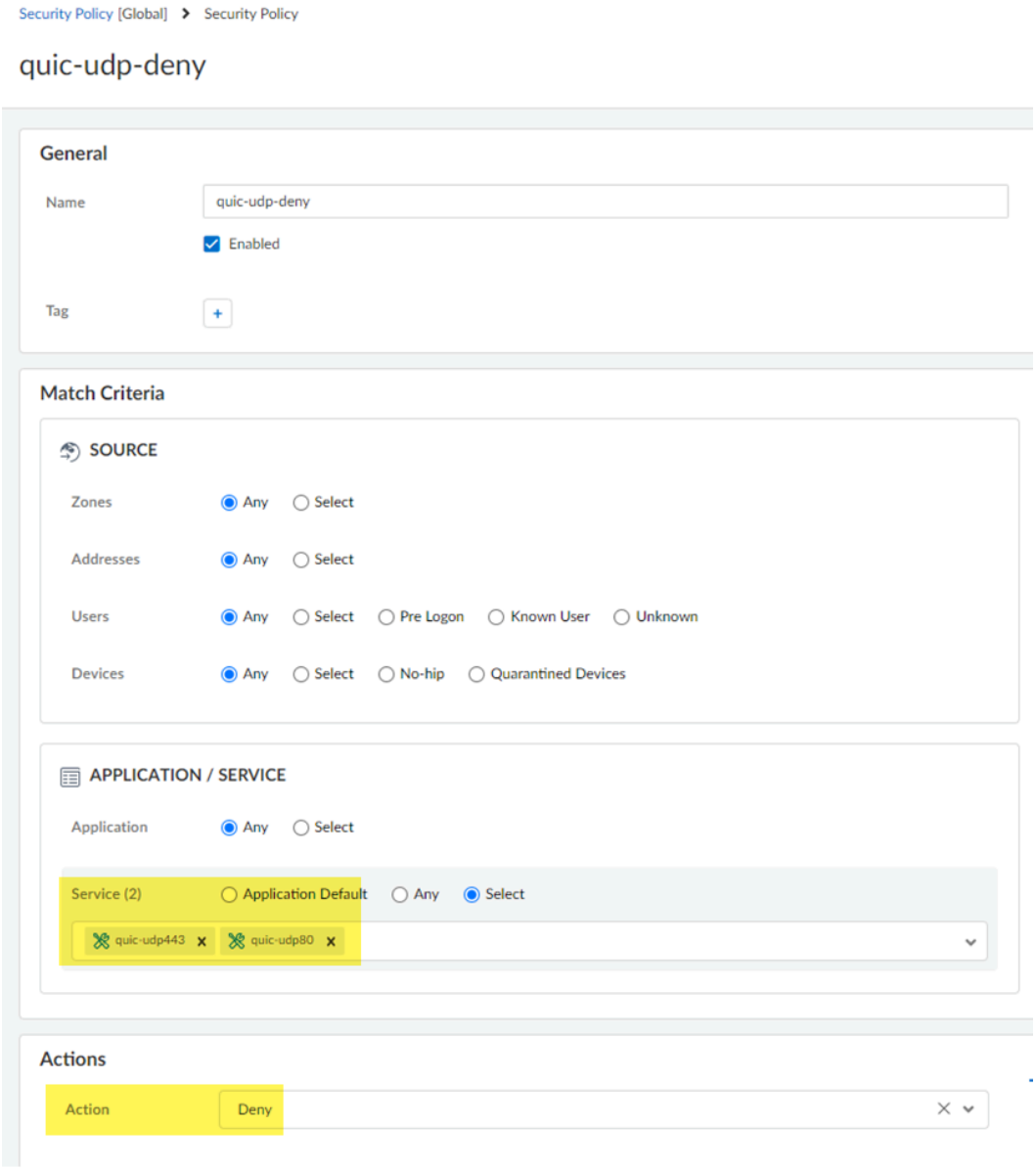
puertos, porque las versiones más recientes de QUIC podrían identificarse erróneamente como **unknown-udp (udp desconocido)**.



5. Vuela c **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW & Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)Add Rule (Añadir regla)** para una segunda política de seguridad,

 ©2025 Palo Alto Networks, Inc.

especificando los servicios en**Application / Services (Servicios / Aplicación)** y una **Action (Acción)** de **Deny (Denegar)**.



Cuando se complete, tendrá dos políticas de seguridad: Uno que bloquea el protocolo QUIC y otro que bloquea el tráfico en los puertos UDP 80 y 443.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Importe un certificado de autoridad de certificación raíz (CA) y una clave privada en Strata Cloud Manager en el ámbito de Prisma Access para usar con la aceleración de aplicaciones y enviar sus cambios.

Un certificado/CA raíz autofirmado es el certificado de mayor nivel de una cadena de certificados. La aceleración de aplicaciones utiliza los certificados/CA raíz para crear certificados para las aplicaciones aceleradas. Presione la CA raíz/certificado en Prisma Access para que la Aceleración de aplicaciones pueda comenzar la creación de los certificados específicos de la aplicación.

El CA raíz/certificado debe tener estas características: :

- La CA debe ser una CA de confianza.
- (Recomendado) La CA debe ser única y usarse solo para la aceleración de aplicaciones.
- La CA no puede estar caducada. Tome nota de la fecha de vencimiento de la CA y renueve el certificado antes de que caduque. Si la aceleración de aplicaciones que utiliza una CA/certificado caduca, los usuarios recibirán un error SSL al intentar acceder a aplicaciones

 ©2025 Palo Alto Networks, Inc.

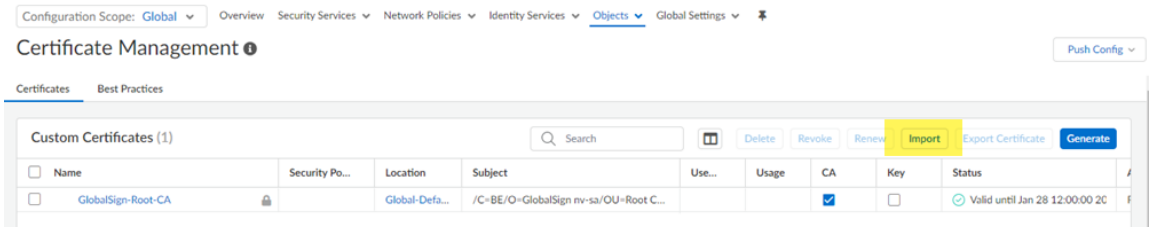
aceleradas. Es fundamental asegurarse de que la CA es válida cuando su organización utiliza la aceleración de aplicaciones.

- Debe incluir una clave.
- Debe usar una frase de contraseña.
- Debe estar en el ámbito del **Prisma Access**.
- (Usuarios móviles: solo implementaciones de GlobalProtect) Debe instalarse en el almacén local de certificados raíz.

  Puede realizar esta instalación añadiéndola a la lista de certificados de confianza como se describe en este procedimiento o, si utiliza ActiveDirectory, puede distribuir la CA raíz desde AD mediante un objeto de política de grupo (GPO) de Active Directory.

Si alguna vez necesita cambiar la CA/certificado raíz, debe cargarlo y enviar sus cambios antes de poder usar el certificado cambiado.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Certificate Management (Gestión de certificados)**.
2. **Import (Importar)** un certificado.



3. Seleccione los siguientes parámetros:
   - Introduzca un **Certificate Name (Nombre de certificado)** único para el certificado, como `AppAcceleration_CA`.

     El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 31 caracteres de longitud. Utilice solamente letras, números, guiones y guiones bajos.
   - Seleccione **Choose File (Seleccionar archivo)** y busque el **Certificate File (Archivo de certificado)** recibido de la CA y Seleccione **Open (Abrir)**.
   - Seleccione un **Format (Formato)**:
     - **Encrypted Private Key and Certificate (PKCS12) [Clave privada cifrada y certificado (PKCS12)]**: este es el formato predeterminado y más común, en el que la clave y el certificado están en un único contenedor (Archivo del certificado).
     - **Certificado codificado en Base64 (PEM)**: debe importar la clave independientemente del certificado. Debe seleccionar un **Key File (Archivo clave)** si selecciona este formato.
     - Introduzca una **Passphrase (Frase de contraseña)** y seleccione **Confirm Passphrase (Confirmar frase de contraseña)**.
4. Haga clic en **Save (Guardar)** para guardar sus cambios.

 ©2025 Palo Alto Networks, Inc.

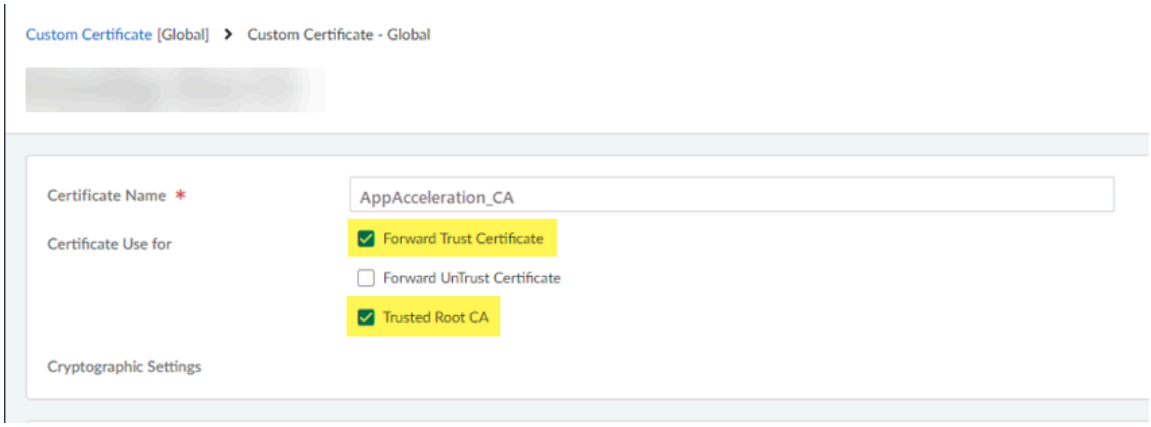


 ©2025 Palo Alto Networks, Inc.

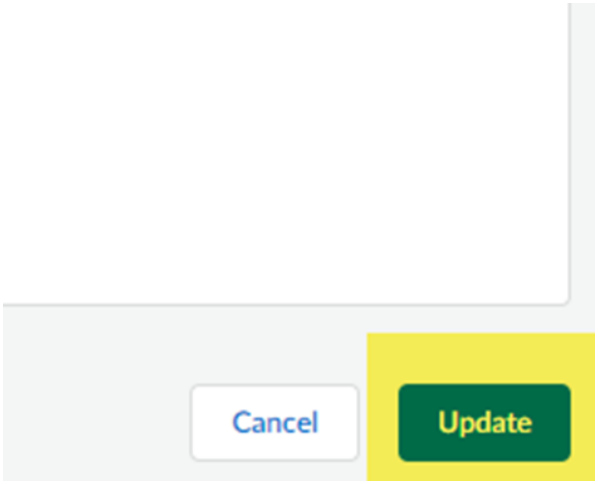
STEP 3 | Marque la CA raíz/certificado que añadió como un certificado de confianza de reenvío y una CA raíz de confianza.

Si no especifica el certificado como un certificado de confianza de reenvío y una CA raíz de confianza, los usuarios encontrarán errores SSL al intentar acceder a aplicaciones aceleradas al usar el descifrado SSL.

1. Seleccione la CA raíz/certificado que añadió.
2. Seleccione el certificado como un **Forward Trust Certificate (Certificado de reenvío fiable)** y **Trusted Root CA (CA raíz de confianza)**.

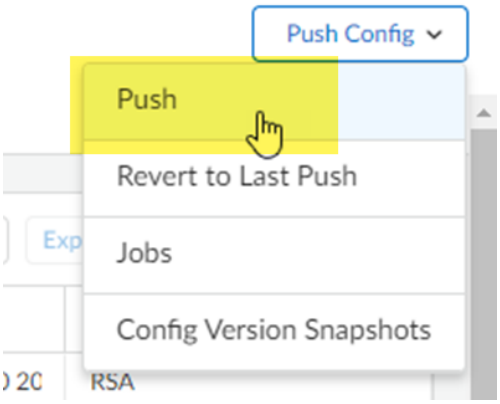


3. **Update (Actualizar)** el certificado.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Push (Enviar)** sus cambios.

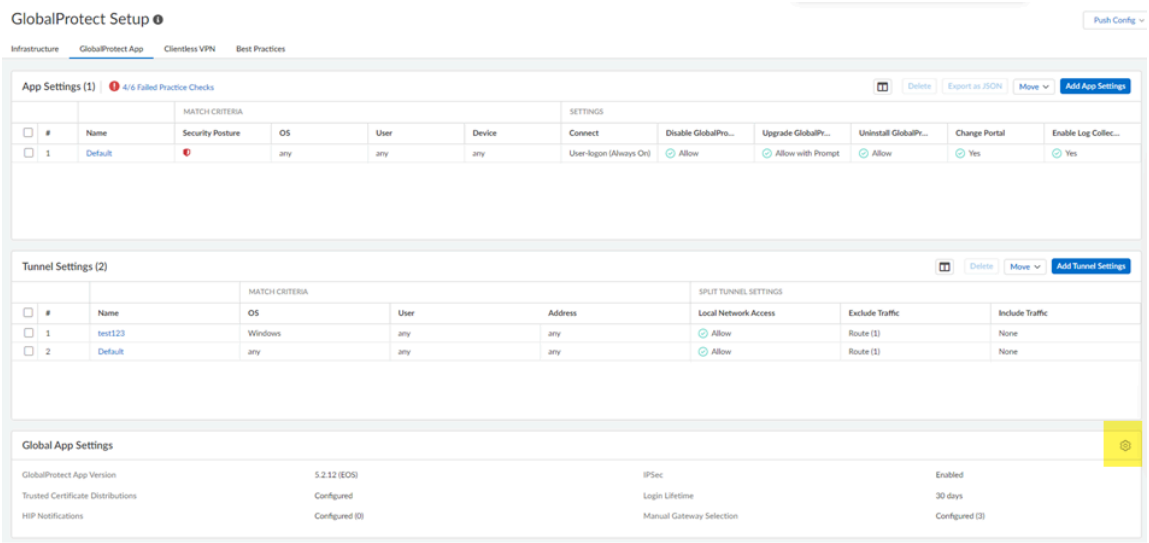


 ©2025 Palo Alto Networks, Inc.

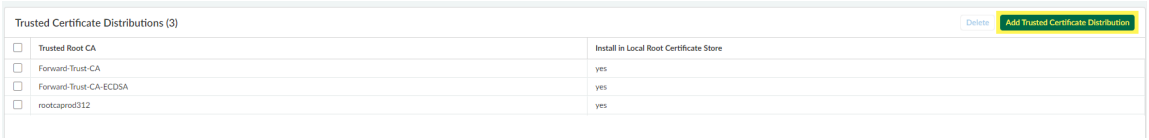
STEP 5 | (Usuarios móviles: solo implementaciones de GlobalProtect) Añada la CA/certificado raíz que añadió a la lista de certificados de confianza de GlobalProtect e instálelo en el almacén de certificados raíz local.

De forma alternativa, si está usando ActiveDirectory, puede distribuir la CA raíz desde AD usando un GPO de Active Directory.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Aplicación de GlobalProtect)** > **Global App Settings (Configuración global de la aplicación)**.
2. Haga clic en el engranaje para editar la **Settings (Configuración)**.



3. **Añadir distribución de certificados de confianza**.



4. Seleccione la **Trusted Root CA (CA raíz de confianza)** que creó en un paso anterior y seleccione **Install in Local Root Certificate Store (Instalar en el almacén de certificados raíz local)**.

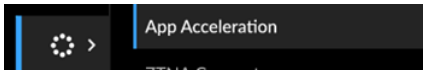


5. Haga clic en **Save (Guardar)** para guardar sus cambios.
6. Seleccione **Push (Enviar)** sus cambios.

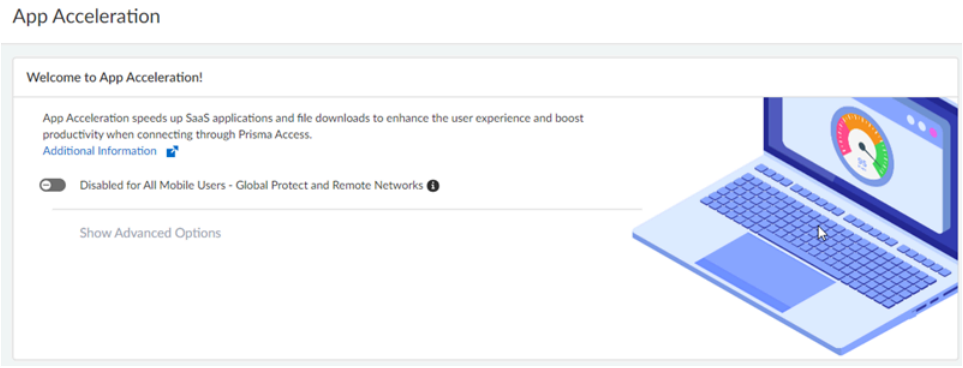
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Habilite la aceleración de aplicaciones y elija el archivo de certificado que creó.

1. Vaya a **Workflows (Flujos de trabajo)** > **App Acceleration (Aceleración de aplicaciones)** desde la barra de navegación izquierda..

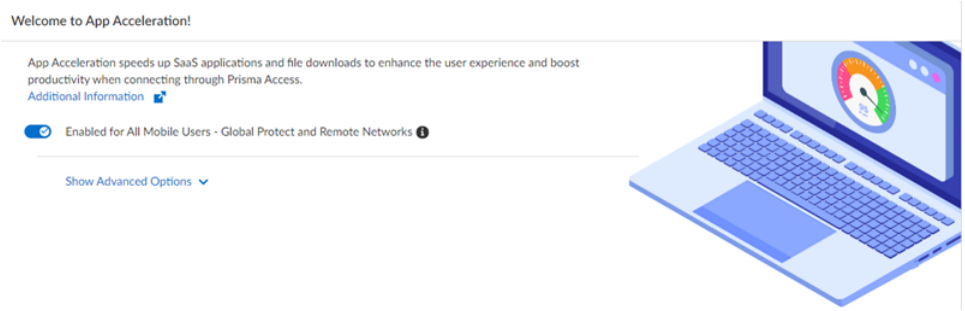


Aparecerá la ventana de aceleración de aplicaciones.



2. Mueva el control deslizante hacia la derecha para que la aceleración de aplicaciones esté **Enabled for all Mobile Users—GlobalProtect and Remote Networks (Habilitada para todos los usuarios móviles: GlobalProtect y Redes remotas)**.

Si las confirmaciones están en curso, la configuración de aceleración de la aplicación entrará en vigor después de que se completen todos las confirmaciones.

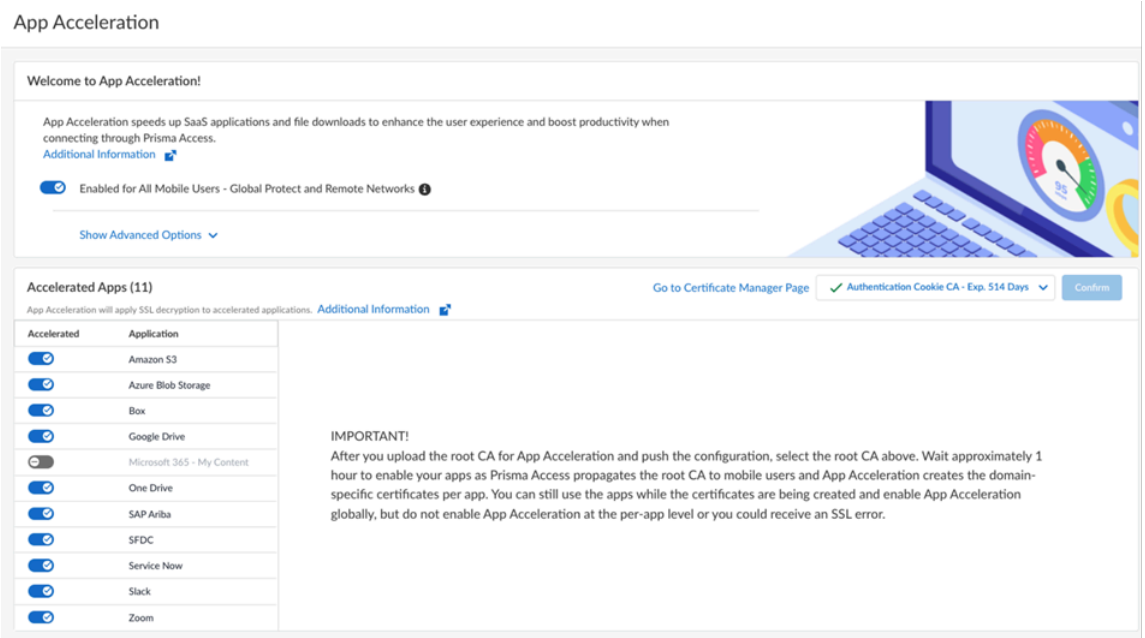


Aceleración de aplicaciones estará habilitada para todo el tráfico TCP. Si desea acelerar las aplicaciones SaaS, deberá seleccionar una CA/certificado raíz, como se muestra en el siguiente paso.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Seleccione el certificado que creó en un paso anterior.

Si necesita cambiar el certificado de uno existente, asegúrese de haber confirmado y enviado el certificado a sus cortafuegos y usuarios, luego selecciónelo aquí. Debes enviar el nuevo certificado antes de seleccionarlo.



*Después de importar el certificado, debe esperar hasta que la Aceleración de aplicaciones genere certificados específicos de dominio para cada aplicación. Este proceso puede tardar hasta una hora. Mientras tanto, puede mover el control deslizante de las **Accelerated Apps (Aplicaciones aceleradas)** a la izquierda para desactivar temporalmente la aceleración de aplicaciones y acceder a las aplicaciones hasta que se generen los certificados; si no lo hace, podría recibir un error SSL hasta que se generen los certificados.*

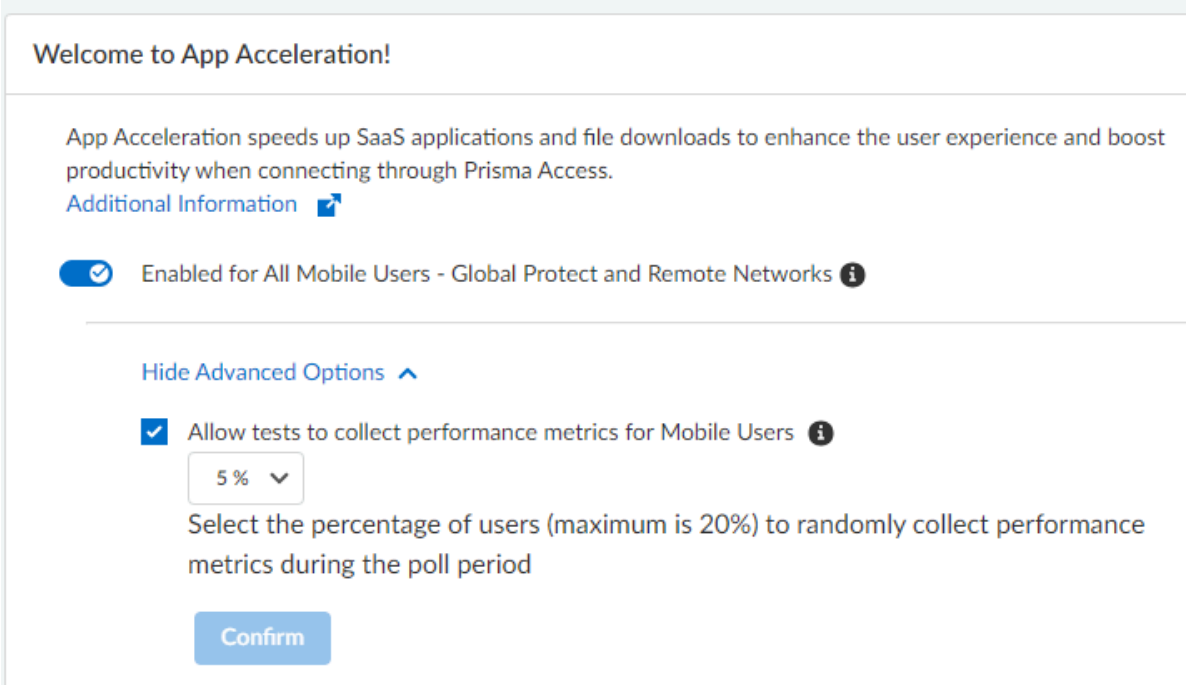
Espere hasta 10 minutos para que la aceleración esté activa después de haberla activado para una aplicación determinada.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | (Opcional) **Show Advanced Options (Mostrar opciones avanzadas)** y cambiar los parámetros de prueba métrica.

- (Opcional) Para deshabilitar la recopilación de métricas para obtener información de rendimiento, anule la selección de **Allow tests to collect performance metrics for Mobile Users (Permitir pruebas para recopilar métricas de rendimiento para usuarios móviles)**.

  Palo Alto Networks recomienda que habilite la recopilación de métricas para ver las mejoras de rendimiento de la aplicación cuando utilice la Aceleración de aplicaciones.
- (Opcional) Para cambiar el porcentaje de usuarios para los que se procesan pruebas predictivas desde el valor predeterminado del 5 %, seleccione otro porcentaje en el menú desplegable y seleccione **Confirm (Confirmar)** para confirmar los cambios.



 ©2025 Palo Alto Networks, Inc.

Configurar la aceleración de aplicaciones en Prisma Access (Panorama)

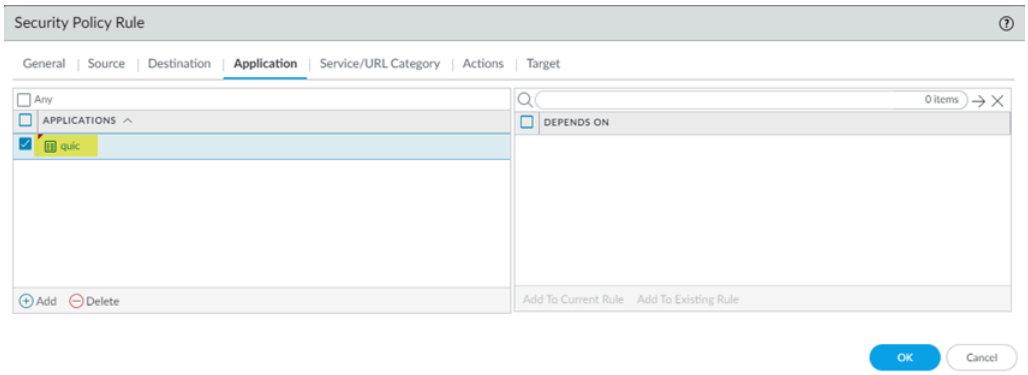
Para configurar la aceleración de aplicaciones en una implementación de Prisma Access (Managed by Panorama), complete esta tarea.

STEP 1 | (Opcional) Deshabilite el protocolo de Conexiones UDP rápidas en Internet (QUIC).

La aceleración de aplicaciones no puede acelerar las aplicaciones en Capa 7 sin deshabilitar QUIC.

1. Vaya a **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)** y seleccione **Add (Añadir)** una política de seguridad.

   Cree esta regla de política de seguridad en el grupo de dispositivos **Shared (Compartido)**.
2. Seleccione una **Application (Aplicación)** de **quic** y una **action (acción)** de **Deny (Denegar)**.



3. Seleccione **Add (Añadir)** para añadir una segunda política de seguridad.

   Es posible que las versiones más recientes de QUIC se identifiquen erróneamente como **unknown-udp**. Por este motivo, Palo Alto Networks recomienda añadir servicios para el puerto UDP 80 y el puerto UDP 443, y crear una política de seguridad adicional para bloquear el tráfico UDP en esos puertos.
4. En **Service/URL Category (Categoría de servicio/URL)**, seleccione **Add (Añadir)** un nuevo servicio para el puerto UDP 80 y el puerto UDP 443 y una **Action (Acción)** de **Deny (Denegar)**.

   Cuando se complete, tendrá dos políticas de seguridad: Uno que bloquea el protocolo QUIC y otro que bloquea el tráfico en los puertos UDP 80 y 443.

	NAME	LOCATION	APPLICATION	TAGS	ACTION	SERVICE	PROFILE
1	quic-deny	Shared	quic	none	Deny	application-...	none
2	quic-udp-deny	Shared	any	none	Deny	quic-udp80 quic-udp443	none

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Importe un certificado de entidad de certificación (CA) raíz y una clave privada en Panorama para usar con la Aceleración de aplicaciones y confirmar y enviar sus cambios.

Un certificado/CA raíz autofirmado es el certificado de mayor nivel de una cadena de certificados. La aceleración de aplicaciones utiliza los certificados/CA raíz para crear certificados para las aplicaciones aceleradas. Presione la CA raíz/certificado en Prisma Access para que Aceleración de aplicaciones pueda comenzar la creación de los certificados específicos de la aplicación.

El CA raíz/certificado debe tener estas características:

- La CA debe ser una CA de confianza.
- (Recomendado) La CA debe ser única y usarse solo para la aceleración de aplicaciones.
- La CA no puede estar caducada. Tome nota de la fecha de vencimiento de la CA y renueve el certificado antes de que caduque. Si la aceleración de aplicaciones que utiliza una CA/certificado caduca, los usuarios recibirán un error SSL al intentar acceder a aplicaciones

 ©2025 Palo Alto Networks, Inc.

aceleradas. Es fundamental asegurarse de que la CA es válida cuando su organización utiliza la aceleración de aplicaciones.

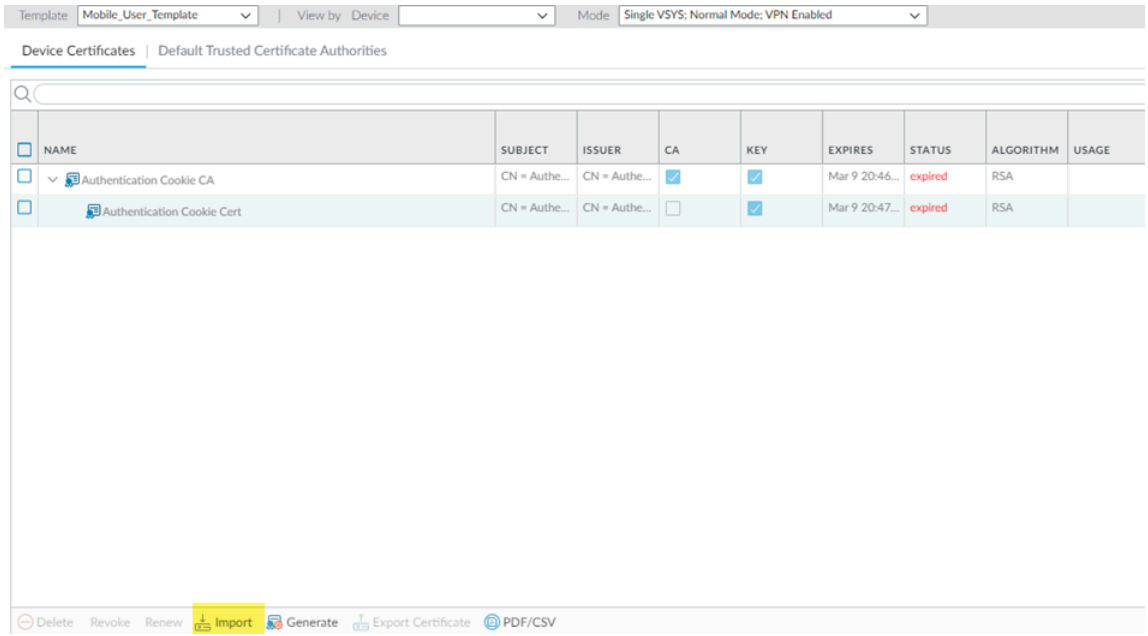
- Debe incluir una clave.
- Debe usar una frase de contraseña.
- (Usuarios móviles: solo implementaciones de GlobalProtect) Debe instalarse en el almacén local de certificados raíz.

  Puede realizar esta instalación añadiéndola a la lista de certificados de confianza como se describe en este procedimiento o, si utiliza ActiveDirectory, puede distribuir la CA raíz desde AD mediante un objeto de política de grupo (GPO) de Active Directory.

Si alguna vez necesita cambiar la CA/certificado raíz, debe cargarlo y confirmar y enviar sus cambios antes de poder usar el certificado cambiado.

1. Vaya a **Device (Dispositivo)** > **Certificates (Certificados)** > **Certificate Management (Gestión de certificados)**.

   Asegúrese de que está en Mobile_User_Template.
2. **Import (Importar)** un certificado.



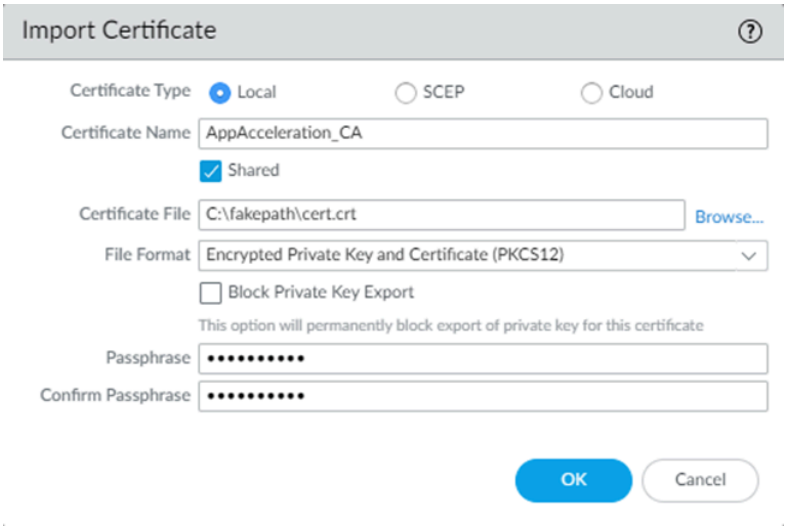
3. Seleccione los siguientes parámetros:
   - Introduzca un **Certificate Name (Nombre de certificado)** único para el certificado, como `AppAcceleration_CA`.

     El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 31 caracteres de longitud. Utilice solamente letras, números, guiones y guiones bajos.
   - Busque el **Certificate File (Archivo de certificado)** recibido de la CA y seleccione **Open (Abrir)** para abrirlo.
   - Seleccione un **Format (Formato)**:

 ©2025 Palo Alto Networks, Inc.

- **Encrypted Private Key and Certificate (PKCS12) [Clave privada cifrada y certificado (PKCS12)]**: este es el formato predeterminado y más común, en el que la clave y el certificado están en un único contenedor (Archivo del certificado).
- **Certificado codificado en Base64 (PEM)**: debe importar la clave independientemente del certificado. Debe **Import Private Key (Importar clave privada)** y seleccionar un **Key File (Archivo de clave)** si selecciona este formato.
- Introduzca una **Passphrase (Frase de contraseña)** y seleccione **Confirm Passphrase (Confirmar frase de contraseña)**.

4. Haga clic en **OK (Aceptar)**.



5. Repita estos pasos, sustituyendo Remote_Network_Template para la Mobile_User_Template.

   Debe importar estos certificados tanto en Mobile_User_Template como Remote_Network_Template para acelerar las aplicaciones para sus usuarios móviles y usuarios en sitios de red remotos.

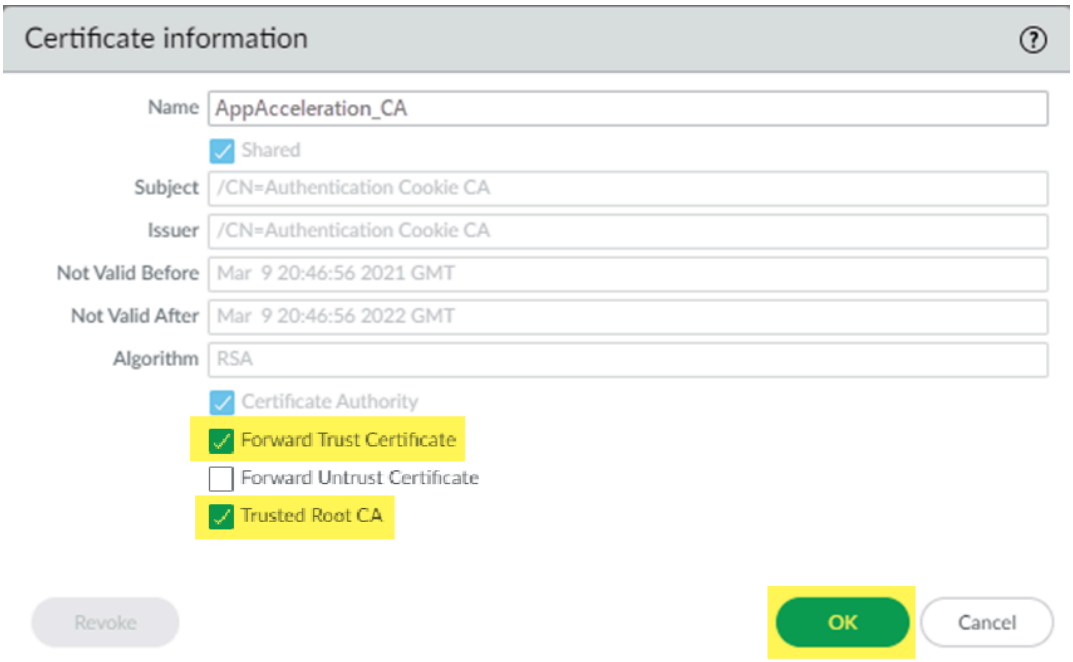
STEP 3 | Marque la CA raíz/certificado que añadió como un certificado de confianza de reenvío y una CA raíz de confianza.

Si no especifica el certificado como un certificado de confianza de reenvío y una CA raíz de confianza, los usuarios encontrarán errores SSL al intentar acceder a aplicaciones

 ©2025 Palo Alto Networks, Inc.

aceleradas al usar el descifrado SSL. Si tiene certificados en Mobile_User_Template y Remote_Network_Template, realice este paso en ambas plantillas.

1. Seleccione la CA raíz/certificado que añadió.
2. Seleccione el certificado como un **Forward Trust Certificate (Certificado de reenvío fiable)** y **Trusted Root CA (CA raíz de confianza)** y haga clic en **OK (Aceptar)**.



STEP 4 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

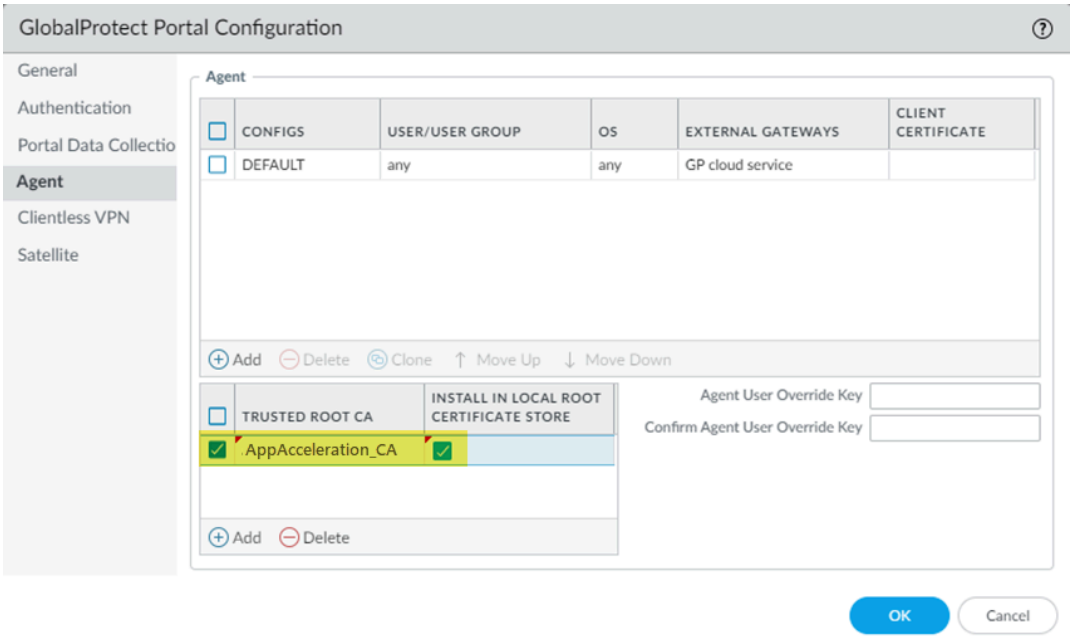
 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Usuarios móviles: solo implementaciones de GlobalProtect) Añada la CA raíz/certificado que añadió a la lista de certificados de confianza de GlobalProtect en la configuración del portal de GlobalProtect.

De forma alternativa, si está usando ActiveDirectory, puede distribuir la CA raíz desde AD usando un GPO de Active Directory.

1. Vaya a **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **GlobalProtect_Portal** > **Agent (Agente)**.

   Asegúrese de que está en Mobile_User_Template.
2. Seleccione **Add (Añadir)** la CA raíz de confianza que creó en un paso anterior.
3. Seleccione **Install in Local Root Certificate Store (Instalar en el almacén de certificados raíz local)**.
4. Haga clic en **OK (Aceptar)**.

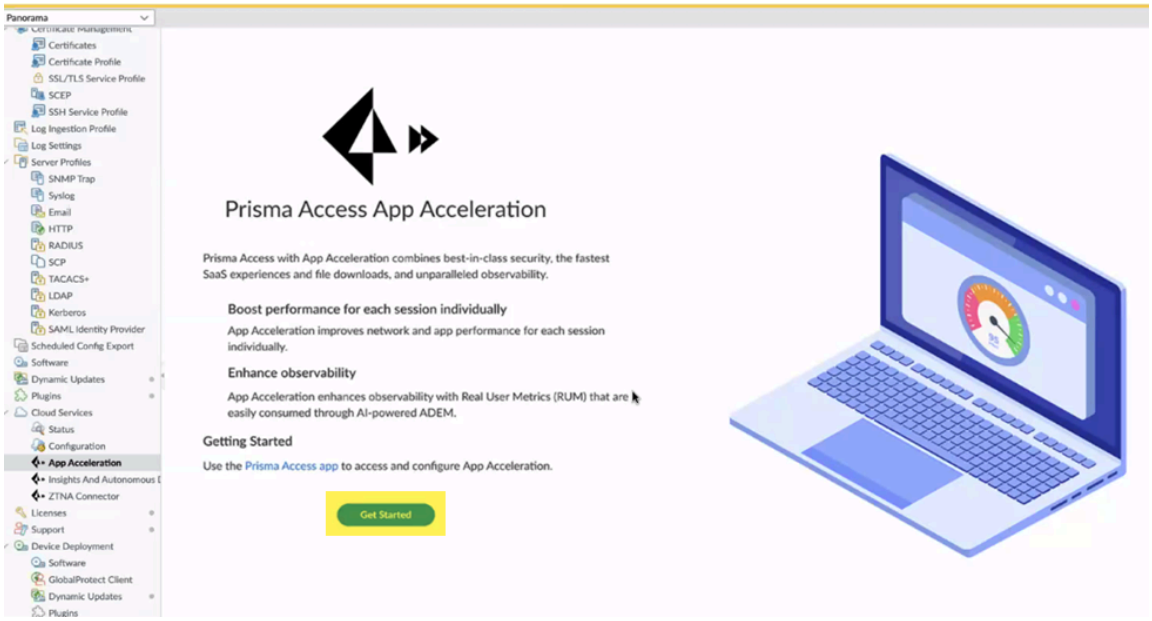


5. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

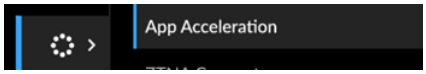
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Habilite la aceleración de aplicaciones y elija el archivo de certificado que creó.

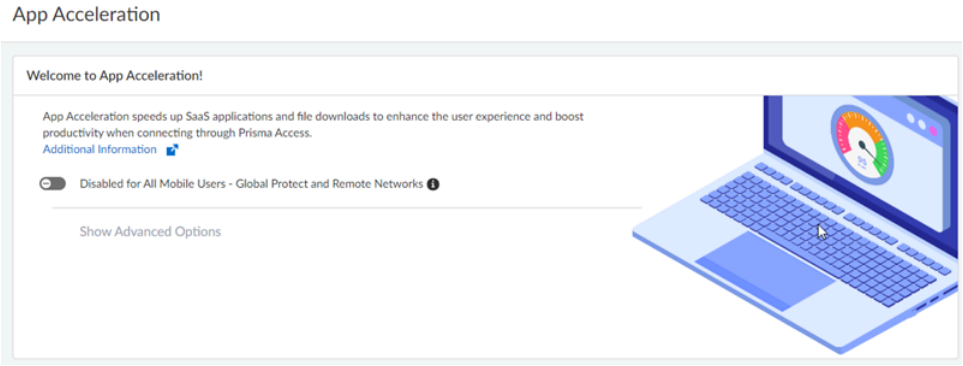
1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **App Acceleration (Aceleración de aplicaciones)** y **Get Started (Comenzar)** con la aceleración de aplicaciones.



2. Vaya a **Workflows (Flujos de trabajo)** > **App Acceleration (Aceleración de aplicaciones)** desde la barra de navegación izquierda..



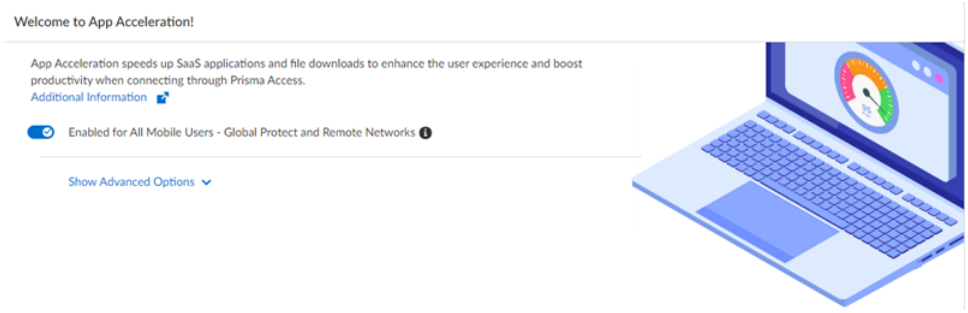
Aparecerá la ventana de aceleración de aplicaciones.



3. Mueva el control deslizante hacia la derecha para que la aceleración de aplicaciones esté **Enabled for all Mobile Users—GlobalProtect and Remote Networks (Habilitada para todos los usuarios móviles: GlobalProtect y Redes remotas)**.

Si las confirmaciones están en curso, la configuración de aceleración de la aplicación entrará en vigor después de que se completen todos las confirmaciones.

 ©2025 Palo Alto Networks, Inc.



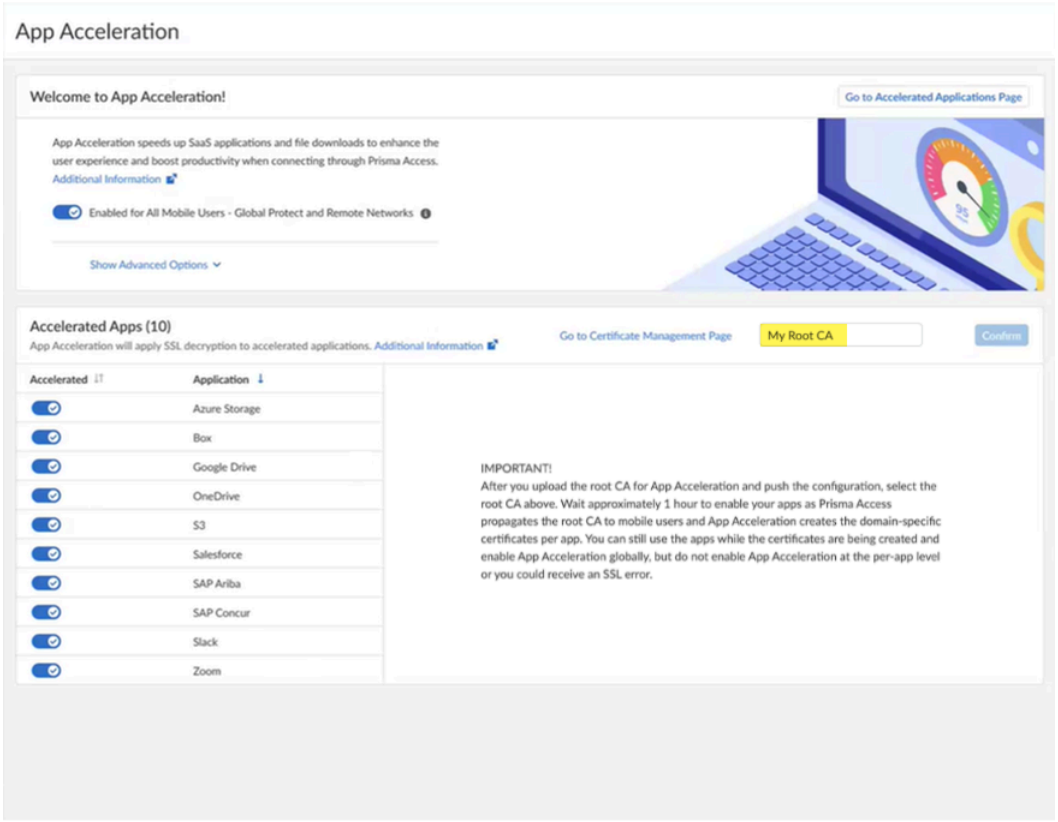
Aceleración de aplicaciones estará habilitada para todo el tráfico TCP. Si desea acelerar las aplicaciones SaaS, deberá seleccionar una CA/certificado raíz, como se muestra en el siguiente paso.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | En la configuración de Aceleración de aplicaciones, escriba el nombre del certificado que creó en un paso anterior exactamente como se muestra en Panorama.

Asegúrese de haber confirmado y enviado el certificado antes de escribirlo.

Si necesita cambiar el certificado de uno existente, escriba el nuevo nombre. Debe escribir el nombre (no puede seleccionarlo de una lista) y debe confirmar y enviar el nuevo certificado antes de introducir el nombre.



Después de importar el certificado, debe esperar hasta que la Aceleración de aplicaciones genere certificados específicos de dominio para cada aplicación. Este proceso puede tardar hasta una hora. Mientras tanto, puede mover el control deslizante de las ***Accelerated Apps (Aplicaciones aceleradas)*** *a la izquierda para desactivar temporalmente la aceleración de aplicaciones y acceder a las aplicaciones hasta que se generen los certificados; si no lo hace, podría recibir un error SSL hasta que se generen los certificados.*

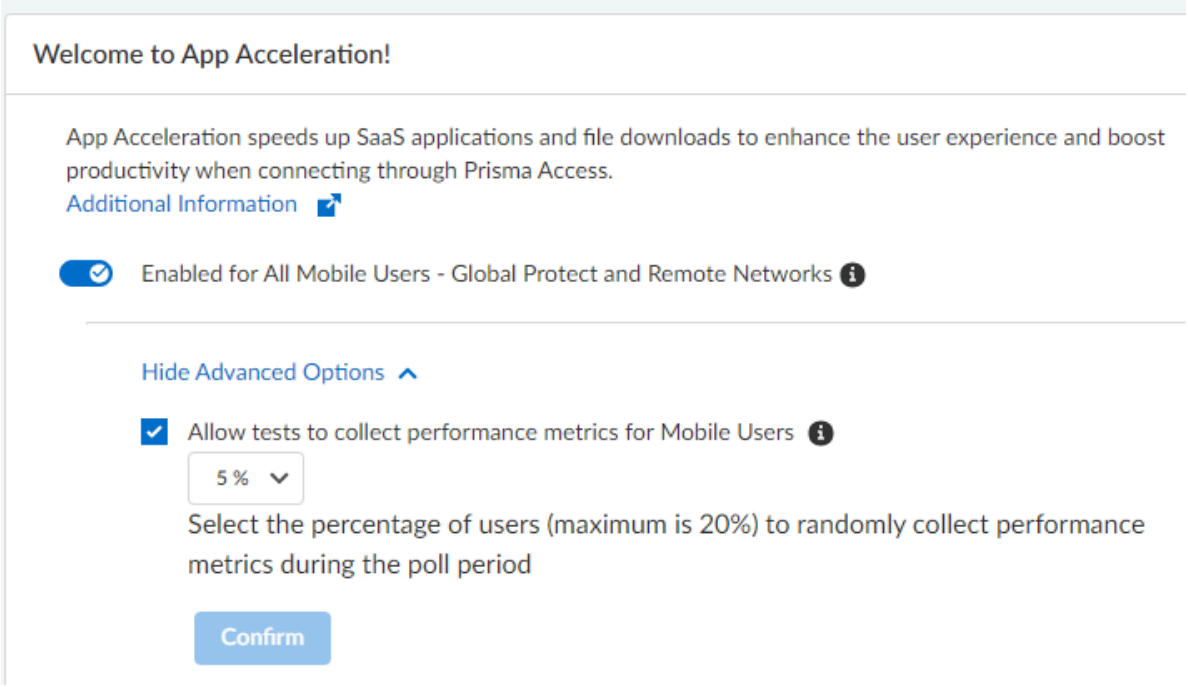
Espere hasta 10 minutos para que la aceleración esté activa después de haberla activado para una aplicación determinada.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | (Opcional) **Show Advanced Options (Mostrar opciones avanzadas)** y cambiar los parámetros de prueba métrica.

- (Opcional) Para deshabilitar la recopilación de métricas para obtener información de rendimiento, anule la selección de **Allow tests to collect performance metrics for Mobile Users (Permitir pruebas para recopilar métricas de rendimiento para usuarios móviles)**.

  Palo Alto Networks recomienda que habilite la recopilación de métricas para ver las mejoras de rendimiento de la aplicación cuando utilice la Aceleración de aplicaciones.
- (Opcional) Para cambiar el porcentaje de usuarios para los que se procesan pruebas predictivas desde el valor predeterminado del 5 %, seleccione otro porcentaje en el menú desplegable y seleccione **Confirm (Confirmar)** para confirmar los cambios.



 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access usuarios móviles

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access ofrece dos métodos de conexión para proteger a los usuarios móviles: los usuarios pueden conectarse a Prisma Access mediante la aplicación GlobalProtect o mediante un archivo de configuración automática de proxy (PAC).

- **Proteja a los usuarios móviles con la aplicación GlobalProtect**

  Puede utilizar GlobalProtect en los siguientes modos:

  - Modo túnel: el modo de agente predeterminado para GlobalProtect en Prisma Access. Establece un túnel (IPSec o SSL) a Prisma Access para asegurar el acceso de los usuarios móviles a todas las aplicaciones, puertos y protocolos, y para obtener una seguridad consistente tanto si el usuario está dentro como fuera de su red.

    La aplicación GlobalProtect instalada en el endpoint de los usuarios asegura el tráfico de usuarios a Internet, las aplicaciones SaaS y sus recursos internos y de nube pública. Implemente la aplicación GlobalProtect a sus usuarios (disponible para teléfonos inteligentes, tabletas o portátiles con Microsoft Windows, Apple macOS e iOS, Android, Google Chrome OS y Linux) para que puedan tunelizar el tráfico a Prisma Access para la aplicación de políticas y la prevención de amenazas. La aplicación GlobalProtect también proporciona informes de perfil de información de host (HIP) para que pueda crear reglas granulares basadas en el estado del dispositivo para garantizar que los endpoints se adhieran a sus estándares de seguridad (por ejemplo, están equipados con los parches, cifrado y definiciones de virus más actualizados) para acceder a sus aplicaciones más sensibles. O, para permitir el acceso seguro a los usuarios en dispositivos no gestionados, puede habilitar VPN sin cliente. Prisma Access escala dinámicamente dentro y fuera por región según dónde se encuentren sus usuarios en ese momento.
  - Modo proxy: este modo le permite usar un agente VPN de terceros sin dejar de usar Prisma Access como una puerta de enlace web segura para una seguridad SaaS coherente y superior. Este método de conexión es ideal si aún no está listo para reemplazar su VPN de aplicación privada existente, pero desea reemplazar su puerta de enlace web segura. Por ejemplo, está usando un agente VPN de terceros para el acceso privado, pero quiere usar solo Prisma Access para su seguridad en Internet. Los beneficios de este método de conexión incluyen:
    - Cumple con los requisitos de red o de cumplimiento que requiere un proxy
    - Reduce la carga de la gestión de archivos PAC y admite aplicaciones compatibles con proxy más allá del navegador
    - Mejora la experiencia del usuario evitando la necesidad de volver a un proxy web local

- Modo túnel y proxy: este modo le permite asegurar el acceso a Internet y a las aplicaciones SaaS a través del modo proxy, y asegurar el acceso a las aplicaciones privadas a través del modo túnel. Esto es especialmente útil si necesita el acceso más rápido y de menor latencia a una aplicación privada y su ubicación de Prisma Access no se encuentra en su región.

  De este modo, la aplicación GlobalProtect evalúa primero las reglas de reenvío del proxy explícito que has definido y envía todo el tráfico vinculado a Internet al proxy explícito de Prisma Access. Para el resto del tráfico, la aplicación determina qué tráfico enviar a través del túnel a la puerta de enlace de GlobalProtect y qué tráfico excluir del túnel, en función de las reglas de túnel dividido que haya definido. También puede usar el túnel para proteger cualquier aplicación que no detecta el proxy.

- **Proteja a los usuarios móviles usando un archivo PAC**

  Además de proteger a usuarios móviles con GlobalProtect, puede configurar un proxy explícito utilizando Prisma Access. Con Proxy explícito, un endpoint utiliza un archivo PAC que indica a un navegador web y a las aplicaciones compatibles con proxy que reenvíen tráfico al servidor proxy web en lugar de al servidor de destino, protegiendo el tráfico de Internet basado en web (HTTP y HTTPS).

  Si la red existente de su organización ya utiliza proxies explícitos e implementa archivos PAC en los endpoints y servidores de sus clientes, puede migrar sin problemas de las soluciones SWG basadas en proxies heredados de Prisma Access a la protección del tráfico de internet saliente de los usuarios móviles. También puede usar un proxy explícito si necesita usar un proxy por motivos de auditoría o cumplimiento.

- **Usuarios móviles seguros con Prisma Access Browser Mobile**

  Prisma Access Browser Mobile simplifica la seguridad de los usuarios móviles al combinar controles de acceso fuertes con una interfaz clara e intuitiva. Permite a los usuarios acceder a aplicaciones privadas de forma segura sin depender de VPN, certificados o sistemas de gestión de dispositivos móviles (MDM), lo que reduce la complejidad y facilita la conectividad.

  Diseñado para entornos Bring Your Own Device (BYOD), garantiza el acceso seguro a aplicaciones privadas en dispositivos no gestionados, lo que permite a las organizaciones extender los recursos críticos a toda su fuerza laboral. Las tabletas se convierten en alternativas versátiles de escritorio a través de Prisma Access Browser Mobile, ofreciendo el mismo nivel de seguridad y acceso que los endpoints tradicionales.

  Con Prisma Access Browser Mobile, su organización puede optimizar el acceso a aplicaciones privadas, mejorar la productividad basada en tabletas y mantener una seguridad fiable en diversas plataformas móviles.

 ©2025 Palo Alto Networks, Inc.

Usuarios móviles: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

GlobalProtect le permite proteger a los usuarios móviles instalando la aplicación GlobalProtect en sus dispositivos y configurando los ajustes de GlobalProtect en Prisma Access. GlobalProtect permite asegurar el acceso de los usuarios móviles a todas las aplicaciones, puertos y protocolos, y obtener una seguridad coherente ya sea que el usuario esté dentro o fuera de su red.

Cuando protege a los usuarios móviles utilizando GlobalProtect, necesitará definir la configuración para configurar el portal y las puertas de enlace en la nube. Por ejemplo, definirá un nombre de host del portal, configurará el grupo de direcciones IP para sus usuarios móviles y configurará los ajustes de DNS para sus dominios internos. Es posible que pueda aprovechar las configuraciones existentes para algunos de los ajustes requeridos, como qué perfil de autenticación utilizar para autenticar a los usuarios móviles. Si ya tiene una plantilla con sus perfiles de autenticación, certificados, perfiles de certificados y perfiles de servidor, puede añadir esa plantilla a la pila de plantillas predefinidas durante la incorporación para simplificar el proceso de configuración.

Además, si desea que sus usuarios móviles puedan conectarse a sus ubicaciones de red remotas, o si tiene usuarios móviles en diferentes áreas geográficas que necesitan acceso directo a los endpoints de los demás, debe configurar al menos una conexión de servicio con valores de marcador de posición, incluso si no planea usar la conexión para proporcionar acceso a su centro de datos o ubicaciones de la sede. La razón por la que esto es necesario es porque, aunque todas las ubicaciones de red remotas están completamente interconectadas, las puertas de enlace de Prisma Access (también conocidas como *ubicaciones*) se conectan a la conexión de servicio en una arquitectura de hub y radio para proporcionar acceso a las redes internas de su infraestructura de Prisma Access.

- Lista de verificación de planificación para GlobalProtect en Prisma Access
- Configurar usuarios móviles de GlobalProtect
- GlobalProtect: Personalizar la configuración del túnel
- Solicitud de ticket para desactivar GlobalProtect (Strata Cloud Manager)
- Supervisar Usuarios móviles de GlobalProtect
- Grupos de direcciones IP para una implementación de usuarios móviles de GlobalProtect
- Cómo selecciona la aplicación GlobalProtect Ubicaciones de Prisma Access para usuarios móviles
- Lista de permitidos de usuarios móviles de GlobalProtect
- Actualizaciones de la aplicación GlobalProtect
- Integrar Prisma Access con las puertas de enlace GlobalProtect locales

 ©2025 Palo Alto Networks, Inc.

Lista de verificación de planificación para GlobalProtect en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Si usa GlobalProtect para proteger a los usuarios móviles, utilice la siguiente lista de comprobación para asegurarse de que podrá habilitar correctamente el servicio y aplicar una política coherente para sus usuarios móviles (proteger a los usuarios con la aplicación GlobalProtect instalada en sus terminales y permitir que los usuarios accedan de forma segura a las aplicaciones utilizando la VPN sin cliente).

- ☐ **Lista de verificación previa a la instalación:**
  - **Grupo de direcciones IP**: para configurar Prisma Access para los usuarios, debe proporcionar un Grupo de direcciones IP que no se superponga con otras direcciones IP que utilice internamente o con el grupo de direcciones IP que designó para la Subred de infraestructura.

    Recomendamos usar un grupo de direcciones IP compatible con RFC 1918 y RFC 6598. Aunque se admite el uso de direcciones IP (públicas) no compatibles con RFC 1918, no lo recomendamos debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.

    No especifique ninguna subred que se solape con las siguientes direcciones IP y subredes, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno:

    169.254.0.0/16 y 100.64.0.0/10

    Prisma Access usa este grupo de direcciones IP para asignar direcciones IP a los adaptadores de red virtual de los endpoints cuando se conectan a Prisma Access utilizando la aplicación GlobalProtect. Cada dispositivo que se conecta a una puerta de enlace de usuario móvil de Prisma Access requiere su propia dirección IP. Estos grupos se especifican durante el proceso de incorporación de usuarios móviles.

    Palo Alto Networks recomienda que el número de direcciones IP en el grupo sea 2 veces el número de dispositivos de usuario móvil que se conectarán a Prisma Access. Si su organización tiene una política de traer su propio dispositivo (BYOD), o si un solo usuario tiene varias cuentas de usuario, asegúrese de tener en cuenta esos dispositivos y cuentas adicionales al asignar sus grupos de IP. Si el grupo de direcciones IP alcanza su límite, los dispositivos de usuario móvil adicionales no podrán conectarse.

    Cuando los dispositivos de usuario móvil se conectan a una puerta de enlace, Prisma Access toma direcciones IP de los grupos especificados y las asigna a la puerta de enlace en bloques /24. Cuando un bloque /24 alcanza su límite a medida que más dispositivos de usuario inician sesión, Prisma Access asigna más bloques /24 del grupo a la puerta de enlace. Prisma Access anuncia estas subredes /24 en su red troncal, ya que se asignan en función de sus asignaciones de puerta de enlace.

 ©2025 Palo Alto Networks, Inc.

- **Plantilla**: la implementación Prisma Access GlobalProtect crea automáticamente una pila de plantillas y una plantilla de nivel superior. Si ya está ejecutando GlobalProtect en las instalaciones y desea aprovechar su configuración existente, puede añadir plantillas adicionales a la pila para impulsar las existentes Portal GlobalProtect, Puerta de enlace de GlobalProtect, User-ID, perfil del servidor (por ejemplo, para conectarse a su servicio de autenticación), certificado y configuraciones de Perfil de servicio SSL/TLS para los usuarios de Prisma Access. Si no dispone de plantillas con los valores de configuración existentes, puede introducir manualmente los ajustes de configuración necesarios cuando configura GlobalProtect en Prisma Access (Managed by Panorama). Además, las plantillas que añada a la pila deben contener la configuración de zona de las zonas que utilice para aplicar la política de seguridad a los usuarios móviles.
- **Grupo de dispositivos principales**: al configurar Prisma Access para los usuarios, debe especificar un grupo de dispositivos principal que se utilizará al insertar los grupos de direcciones y Política de seguridad, Perfiles de seguridad, otros objetos de política (como grupos de aplicaciones y objetos), Objetos y perfiles HIP y política de autenticación que el servicio requiere para aplicar una política coherente para los usuarios remotos.
- **Ubicaciones a incorporar**: Prisma Access le proporciona ubicaciones en todo el mundo donde puede configurar GlobalProtect en Prisma Access (Managed by Panorama). Antes de incorporar sus ubicaciones, consulte esta lista para determinar qué ubicaciones debe incorporar para la implementación de usuarios móviles.

  Elija las ubicaciones más cercanas a sus usuarios o en el mismo país que sus usuarios. Si una ubicación no está disponible en el país donde residen los usuarios de dispositivos móviles, puede elegir una ubicación que utilice el mismo idioma que los usuarios de dispositivos móviles.

  También puede dividir las ubicaciones por región geográfica. Mantener todas las ubicaciones en una sola región le permite: especificar un grupo de direcciones IP solo para esa región, lo que puede ser útil si tiene un número limitado de direcciones IP que puede asignar al grupo. Un único grupo de direcciones IP regionales también proporciona un control más granular sobre las regiones implementadas y le permite excluir regiones según lo requieran las regulaciones de su política o del sector.

  Si tiene una licencia local para Prisma Access para Usuarios y tiene una implementación de GlobalProtect, así como una implementación de Proxy explícito, puede implementar un máximo de cinco ubicaciones para ambas implementaciones combinadas. Debe asignar las cinco ubicaciones entre ambas implementaciones (por ejemplo, dos ubicaciones para usuarios móviles: GlobalProtect y tres ubicaciones para Usuarios móviles: Proxy explícito). Si tiene una licencia Worldwide, no hay restricciones para el número máximo de ubicaciones.
- **Nombre de host del portal**: Prisma Access para usuarios le permite configurar de forma rápida y sencilla el nombre de host del portal mediante un nombre de dominio predeterminado (`.gpcloudservice.com`). En este caso, el servicio en la nube publica automáticamente el nombre de host en servidores DNS públicos y se encarga de toda la generación de certificados. Sin embargo, puede optar por utilizar el nombre de dominio de su propia empresa en el nombre de host del portal. Si planifica utilizar el nombre de dominio de su empresa, debe obtener sus propios certificados para el portal y configurar un Perfil de servicio SSL/TLS para apuntar al certificado antes de configurar el servicio. Además, si utiliza su propio nombre de dominio en el nombre de host del portal, también debe configurar los servidores DNS para que apunten al CNAME DNS del portal, que se proporciona durante el proceso de configuración.

 ©2025 Palo Alto Networks, Inc.

- **Conexión de servicio**: debe crear y configurar una conexión de servicio si desea permitir que los usuarios móviles accedan a recursos, como servidores de autenticación, en su red interna (por ejemplo, un servidor de autenticación en su centro de datos o ubicación central) o permitir que los usuarios móviles accedan a sus ubicaciones de red remotas.

  Incluso si no planea usar la conexión para proporcionar acceso a los recursos internos, debe configurar al menos una conexión de servicio con valores de marcador de posición si desea que los usuarios móviles puedan conectarse a las ubicaciones de red remotas o si tiene usuarios móviles en diferentes áreas geográficas que necesitan acceso directo a los endpoints de los otros.
- **Uso de IPv6 en su red**: determine si desea realizar alguna mitigación para el tráfico IPv6 en su red para reducir la superficie expuesta a ataques. En un endpoint de pila dual que puede procesar tráfico IPv4 e IPv6, el tráfico IPv6 del usuario móvil no se envía a Prisma Access de forma predeterminada y, en su lugar, se envía al adaptador de red local en el endpoint. Por este motivo, Palo Alto Networks recomienda configurar Prisma Access para el tráfico IPv6 de sumidero.
- **Registro de logs de endpoints de GlobalProtect**: tiene dos opciones para recopilar logs de los usuarios móviles que utilizan la aplicación GlobalProtect:
  - **Recopilación manual de logs de los endpoints de GlobalProtect**: pida a los usuarios móviles que recopilen los logs de la aplicación GlobalProtect para dispositivos Windows, macOSy Linux. Esta opción no requiere ninguna configuración adicional.
  - **Recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas**: permite que la aplicación GlobalProtect realice pruebas de diagnóstico de extremo a extremo para resolver problemas de conexión, rendimiento y acceso, y generar logs de diagnóstico y resolución de problemas para enviarlos a Strata Logging Service para un análisis más detallado. Debe generar un certificado para que la aplicación GlobalProtect pueda autenticarse con Strata Logging Service para recopilar los logs de resolución de problemas. Con **Prisma Access (Managed by Strata Cloud Manager)**, puede permitir que la aplicación GlobalProtect recopile logs de Strata Logging Service para la resolución de problemas. Para **Prisma Access (Managed by Panorama)**, esta funcionalidad se encuentra en **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** > **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Generar certificado para la recopilación de logs de la aplicación de GlobalProtect y Autonomous DEM)**. Consulte Recopilación de logs de aplicaciones GlobalProtect para la resolución de problemas para obtener detalles de configuración.

☐ **Lista de verificación posterior a la instalación:**

- **Añada las direcciones IP públicas a una lista de permitidos en su red**: después de incorporar sus ubicaciones, necesita las direcciones IP y públicas utilizadas por cada ubicación y añada las direcciones IP de estas ubicaciones a una lista de permitidos en su red para permitir que los usuarios móviles accedan a SaaS o aplicaciones públicas. Si añade más ubicaciones, también deberá recuperar las nuevas direcciones IP que Prisma Access asigna para la ubicación o ubicaciones recién añadidas.
- **Coherencia de nomenclatura de puerta de enlace**: si ya tiene una implementación de Usuarios móviles: GlobalProtect y su organización tiene una actividad de fusiones y adquisiciones (M&A), es posible que necesite que las puertas de enlace existentes no hagan referencia a un nombre de marca anterior o que hagan referencia a un nuevo nombre de

 ©2025 Palo Alto Networks, Inc.

marca. En este caso, póngase en contacto con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de SRE para gestionar la solicitud. Palo Alto Networks recomienda que programe este cambio durante una ventana de mantenimiento o durante las horas de menor actividad. Palo Alto Networks actualiza todas las puertas de enlace de su implementación que requieren el cambio de nombre durante el período de mantenimiento.

Configurar usuarios móviles de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Antes de configurar los usuarios móviles, asegúrese de tener las licencias necesarias (licencia de Prisma Access para usuarios móviles y una licencia de Strata Logging Service con espacio de almacenamiento de cortafuegos adecuado). Si los usuarios de dispositivos móviles se conectan a otras redes conectadas, necesitará la licencia Zero Trust Network Access (ZTNA) o Prisma Access Enterprise Edition que proporcionará el nodo de acceso corporativo (CAN) necesario para conectarse.

Para configurar Prisma Access para usuarios móviles, necesitará lo siguiente:

- Prisma Access para usuarios móviles: Compruebe que la licencia de Prisma Access para usuarios móviles está activada.
- Grupo de direcciones IP para usuarios móviles: Compruebe que tiene uno o más grupos de direcciones IP no superpuestos disponibles para usuarios móviles.
- Nombre de host del portal Asegúrese de conocer el nombre de dominio completamente cualificado (FQDN) del portal.
- Agente GlobalProtect para usuarios móviles: Prisma Access para usuarios móviles requiere la aplicación GlobalProtect en cada endpoint compatible. Necesitará una estrategia de implementación para instalar el agente de Prisma Access en dispositivos de usuario móviles.
- Información de la Regla de la política de seguridad: Implementará reglas de política de seguridad para permitir o denegar el tráfico a través de Prisma Access. Deberá saber qué reglas implementar al configurar Prisma Access para sus usuarios móviles.
- Ubicaciones geográficas de sus usuarios móviles: Cuando aprovisiona usuarios móviles, debe seleccionar una ubicación geográfica disponible que esté cerca de sus usuarios móviles.

Aprenda cómo incorporar a los usuarios móviles de GlobalProtect a Prisma Access.

- Strata Cloud Manager
- Panorama

Configurar usuarios móviles de GlobalProtect (Strata Cloud Manager)

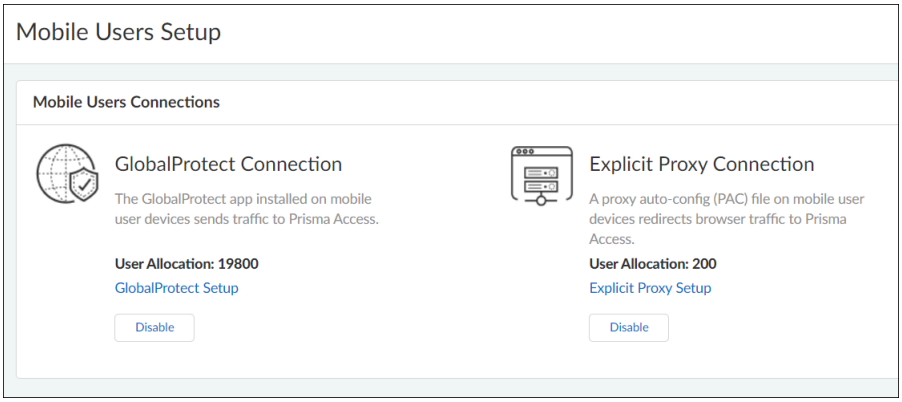
En solo unos pocos pasos, aquí le mostramos cómo comenzar a incorporar Usuarios móviles: GlobalProtect a Prisma Access.

 ©2025 Palo Alto Networks, Inc.

1. **Habilite GlobalProtect como tipo de conexión de usuario móvil**

   Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)**.

   Puede dividir su licencia de usuario móvil entre GlobalProtect y conexiones proxy explícitas; algunos usuarios pueden conectarse a través de GlobalProtect y otros a través de Proxy explícito. Con una **conexión GlobalProtect**, la aplicación GlobalProtect instalada en los dispositivos móviles de los usuarios envía tráfico a Prisma Access.

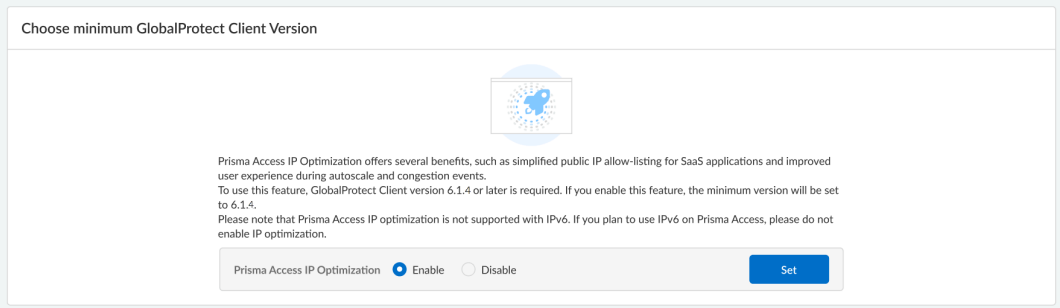


 ©2025 Palo Alto Networks, Inc.

2. **Establecer la configuración básica de la infraestructura**

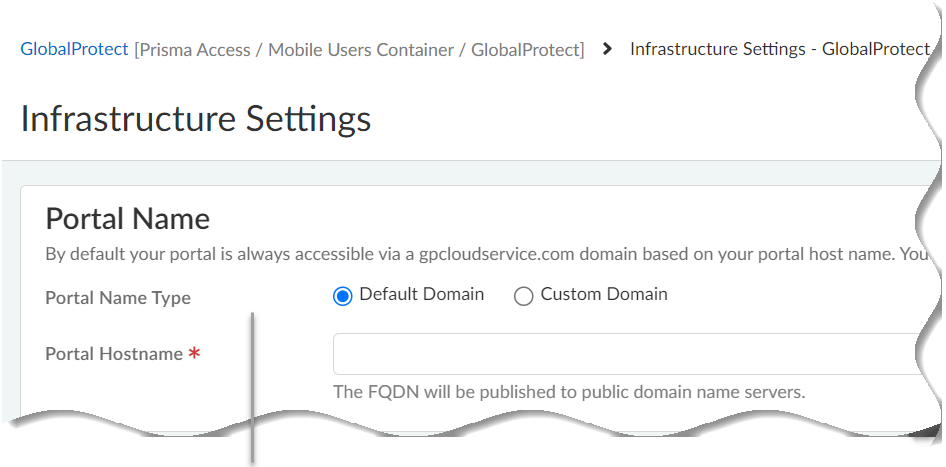
   Configure los ajustes de infraestructura que son específicos de GlobalProtect. Hay algunas configuraciones obligatorias que deberá completar inicialmente, para que Prisma Access pueda aprovisionar su entorno de usuario móvil.

   - *Cuando configure GlobalProtect por primera vez, decidirá si habilitar o no la optimización de IP de Prisma Access. La elección de habilitar la Optimización de IP requiere la versión de cliente GlobalProtect 6.1.4 y posteriores, 6.2.3 y posteriores o 6.3.0 y posteriores, y no es compatible con IPv6. Seleccione con cuidado, ya que no podrá cambiar esta configuración más adelante.*
   - *La funcionalidad de optimización de IP es para nuevas implementaciones de Prisma Access únicamente. Las implementaciones existentes de GlobalProtect, incluidos los nuevos inquilinos que cree a partir de una implementación multiinquilino existente, no son elegibles.*
   - *Si está migrando su implementación de GlobalProtect a Prisma Access (lejos de utilizar portales y puertas de enlace locales), asegúrese de que todos los usuarios estén ejecutando la versión 6.1.4 y posteriores de la aplicación GlobalProtect, 6.2.3 y posteriores, o 6.3 y posteriores antes de habilitar esta funcionalidad.*



   Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** > **Infrastructure Settings (Configuración de infraestructura)**.

 ©2025 Palo Alto Networks, Inc.



GlobalProtect Infrastructure Settings

- Especifique el **nombre del portal**.
  - **Default Domain (Dominio predeterminado)**: si selecciona esta opción, el nombre de host de su portal utiliza el nombre de dominio predeterminado: `.gpcloudservice.com`. En este caso, basta con introducir un **Portal Hostname (Nombre de host del portal)** para anexar al nombre de dominio predeterminado. Prisma Access para usuarios creará automáticamente los certificados necesarios y publicará el nombre de host en servidores DNS públicos.
  - **Custom Domain (Dominio personalizado)**: también puede personalizar la dirección del portal si desea que el dominio del nombre de host del portal coincida con el nombre de dominio de su empresa (por ejemplo, myportal.mydomain.com).
- Introduzca la configuración de resolución de **DNS Client (DNS del cliente)** para su implementación de GlobalProtect.
  - Seleccione una región para los **DNS Servers (Servidores DNS)** [**Add Region (Añadir región)**].

    Seleccione **Worldwide (Mundial)** o un teatro. Si especifica varias configuraciones de proxy con una combinación de configuraciones Worldwide (Mundial) y de teatro, Prisma Access utiliza la configuración del grupo de ubicación, luego teatro y luego Mundial. Prisma Access evalúa las reglas de arriba hacia abajo en la lista.
  - Elija si desea o no que Prisma Access proceda a **Resolve internal domains (Resolver dominios internos)**; si lo hace, deberá **Add (Añadir)** una o más **Internal Domain Resolve Rules (Reglas internas de resolución de dominio)**.
  - Introduzca un **Name (Nombre)** único para la plantilla.
  - Seleccione **Prisma Access Default (Prisma Access predeterminado)** para utilizar el servidor DNS predeterminado de Prisma Access para resolver dominios internos. Si desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios a resolver en la **Domain List (Lista de dominios)**. Especifique un asterisco

 ©2025 Palo Alto Networks, Inc.

delante del dominio; por ejemplo, *.acme.com. Puede especificar un máximo de 1.024 entradas de dominio.

- Si tiene un servidor DNS **Custom (Personalizado)** que pueda acceder a sus dominios internos, especifique las direcciones IP del servidor **Primary DNS (DNS primario)** y **Secondary DNS (DNS secundario)**.
- Si desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios que desea resolver en las **Domain Lists (Listas de dominios)**. Especifique un asterisco delante del dominio; por ejemplo, *.acme.com. Puede especificar un máximo de 1.024 entradas de dominio.
- Cuando haya terminado, deberá **Save (Guardar)** los cambios.

- (Opcional) Especifique un **Client IP Pool (Grupo de direcciones IP de cliente)**.

  Por defecto, Prisma Access le proporciona un grupo de direcciones IP de usuario móvil predeterminado de 100.127.0.0/16 que se puede usar en cualquier ubicación del mundo. Prisma Access asigna una dirección IP de este grupo a cada dispositivo conectado a GlobalProtect. Opcionalmente, puede añadir un grupo de direcciones IP por región aquí.

  - Introduzca una subred mínima requerida de /23 (512 direcciones IP) por ubicación. Las ubicaciones adicionales requieren una subred /23 como mínimo. Si especifica una subred mundial, la subred mínima requerida es /23, pero recomendamos Grupos de direcciones IP para una implementación de usuarios móviles de GlobalProtect asignar un número de direcciones IP igual o mayor que el número de usuarios móviles con licencia para que puedan iniciar sesión al mismo tiempo.

    No especifique direcciones que se superpongan con otras redes que utiliza internamente o con los grupos que asignó cuando Configure la Infraestructura de servicios de Prisma Access (Panorama). Además, no utilice las siguientes direcciones IP y subredes, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno:

    - 169.254.0.0/16
    - 100.64.0.0/10

    Recomendamos usar un grupo de direcciones IP compatible con RFC 1918. Si bien apoyamos el uso de direcciones IP (públicas) que no cumplan con RFC 1918 para usuarios móviles, recomendamos no usarlas debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.

- Especifique la configuración DNS para **Primary DNS for public domains (DNS primario para dominios públicos)** y **Secondary DNS for public domains (DNS secundario para dominios públicos)**.
  - **Prisma Access Default (Prisma Access predeterminado)**: utilice el valor predeterminado del servidor DNS de Prisma Access.
  - **Internal DNS (DNS interno)**: utilice el mismo servidor que utiliza para resolver dominios internos.
  - **Custom (Personalizado)**: si tiene un servidor DNS que puede acceder a sus dominios públicos (externos), introduzca la dirección del servidor DNS principal en ese campo.
  - Puede añadir una **Client DNS Suffix List (Lista de sufijos DNS de cliente)** para especificar el sufijo que el cliente debe usar localmente cuando se introduce un nombre de host no cualificado que no puede resolver, por ejemplo, acme.local. No introduzca un carácter

 ©2025 Palo Alto Networks, Inc.

comodín (*) antes del sufijo de dominio (por ejemplo, acme.com). Puede añadir varios sufijos.

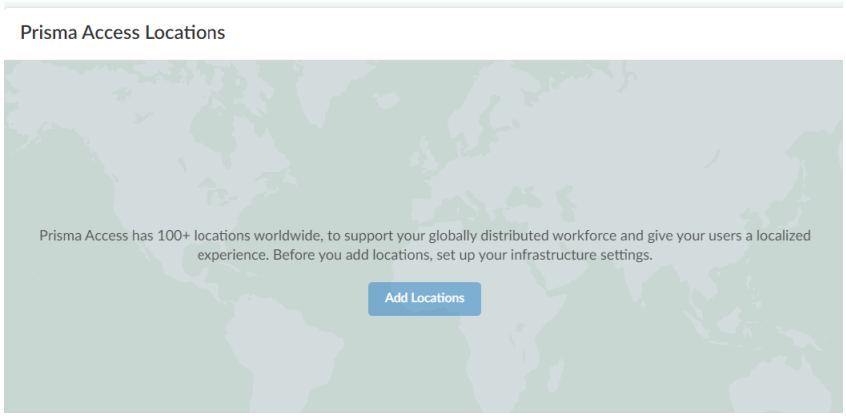
3. Configurar **Advanced Settings (Configuración avanzada)**.
   - (Opcional) Utilice **Static Entries (Entradas estáticas)** para resolver FQDNs a direcciones IP específicas.

     Esta funcionalidad puede ser útil si tiene servicios de internet para invitados en su organización y desea que sus invitados utilicen motores de búsqueda de forma segura, evitando que busquen material potencialmente inapropiado u ofensivo que podría estar en contra de la política de la empresa. Para ello, introduzca un **Name (Nombre)** único en el caso de la regla de entrada estática, un **FQDN** y la **Address (Dirección)** IP a dónde se debe dirigir la solicitud de FQDN.

   - Si desea que Prisma Access realice el proxy de las solicitudes DNS, configure valores para **UDP Queries Retries (Reintentos de consultas de UDP)** [el **Interval (Sec) [Intervalo (Seg)]** para reintentar la consulta en segundos y el número de **Attempts (Intentos)** de reintento que debe realizar.
4. **Elija la ubicación de Prisma Access a la que se conectarán sus usuarios de GlobalProtect**

   Añade las ubicaciones de Prisma Access donde desea brindar soporte a los usuarios de GlobalProtect. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** > **Prisma Access Locations (Ubicaciones de Prisma Access)**.

   El mapa muestra las regiones globales donde puede implementar Prisma Access para los usuarios. Además, Prisma Access proporciona múltiples ubicaciones dentro de cada región para garantizar que sus usuarios puedan conectarse a una ubicación que proporcione una experiencia de usuario adaptada a la configuración regional de los usuarios. Para obtener el mejor rendimiento, deberá **Select All (Seleccionar todo)**. Alternativamente, seleccione las ubicaciones específicas dentro de cada región seleccionada donde sus usuarios necesitarán acceso. Al limitar su implementación a una sola región, puede tener un control más granular

 ©2025 Palo Alto Networks, Inc.

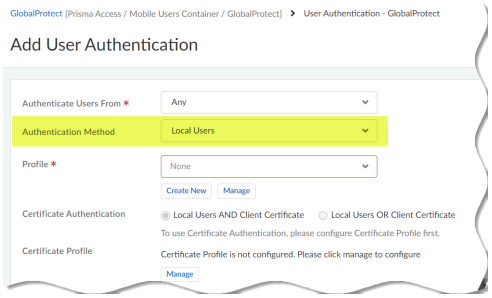
sobre sus regiones implementadas y excluir las regiones requeridas por su política o regulaciones de la industria.

Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a sus usuarios o en el mismo país que sus usuarios. Si una ubicación no está disponible en el país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a sus usuarios para obtener el mejor rendimiento.

5. **Autenticar usuarios de GlobalProtect**

   Configure la autenticación de usuario para que solo los usuarios legítimos tengan acceso a sus servicios y aplicaciones. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** > **User Authentication (Autenticación de usuarios)**.

   Para probar la configuración, puede añadir usuarios que Prisma Access autentique localmente o puede ir directamente a configurar la autenticación a nivel empresarial. Aquí encontrará más información sobre cómo Habilite usuarios móviles para autenticarse en Prisma Access



6. Prisma Access aplica las reglas de política de seguridad de procedimientos recomendados de forma predeterminada. Estas reglas permiten a los usuarios navegar de forma segura por sitios generales de Internet. Los usuarios son:

   - Bloqueado para visitar sitios web malos conocidos en función de la URL
   - Bloqueado para cargar o descargar archivos que se sabe que son maliciosos
   - Protegido de amenazas desconocidas y nunca antes vistas
   - Protegido contra malware, spyware (ataques de comando y control) y vulnerabilidades

   Después de pasar por la configuración inicial, puede revisar y actualizar estas reglas predeterminadas para satisfacer las necesidades de su empresa.

7. **Verifique que la ubicación del usuario móvil esté activa**

   Después de enviar su configuración inicial a Prisma Access, Prisma Access comenzará a aprovisionar su entorno de usuario móvil. Esto puede tardar hasta 15 minutos.

   *También puede validar su configuración seleccionando **Flujos de trabajo** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)** y edite la configuración de infraestructura para confirmar que haya una puerta de enlace configurada en cada una de las ubicaciones que aprovisionó.*

 ©2025 Palo Alto Networks, Inc.

GlobalProtect: personalizar la dirección del portal

Prisma Access requiere solo las configuraciones mínimas para aprovisionar el entorno de su usuario móvil para que pueda probarlo. Si prefiere utilizar el dominio de su empresa en la dirección del portal, puede cambiar la dirección después de la configuración inicial del entorno.

Por defecto, Prisma Access utiliza el dominio *gpcloudservice.com* para configurar la dirección del portal de Prisma Access a la que sus usuarios móviles deberán conectarse para tener acceso seguro a Internet y a su sede central y centros de datos. Debe utilizar este dominio predeterminado cuando configure y pruebe inicialmente su entorno. Si desea personalizar el nombre de dominio después de la configuración inicial para usar el dominio de su empresa, puede regresar y editar la configuración del entorno para que la dirección del portal al que se conectan sus usuarios contenga su propio dominio de empresa (por ejemplo, prisma-access.acme.com).

*El dominio *..gpcloudservice.com está asociado con la aplicación Palo Alto Networks.*

Para configurar Prisma Access para utilizar su propio dominio, debe:

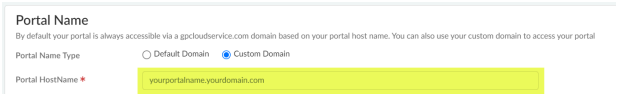
- Obtener certificados para el servicio.
- Cree una entrada CNAME de DNS en sus servidores DNS que asigne la dirección del portal predeterminada que usa el dominio predeterminado a la dirección del portal personalizada que usa el dominio de su empresa. Necesita hacer esto porque Prisma Access publica la dirección del portal que configuró en servidores de dominio público durante el aprovisionamiento inicial.

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** y edite la **Infrastructure Settings (Configuración de infraestructura)**.

En Strata Cloud Manager, la redundancia de red está habilitada de forma predeterminada entre portales o puertas de enlace y conexiones de servicio, lo que garantiza una conectividad redundante para los usuarios móviles con servicios y aplicaciones accesibles.

STEP 2 | Establezca el tipo de nombre del portal en **Custom Domain (Dominio personalizado)**.

STEP 3 | Introduzca el **Portal Hostname (Nombre de host del portal)** que desea utilizar.



STEP 4 | Añada el **Portal DNS CNAME (CNAME DNS del portal**) al cual asignar las entradas de su servidor DNS.

STEP 5 | **Import (Importar)** el **Certificate (Certificado)** que aprovisionó para la dirección del portal de dominio personalizado.

1. Seleccione el**Format (Formato)** de certificado para el certificado que está importando:
   - **Encrypted Private Key and Certificate (PKCS12) [Clave privada y certificado cifrados (PKCS12)]**: la clave y el certificado se encuentran en un único contenedor (archivo de certificado). Haga clic en **Choose File (Elegir archivo)** y busque el archivo PKCS12 para importar.

 ©2025 Palo Alto Networks, Inc.

- **Base64 Encoded Certificate (PEM) [Certificado codificado Base64 (PEM)]**: si selecciona esta opción, debe importar el **Key File (Archivo de claves)** por separado del certificado. Para importar el certificado PEM y el archivo de clave, haga clic en **Choose File (Elegir archivo)**.

2. Introduzca la **Passphrase (frase de contraseña)** para cifrar la clave y **Confirm Passphrase (Confirmar la frase de contraseña)** y, a continuación, haga clic en **Save (Guardar)**.

STEP 6 | Si aún no lo ha hecho, configure sus servidores DNS para que apunten a la DNS CNAME de Prisma Access que usted definió.

STEP 7 | **Save (Guardar)** la configuración del entorno y **Push Config (Enviar la configuración)** a Prisma Access.

Asegúrese de seleccionar los ámbitos de configuración de **Explicit Proxy (Proxy explícito)** y **GlobalProtect**.

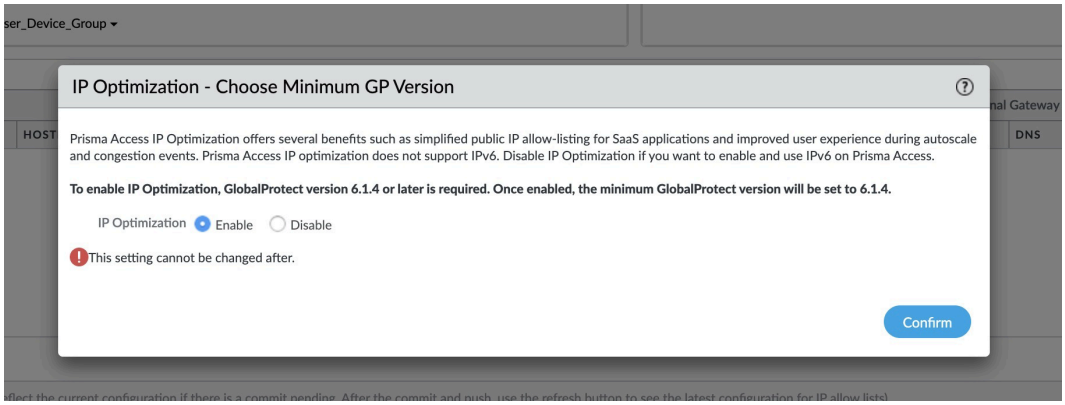
Configurar usuarios móviles de GlobalProtect (Panorama)

Para configurar una implementación de Usuarios móviles: GlobalProtect, complete los siguientes pasos. Antes de comenzar, asegúrese de entender cómo Prisma Access funciona y utiliza la lista de verificación para planificar su implementación de GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**.

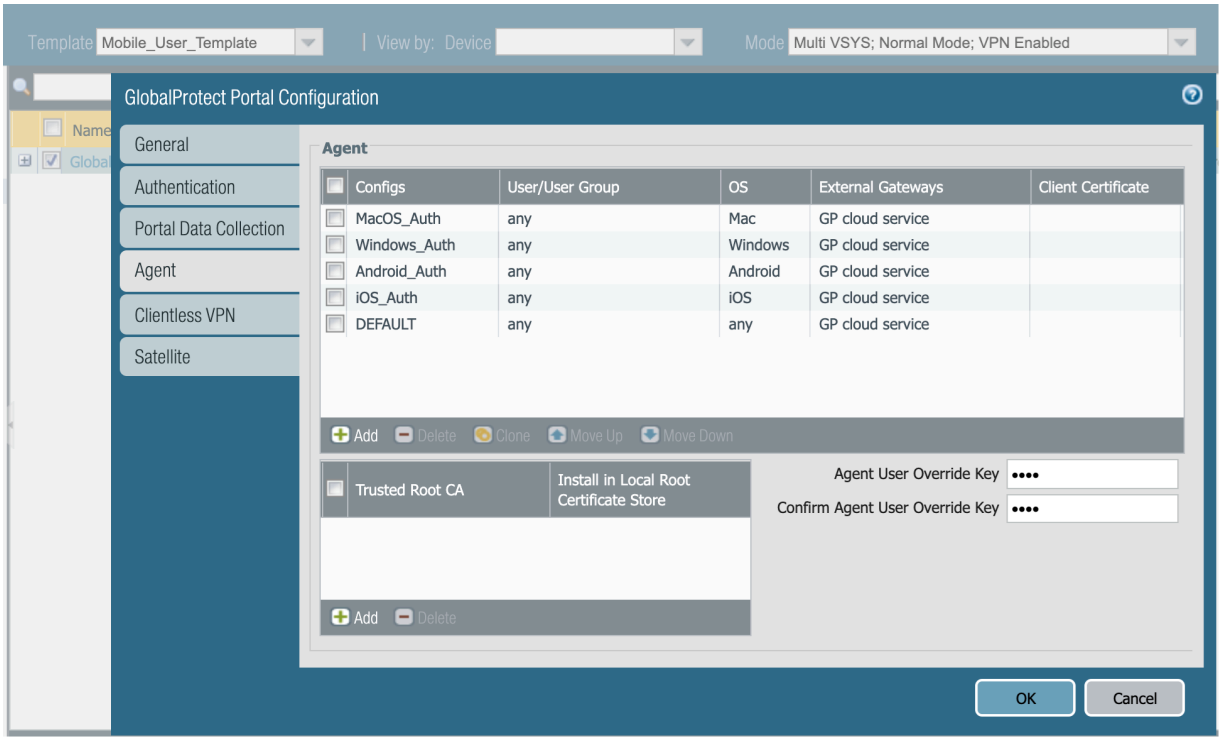
- *Cuando configure GlobalProtect por primera vez, se le preguntará si desea habilitar o no la optimización IP de Prisma Access. La elección de habilitar la Optimización de IP requiere* la versión de cliente GlobalProtect *6.1.4 y posteriores, 6.2.3 y posteriores o 6.3.0 y posteriores, y no es compatible con IPv6. Seleccione con cuidado, ya que no podrá cambiar esta configuración más adelante.*
- *La funcionalidad de optimización de IP es para nuevas implementaciones de Prisma Access únicamente. Las implementaciones existentes de Global Protect, incluidos los nuevos inquilinos que cree a partir de una implementación multiinquilino existente, no son elegibles.*
- *Si está migrando su implementación de GlobalProtect a Prisma Access (lejos de utilizar portales y puertas de enlace locales), asegúrese de que todos los usuarios estén ejecutando la versión 6.1.4 y posteriores de la aplicación GlobalProtect, 6.2.3 y posteriores, o 6.3 y posteriores antes de habilitar esta funcionalidad*



STEP 2 | (Opcional) Si deseas personalizar la configuración del agente que Prisma Access envía a los clientes, edita la configuración del portal GlobalProtect en la Plantilla_Usuario_Móvil para añadir una nueva configuración de agente. Después de configurar la configuración del agente, páselo por encima de la configuración del agente PREDETERMINADO que está predefinida en la plantilla para asegurarse de que sus ajustes tengan prioridad sobre los

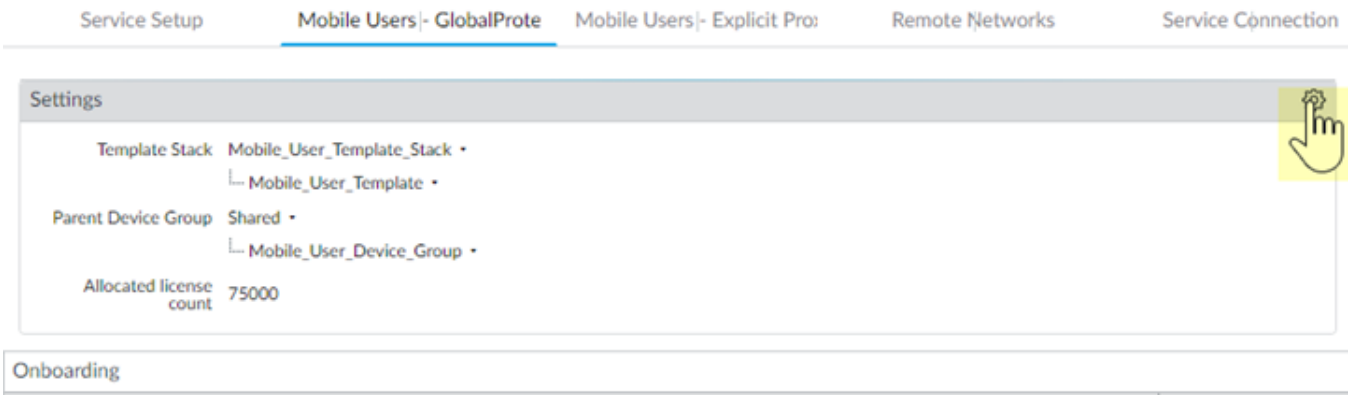
 ©2025 Palo Alto Networks, Inc.

ajustes predeterminados. Al editar esta plantilla, no elimine ni cambie la entrada de la Puerta de enlace externa.



STEP 3 | Configure la jerarquía del grupo de dispositivos que el servicio en la nube enviará al portal y a la puerta de enlace.

1. Editar la **Settings (Configuración)**.



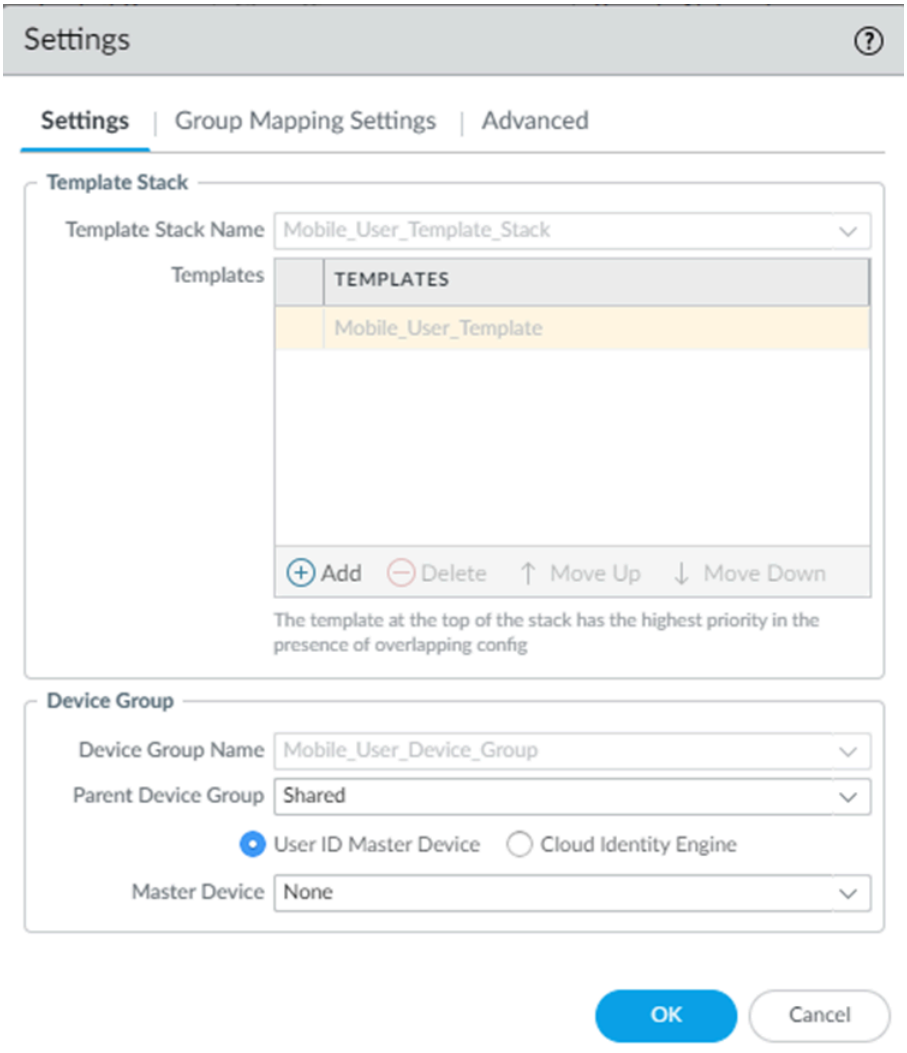
2. En la sección del Grupo de dispositivos, seleccione el **Parent Device Group (Grupo de dispositivos primario)** que contiene la configuración que desea enviar a Prisma Access

 ©2025 Palo Alto Networks, Inc.

para los Usuarios, o deje el grupo de dispositivos padre como **Shared (Compartido)** para utilizar la jerarquía de grupo de dispositivos compartidos de Prisma Access.

Enviará toda la configuración, incluidos los grupos de direcciones, política de seguridad, perfiles de seguridad y otros objetos de política (como grupos y objetos de aplicaciones), objetos y perfiles HIP y política de autenticación, esa Prisma Access para Usuarios necesita aplicar una política coherente a sus usuarios móviles utilizando la jerarquía de grupos de dispositivos que especifique aquí. Además, debe asegurarse de que ha configurado un perfil de reenvío de logs que reenvíe los tipos de logs deseados a **Panorama/Strata Logging Service** en un grupo de dispositivos que se envía a Prisma Access para Usuarios; esta es la única forma en que el servicio en la nube sabe qué logs reenviar a Strata Logging Service.

3. (Opcional) Si ha configurado un cortafuegos de nueva generación como dispositivo principal o añadió un perfil de Cloud Identity Engine para hacer que la información de usuario y grupo se pueda seleccionar en las políticas de seguridad, seleccione **User-ID Master Device (Dispositivo maestro de User-ID)** o **Cloud Identity Engine**; luego, seleccione el perfil Dispositivo maestro o el perfil de Cloud Identity Engine que creó.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Configure Prisma Access para utilizar el componente de Sincronización de directorios de Cloud Identity Engine en la nube para recuperar información de usuarios y grupos.

Debe configurar el componente de sincronización de directorios de Cloud Identity Engine en la nube para recuperar información de usuarios y grupos del directorio en la nube o de Active Directory (AD) antes de habilitar y configurar la integración de sincronización de directorios en la **Group Mapping Settings (Configuración de asignación de grupos)** de Prisma Access.

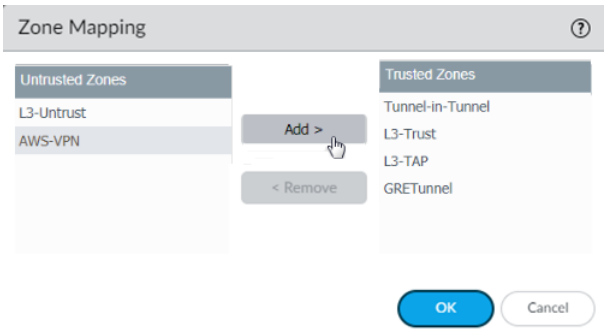
STEP 5 | Haga clic en **OK (Aceptar)** para guardar la configuración del usuario móvil.

STEP 6 | Asigne las zonas configuradas dentro de la pila de plantillas como de confianza o de no confianza.

En un cortafuegos de nueva generación de Palo Alto Networks, la política de seguridad se aplica entre zonas, que se asignan a interfaces físicas o virtuales en el cortafuegos. Sin embargo, con Prisma Access para Usuarios, la infraestructura de red se configura automáticamente para usted, lo que significa que ya no necesita configurar interfaces y asociarlas con zonas. Sin embargo, para permitir la aplicación coherente de la política de seguridad, debe asignar las zonas que utiliza dentro de su organización como de confianza o no de confianza, de modo que Prisma Access para usuarios puedan traducir las reglas de política que envía al servicio en la nube a las zonas internas dentro de la infraestructura de red.

1. Edite la configuración de Zone Mapping (Asignación de zonas).

   Por defecto, todas las zonas en la Mobile_User_Template_Stack se clasifican como Zonas No fiables.
2. Para cada zona que desee designar como de confianza, selecciónela y haga clic en **Add (Añadir)** para moverla a la lista de **Trusted Zones (Zonas de confianza)**.



3. Haga clic en **OK (Aceptar)** para guardar los cambios.

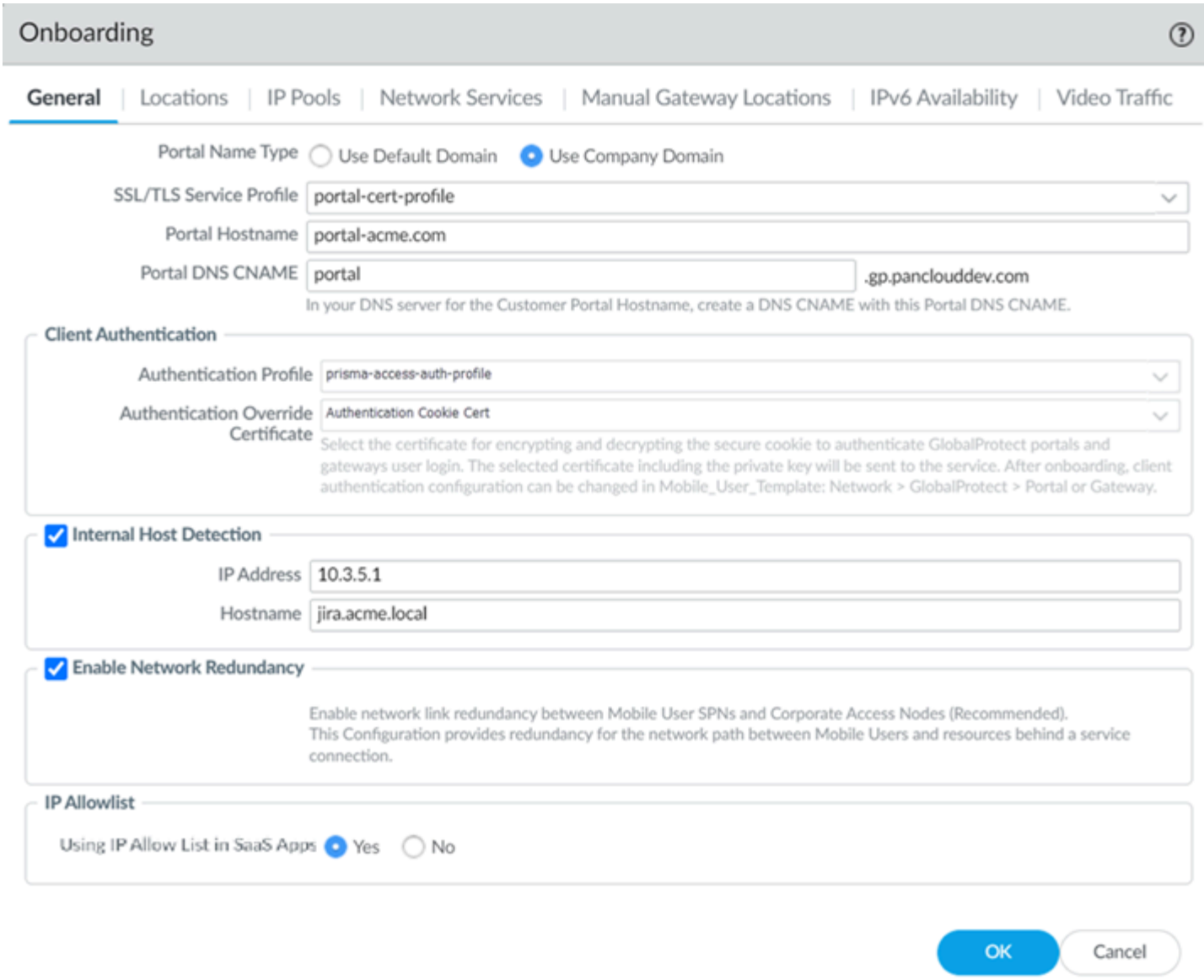
STEP 7 | Configure los ajustes del portal de GlobalProtect y de la puerta de enlace externa.

Puede configurar las puertas de enlace de Prisma Access como puertas de enlace externas solamente, no como puertas de enlace internas.

1. En la sección de Incorporación, haz clic en **Configure (Configurar)**.
2. En la pestaña **General**, especifique el **Portal Name Type (Tipo de nombre del portal)**:
   - **Use Default Domain (Utilizar dominio predeterminado)**: si selecciona esta opción, el nombre de host del portal utiliza el nombre de dominio predeterminado: `.gpcloudservice.com`. En este caso, basta con introducir un **Portal Hostname (Nombre de host del portal)** para anexar al nombre de dominio predeterminado.

 ©2025 Palo Alto Networks, Inc.

Prisma Access para usuarios creará automáticamente los certificados necesarios y publicará el nombre de host en servidores DNS públicos.



Si ya tiene una implementación de GlobalProtect con un nombre de portal existente y desea seguir utilizando ese nombre de portal, añada una entrada CNAME que asigne el nombre del portal de Prisma Access a su nombre de portal existente. Por ejemplo, si tiene un portal existente llamado portal.acme.com y quiere asignar el nuevo portal de Prisma Access a este mismo nombre, añadiría un CNAME de gpcs2.gpcloudservice.com a la entrada DNS de su portal existente.

*El dominio *..gpcloudservice.com está asociado con la aplicación Palo Alto Networks.*

- **Use Company Domain (Utilizar el dominio de la empresa)**: seleccione esta opción si desea que el dominio en el nombre de host del portal coincida con el nombre de dominio de su empresa (por ejemplo, myportal.mydomain.com). Si desea utilizar esta opción, primero debe obtener su propio certificado y configurar un perfil de servicio

 ©2025 Palo Alto Networks, Inc.

SSL/TLS que apunte a él. Luego puede configurar el nombre del portal seleccionando el **SSL/TLS Service Profile (Perfil de Servicio SSL/TLS)** e introduciendo el **Portal Hostname (Nombre de Host del Portal)**. Si utiliza esta opción, debe apuntar sus servidores DNS internos al **CNAME de DNS del Portal**, que es el nombre de host del portal con el `dominio .gpcloudservice.com`. Por ejemplo, si especificó un nombre de host DNS de acme-portal.acme.com, necesitaría crear una entrada CNAME DNS que asigne ese nombre de host a acme-portal.gpcloudservice.com en sus servidores DNS internos.



*Si necesita subir un nuevo certificado, importe el certificado y la clave privada; luego, visualice el servicio SSL/TLS que se está utilizando Prisma Access en **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **GlobalProtect_Portal** > **Authentication (Autenticación)** y verifique el nombre del **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Este campo solo se muestra si está utilizando un dominio de empresa en lugar del dominio predeterminado. A continuación, puede seleccionar **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Certificate Profile (Perfil de Certificado SSL/TLS)** y reemplazar el certificado en el perfil SSL/TLS utilizado por el portal con el certificado que importó.*

3. Seleccione un **Authentication Profile (Perfil de autenticación)** que especifica cómo Prisma Access debe autenticar a los usuarios móviles o crear uno nuevo.

   Si ha añadido un grupo de dispositivos principal que contiene una configuración de perfil de autenticación, debería verlo en la lista de perfiles disponibles. Si no ha enviado el perfil en el grupo de dispositivos, puede crear un perfil de autenticación ahora.

   *Una vez confirme y envíe sus cambios, no podrá hacer ningún cambio en el perfil de autenticación y el certificado de anulación de autenticación en esta área y las opciones se vuelven de solo lectura. Para realizar cambios después de la incorporación inicial, modifica o añade una o más configuraciones de autenticación del cliente GlobalProtect en la **Mobile_User_Template**.*

4. Seleccione un **Authentication Override Certificate (Certificado de anulación de autenticación)** para cifrar las cookies seguras a las que los usuarios móviles se autentican en el portal y la puerta de enlace.

   Si ha añadido un grupo de dispositivos principal que contiene el certificado que desea utilizar para cifrar las cookies de autenticación, deberá verlo en la lista de certificados disponibles. Si no ha enviado un certificado en el grupo de dispositivos, puede import (importar) o generate one (generar uno) ahora.

5. (Opcional) Para garantizar que sus usuarios móviles siempre tengan acceso a los servicios y aplicaciones que son accesibles desde las conexiones de servicio, debe **Enable Network Redundancy (Habilitar redundancia de red)** entre los portales o puertas de enlace y las conexiones de servicio.

   Esta funcionalidad proporciona rutas de red redundantes entre el plano de datos del usuario móvil y las conexiones de servicio en diferentes ubicaciones de cómputo. Habilitar la redundancia proporciona a los usuarios un acceso más resistente a los recursos detrás de las conexiones de servicio en un centro de datos o en las ubicaciones de la sede. Dado que se requiere una conexión de servicio para que los usuarios móviles accedan a recursos desde redes remotas, los usuarios también tienen más capacidad de recuperación para acceder a recursos en ubicaciones de redes remotas.

 ©2025 Palo Alto Networks, Inc.

6. (Opcional) Si no requiere que los endpoints de GlobalProtect tengan conexiones de túnel cuando están en la red interna, habilite la **Internal Host Detection (Detección de host interno)**.
   1. Seleccione la casilla de verificación de **Internal Host Detection (Detección de Host interno)**.
   2. Introduzca la **IP Address (Dirección IP)** de un host que los usuarios pueden alcanzar solo desde la red interna.
   3. Introduzca el **Hostname (Nombre de host)** de DNS que corresponda a la dirección IP que introduce. Los clientes que intentan conectarse realizan una búsqueda inversa de DNS en la dirección especificada. Si la búsqueda falla, el cliente determina que necesita una conexión de túnel para Prisma Access para Usuarios.

   > *Prisma Access copia la configuración de detección de host interno que usted especifica aquí a la configuración predeterminada del agente en la configuración de su* Configuración de portal de GlobalProtect *[**Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **<portal-config>** > **Agent (Agente)** > **DEFAULT (PREDETERMINADA)** > **Internal (Interno)**]. Si has introducido la configuración de detección de hosts internos para el agente predeterminado en el portal de GlobalProtect, no podrá cambiar las opciones aquí y deberá cambiarlas en el portal. Si necesita múltiples configuraciones de agente, introduzca la configuración para la configuración de agente predeterminada en el portal de GlobalProtect y use esa configuración para Prisma Access, luego seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **<portal-config>** > **Agent (Agente)** y **Add (Añadir)**, Añada una configuración no predeterminada, y especifique esa configuración en otras partes de su implementación.*

7. (Opcional) Si su organización utiliza listas de permitidos para controlar el acceso a aplicaciones públicas o SaaS, especifique si está **Using IP Allow Lists in SaaS Apps (Utilizando listas de permitidos de IP en aplicaciones SaaS)**.

   Para permitirle añadir las direcciones IP públicas (de salida) para su implementación de GlobalProtect—Mobile User a cualquier lista de permitidos de aplicaciones SaaS que utilice dentro de su organización, Prisma Access le proporciona las direcciones IP y le permite verificar que las haya añadido a su lista de permitidos antes de usarlas en su entorno. Puede implementar una lista de permitidos para las direcciones IP de salida de Prisma Access, tanto para implementaciones existentes como para nuevas implementaciones.

8. (Opcional) Personalice la configuración de la aplicación GlobalProtect (por ejemplo, especifique el método de conexión que utiliza GlobalProtect) seleccionando **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **GlobalProtect_Portal** > **Agent (Agente)**, seleccionando la configuración que desea personalizar o seleccionando **DEFAULT (PREDETERMINADO)**, seleccionando **App (Aplicación)**, luego personalizando la aplicación GlobalProtect.

STEP 8 | Seleccione las **Locations (Ubicaciones)** y las regiones asociadas con esas ubicaciones donde desea implementar sus usuarios móviles.

La pestaña **Locations (Ubicaciones)** muestra un mapa. Al resaltar el mapa se muestran las regiones globales (América, Europa y Asia Pacífico) y las ubicaciones disponibles dentro de

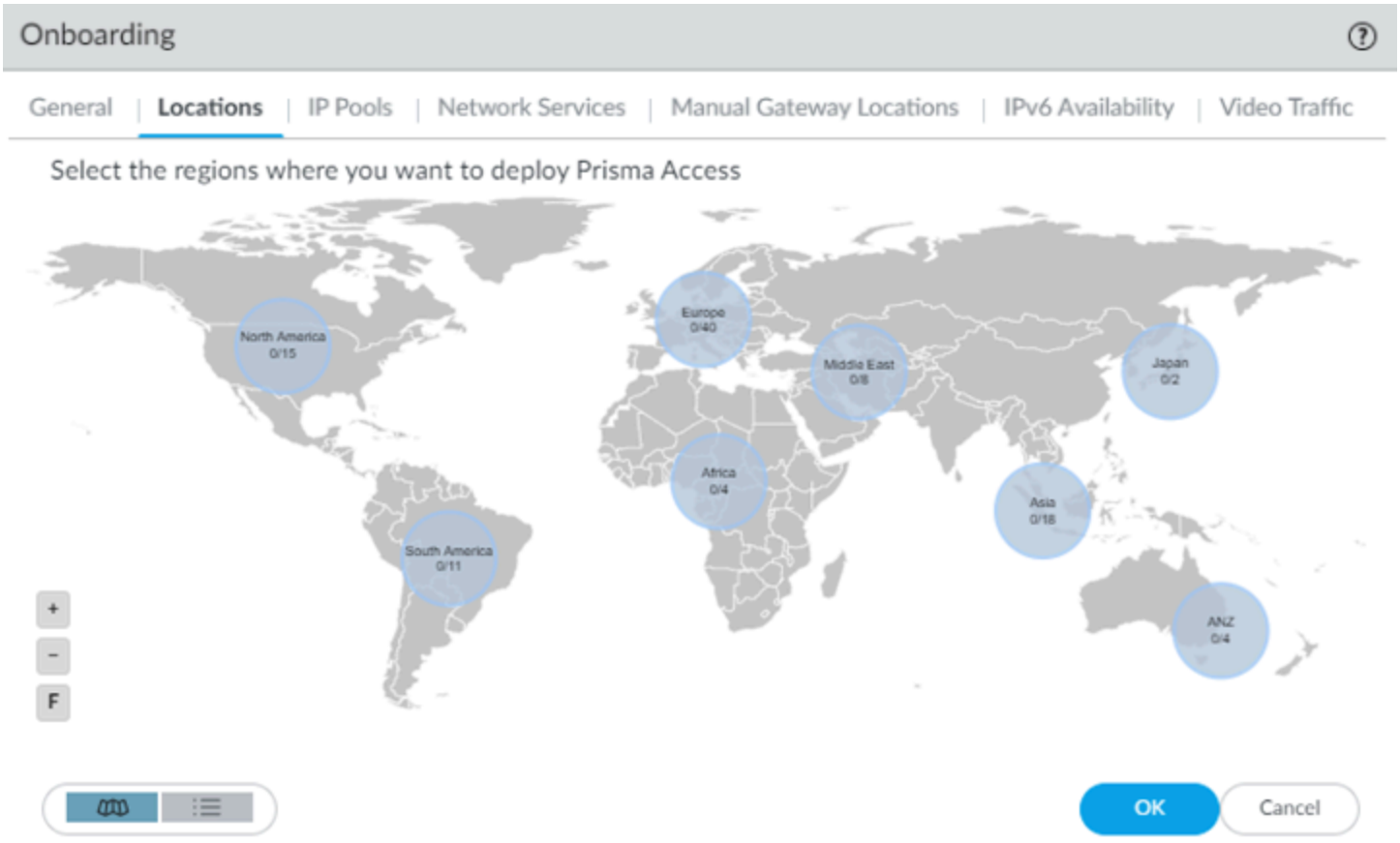
 ©2025 Palo Alto Networks, Inc.

cada región. Seleccione una región y luego seleccione las ubicaciones que desea implementar en cada región. Al limitar su implementación a una sola región, puede tener un control más granular sobre sus regiones implementadas y excluir las regiones requeridas por su política o las regulaciones del sector. Puede seleccionar una ubicación en una región que esté más cerca de sus usuarios móviles, o seleccionar una ubicación según lo requiera su política o las regulaciones del sector.

Prisma Access utiliza las ubicaciones de Hong Kong, del Banco Central de los Países Bajos y de EE. UU. Noroeste como ubicaciones de usuario móvil de respaldo si no hay otras ubicaciones disponibles. Por esta razón, Palo Alto Networks recomienda encarecidamente que habilite al menos una de estas ubicaciones durante la incorporación de usuarios móviles.

Las ubicaciones denotadas con dos asteriscos son **Local Zones (Zonas locales)**. Estas ubicaciones colocan los servicios de cómputo, almacenamiento, bases de datos e infraestructura cerca de grandes centros de población e industrias, sin embargo, también tienen algunas limitaciones. Para añadir una zona local, póngase en contacto con su representante de Palo Alto Networks.

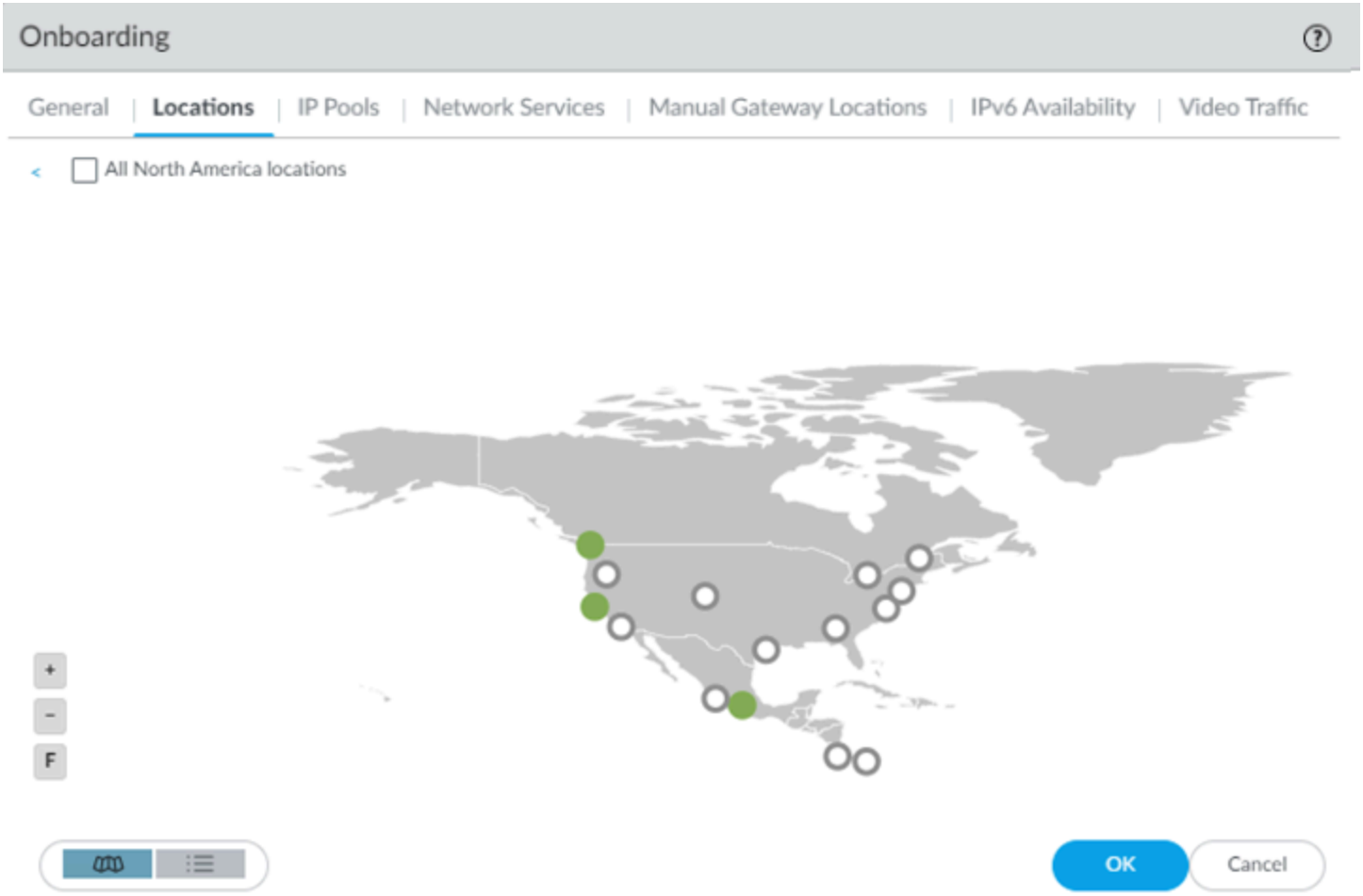
1. Haga clic en la pestaña **Location (Ubicaciones)** y seleccione una región.



 ©2025 Palo Alto Networks, Inc.

2. Seleccione una o más puertas de enlace de Prisma Access dentro de la región seleccionada utilizando el mapa.

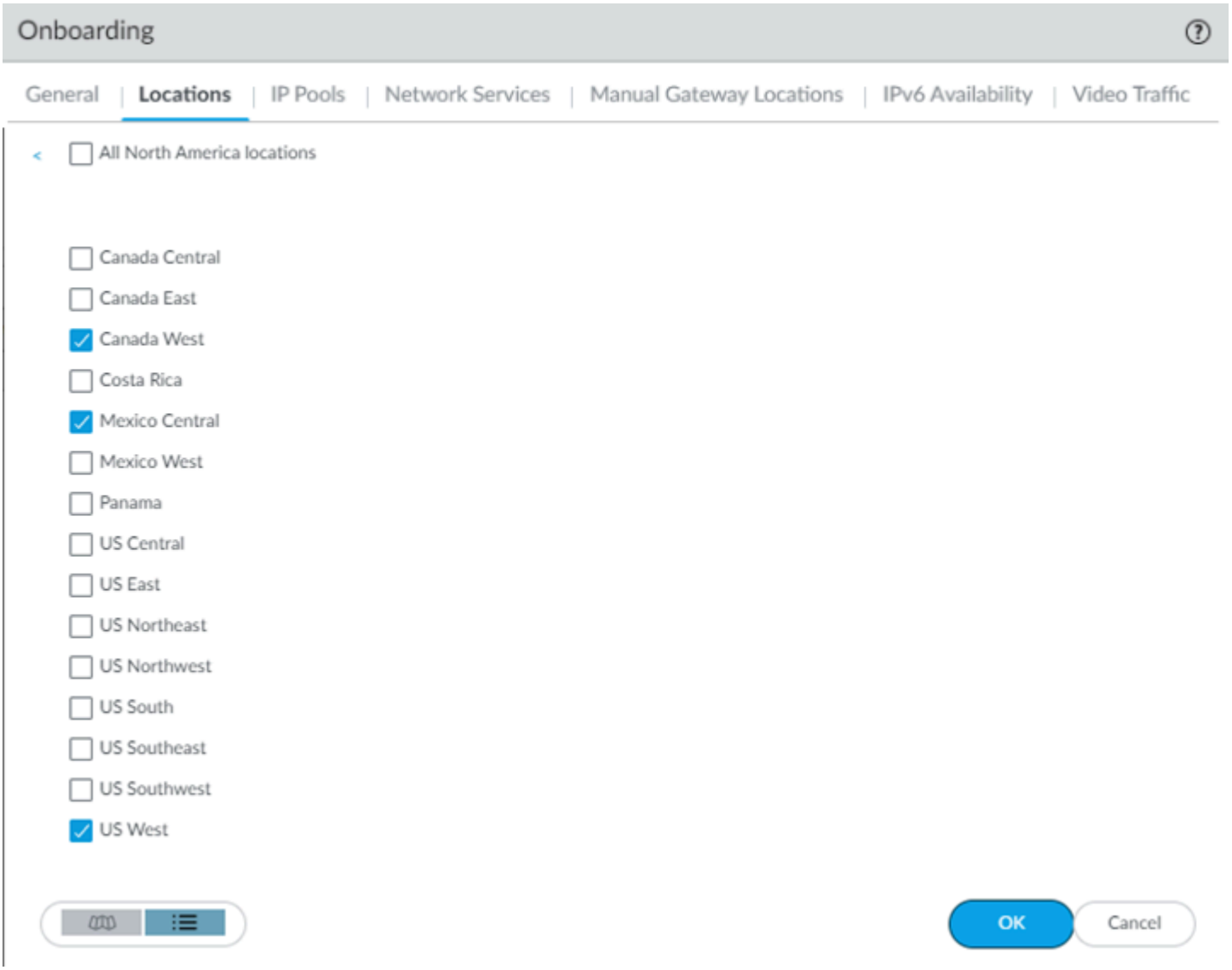
   Al pasar el cursor sobre una ubicación, ésta se resalta. Los círculos blancos indican una ubicación disponible; los círculos verdes indican que ha seleccionado esa ubicación.



   Además de la vista del mapa, puede ver una lista de regiones y ubicaciones. Elija entre la vista de mapa y la vista de lista en la esquina inferior izquierda. En la vista de lista, la lista muestra regiones ordenadas por columnas, con todas las ubicaciones ordenadas por

 ©2025 Palo Alto Networks, Inc.

región. Puede seleccionar **All (Todos)** los sitios dentro de una región (parte superior del cuadro de diálogo).



STEP 9 | Configure los grupos de direcciones IP utilizados para asignar direcciones IP a los endpoints de GlobalProtect seleccionando la pestaña **IP Pools (Grupos de IP)** y **Add (Añadir)** para añadir un grupo de direcciones IP.

1. Especifique una **Region (Región)** para el grupo de direcciones IP.

   Puede usar un solo grupo de direcciones IP para todos los endpoints de GlobalProtect en el mundo [**Worldwide (Mundial)**], puede usar grupos separados para cada sala donde tenga usuarios móviles o puede especificar grupos por grupo de ubicaciones (un grupo de ubicaciones que es más pequeño que el teatro). También puede especificar una combinación de grupos de IP mundial, por teatro o por ubicación. Por ejemplo, puede añadir un grupo para un grupo específico de ubicaciones y, a continuación, añadir un grupo **Worldwide (Mundial)** para usarlo en todas las demás ubicaciones.

   Utilice grupos de direcciones IP específicas de la ubicación si tiene servicios que dependen de la dirección IP de origen del usuario para identificar los detalles del

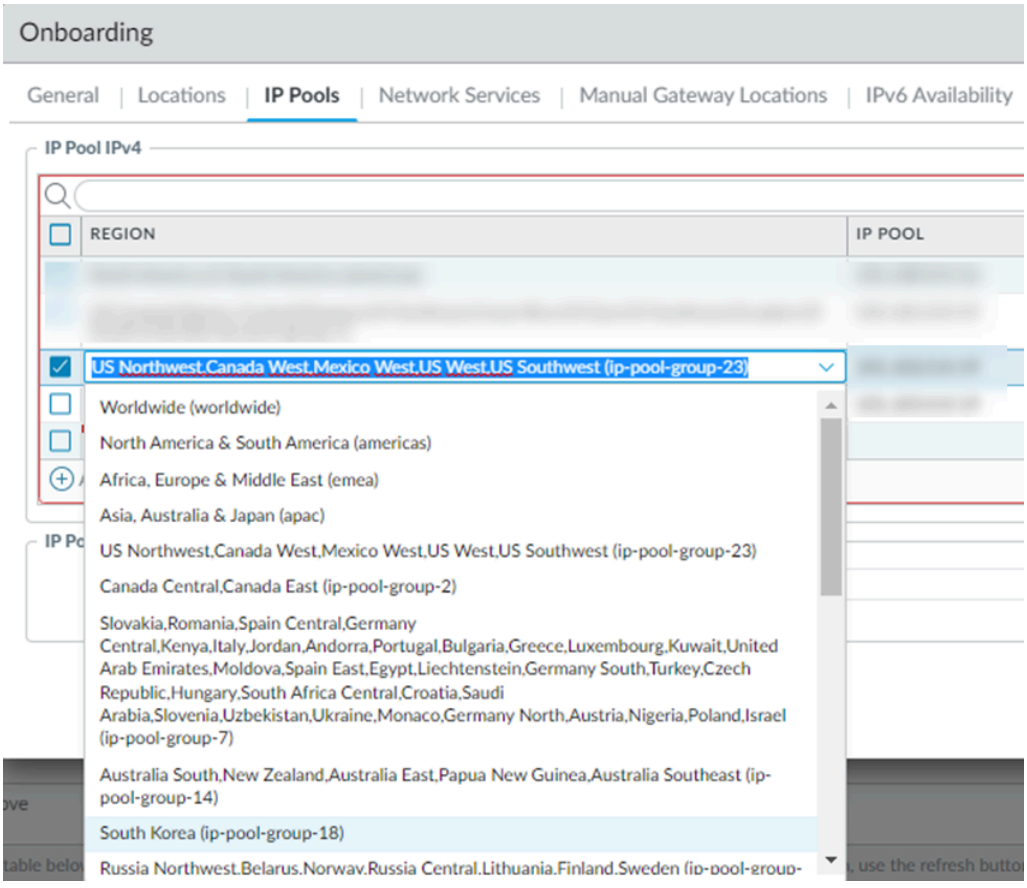
 ©2025 Palo Alto Networks, Inc.

usuario (como servicios basados en la ubicación o servicios basados en un grupo o función de usuario) para que pueda aplicar políticas de control de acceso, o para realizar operaciones de enrutamiento o políticas en diferentes países si los países están en diferentes regiones de cómputo. Por ejemplo, puede utilizar un grupo de direcciones IP para Canadá y uno para Brasil, que se encuentran en diferentes ubicaciones de proceso, para proporcionar controles de acceso y seguridad distintos.

Para usar grupos de direcciones IP específicos de un grupo de ubicaciones, también debe especificar un grupo específico de mundial (Worldwide) o de teatro.

Los usuarios móviles de GlobalProtect consumen las direcciones IP en el grupo de ubicaciones primero, luego las direcciones IP específicas del teatro y luego las direcciones IP mundiales. Por ejemplo, si especifica un grupo para un grupo de ubicaciones y Worldwide (mundial), y luego agota las direcciones IP disponibles en el grupo de ubicaciones, Prisma Access tomará las direcciones IP del grupo **Worldwide (Mundial)** para usarlas en ese grupo de ubicaciones.

- Para especificar los grupos de IP que pueden utilizar todos los usuarios del agente de Prisma Access, seleccione **Worldwide (Mundial)**.
- Para especificar los grupos de IP que pueden utilizar los usuarios del GlobalProtect en un teatro específico, seleccione el teatro.
- Para especificar grupos de IP específicos para el grupo de ubicaciones, selecciónelo de la lista.



 ©2025 Palo Alto Networks, Inc.

2. Introduzca un **IP Pool (Grupo de IP)** para asignar a los endpoints en la región que ha seleccionado.
   - Introduzca una subred mínima requerida de /23 (512 direcciones IP) por ubicación. Las ubicaciones adicionales requieren una subred /23 como mínimo. Si especifica una subred mundial, la subred mínima requerida es /23, pero recomendamos Grupos de direcciones IP para una implementación de usuarios móviles de GlobalProtect asignar un número de direcciones IP igual o mayor que el número de usuarios móviles con licencia para que puedan iniciar sesión al mismo tiempo.

     No especifique direcciones que se superpongan con otras redes que utiliza internamente o con los grupos que asignó cuando Configure la Infraestructura de servicios de Prisma Access (Panorama). Además, no utilice las siguientes direcciones IP y subredes, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno:
     - 169.254.0.0/16
     - 100.64.0.0/10

     Recomendamos usar un grupo de direcciones IP compatible con RFC 1918 y RFC 6598. Si bien apoyamos el uso de direcciones IP (públicas) que no cumplan con RFC 1918 para usuarios móviles, recomendamos no usarlas debido a posibles conflictos con el espacio de direcciones IP públicas de Internet.

STEP 10 | Para especificar la configuración de resolución DNS para sus dominios internos y externos (públicos), seleccione la pestaña **Network Services (Servicios de red)** y **Add (Añadir)** la configuración.

Los endpoints de GlobalProtect con una conexión de túnel activa utilizan sus adaptadores de red virtuales en lugar de sus adaptadores de red físicos y, por lo tanto, requieren configuraciones de resolución DNS separadas.

Configure la configuración de red en la ventana **Network Services (Servicios de red)**.

- Seleccione una **Región (Región)** del menú desplegable.

  Seleccione **Worldwide (Mundial)**, seleccione un teatro o seleccione un grupo de ubicaciones para aplicar la configuración de DNS a nivel global. Si especifica varias configuraciones de proxy con una combinación de configuraciones Worldwide (Mundial), de teatro y específicas del grupo de ubicación, Prisma Access utiliza la configuración del grupo de ubicación, luego teatro y luego Mundial. Prisma Access evalúa las reglas de arriba hacia abajo en la lista.
- **Add (Añadir)** una o más reglas para configurar los ajustes de DNS para **Internal Domain (Dominio interno)**.
  - Introduzca un **Rule Name (Nombre de regla)** único para la regla.
  - No introduzca una dirección 127.0.0.1 ya que puede causar problemas de enrutamiento interno de Prisma Access.
  - Sí desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios que desea resolver en la **Lista de dominios**. Especifique un

 ©2025 Palo Alto Networks, Inc.

asterisco delante del dominio; por ejemplo, *.acme.com. Puede especificar un máximo de 1.024 entradas de dominio.

*Prisma Access tiene una regla predefinida para resolver los dominios *.amazonaws.com, *.aws.amazon.com, *.googleapis.com y *.google.internal utilizando el servidor predeterminado en la nube. Si quiere que sus servidores DNS internos resuelvan un dominio más específico (por ejemplo, *.s3.amazonaws.com en lugar de *.amazonaws.com), introduzca la URL en la **Domain List (Lista de Dominios)**. Prisma Access evalúa los nombres de dominio de más largo a más corto, luego de arriba a abajo en la lista.*

- Si tiene un **Custom DNS server (Servidor DNS personalizado)** que puede acceder a sus dominios internos, especifique las direcciones IP del servidor **Primary DNS DNS principal** y del servidor **Secondary DNS DNS secundario**, o seleccione **Use Cloud DefaultUsar Cloud Default** para usar el valor predeterminado del servidor DNS de Prisma Access.

- Especifique la configuración de DNS para **Public Domains (Dominios Públicos)**.
  - **Use Cloud Default (Usar Cloud Default)**: Usar el servidor DNS predeterminado Prisma Access.
  - **Same as Internal Domains (Igual que dominios internos)**: utilice el mismo servidor que utiliza para resolver dominios internos. Cuando selecciona esta opción, el servidor DNS utilizado para resolver dominios públicos es el mismo que el servidor configurado para la primera regla en la sección **Internal Domains (Dominios internos)**.
  - **Custom DNS server (Servidor DNS personalizado)**: si tiene un servidor DNS que puede acceder a sus dominios públicos (externos), introduzca la dirección del servidor DNS principal en ese campo.

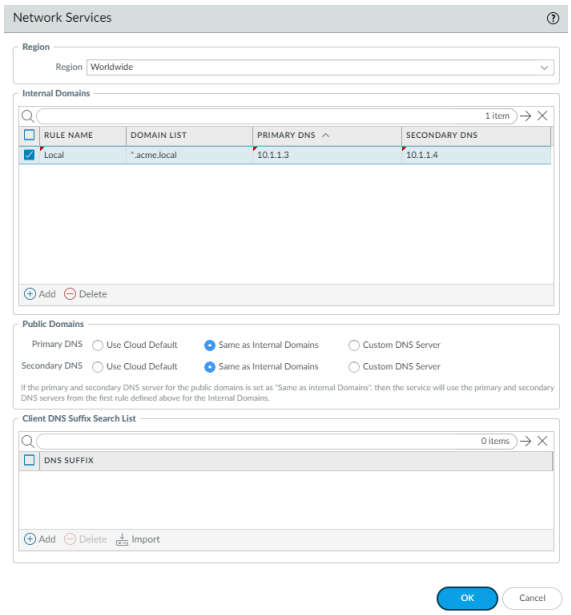
  (Opcional) Puede **Add (Añadir)** un **DNS Suffix (Sufijo DNS)** para especificar el sufijo que el cliente deberá usar localmente cuando se introduce un nombre de host no cualificado que

 ©2025 Palo Alto Networks, Inc.

no puede resolver, por ejemplo, acme.local. No introduzca un carácter comodín (*) antes del sufijo de dominio (por ejemplo, acme.com). Puede añadir varios sufijos.

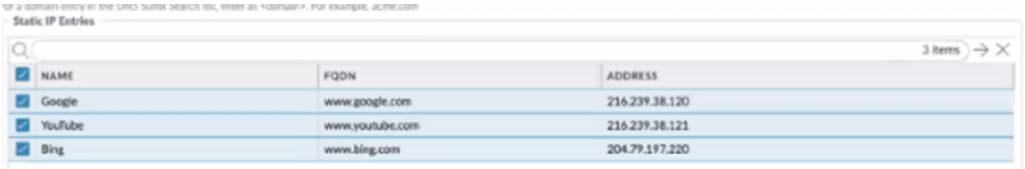
- Si desea que Prisma Access realice el proxy de las solicitudes DNS, configure valores para las consultas UDP (el **Interval (Intervalo)** para reintentar la consulta en segundos y el número de **Attempts (Intentos)** de reintento que debe realizar.

  Para obtener más información sobre cómo Prisma Access realiza el proxy de las solicitudes DNS, consulte la Resolución DNS para usuarios móviles: implementaciones de GlobalProtect.



STEP 11 | (Opcional) Utilice **Static Entries (Entradas estáticas)** para resolver FQDN en direcciones IP específicas.

Esta funcionalidad puede ser útil si tiene servicios de Internet para invitados en su organización y desea que sus invitados utilicen los motores de búsqueda de forma segura, lo que les impide buscar material potencialmente inapropiado u ofensivo que podría ir en contra de la política de la empresa. Para ello, introduzca un **Name (Nombre)** único en el caso de la regla de entrada estática, un **FQDN** y la **Address (Dirección)** IP a dónde se debe dirigir la solicitud de FQDN.



STEP 12 | (Opcional) Si su implementación utiliza el Servicio de Nombres de Internet de Windows (WINS), puede especificar servidores WINS para resolver la asignación de nombres NetBIOS a direcciones IP seleccionando **WINS Configuration (Configuración de WINS)**; seleccionando una región para el servidor WINS o seleccionando Mundial para aplicar la configuración

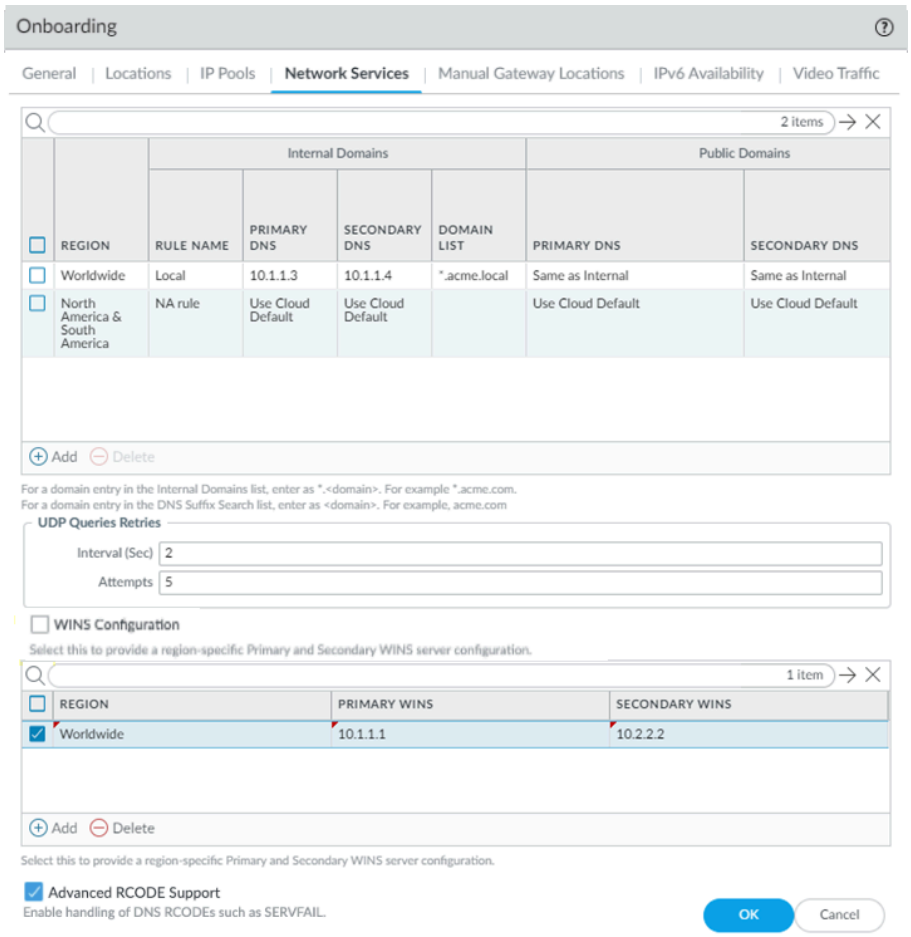
 ©2025 Palo Alto Networks, Inc.

de WINS a nivel mundial, luego especificando una dirección de servidor **WINS primario** y, opcionalmente, una dirección de servidor **WINS secundario**.

Después de habilitar WINS, Prisma Access puede enviar la configuración de WINS a los endpoints de los usuarios móviles a través de GlobalProtect.

STEP 13 | (Opcional) Seleccione Advanced RCODE Support (Compatibilidad avanzada con RCODE) para permitir que el servidor DNS primario falle al servidor DNS secundario si se recibe un código de retorno DNS RCODE 2 (SERVFAIL) y RCODE 5 (REFUSED).

Un código de respuesta DNS de SERVFAIL hace referencia a un error de comunicación con el servidor DNS primario, y un código de respuesta DNS de REFUSED significa que el servidor DNS primario se negó a proporcionar la información solicitada. En ambos casos, el servicio realiza la conmutación por error al servidor DNS secundario.



STEP 14 | (Opcional) Si permite que sus usuarios móviles seleccionen manualmente las puertas de enlace desde la aplicación GlobalProtect, seleccione las **Manual Gateway Locations**

 ©2025 Palo Alto Networks, Inc.

(Ubicaciones de puerta de enlace manual) que los usuarios pueden ver desde su aplicación GlobalProtect.

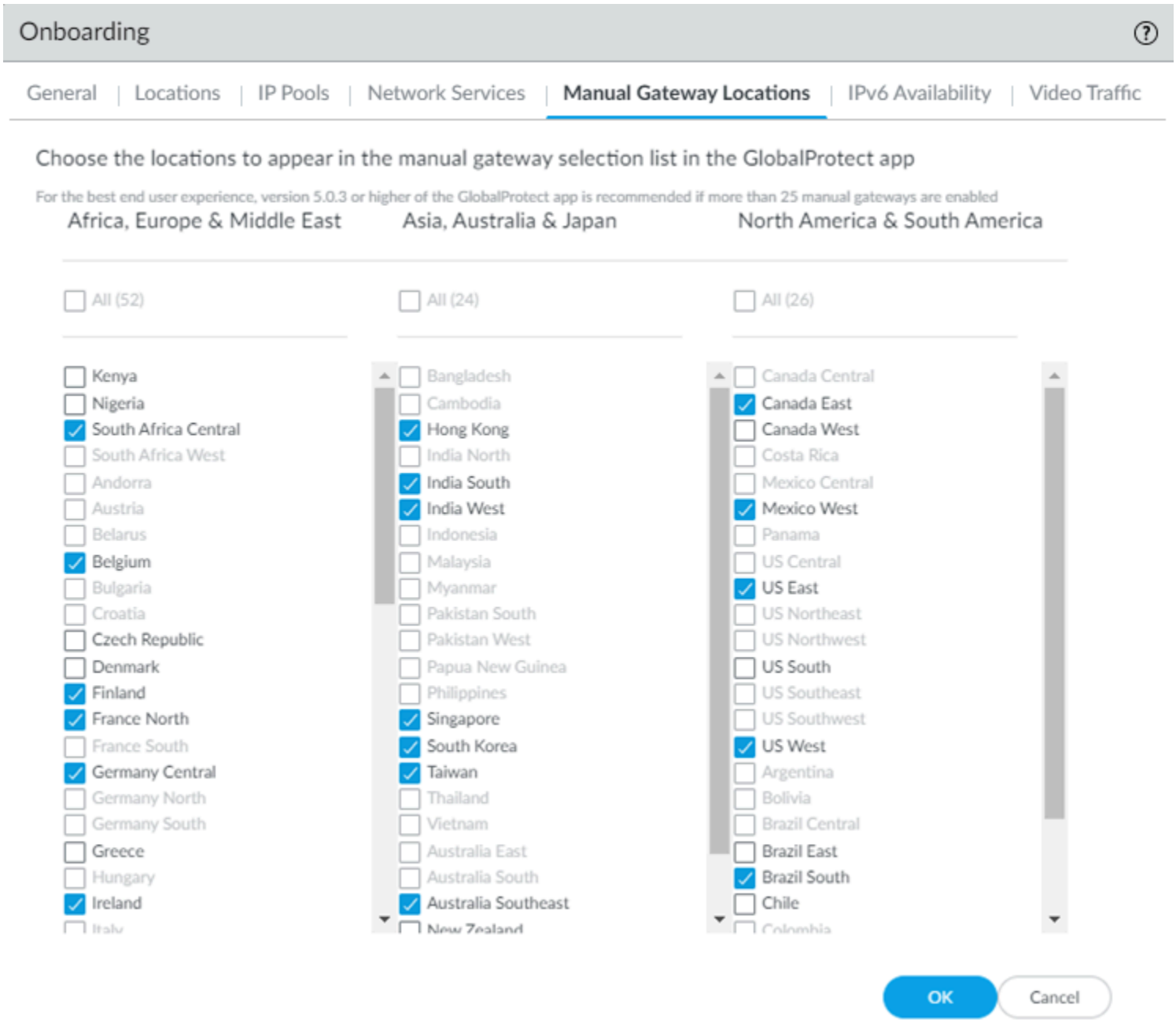
Elegir un subconjunto de ubicaciones incorporadas reduce el número de puertas de enlace disponibles que los usuarios móviles pueden ver en su aplicación GlobalProtect para la selección manual de puertas de enlace.

Si no selecciona puertas de enlace manuales en esta pestaña, Prisma Access selecciona la siguiente lista de puertas de enlace por defecto.

- Sureste de Australia
- Bélgica
- Brasil Sur
- Canadá Este
- Finlandia
- Francia Norte
- Alemania Central
- Hong Kong
- India Oeste
- Irlanda
- Israel
- Japón Central
- Países Bajos Central
- Arabia Saudí
- Singapur
- Sudáfrica Central
- Corea del Sur
- Taiwán
- RU
- EE. UU. Este
- EE. UU. Oeste

Prisma Access le permite seleccionar solo las puertas de enlace que has incorporado. Por ejemplo, si no elige **Reino Unido** cuando selecciona ubicaciones, no puede seleccionar **Reino Unido** como una puerta de enlace manual (la ubicación está atenuada).

 ©2025 Palo Alto Networks, Inc.



. *Si necesita eliminar una ubicación después de incorporarla, y está seleccionada como una de las* ***Manual Gateway Locations (Ubicaciones de puerta de enlace manual)****, asegúrese de quitar la selección aquí así como en la pestaña de* ***Locations (Ubicaciones)****.*

STEP 15 | Haga clic en **OK (Aceptar)** para guardar la configuración de incorporación.

STEP 16 | Configurar las opciones de **IPv6 Availability (Disponibilidad de IPv6)**.

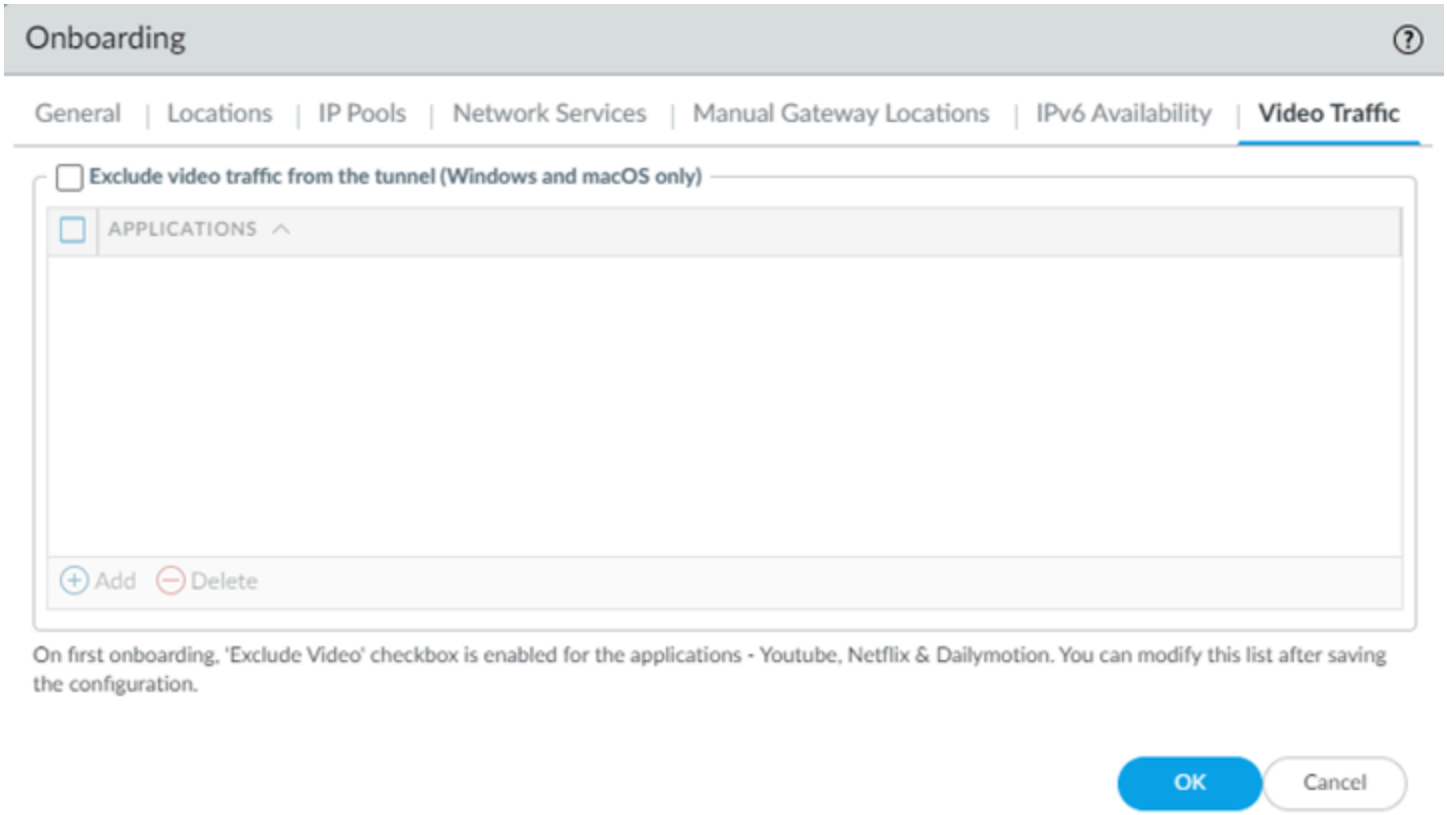
Si utiliza la red IPv6 en su implementación de Usuarios móviles: GlobalProtect, puede configurar Prisma Access para usar direcciones IPv6 en la red de sus usuarios móviles. También

 ©2025 Palo Alto Networks, Inc.

necesita habilitar IPv6 networking globalmente en su infraestructura de Prisma Access antes de poder usar el direccionamiento IPv6.

STEP 17 | (Opcional, Windows y macOS únicamente) Excluir el tráfico de vídeo del túnel de GlobalProtect.

Exclude video traffic from the tunnel (Excluir el tráfico de vídeo del túnel); luego, **Add (Añadir)** o **Delete (Eliminar)** aplicaciones de transmisión de vídeo que desee excluir del túnel de GlobalProtect.



STEP 18 | Cree reglas de política de seguridad para asegurar el tráfico de sus usuarios móviles.

1. Seleccione el **Device Group (Grupo de dispositivos)** en el que desea añadir reglas de política. Puede seleccionar el Grupo_de_Dispositivos_Usuario_Móvil o el grupo de dispositivos principal que ha seleccionado al configurar Prisma Access para usuarios móviles.
2. Cree reglas de políticas de seguridad. Asegúrese de no definir reglas de política de seguridad que permitan el tráfico de cualquier zona a cualquier zona. En las reglas de la política de seguridad, utilice las zonas que ha definido previamente en la pila de plantillas.

 ©2025 Palo Alto Networks, Inc.

STEP 19 | Configurar los logs para que se reenvíen a Strata Logging Service.

El complemento Cloud Services añade automáticamente la siguiente configuración de logs [**Device (Dispositivo)** > **Log Settings (Configuración de logs)**] después de una nueva instalación o al retirar plantillas de Prisma Access de una pila de plantillas de Prisma Access:

- La configuración de logs para los logs del sistema (**sistema-gpcs-default**), logs de User-ID (**userid-gpcs-default**), logs de coincidencias HIP (**hipmatch-gpcs-default**) y los logs de GlobalProtect (**gp-prismaaccess-default**) se añaden a Mobile_User_Template.
- La configuración de logs para los logs del sistema (**sistema-gpcs-default**), los logs de User-ID (**userid-gpcs-default**) y los logs de GlobalProtect (**gp-prismaaccess-default**) se añaden a Remote_Network_Template.
- La configuración de logs para los logs del sistema (**sistema-gpcs-default**) y los logs de GlobalProtect (**gp-prismaaccess-default**) se añade a Service_Conn_Template.

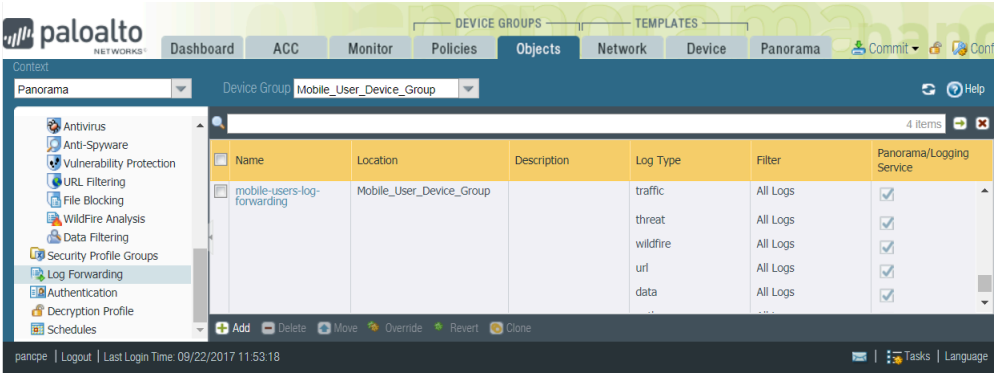
Estas configuraciones de configuración de logs reenvían automáticamente los logs del sistema, User-ID y coincidencia HIP a Strata Logging Service.

STEP 20 | (Opcional) Reenviar logs para otros tipos de logs a Strata Logging Service.

Para reenviar estos logs, debe crear y adjuntar un perfil de reenvío de logs a cada regla de política para la cual desea reenviar logs.

1. Seleccione el **Device group (Grupo de Dispositivos)** en el que añadió las reglas de la política.
2. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)** y luego **Add (Añadir)** para añadir un perfil. En la lista de coincidencia del perfil de reenvío de logs, **Add (Añadir)** todos los tipos de log que desea reenviar.

   El siguiente ejemplo permite el reenvío de logs de tráfico, prevención de amenazas, envíos de WildFire, filtrado de URL, filtrado de datos y autenticación.
3. Seleccione **Panorama/Strata Logging Service** como el Método de reenvío. Cuando selecciona Panorama, los logs se envían a Strata Logging Service. Podrá supervisar los registros y generar informes desde Panorama. Strata Logging Service proporciona una integración fluida para almacenar logs sin tener que enviarlos de vuelta a su Panorama en la sede corporativa, y Panorama puede consultar a Strata Logging Service según sea necesario.

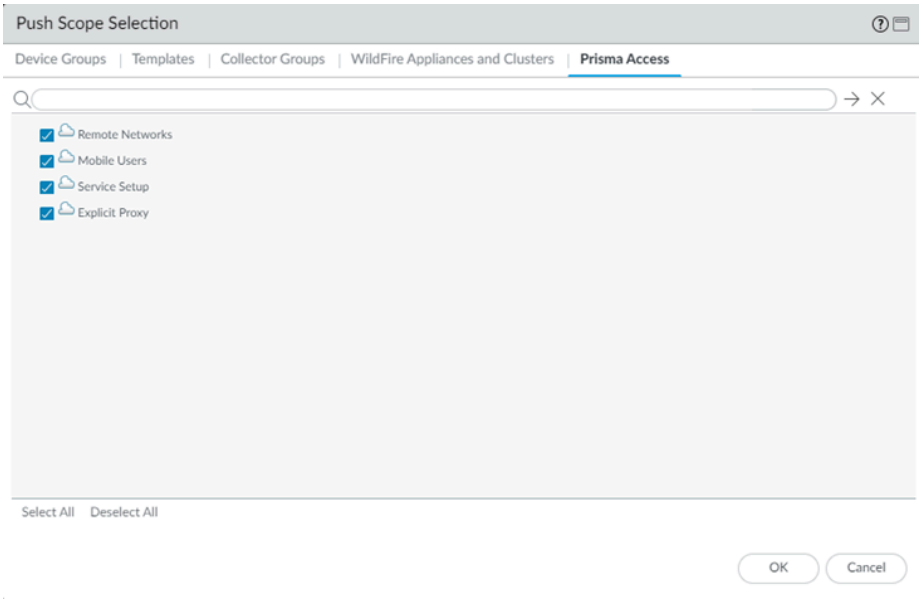


4. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y modifique la regla de políticas. Seleccione **Actions (Acciones)** y seleccione el perfil de Reenvío de logs que ha creado.

 ©2025 Palo Alto Networks, Inc.

STEP 21 | Realice todos sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access** , asegúrese de que **Mobile Users (Usuarios móviles)** y **Explicit Proxy (Proxy explícito)**están seleccionadas en **Push Scope (Ámbito de envío)**, luego haga clic en **OK (Aceptar)**.



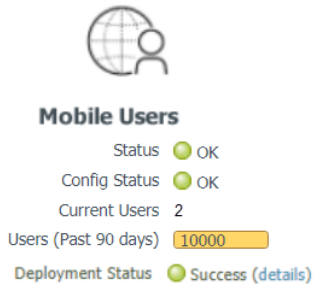
3. En la pestaña **Device Groups (Grupos de dispositivos)**, asegúrese de haber seleccionado los grupos de dispositivos de **Explicit Proxy (Proxy explícito)** y **GlobalProtect**.
4. Haga clic en **Commit and Push (Confirmar y enviar)**.

 ©2025 Palo Alto Networks, Inc.

STEP 22 | Para verificar que Prisma Access para Usuarios está implementado y activo, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)**.

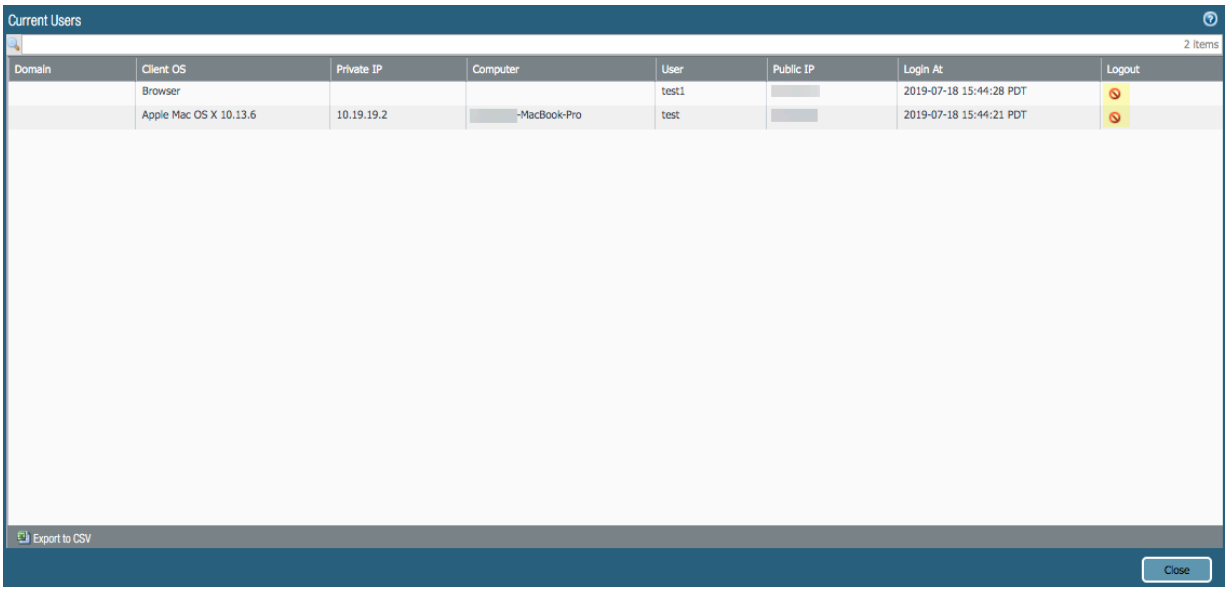
Después de que se complete la provisión, el **Status (Estado)** de los usuarios móviles y el **Config Status (Estado de configuración)** deberían mostrar **OK (Aceptar)**.

El área de **Deployment Status (Estado de implementación)** le permite ver el progreso de los trabajos de incorporación y implementación antes de que se completen, así como ver más información sobre el estado de los trabajos completados.



Para ver el número de usuarios únicos que están actualmente conectados, o para cerrar sesión de un usuario conectado, haga clic en el número hipervinculado junto a **Current Users (Usuarios Actuales)**.

 ©2025 Palo Alto Networks, Inc.

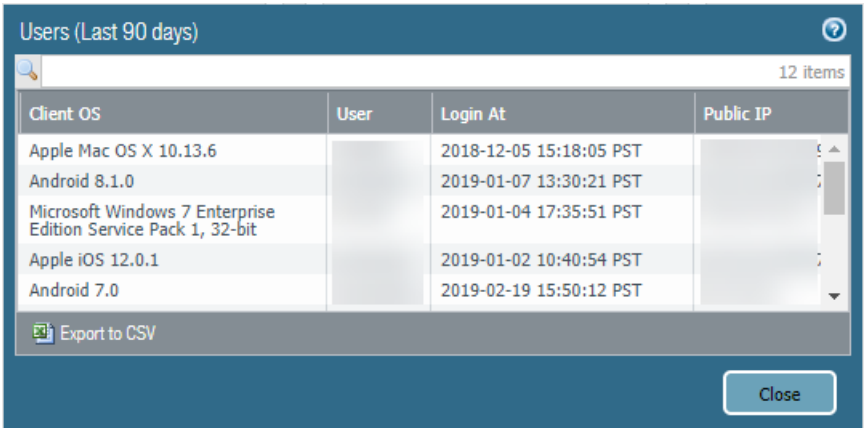


Para ver la información histórica de los usuarios que han iniciado sesión anteriormente durante un período de 90 días, haga clic en el número junto a **Users (Last 90 days) [Usuarios (Últimos 90 días)]**.

Cuando el número de usuarios en el campo Usuarios (Últimos 90 días) alcanza el 80 % del número total de licencias, el número se muestra en color rojo.

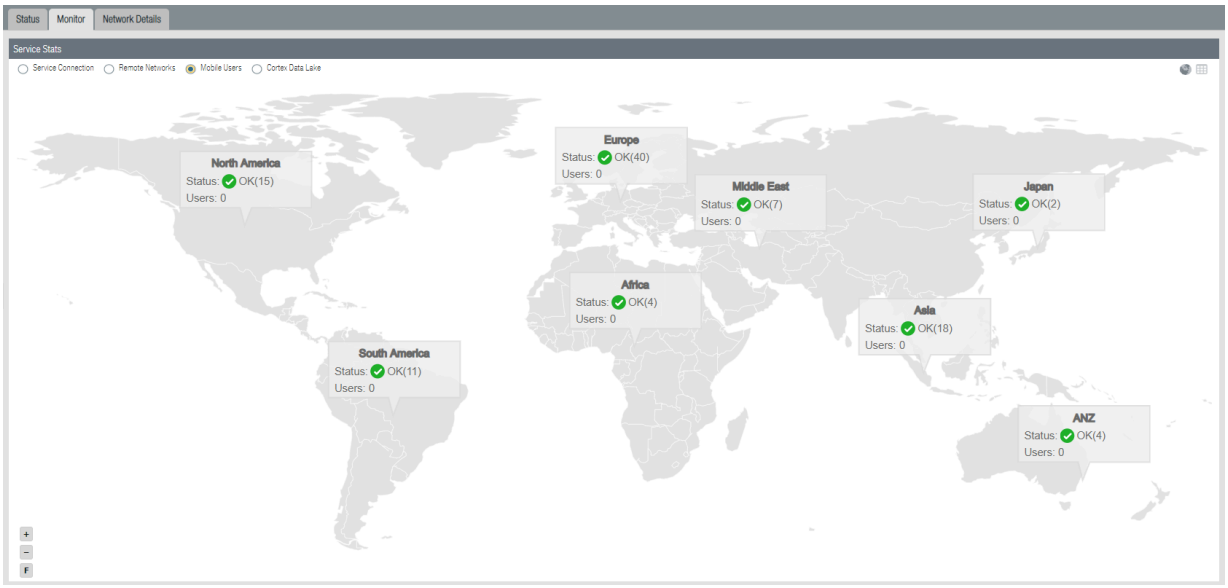
Para exportar la lista de usuarios a un archivo CSV, seleccione **Export to CSV (Exportar a CSV)**. Tenga en cuenta que se pueden exportar un máximo de 45.000 usuarios a un archivo CSV.

 ©2025 Palo Alto Networks, Inc.



Para mostrar un mapa que muestre las ubicaciones de los portales y puertas de enlace de Prisma Access que funcionan en las regiones que has seleccionado, seleccione **Monitor (Supervisar)**; luego seleccione **Mobile Users (Usuarios móviles)**.

 ©2025 Palo Alto Networks, Inc.



Seleccione una región para obtener más detalles sobre esa región.

- **Location (Ubicación)**: la ubicación donde se implementa la infraestructura de servicio en la nube para asegurar a los usuarios móviles en su red.

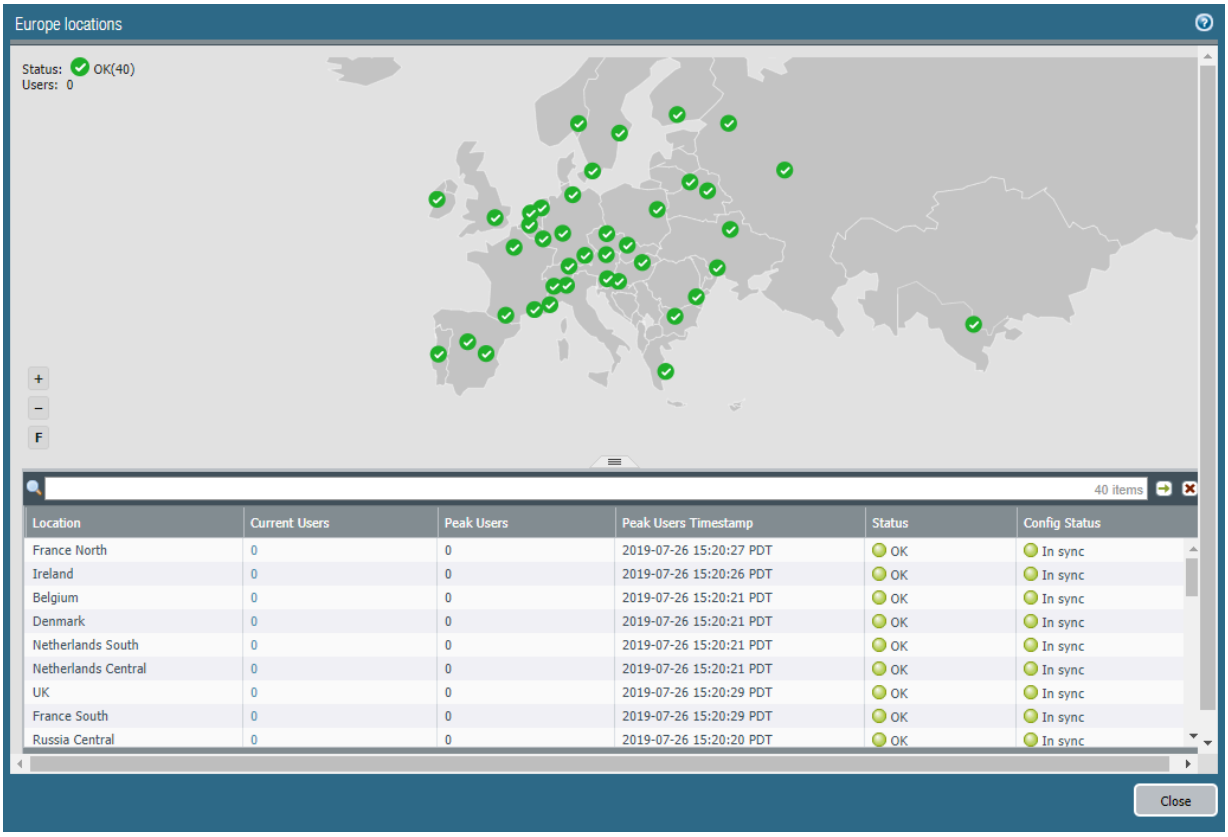
 ©2025 Palo Alto Networks, Inc.

- **Usuarios actuales**: el número de usuarios que están conectados y protegidos por el servicio.

  Cuando el recuento actual de usuarios móviles alcanza el 80% de su número total de licencias, este número se muestra en rojo.
- **Peak Users (Pico de usuarios)**: el recuento del número máximo de usuarios concurrentes.
- **Peak Users Timestamp (Marca de tiempo de pico de usuarios)**: la marca de tiempo cuando se recuperaron por última vez los datos de usuarios máximos.
- **Status (Estado)**: el estado operativo de la conexión entre Prisma Access y sus usuarios móviles.
- **Config Status (Estado de configuración)**: el estado de su último envío de configuración al servicio. Si ha realizado un cambio localmente y aún no ha enviado la configuración a la nube, es posible que se muestre el estado **Out of sync (Fuera de sincronización)**. Pase el cursor sobre el indicador de estado para obtener información más detallada. Después de

 ©2025 Palo Alto Networks, Inc.

confirmar y enviar la configuración a Prisma Access, el estado de configuración cambia a **In sync (Sincronizado)**.



STEP 23 | Si eligió **Use Company Domain (Utilizar dominio de la empresa)** para el nombre de host de su portal, debe añadir una entrada DNS en sus servidores DNS internos para asignar el nombre de host del portal que definió al CNAME DNS del portal que se muestra en la pestaña **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)** > **Onboarding (Incorporación)** > **General** (por ejemplo, `<portal_hostname>.gpcloudservice.com`)

 ©2025 Palo Alto Networks, Inc.

STEP 24 | Implemente el software de la aplicación GlobalProtect a sus usuarios finales.

Para usuarios de Mac OS o Windows, pueden dirigir a los usuarios a la dirección del portal de Prisma Access, donde pueden descargar la aplicación GlobalProtect desde el portal.

Prisma Access gestiona la versión de la aplicación GlobalProtect en el portal y puede seleccionar la versión activa de las versiones que Prisma Access aloja, así como controlar la capacidad de los usuarios para descargarla.

Alternativamente, puede alojar el software de la aplicación GlobalProtect en un servidor web para sus usuarios de Mac OS y Windows. Prisma Access es compatible con cualquier versión de la aplicación GlobalProtect que no esté enumerada como obsoleta.

Los usuarios de aplicaciones móviles pueden descargar e instalar la aplicación móvil de GlobalProtect desde la tienda de aplicaciones adecuada para sus sistemas operativos.

GlobalProtect: Personalizar la configuración del túnel

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Personalice la configuración del túnel VPN que la aplicación GlobalProtect establece para conectarse a Prisma Access. La configuración del túnel incluye opciones de túnel dividido que puede usar para definir qué tráfico envía la aplicación a Prisma Access y qué puede ser enrutado localmente en su lugar (como aplicaciones que consumen mucho ancho de banda y que no son necesarias para el uso empresarial).

Los **Match Criteria (Criterios de coincidencia)** que define para la configuración del túnel le indican a Prisma Access los usuarios, dispositivos o sistemas que deben recibir la configuración. Por ejemplo, podría especificar que una regla de configuración de túnel se aplique a todas las instancias de la aplicación GlobalProtect en una región determinada. En Prisma Access (Managed by Panorama), puede configurar los ajustes del túnel dividido en función de la Ruta de acceso y el Dominio y la aplicación.

- Strata Cloud Manager
- Panorama

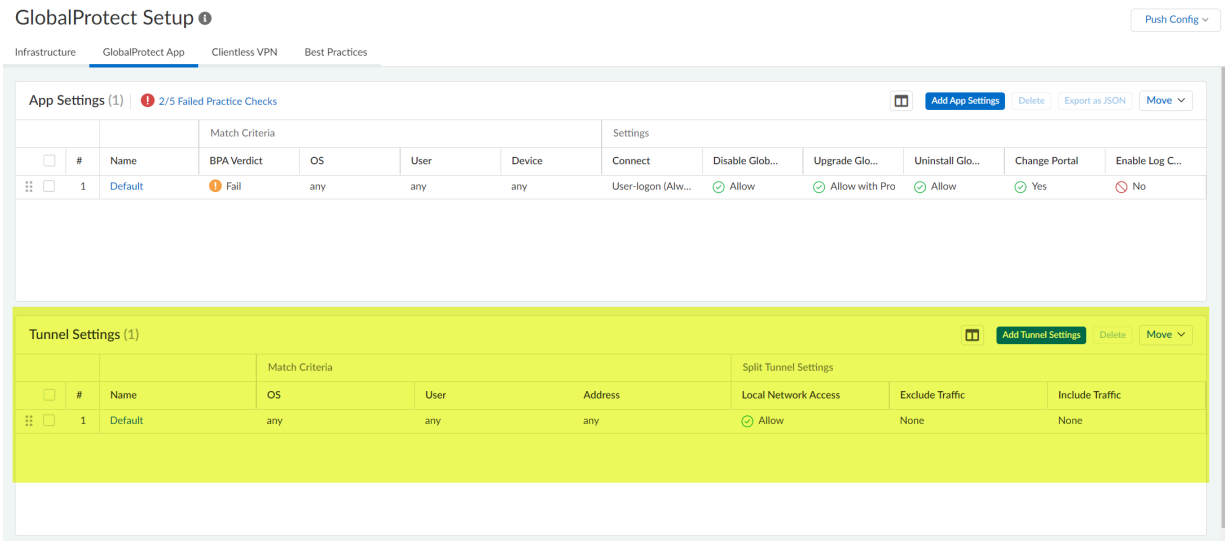
GlobalProtect: personalizar la configuración del túnel (Strata Cloud Manager)

STEP 1 | Haga clic en **Manage > Service Setup > Mobile Users > GlobalProtect Setup > GlobalProtect App > Add Tunnel Settings (Gestionar > Configuración de servicio > Usuarios móviles >**

 ©2025 Palo Alto Networks, Inc.

Configuración de GlobalProtect > Aplicación de GlobalProtect > Añadir configuración de túnel).

*Si está utilizando Strata Cloud Manager, haga clic en **Workflow > Prisma Access Setup > Mobile User > GlobalProtect Setup > GlobalProtect App > Add Tunnel Settings (Flujo de trabajo > Configuración de Prisma Access > Usuario móvil > Configuración de GlobalProtect > Aplicación GlobalProtect > Añadir configuración de túnel)**.*



STEP 2 | Introduzca un nombre y los **Match Criteria (Criterios de coincidencia)** para especificar los usuarios, dispositivos o sistemas que deben recibir la configuración. Por ejemplo, podría especificar que una regla de configuración de túnel se aplique a todas las instancias de la aplicación GlobalProtect en una región determinada.

STEP 3 | Habilite la **Anulación de autenticación** para Prisma Access para generar y aceptar cookies seguras y cifradas para la autenticación del usuario. Esta configuración permite al usuario proporcionar credenciales de inicio de sesión solo una vez durante el período de tiempo especificado.

- **Generar cookie para la anulación de la autenticación**: permite que Prisma Access genere cookies cifradas y específicas del endpoint y emite cookies de autenticación al endpoint.
- **Accept cookie for authentication override (Aceptar cookie para la anulación de autenticación)**: permite a Prisma Access autenticar usuarios con una cookie válida y cifrada.

 ©2025 Palo Alto Networks, Inc.

Cuando la aplicación presenta una cookie válida, Prisma Access verifica que Prisma Access cifró la cookie originalmente, descifra la cookie y luego autentica al usuario.

La aplicación GlobalProtect debe conocer el nombre de usuario del usuario que se conecta para coincidir y recuperar las cookies de autenticación asociadas del endpoint del usuario. Después de que la aplicación recupera las cookies, las envía a Prisma Access o a la puerta de enlace para proceder a la autenticación del usuario.

STEP 4 | Habilite la **tunelización dividida** para definir qué tráfico permite o restringe la aplicación GlobalProtect a través del túnel VPN a Prisma Access. La tunelización dividida conserva el ancho de banda al excluir el tráfico de Prisma Access que no es crítico para el negocio o no permite la productividad.

- **Acceso a red local**: proporcione a los usuarios de Windows y Mac acceso a recursos locales, sin necesidad de que se conecten primero a Prisma Access.

  Excluir tráfico: especifique el tráfico que desea excluir de la inspección y aplicación de políticas de Prisma Access basadas en la aplicación, el dominio y la ruta (como una dirección IP).

  Personalizar Incluir tráfico: de forma predeterminada, la aplicación GlobalProtect enruta todo el tráfico a Prisma Access, excepto lo que está en la lista de exclusión. Especifique el tráfico que la aplicación GlobalProtect siempre debe enrutar a Prisma Access, incluso cuando cumpla con los criterios de la lista de exclusión.

STEP 5 | **Excluir tráfico de transmisión de vídeo** para no enviar tráfico de transmisión de vídeo desde las aplicaciones enumeradas a Prisma Access. 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. Las exclusiones de transmisión de video se aplican a todo el tráfico que la aplicación GlobalProtect envía a Prisma Access, no solo los criterios de coincidencia que ha definido para esta regla.

STEP 6 | Guardar la configuración. Repita los pasos anteriores para añadir más configuraciones de túnel.

STEP 7 | (Opcional) **Mueva** para establecer el orden de prioridad en el que se utiliza la configuración del túnel VPN al conectarse a Prisma Access.

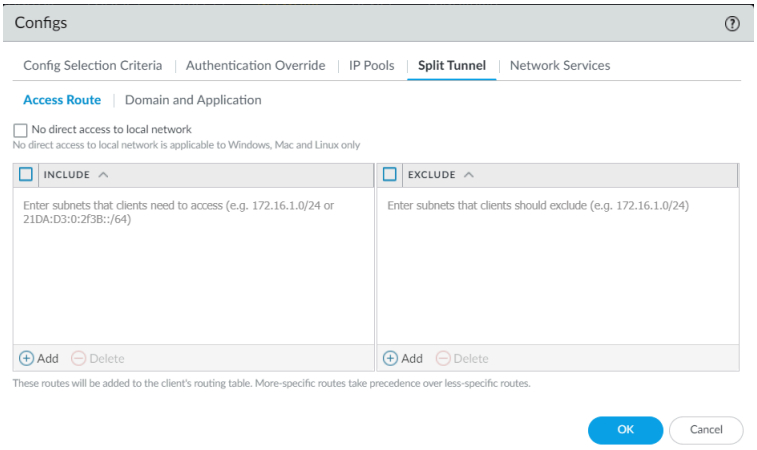
GlobalProtect: personalizar la configuración del túnel (Panorama)

Puede configurar los ajustes del túnel dividido en función de la Ruta de acceso o el Dominio y la Aplicación.

- Configure la configuración del túnel dividido según la ruta de acceso.
  1. Haga clic en **Panorama > Red > GlobalProtect > Puertas de enlace** y seleccione la puerta de enlace que desee personalizar.
  2. Haga clic en **Agent (Agente) > Client Settings (Configuración del cliente)** y seleccione la configuración.
  3. Haga clic en **Split Tunnel (Túnel dividido) > Access Route (Ruta de acceso)**. Los ajustes de división de túneles se asignan al adaptador de red virtual en el endpoint cuando la aplicación

 ©2025 Palo Alto Networks, Inc.

de GlobalProtect establece un túnel con Prisma Access. Puede incluir o excluir el tráfico de subred IP de destino específico para que no se envíe a través del túnel VPN.



4. Active la opción **Sin acceso directo a la red local** para evitar que los usuarios envíen tráfico directamente a proxys o recursos locales mientras están conectados a GlobalProtect.

   *Habilite la configuración **No direct access to local network (Sin acceso directo a la red local)** para reducir los riesgos en redes no fiables, como los puntos de acceso Wi-Fi fraudulentos.*

5. Seleccione **Include (Incluir)** y **Add (Añadir)** para añadir las subredes de destino o el objeto de dirección (del tipo Máscara de red IP) para dirigir solo determinado tráfico destinado para su red LAN a GlobalProtect. Puede incluir subredes IPv6 o IPv4. Para incluir todas las subredes de destino o todos los objetos de dirección, seleccione **Include (Incluir)** para incluir 0.0.0.0/0 y ::/0 como rutas de acceso.
6. Seleccione **Exclude (Excluir) Add (Añadir)** las subredes de destino o el objeto de dirección (del tipo 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.

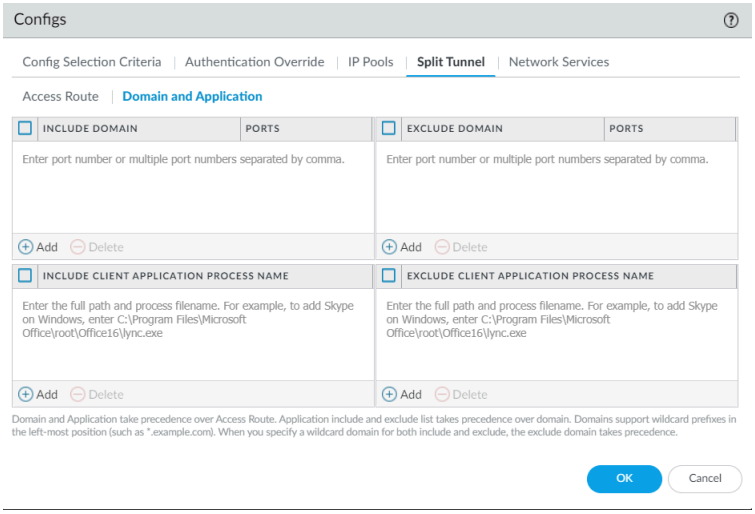
   No puede excluir rutas de acceso para endpoints que ejecutan Android en Chromebooks. Solo las rutas IPv4 son compatibles con Chromebooks.

7. Guarde la configuración del túnel.

 ©2025 Palo Alto Networks, Inc.

- Configure la configuración del túnel dividido en función del dominio y la aplicación.
  1. Haga clic en **Panorama > Red > GlobalProtect > Puertas de enlace** y seleccione la puerta de enlace que desee personalizar.
  2. Haga clic en **Agent (Agente) > Client Settings (Configuración del cliente)** y seleccione la configuración.
  3. Haga clic en la pestaña **Túnel dividido > Dominio y aplicación** para configurar la configuración del túnel dividido en función del dominio de destino.

     Es posible que experimente algunos problemas de incompatibilidad al usar un producto de seguridad de endpoints de terceros como Sophos en endpoints de macOS.



     - (Opcional) Seleccione **Include Domain (Incluir dominio)** y **Add (Añadir)** 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. 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.
     - (Opcional) Seleccione **Excluir dominio** y **Añadir** para añadir aplicaciones de nube pública o SaaS que desea excluir del túnel VPN mediante el dominio de destino y puerto. Puede añadir hasta 200 entradas a la lista. Por ejemplo, añada *.target.com para excluir todo el tráfico de destino del túnel VPN.
  4. Configure los ajustes de túnel dividido en función de la aplicación.

     No se puede añadir tráfico de Safari a la regla de túnel dividido basado en la aplicación en los endpoints de macOS.

     Puede usar variables de entorno para configurar un túnel dividido basado en la aplicación en los endpoints de Windows y macOS.

     - (Opcional) Seleccione **Incluir nombre de proceso de la aplicación cliente** y haga clic en **Add (Añadir)** para añadir aplicaciones de nube pública o SaaS que desea enrutar

 ©2025 Palo Alto Networks, Inc.

a GlobalProtect a través de la conexión VPN mediante el nombre de proceso de la aplicación. Puede añadir hasta 200 entradas a la lista.

- (Opcional) Seleccione **Exclude Client Application Process Name (Excluir nombre de proceso de la aplicación cliente)** y **Add (Añadir)** para añadir aplicaciones de nube pública o SaaS que desea excluir del túnel VPN mediante el nombre de proceso de la aplicación. Puede añadir hasta 200 entradas a la lista.

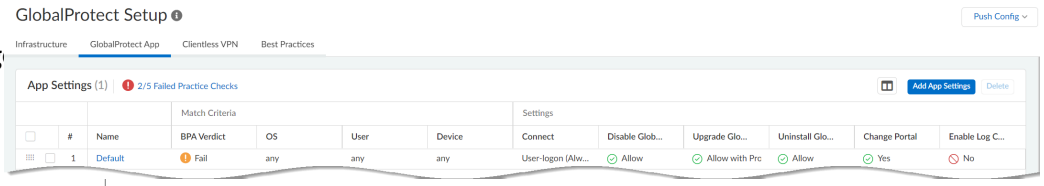
5. Guarde la configuración del túnel.

GlobalProtect: Personalizar la configuración de la aplicación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

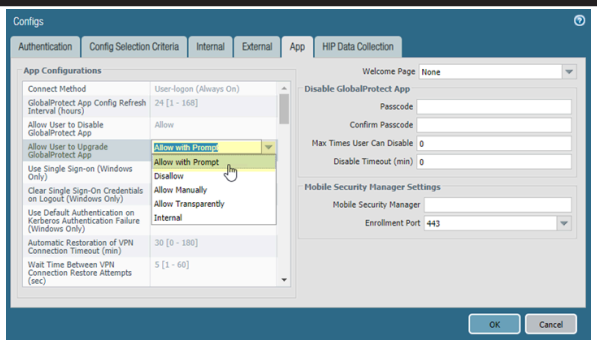
Personalice cómo sus usuarios finales interactúan con la aplicación GlobalProtect.

Hay algunas configuraciones que puede personalizar globalmente. Estas **global app settings (configuraciones de aplicaciones globales)** se aplican a la aplicación GlobalProtect en todos los dispositivos. Las demás configuraciones de la aplicación GlobalProtect se establecen de forma predeterminada. Luego puede personalizar estas opciones y, en función de los **criterios de coincidencia**, orientarlas a usuarios y dispositivos específicos. Los criterios de coincidencia que defina para la configuración de la aplicación indicarán a Prisma Access los usuarios, dispositivos o sistemas que deben recibir la configuración. Por ejemplo, podría especificar que una regla se aplique solo a dispositivos con números de serie que coincidan con las entradas de Active Directory.

Configuración de la aplicación GlobalProtect	
Explore y personalice la configuración de la aplicación aquí (a continuación se muestran ejemplos de g de la nube) —>	Prisma Access (Managed by Strata Cloud Manager)  Panorama Managed Prisma Access

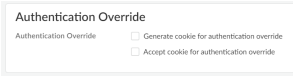
 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect



Cancelación de autenticación

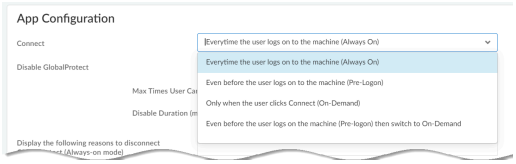
Permitir que Prisma Access genere y acepte cookies seguras y cifradas para la autenticación del usuario. Activar esta opción permite al usuario proporcionar credenciales de inicio de sesión solo una vez durante el período de tiempo especificado.



- **Generate cookie for authentication override (Generar cookie para la anulación de la autenticación)**: permite que Prisma Access genere cookies cifradas y específicas del endpoint y emite cookies de autenticación al endpoint.
- **Accept cookie for authentication override (Aceptar cookie para la anulación de autenticación)**: permite a Prisma Access autenticar usuarios con una cookie válida y cifrada. Cuando la aplicación presenta una cookie válida, Prisma Access verifica que Prisma Access originalmente cifró 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 que la aplicación recupera las cookies, las envía a Prisma Access o a la puerta de enlace para proceder a la autenticación del usuario.
- **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 luego Prisma Access cifra una cookie nueva para enviarla a la aplicación. Este valor puede ser el mismo o diferente a la vida útil de la cookie que configuró para el portal.

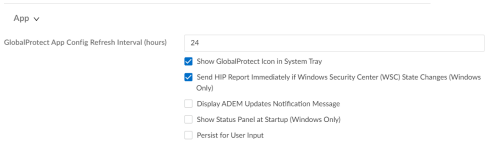
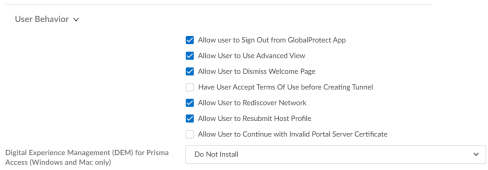
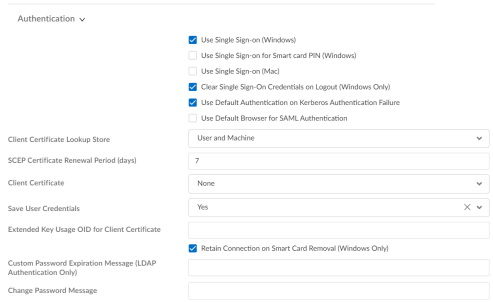
©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	• **Certificate to Encrypt/Decrypt Cookie (Certificado para cifrar/descifrar la cookie)**: seleccione el certificado de RSA para cifrar o descifrar la cookie.
Configuración de conexión	Especifique el método que utiliza la aplicación GlobalProtect para **Connect (Conectarse)** a Prisma Access.  • **User-logon (Always On) [Inicio de sesión de usuario (siempre activo)]**: la aplicación GlobalProtect se conecta automáticamente a Prisma Access tan pronto como el usuario inicia sesión. Cuando se usa en conjunto con el SSO (solo en los endpoints de Windows), el inicio de sesión 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 la aplicación de 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 VPN con Prisma Access antes de que el usuario inicie sesión. Esta opción requiere que utilice una solución de PKI externa para implementar previamente un certificado de equipo en cada dispositivo que reciba estos ajustes. • **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. • **Pre-logon then On-demand (Inicio de sesión previo y luego bajo demanda)**: similar al método de conexión de Inicio de sesión previo (siempre activado), este método (que requiere la versión de publicación de contenido 590-3397 o posterior) permite que la aplicación de GlobalProtect autentique al usuario y establezca un túnel de VPN a Prisma Access 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, los usuarios deben iniciar manualmente la aplicación para conectarse con GlobalProtect si la conexión finaliza por algún motivo. La ventaja de esta opción es

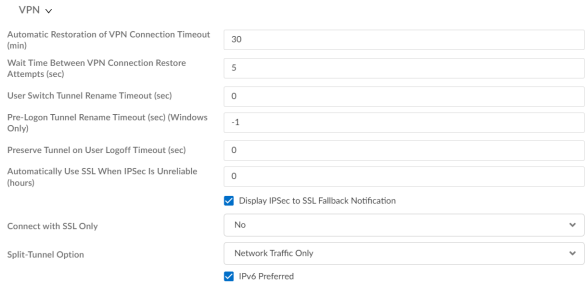
 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	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.
GlobalProtect	Decida qué configuraciones de la aplicación GlobalProtect puede ajustar el usuario: • **Disable GlobalProtect (Deshabilitar GlobalProtect)**: decide si los usuarios pueden o no deshabilitar la aplicación GlobalProtect. Los usuarios que deshabilitan la aplicación GlobalProtect no pueden conectarse a Prisma Access (y los recursos protegidos de su empresa) hasta que vuelvan a activar la aplicación. • **Upgrade GlobalProtect (Actualizar GlobalProtect)**: especifique cómo deben funcionar las actualizaciones de la aplicación, incluido si los usuarios pueden iniciar actualizaciones. 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. ◦ **Allow with Prompt (Permitir con mensaje emergente)**: solicite a los usuarios que actualicen cuando haya una nueva versión de la aplicación disponible. ◦ **Allow Transparently (Permitir de forma transparente)**: las actualizaciones se producen automáticamente sin la interacción del usuario. ◦ **Internal (Interno)**: las actualizaciones se producen automáticamente sin interacción del usuario cuando el usuario está conectado a Prisma Access. ◦ **Disallow (No permitir)**: evita actualizaciones de aplicaciones. ◦ **Allow Manually (Permitir manualmente)**: permita que los usuarios inicien actualizaciones de aplicaciones desde dentro de la aplicación GlobalProtect. • **Uninstall GlobalProtect (Desinstalar GlobalProtect)**: permita a los usuarios desinstalar la aplicación de

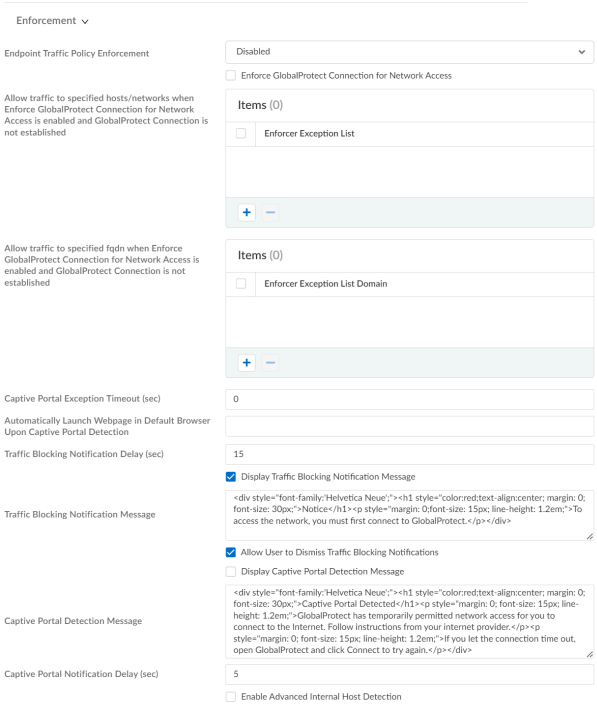
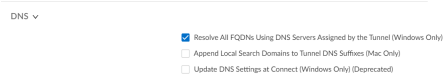
 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	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. • **User Can Change Portal (El usuario puede cambiar el portal)**: permite que los usuarios cambien el portal que utiliza la aplicación GlobalProtect para conectarse Prisma Access.
Configuración de la aplicación: Opciones avanzadas	
Ajustes de Aplicación	• Enviar informe de HIP de inmediato si cambia el estado del Centro de seguridad de Windows (WSC) (solo Windows): 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 Sí (valor por defecto) para enviar inmediatamente datos HIP cuando cambia el estado de WSC. 
Configuración del comportamiento del usuario	La configuración del comportamiento del usuario incluye: 
Configuración de autenticación	La configuración de autenticación incluye: 
Configuración de VPN	Configurar el tiempo de espera de la VPN y la configuración del túnel: • **Mostrar notificación de respaldo de IPSec a SSL**: seleccione **No** para evitar notificaciones emergentes

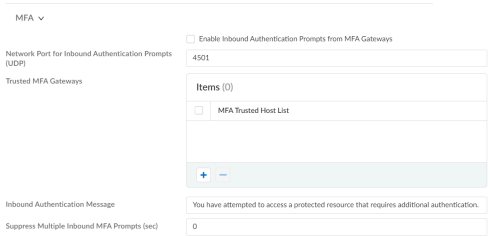
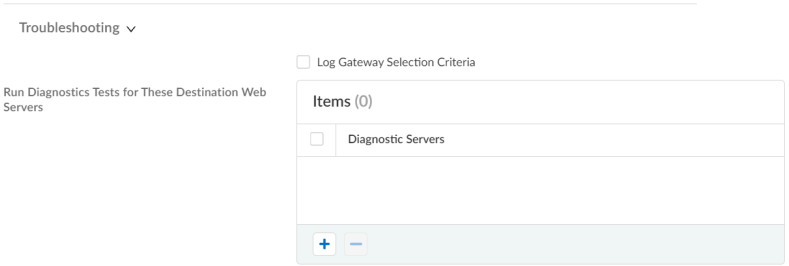
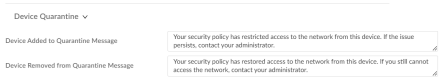
 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	cuando la aplicación GlobalProtect no logra establecer conexión a un túnel IPSec y vuelve a un túnel SSL. Seleccione **Sí** (predeterminado) para permitir notificaciones emergentes cuando cambie la conexión. 
Configuración de cumplimiento	Aplicar configuraciones para el tráfico especificado: • **Permitir el tráfico al FQDN especificado cuando la opción Aplicar conexión de GlobalProtect para acceso de red está habilitada y la opción Conexión de GlobalProtect no está establecida**: Obtener información. • **Automáticamente inicie la página web en el navegador web predeterminado después de la detección del portal cautivo**: para iniciar automáticamente sus navegadores web predeterminados para que los usuarios puedan iniciar sesión en el portal de autenticación sin problemas, introduzca el nombre de dominio cualificado 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). Luego, el portal de autenticación intercepta este intento de conexión del sitio web y redirige el navegador web predeterminado a la página de inicio de sesión del portal de autenticación. Si este campo está vacío (predeterminado), Prisma Access no inicia el navegador web predeterminado automáticamente al detectar el portal cautivo. • **Habilitar la detección avanzada de host interno**: habilite la detección avanzada de host interno para añadir una capa de seguridad adicional durante la detección de host interno por parte de la aplicación GlobalProtect. Con la detección avanzada de host interno, la aplicación valida el certificado del servidor de las puertas de enlace internas además de realizar una búsqueda de DNS inversa del host interno para determinar si la aplicación está dentro de la red empresarial. Al habilitar la detección avanzada de host interno, se evita que actores maliciosos falsifiquen la respuesta del servidor DNS inverso durante la detección de host interno y, de ese modo, se evita el acceso no

 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	autorizado a los endpoints de la red empresarial. Si no habilita la detección avanzada de host interno, la detección de host interno existente funciona como se espera. 
Configuración del comportamiento de la conexión	La configuración del comportamiento de conexión incluye:  Más información.
Configuración DNS	La configuración DNS incluye: 
Configuración de proxy	Especifique la **Proxy Auto-Configuration (PAC) File URL [URL del archivo de configuración automática de proxy (PAC)]** que desea enviar al endpoint para configurar los ajustes del proxy. La longitud máxima de la URL es de 256 caracteres. Se admiten los siguientes métodos de URL de archivo de configuración automática de proxy (PAC): • Estándar de configuración automática de proxy (PAC) (por ejemplo, http://pac.<hostname or IP>/proxy.pac).

 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	• Estándar de protocolo de detección automática de proxy web (WPAD) (por ejemplo, http://wpad.<hostname or IP>/wpad.dat). 
Configuración de MFA	La configuración MFA incluye: 
Configuración de resolución de problemas	Las configuraciones para resolución de problemas incluyen: 
Configuración de cuarentena del dispositivo	La configuración de cuarentena del dispositivo incluye: 
Detección de host interno	Si no necesita que sus usuarios móviles se conecten a Prisma Access cuando están en la red interna, habilite la detección de host interno para permitir que la aplicación GlobalProtect determine si está en una red interna o externa. • Introduzca la dirección IP (IPv4 o IPv6) de un host al que solo se tenga acceso desde la red interna. • Introduzca el Nombre de host del DNS que se resuelve en la dirección IP que ha introducido. Cuando un usuario móvil se conecta a Prisma Access, la aplicación GlobalProtect intenta realizar una búsqueda de DNS inversa en la dirección especificada. Si la búsqueda

 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	falla, la aplicación GlobalProtect determina que está en la red externa y luego inicia una conexión a Prisma Access.
Habilitar detección de host interno	Si desea que la aplicación GlobalProtect vuelva a intentar la detección de red cuando se configuran una puerta de enlace interna y una detección de host interna sin una puerta de enlace externa y la detección de host interna falla, establezca el parámetro **Enable Intelligent Internal Host Detection (Habilitar detección inteligente de host interno)** en Sí.
Gateways	De forma predeterminada, todas las puertas de enlace de sus ubicaciones de Prisma Access están disponibles para los usuarios. Si tiene puertas de enlace GlobalProtect adicionales (internas o externas) a las que desea que sus usuarios puedan conectarse, puede añadirlas aquí.
Recopilación de datos HIP	Defina los datos personalizados del perfil de información de hosts (HIP) que la aplicación debe recopilar o excluir de la recopilación. Cuando esta opción está habilitada, la aplicación recopila datos de dispositivos que ejecutan sistemas operativos Windows, Mac o Linux. Por ejemplo, una verificación personalizada podría permitirle saber si una determinada aplicación está instalada o ejecutándose en un endpoint. Los datos que usted define para su recopilación en una verificación personalizada se incluyen en los datos de información del host sin procesar que la aplicación GlobalProtect recopila y luego envía a Prisma Access cuando la aplicación se conecta. 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. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **HIP** y **HIP Objects (Objetos HIP)** o **HIP Profiles (Perfiles HIP)**. Seleccione el ámbito de configuración **Prisma Access** > **Mobile Users Container (Contenedor de usuarios móviles)** > **GlobalProtect**.
Configuración de tiempo de espera	• En la página de configuración de GlobalProtect, seleccione el icono de engranaje en el área de Configuración global de la aplicación. • Modifique la vigencia máxima de la **Login Lifetime (Duración de sesión)** para una única sesión de inicio de sesión de la puerta de enlace (el valor predeterminado

 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	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. • Establezca la cantidad de avisos anticipados que se debe proporcionar a los usuarios para indicar que sus sesiones de aplicación están a punto de expirar debido al vencimiento del período de vida útil del inicio de sesión. El valor predeterminado es de 30 horas. El intervalo aceptado es de 0 a 60 minutos. • Personalice el mensaje de notificación de tiempo de espera. • Modifique el período de **Inactivity Logout (Cierre de sesión por inactividad)** para especificar el periodo de tiempo después del cual se cierra la sesión de GlobalProtect de los usuarios inactivos (el rango es de 5 a 43200 minutos; el valor predeterminado es de 180 minutos). Puede aplicar una política de seguridad para supervisar el tráfico de los endpoints mientras está conectado a GlobalProtect y para cerrar con rapidez las sesiones inactivas de GlobalProtect estableciendo un período de cierre de sesión por inactividad más corto. Los usuarios se desconectan de GlobalProtect si la aplicación de GlobalProtect no ha enrutado tráfico a través del túnel VPN o si la puerta de enlace no recibe una comprobación HIP del endpoint en el período establecido. El valor predeterminado es 180 minutos El rango aceptado es de 5-43200 minutos. • Establezca la cantidad de aviso anticipado que se debe proporcionar a los usuarios para indicar que sus sesiones de aplicación están a punto de expirar debido a la inactividad. El valor predeterminado es de 30 horas. El intervalo aceptado es de 0 a 60 minutos. • Personalice el mensaje de notificación de inactividad. • Especifique si desea notificar a los usuarios finales si su administrador cierra su sesión y configure el mensaje que se mostrará. • Haga clic en **Save (Guardar)**.
Aplicación de la dirección IP de origen para las cookies de autenticación.	Configure los ajustes de conexión VPN y las restricciones de uso de cookies de autenticación para una postura de seguridad mejorada.

©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	• En la página de configuración de GlobalProtect, seleccione el icono de engranaje en el área de Configuración global de la aplicación. • Configure la restauración automática de los túneles VPN SSL. Si la restauración automática de la conexión VPN está habilitada en el portal GlobalProtect, puede deshabilitarla para esta puerta de enlace seleccionando **Disable Automatic Restoration of SSL VPN (Deshabilitar la restauración automática de la VPN SSL)**. • Configure la aplicación de la dirección IP de origen para las cookies de autenticación. Puede configurar el portal o la puerta de enlace de GlobalProtect para que acepte las cookies de los endpoints 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 originalmente se emitió una cookie de autenticación para un endpoint con una dirección IP de origen pública de 201.109.11.10, y la máscara de subred del rango de direcciones IP de red está configurada en /24, la cookie de autenticación será posteriormente válida en endpoints con direcciones IP de origen públicas dentro del rango de direcciones IP de red 201.109.11.0/24. En la sección Restricciones de uso de cookies de autenticación, seleccione **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) [Restringir el uso de cookies de autenticación (para la restauración automática del túnel VPN o la anulación de la autenticación)]** y luego configure una de las siguientes 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. Introduzca una máscara

 ©2025 Palo Alto Networks, Inc.

Configuración de la aplicación GlobalProtect	
	de red IPv4 de origen o una máscara de red IPv6 de origen para definir 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).

Solicitud de ticket para desactivar GlobalProtect

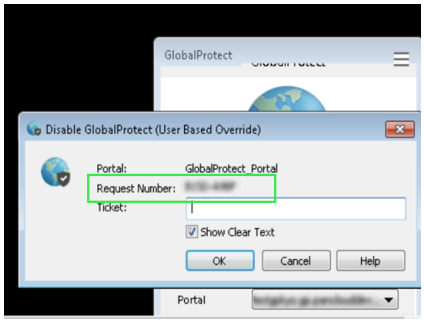
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En lugar de permitir que los usuarios deshabiliten directamente GlobalProtect, puede permitir que un usuario cree un ticket de incidencia para deshabilitar GlobalProtect. El administrador de GlobalProtect puede luego decidir si permite o no que cada usuario específico desactive GlobalProtect.

Cómo funciona

Una vez que haya configurado esta función, este es el flujo de trabajo para una solicitud de ticket para deshabilitar GlobalProtect:

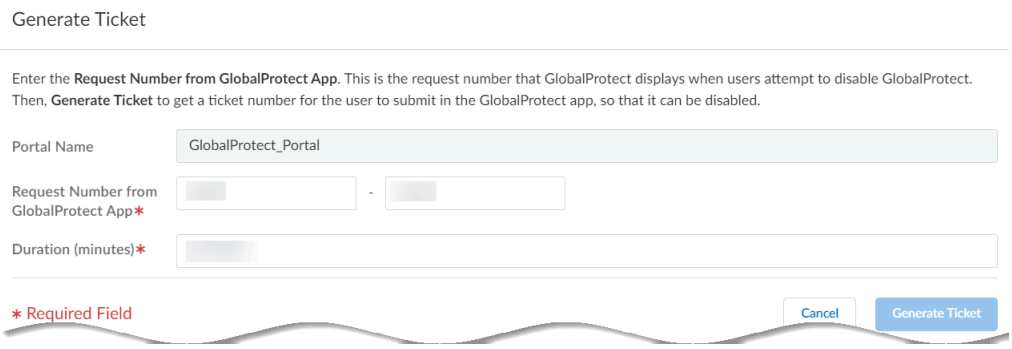
- Un usuario intenta deshabilitar GlobalProtect en la aplicación GlobalProtect. GlobalProtect muestra un número de solicitud al usuario.



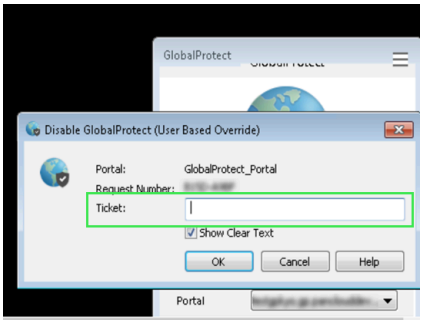
- El usuario comparte el número de solicitud con el administrador de GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

- El administrador de GlobalProtect inicia sesión en Prisma Access (Managed by Strata Cloud Manager) y utiliza el número de solicitud para generar un ticket.



- El administrador de GlobalProtect comparte el número de ticket con el usuario. El usuario introduce el número de ticket en la aplicación para desactivar GlobalProtect.



Configurarlo

- Strata Cloud Manager
- Panorama

Solicitud de ticket para desactivar GlobalProtect (Strata Cloud Manager)

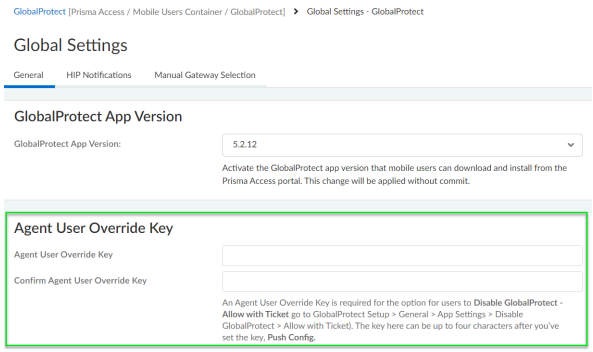
STEP 1 | Establecer una clave de anulación de agente

Antes de poder habilitar la opción para solicitudes de tickets de incidencia para deshabilitar GlobalProtect, primero debe establecer una clave de anulación de usuario de agente.

Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect app (Aplicación de GlobalProtect)** > **Global App Settings**

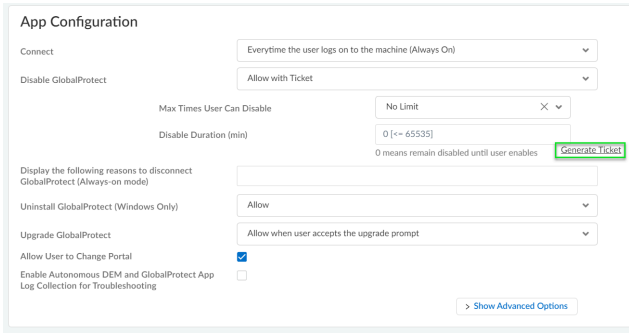
 ©2025 Palo Alto Networks, Inc.

(Configuración global de la aplicación) e introduzca una tecla de cuatro caracteres para establecer la **Agent Override Key (Clave de anulación del agente)**.



STEP 2 | Permitir que GlobalProtect se deshabilite con un ticket

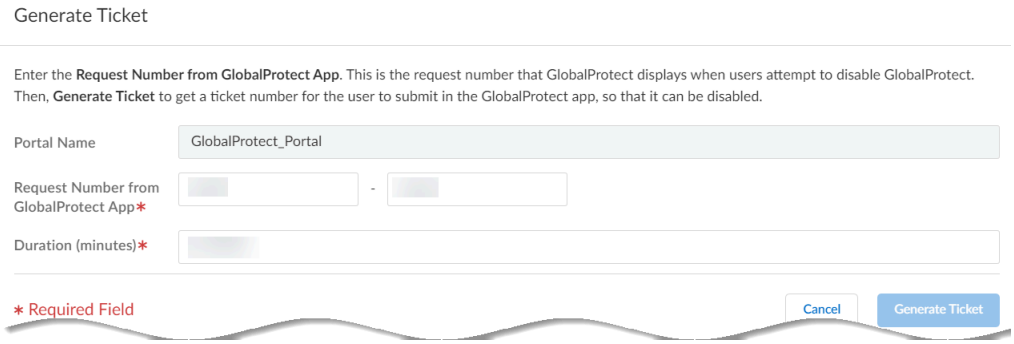
Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect app (Aplicación de GlobalProtect)** > **App Settings (Configuración de la aplicación)** > **App Configuration (Configuración de la aplicación)** > **Disable GlobalProtect (Desactivar GlobalProtect)** y establezca la opción en **Allow with Ticket (Permitir con ticket de incidencia)**.



STEP 3 | Generar un ticket

Después de configurar la **Agent Override Key (Clave de anulación del agente)** y la opción de **Allow with Ticket (Permitir con ticket)**, podrá: **Generate Ticket (Generar ticket)**.

Cuando un usuario intenta desactivar GlobalProtect en la aplicación, GlobalProtect le mostrará un número de solicitud. Envíe ese número de solicitud aquí para generar un ticket para que GlobalProtect se deshabilite para ese usuario.



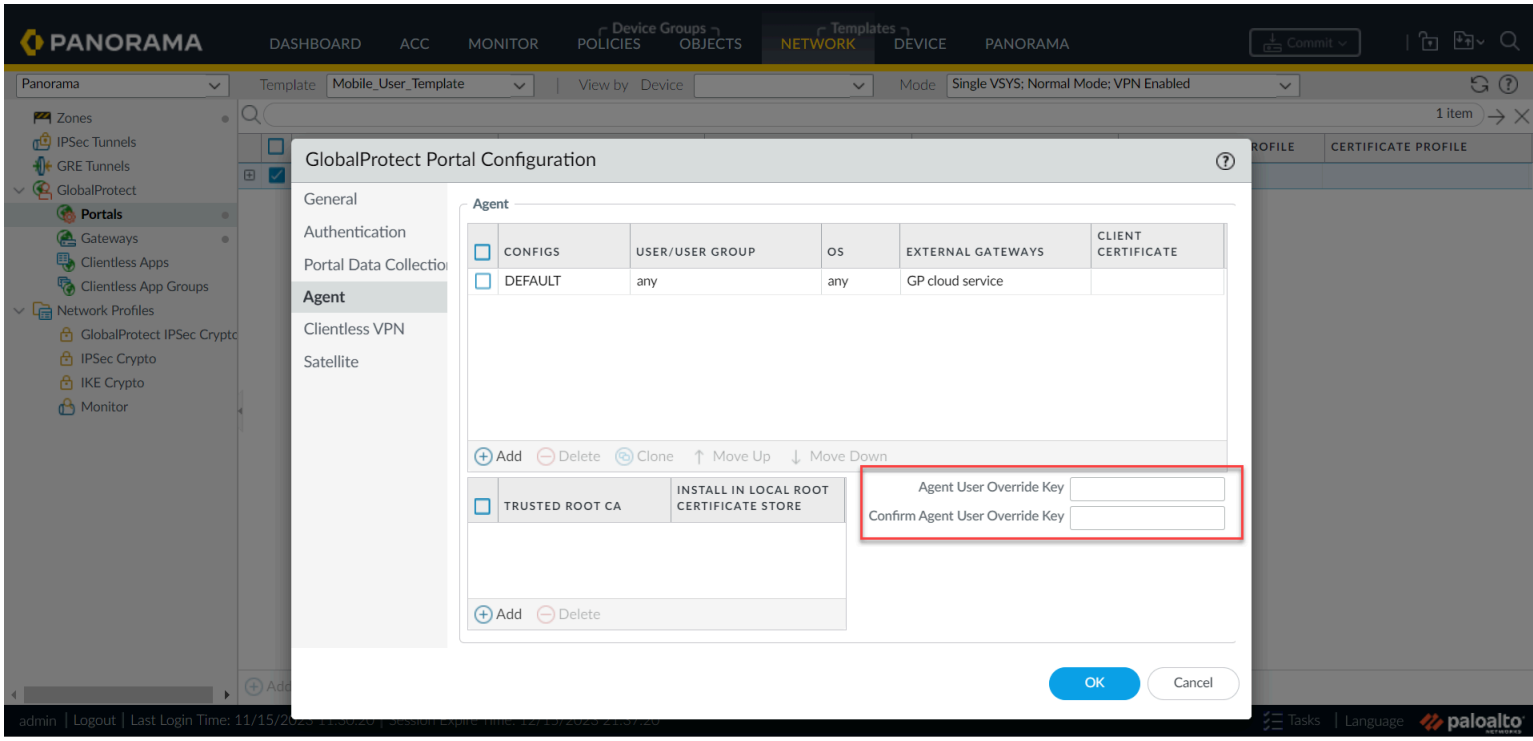
 ©2025 Palo Alto Networks, Inc.

Solicitud de ticket para desactivar GlobalProtect (Panorama)

STEP 1 | Establecer una clave de anulación de agente

Antes de poder habilitar la opción para solicitudes de tickets de incidencia para deshabilitar GlobalProtect, primero debe establecer una clave de anulación de usuario de agente.

Vaya a **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y seleccione el nombre de conexión para el que desea establecer una clave de anulación. Seleccione **Agent (Agente)** y, a continuación, introduzca una clave para establecer la **Agent Override Key (Clave de anulación del agente)**.

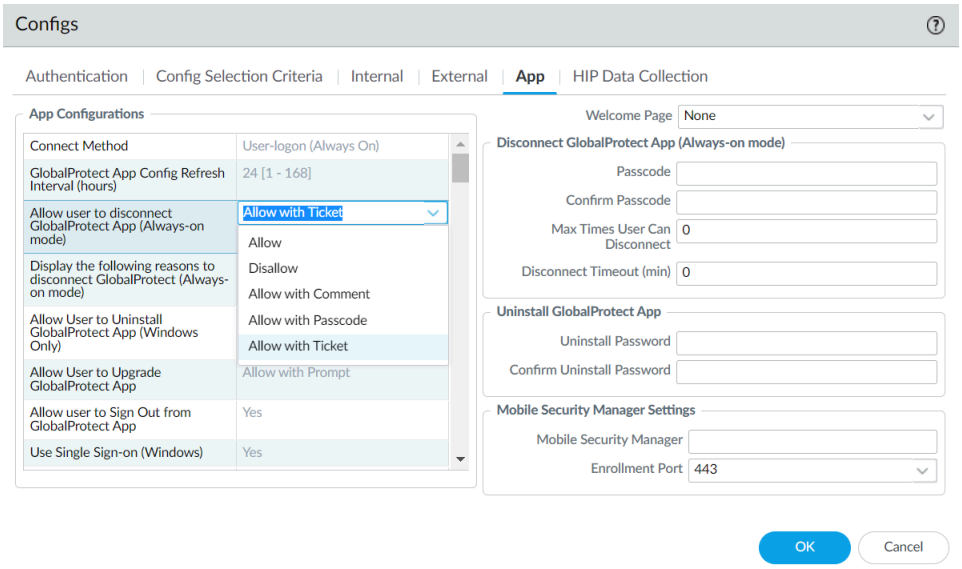


STEP 2 | Permitir que GlobalProtect se deshabilite con un ticket

Vaya a **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y seleccione el nombre de conexión del que desea permitir que los usuarios se desconecten. Seleccione **Agent (Agente)**, elija un **Config (Configuración)**, seleccione **App (Aplicación)** > **App Configurations (Configuraciones de aplicación)** > **Allow user to disconnect GlobalProtect App (Always-on mode) [Permitir al**

©2025 Palo Alto Networks, Inc.

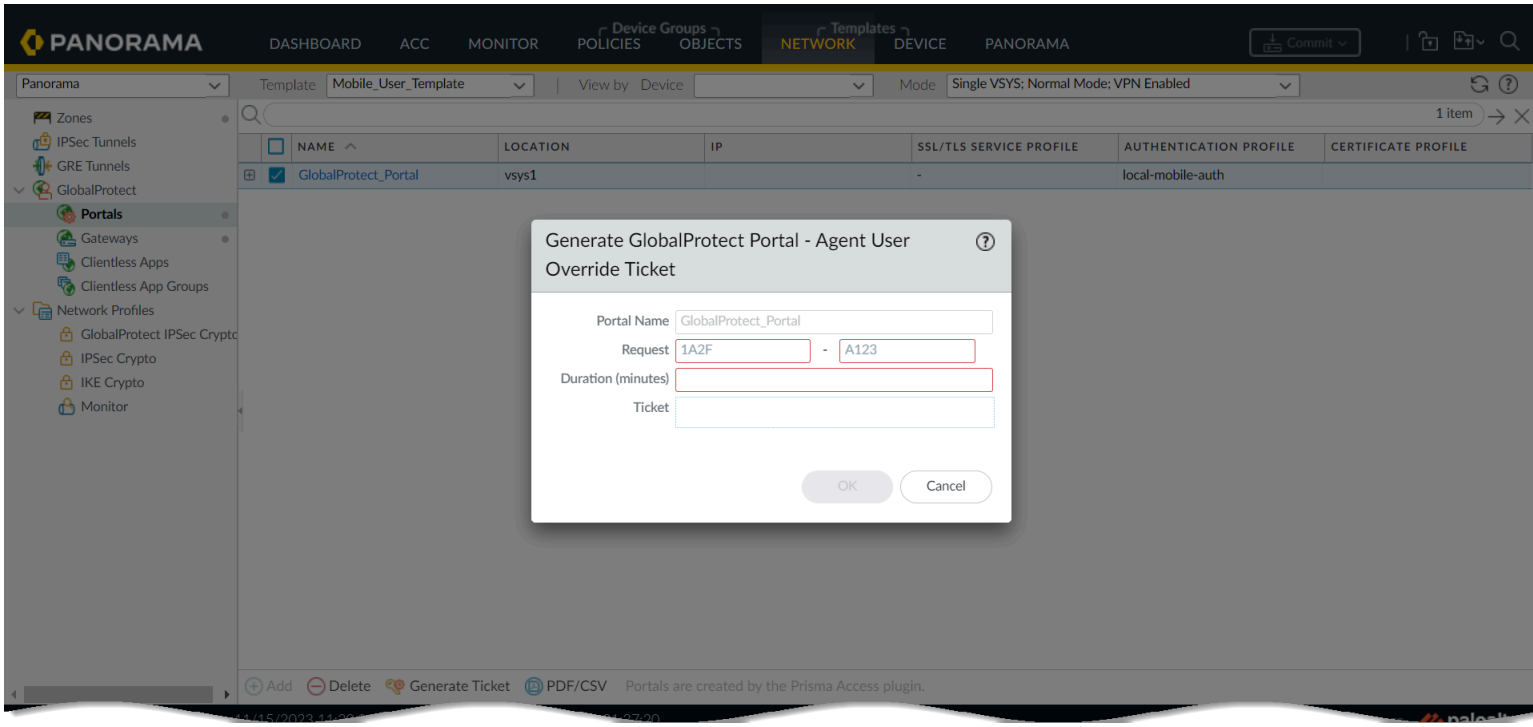
usuario desconectar la aplicación GlobalProtect (modo siempre activa)] y establezca la opción en **Allow with Ticket (Permitir con Ticket de incidencia)**.



STEP 3 | Generar un ticket

Después de configurar la **Agent Override Key (Clave de anulación del agente)** y la opción de **Allow with Ticket (Permitir con ticket)**, podrá: **Generate Ticket (Generar ticket)**.

Cuando un usuario intenta desactivar GlobalProtect en la aplicación, GlobalProtect le mostrará un número de solicitud. Envíe ese número de solicitud aquí para generar un ticket para que GlobalProtect se deshabilite para ese usuario.



 ©2025 Palo Alto Networks, Inc.

Inicio de sesión previo de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access ❑ Acceso de administrador al endpoint para instalar el certificado de máquina ❑ Certificado PKI de confianza implementado en el endpoint

El inicio de sesión previo es un método de conexión que establece un túnel VPN antes de que un usuario inicie sesión. El objetivo 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 preinicio de sesión utiliza un nombre de usuario genérico de preinicio de sesión porque el usuario no ha iniciado sesión. Para permitir que los endpoints accedan a los recursos, debe crear reglas de políticas de seguridad que coincidan con el usuario anterior al inicio de sesión. Estas reglas de políticas deben permitir el acceso solo a los servicios básicos para iniciar el sistema, por ejemplo, DHCP, DNS, servicios específicos de Active Directory, antivirus u otros servicios de actualización. Después de que el usuario se autentique en la puerta de enlace, la aplicación GlobalProtect reasigna el túnel VPN a ese usuario. La asignación de direcciones IP en Prisma Access cambia del endpoint de preinicio de sesión al usuario autenticado.

El certificado utilizado para la autenticación previa al inicio de sesión reside en el almacén de certificados personal del endpoint. Utilice una CA de terceros de confianza, una CA autofirmada o una CA de PKI interna para emitir un certificado de máquina. Necesita configurar un certificado de máquina como método de autenticación para establecer un túnel desde un endpoint antes de iniciar sesión en Prisma Access, y luego crear un perfil de certificado que incluya el certificado CA de inicio de sesión previo.

- Strata Cloud Manager
- Panorama

Inicio de sesión previo de GlobalProtect (Strata Cloud Manager)

Importar un certificado CA raíz de terceros

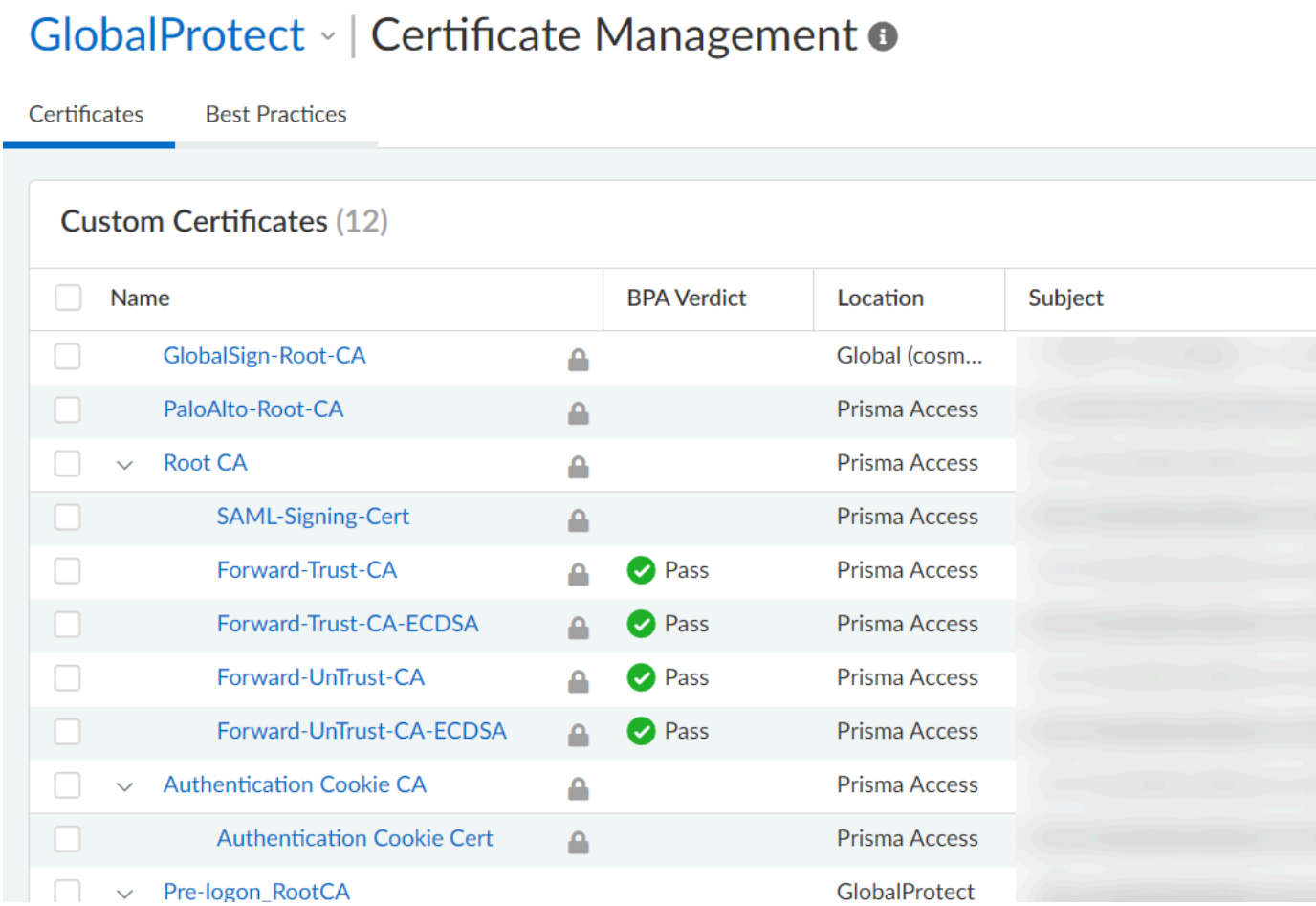
Utilice un certificado de máquina como método de autenticación para establecer un túnel desde un endpoint antes de iniciar sesión en Prisma Access.

STEP 1 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Certificate Management (Gestión de certificados)**. Seleccione el ámbito de configuración de **Prisma Access**

Asegúrese de estar importando el certificado para los usuarios móviles de GlobalProtect.

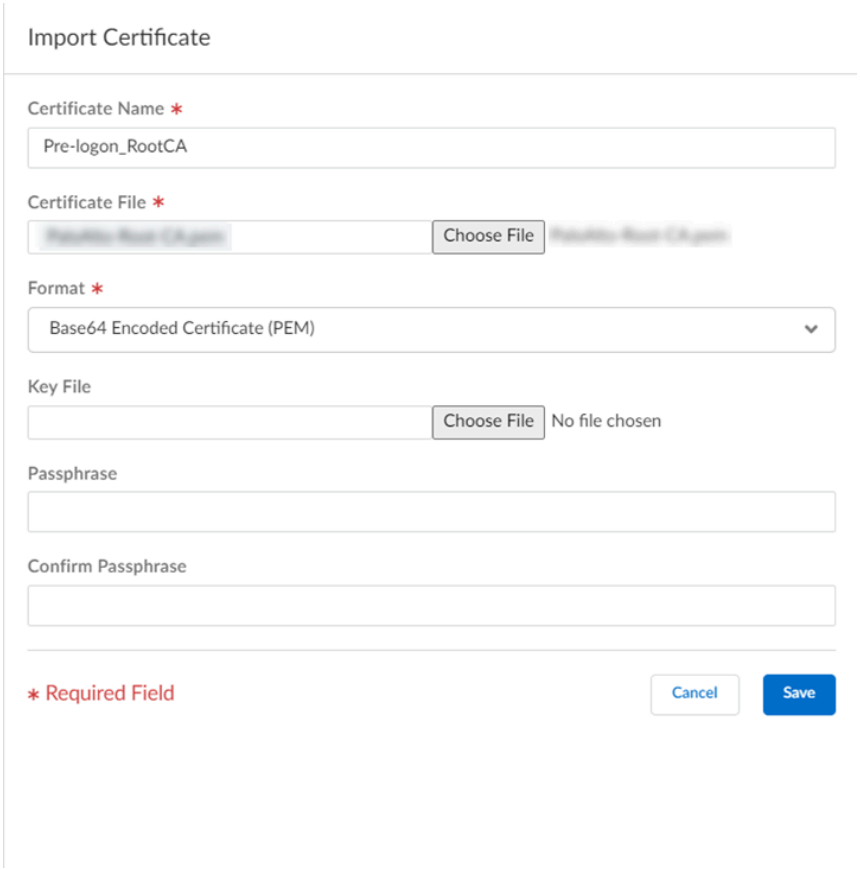
 ©2025 Palo Alto Networks, Inc.

STEP 2 | **Import (Importar)** un certificado personalizado.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Introduzca valores y elija **Save (Guardar)** la configuración del certificado.



Crear un perfil de certificado previo al inicio de sesión

Cree un perfil de certificado e incluya la CA raíz autofirmada. Esta CA valida el certificado de la máquina por parte del usuario móvil de GlobalProtect durante el inicio de sesión previo.

STEP 1 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Objects (Objetos)** > **Certificate Management (Gestión de certificados)**. Seleccione el ámbito de configuración de **Prisma Access**

STEP 2 | **Añadir perfil**

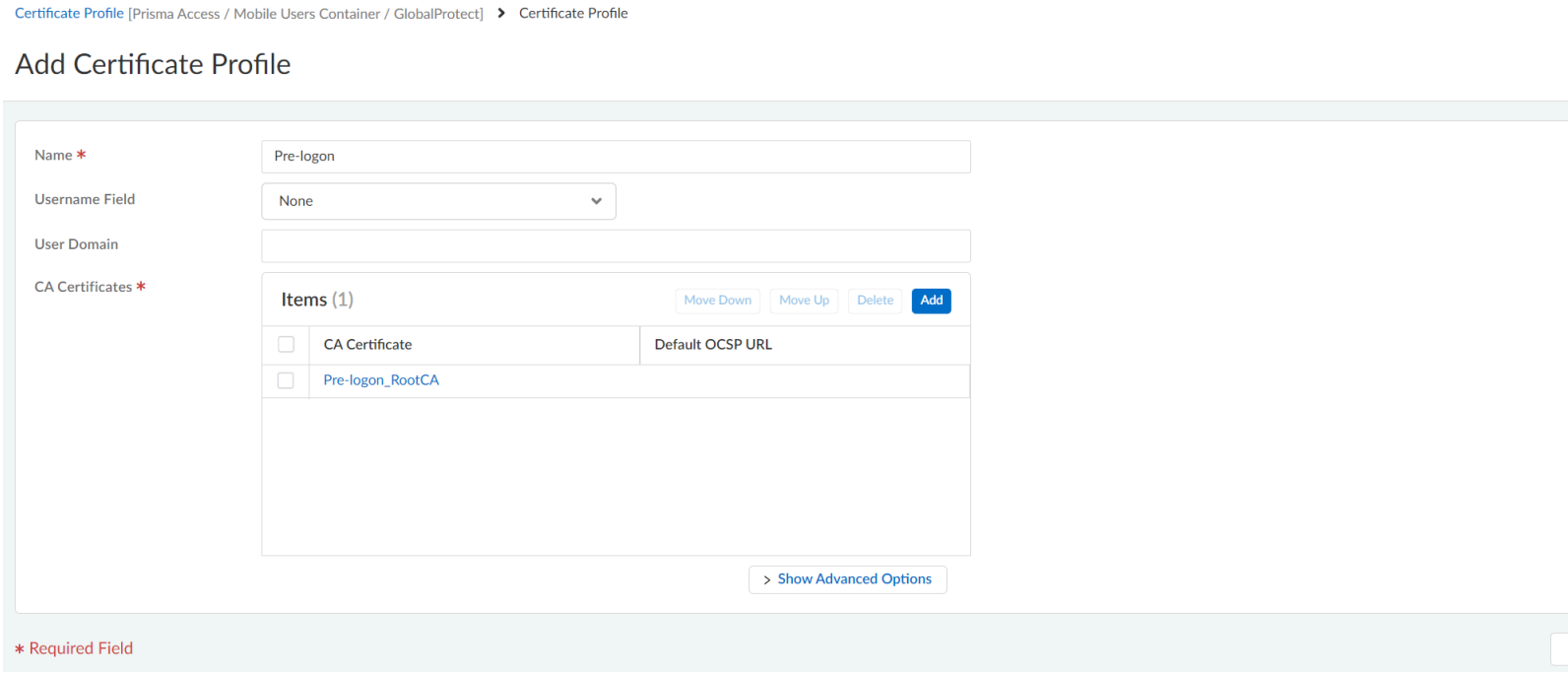
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Introduzca valores.

1. Asegúrese de que el **Username Field (Campo Nombre de usuario)** sea **None (Ninguno)** para evitar la asignación del certificado a un usuario.

   *El **Username Field (Campo de nombre de usuario)** no puede ser **None (Ninguno)** si autentica su certificado mediante cualquier método de autenticación **O** certificado de cliente como se menciona en el paso 2.*

2. **Add (Añadir)** el certificado raíz de autoridad de certificación (CA) para inicio de sesión previo que importó en el Paso 1.
3. Deberá **Save (Guardar)** la configuración de perfiles de certificado



Configurar el portal de GlobalProtect para el Inicio de sesión previo

Configure el portal GlobalProtect para autenticar conexiones con un certificado de máquina.

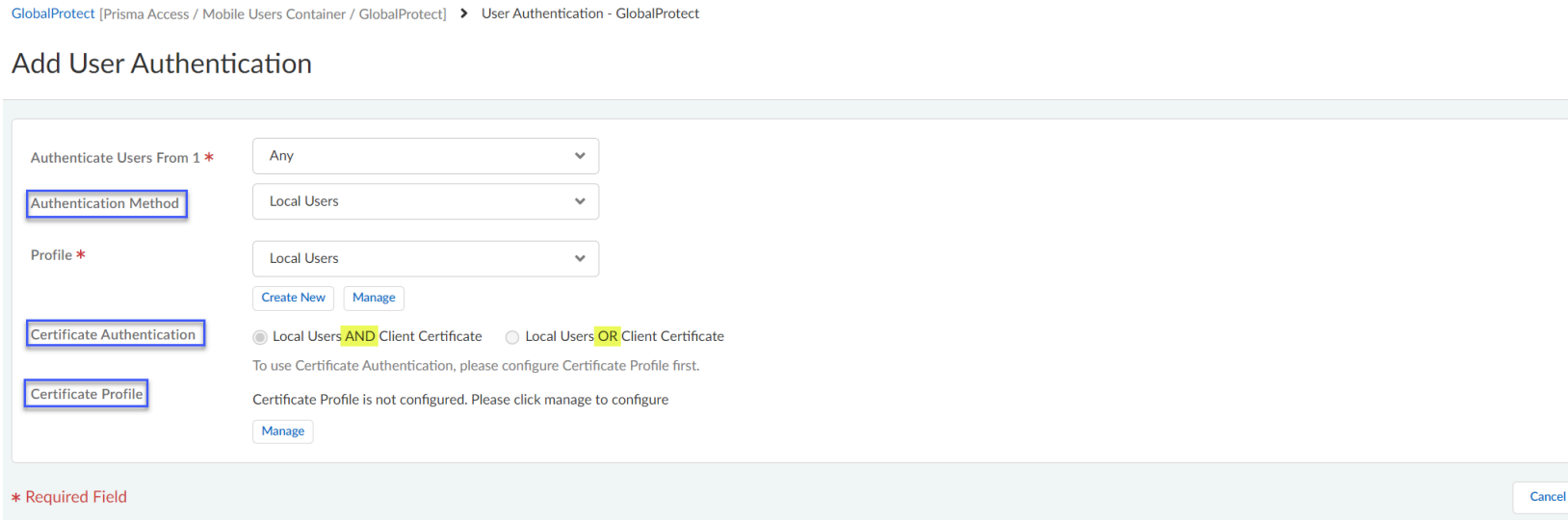
STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Editar la configuración de autenticación de usuario.

Seleccione un método de autenticación que admita GlobalProtect, el perfil de certificado previo al inicio de sesión que creó y la autenticación del certificado.

Elija cualquier autenticación de certificado que admita GlobalProtect.

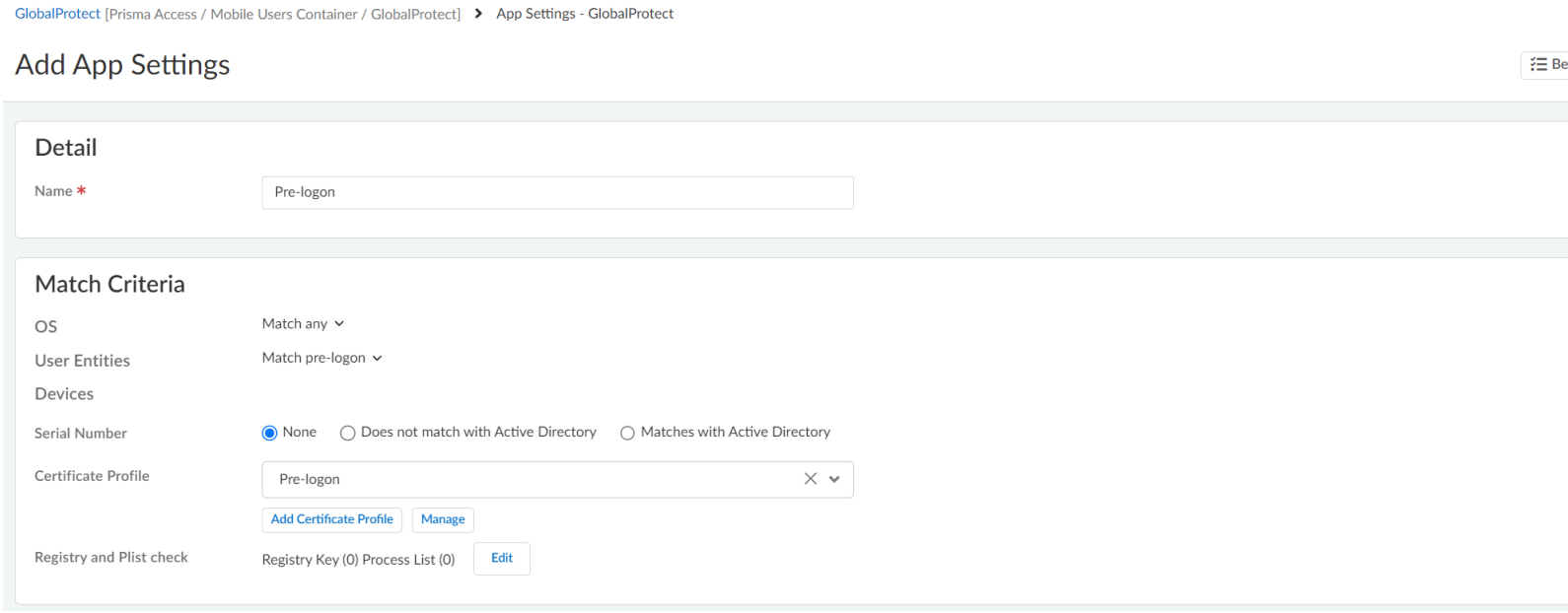


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure los ajustes de la aplicación GlobalProtect para que coincidan con los criterios previos al inicio de sesión.

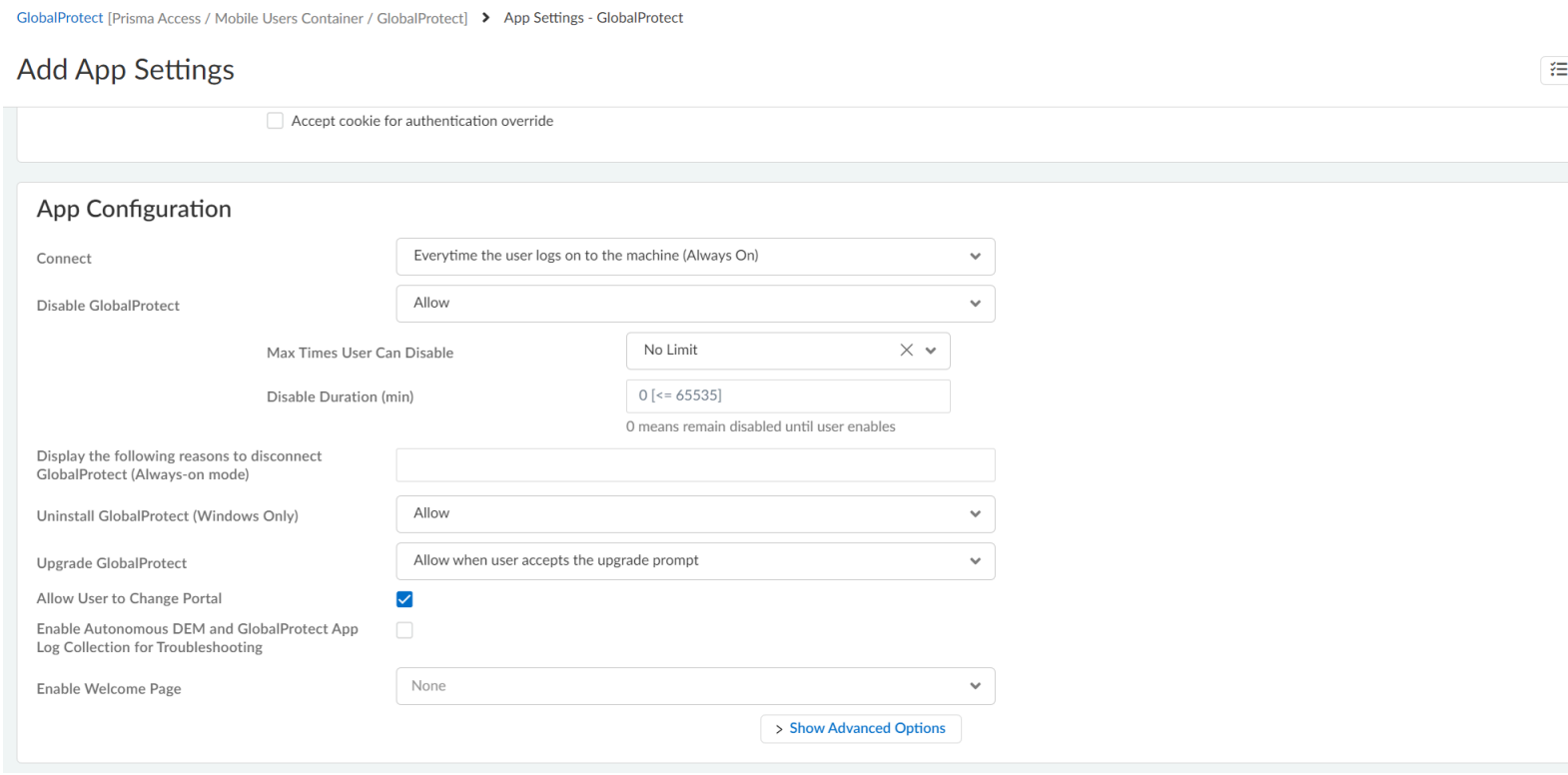
1. Vaya a la pestaña de **GlobalProtect App (Aplicación de GlobalProtect)**.
2. **Añadir ajustes de aplicación.**

*Al introducir valores, asegúrese de **Match pre-logon (Hacer coincidir el inicio de sesión previo)** con las entidades de usuario y el perfil de certificado previo al inicio de sesión.*



- Seleccione un método de conexión previo al inicio de sesión.

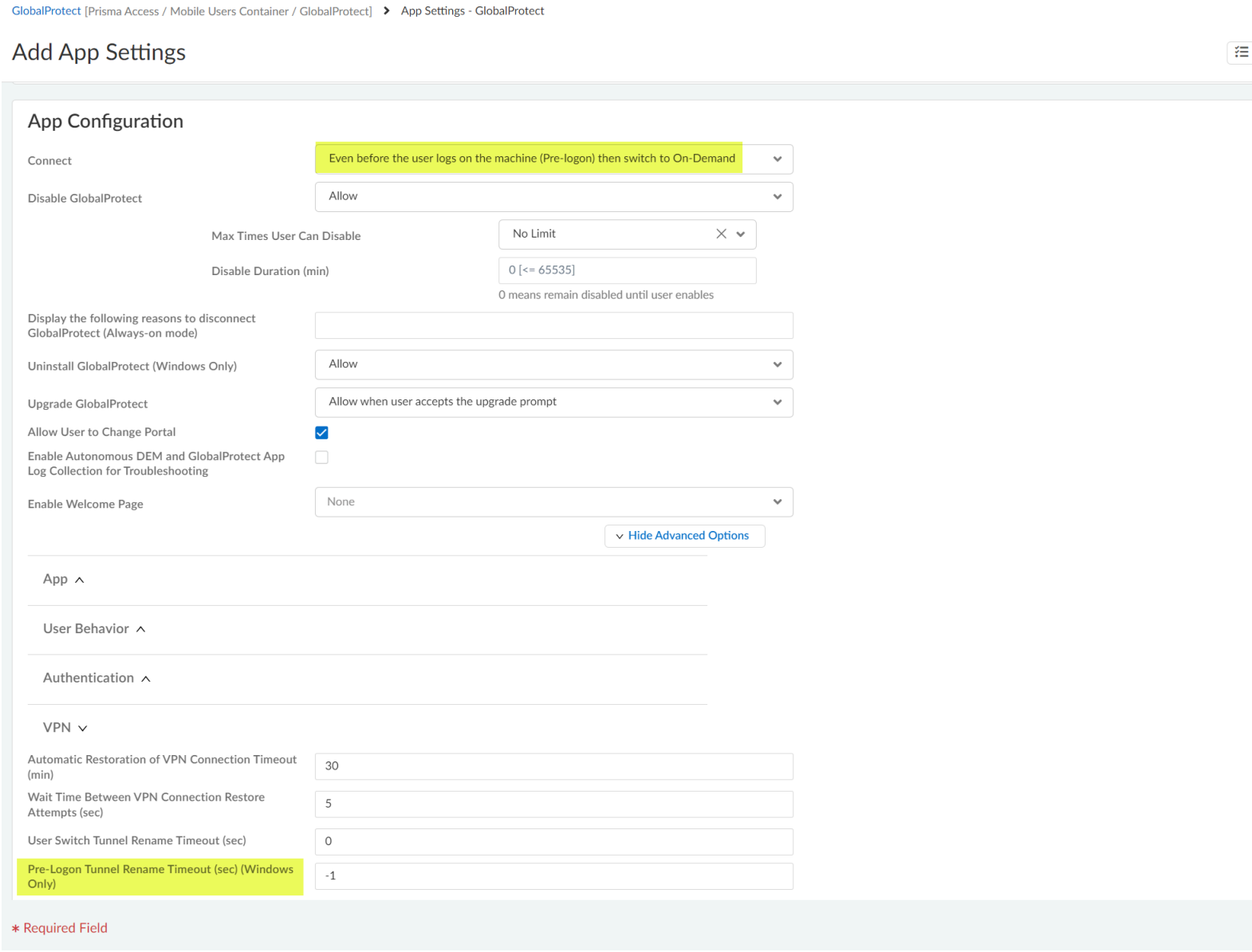
 ©2025 Palo Alto Networks, Inc.



- Si selecciona **Even before the user logs on the machine (Pre-logon) then switch to On-Demand (Incluso antes de que el usuario inicie sesión en la máquina (Inicio de sesión previo) y luego cambia a Bajo demanda)**, configure el valor de **Pre-logon**

 ©2025 Palo Alto Networks, Inc.

Tunnel Rename Timeout (Tiempo de espera de cambio de nombre del túnel de inicio de sesión anterior) en -1. Vea las opciones avanzadas de VPN para editar este campo.



3. Mueva la configuración de la aplicación previa al inicio de sesión por encima de otras configuraciones de la aplicación.
4. Edite todas las demás configuraciones de la aplicación para usuarios autenticados.

   Actualice el método de conexión y el perfil del certificado.

STEP 4 | Enviar los cambios a Prisma Access.

Instalar un certificado de máquina: Windows

Instale el certificado de la máquina en el endpoint, que se utiliza para la autenticación.

STEP 1 | Exporte el certificado CA raíz autofirmado desde su PKI en formato de **Binary Encoded Certificate (DER) [Certificado codificado en binario (DER)]**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Transfiera los archivos del certificado a un equipo Windows.

STEP 3 | Instale el certificado CA de inicio previo a la sesión raíz en el almacén **Trusted Root Certification Authorities (Autoridades de certificación raíz de confianza)** de su máquina local.

STEP 4 | Instale el certificado de la máquina previa al inicio de sesión en la ubicación de almacenamiento de la máquina local.

STEP 5 | Continúe con la instalación, introduzca la contraseña cuando se le solicite y complete la instalación.

STEP 6 | Conéctese al portal GlobalProtect y elimine todas las cookies del host.

STEP 7 | (Opcional) Cierre la sesión de su máquina y vea los logs de GlobalProtect para verificar la conexión previa al inicio de sesión.

Inicio de sesión previo de GlobalProtect (Panorama)

Configurar el certificado y el perfil previos al inicio de sesión

Configure un certificado de máquina como método de autenticación para establecer un túnel desde un endpoint antes de iniciar sesión en Prisma Access, y luego crear un perfil de certificado que incluya el certificado CA de inicio de sesión previo.

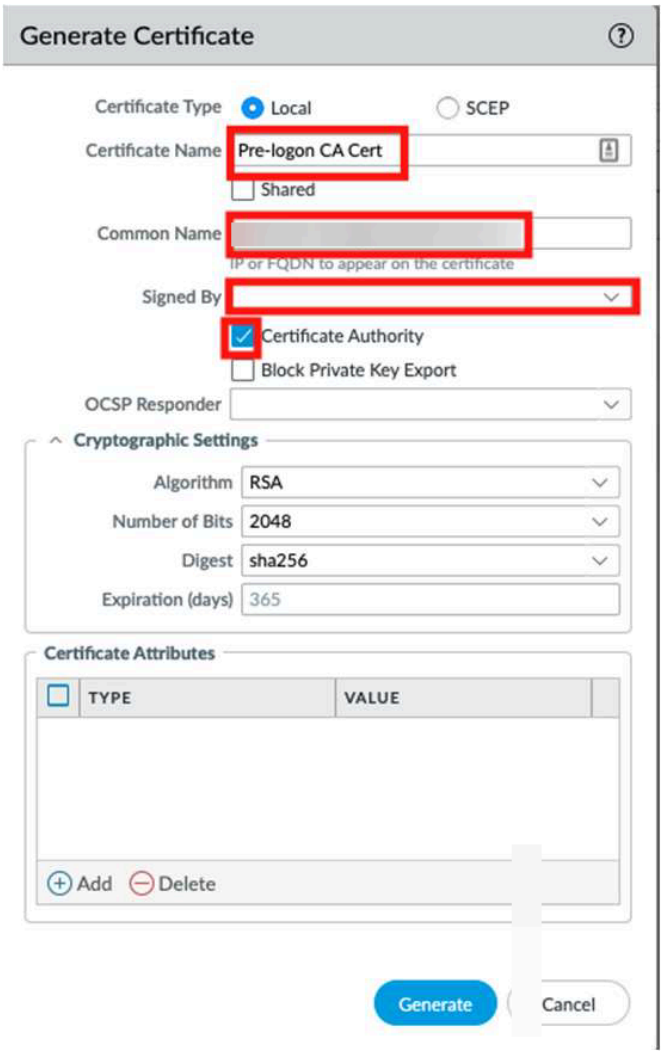
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configure una CA autofirmada y utilícela para generar un certificado de máquina en la plantilla Usuario móvil. Vaya a **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.

Asegúrese de estar en el **Mobile_User_Template** y la **Ubicación** se establece en **Compartido**.

1. Asigne un nombre al certificado; por ejemplo, **Certificado de CA previo al inicio de sesión**.
2. Introduzca un **Common Name (Nombre común)**.

   El nombre común (CN) es el nombre de dominio, como www.yourdomainname.com, que desea proteger con su certificado.
3. Deje el campo **Signed By (Firmado por)** en blanco y haga clic en la casilla de verificación **Autoridad de certificación**.
4. Debe **Generate (Generar)** el certificado para su uso en conexiones previas al inicio de sesión.

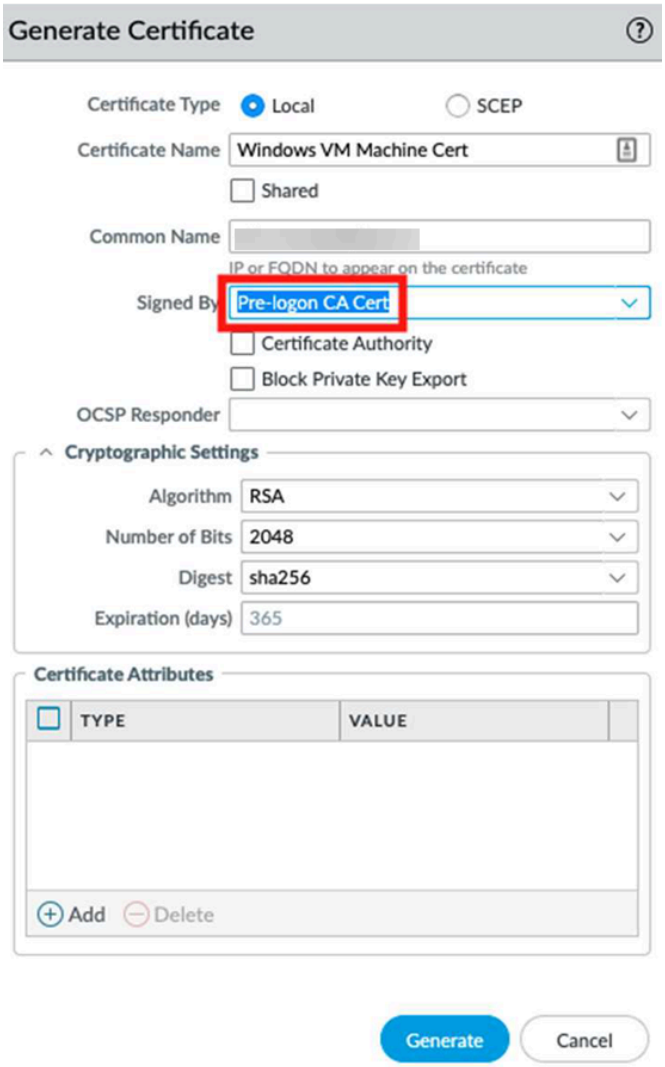


 ©2025 Palo Alto Networks, Inc.

STEP 2 | Después de configurar la CA autofirmada, genere el certificado de la máquina.

1. Introduzca un **Nombre del certificado** y un **Common Name (Nombre común)**.
2. En el menú desplegable **Firmado por**, seleccione el **Pre-logon CA Cert (Certificado de CA previo al inicio de sesión)** que creó en el paso 1.
3. **Generate (Generar)** el **Certificado de máquina virtual de Windows** que luego instale en una máquina con Windows.

   Este certificado es un elemento secundario de la CA previa al inicio de sesión.

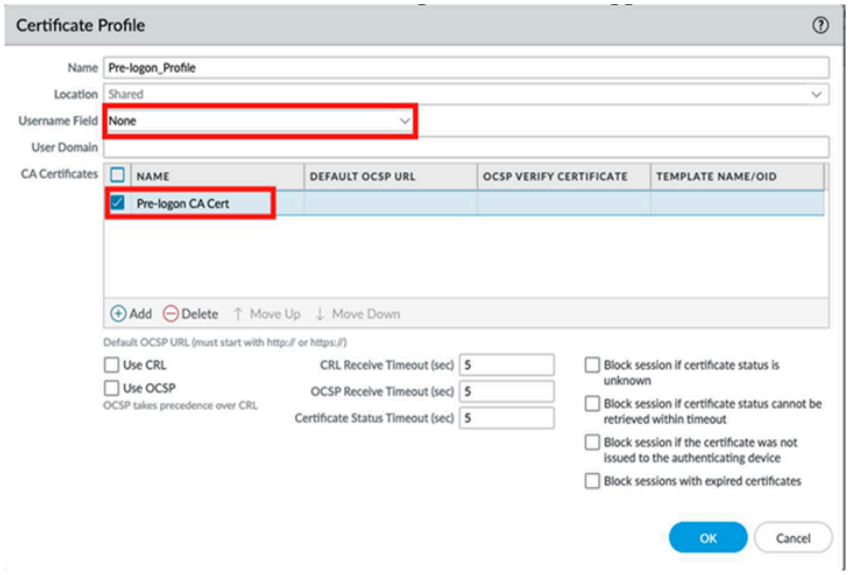


STEP 3 | Para crear un perfil de certificado que incluya el certificado de CA previo al inicio de sesión, vaya a **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)**.

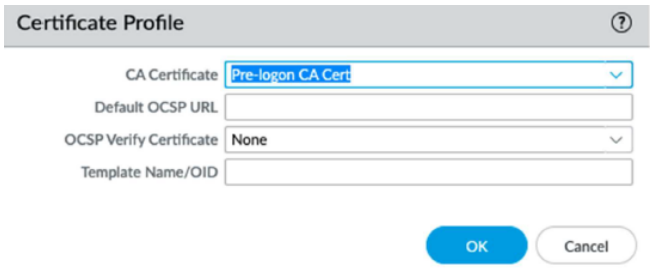
Utilice esta CA para validar el certificado de máquina presentado por el cliente GlobalProtect durante la inicialización del túnel previo al inicio de sesión.

©2025 Palo Alto Networks, Inc.

STEP 4 | Crear y asignar el perfil. Asegúrese de que el **Username Field (Campo de nombre de usuario)** es **None (Ninguno)** para evitar la asignación de certificados a un usuario.



STEP 5 | En **Certificados de CA**, seleccione **Add (Añadir)** y seleccione **Certificado de CA previo al inicio de sesión** en el menú desplegable.



STEP 6 | Seleccione **OK (Aceptar)** y, a continuación, seleccione **OK (Aceptar)** otra vez.

Configurar el portal de GlobalProtect para el Inicio de sesión previo

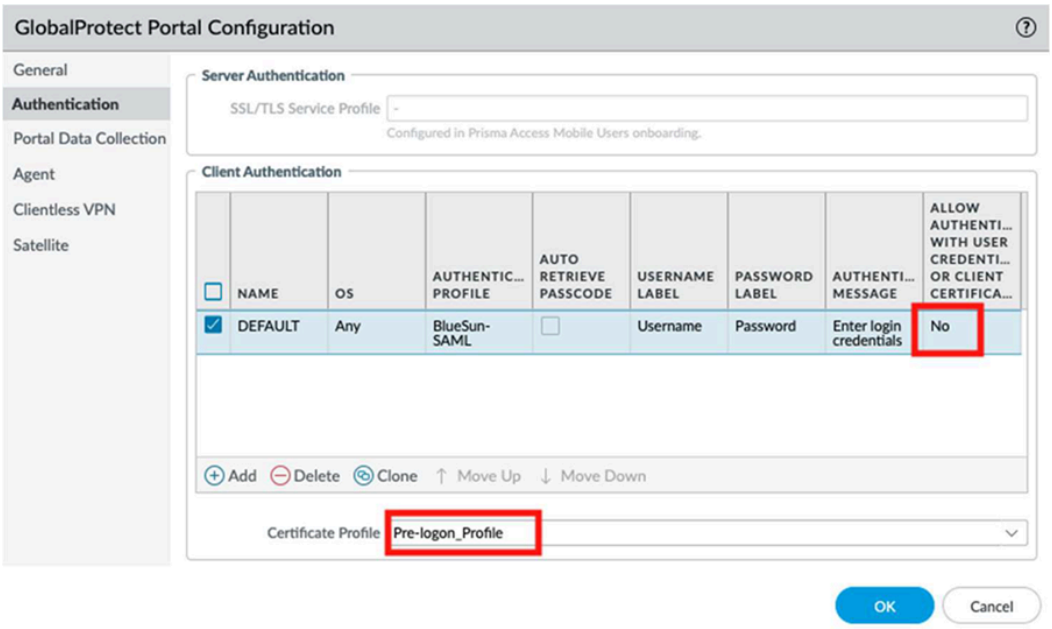
Configure el portal GlobalProtect para autenticar conexiones con un certificado de máquina.

STEP 1 | Vaya a **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **GlobalProtect_Portal** > **Authentication (Autenticación)**.

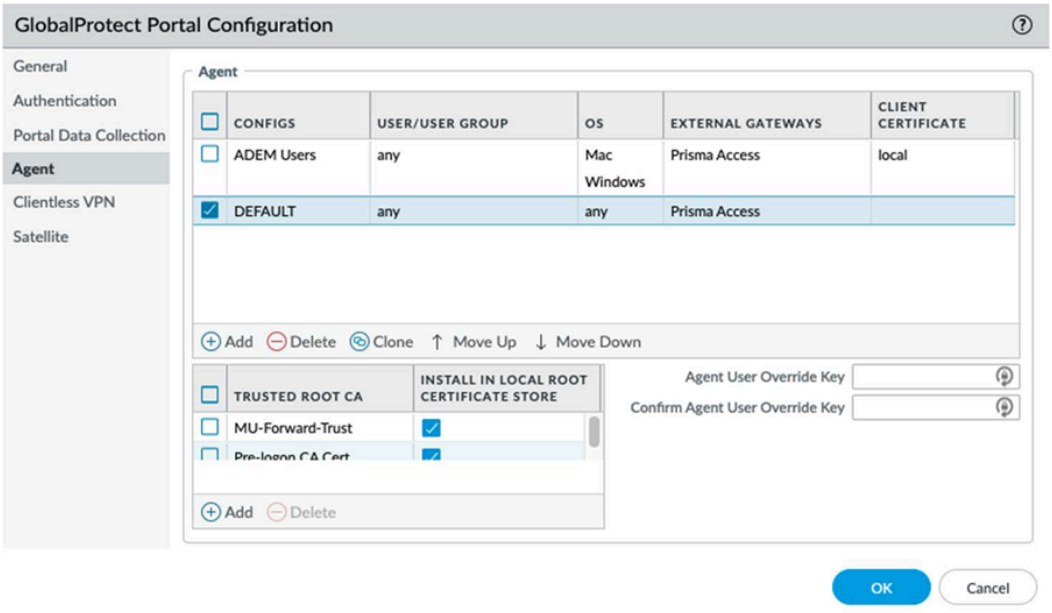
STEP 2 | En **Permitir la autenticación con credenciales de usuario O certificado de cliente**, seleccione **No** para aplicar solo la autenticación basada en certificados.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Para el **Perfil de certificado**, seleccione la opción **Pre-logon_Profile** que ha creado y haga clic en **OK (Aceptar)**.



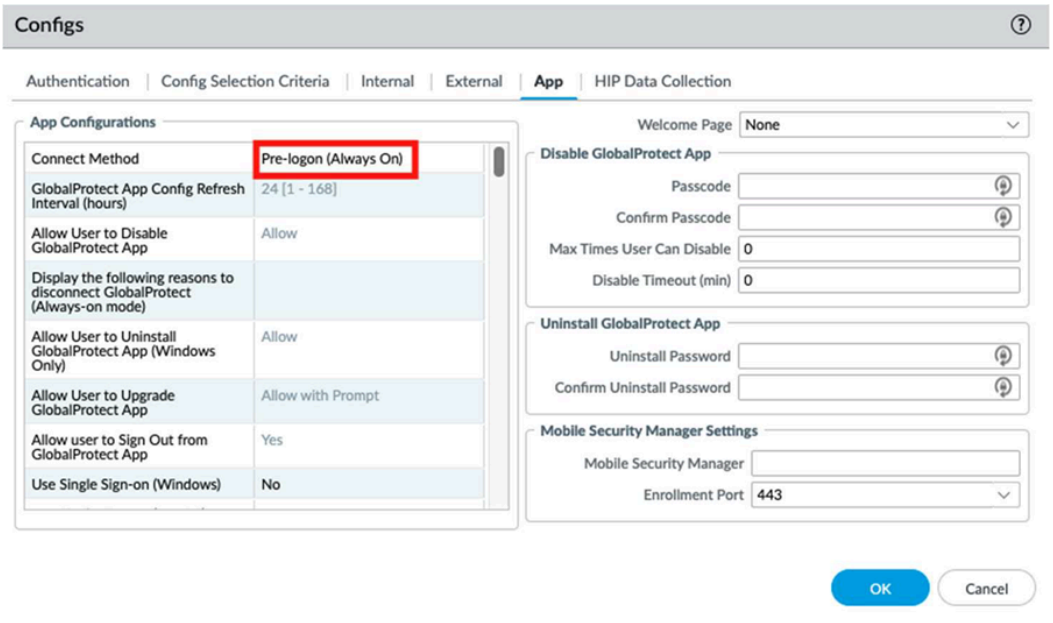
STEP 4 | Seleccione **Agent (Agente)** y abra la Configuración del agente para usuarios autenticados.



STEP 5 | Seleccione la pestaña **App (Aplicación)**.

 ©2025 Palo Alto Networks, Inc.

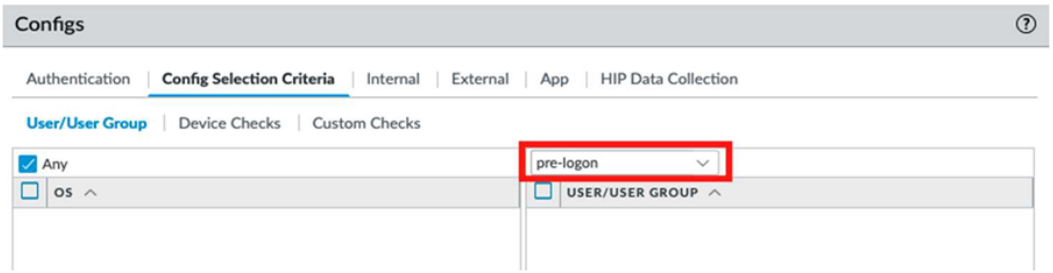
STEP 6 | Seleccione **Pre-logon (Always On) [Inicio de sesión previo (siempre activado)]** y seleccione **OK (Aceptar)** para volver al área de Agente.



STEP 7 | En el área Agente, debe **Clone (Duplicar)** la configuración predeterminada. Cambie el nombre de la configuración a **Pre-logon (Inicio de sesión previo)** para que coincida con el método de conexión para la autenticación de certificados de máquina.

STEP 8 | Seleccione la configuración del agente recién clonado.

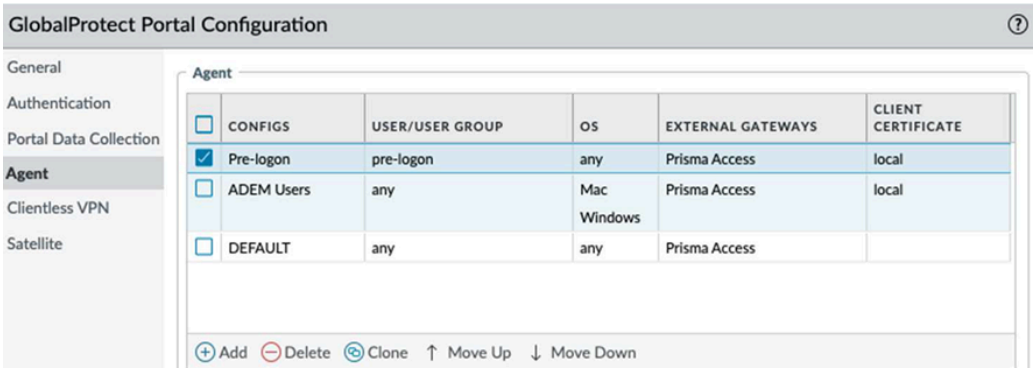
STEP 9 | Seleccione **Criterios de selección de configuración**. En la configuración **Usuario/Grupo de usuarios**, seleccione **Inicio de sesión previo** en el menú desplegable encima del cuadro de configuración **Grupo de USUARIOS/USUARIOS** y asegúrese de que la configuración esté establecida en **Cualquiera**.



STEP 10 | Configure los ajustes de la aplicación según sea necesario y seleccione **OK (Aceptar)**. Asegúrese de seleccionar un método de conexión previo al inicio de sesión para la configuración previa y la configuración actual.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | Mueva la configuración del agente previo al inicio de sesión a la parte superior de la lista de **CONFIGURACIONES** para asegurarse de que coincida primero con la condición previa al inicio de sesión.



STEP 12 | Haga clic en **ACEPTAR** para guardar la configuración de portal.

Configurar las puertas de enlace Prisma Access GlobalProtect

Configure las puerta de enlace de GlobalProtect en Prisma Access gestionado por Panorama.

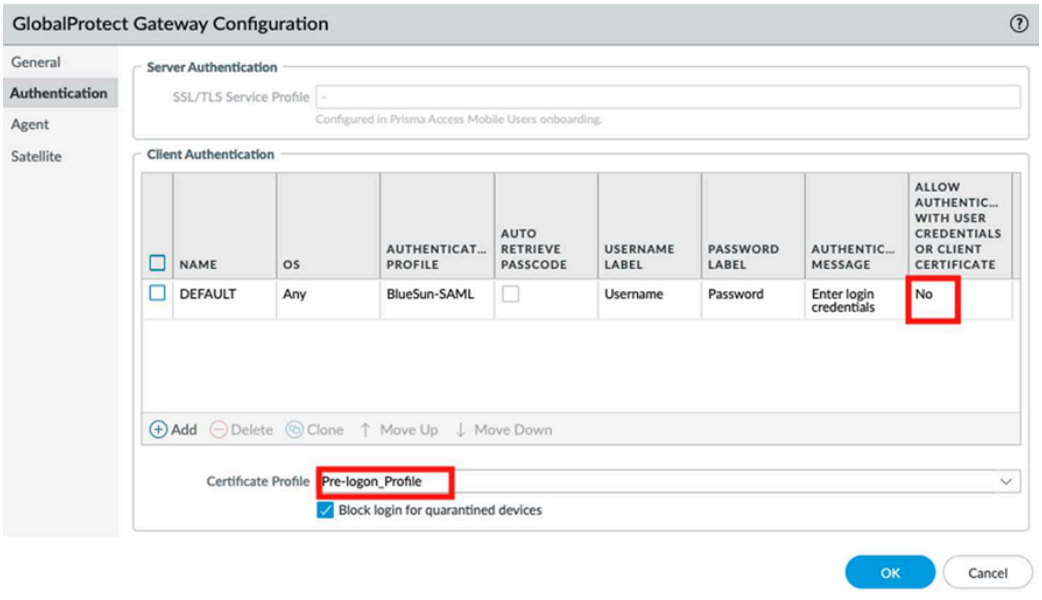
Esta configuración solo aplica la autenticación basada en certificados.

STEP 1 | Vaya a **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > **GlobalProtect_External_Gateway** > **Authentication (Autenticación)**.

STEP 2 | Seleccione el método de autenticación **Default (Predeterminado)**.

Si ya tiene configurada una autenticación de cliente (como SAML), selecciónela en lugar de **Default (Predeterminado)**.

STEP 3 | En **Allow Authentication with User Credentials or Client Certificate (Permitir la autenticación con credenciales de usuario o certificado de cliente)**, seleccione **No** y, a continuación, seleccione **OK (Aceptar)** para guardar la configuración.



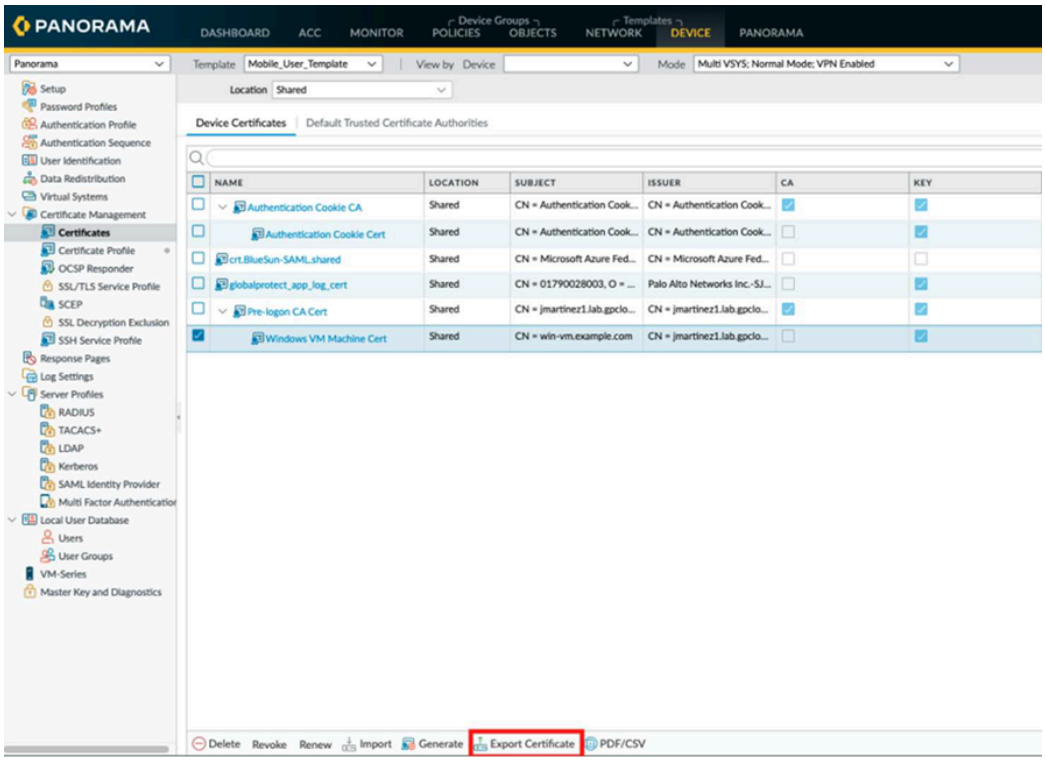
 ©2025 Palo Alto Networks, Inc.

Instalar un certificado de máquina: Windows

Instale el certificado de máquina en los endpoints de los usuarios móviles, que se utilizan para la autenticación.

STEP 1 | Vaya a **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.

STEP 2 | Asegúrese de que siga en el Mobile_User_Template. Seleccione la opción **Windows VM Machine Cert (Certificado de máquina virtual de Windows)** que creó anteriormente y seleccione **Export Certificate (Exportar certificado)** para descargarlo como un archivo PKCS12 con una frase de contraseña.

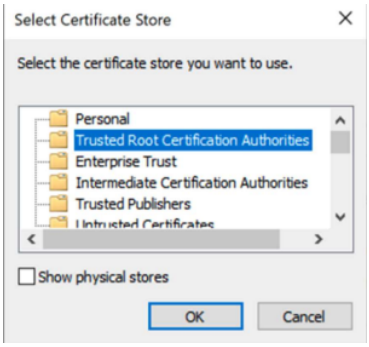


STEP 3 | Exporte el certificado de CA previo al inicio de sesión como un certificado codificado en base64.

STEP 4 | Transfiera los archivos del certificado a un equipo Windows.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Instale el certificado CA de inicio previo a la sesión raíz en el almacén **Trusted Root Certification Authorities (Autoridades de certificación raíz de confianza)** de su máquina local.



STEP 6 | Instale el certificado de la máquina previa al inicio de sesión en la ubicación de almacenamiento de la máquina local. Complete los permisos y seleccione **Next (Siguiente)** para continuar con la instalación.

STEP 7 | Valide el nombre de archivo en el certificado y seleccione **Next (Siguiente)**.

STEP 8 | Introduzca la contraseña, que es la frase de contraseña que utilizó durante la exportación del certificado desde Panorama, y seleccione **Next (Siguiente)**.

STEP 9 | En el cuadro de diálogo **Certificate Store (Almacén de certificados)**, seleccione **Place all certificates in the following store (Colocar todos los certificados en el siguiente almacén)** y seleccione **Browse (Examinar)**.

STEP 10 | Seleccione la **Personal folder (Carpeta personal)** donde desea instalar el certificado de máquina y seleccione **OK (Aceptar)**.

STEP 11 | Seleccione **Next (Siguiente)** para continuar con la instalación.

STEP 12 | Conéctese al portal GlobalProtect y elimine todas las cookies del host.

STEP 13 | (Opcional) Cierre la sesión de su máquina y vea los logs de GlobalProtect para verificar la conexión previa al inicio de sesión.

VPN sin cliente de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

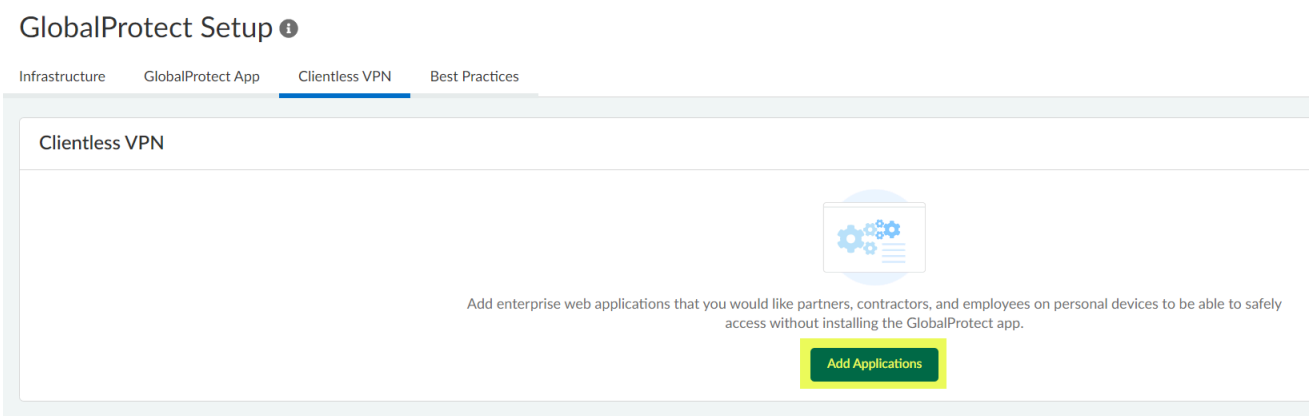
La VPN sin cliente permite el acceso remoto seguro a aplicaciones empresariales desde navegadores web con SSL habilitado. Con VPN sin clientes, los usuarios finales no necesitan instalar el software de la aplicación GlobalProtect en sus endpoints, lo que resulta útil cuando

 ©2025 Palo Alto Networks, Inc.

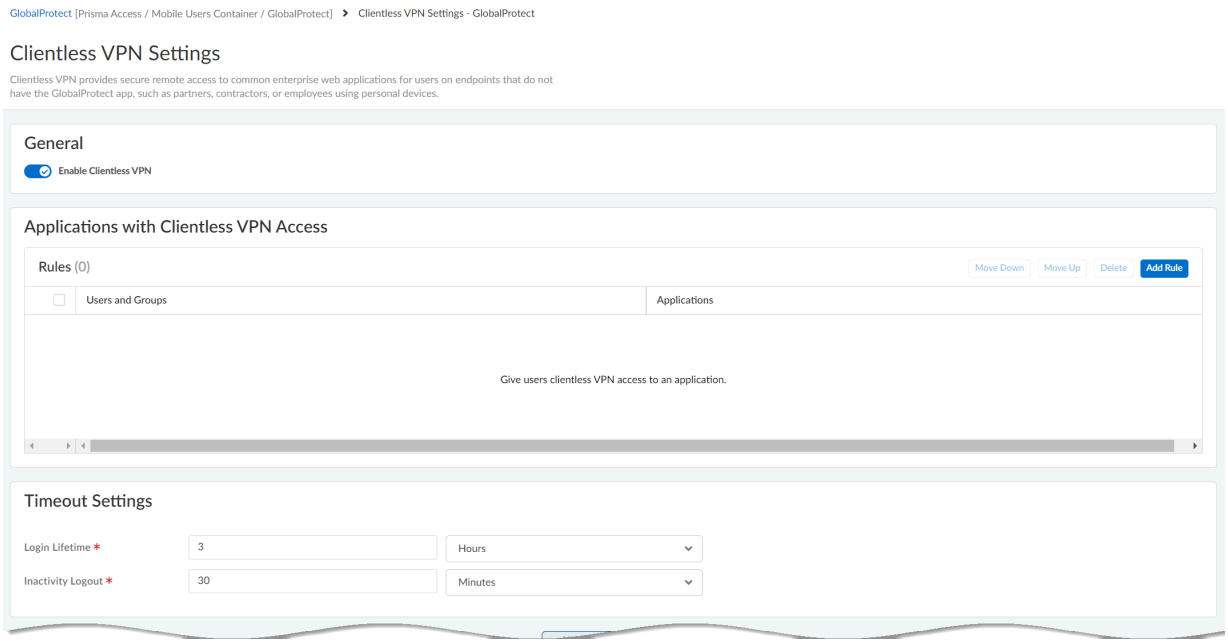
necesita habilitar el acceso de socios o contratistas a las aplicaciones y habilitar de forma segura activos no gestionados, incluidos los endpoints personales.

Utilice los siguientes pasos para configurar una VPN sin cliente para Prisma Access:

STEP 1 | Vaya a **Settings (Configuración)** > **Prisma Access Setup (Configurar Prisma Access)** > **GlobalProtect** > **GlobalProtect Setup (Configurar GlobalProtect)** > **Clientless VPN (VPN sin cliente)** y luego **Add Applications (Añadir aplicaciones)**.



STEP 2 | **Enable Clientless VPN (Habilitar VPN sin cliente)**



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Añadir reglas de VPN sin cliente

Especifique los usuarios y aplicaciones que pueden usar VPN sin cliente.

STEP 4 | Si los usuarios necesitan llegar a las aplicaciones a través de un servidor proxy, especifique un **Proxy Server (Servidor proxy)**.

Solo se admite la autenticación básica del proxy (nombre de usuario y contraseña). Puede añadir múltiples configuraciones de servidor proxy, una para cada conjunto de dominios. Algunas de las configuraciones para añadir incluyen:

- **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.
- **Enable Proxy (Habilitar proxy)**: 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 and Password (Usuario y contraseña)**: especifica el usuario) y contraseña necesarios para iniciar sesión en el servidor proxy. Especifica la contraseña nuevamente para verificación.

STEP 5 | Modifique la **Crypto Settings (Configuración de cifrado)** predeterminada para especificar los algoritmos de autenticación y cifrado para las sesiones SSL entre Prisma Access y las aplicaciones que utilizan VPN sin cliente.

STEP 6 | Añadir dominios a la **Rewrite Exclude Domain List (Reescribir lista de dominios excluidos)**.

La VPN sin cliente actúa como un proxy inverso y modifica las páginas web devueltas por las aplicaciones web publicadas. Este reescribe todas las URL y presenta una página reescrita a los usuarios remotos de modo que cuando acceden a cualquiera de esas URL, las solicitudes pasan por el portal 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 de cotización bursátil de yahoo.finance.com). Puede excluir estas páginas. Los dominios que añada a la **Rewrite Exclude Domain List (Reescribir lista de dominios excluidos)** se excluyen de las reglas de reescritura y no se pueden reescribir. Las rutas no son compatibles con los nombres de dominio. El carácter comodín (*) para los nombres de dominio sólo puede aparecer al principio del nombre (por ejemplo, * .etrade.com).

Supervisar Usuarios móviles de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

Prisma Access (Managed by Strata Cloud Manager)

Los usuarios de Prisma Access (Managed by Strata Cloud Manager) pueden usar el**Monitor (Supervisar)** > **Users (Usuarios)**. Seleccione **GlobalProtect** o método conectado de **Explicit Proxy (Proxy explícito)**. La página **Mobile Users (Usuarios Móviles)** es específica para el método de conexión que está utilizando.

Prisma Access (Managed by Panorama)

Hay varias ubicaciones en Panorama donde puede ver la lista de usuarios conectados. Puede ver usuarios únicos, la ubicación en la que los usuarios han iniciado sesión y tablas que proporcionan información adicional. También es importante entender cómo Prisma Access cuenta el número de usuarios en cada ubicación en un despliegue de Usuarios móviles: GlobalProtect.

Puede obtener una vista detallada de los usuarios de varias ubicaciones:

- Para ver una visión general de los usuarios y abrir una tabla que te permita ver y cerrar sesión en los usuarios conectados, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)**.
- Para ver una vista gráfica de los usuarios en una vista de mapa, y para ver usuarios por región y ubicación, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Service Stats (Estadísticas de servicio)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**.
- También puede aprender más sobre cómo Prisma Access cuenta los usuarios móviles.

Ver usuarios móviles de GlobalProtect desde la pestaña de estado

Para ver el número total de usuarios únicos que están conectados actualmente en todas las ubicaciones, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**



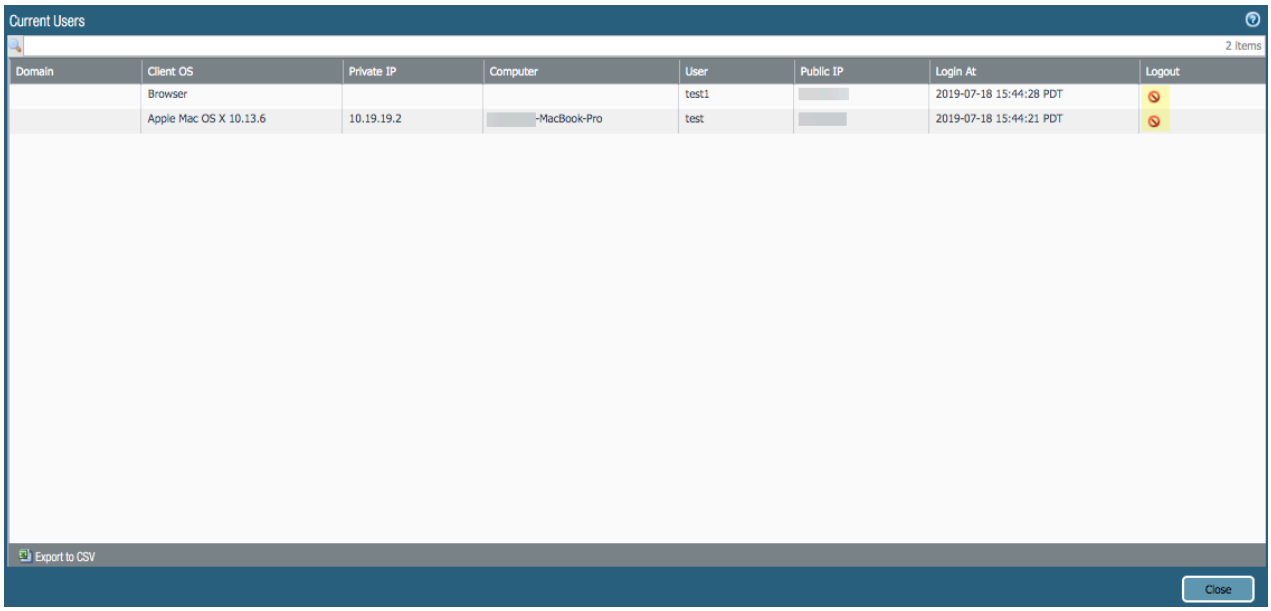
Para ver más detalles sobre los usuarios que están actualmente conectados, haga clic en el número hipervinculado junto a **Current Users (Usuarios actuales)** para mostrar la tabla de **Current Users (Usuarios actuales)**.

 ©2025 Palo Alto Networks, Inc.

El número total de usuarios que se muestra en la página Estado, y el número que se muestra en la tabla emergente, puede ser diferente; el número que se muestra en la tabla *puede ser mayor.*

Puede cerrar sesión a los usuarios activos desde la tabla de **Current Users (Usuarios actuales)**; para hacerlo, seleccione al usuario y haga clic en **Logout (Cerrar sesión)**. Tenga en cuenta que es posible que tenga que cerrar y luego volver a abrir la pantalla para que Prisma Access elimine al usuario desconectado de la página de **Current Users (Usuarios actuales)**.

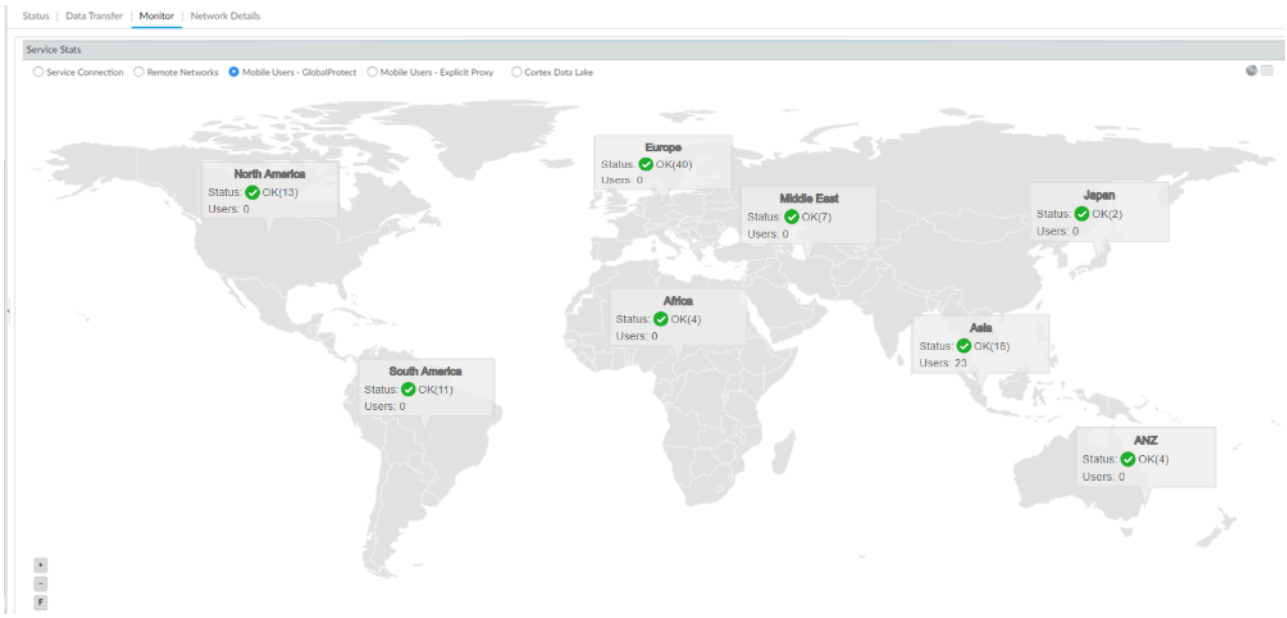
La siguiente pantalla muestra a los usuarios que iniciaron sesión con la aplicación GlobalProtect y con VPN sin cliente. La pantalla muestra el nombre de usuario, la IP pública y la hora del último inicio de sesión del usuario. Si el usuario ha iniciado sesión con la aplicación GlobalProtect, también muestra su sistema operativo cliente, dirección IP privada y nombre del ordenador.



Ver usuarios móviles de GlobalProtect desde la pestaña de supervisión

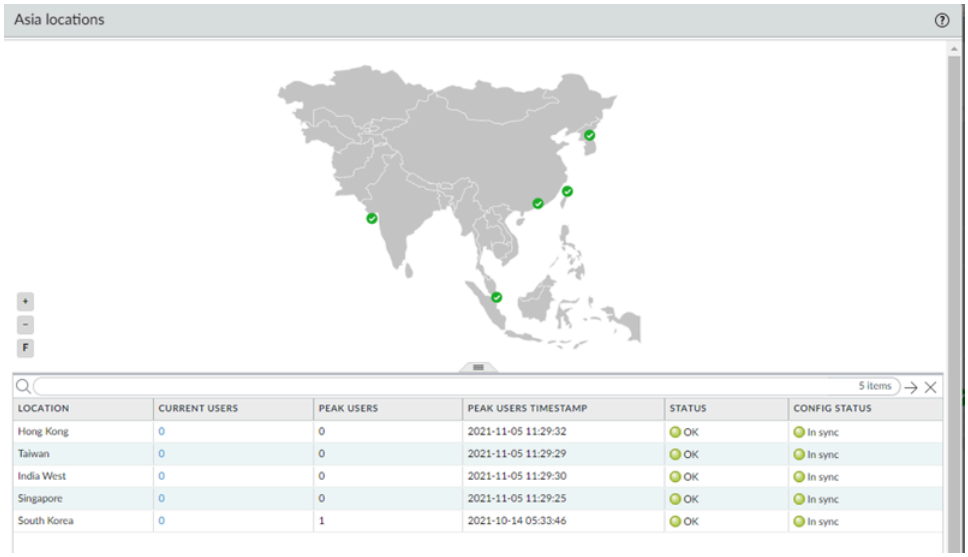
Para ver el número de usuarios únicos que han iniciado sesión por región, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Service Stats (Estadísticas de servicios)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**.

 ©2025 Palo Alto Networks, Inc.



Para ver detalles sobre las ubicaciones en una región, haz clic en la región.

El número de usuarios que se muestra en la página de vista del mapa global y el número que se muestra en la tabla por región pueden ser diferentes; el número que se muestra en la tabla puede ser mayor.



Cómo Prisma Access cuenta los usuarios móviles de GlobalProtect

El número total de usuarios que se muestra en las áreas de estado puede ser diferente al número que se muestra en las tablas asociadas. La siguiente sección describe las diferencias.

- Pestaña **Status (Estado)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)**]: el número de usuarios que se muestra en la página principal, en el área **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**, puede ser diferente al número que se muestra en la tabla cuando hace clic en el hipervínculo de **Current Users (Usuarios actuales)**. El número que se muestra en el área de **Mobile Users—GlobalProtect (Usuarios Móviles: GlobalProtect)** cuenta el número de usuarios únicos; la lista de usuarios en la tabla de

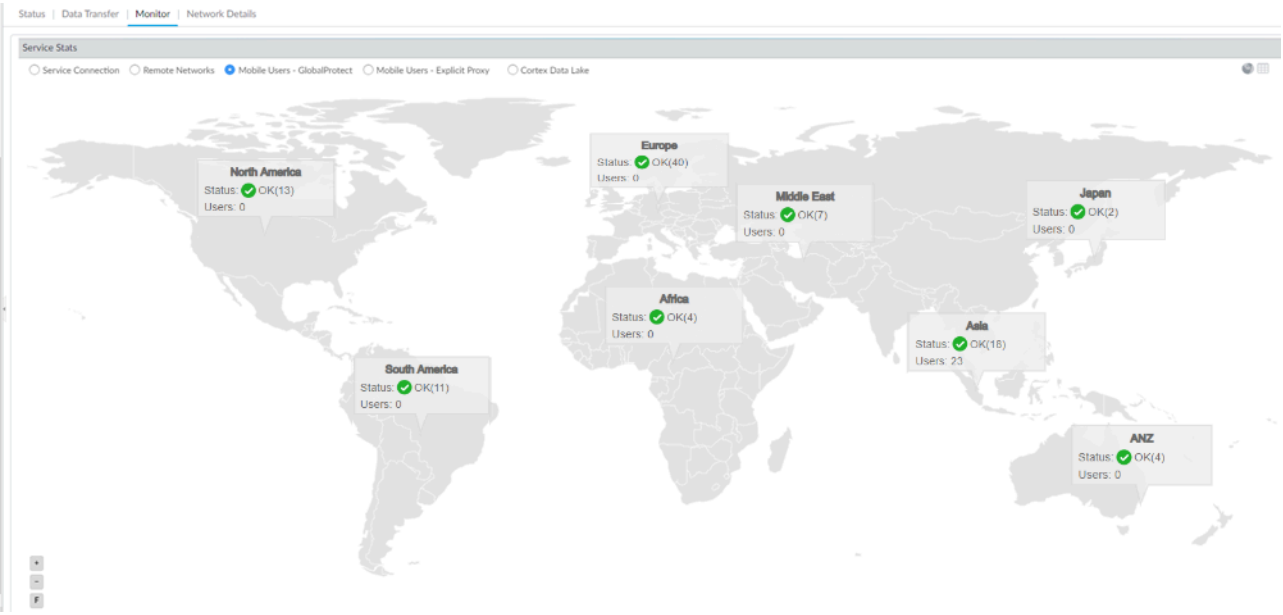
 ©2025 Palo Alto Networks, Inc.

Current Users (Usuarios actuales) cuenta todos los usuarios por inicio de sesión o conexión. Si un solo usuario ha iniciado sesión en más de una puerta de enlace o está conectado con varios dispositivos, es posible que el número de la tabla sea mayor.

Por ejemplo, un usuario **user1** ha iniciado sesión en dos puertas de enlace en la ubicación del **Reino Unido**; esta condición podría haber ocurrido porque Prisma Access añadió automáticamente puertas de enlace cuando un gran número de usuarios iniciaron sesión en la misma ubicación. En este caso, Prisma Access cuenta a **user1 (usuario1)** una vez en el área de **Mobile Users—GlobalProtect (Usuarios Móviles: GlobalProtect)**, pero dos veces en la tabla de **Current Users (Usuarios actuales)**.

- Pestaña **Monitor (Supervisar)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Service Stats (Estadísticas de servicio)** > **Mobile Users: GlobalProtect (Usuarios móviles: GlobalProtect)**]: el número de **Users (Usuarios)** que ve en el mapa global puede ser diferente al número que se muestra en la tabla cuando selecciona una región. Un usuario que ha iniciado sesión en más de una puerta de enlace o está conectado con múltiples dispositivos puede aparecer varias veces en la tabla.

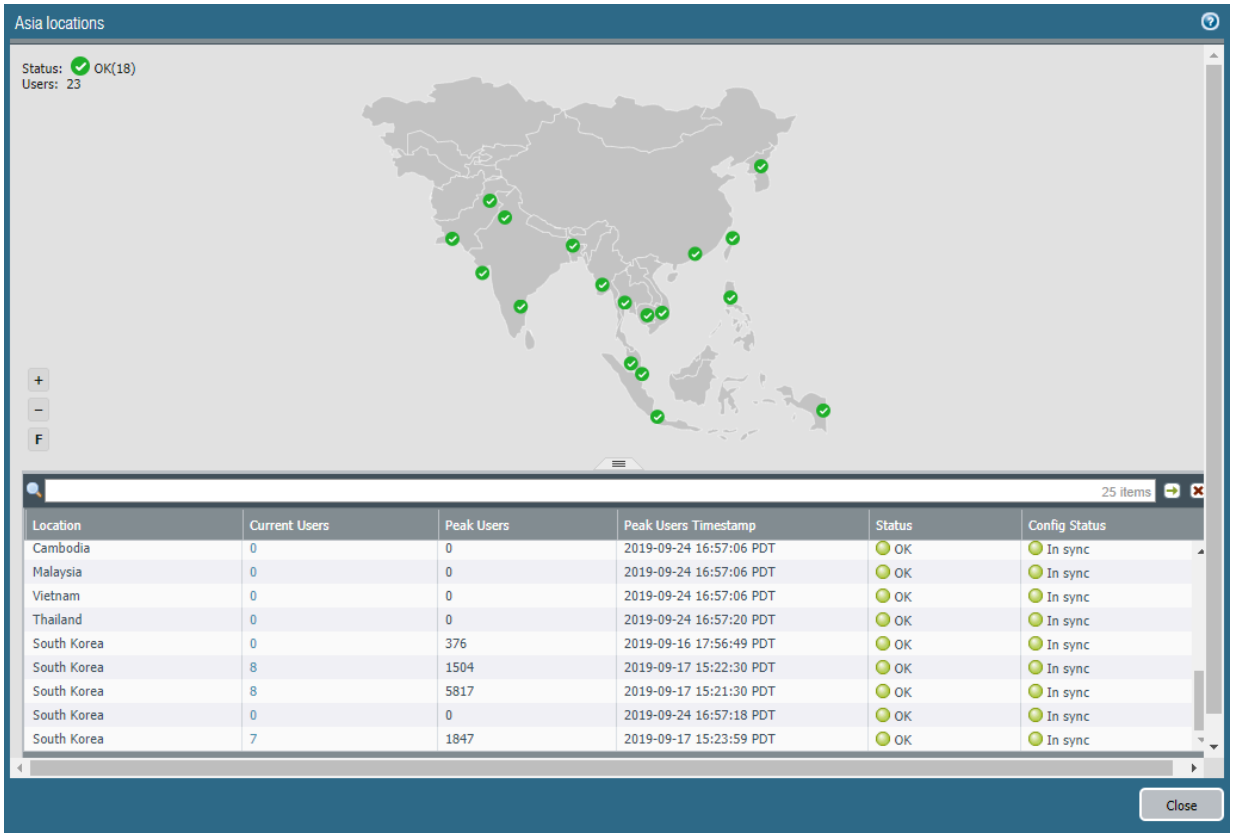
  Las siguientes capturas de pantalla proporcionan un ejemplo. Hay 23 usuarios únicos conectados en la región de **Asia**, como se muestra en el mapa global.



Si selecciona la región de **Asia**, Prisma Access muestra el número de usuarios únicos (23) en la parte superior izquierda de la página de la región. Sin embargo, dos usuarios están conectados a través de varios dispositivos en la ubicación de **Corea del Sur** (por ejemplo, un teléfono

 ©2025 Palo Alto Networks, Inc.

inteligente y un ordenador). Debido a que los usuarios tienen dos conexiones separadas, Prisma Access los cuenta dos veces en la tabla, dando un total de 25 en la tabla.



 ©2025 Palo Alto Networks, Inc.

Grupos de direcciones IP para una implementación de usuarios móviles de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Asegúrese de que ha especificado un grupo de direcciones IP que permita suficiente cobertura para los usuarios móviles de su organización. Es importante recordar que cada usuario único puede utilizar varios dispositivos para conectarse a Prisma Access al mismo tiempo, cada dispositivo conectado requiere una dirección IP única del grupo. Las direcciones de este grupo no deben superponerse con otros grupos de direcciones que utilice internamente ni con la subred IP que asigne cuando Habilita la infraestructura de servicio.

Se recomienda que el número de direcciones IP en el grupo sea 2 veces el número de dispositivos de usuario móvil que se conectarán a Prisma Access. Si su organización tiene una política de traer su propio dispositivo (BYOD), o si un solo usuario tiene varias cuentas de usuario, asegúrese de tener en cuenta esos dispositivos y cuentas adicionales al asignar sus grupos de IP. Si el espacio de su grupo es limitado, puede especificar un grupo de direcciones más pequeño; sin embargo, si su grupo de direcciones IP alcanza su límite, los dispositivos de usuarios móviles adicionales no podrán conectarse.

La interfaz de usuario valida que introduzca subredes IP válidas (por ejemplo, si introduce un grupo con una subred menor a /23, le solicitará que la cambie). Sin embargo, no verifica que haya asignado suficientes direcciones IP para su implementación.

Esta validación no está disponible si configura ubicaciones mediante la CLI. Si implementa todas las ubicaciones mediante la CLI, le recomendamos que añada una dirección /18 en el grupo mundial para usuarios móviles.

Prisma Access comprueba su configuración para asegurarse de que haya especificado el siguiente grupo mínimo de direcciones IP:

- Se requiere un mínimo de /23 (512 direcciones IP) para un grupo de direcciones mundial o regional.
- Si una ubicación existente se convierte en una ubicación de cómputo, esa ubicación requiere una subred mínima /23 después de la conversión.
- Si no incorpora ninguna puerta de enlace de Prisma Access en una región, no se requiere un grupo de direcciones IP para dicha región. Por ejemplo, si especifica puertas de enlace en las ubicaciones EE. UU. Este, EE. UU. Noroeste y EE. UU. Noreste, solo deberá especificar un grupo de direcciones IP para las regiones de América del Norte y América del Sur. Por el contrario, si habilita las ubicaciones de usuarios móviles en Europa sin especificar un grupo de direcciones mundial o un grupo de direcciones IP en África, Europa y Medio Oriente, su implementación fallará.
- Los usuarios móviles de GlobalProtect consumen las direcciones IP en el grupo de ubicaciones primero, luego las direcciones IP específicas del teatro y luego las direcciones IP mundiales.

 ©2025 Palo Alto Networks, Inc.

Por ejemplo, si especifica un grupo para un grupo de ubicaciones y Worldwide (mundial), y luego agota las direcciones IP disponibles en el grupo de ubicaciones, Prisma Access tomará las direcciones IP del grupo **Worldwide (Mundial)** para usarlas en ese grupo de ubicaciones.

Si especifica más de un bloque de grupos de direcciones IP, Prisma Access utiliza los grupos en el orden en que los ingresó durante la configuración del usuario móvil.

Asignación de direcciones IP estáticas para usuarios móviles: implementaciones de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access versión 5.2.1 • La versión 11.2.4 del plano de datos de PAN-OS incluye compatibilidad con Activity Insights, grupos de usuarios y grupos de ubicación • GlobalProtect versión 6.1.4 *Esta es una versión de disponibilidad limitada. Para activar esta funcionalidad, póngase en contacto con su representante de cuenta de Palo Alto Networks después de activar el inquilino.*

Algunas redes heredadas utilizan autorización basada en direcciones IP para restringir el acceso de los usuarios a recursos internos o externos. Una implementación de Usuarios móviles: GlobalProtect de Prisma Access asigna a los usuarios una dirección IP del grupo de direcciones IP de usuarios móviles que usted asigna durante la incorporación, y esta asignación de usuario a dirección IP puede cambiar en inicios de sesión posteriores. Para conservar la asignación de direcciones de usuario a IP, Prisma Access permite asignar direcciones IP estáticas a los usuarios.

Esta funcionalidad está disponible solo para nuevas implementaciones de Prisma Access.

Para crear un perfil de grupo de IP, utilice uno o más de estos criterios:

- **Un teatro**: asigne direcciones IP según el teatro en el que se encuentren sus usuarios. Por ejemplo, puede crear una subred /30 para un teatro específico. Estas direcciones IP son estáticas para ese teatro. Puede aplicar acceso a recursos según el teatro creando reglas de política de seguridad utilizando las direcciones IP que especifique para ese teatro.
- **Un usuario:**asigne direcciones IP en función de un ID de usuario configurando una dirección /30 o /32 en el grupo de direcciones IP de usuarios móviles y utilizando criterios de coincidencia para asociar ese usuario con una dirección IP. De esta manera, asigna una dirección IP estática que Prisma Access conserva para un usuario específico, lo que le permite

 ©2025 Palo Alto Networks, Inc.

mantener sus reglas de política de seguridad basadas en direcciones IP actuales para controlar el acceso de un usuario a los recursos.

- **Un grupo de usuarios**: asignar direcciones IP según el grupo de usuarios. El usuario obtendrá la dirección IP de la subred del grupo de IP definido si es parte del grupo de usuarios configurado.
- **Un grupo de ubicaciones** : asigna direcciones IP según el grupo de ubicaciones definido en el perfil del grupo de IP.

Utilice las siguientes pautas al asignar direcciones IP estáticas:

- Si especifica varios grupos de IP, Prisma Access evalúa las reglas de arriba hacia abajo y asigna direcciones IP según la primera coincidencia en la lista de reglas.
- Integre su implementación de Prisma Access con Cloud Identity Engine si desea utilizar el User-ID o el User-Group como criterios para hacer coincidir los grupos de IP.
- Las siguientes asignaciones máximas son compatibles por inquilino:
  - 20.000 usuarios
  - 5.000 grupos de usuarios con 50.000 usuarios por grupo de usuarios
  - 10.000 perfiles de grupos de direcciones IP
  - 10.000 grupos de direcciones IP
- Introduzca una longitud de prefijo entre /23 y /32.
- Para cada perfil de **Client IP Pool (Grupo de direcciones IP de cliente)** de usuario móvil que cree:
  - Se admiten hasta 10 prefijos IP.
  - Se admiten hasta 256 usuarios.
- El direccionamiento IP estático utiliza un **período de arrendamiento** y un **período de gracia** para especificar cuánto tiempo Prisma Access mantiene una asociación de usuario a dirección IP.
  - El **Lease Period (Período de concesión)** es el tiempo durante el cual la asignación de dirección de usuario a IP es válida después de su asignación.

    El período de concesión predeterminado es de 86400 segundos (24 horas).

    El período mínimo de concesión es de 3600 segundos (1 hora).

    El período máximo de arrendamiento es de 7776000 segundos (90 días).
  - El **Grace Period (Período de gracia)** es la cantidad de tiempo que, después de que expira un período de arrendamiento, Prisma Access conserva esa asignación de dirección de usuario a IP sin asignarla a otro usuario.

    El período de gracia predeterminado es de 14400 segundos (4 horas).

    El período de gracia mínimo es de 60 segundos.

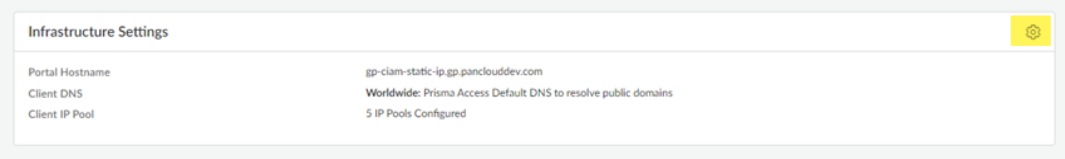
    El período de gracia máximo es de 7776000 segundos (90 días).

Configure la asignación de dirección IP estática

Para configurar una asignación de dirección IP estática en una implementación, complete estos pasos.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** y haga clic en el engranaje para resaltar la **Infrastructure Settings (Configuración de infraestructura)**.



STEP 2 | En el área Grupo de IP del cliente, deberá **Add IP Pool (Añadir grupo de IP)** para las direcciones IP estáticas.

STEP 3 | Asignar una dirección IP estática a un teatro, grupo de ubicación o usuario de Prisma Access.

1. Asigne un **Name (Nombre)**único al grupo de direcciones IP.
2. Deberá **Select (Seleccionar)** uno o más de los **Theatres (Teatros)** para permitir que el grupo se use en esos teatros, o seleccione **Any (Cualquiera)** para permitir que el grupo se use en todos los teatros.
3. Deberá **Select (Seleccionar)** uno o más de los **Prisma Access Location Groups (Grupos de ubicaciones de Prisma Access)** para permitir que el grupo se use en ese grupo de

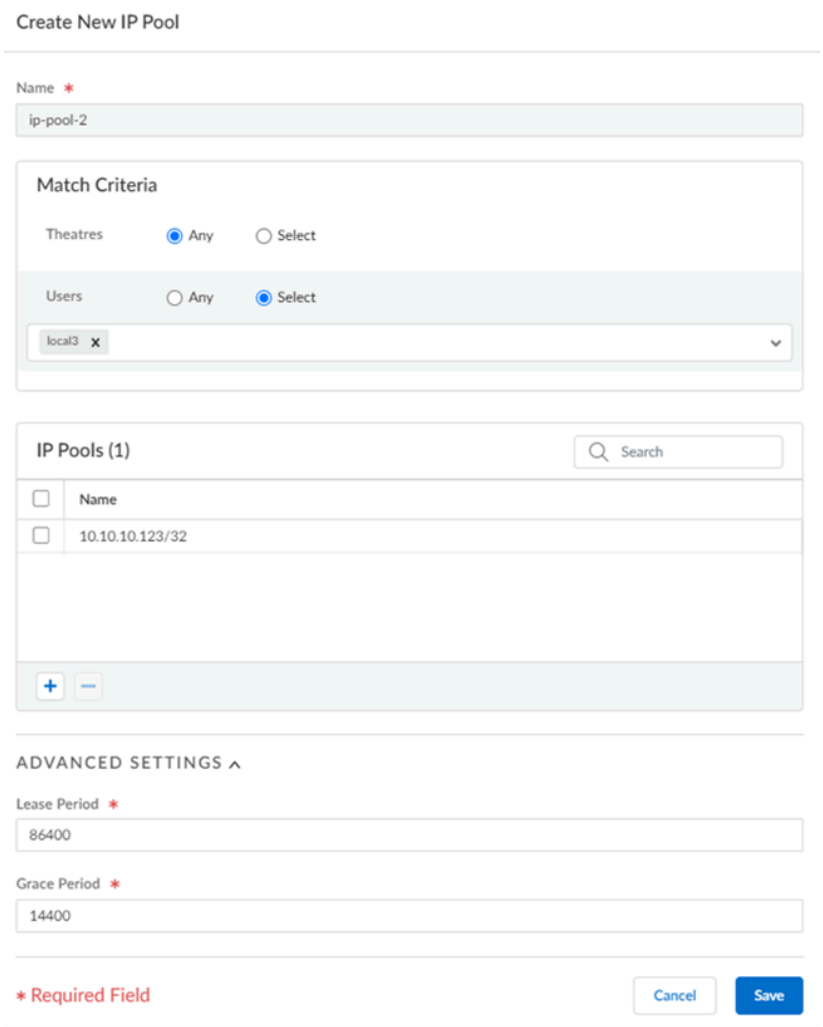
 ©2025 Palo Alto Networks, Inc.

ubicaciones, o seleccione **Any (Cualquiera)** para permitir que el grupo se use en todos los grupos de ubicaciones.

4. **Select (Seleccionar)** un usuario o grupo de usuarios, o seleccione **Any (Cualquier)** para permitir que el grupo sea utilizado por cualquier usuario o grupo de usuarios.
   - Para asignar uno o más usuarios a un grupo de direcciones IP, seleccione el usuario en la pestaña **Users (Usuarios)** .
   - Para asignar uno o más grupos de usuarios a un grupo de direcciones IP, seleccione el usuario en la pestaña **User Groups (Grupos de usuarios)**.
5. En el área **IP Pools (Grupos de IP)**, introduzca un grupo de direcciones IP.

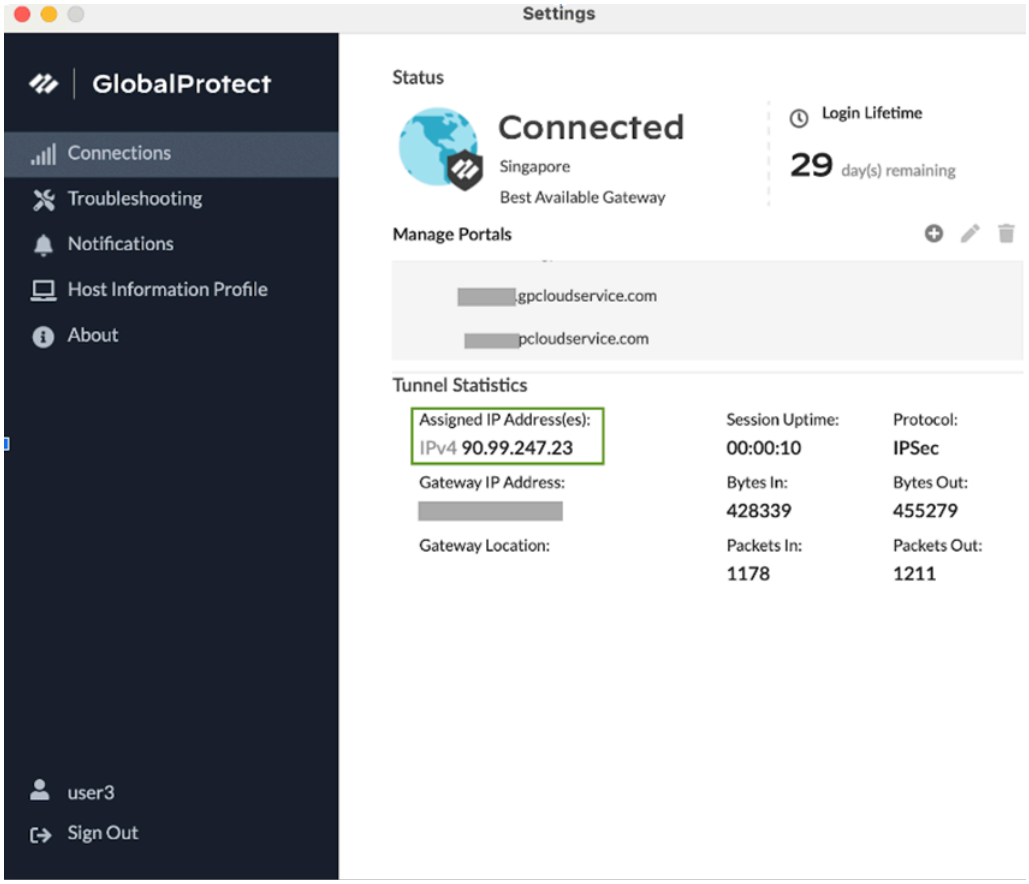
   Para limitar a un usuario a una sola dirección IP, especifique una dirección IP /30 o /32; Prisma Access asigna el usuario a esa dirección. Dado que un /32 proporcionaría solo una dirección IP, recomendamos una subred mínima de /30 y restringir al usuario a esa subred.
6. (Opcional) Introduzca un **Lease Period (Período de arrendamiento)** y un **Grace Period (Período de gracia)** para la asignación de dirección de usuario a IP.
7. Haga clic en **Save (Guardar)** para guardar sus cambios.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Verifique sus cambios yendo a **GlobalProtect** > **Settings (Configuración)** en la máquina del cliente, visualizando las **Tunnel Statistics (Estadísticas del túnel)** y verificando las **Assigned IP Address(es) [Direcciones IP asignadas]**.



Cómo selecciona la aplicación GlobalProtect Ubicaciones de Prisma Access para usuarios móviles

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Cuando un usuario móvil se conecta a una ubicación de Prisma Access, la aplicación utiliza el siguiente proceso de selección para determinar a qué ubicación se conecta.

Habilite las ubicaciones de los usuarios móviles donde desea que Prisma Access esté presente durante la incorporación de usuarios móviles. Si no selecciona la ubicación durante la incorporación, Prisma Access no lo utiliza en su implementación.

- Si el usuario móvil se conecta en un país que tiene una ubicación Prisma Access, el usuario se conecta a la ubicación en ese país.

 ©2025 Palo Alto Networks, Inc.

- Si el usuario móvil no puede conectarse a una ubicación dentro del país por cualquier motivo, Prisma Access selecciona una de las siguientes ubicaciones de usuario móvil para conectar al usuario según la región.
  - **Asia, Australia y Japón**: Hong Kong, Japón central o Japón sur
  - **África, Europa y Oriente Medio**: Países Bajos Central
  - **América del Norte y América del Sur**: Noroeste de EE.UU.

  Palo Alto Networks recomienda que habilite al menos una de estas ubicaciones en sus respectivas regiones durante la incorporación de usuarios móviles para proporcionar redundancia. Si tiene usuarios móviles que se conectan a Prisma Access de un país que no tiene una ubicación de Prisma Access, debe habilitar al menos una de las ubicaciones de respaldo en la lista anterior.

  Las ubicaciones de Hong Kong, Japón Central, Japón Sur, Países Bajos Central y EE. UU. Noroeste pueden aceptar conexiones de clientes desde cualquier lugar y se conocen como *ubicaciones de respaldo global*. Además de estas ubicaciones, puede habilitar una o más de las siguientes ubicaciones que también actúan como ubicaciones de respaldo globales:
  - Baréin
  - Francia Norte
  - Irlanda
  - Sudáfrica Oeste
  - Corea del Sur
- Palo Alto Networks recomienda que habilite ubicaciones en más de una ubicación de cómputo para fines de redundancia.
- Si utiliza puertas de enlace locales con ubicaciones de Prisma Access, puede especificar prioridades en Prisma Access para permitir que los usuarios móviles se conecten a una puerta de enlace GlobalProtect local específica o a una ubicación de Prisma Access. Consulte Gestionar prioridades para Prisma Access y puertas de enlace locales para obtener detalles.
- Cuando los usuarios móviles se conectan, la aplicación GlobalProtect no utiliza las siguiente ubicaciones de Prisma Access en el proceso de selección automática de puerta de enlace, incluso si seleccionó las ubicaciones de Prisma Access en el complemento durante la incorporación. Sin embargo, los usuarios móviles aún pueden seleccionar manualmente una de estas ubicaciones y configurarla como ubicación preferida (puerta de enlace) siempre que les permita seleccionar manualmente esas ubicaciones durante la incorporación del usuario móvil:
  - Australia: Australia Este
  - Brasil: Brasil Este y Brasil Central
  - Francia: Francia Sur
  - Alemania: Alemania Norte y Alemania Sur
  - India: India del Sur
  - México: México Oeste
  - Países Bajos: Países Bajos del Sur
  - Pakistán: Pakistán occidental
  - Rusia: Noroeste de Rusia

 ©2025 Palo Alto Networks, Inc.

- España: España Este

*Es posible que tenga que cambiar su **Connect Method (Método de conexión)** a **On-Demand (Bajo demanda)** para que el usuario móvil se conecte manualmente a una puerta de enlace.*

Lista de permitidos de usuarios móviles de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Minimum Required Prisma Access Version: 3.0 Preferido

Conozca cómo habilitar las listas de direcciones IP permitidas de salida para los usuarios móviles existentes.

Para permitirle añadir las direcciones IP públicas (salida) para su implementación de GlobalProtect: usuario móvil a cualquier lista de permisos de aplicación SaaS que utilice dentro de su organización, Prisma Access proporciona las direcciones IP y le permite verificar que las ha añadido a su lista de permisos antes de usarlas en su entorno. Si habilita las listas de direcciones IP permitidas de salida para implementaciones de Prisma Access, Prisma Access migra todas las direcciones IP de salida ya asignadas para sus ubicaciones a las listas de direcciones IP permitidas de salida. Para las nuevas implementaciones de Prisma, habilite la lista de permisos IP de salida mientras se incorporan los usuarios móviles de Global Protect.

Una vez que haya añadido las direcciones IP de salida a las listas de permisos de su organización, regrese a la interfaz de usuario de Prisma Access, confirme que las direcciones IP de salida de GlobalProtect figuran en la lista de permisos y seleccione **Push (Enviar)** para enviar los cambios. Prisma Access luego libera estas direcciones IP de salida y las añade a su implementación. Si Prisma Access añade más direcciones IP después de la configuración inicial como resultado de un evento de escalado automático, confirme que las nuevas direcciones IP de salida se añadieron antes de que Prisma Access las añada a su implementación.

Una vez habilitada, la tabla Listas de direcciones IP permitidas de salida proporciona información sobre las direcciones IP que están confirmadas o aún por confirmar, así como su estado de aprovisionamiento.

- Strata Cloud Manager
- Panorama

Lista de permitidos de usuarios móviles de GlobalProtect (Strata Cloud Manager)

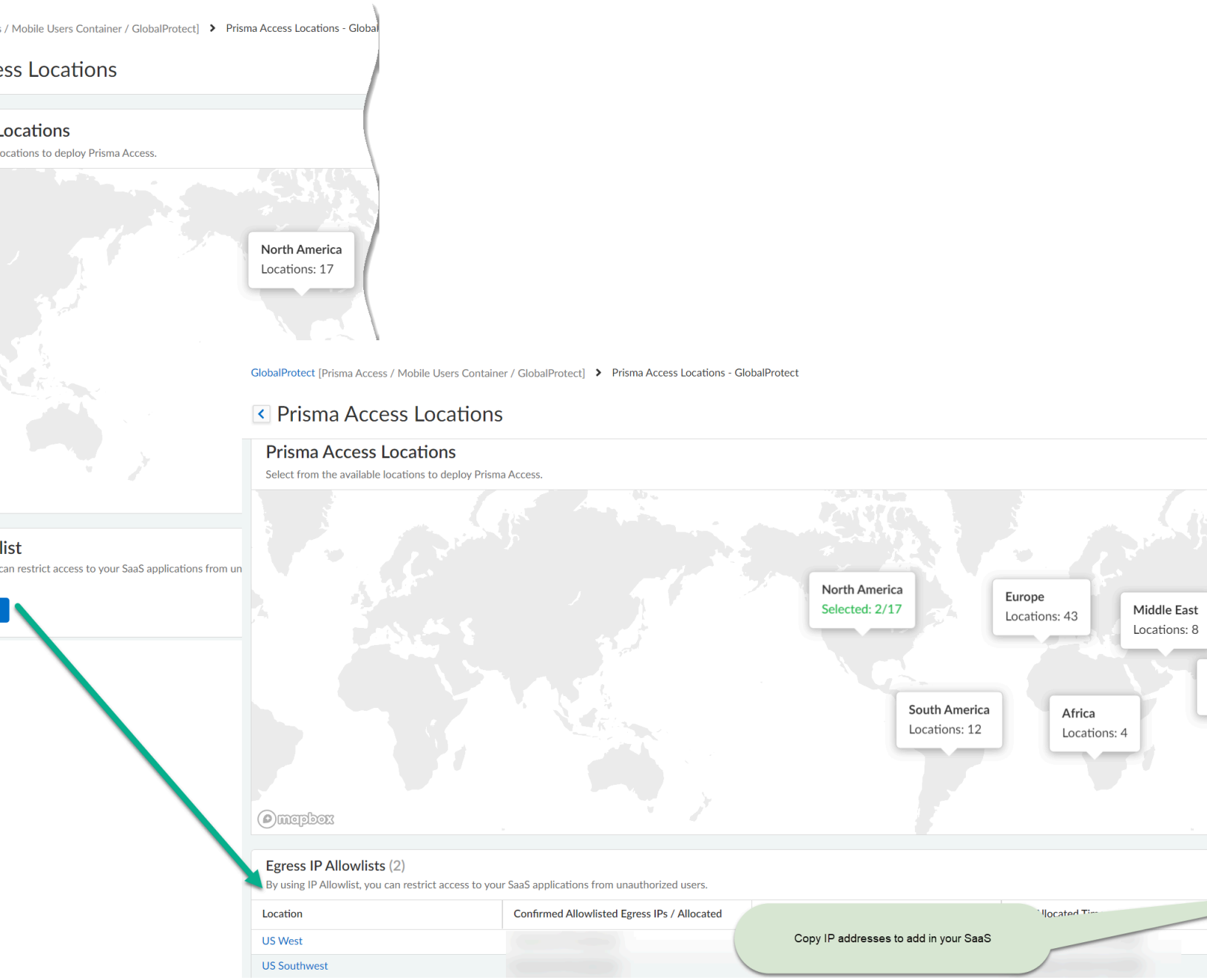
Permita a Prisma Access mostrar las direcciones IP de salida para el tráfico de Prisma Access. Utilice estas direcciones IP en las listas de direcciones IP permitidas para sus aplicaciones SaaS, donde está restringiendo el uso a usuarios o fuentes autorizados.

STEP 1 | Vaya a**Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configurar Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** y edite la configuración de **Prisma Access Locations (Ubicaciones de Prisma Access)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Mostrar las direcciones IP para ubicaciones de Prisma Access.

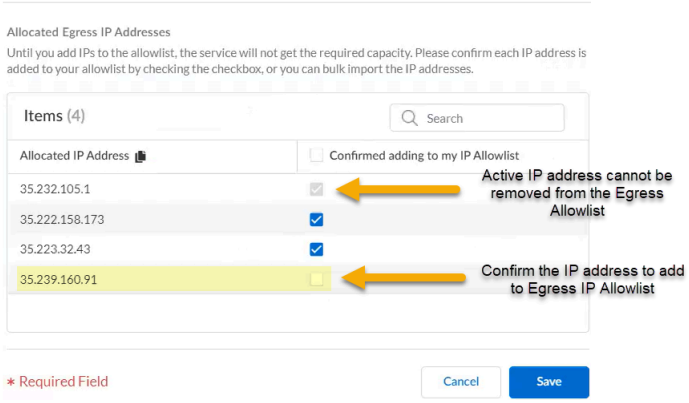
1. **Habilite** la lista de direcciones IP permitidas de salida para mostrar las direcciones IP de las ubicaciones de Prisma Access incorporadas.
2. Copie y añada las direcciones IP asignadas a las listas de permitidos de sus aplicaciones SaaS.
3. Seleccione**Migrate (Migrar)** para confirmar las direcciones IP asignadas a las ubicaciones incorporadas en Prisma Access.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Recupere las direcciones IP de las nueva ubicación incorporada o durante un evento de escalado automático.

1. Seleccione el nombre de la **Location (Ubicación)** para encontrar las nuevas direcciones IP de salida asignadas a la ubicación.
2. Seleccione **Confirmed adding to my IP Allowlist (Confirmado la adición a mi lista de IP permitidas)** para añadir estas direcciones IP a las listas de permitidos para sus aplicaciones SaaS antes de confirmarlas en Prisma Access.



Si tiene direcciones IPv6, seleccione **Confirmed adding to my IPv6 Allowlist (Confirmado la adición a mi lista de permitidos de IPv6)**.



STEP 4 | Envíe sus cambios a Prisma Access.

Deberá Estados de direcciones IP de salida asignadas.

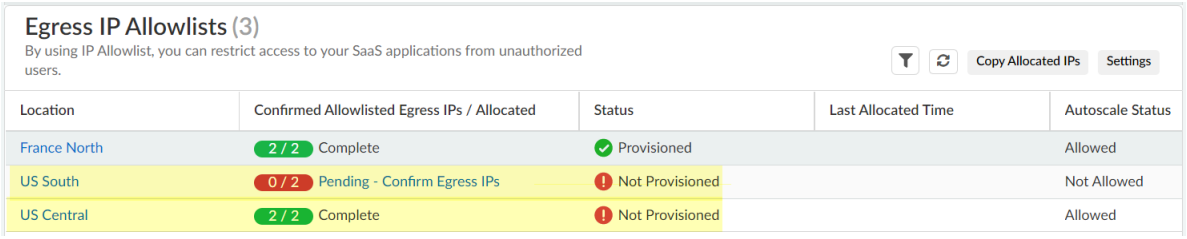
La columna de estado en las listas de direcciones IP permitidas de salida indica si todas las direcciones IP asignadas para las ubicaciones están aprovisionadas para su implementación. Continúe leyendo para conocer cada estado.

- **Aprovisionado**: ha añadido las direcciones IP de salida a las listas de permitidos de sus aplicaciones SaaS, confirmó las direcciones IP en Prisma Accessy envió sus cambios para que se implementaran por completo.
- **Parcialmente aprovisionado**: ha añadido el primer conjunto de direcciones IP de salida y lo ha confirmado en el Prisma Access, y enviado sus cambios. Sin embargo, Prisma Access ha añadido otro conjunto de direcciones IP como parte de un evento de escalado automático, y esas direcciones IP no están confirmadas en Prisma Access.
- **No aprovisionado**: Prisma Access ha asignado direcciones IP para la ubicación y ha añadido las direcciones IP de salida a las listas de permitidos de sus aplicaciones SaaS, y las ha confirmado en Prisma Access, pero aún no ha incorporado esta ubicación.

©2025 Palo Alto Networks, Inc.

- **No se puede aprovisionar**: ha incorporado esta ubicación pero aún no la ha confirmado en Prisma Access y enviado sus cambios.

La tabla de listas de direcciones IP permitidas de salida también indica el número de direcciones IP que están confirmadas y aún deben confirmarse en Prisma Access. Por ejemplo, 1/2 significa que 1 de cada 2 direcciones IP asignadas para la ubicación está confirmada Prisma Access.



Lista de permitidos de usuarios móviles de GlobalProtect (Panorama)

Para permitirle añadir las direcciones IP públicas (de salida) para su implementación de GlobalProtect—Mobile User a cualquier lista de permitidos de aplicaciones SaaS que utilice dentro de su organización, Prisma Access proporciona las direcciones IP y le permite verificar que las haya añadido a su lista de permitidos antes de usarlas en su entorno.

Este método de asignación de direcciones IP de salida tiene los siguientes beneficios:

- Se asegura de que Prisma Access solo proporciona direcciones IP que usted haya listado como permitidas.
- Evita que los usuarios móviles intenten conectarse a Prisma Access desde una dirección IP que esté bloqueada por la red de su organización. Prisma Access no libera direcciones IP para su implementación hasta que usted haya confirmado que están en la lista de permitidos.
- Proporciona una manera de recuperar sus direcciones IP de salida actuales sin utilizar la API.

Prisma Access asigna direcciones IP de salida en las siguientes situaciones:

- Al incorporar sus ubicaciones durante la incorporación de usuarios móviles.

  Prisma Access asigna dos direcciones IP de puerta de enlace para cada ubicación que incorpore.

  Si incorpora una ubicación y otras ubicaciones en la misma ubicación de cómputo experimentan un evento de escalado automático, Prisma Access podría asignar más de dos direcciones IP para la nueva ubicación. En esta situación, asegúrese de añadir todas estas direcciones IP a sus listas de permitidos y confirme que todas las direcciones están ***Added to My Allow List (Añadidas a mi lista de permitidos)****.*

- Durante un gran evento de escalado.

  Si el número de usuarios móviles excede la capacidad de las dos direcciones IP preasignadas, Prisma Access asigna un conjunto más de dos direcciones IP.

  Los eventos de escalado automático afectan a todas las ubicaciones incorporadas en una ubicación de cómputo. Cuando un evento de escalado automático se produce para una ubicación y aún no ha confirmado que las direcciones se añadirán a sus listas de permitidos,

 ©2025 Palo Alto Networks, Inc.

todas las ubicaciones en esa ubicación de cómputo mostrarán un **Autoscale Status (Estado de escalado automático)** de **Not Allowed (No permitido)**.

*El **Autoscale Status (Estado de escalado automático)** muestra el estado del escalado automático en Prisma Access.*

- ***Allowed (Permitido)**: ha añadido direcciones IP a las listas de permitidos. Si un gran número de usuarios móviles inician sesión en una única ubicación y activan un evento de escalado automático, Prisma Access utilizará las direcciones IP permitidas enumeradas para el evento de escalado automático.*
- ***No permitido**: no ha especificado todas las direcciones IP que se añadirán a sus listas de permitidos en la interfaz de usuario de Prisma Access, o no ha confirmado ni enviado sus cambios después de marcarlos como añadidos. Si Prisma Access activa un evento de escalado automático, Prisma Access no proporcionará más direcciones IP para añadir más capacidad para la ubicación.*

  *Cada vez que añade una ubicación, o cada vez que Prisma Access añade direcciones IP como resultado de un evento de escalado automático, debe actualizar la página que contiene la tabla **Egress IP Allow List (Lista de permitidos de IP de salida)**, especificar **Added to My Allow List (Añadido a mi lista de permitidos)** para marcar las direcciones IP como añadidas a las listas de permitidos de su organización y **Commit and Push (Confirmar y enviar)** sus cambios.*

Para mantenerse informado de cualquier dirección IP que Prisma Access añade como resultado de un evento de escalado automático, puede configurar una URL donde Prisma Access le notificará los cambios de dirección IP.

No es necesario que habilite esta funcionalidad; usted debe seleccionar si permite o no que Prisma Access libere las direcciones IP hasta que las haya confirmado como permitidas en la interfaz de usuario.

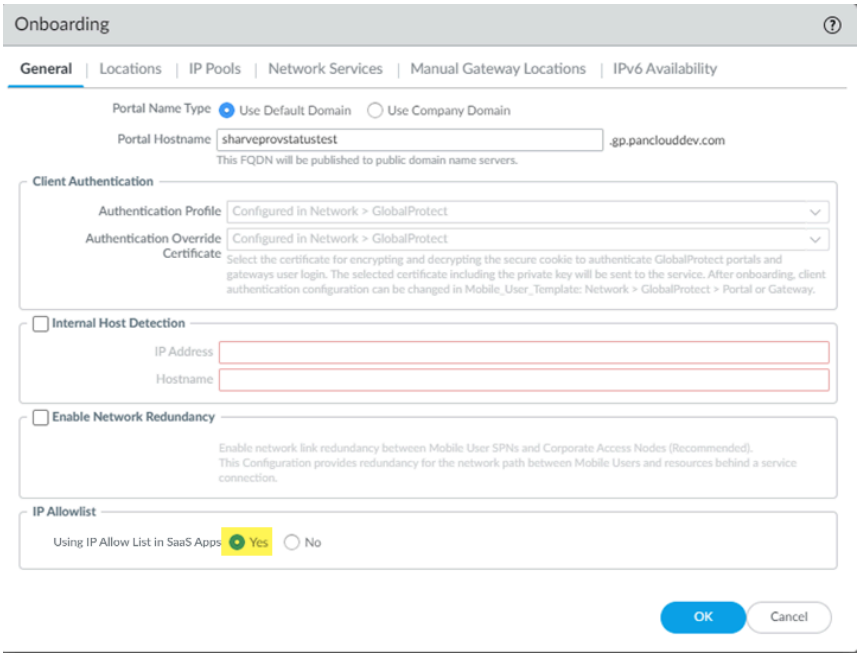
Para impedir que Prisma Access aprovisione direcciones IP públicas (de salida) de GlobalProtect a su implementación hasta que las haya añadido a sus listas de permitidos, especifique **Yes (Sí)** en la configuración **Using IP Allow List in SaaS Apps (Usar lista de direcciones IP permitidas en aplicaciones SaaS)** durante la incorporación de Usuarios móviles: GlobalProtect. Confirme que los ha añadido en la UI de Prisma Access completando la siguiente tarea.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**.

STEP 2 | Seleccione su **Hostname (Nombre de host)** y **Configure (Configurar)** para configurarlo (para una implementación existente) o **Configure (Configurar)** para configurar su implementación por primera vez (para una nueva implementación).

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Especifique el **Using IP Allow List in SaaS Apps (Uso de la lista de direcciones IP permitidas en aplicaciones SaaS)** como **Yes (Sí)**.



STEP 4 | Continúe su incorporación de Prisma Access, incluida la selección de las ubicaciones que se utilizarán en la implementación de Usuarios móviles: GlobalProtect, y seleccione **Commit and Push (Confirmar y enviar)** y confirmar y enviar sus cambios.

Podría tardar hasta un minuto para que los cambios se reflejen en la interfaz de usuario. Si ve la **Egress IP Allow List (Lista de direcciones IP de salida permitidas)** antes de confirmar y enviar sus cambios, muestra un estado de **0/0 Egress IPs Confirmed Allow Listed (0/0 Direcciones IP de salida incluidas en la lista de permitidos confirmadas)**, porque Prisma Access no ha asignado ninguna dirección IP de salida a su implementación.

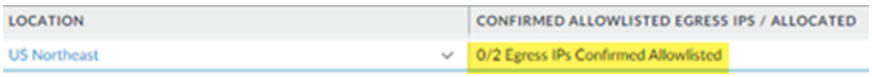
STEP 5 | Vea la tabla **Egress IP Allow List (Lista de direcciones IP permitidas de salida)** y tome nota de las direcciones IP de salida que deben añadirse a sus listas de direcciones permitidas.

Puede ver las direcciones IP de salida en el campo **Confirmed Allow Listed Egress IPs / Allocated (Direcciones IP de salida incluidas en la lista de permitidos confirmadas/asignadas)** de la tabla **Egress IP Allow List (Lista de direcciones IP permitidas de salida)**. El primer número indica si se ha confirmado o no que la dirección IP se ha agregado a sus listas de permitidos.

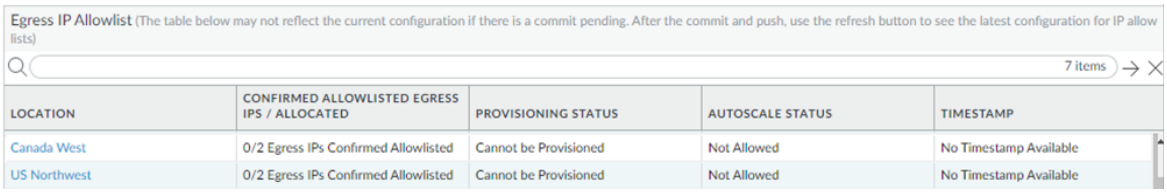
El siguiente ejemplo muestra las direcciones IP para la ubicación noreste de EE. UU. La descripción de `0/2 direcciones IP de salida incluidas en la lista de`

 ©2025 Palo Alto Networks, Inc.

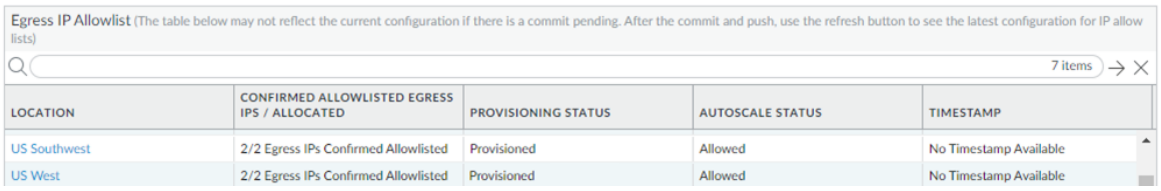
`permitidos confirmadas` indica que 0 de las dos direcciones IP de salida se han marcado como añadidas a sus listas de permitidos y necesita añadirlas.



Si tiene una nueva implementación de Prisma Access, o si ha añadido ubicaciones o ha tenido un evento de escalado automático, la tabla muestra que ninguna de las direcciones IP de salida se ha añadido a la lista de permitidos de su organización.

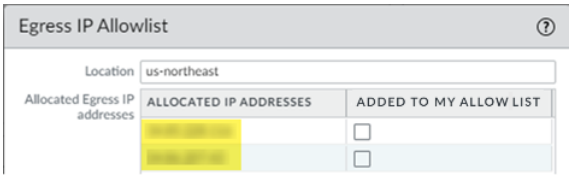


Si ya tiene una implementación de Prisma Access, la tabla muestra un **Provisioning Status (Estado de aprovisionamiento)** de **Provisioned (Aprovisionado)** y un **Autoscale Status (Estado de escalado automático)** de **Allowed (Permitido)**, lo que indica que Prisma Access marcó las direcciones IP de salida como añadidas.



Prisma Access asignará dos direcciones para cada ubicación recién añadida. Si una ubicación existente tuvo previamente un evento de escalado automático cuando una gran cantidad de usuarios móviles iniciaron sesión en una sola ubicación al mismo tiempo, Prisma Access asigna direcciones IP de salida adicionales en múltiplos de dos, y una ubicación existente podría tener cuatro o más direcciones.

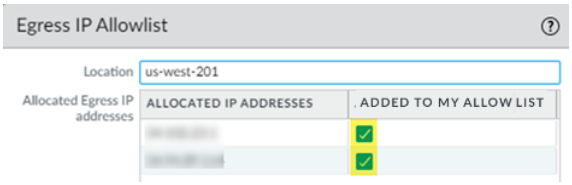
STEP 6 | Encuentre las nuevas direcciones IP de salida que deben añadirse a las listas de permitidos de su organización seleccionando el nombre de la **Location (Ubicación)** en la tabla.



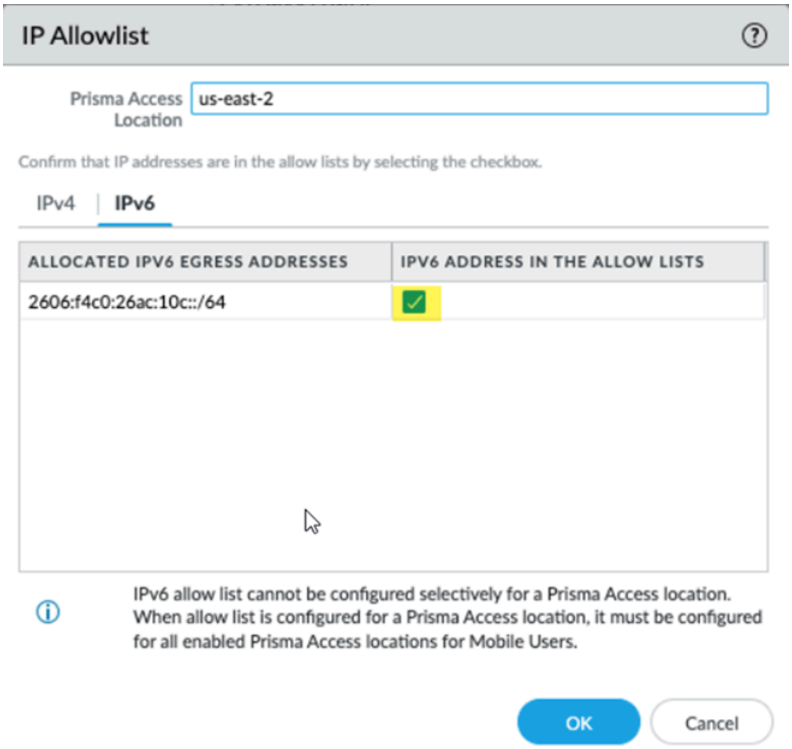
STEP 7 | Añada estas direcciones IP de salida a las listas de permitidos de su organización.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Después de haber permitido la dirección IP de salida, regrese al área de IP de salida e indique que la ha añadido a su lista de permitidos seleccionando **Added to My Allow List (Añadido a mi lista de permitidos)**.



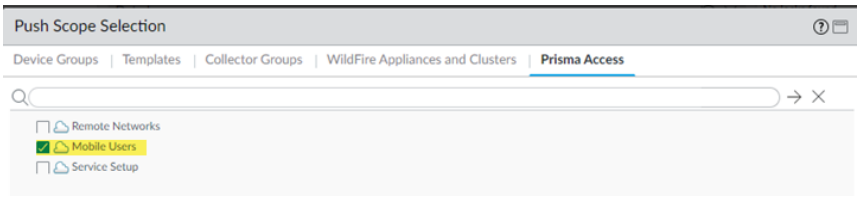
Si tiene direcciones IPv6, seleccione **IPv6 Address in the Allow Lists (Dirección IPv6 en las Listas de permitidos)**.



 ©2025 Palo Alto Networks, Inc.

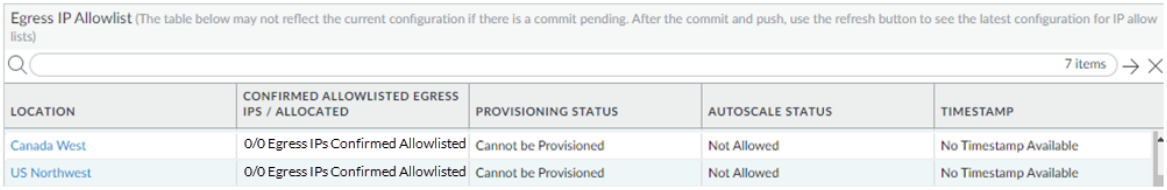
STEP 9 | Confirme y envíe sus cambios para que estén activos en Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Prisma Access**, luego asegúrese de que **Mobile Users (Usuarios móviles)** esté seleccionado.



3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Seleccione **Commit (Confirmar)** y **Push (Enviar)**sus cambios.

Si visualiza la tabla **Egress IP Allow List (Lista de direcciones IP de salida permitidas)** antes de confirmar y enviar sus cambios, la columna Confirmado muestra un estado de **0/0 Egress IPs Confirmed Allow Listed (0/0 direcciones IP de salida incluidas en la lista de permitidos confirmadas)** porque Prisma Access no ha asignado ninguna dirección IP a su implementación hasta que seleccione la opción **Commit and Push (Confirmar y enviar)**.



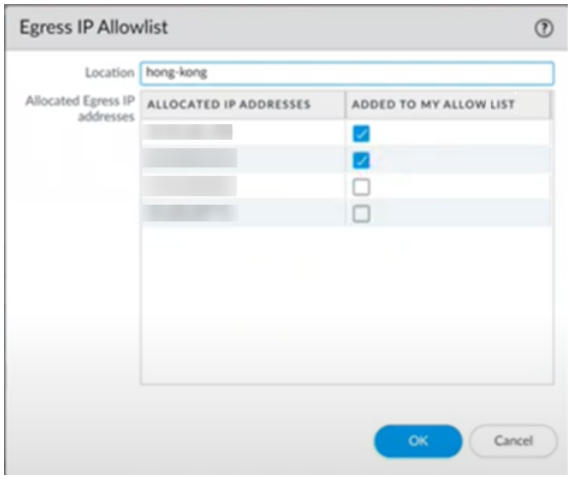
La tabla **Egress IP Allow List (Lista de direcciones IP permitidas de salida)** contiene los siguientes campos adicionales:

Campo	Descripción
Ubicación	La ubicación del usuario móvil incorporado.
Direcciones IP de salida incluidas en la lista de permitidos confirmadas/asignadas	El número de direcciones IP de salida que se han confirmado como permitidas y el número de direcciones IP de salida que se han asignado.
Estado de aprovisionamiento	El estado de lista de permitidos de las direcciones IP de salida. • **Provisioned (Aprovisionado)**: ha añadido las direcciones IP de salida a las listas de permitidos de su organización y ha confirmado que se añadieron en la UI de Prisma Access marcando **Added to My Allow List (Añadido a mi lista de permitidos)** y habiendo confirmado y enviado sus cambios para que estén completamente aprovisionados.

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción
	• **Not Provisioned (No aprovisionado)**: Prisma Access ha asignado direcciones IP para la ubicación y usted ha añadido las direcciones IP de salida a las listas de permitidos de su organización y ha confirmado que se añadieron en la interfaz de usuario de Prisma Access, pero aún no ha incorporado esta ubicación. • **Cannot Be Provisioned (No se puede aprovisionar)**: ha incorporado esta ubicación, pero aún no ha marcado **Add to My Allow List (Añadir a mi lista de permitidos)** ni ha confirmado y enviado sus cambios. Hasta que especifique en Prisma Access que ha añadido estas direcciones IP de salida a las listas de permitidos de su organización y ha seleccionado **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios, Prisma Access no proporcionará estas direcciones IP a su implementación. • **Provisioned with partial capacity (Aprovisionado con capacidad parcial)**: ha añadido el primer conjunto de direcciones IP de salida y ha confirmado que se añadieron en la UI de Prisma Access, y ha confirmado y enviado sus cambios. Sin embargo, Prisma Access ha añadido otro conjunto de direcciones IP como parte de un evento de escalado automático, y esas direcciones IP no se han especificado como añadidas a sus listas de permitidos en la interfaz de usuario de Prisma Access. La siguiente captura de pantalla muestra un ejemplo de una implementación que se marcaría como **Provisioned with partial capacity (Aprovisionada con capacidad parcial)**. Se han marcado dos direcciones IP como **Added to My Allow List (Añadidas a mi lista de permitidos)**; sin embargo, Prisma Access ha añadido dos direcciones IP más a

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción
	esta ubicación, y esas ubicaciones no se han añadido a la interfaz de usuario. 
Estado de escalado automático	Muestra el estado del escalado automático en Prisma Access. • **Allowed (Permitido)**: ha añadido direcciones IP a las listas de permitidos. Si un gran número de usuarios móviles inician sesión en una única ubicación y activan un evento de escalado automático, Prisma Access utilizará las direcciones IP permitidas enumeradas para el evento de escalado automático. • **Not Allowed (No permitido)**: no ha especificado todas las direcciones IP que se añadirán a sus listas de permitidos en la UI de Prisma Access, o no ha confirmado ni enviado sus cambios después de marcarlos como añadidos. Si Prisma Access activa un evento de escalado automático, Prisma Access no proporcionará más direcciones IP para añadir más capacidad para la ubicación. Cada vez que añade una ubicación, o cada vez que Prisma Access añade direcciones IP como resultado de un evento de escalado automático, debe actualizar la página que contiene la tabla **Egress IP Allow List (Lista de permitidos de IP de salida)**, especificar **Added to My Allow List (Añadido a mi lista de permitidos)** para marcar las direcciones IP como añadidas a las listas de permitidos de su organización y **Commit and Push (Confirmar y enviar)** sus cambios.

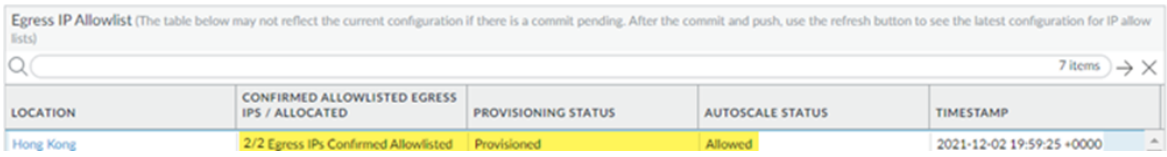
 ©2025 Palo Alto Networks, Inc.

Campo	Descripción
	Para mantenerse informado de cualquier dirección IP que Prisma Access añada como resultado de un evento de escalado automático, debe configurar una URL donde Prisma Access le notificará los cambios de dirección IP.
Marca de tiempo	La última hora conocida en que se asignó una IP para esta región en el Tiempo Universal Coordinado (UTC).

Después de **Commit and Push (Confirmar y enviar)**, la columna Confirmado mostrará un estado de **0/2 Egress IPs Confirmed Allow Listed (0/2 direcciones IP de salida incluidas en la lista de permitidos confirmadas)**, porque aún no ha confirmado que las direcciones IP se hayan incluido en la lista de permitidos de la interfaz de usuario de Prisma Access.

Cuando se incorpora la ubicación de un usuario móvil, Prisma Access le proporciona dos direcciones IP de salida: una dirección IP activa y una dirección para usar en caso de un evento de escalado automático. A continuación se ofrecen ejemplos de cómo Prisma Access asigna y aprovisiona direcciones IP de salida después de un evento de escalado automático.

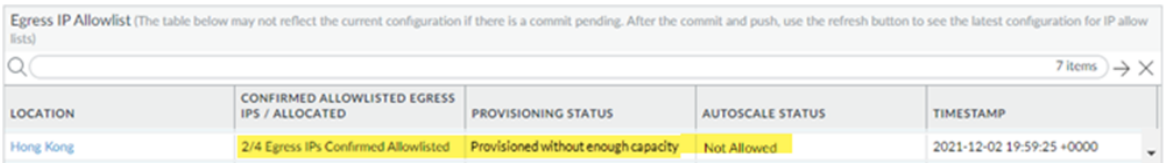
Evento de escalado automática: si una gran cantidad de usuarios móviles inician sesión en una ubicación de usuario móvil al mismo tiempo, ese evento podría hacer que Prisma Access asigne un conjunto adicional de dos direcciones IP de salida para dar cabida al gran número de usuarios. Una vez que haya incluido en la lista de permitidos las dos primeras direcciones IP de salida, el estado antes de un evento de escalado automático muestra las dos direcciones IP de salida como incluidas en la lista de permitidos con un estado confirmado de **2/2 Egress IPs Confirmed Allow Listed (2/2 direcciones IP de salida confirmadas permitidas enumeradas)**, un estado de aprovisionamiento de **Provisioned (Aprovisionado)** y un estado de escalado automático de **Allowed (Permitido)**, como se muestra en la ubicación de Hong Kong en la siguiente captura de pantalla.



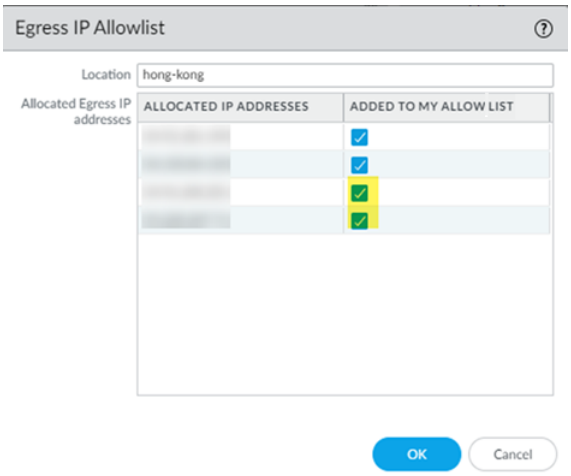
Si una gran número de usuarios móviles inician sesión en la ubicación de Hong Kong al mismo tiempo, Prisma Access activa la dirección IP de salida de respaldo y asigna dos direcciones IP más, y hace que una de ellas esté activa. Cuando se produce un evento de escalado automático, las direcciones IP de salida se han asignado pero no se han aprovisionado, el estado confirmado es **2/4 Egress IPs Confirmed Allow Listed (2/4 direcciones IP de salida incluidas en la lista de**

 ©2025 Palo Alto Networks, Inc.

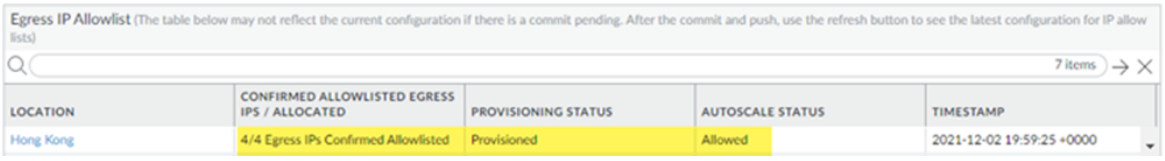
permitidos confirmadas) y el estado de aprovisionamiento muestra **Provisioned without enough capacity (Aprovisionado sin suficiente capacidad)**. Además, el estado de escalado automático muestra **Not Allowed (No permitido)**, lo que significa que Prisma Access no proporcionará la dirección IP de salida adicional a su implementación si ocurre un evento de escalado automático.



Después de haber añadido las nuevas direcciones IP de salida a sus listas de permitidos, seleccione el nombre de la ubicación; luego, seleccione **Added to My Allow List (Añadido a mi lista de permitidos)** para las dos direcciones IP que se añadieron y seleccione **Commit and Push (Confirmar y enviar)** sus cambios.



Cuando se completa, la ubicación de Hong Kong muestra que las cuatro direcciones IP de salida están confirmadas y aprovisionadas, y el escalado automático está activo.



Actualizaciones de la aplicación GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

Prisma Access aloja la versión de la aplicación GlobalProtect que los usuarios de macOS y Windows de su organización pueden descargar desde portal de Prisma Access. Prisma Access ofrece varias versiones de la aplicación GlobalProtect y puede elegir que una de esas versiones sea la versión activa. También puede gestionar el acceso de los usuarios móviles a la aplicación GlobalProtect o realizar actualizaciones por etapas.

- Seleccione la versión activa de la aplicación GlobalProtect para Prisma Access
- Permitir a los usuarios actualizar la aplicación GlobalProtect
- Escalonar actualizaciones de la aplicación GlobalProtect

Seleccione la versión activa de la aplicación GlobalProtect para Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access gestiona la versión de la aplicación GlobalProtect para los usuarios de Windows y macOS de su organización. Mientras Prisma Access aloja varias versiones de la aplicación GlobalProtect, solo una de las versiones alojadas está activa. Cuando los usuarios móviles inician sesión en el portal de Prisma Access, la versión activa es la que está disponible para que los usuarios móviles la descarguen e instalen en sus dispositivos Windows y macOS.

Puede seleccionar varias versiones de GlobalProtect en una Implementación multiinquilino. La configuración de la versión de la aplicación GlobalProtect que se aplica es por inquilino y no global; la versión de la aplicación se controla por inquilino.

Algunas funciones, como la optimización de IP, requieren que los usuarios tengan versiones suficientemente actualizadas de GlobalProtect. Continúe leyendo para saber cómo seleccionar la versión de la aplicación de GlobalProtect en Prisma Access.

- Strata Cloud Manager
- Panorama

Seleccione la versión activa de la aplicación GlobalProtect para Prisma Access (Managed by Strata Cloud Manager)

Puede reemplazar la versión activa actual con otra versión alojada desde la página Configuración del servicio completando los siguientes pasos.

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configurar Prisma Access)** > **Mobile Users (Usuarios móviles)** y luego ubique el panel **GlobalProtect Connection (Conexión GlobalProtect)**.

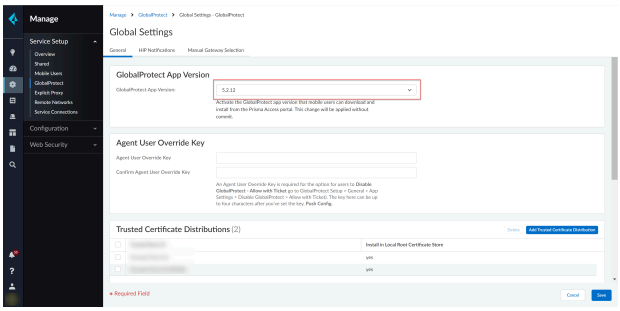
STEP 2 | Seleccione **GlobalProtect Setup (Configuración de GlobalProtect)** o **Enable (Habilitar)** > **GlobalProtect Setup (Configuración de GlobalProtect)** si GlobalProtect aún no está habilitado.

STEP 3 | Seleccione la pestaña **GlobalProtect app (Aplicación de GlobalProtect)** y luego edite la **Global App Settings (Configuración global de la aplicación)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | En la pestaña **General** de la página **Global Settings (Configuración global)**, seleccione la **GlobalProtect App Version (Versión de la aplicación de GlobalProtect)** que desea permitir que los usuarios móviles descarguen e instalen desde el portal de Prisma Access.

La versión activa se indica en la lista desplegable.



Seleccione la versión activa de la aplicación GlobalProtect para Prisma Access (Managed by Panorama)

Si su versión actualmente activa ha llegado al final de su vida útil, Prisma Access le notifica y le solicita que active una versión compatible.

Puede reemplazar la versión activa actual con otra versión alojada desde la página Configuración del servicio completando los siguientes pasos.

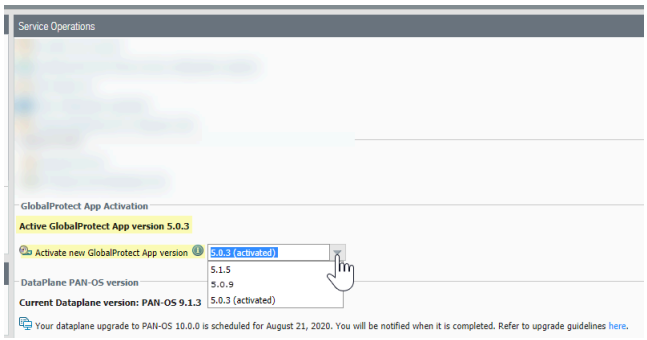
Si está usando Prisma Access en un entorno FedRAMP, debe utilizar la versión certificada FIPS de GlobalProtect, que es la versión 5.1.4. Si usted cambia la versión predeterminada de GlobalProtect de 5.1.4, no puede seleccionar la versión 5.1.4 en la interfaz de usuario de Panorama y debe abrir un Caso de asistencia con el Soporte Técnico de Palo Alto Networks para volver a añadirlo.

STEP 1 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.

©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Activate new GlobalProtect App version (Activar nueva versión de la aplicación GlobalProtect)**.

La versión activa se indica en la lista desplegable.

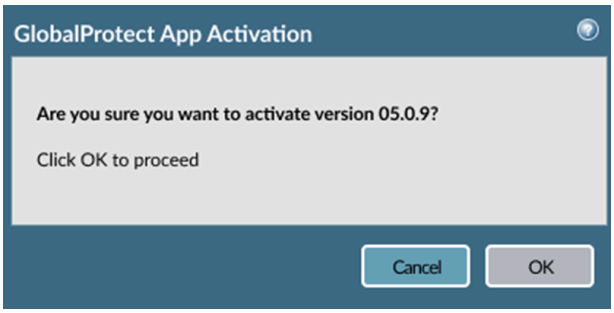


Si su versión actual de GlobalProtect está al final de su vida útil (EoL), aparecerá un mensaje en esta área de la página Configuración de servicio; si recibe este mensaje, actualice la versión de su aplicación GlobalProtect continuando con el siguiente paso.

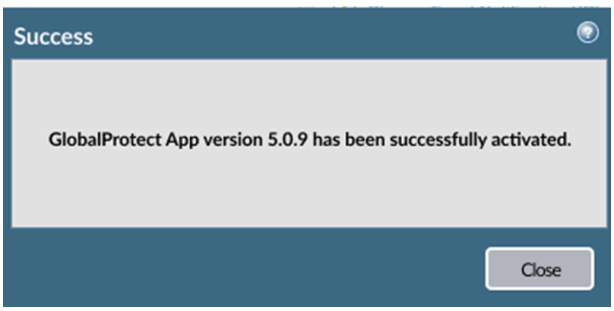


STEP 3 | Seleccione la versión a la que desea actualizar y haga clic en **OK (Aceptar)**.

Aparecerá una ventana para verificar su elección.



Después de que se haya activado la aplicación, recibirá un mensaje indicándole que se ha activado correctamente.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Vea la página Estado del sistema para verificar la **Active GlobalProtect App version (Versión activa de la aplicación GlobalProtect)**.

Permitir a los usuarios actualizar la aplicación GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Conozca cómo controlar el acceso de los usuarios móviles a la versión de la aplicación GlobalProtect para implementaciones de Prisma Access GlobalProtect.

- Strata Cloud Manager
- Panorama

Permita a los usuarios actualizar la aplicación GlobalProtect (Strata Cloud Manager)

Puede gestionar el acceso de los usuarios móviles a la versión activa de la aplicación GlobalProtect alojada por Prisma Access. Para hacer esto en Prisma Access (Managed by Strata Cloud Manager), configure el ajuste de **Upgrade Global Protect (Actualización de Global Protect)**GlobalProtect: Personalizar la configuración de la aplicación. Para Prisma Access (Managed by Strata Cloud Manager), complete los siguientes pasos.

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configurar Prisma Access)** > **Mobile Users (Usuarios móviles)** y luego ubique el panel **GlobalProtect Connection (Conexión GlobalProtect)**.

STEP 2 | Seleccione **GlobalProtect Setup (Configuración de GlobalProtect)** o **Enable (Habilitar)** > **GlobalProtect Setup (Configuración de GlobalProtect)** si GlobalProtect aún no está habilitado.

STEP 3 | Seleccione la pestaña **GlobalProtect App (Aplicación GlobalProtect)** y luego **Add App Settings (Añadir configuración de la aplicación)**.

STEP 4 | En el área **App Configuration (Configuración de la aplicación)**, seleccione una opción en **Upgrade GlobalProtect App (Actualizar aplicación de GlobalProtect)** para especificar si los usuarios móviles pueden actualizar su versión de la aplicación GlobalProtect a la versión activa alojada en Prisma Access y, si pueden, si pueden elegir cuándo actualizar:

- **Allow when user accepts the upgrade Prompt (Permitir cuando el usuario acepta la solicitud de actualización)**(predeterminado): indica a los usuarios cuando una versión está activa en el cortafuegos y permite a los usuarios actualizar su software cuando es conveniente.
- **Disallow (No permitir)**: impide que los usuarios actualicen el software de la aplicación.
- **Allow Manually (Permitir manualmente)**: permite que los usuarios comprueben e inicien las actualizaciones manualmente seleccionando **Check Version (Comprobar versión)** en la aplicación de GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

- **Allow Transparently (Permitir de manera transparente)**: actualiza automáticamente el software de la aplicación cuando hay una nueva versión disponible en el portal.
- **Allow when the user is in the corporate network (Permitir cuando el usuario está en la red corporativa)**: actualiza automáticamente el software de la aplicación siempre que una nueva versión esté disponible en el portal, pero espera hasta que el enpoint esté conectado internamente a la red corporativa. Esto evita retrasos causados por actualizaciones sobre conexiones de bajo ancho de banda.

Permita a los usuarios actualizar la aplicación GlobalProtect (Panorama)

Puede gestionar el acceso de los usuarios móviles a la versión activa de la aplicación GlobalProtect alojada por Prisma Access. Para hacer esto en Prisma Access (Managed by Strata Cloud Manager), configure el ajuste de **Upgrade Global Protect (Actualización de Global Protect)**GlobalProtect: Personalizar la configuración de la aplicación. Para Prisma Access (Managed by Panorama), complete los siguientes pasos.

STEP 1 | Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.

STEP 2 | Seleccione **Mobile_User_Template** del menú desplegable **Template (Plantilla)**.

STEP 3 | Seleccione **GlobalProtect_Portal** para editar la configuración del portal de Prisma Access.

STEP 4 | Seleccione la pestaña **Agent (Agente)** y seleccione la configuración de la aplicación.

STEP 5 | Seleccione la pestaña **App (Aplicación)**.

STEP 6 | En el área de **App Configurations (Configuraciones de la aplicación)**, seleccione una opción en **Allow User to Upgrade GlobalProtect App (Permitir al usuario actualizar la aplicación de GlobalProtect)** para especificar si los usuarios móviles pueden actualizar su versión de la aplicación GlobalProtect a la versión activa que está alojada en Prisma Access y, si pueden, si pueden elegir cuándo actualizar:

- **Allow with Prompt (Permitir con solicitud)**(predeterminado): indique a los usuarios cuando una versión está activa y permita a los usuarios actualizar su software cuando sea conveniente.
- **Disallow (No permitir)**: impide que los usuarios actualicen el software de la aplicación.
- **Allow Manually (Permitir manualmente)**: permite que los usuarios comprueben e inicien las actualizaciones manualmente seleccionando **Check Version (Comprobar versión)** en la aplicación de GlobalProtect.
- **Allow Transparently (Permitir de manera transparente)**: actualiza automáticamente el software de la aplicación cuando hay una nueva versión disponible en el portal.
- **Internal (Interno)**: actualiza automáticamente el software de la aplicación siempre que una nueva versión esté disponible en el portal, pero espera hasta que el enpoint esté conectado internamente a la red corporativa. Esto evita retrasos causados por actualizaciones sobre conexiones de bajo ancho de banda.

 ©2025 Palo Alto Networks, Inc.

Escalonar actualizaciones de la aplicación GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Si gestiona una organización grande, es posible que desee actualizar a los usuarios móviles a la última versión de la aplicación GlobalProtect en etapas. Por ejemplo, puede asignar un grupo más pequeño para actualizar su aplicación GlobalProtect antes de implementar la actualización para todos en su organización. Para hacerlo, puede completar las siguiente tarea.

STEP 1 | Si aún no lo ha creado, cree un grupo de usuarios para el primer grupo de usuarios al que desea implementar la actualización de la aplicación GlobalProtect.

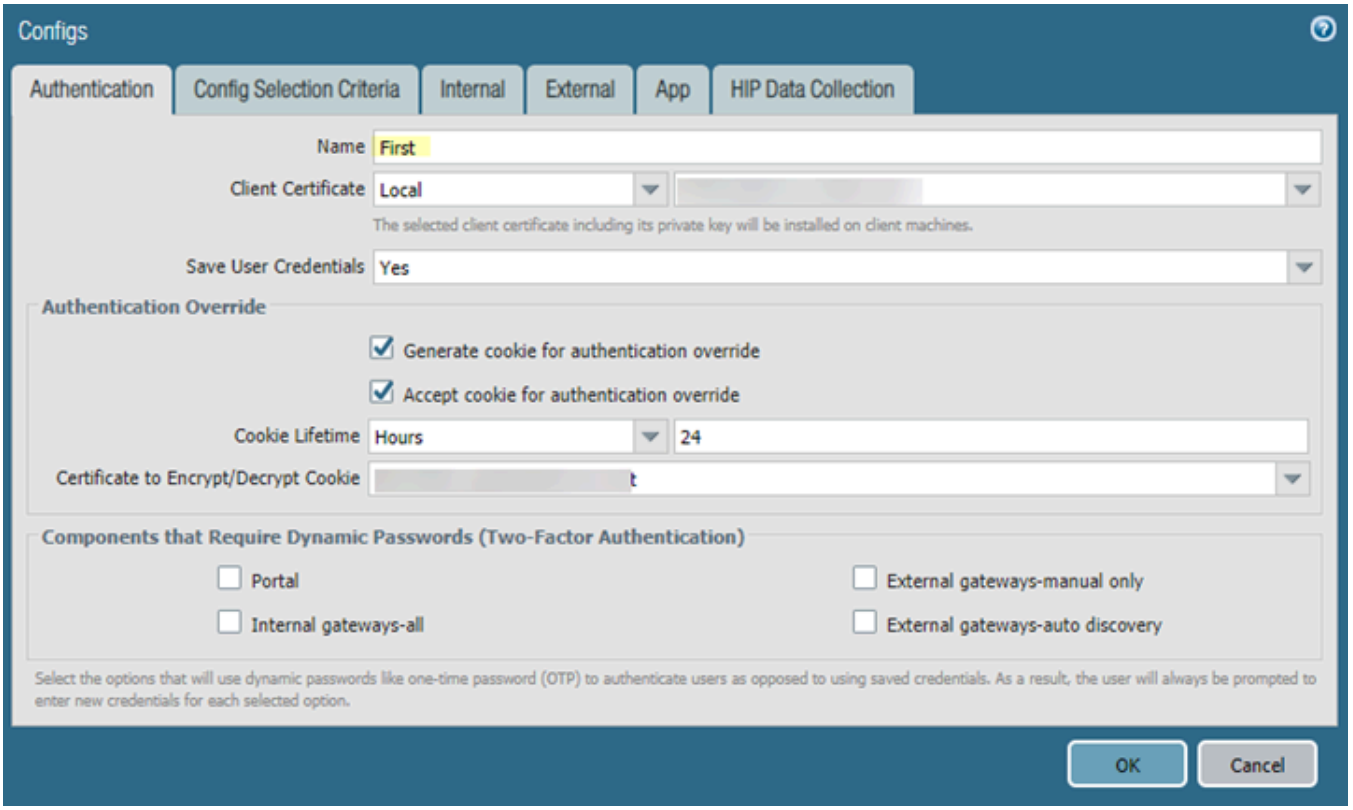
Puede utilizar User-ID para asignar usuarios a grupos o seleccionar **Device (Dispositivo)** > **Local User Database (Base de datos de usuarios local)** > **User Groups (Grupos de usuarios)** para crear un grupo manualmente.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Cree una nueva configuración de agente de GlobalProtect para usar con el primer grupo de usuarios.

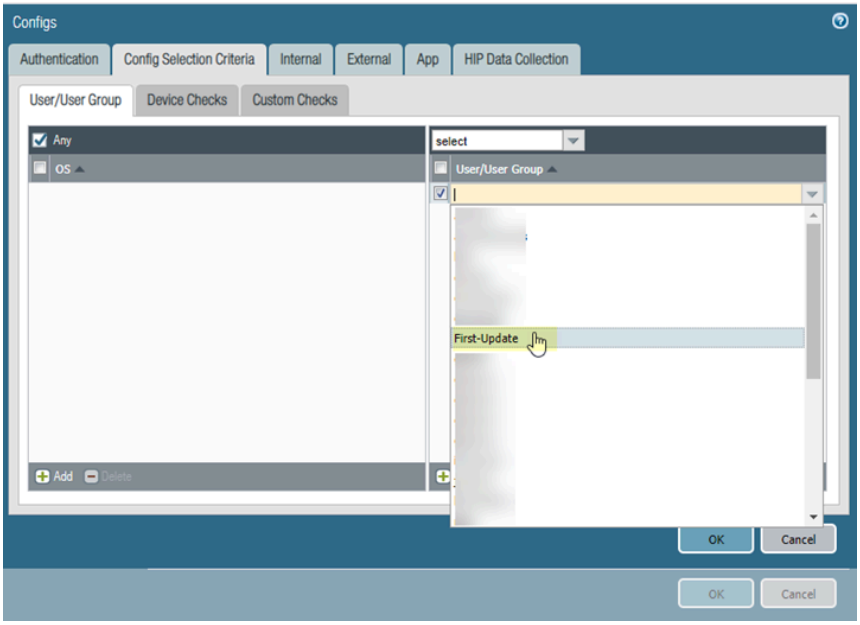
1. En Panorama, seleccione **Network (Red)** > **GlobalProtect (GlobalProtect)** > **Portals (Portales)**.
2. Seleccione **Mobile_User_Template** del menú desplegable **Template (Plantilla)**.
3. Seleccione **GlobalProtect_Portal** para editar la configuración del portal de Prisma Access.
4. Seleccione la pestaña **Agent (Agente)**.
5. Seleccione la configuración **DEFAULT (PREDETERMINADA)** y elija **Clone (Clonar)**.

   También puede **Add (Añadir)** una nueva configuración; pero duplicar la configuración existente copia la información necesaria para la nueva configuración.
6. Introduzca un **Name (Nombre)** para la configuración.



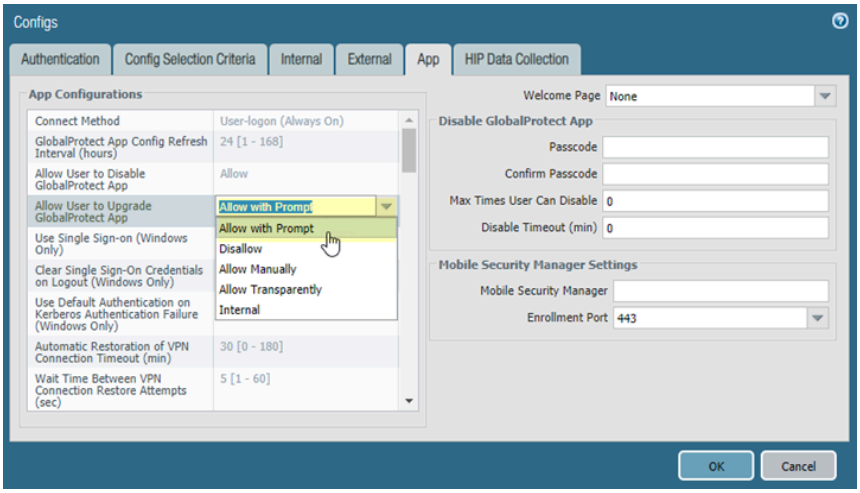
7. Seleccione la pestaña **Config Selection Criteria (criterios de selección de configuración)**
8. En el área **User/User Group (Usuario/Grupo de usuarios)**, seleccione el usuario que creó en el Paso 1.

 ©2025 Palo Alto Networks, Inc.



9. Seleccione la pestaña **App (Aplicación)**.
10. Cambie **Allow User to Upgrade GlobalProtect App (Permitir al usuario actualizar la aplicación GlobalProtect)** a **Allow with Prompt (Permitir con aviso)** o **Allow Transparently (Permitir de forma transparente)**.

    Allow with Prompt (Permitir con aviso) avisa a los usuarios cuando se activa una nueva versión y les permite actualizar su software cuando sea conveniente; **Allow Transparently (Permitir de forma transparente)** actualiza automáticamente el software de la aplicación cada vez que hay una nueva versión disponible en el portal.



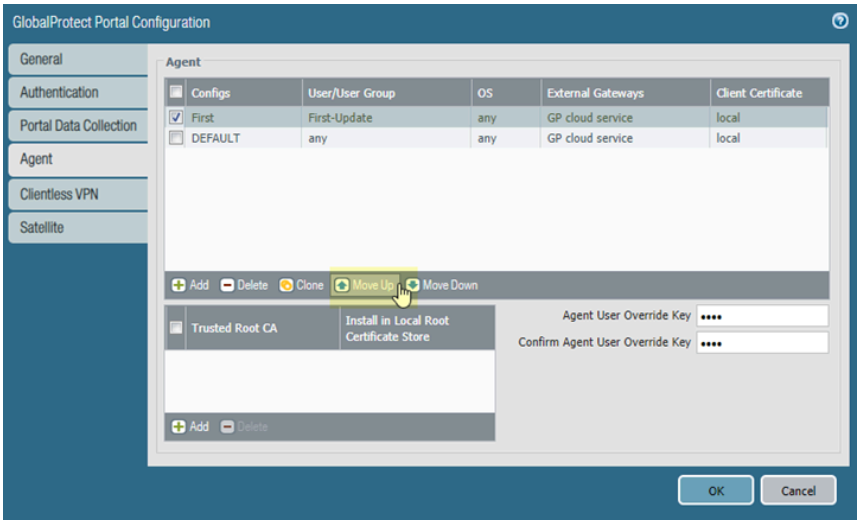
11. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 3 | Seleccione **Move Up (Mover hacia arriba)** para mover su configuración por encima de la configuración predeterminada.

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,

 ©2025 Palo Alto Networks, Inc.

el portal busca una coincidencia empezando por la parte superior de la lista. Cuando encuentra una coincidencia, brinda la configuración correspondiente a la aplicación.



STEP 4 | Repita estos pasos para la configuración **DEFAULT (PREDETERMINADA)**, pero cambie **Allow User to Upgrade GlobalProtect App (Permitir al usuario actualizar la aplicación GlobalProtect)** a **Disallow (No permitir)** para evitar que los usuarios actualicen al software más reciente de la aplicación GlobalProtect.

STEP 5 | Cuando desee permitir que el resto de usuarios actualicen sus aplicaciones, cambie **Allow User to Upgrade GlobalProtect App (Permitir al usuario actualizar la aplicación GlobalProtect)** en la configuración **DEFAULT (PREDETERMINADA)** a una selección que lo permita [ya sea **Allow with prompt (Permitir con aviso)** o **Allow Transparently (Permitir de forma transparente)**].

Integrar Prisma Access con las puertas de enlace GlobalProtect locales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Licencia de Prisma Access

Prisma Access le permite ampliar la plataforma de seguridad de Palo Alto Networks a sus ubicaciones de red remotas y a sus usuarios móviles sin tener que construir su propia infraestructura de seguridad global y expandir su capacidad operativa. En los casos en los que ya haya implementado puertas de enlace GlobalProtect en regiones donde ya tiene la infraestructura para gestionarlas, puede aprovechar esta inversión configurando Prisma Access para dirigir a los usuarios móviles a sus puertas de enlace externas existentes cuando sea apropiado.

Puede gestionar las prioridades para Prisma Access y puertas de enlace locales, lo que le permite especificar prioridades para las instalaciones locales y puertas de enlace para Prisma Access. Los administradores no pueden especificar usuarios móviles para que se conecten a una puerta d

 ©2025 Palo Alto Networks, Inc.

enlace específica de Prisma Access; sin embargo, los administradores pueden permitir que los usuarios móviles seleccionen manualmente puertas de enlace específicas de Prisma Access que utilizan la aplicación GlobalProtect.

No es posible utilizar su propio portal con Prisma Access. Solo puede utilizar el portal que se implementa cuando su Prisma Access para usuarios móviles se aprovisiona.

- Strata Cloud Manager
- Panorama

Integre Prisma Access con puertas de enlace GlobalProtect locales (Prisma Access (Managed by Strata Cloud Manager))

STEP 1 | Añada su puerta de enlace local a la lista de puertas de enlace en la configuración del agente.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** y seleccione la pestaña **GlobalProtect App (Aplicación GlobalProtect)**.
2. **Add App Settings (Añadir configuración de aplicación)**.
3. **Add (Añadir)** una puerta de enlace externa

   *Si añade una nueva configuración de agente y desea añadir las puertas de enlace de Prisma Access a la lista de puertas de enlace externas en esa configuración, debe establecer el **Name (Nombre)** en **GP cloud service (Servicio en la nube de GP)** y la **Address (Dirección)** en **gpcloudservice.com**. Introduzca estos valores exactamente como se muestran y no podrá usar ninguno de estos valores para puertas de enlace sin Prisma Access.*
4. Introduzca el **Name (Nombre)** de la puerta de enlace y especifique el **FQDN** o la dirección **IP** de la puerta de enlace en el campo **Address (Dirección)**; este valor debe coincidir exactamente con el nombre común (CN) en el certificado de la puerta de enlace.
5. (Opcional) Si desea que los usuarios móviles solo se conecten a la puerta de enlace cuando estén en la región correspondiente, seleccione **Add (Añadir)** para añadir la **Source Region (Región de origen)** para restringir la puerta de enlace. Por ejemplo, si

 ©2025 Palo Alto Networks, Inc.

tiene una puerta de enlace en Francia, debería seleccionar FR (Francia). Si tiene una puerta de enlace en Suecia, debería seleccionar Suecia (SE).

Una ventaja de esto es que los usuarios podrán entonces acceder a una puerta de enlace que les permitirá acceder a recursos de Internet en su propio idioma.

6. (Opcional) Especifique las prioridades en la configuración de su puerta de enlace.

   Puede configurar la puerta de enlace local con una prioridad más alta o más baja.

   - Para establecer la puerta de enlace local con una prioridad menor que la puerta de enlace de Prisma Access predeterminada, establezca la **Priority (Prioridad)** en **High (Alta)** o **Medium (Media)**.

     Si añade más puertas de enlace y desea establecer diferentes prioridades para cada una, puede establecer la **Priority (Prioridad)** en **High (Alta)**, **Medium (Media)**, **Low (Baja)** o **Lowest (Más baja)**.
   - Para configurar la puerta de enlace local con una prioridad más alta que la predeterminada, establezca la **Priority (Prioridad)** en **Highest (La más alta)**.

     Si desea configurar la puerta de enlace local con una prioridad más alta, también debe editar la puerta de enlace predeterminada de **Prisma Access** y configurar la prioridad con una **Priority (Prioridad)** que sea menor que **Highest (la más alta)**.

7. Seleccionar **Manual**.

   Al seleccionar esta casilla de verificación, los usuarios de GlobalProtect podrán seleccionar manualmente esta puerta de enlace externa en su aplicación GlobalProtect.

STEP 2 | Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 3 | **Push Config (Enviar configuración)**.

Integrar Prisma Access con puertas de enlace de GlobalProtect locales (Prisma Access (Managed by Panorama))

Para configurar una de estas implementaciones de Prisma Access híbridas, debe editar la configuración de GlobalProtect_Portal dentro de Mobile_User_Template para añadir sus puertas de enlace locales a las regiones apropiadas.

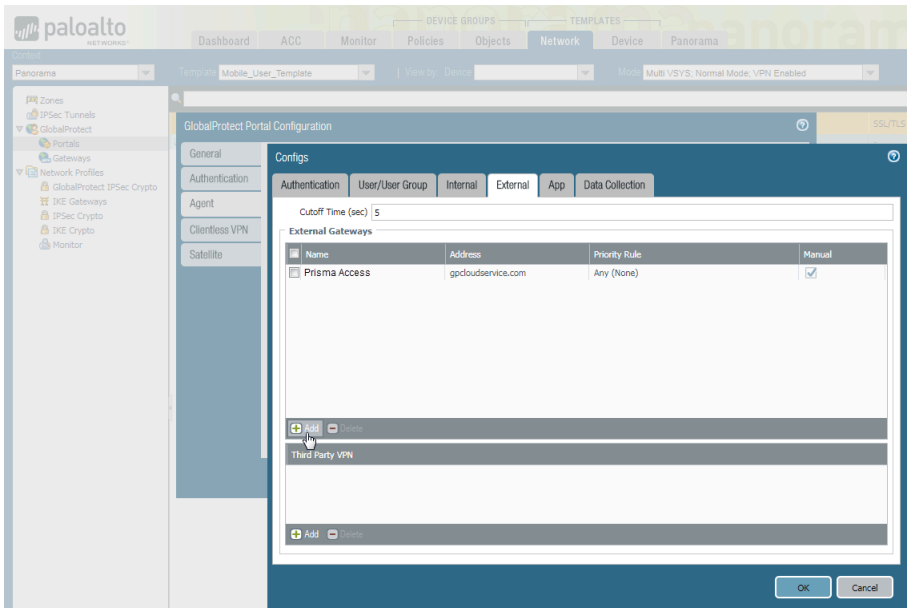
STEP 1 | Edite la configuración del portal de Prisma Access.

1. Para añadir una puerta de enlace existente a la lista de puertas de enlace disponibles, seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.
2. Seleccione **Mobile_User_Template** del menú desplegable **Template (Plantilla)**.
3. Seleccione **GlobalProtect_Portal** para editar la configuración del portal de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada su puerta de enlace local a la lista de puertas de enlace en la configuración del agente.

1. Seleccione la pestaña **Agent (Agente)** y seleccione la configuración del agente **DEFAULT (PREDETERMINADA)** o seleccione **Add (Añadir)** para añadir una nueva.
2. Seleccione la pestaña **External (Externa)** y **Add (Añadir)** para añadir su puerta de enlace local.



> *Si añade una nueva configuración de agente y desea añadir las puertas de enlace de Prisma Access a la lista de puertas de enlace externas en esa configuración, debe establecer el **Name (Nombre)** en **GP cloud service (Servicio en la nube de GP)** y la **Address (Dirección)** en **gpcloudservice.com**. Debe introducir estos valores exactamente como se muestran y no podrá usar ninguno de estos valores para puertas de enlace sin Prisma Access.*

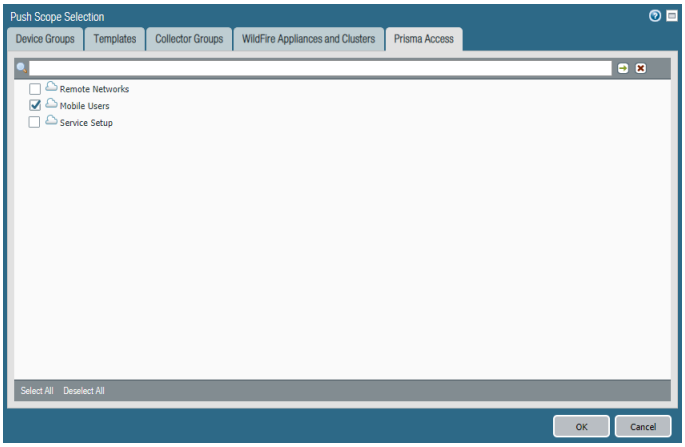
3. Introduzca el **Name (Nombre)** de la puerta de enlace y especifique el **FQDN** o la dirección **IP** de la puerta de enlace en el campo **Address (Dirección)**; este valor debe coincidir exactamente con el nombre común (CN) en el certificado de la puerta de enlace.
4. (Opcional) Si desea que los usuarios móviles solo se conecten a la puerta de enlace cuando estén en la región correspondiente, seleccione **Add (Añadir)** para añadir la **Source Region (Región de origen)** para restringir la puerta de enlace. Por ejemplo, si tiene una puerta de enlace en Francia, debería seleccionar FR (Francia). Si tiene una puerta de enlace en Suecia, debería seleccionar Suecia (SE).

   Una ventaja de esto es que los usuarios podrán entonces acceder a una puerta de enlace que les permitirá acceder a recursos de Internet en su propio idioma.
5. (Opcional) Establezca la prioridad de la puerta de enlace.
6. Configure otros ajustes de agente según sea necesario para completar la configuración del agente.
7. Haga clic en **ACEPTAR** para guardar la configuración de portal.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirme todos sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.
2. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y haga clic en **Edit Selections (Editar selecciones)**.
3. En la pestaña **Prisma Access**, asegúrese de que **Prisma Access for users (Prisma Access para usuarios)** está seleccionado y, a continuación, haga clic en **OK (Aceptar)**.



4. Haga clic en **Push (Enviar)**.

Establecer prioridad para Prisma Access y puertas de enlace locales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Puede seleccionar una puerta de enlace local que esté físicamente más cerca de sus usuarios móviles y permitir que los usuarios se conecten a una puerta de enlace diferente (ya sea local o en la nube) para garantizar un acceso seguro para los usuarios móviles si cambian de ubicación. También puede especificar prioridad para las puertas de enlace que están en el mismo país o en la misma área lingüística que sus usuarios móviles.

Si requiere que los usuarios se conecten a una puerta de enlace específica de Prisma Access, puede permitir que los usuarios móviles seleccionen manualmente puertas de enlace específicas de Prisma Access. Los usuarios móviles eligen una de las puertas de enlace de Prisma Access utilizando la aplicación GlobalProtect que está instalada en su dispositivo.

Complete el siguiente flujo de trabajo para configurar las prioridades de la puerta de enlace en Prisma Access.

- Establecer prioridades de puerta de enlace iguales para puertas de enlace locales y de Prisma Access
- Establezca una prioridad de puerta de enlace más alta para una puerta de enlace local
- Establecer prioridades más altas para varias puertas de enlace locales
- Configurar prioridades para Prisma Access y puertas de enlace locales

 ©2025 Palo Alto Networks, Inc.

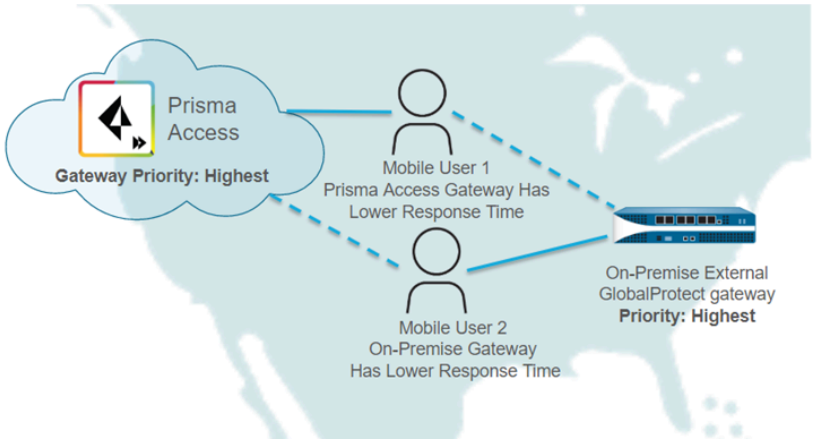
Establecer prioridades de puerta de enlace iguales para puertas de enlace locales y de Prisma Access

Para habilitar el acceso seguro para su fuerza laboral móvil, sin importar dónde se encuentren, puede establecer prioridades iguales para las puertas de enlace GlobalProtect locales y las puertas de enlace de Prisma Access. La aplicación GlobalProtect utiliza la Prioridad de puerta de enlace en una Configuración de Múltiples puerta de enlaces para determinar el puerta de enlace preferido.

Puede usar esta configuración si sus usuarios móviles están más cerca de una puerta de enlace local. Cuando los usuarios cambian de ubicación, la aplicación GlobalProtect elige otra puerta de enlace de Prisma Access (ya sea en las instalaciones o en la nube) basado en la mayor prioridad y el menor tiempo de respuesta.

La siguiente imagen muestra una configuración de muestra con dos usuarios móviles en América del Norte. Ha establecido la prioridad de la puerta de enlace en **Highest (Más alta)** tanto para las puertas de enlace como para las puertas de enlace locales de Prisma Access.

En este ejemplo, la aplicación GlobalProtect del Usuario 1 determina que la puerta de enlace de Prisma Access tiene un tiempo de respuesta más bajo que la puerta de enlace local, y la aplicación GlobalProtect del usuario 2 determina que la puerta de enlace local tiene un tiempo de respuesta más bajo. Dado que todas las puertas de enlace tienen la misma prioridad, el Usuario 1 se conecta a la puerta de enlace de Prisma Access y el Usuario 2 se conecta a la puerta de enlace local, basándose en el menor tiempo de respuesta.



Establezca una prioridad de puerta de enlace más alta para una puerta de enlace local

En situaciones en las que desee dirigir a los usuarios móviles a utilizar una puerta de enlace local en lugar de las puertas de enlace de Prisma Access, especifique las puertas de enlace locales con una región de origen y una prioridad más alta que la puerta de enlace de Prisma Access.

La siguiente imagen muestra una configuración de muestra para usuarios móviles en Indonesia. Para evitar la posibilidad de que los usuarios móviles se conecten a la puerta de enlace de Prisma Access más cercana en Singapur, establece la prioridad de la puerta de enlace en **Más alta** para la puerta de enlace local en Indonesia y establece la prioridad en **Media** para las puertas de enlace Prisma Access.

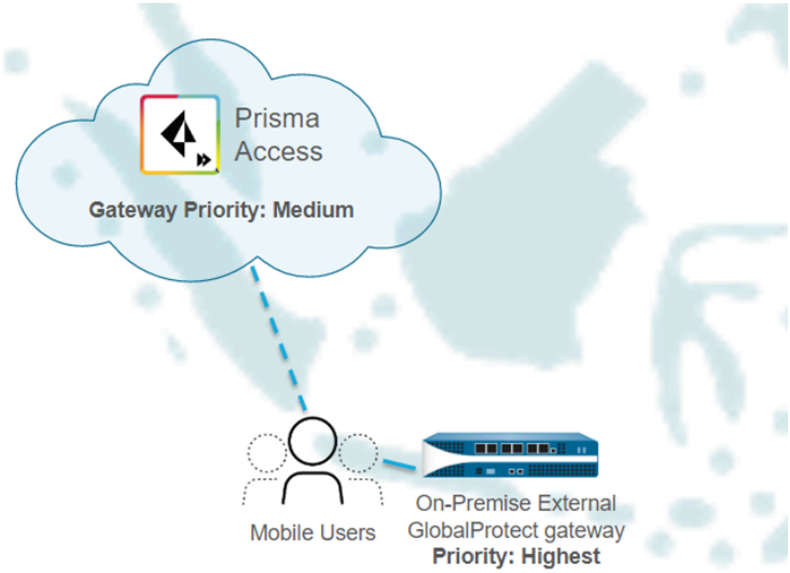
Este ejemplo también especifica una región de origen de Indonesia para la puerta de enlace local. Recomendamos especificar una región de origen por las siguientes razones:

- Especificar una región de origen para una puerta de enlace local permite a los usuarios de una región acceder a esa puerta de enlace y evita que los usuarios fuera de esa región se conecten a esa puerta de enlace. En este ejemplo, solo los usuarios móviles en Indonesia

 ©2025 Palo Alto Networks, Inc.

pueden conectarse a la puerta de enlace local con la región de origen de Indonesia, y la mayor prioridad significa que la puerta de enlace local tiene prioridad sobre las puertas de enlace de Prisma Access.

- Si establece una región de origen de **Any (Cualquiera)** para la puerta de enlace local en Indonesia, cada usuario móvil en su organización preferiría la puerta de enlace local en Indonesia, debido a su mayor prioridad y accesibilidad mundial. Esta configuración significa que los usuarios móviles podrían nunca conectarse a las puertas de enlace de Prisma Access.



Establecer prioridades más altas para varias puertas de enlace locales

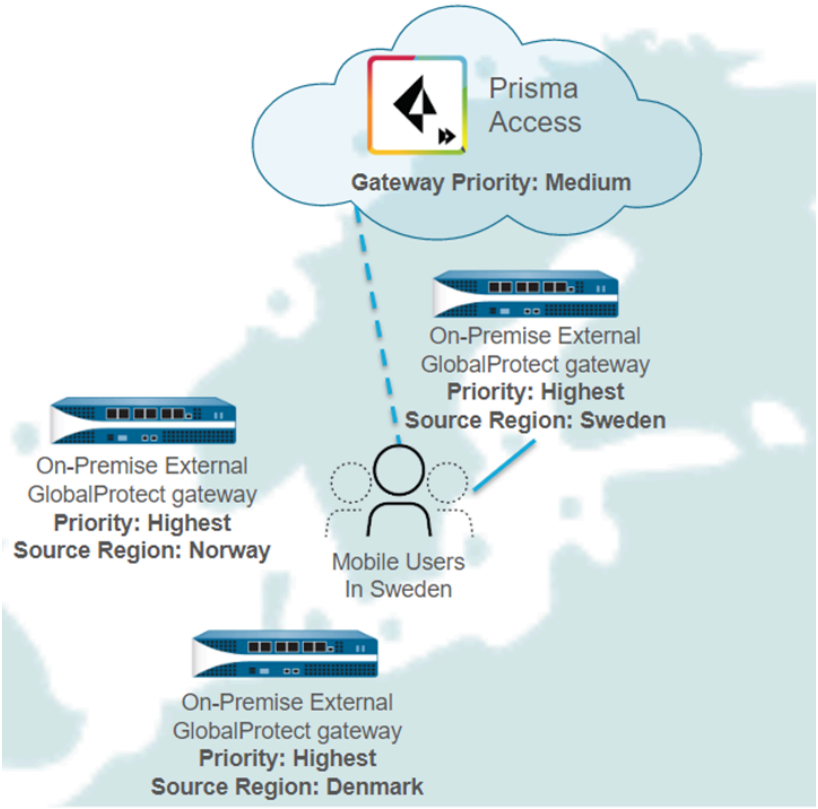
Para garantizar que el tráfico a Internet permanezca en regiones específicas de idioma, puede configurar múltiples puertas de enlace en múltiples regiones de origen, estableciendo la prioridad de las puertas de enlace locales en **Highest (Máxima)** y la prioridad de las puertas de enlace de Prisma Access en **Medium (Media)**.

La siguiente imagen muestra una configuración de muestra para usuarios móviles en Escandinavia. Mediante esta configuración, cuando los usuarios móviles acceden a sitios web de internet, los sitios web utilizan el conjunto de codificación de caracteres que es específico para sus idiomas.

En este ejemplo, usted configura puertas de enlace locales con regiones de origen en Dinamarca, Noruega y Suecia. Estableció la prioridad de esas puertas de enlaces en **Highest (La más alta)** y estableció la prioridad de las puertas de enlaces de Prisma Access en **Medium (Media)**. Especificar una región de origen para las puertas de enlace locales permite a los usuarios en esas regiones acceder a esas puertas de enlace y evita que los usuarios fuera de esas regiones se conecten a esas puertas de enlace.

En este ejemplo, la aplicación GlobalProtect para usuarios móviles en Suecia selecciona la puerta de enlace local en Suecia debido a la región de origen y a la mayor prioridad de la puerta de enlace.

©2025 Palo Alto Networks, Inc.



Configurar prioridades para Prisma Access y puertas de enlace locales

Utilice este flujo de trabajo para configurar prioridades para una implementación que utiliza puertas de enlace locales con Prisma Access.

STEP 1 | Inicie sesión en Prisma Access.

STEP 2 | Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** en la plantilla **Mobile_User_Template**.

STEP 3 | Haga clic en el nombre del portal en el campo **Name (Nombre)**.

STEP 4 | Haga clic en la pestaña **Agent (Agente)**.

STEP 5 | Haga clic en el nombre del agente para configurarlo.

El agente predeterminado se llama **DEFAULT (PREDETERMINADO)**.

STEP 6 | Haga clic en la pestaña **External (Externa)**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Establecer la prioridad de las puertas de enlace de Prisma Access.

1. Haga clic en el **GP cloud service (Servicio en la nube de GP)**.
2. Establezca la prioridad para su configuración preferida.
   - Para establecer prioridades de puerta de enlace iguales para las puertas de enlace locales y de Prisma Access, cambie la prioridad de **None (Ninguna)** a **Highest (la más alta)**.
   - Para establecer una prioridad de puerta de enlace más alta para una puerta de enlace local o establecer prioridades más altas para múltiples puertas de enlace locales, cambie la prioridad de **None (Ninguna)** a **Medium (Media)**.
3. Asegúrese de que la casilla de verificación **Manual** esté seleccionada.

   Marcar la casilla de verificación **Manual** asegura que los usuarios móviles puedan seleccionar una puerta de enlace específica de Prisma Access si es necesario.

   No añada una región de origen para las puertas de enlace de Prisma Access; cualquier región que especifique no se aplica a la configuración.
4. Haga clic en **OK (Aceptar)**.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Debe **Add (Añadir)** una o más puertas de enlace externas locales a su configuración.

1. 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 deberá ser lo suficientemente descriptivo para que los usuarios conozcan la ubicación de la puerta de enlace a la que están conectados.
2. Introduzca el FQDN o la dirección IP de la interfaz donde está configurada la puerta de enlace en el campo Dirección.

   Puede configurar una dirección IPv4 . La dirección que especifique debe coincidir exactamente con el nombre común (common name, CN) en el certificado del servidor de la puerta de enlace.
3. Añada una o más **Source Regions (Regiones de origen)** para la puerta de enlace, o seleccione **Any (Cualquiera)** para hacer que la puerta de enlace esté disponible para todas las regiones.

   *Si establece la prioridad de las puertas de enlace externas locales más alta que la de las puertas de enlace de Prisma Access, le recomendamos que especifique las regiones de origen para las puertas de enlace externas. Si especifica **Any (Cualquiera)** para la región, la aplicación GlobalProtect podría nunca seleccionar puertas de enlace de Prisma Access sobre las puertas de enlace locales debido a la mayor prioridad de las puertas de enlace locales.*
4. Seleccione la casilla de verificación **Manual** para permitir que los usuarios puedan cambiar manualmente a la puerta de enlace.
5. Establezca la **Priority (Prioridad)** de la puerta de enlace local en la **Highest (Más alta)** (la predeterminada).
6. Haga clic en **OK (Aceptar)**.

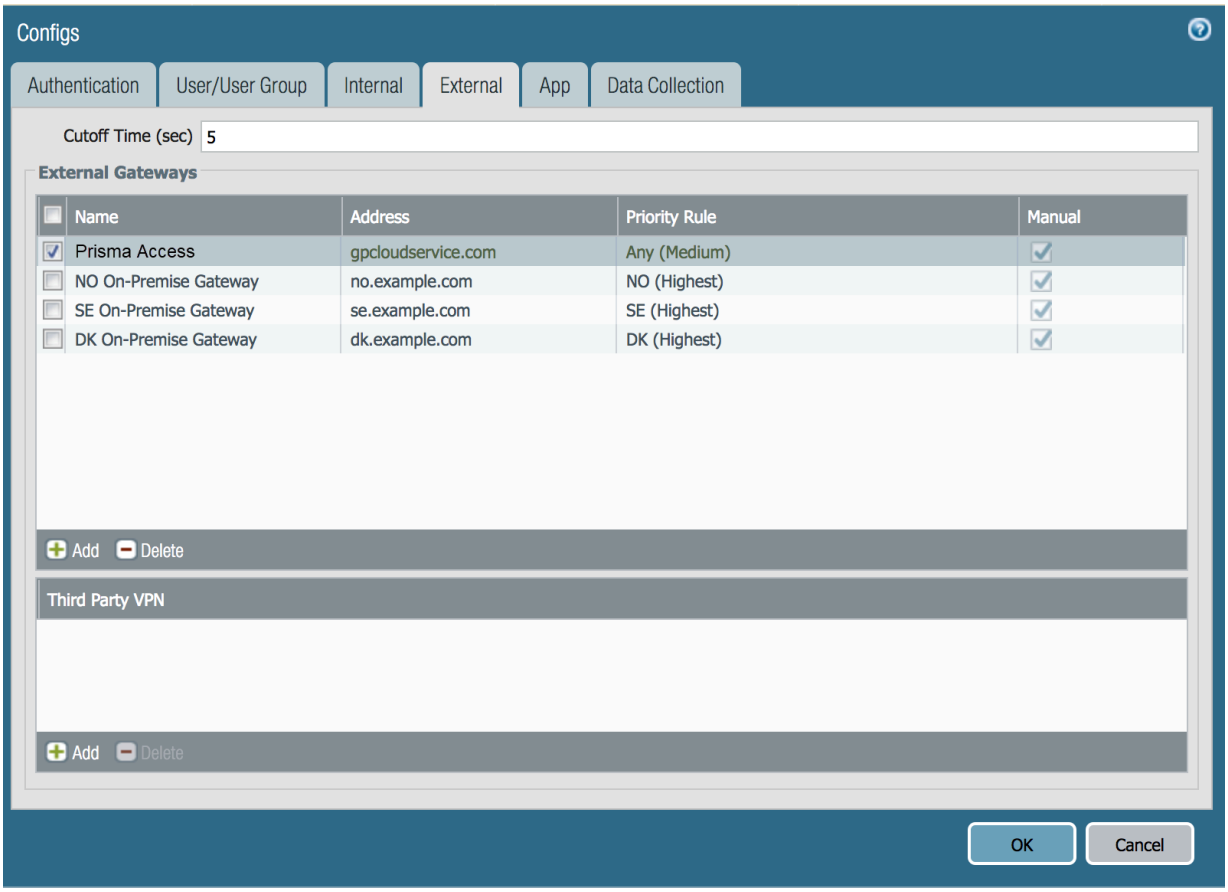
STEP 9 | (Opcional) Establezca la prioridad para las puertas de enlace adicionales repitiendo el Paso 8.

Asegúrese de especificar las regiones de origen correctas.

La siguiente imagen muestra una configuración de muestra con varias puertas de enlace que tienen regiones de origen en Noruega, Suecia y Dinamarca. Tenga en cuenta que la casilla de

 ©2025 Palo Alto Networks, Inc.

verificación **Manual** está seleccionada, lo que indica que un usuario móvil puede seleccionar manualmente cualquiera de estas puertas de enlace.



 ©2025 Palo Alto Networks, Inc.

Usuarios móviles: Proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Prisma Access por Palo Alto Networks, es una solución SSE (Security Service Edge) que ofrece funcionalidad de SWG en la nube de primera clase, incluyendo Advanced URL filtering, descifrado SSL, control de aplicaciones SaaS y Advanced Threat Prevention. Prisma Access operacionaliza implementaciones de seguridad de nueva generación con una infraestructura nativa de la nube omnipresente y siempre activa, completamente gestionada por Palo Alto Networks. Los usuarios móviles y los sitios remotos pueden acceder de forma segura a Internet y a aplicaciones SaaS de acuerdo con las políticas corporativas. Prisma Access ofrece opciones de conectividad flexibles: Archivos PAC, Agente, Sin Agente e IPSEC de sitio a sitio para garantizar que cualquier arquitectura de proxy en la nube heredada o alternativa pueda trasladarse a Prisma Access con cambios mínimos en la red.

Proxy explícito

Prisma Access proporciona una capacidad completa de puerta de enlace web segura (SWG) en la nube, incluyendo un método de conexión de proxy explícito basado en la nube. Si la red existente de su organización ya utiliza proxies explícitos e implementa archivos PAC en los endpoints de sus clientes, puede migrar sin problemas de las soluciones SWG basadas en proxies heredados de Prisma Access a la protección del tráfico de internet saliente de los usuarios móviles. También puede usar un proxy explícito si necesita usar un proxy por motivo de cumplimiento. El proxy explícito utiliza la licencia de Usuario móvil.

Si utiliza múltiples archivos PAC para definir cómo dirigir el tráfico web para diferentes usuarios o sistemas, Prisma Access le da la capacidad de asociar esos archivos PAC con Perfiles de Reenvío para que pueda usar varios archivos PAC a la vez. Además, en lugar de crear un archivo PAC, los Perfiles de reenvío le permiten configurar reglas de reenvío simples para definir la dirección de su tráfico web.

- Ubicaciones compatibles
- Proxy explícito con la aplicación GlobalProtect
  - GlobalProtect en modo proxy
  - GlobalProtect en modo Túnel y proxy
- Proxy explícito con archivos PAC
  - Configurar con SAML
  - Configurar con Kerberos

 ©2025 Palo Alto Networks, Inc.

- Perfiles de reenvío
  - Compatibilidad con varios archivos PAC
  - Reglas de reenvío
  - Perfiles de reenvío con GlobalProtect

Características de Proxy explícito de Prisma Access

Función	Descripción
App-ID	Clasifica continuamente todas las aplicaciones independientemente del puerto, el cifrado TLS/SSL o la técnica utilizada por un atacante para evadir la detección. A diferencia de las soluciones heredadas que dependen de las Capas 3 y 4 como las primeras capas de control antes de que se aplique la clasificación de aplicaciones, Prisma Access aplica App-ID junto con otros controles de la Capa 7, como User-ID.
User-ID	Se integra con una amplia gama de repositorios de identidad de usuarios para que sus políticas sigan a sus usuarios y grupos sin importar su ubicación.
Descifrado SSL	Inspecciona y aplica políticas al tráfico cifrado con TLS/SSL. Para la privacidad y el cumplimiento normativo, puede habilitar o deshabilitar el descifrado de manera flexible según la URL, la fuente, el destino, el usuario, el grupo de usuarios y el puerto.
Detección basada en IA/ML	Proporciona detección de ataques en línea sin firma y prevención de exploits de día cero. Prisma Access se adapta y proporciona protección instantánea en tiempo real frente a actualizaciones programadas. Previene hasta el 95 % de las amenazas desconocidas al instante, con una entrega de firmas de menos de 10 segundos, lo que resulta en una reducción del 99,5 % en los sistemas infectados.
DNS Security	Aplica protecciones en tiempo real y aprendizaje automático en línea para interrumpir las llamadas de retorno C2 y otros ataques que utilizan DNS. Integrado de forma nativa en Prisma Access, Advanced DNS Security proporciona protecciones automatizadas, evitando que los atacantes eludan las medidas de seguridad y elimina la necesidad de herramientas independientes o cambios en el enrutamiento DNS.
Filtrado de URL avanzado	Protección superior contra amenazas basadas en la web, como phishing, malware y C2, que combina potentes protecciones de base de datos con un motor de seguridad web impulsado por aprendizaje automático que categoriza y bloquea nuevas URL maliciosas en tiempo real. La protección contra phishing líder del sector aborda las causas más comunes de las brechas, permitiéndole recuperar el control de su tráfico web a través de controles detallados y configuraciones de políticas que automatizan las acciones de seguridad en función de los usuarios, las calificaciones de riesgo y las categorías de contenido.

 ©2025 Palo Alto Networks, Inc.

Función	Descripción
Advanced Threat Prevention	Detener amenazas de día cero, exploits conocidos, malware, spyware y comando y control (C2) maliciosos con la prevención de amenazas líder del sector. Prevenga un 60 % más de ataques de inyección desconocidos y un 48 % más de tráfico C2 altamente evasivo que los sistemas tradicionales de prevención de intrusiones.
Advanced WildFire	Asegure los archivos de forma segura al prevenir automáticamente malware conocido, desconocido y altamente evasivo 60 veces más rápido con el mayor motor de inteligencia de amenazas y prevención de malware del sector.
NG-CASB*	Obtenga visibilidad proactiva de SaaS, protección contra configuraciones incorrectas y protección de datos en tiempo real para una seguridad de SaaS de primera clase.
Prevención de pérdida de datos (DLP)*	La prevención de pérdida de datos (DLP, Data Loss Prevention) es un conjunto de herramientas y procesos que le permiten proteger la información confidencial frente al acceso no autorizado, al uso indebido, la extracción o el intercambio no autorizado. La DLP en Prisma Access permite hacer cumplir las políticas de seguridad de datos y prevenir la pérdida de datos sensibles entre usuarios móviles y redes remotas.
Soporte de Aislamiento remoto del navegador	A través de CloudBlades, se integra con nubes RBI de terceros aprovechando la categorización de URL y las funciones de reescritura de URL de NGFW existentes para redirigir el tráfico seleccionado/todo hacia Internet a la nube RBI. Esta capacidad proporciona una experiencia de usuario fluida mientras reenvía cierto tráfico (categorías desconocidas o de alto riesgo) a RBI para una inspección adicional, mientras que el tráfico restante puede ser inspeccionado por Prisma Access y salir directamente a Internet.
Generación de informes	Incluye, como estándar, un informe de uso de aplicación SaaS detallado y personalizable que proporciona información sobre todo el tráfico SaaS, tanto autorizado como no autorizado, en su red. También puede crear informes personalizados según sus necesidades y programarlos, descargarlos y compartirlos fácilmente con otros en su organización.
Autenticación de usuario	Admite todos los métodos de autenticación de PAN-OS existentes, incluidos Kerberos, RADIUS, SAML, LDAP, certificados de cliente y una base de datos de usuarios local. Con PAC solamente, compatible con Kerberos y SAML.
VPN IPsec de sitio a sitio	Admite túneles de sitio a sitio sobre IPv4 e IKEv1/IKEv2 para garantizar la compatibilidad. Para múltiples sitios de conexión, el enrutamiento ECMP puede proporcionar redundancia adicional y

 ©2025 Palo Alto Networks, Inc.

Función	Descripción
	eficiencia de costes al equilibrar las sesiones sobre las conexiones a Internet disponibles.
Registro de logs	Muestra el tráfico general, la aplicación, el usuario, la amenaza, la URL y el registro de logs de filtros de datos para facilitar la organización de datos a través de Strata Logging Service basado en la nube.
Perfiles de reenvío	Permite el uso de múltiples archivos PAC para diferentes grupos de usuarios o sistemas. También admite la creación de reglas de reenvío para definir la dirección del tráfico web y proporcionar una alternativa más sencilla para crear y mantener un archivo PAC.

Requiere una licencia de complemento

Para una descripción detallada de las características y capacidades del producto, consulte la hoja de datos de Prisma Access.

Directrices de la configuración de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Requisitos del sistema y funciones compatibles

Estos son los requisitos del sistema y las características compatibles para los diferentes métodos de conexión que puede usar con Proxy explícito.

	SAML sin agentes	Kerberos sin agente	Modo de proxy en el agente (requiere GP 6.2 o posterior)	Modo proxy para redes remotas
Aplicaciones y Soporte para Sistemas operativos				
Tipo de trafico	Solo tráfico de Internet y SaaS público	Solo tráfico de Internet y SaaS público	Solo tráfico de Internet y SaaS público	Solo tráfico de Internet y SaaS público
Compatibilidad con protocolos	HTTP o HTTPS con reconocimiento de proxy	HTTP o HTTPS con reconocimiento de proxy	HTTP o HTTPS con reconocimiento de proxy	HTTP o HTTPS con reconocimiento de proxy

 ©2025 Palo Alto Networks, Inc.

Canal de transporte a Prisma Access	Conexión HTTP	Conexión HTTP	Conexión HTTP dentro de TLS	Conexión HTTP dentro de IPSec desde la sucursal hasta el nodo de procesamiento de seguridad de red (SPN) remoto
Entornos compatibles	Windows, Mac, Linux, ChromeOS, VDI	Windows, Mac, Linux, ChromeOS, VDI	Windows y Mac	Windows, Mac, Linux, ChromeOS, VDI
Compatibilidad de aplicaciones	Aplicaciones HTTP(s) con reconocimiento de proxy	Cualquier aplicación que respete un archivo PAC o una configuración de proxy del sistema y admita Kerberos	Aplicaciones HTTP(s) con reconocimiento de proxy	Aplicaciones HTTP(s) con reconocimiento de proxy
Compatibilidad con navegadores	Chrome#, Edge, Firefox versiones 115 o posteriores	Chrome#, Edge, Firefox versiones 115 o posteriores	Chrome#, Edge, Firefox versiones 115 o posteriores*	Chrome#, Edge, Firefox versiones 115 o posteriores
O365 Support†	Aplicaciones de navegador y cliente	Aplicaciones de navegador y cliente	Aplicaciones de navegador y cliente	Aplicaciones de navegador y cliente
Identidad				
ID de usuario‡	Tráfico CORS descifrado y no HTTP	Todo el tráfico compatible	Todo el tráfico compatible	En función de si usa SAML o Kerberos: tráfico de usuario autenticado X no CORS/ descifrado
Autenticación compatible	SAML (cualquier IDP de SAML 2.0 o a través de CIE)	Kerberos	Todas las autenticaciones compatibles con GlobalProtect	SAML, Kerberos, Autenticado X basado en usuarios
Omitir autenticación	Por dominio y por IP de origen	Por dominio y por IP de origen	Por dominio	Por dominio y por IP de origen

 ©2025 Palo Alto Networks, Inc.

Directorio de grupos de usuarios	Todos los directorios compatibles con CIE	Todos los directorios compatibles con CIE	Todos los directorios compatibles con CIE	Todos los directorios compatibles con CIE
Licencia	Unidad de usuario móvil por usuario	Unidad de usuario móvil por usuario	Unidad de usuario móvil por usuario	Unidad de usuario móvil por usuario o dispositivo sin cabeza, y unidades NET para ancho de banda para redes remotas
Gestión				
Multitenant Panorama	Compatible con el primer inquilino	Compatible con el primer inquilino	Compatible con el primer inquilino	Compatible con el primer inquilino
Multitenant Cloud Management	Compatible	Compatible	Compatible	Compatible
Servicios de seguridad				
SaaS en línea	Compatible	Compatible	Compatible	Compatible
DLP	Compatible	Compatible	Compatible	Compatible
Seguridad DNS§	Compatible	Compatible	Compatible	Compatible
Filtrado de URL avanzado	Compatible	Compatible	Compatible	Compatible
Advanced WildFire	Compatible	Compatible	Compatible	Compatible
Advanced Threat Prevention	Compatible	Compatible	Compatible	Compatible
Aislamiento remoto del navegador	Compatible	Compatible	Compatible	Compatible

 ©2025 Palo Alto Networks, Inc.

Visibilidad y aplicación de IP privada	No compatible	No compatible	Compatible con sitios o sucursales conocidos	Compatible
NAT de salida	Compatible	Compatible	Compatible	Compatible
Acceso a aplicaciones privadas	No compatible	No compatible	Compatible a través de conexiones de servicio	No compatible
Todo el tráfico TCP	No compatible	No compatible	Compatible (con la versión 6.3.1 de GlobalProtect)	No compatible
Conector ZTNA	No compatible	No compatible	Compatible	No compatible
Colo Connect	No compatible	No compatible	Compatible	No compatible
Conexiones de servicio	Compatible	Compatible	Compatible	Compatible
Compatibilidad con HIP (modo túnel y proxy)	No compatible	No compatible	Compatible	No compatible

Para el navegador Chrome, siga las instrucciones que se enumeran a continuación para deshabilitar TLS 1.3 Kyber, si el descifrado está habilitado:

1. Abra el navegador Chrome.
2. Añada `chrome://flags/#enable-tls13-kyber` en la barra de direcciones y desactívelo.
3. Haga clic en **Relaunch (Reiniciar)**.

* Para el modo proxy en el agente, Firefox requiere el envío manual de una regla de política a través de la Mobile Device Management (Gestión de dispositivos móviles) que le indica que respete el proxy del sistema

† El proxy explícito solo admite tráfico HTTP, no UDP. Con SAML, el Proxy explícito no proporciona el ID de usuario para los flujos de aplicaciones cliente. Para el proxy de agente, debe usar un archivo PAC para enviar flujos de autenticación de aplicaciones cliente al proxy en la nube.

‡ No hay ningún ID de usuario disponible para la omisión de autenticación.

§ No se pueden aplicar perfiles de seguridad DNS a flujos de proxy explícito. En su lugar, bloquee dominios.

Consideraciones sobre la compatibilidad de aplicaciones

1. El proxy explícito no admite aplicaciones que necesiten afinidad de IP. La aplicación debe admitir el tráfico procedente de varias direcciones IP para una sesión de usuario determinada.

 ©2025 Palo Alto Networks, Inc.

2. El proxy explícito cambia los flujos de HTTP/2 descifrados a HTTP/1.
3. El proxy explícito no recupera listas dinámicas externas locales.
4. Solo SAML sin agente:
   1. Configure una política de descifrado SSL para permitir la omisión de autenticación por dominio para el proxy explícito basado en PAC sin agente con autenticación SAML

      El descifrado es necesario para que Prisma Access lea la cookie de estado de autenticación configurada por Prisma Access en el navegador del usuario móvil. Si no se aplica el descifrado, se permite el abuso del proxy explícito como proxy abierto que los atacantes pueden usar como servicio de reenvío para ataques de denegación de servicio.
   2. En los logs de tráfico, el proxy explícito mostrará los logs de tráfico de usuarios móviles sin descifrar y HTTP-CORS como usuarios autenticados por SWG.
   3. Tenga en cuenta los siguientes requisitos del navegador y las pautas de uso:
      - Si utiliza el Proxy explícito, no deshabilite las cookies en su navegador; si lo hace, no podrá navegar por ninguna página web.
      - Si usa un proxy explícito con Microsoft Edge, asegúrese de establecer **Settings (Configuración)** > **Privacy, Search, and Services (Privacidad, búsqueda y servicios)** > **Tracking prevention (Prevención de seguimiento)** en **Basic (Básico)**.

Requisitos de conectividad

Si los usuarios móviles se conectan desde sitios remotos o ubicaciones de oficinas centrales o centros de datos mediante un proxy explícito, el endpoint del usuario móvil debe poder llegar y enrutar al IdP, el FQDN de ACS, la URL de proxy explícita y la URL del archivo PAC alojado por Prisma Access.

Requisitos y directrices del archivo PAC: siga las instrucciones de Directrices del archivo PAC al configurar el archivo PAC para usarlo con Proxy explícito.

Directrices de encadenamiento de proxy: si utiliza el encadenamiento de proxy desde un proxy de terceros a un proxy explícito, especifique el **Explicit Proxy URL (URL de proxy explícito** en el proxy de terceros para reenviar el tráfico al proxy explícito

Soporte local: Proxy explícito, Explicit Proxy, es una solución de proxy basada en la nube y no un producto local. En el caso de una solución de proxy local, configure un proxy web PAN-OS.

GlobalProtect en modo proxy

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) Si desea utilizar esta función en su entorno de Prisma Access, póngase en contacto con su equipo de cuenta para obtener más información.	• Prisma Access 5.2 • Versión 6.2 de la aplicación GlobalProtect para Windows o macOS • Versión de publicación de contenido 8700-7994 • Licencia de usuario móvil de Prisma Access

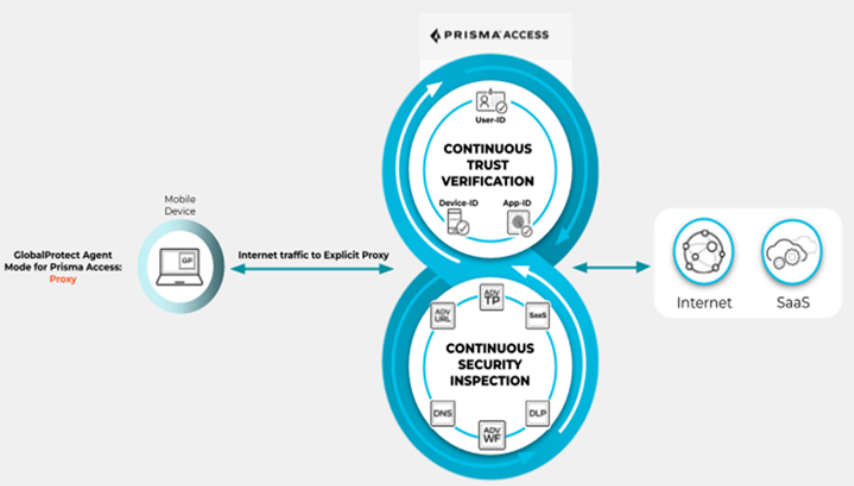
 ©2025 Palo Alto Networks, Inc.

Con el modo **Proxy**, la aplicación GlobalProtect proporciona seguridad en Internet siempre activa. En este modo, la aplicación GlobalProtect dirige el tráfico a Prisma Access basado en las reglas de reenvío y la lógica del archivo PAC, alojado en Prisma Access o en su entorno. Esto es útil si tiene una arquitectura de proxy existente (heredada) o si tiene la necesidad de mantener la arquitectura de proxy por motivos normativos o de cumplimiento.

La función de proxy basado en agentes facilita la coexistencia y la interoperabilidad de la aplicación GlobalProtect con VPN de terceros, en la que puede proteger el tráfico de Internet de sus usuarios móviles a través de la aplicación GlobalProtect al proxy explícito y utilizar la VPN de terceros de su elección para proteger el acceso a aplicaciones privadas.

Necesita Strata Cloud Manager y la versión 6.3.0 del agente de GlobalProtect para que el canal Proxy de GlobalProtect admita todas las conexiones TCP IPv4, incluido el tráfico no compatible con proxy. Para garantizar una funcionalidad perfecta, el DNS configurado en los endpoints deben ser capaces de resolver el FQDN de destino.

En este escenario, la aplicación GlobalProtect envía el tráfico de Internet a Prisma Access en función de las reglas de archivo PAC que defina, mientras que el punto de conexión enruta el acceso a sus aplicaciones privadas a través de una VPN de terceros mediante un túnel IPSec/TLS.



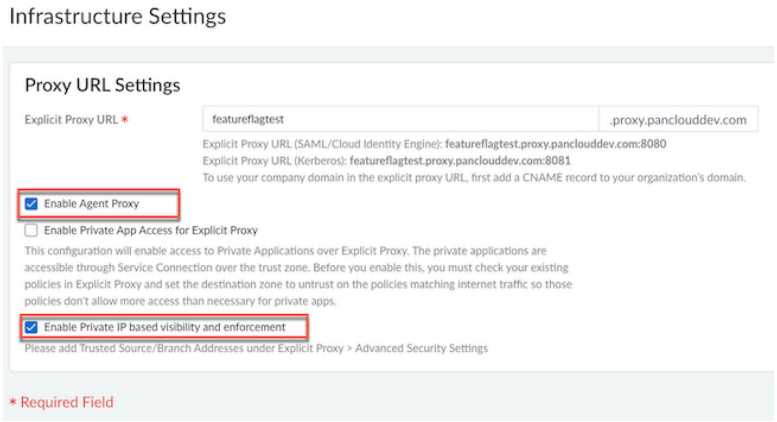
- Strata Cloud Manager
- Panorama

GlobalProtect en modo proxy (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Habilite la funcionalidad de proxy basada en agente para usuarios móviles en Prisma Access.

1. Habilite el proxy explícito.
   1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** y haga clic en **Explicit Proxy Setup (Configuración de proxy explícito)**.
   2. En el área Configuración de infraestructura, haga clic en **Setup Proxy Settings (Configurar la configuración del proxy)** y especifique una **Explicit Proxy URL (URL de proxy explícito)**.
2. Seleccione **Enable Agent Proxy (Habilitar proxy de agente)**y opcionalmente **Enable Private IP based visibility and enforcement (Habilitar la visibilidad y el cumplimiento basados en IP privadas)** y haga clic en **Save (Guardar)**.



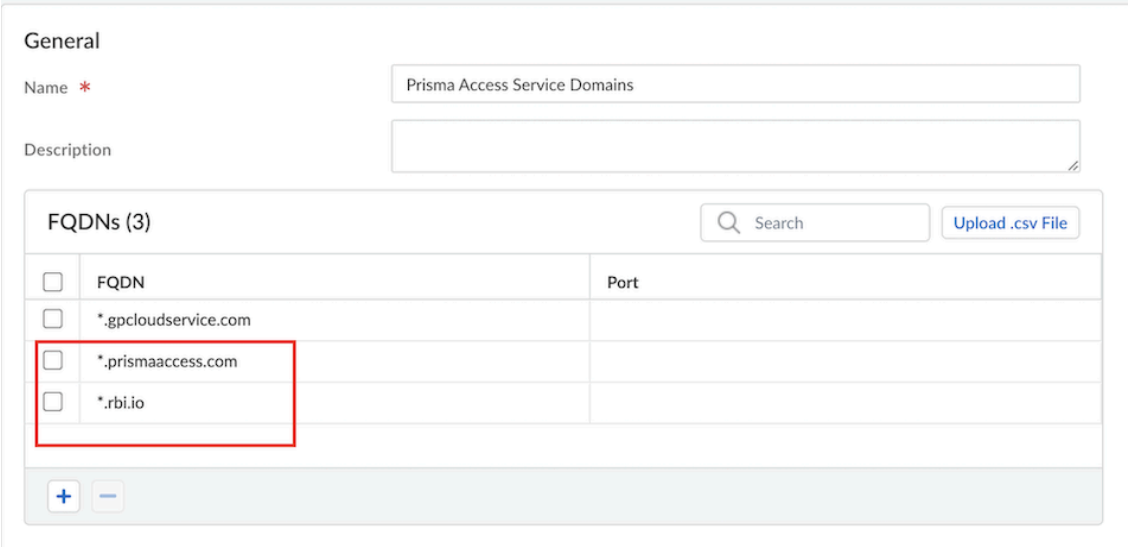
3. Seleccione las Prisma Access locations (Ubicaciones de Prisma Access) donde desea admitir usuarios móviles.

   Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a los usuarios finales. Si una ubicación no está disponible en el

 ©2025 Palo Alto Networks, Inc.

país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a los usuarios móviles.

4. Crear un Perfil de reenvío para definir el tráfico que desea enviar a través de Proxy explícito. Al configurar el perfil de reenvío, omita los dominios *.prismaaccess.com y *.gpcloudservice.com.



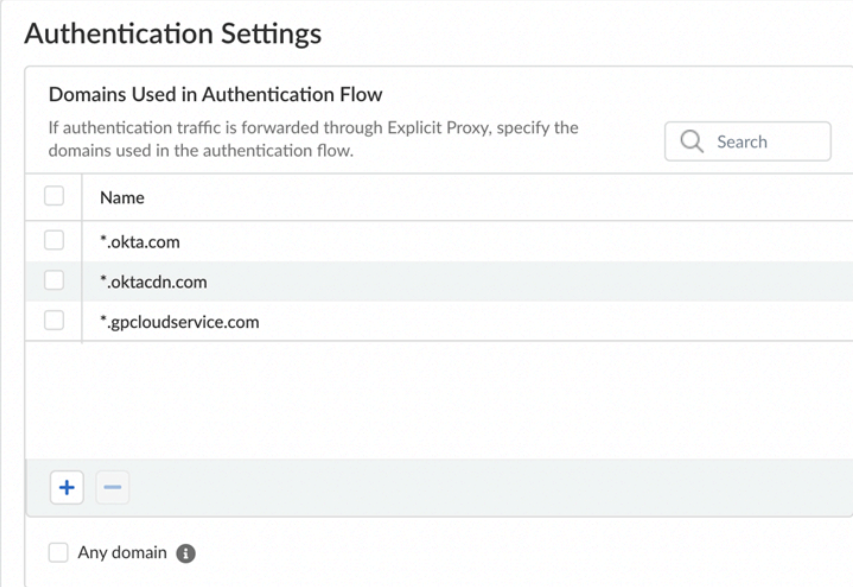
5. Adjunte el perfil de reenvío a la configuración de la aplicación de GlobalProtect.
6. Seleccione **Workflows (Flujos de trabajo)** > **Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Advanced Security Settings (Configuración de**

 ©2025 Palo Alto Networks, Inc.

seguridad avanzada) > **Authentication Settings (Configuración de autenticación)** y añada los dominios que necesita omitir.

Todas las solicitudes al proxy se someten a autenticación. Sin embargo, si está pasando flujos de IdP a través del proxy, debe omitirlos para que la autenticación se realice correctamente.

En este ejemplo, estamos omitiendo el portal de GlobalProtect y Okta, pero personalícelos según los IdP que utiliza.

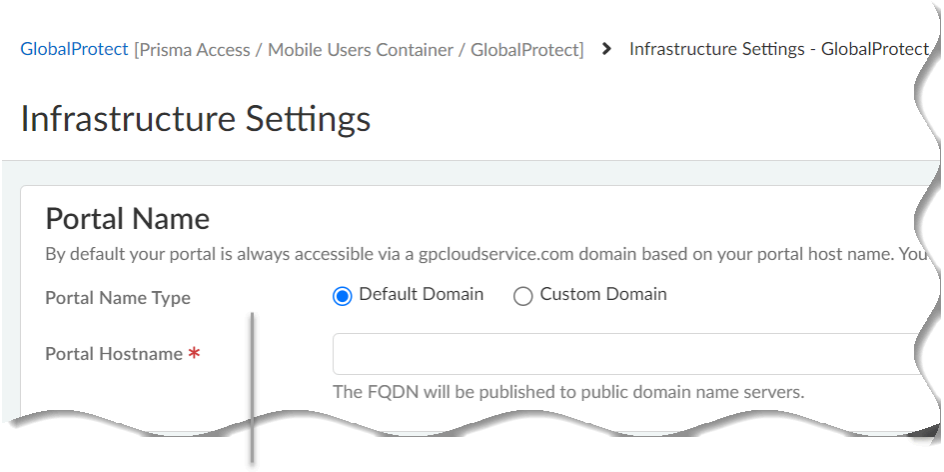


STEP 2 | Configure el portal de GlobalProtect, la autenticación y configure el modo de proxy para la aplicación de GlobalProtect.

1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** > **Infrastructure**

 ©2025 Palo Alto Networks, Inc.

Settings (Configuración de la infraestructura) y especifique el **Portal Name (Nombre del portal)**.



GlobalProtect Infrastructure Settings

- **Default Domain (Dominio predeterminado)**: si selecciona esta opción, el nombre de host del portal utiliza el nombre de dominio predeterminado: `.gpcloudservice.com`. En este caso, basta con introducir un **Portal Hostname (Nombre de host del portal)** para anexar al nombre de dominio predeterminado. Prisma Access para usuarios creará automáticamente los certificados necesarios y publicará el nombre de host en servidores DNS públicos.
- **Custom Domain (Dominio personalizado)**: también puede personalizar la dirección del portal si desea que el dominio del nombre de host del portal coincida con el nombre de dominio de su empresa (por ejemplo, myportal.mydomain.com).

2. Permitir a los usuarios móviles autenticarse en Prisma Access.
3. Habilite el modo de proxy de GlobalProtect para Prisma Access en la configuración de la aplicación GlobalProtect para enviar tráfico de Internet al proxy basado en agente.

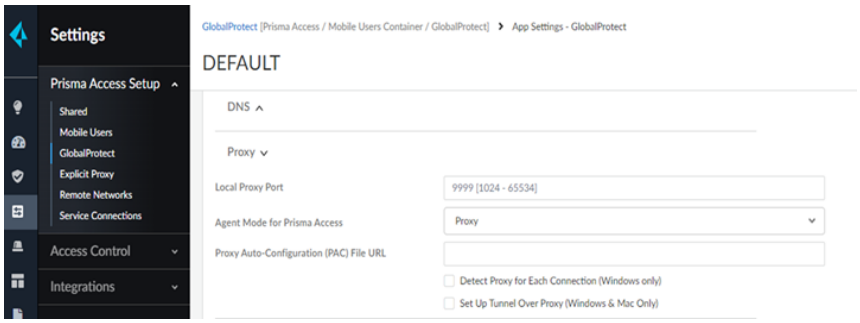
   El método de conexión de GlobalProtect no se aplica en modo proxy, ya que siempre está activado.

   - Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect**.
   - En el **GlobalProtect App (Aplicación GlobalProtect)**, haga clic en **Default (Predeterminado)** para personalizar la configuración de la aplicación o seleccione **Add App Settings (Añadir configuración de la aplicación)** para añadir una nueva configuración.
   - Haga clic en **Show Advanced Options (Mostrar opciones avanzadas)** y en **App Configuration (Configuración de la aplicación)**.
   - Establezca **Agent Mode for Prisma Access (Modo de agente para Prisma Access)** en **Proxy** para indicar a la aplicación de GlobalProtect que envíe el tráfico de Internet al proxy explícito en Prisma Access.
   - (Opcional) Configure el puerto proxy local. El intervalo de puertos es de 1024 a 65534 y el puerto predeterminado es 9999. Si el puerto predeterminado no está

 ©2025 Palo Alto Networks, Inc.

disponible, GlobalProtect intentará otros 10 puertos en el rango de 9999 a 10009 y utilizará el puerto que esté disponible. También puede elegir su propio número de puerto dentro del rango.

- (Opcional) Configure la URL del archivo de configuración automática de proxy (PAC) si desea enviar la nueva URL de PAC para la configuración del proxy al endpoint. La URL de PAC se envía al endpoint una vez que el usuario se conecta. Cuando el usuario desconecta la aplicación GlobalProtect, las configuraciones del proxy de endpoint se desactivan automáticamente y vuelven a la configuración anterior.
- (Opcional) Habilite Allow User to Rediscover Network (Permitir que el usuario redescubra la red) si desea que el usuario compruebe si hay nuevas configuraciones en el portal.
- (Opcional) Configure GlobalProtect App Config Refresh Interval (hours) [Intervalo de actualización de configuración para la aplicación de GlobalProtect (horas)]. De forma predeterminada, el cliente de GlobalProtect actualiza la configuración del portal almacenada en caché cada 24 horas. Puede cambiar el intervalo de actualización en función de los requisitos de su empresa.
- Deshabilite **Set Up Tunnel Over Proxy (Windows & Mac Only) [Configurar el túnel sobre proxy (Solo Windows y Mac)]**

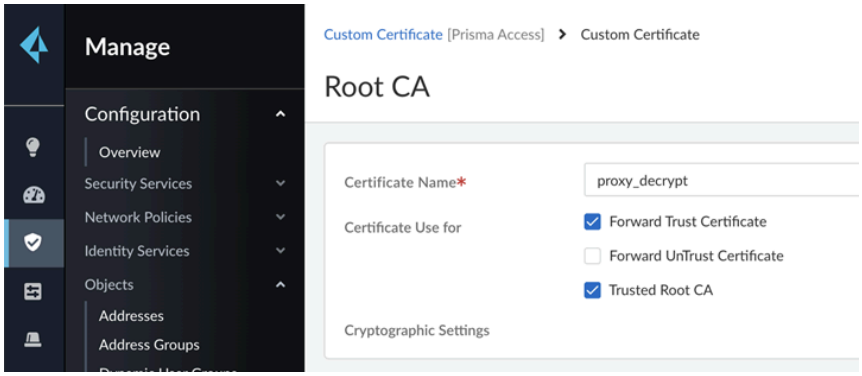


4. Habilite la seguridad de Internet siempre activa configurando los siguientes ajustes en la página **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Aplicación de GlobalProtect)** > **Add App Settings (Añadir configuración de la aplicación)**:
   1. Establezca Disable GlobalProtect (Deshabilitar GlobalProtect) para **Disallow (Prohibir)**, **Allow with Passcode (Permitir con código de acceso)** o **Allow with Ticket (Permitir con ticket de incidencia)**.
   2. Deshabilite Permitir al usuario cerrar sesión desde la aplicación de GlobalProtect

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure el descifrado para el tráfico de Proxy explícito.

- Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y (NGFW y Prisma Access)** > **Security Services (Servicios de Seguridad)** > **Decryption (Descifrado)**.
- Si habilita el descifrado, asegúrese de configurar el certificado de descifrado como una CA raíz de confianza.



STEP 4 | Configure las reglas de la política de seguridad para el tráfico de proxy explícito.

- Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de Seguridad)** > **Security Policy (Política de seguridad)**.
- Siga las Prácticas recomendadas de la política de seguridad de puerta de enlace de Internet.

STEP 5 | (Opcional) Configure la aplicación GlobalProtect en modo proxy en una red de ruta no predeterminada.

- (Opcional) Aloje un archivo PAC internamente y añada el FQDN de proxy explícito de Prisma Access como proxy en el archivo PAC, o hospede el archivo PAC en un Perfil de reenvío y añada rutas en su red para Direcciones IP del servicio PAC.
- En el archivo PAC, reenvíe la URL del IdP y URL del portal de Prisma Access al proxy explícito.
- En Proxy explícito, excluya el IdP y la URL del portal de la configuración de autenticación. Añada el IdP y la URL del portal al dominio utilizado en los flujos de autenticación.
- Configure rutas al FQDN de proxy explícito o a las direcciones IP en dispositivos perimetrales para permitir que los usuarios accedan a Internet a través del proxy explícito.
- (Opcional) Añada registros DNS para resolver el problema Prisma Access FQDN de proxy explícito a una dirección IP interna si los usuarios no pueden resolver dominios públicos en la red de sucursal y añadir NAT de destino para la dirección IP interna al FQDN de proxy explícito o a la dirección IP.

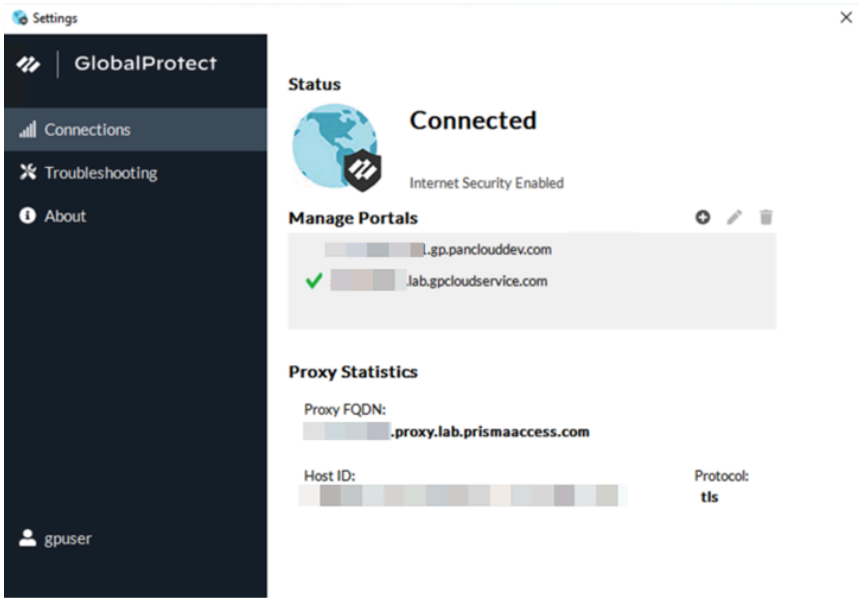
STEP 6 | Haga clic en **Save (Guardar)** y **Push Config (Enviar configuración)** a **GlobalProtect** y **Proxy explícito**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Verifique y solucione problemas de la implementación del proxy de agente.

1. Verifique la información sobre su conexión de red en la pestaña **Connections (Conexiones)** de la aplicación GlobalProtect en **Settings (Configuración)**.

   1. Abra la aplicación GlobalProtect.
   2. Seleccione **Settings (Configuración)** para abrir el panel de configuración de GlobalProtect y, a continuación, seleccione **Connections (Conexiones)**.



2. Consultar y recopilar logs de GlobalProtect

   Consulte el log de PanGPS para verificar la configuración del modo proxy en el portal de GlobalProtect.

   Puede verificar que el modo Proxy está configurado buscando el siguiente evento en el log de PanGPS:

   ```
   OnProxyAgentMode: modo solo proxy
   ```

   Para ver los logs de GlobalProtect en , seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)** y:

   - **Protección global**, para logs de autenticación
   - **Traffic (Tráfico)** y **Decryption (Descifrado)** para los logs de acceso de usuarios

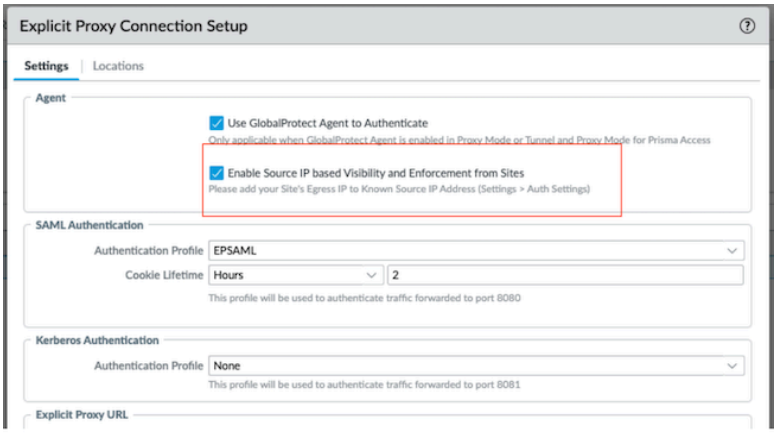
GlobalProtect en modo proxy (Panorama)

Si convierte una implementación de Prisma Access (Managed by Panorama) de inquilino único a varios inquilinos, solo el primer inquilino (el inquilino que migró) admite esta característica. Además, en este primer inquilino, debe configurar las reglas de la política en el Explicit_Proxy_Device_Group predefinido en lugar de en un grupo de dispositivos personalizado. Los inquilinos posteriores que cree para la implementación de varios inquilinos después de la primera no admiten esta característica.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Habilite la funcionalidad de proxy basada en agente para usuarios móviles.

1. Habilitar el proxy explícito.
   1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: proxy explícito)**.
   2. Seleccione **Configure (Configurar)** la configuración explícita del proxy para especificar un **Explicit Proxy URL (URL de proxy explícito**.
2. Seleccione **Use GlobalProtect app to Authenticate (Utilizar la aplicación GlobalProtect para autenticarse)** para habilitar la funcionalidad de proxy basado en agente, y opcionalmente **Enable Source IP based Visibility and Enforcement from Sites (Habilitar la visibilidad y el cumplimiento de los sitios basados en IP de origen)**.



3. Introduzca la URL del **PAC (Proxy Auto-Configuration) File (Archivo PAC (configuración automática de proxy)**. Asegúrese de introducir un puerto de 8080 en el archivo PAC.
   - Asegúrese de introducir un puerto de 8080 en el archivo PAC.
   - La Declaración proxy en el archivo PAC debe usar el FQDN de Prisma Access que configuró anteriormente.
   - El archivo PAC debe estar configurado para omitir el tráfico de VPN de terceros.

   Ejemplo de archivo PAC:

```
function FindProxyForURL (url, host) { /* Bypass localhost
 and Private IPs * / var resolved_ ip = dnsResolve (host) ;
 if (isplainHostName (host) || shExpMatch (host,"* ,local")
 || isInNet (resolved_ip,"10.0.0.0", "255.0.0.0") ||
 isInNet (resolved ip,"172.16.0.0","255.240.0.0") ||
 isInNet (resolved_ip,"192.168.0.0","255.255.0.0") ||
 isInNet (resolved ip, "127.0.0.0", "255.255.255.0" ))
 return "DIRECT"; /* Bypass Non-HTTP * / if (url.substring
 (0,4) == "ftp: ") return "DIRECT”; /* Bypass VPN */ if
 (shExpMatch (host, "vpn. acme.com") || shExpMatch (host,
 "gateway. acme.com" )) return "DIRECT"; /* Bypass Private
 Apps */ if (shExpMatch (host,"internalapps. acme.com" ) )
 return "DIRECT"; /* Forward to  */ return "PROXY acme-
demo.proxy.prismaaccess.com: 8080";}
```

4. Seleccione la opción **Connection Name (Nombre de la conexión)** para la configuración de proxy explícito que ha configurado.

 ©2025 Palo Alto Networks, Inc.

5. Seleccione las **Locations (Ubicaciones)** y las regiones en las que desea implementar el proxy explícito para usuarios móviles.

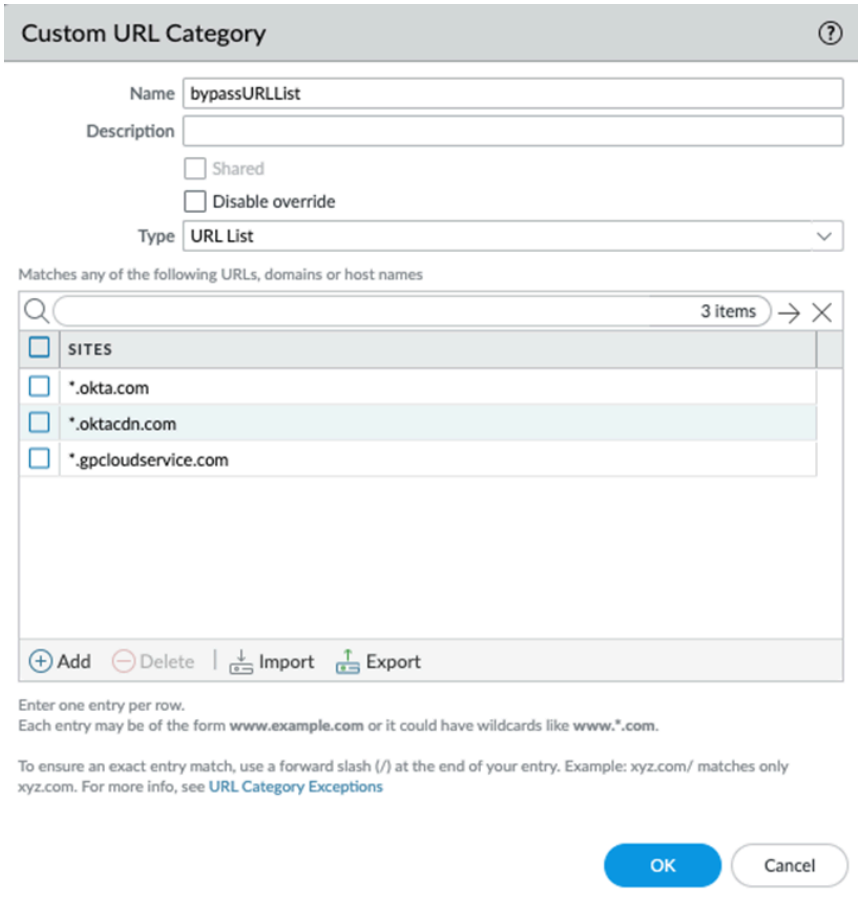
   Prisma Access añade un nodo proxy en cada ubicación que usted seleccione. El proxy explícito es compatible con un subconjunto de todas las ubicaciones de Prisma Access. Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a sus usuarios o en el mismo país que sus usuarios. Si una ubicación no está disponible en el país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a los usuarios móviles.

STEP 2 | Omita los proveedores de identidad (IDP).

Se autentican todas las solicitudes al proxy. Sin embargo, si está pasando flujos de IDP a través del proxy, debe omitirlos para que la autenticación se realice correctamente.

En este ejemplo, estamos omitiendo el portal de GlobalProtect y Okta, pero personalícelos según los IDP que utiliza.

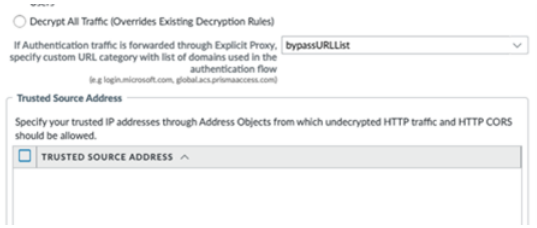
1. Con el **Explicit_Proxy_Device_Group** seleccionado, seleccione **Object (Objeto)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y cree una categoría de URL personalizada.
2. En la categoría de URL personalizada, añada todos los dominios FQDN que se deben omitir de la autenticación EP.



3. Seleccione **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)** > **Explicit Proxy (Proxy explícito)** > **Settings**

 ©2025 Palo Alto Networks, Inc.

(Configuración) > **Authentication Settings (Configuración de autenticación)** y adjunte la categoría de URL personalizada.



4. Confirmar y enviar al **Explicit_Proxy_Device_Group**.

STEP 3 | Configure el Portal de GlobalProtect.

En el modo Proxy, el método de conexión que establezca no cambia el comportamiento de la funcionalidad de proxy. Incluso si establece un método de conexión a petición, todo el tráfico vinculado a Internet seguirá manteniendo la comunicación proxy para la seguridad de Internet siempre activa.

1. En la sección de Incorporación, haga clic en **Configure (Configurar)**.
2. En la pestaña **General**, especifique el **Portal Name Type (Tipo de nombre del portal)**:

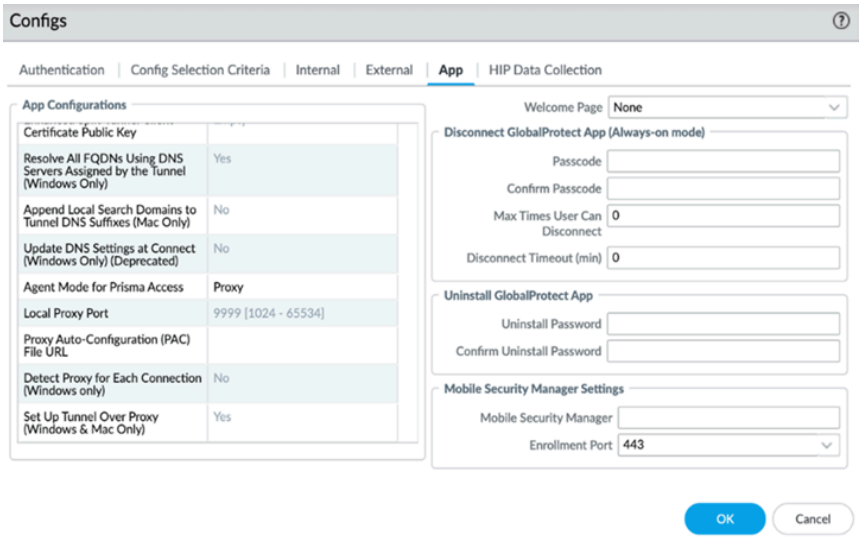
   Use Default Domain— (Usar dominio predeterminado:) Si selecciona esta opción, el nombre de host del portal utiliza el nombre de dominio predeterminado: .gpcloudservice.com. En este caso, simplemente introduzca un nombre de host de Portal para añadir al nombre de dominio predeterminado. Prisma Access creará automáticamente los certificados necesarios y se publicará el nombre de host en los servidores DNS públicos.

   Use Company Domain (Utilizar dominio de la empresa): seleccione esta opción si desea que el dominio en el nombre de host del portal coincida con el nombre de dominio de su empresa (por ejemplo, myportal.mydomain.com).
3. Seleccione un **Authentication Profile (Perfil de autenticación)** que especifica cómo Prisma Access debe autenticar a los usuarios móviles o crear uno nuevo.
4. (Opcional) Seleccione un **Authentication Override Certificate (Certificado de anulación de autenticación)** para cifrar las cookies seguras que los usuarios móviles utilizan para autenticarse en el portal y la puerta de enlace.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Habilite el modo proxy en 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 la pestaña **Agent (Agente)**, seleccione **App (Aplicación)**.
4. En el área de Configuraciones de la aplicación, establezca el **Agent Mode for Prisma Access (Modo de agente para Prisma Access)** en **Proxy** para enviar tráfico de Internet al proxy basado en agentes de GlobalProtect



STEP 5 | Realizar configuraciones opcionales.

1. (Opcional) Configure el puerto proxy local. El intervalo de puertos es de 1024 a 65534 y el puerto predeterminado es 9999. Si el puerto predeterminado no está disponible, GlobalProtect intentará otros 10 puertos en el rango de 9999 a 10009 y utilizará el puerto que esté disponible. También puede elegir su propio número de puerto dentro del rango.
2. (Opcional) Configure la URL del archivo de configuración automática de proxy (PAC) si desea enviar una URL de PAC personalizada para la configuración del proxy al endpoint. La URL de PAC se envía al endpoint una vez que el usuario se conecta. Cuando el usuario desconecta la aplicación GlobalProtect, las configuraciones del proxy de endpoint se desactivan automáticamente y vuelven a la configuración anterior.
3. (Opcional) Habilite Allow User to Rediscover Network (Permitir que el usuario redescubra la red) si desea que el usuario compruebe si hay nuevas configuraciones en el portal.
4. (Opcional) Configure GlobalProtect App Config Refresh Interval (hours) [Intervalo de actualización de configuración para la aplicación de GlobalProtect (horas)]. De forma predeterminada, el cliente de GlobalProtect actualiza la configuración del portal almacenada en caché cada 24 horas. Puede cambiar el intervalo de actualización en función de los requisitos de su empresa.

 ©2025 Palo Alto Networks, Inc.

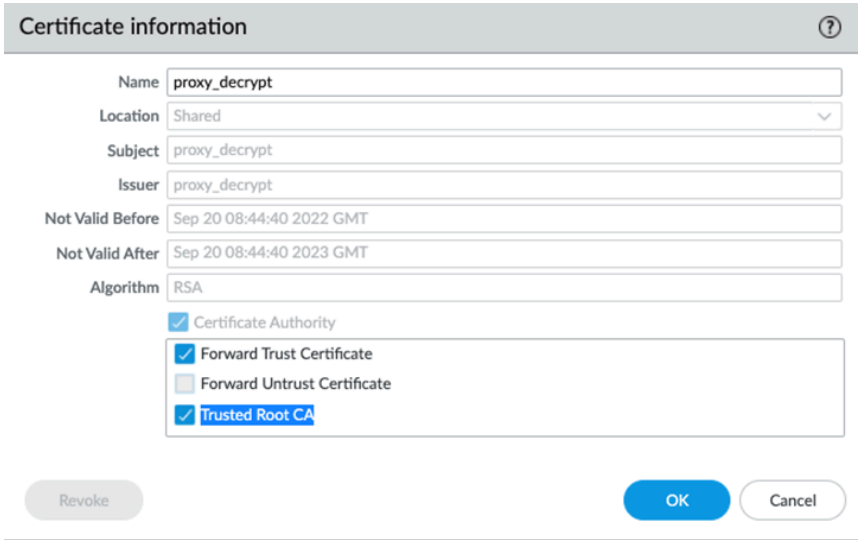
STEP 6 | Habilite la seguridad de internet Siempre activa mediante la configuración de los siguientes ajustes:

1. Establezca Permitir que el usuario deshabilite GlobalProtect en **Disallow (Prohibir)**, **Allow with Passcode (Permitir con código de acceso)**o **Allow with Ticket (Permitir con ticket de incidencia)**.
2. Establezca Permitir al usuario cerrar sesión desde la aplicación de GlobalProtect en **No**.

STEP 7 | (Opcional) Configurar la política de descifrado para el tráfico de proxy explícito.

Si habilita el descifrado, asegúrese de que el certificado de descifrado también esté configurado como una CA raíz de confianza.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión del certificado)** > **Certificates (Certificados)** y cree un certificado que sea una CA raíz de confianza y un certificado de reenvío fiable.



2. Crea una regla de descifrado en**Explicit_Proxy_Device Group** con proxy de reenvío SSL.

STEP 8 | Configure las reglas de la política de seguridad para el tráfico de proxy explícito.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Establezca el **Grupo de dispositivos** en **Explicit_Proxy_Device_Group**.
3. Siga las Prácticas recomendadas de la política de seguridad de puerta de enlace de Internet.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | (Opcional) Configure la aplicación de GlobalProtect en modo proxy en una red de ruta no predeterminada.

- (Opcional) Alojar un archivo PAC internamente y añadir el FQDN de proxy explícito de Prisma Access como proxy en el archivo PAC, o hospede el archivo PAC en un Perfil de reenvío y añada rutas en su red para Direcciones IP del servicio PAC.
- En el archivo PAC, reenvíe la URL del IDP y URL del portal de Prisma Access al proxy explícito.
- En el proxy explícito, excluya el IDP y la URL del portal de la configuración de autenticaciones. Añada el IDP y la URL del portal al dominio utilizado en los flujos de autenticación.
- Establezca rutas al FQDN de proxy explícito o a las direcciones IP en los dispositivos perimetrales para permitir que los usuarios accedan a Internet a través del proxy explícito.
- (Opcional) Añada registros DNS para resolver el FQDN de proxy explícito de Prisma Access a una dirección IP interna si los usuarios no pueden resolver dominios públicos en la red de sucursal y añada NAT de destino para la dirección IP interna al FQDN de proxy explícito o a la dirección IP.

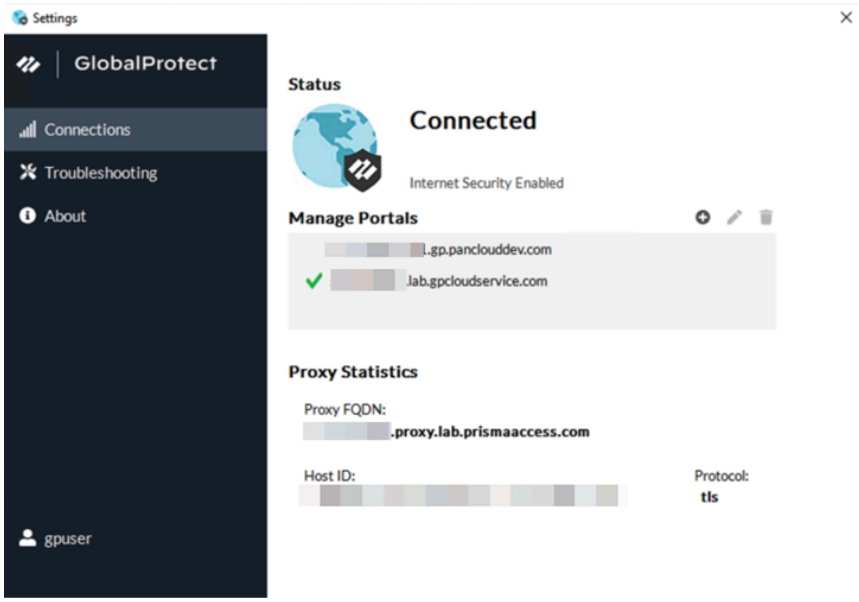
STEP 10 | **Commit (Confirmar)** los cambios en Panorama y **Commit and Push (Confirmar y enviar)** los cambios de configuración a los **Mobile Users (Usuarios móviles)** y **Explicit Proxy (Proxy explícito)** de Prisma Access .

 ©2025 Palo Alto Networks, Inc.

STEP 11 | Verifique y solucione problemas de la implementación del proxy de agente.

1. Verifique la información sobre su conexión de red en la pestaña **Connections (Conexiones)** de la aplicación GlobalProtect en **Settings (Configuración)**.

   1. Abra la aplicación GlobalProtect.
   2. Seleccione **Settings (Configuración)** para abrir el panel de configuración de GlobalProtect y, a continuación, seleccione **Connections (Conexiones)**.



2. Consultar y recopilar los logs de GlobalProtect

   Consulte el log de PanGPS para verificar la configuración del modo proxy en el portal de GlobalProtect.

   Puede verificar que el modo Proxy está configurado buscando el siguiente evento en el log de PanGPS:

   ```
   OnProxyAgentMode: modo solo proxy
   ```

   Para ver los logs de GlobalProtect en Panorama, seleccione **Monitor (Supervisar)** > **Logs (Logs)** y:

   - **Protección global**, para logs de autenticación
   - **Traffic (Tráfico)** y **Decryption (Descifrado)** para los logs de acceso de usuarios

GlobalProtect en modo Túnel y proxy

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 5.2 • Versión 6.2 de la aplicación GlobalProtect para Windows o macOS • Versión de publicación de contenido 8700-7994

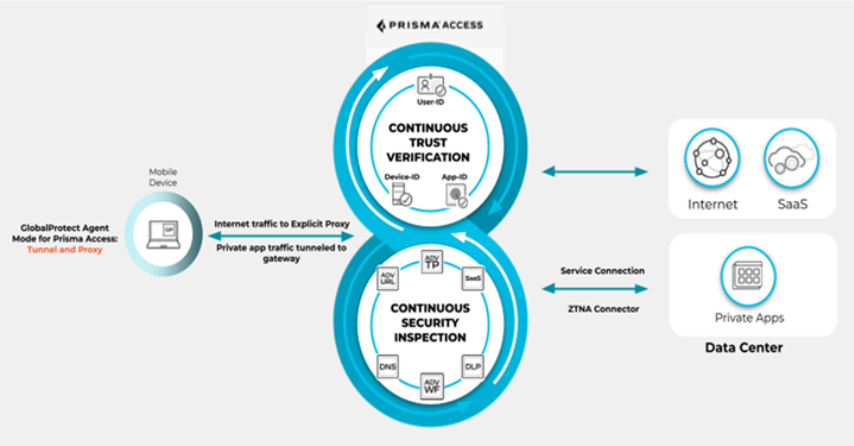
 ©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
Si desea utilizar esta función en su entorno de Prisma Access, póngase en contacto con su equipo de cuenta para obtener más información.	• Licencia de usuario móvil de Prisma Access

En el modo **Tunnel and Proxy (Túnel y proxy)**, la aplicación GlobalProtect envía el tráfico enlazado a Internet al proxy explícito en función de las reglas que defina en un archivo PAC. Para el tráfico restante, utiliza las reglas y la lógica de tunelización dividida definidas en el archivo PAC para determinar qué tráfico enviar a través del túnel y qué tráfico puede omitir el túnel. Si no tiene reglas de túnel dividido definidas, la aplicación envía todo el tráfico restante a través del túnel.

Al ejecutar la aplicación GlobalProtect en modo Túnel y Proxy, la funcionalidad de perfil de información de host (HIP) solo es compatible con el tráfico a través de un túnel GlobalProtect.

Le hace falta Strata Cloud Manager y la versión 6.3.0 del agente de GlobalProtect para que el canal Proxy de GlobalProtect admita todas las conexiones TCP IPv4, incluido el tráfico no compatible con proxy. Para garantizar una funcionalidad perfecta, el DNS configurado en los endpoints debe ser capaz de resolver el FQDN de destino.



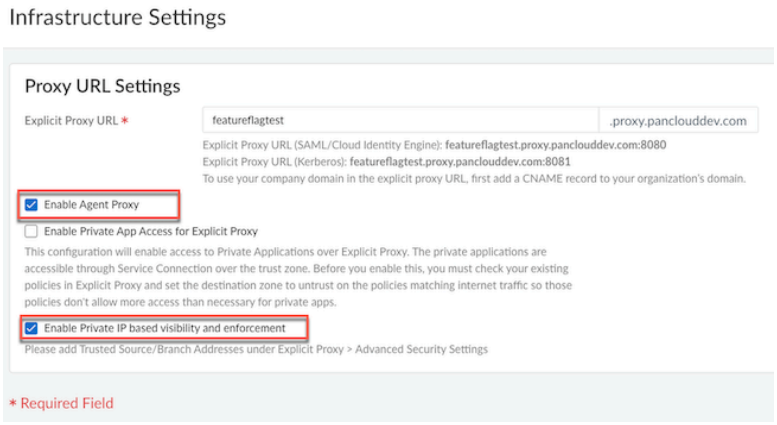
- Strata Cloud Manager
- Panorama

GlobalProtect en modo túnel y proxy (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Habilite la funcionalidad de proxy basado en agente para usuarios móviles en Prisma Access.

1. Habilitar el proxy explícito.
   1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)**.
   2. En el área Configuración de infraestructura, haga clic en **Setup Proxy Settings (Configurar la configuración del proxy)** y especifique una **Explicit Proxy URL (URL de proxy explícito)**.
2. Seleccione **Enable Agent Proxy (Habilitar proxy de agente)**y opcionalmente **Enable Private IP based visibility and enforcement (Habilitar la visibilidad y el cumplimiento basados en IP privadas)** y haga clic en **Save (Guardar)**.



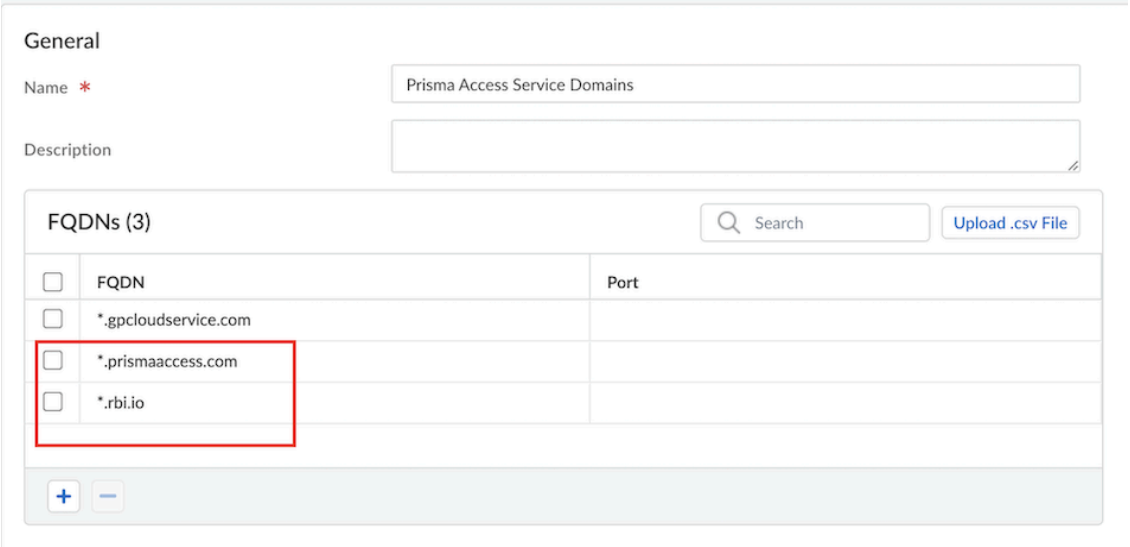
3. Seleccione las Prisma Access locations (Ubicaciones de Prisma Access) donde desea admitir usuarios móviles.

   Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a los usuarios finales. Si una ubicación no está disponible en el

 ©2025 Palo Alto Networks, Inc.

país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a los usuarios móviles.

4. Crear un Perfil de reenvío para definir el tráfico que desea enviar a través de Proxy explícito. Al configurar el perfil de reenvío, omita los dominios *.prismaaccess.com y *.gpcloudservice.com.



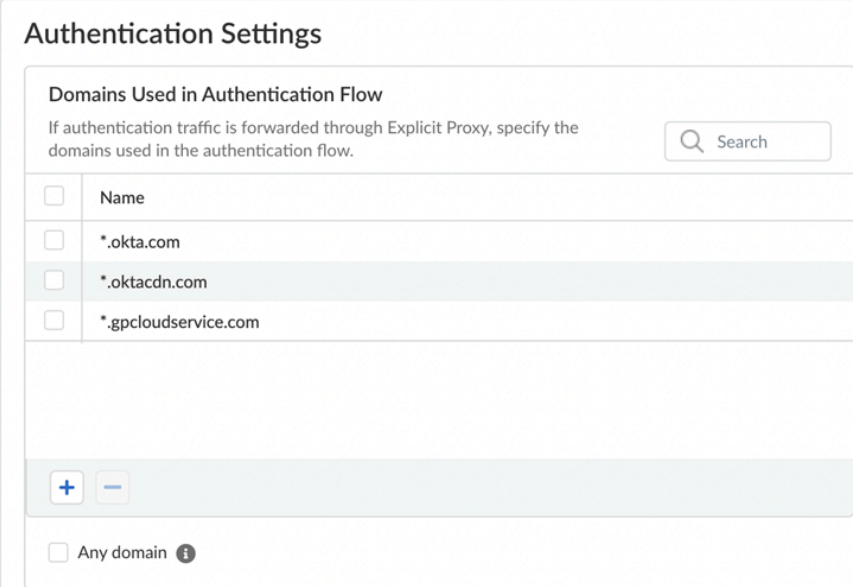
5. Adjunte el perfil de reenvío a la configuración de la aplicación de GlobalProtect.
6. Seleccione **Workflows (Flujos de trabajo)** > **Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Advanced Security Settings (Configuración de**

 ©2025 Palo Alto Networks, Inc.

seguridad avanzada) > **Authentication Settings (Configuración de autenticación)** y añada los dominios que necesita omitir.

Todas las solicitudes al proxy se someten a autenticación. Sin embargo, si está pasando flujos de IdP a través del proxy, debe omitirlos para que la autenticación se realice correctamente.

En este ejemplo, estamos omitiendo el portal de GlobalProtect y Okta, pero personalícelos según los IdP que utiliza.



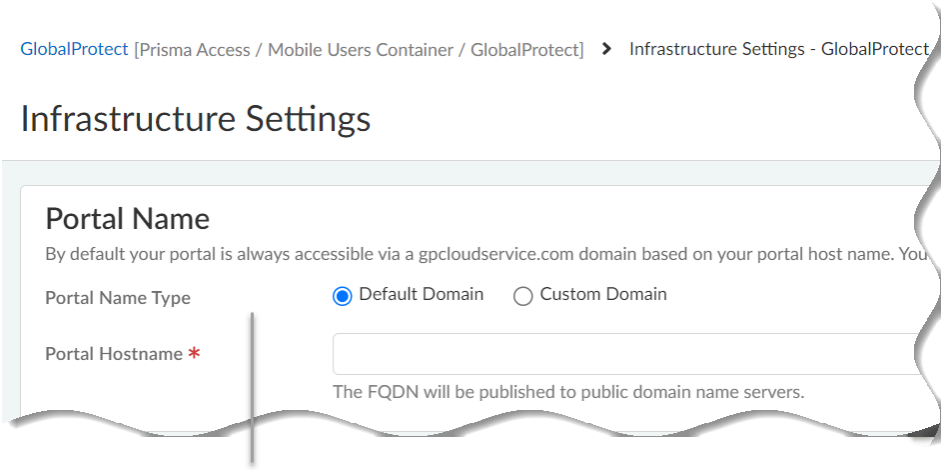
STEP 2 | Configure el modo de túnel y proxy para la aplicación GlobalProtect en Prisma Access.

En el modo Túnel y proxy, el método de conexión establecido solo se aplica al tráfico tunelizado a través de GlobalProtect. La funcionalidad de proxy basada en agentes proporcionará seguridad de Internet siempre activa. Incluso si establece un método de conexión bajo demanda, todo el tráfico a Internet seguirá manteniendo la comunicación proxy para una seguridad en Internet siempre activa, incluso cuando los usuarios desconecten la aplicación GlobalProtect.

1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** > **Infrastructure**

 ©2025 Palo Alto Networks, Inc.

Settings (Configuración de la infraestructura) y especifique el **Portal Name (Nombre del portal)**.



GlobalProtect Infrastructure Settings

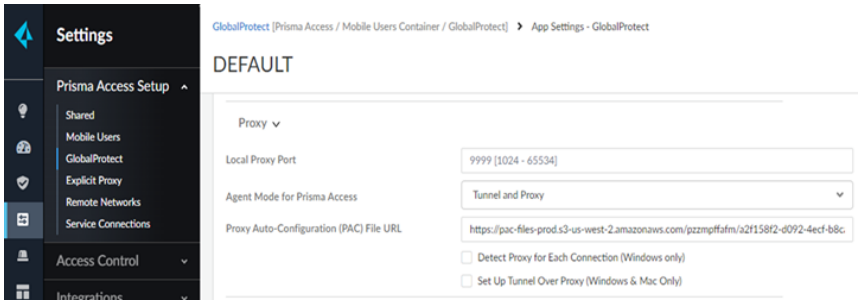
- **Default Domain (Dominio predeterminado)**: si selecciona esta opción, el nombre de host del portal utiliza el nombre de dominio predeterminado: `.gpcloudservice.com`. En este caso, basta con introducir un **Portal Hostname (Nombre de host del portal)** para anexar al nombre de dominio predeterminado. Prisma Access para usuarios creará automáticamente los certificados necesarios y publicará el nombre de host en servidores DNS públicos.
- **Custom Domain (Dominio personalizado)**: también puede personalizar la dirección del portal si desea que el dominio del nombre de host del portal coincida con el nombre de dominio de su empresa (por ejemplo, myportal.mydomain.com).

2. Permitir a los usuarios móviles autenticarse en Prisma Access.
3. Habilite el modo de túnel y proxy de GlobalProtect para Prisma Access en la Configuración de la aplicación GlobalProtect para enviar tráfico de Internet al proxy basado en agente.
   - Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect**.
   - En el **GlobalProtect App (Aplicación GlobalProtect)**, haga clic en **Default (Predeterminado)** para personalizar la configuración de la aplicación o seleccione **Add App Settings (Añadir configuración de la aplicación)** para añadir una nueva configuración.
   - Haga clic en **Show Advanced Options (Mostrar opciones avanzadas)** y en **App Configuration (Configuración de la aplicación)**.
   - En la sección de**Proxy**, establezca **Agent Mode for Prisma Access (Modo de agente para Prisma Access)** en **Tunnel and Proxy (Túnel y proxy)** para indicar a la aplicación GlobalProtect que envíe el tráfico de Internet al proxy explícito en Prisma Access y el tráfico de aplicaciones privadas a la VPN. Después de configurar el modo **Tunnel and Proxy (Túnel y proxy)** en Prisma Access, los usuarios pueden acceder de forma

 ©2025 Palo Alto Networks, Inc.

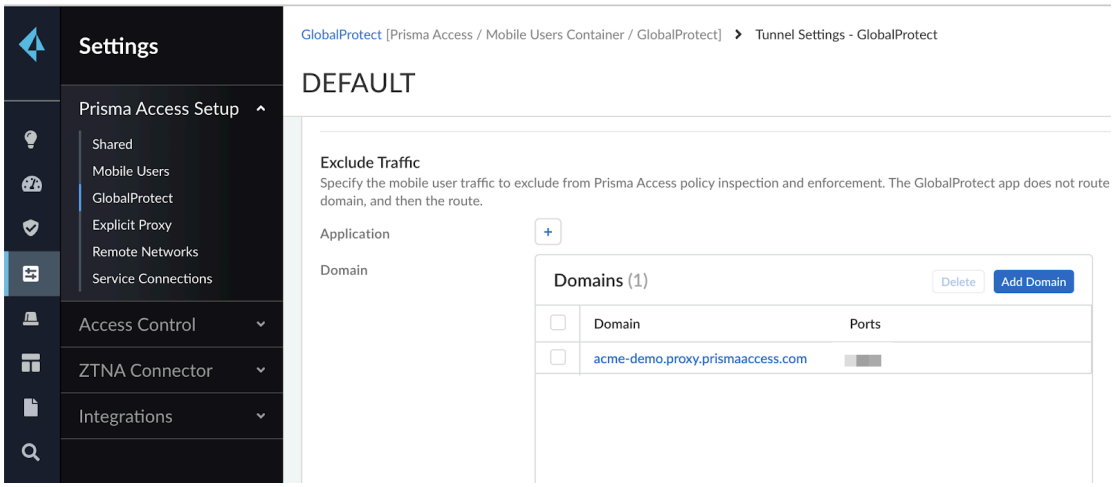
segura a Internet a través de Prisma Access incluso cuando los usuarios desconectan o desactivan la aplicación GlobalProtect.

- (Opcional) Configure el puerto proxy local. El intervalo de puertos es de 1024 a 65534 y el puerto predeterminado es 9999. Si el puerto predeterminado no está disponible, GlobalProtect intentará otros 10 puertos en el rango de 9999 a 10009 y utilizará el puerto que esté disponible. También puede elegir su propio número de puerto dentro del rango.
- (Opcional) Configure la URL del archivo de configuración automática de proxy (PAC) si desea enviar la nueva URL de PAC para la configuración del proxy al endpoint. La URL de PAC se envía al endpoint una vez que el usuario se conecta. Cuando el usuario desconecta la aplicación GlobalProtect, las configuraciones del proxy de endpoint se desactivan automáticamente y vuelven a la configuración anterior.
- (Opcional) Habilite Allow User to Rediscover Network (Permitir que el usuario redescubra la red) si desea que el usuario compruebe si hay nuevas configuraciones en el portal.
- (Opcional) Configure GlobalProtect App Config Refresh Interval (hours) [Intervalo de actualización de configuración para la aplicación de GlobalProtect (horas)]. De forma predeterminada, el cliente de GlobalProtect actualiza la configuración del portal almacenada en caché cada 24 horas. Puede cambiar el intervalo de actualización en función de los requisitos de su empresa.
- Deshabilite **Set Up Tunnel Over Proxy (Windows & Mac Only) [Configurar el túnel sobre proxy (Solo Windows y Mac)]**



 ©2025 Palo Alto Networks, Inc.

4. En la configuración de **Split Tunnel (Túnel dividido)**, excluya el FQDN de proxy explícito y el FQDN del archivo PAC.
   - Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect**.
   - En la **GlobalProtect App (Aplicación de GlobalProtect)**, haga clic en **Default (Predeterminado)** para personalizar la configuración del túnel o seleccione **Add Tunnel Settings (Añadir configuración de túnel)** para añadir una nueva configuración.
   - En **Exclude Traffic (Excluir tráfico)**, **Add Domain (Añadir dominio)**.



 ©2025 Palo Alto Networks, Inc.

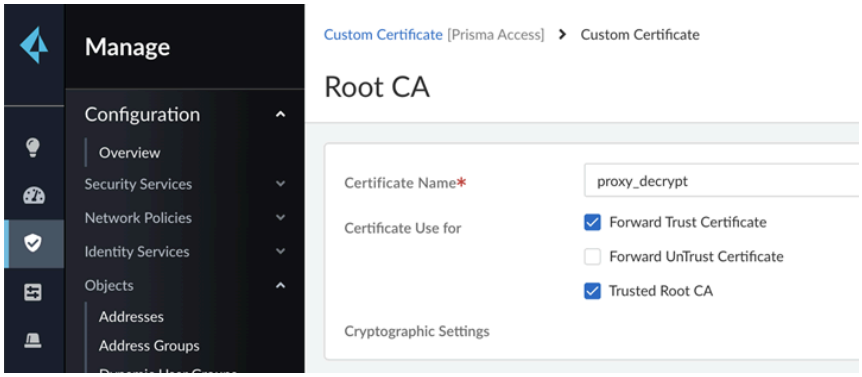
Reemplace el FQDN de la imagen por el FQDN del proxy.

STEP 3 | Habilite la seguridad Siempre activa configurando las siguientes opciones en la página **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Aplicación GlobalProtect)** > **Add App Settings (Añadir configuración de la aplicación)**:

1. Establezca Disable GlobalProtect (Deshabilitar GlobalProtect) para **Disallow (Prohibir)**, **Allow with Passcode (Permitir con código de acceso)** o **Allow with Ticket (Permitir con ticket de incidencia)**.
2. Deshabilite Permitir al usuario cerrar sesión desde la aplicación de GlobalProtect

STEP 4 | Configure el descifrado para el tráfico de Proxy explícito.

- Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y (NGFW y Prisma Access)** > **Security Services (Servicios de Seguridad)** > **Decryption (Descifrado)**.
- Si habilita el descifrado, asegúrese de configurar el certificado de descifrado como una CA raíz de confianza.



STEP 5 | Configure las reglas de la política de seguridad para el tráfico de proxy explícito.

- Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de Seguridad)** > **Security Policy (Política de seguridad)**.
- Siga las Prácticas recomendadas de la política de seguridad de puerta de enlace de Internet.

STEP 6 | (Opcional) Configure la aplicación GlobalProtect en modo Proxy y túnel en una red de ruta no predeterminada.

- (Opcional) Alojar un archivo PAC internamente y añadir el FQDN de proxy explícito de Prisma Access como proxy en el archivo PAC, o hospede el archivo PAC en un Perfil de reenvío y añada rutas en su red para Direcciones IP del servicio PAC.
- Reenvíe las solicitudes de autenticación a Internet para los FQDN del portal y la puerta de enlace, así como para las URL de IdP.
- Establezca rutas al FQDN de proxy explícito o a las direcciones IP en los dispositivos perimetrales para permitir que los usuarios accedan a Internet a través del proxy explícito.
- (Opcional) Añada registros DNS para resolver el FQDN de proxy explícito de Prisma Access a una dirección IP interna si los usuarios no pueden resolver dominios públicos en la red de

 ©2025 Palo Alto Networks, Inc.

sucursal y añada NAT de destino para la dirección IP interna al FQDN de proxy explícito o a la dirección IP.

- Para permitir que los usuarios accedan a aplicaciones privadas directamente cuando están en la oficina:
  - **Acceso directo:** Habilite la detección de host interno y mantenga vacía la lista de puertas de enlace internas.

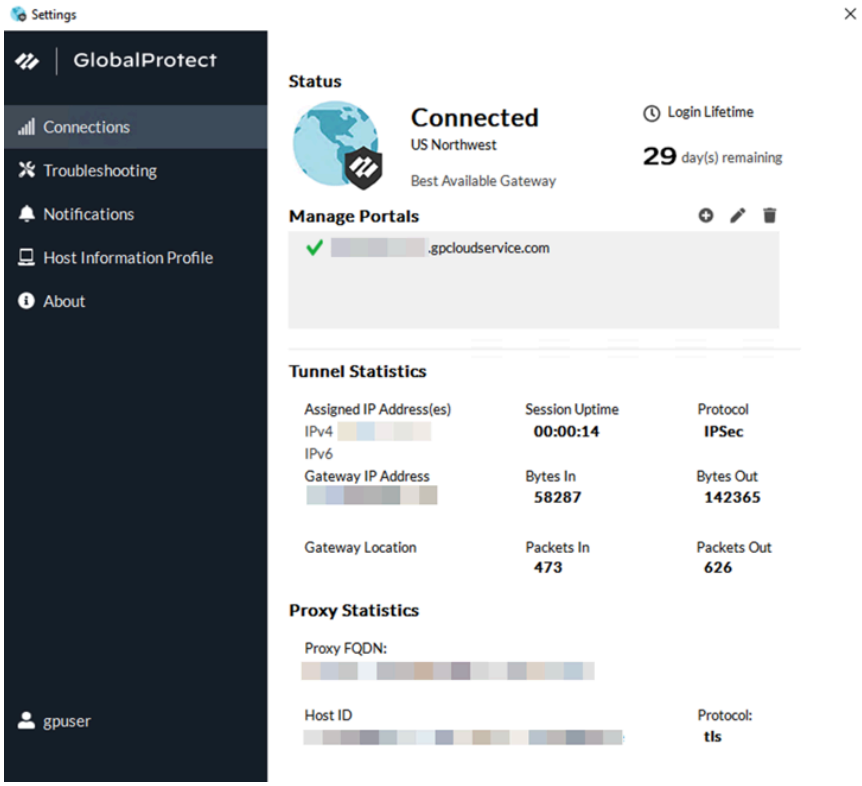
STEP 7 | Haga clic en **Save (Guardar)** y **Push Config (Enviar configuración)** a **GlobalProtect** y **Proxy explícito**.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Verifique y solucione problemas de la implementación del proxy de agente.

1. Verifique la información sobre su conexión de red en la pestaña **Connections (Conexiones)** de la aplicación GlobalProtect en **Settings (Configuración)**.

   1. Abra la aplicación GlobalProtect.
   2. Seleccione **Settings (Configuración)** para abrir el panel de configuración de GlobalProtect y, a continuación, seleccione **Connections (Conexiones)**.



2. Consultar y recopilar logs de GlobalProtect

   Consulte el log de PanGPS para verificar la configuración del modo proxy en el portal de GlobalProtect.

   Puede verificar que el modo Proxy está configurado buscando el siguiente evento en el log de PanGPS:

   ```
   OnProxyAgentMode: modo híbrido
   ```

   Para ver los logs de GlobalProtect en , seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)** y:

   - **Protección global**, para logs de autenticación
   - **Traffic (Tráfico)** y **Decryption (Descifrado)** para los logs de acceso de usuarios

Desconecte y deshabilite el modo de túnel y proxy con el método de conexión siempre activo

A partir de la versión 6.3.1 de GlobalProtect, cuando se configura **Tunnel and Proxy (Túnel y proxy)** para la aplicación GlobalProtect junto con el modo **Always-On (Siempre activo)**

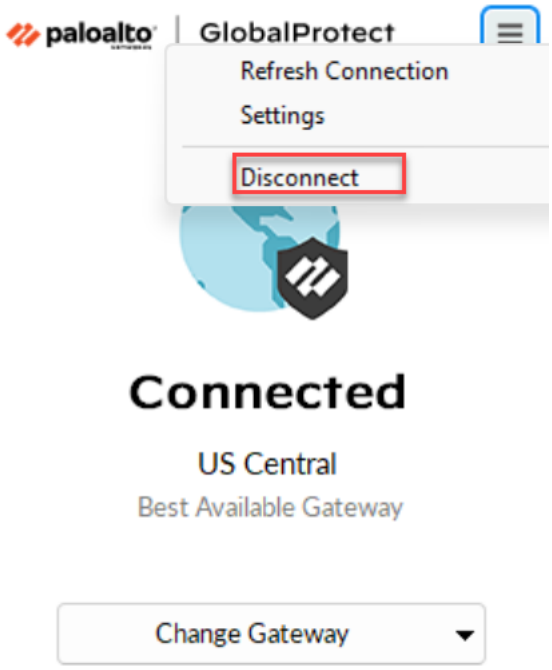
 ©2025 Palo Alto Networks, Inc.

como método de conexión, y desea desconectar el modo de túnel y proxy, debe realizar los siguientes pasos:

1. Desconecte la aplicación GlobalProtect para desconectar la conexión de túnel (VPN). Al desconectar la aplicación, la conexión de túnel (VPN) se desconecta y la aplicación seguirá conectada a través del modo proxy.
2. Deshabilite la aplicación GlobalProtect para desconectar el modo Túnel y proxy. Al deshabilitar la aplicación, tanto el modo de túnel como el de proxy se desconectarán y la aplicación ya no estará conectada.

Para desconectar y deshabilitar la aplicación GlobalProtect configurada con **Tunnel and Proxy (Túnel y proxy)** (modo híbrido) y el método de conexión **Always-On (Siempre activo)**, debe:

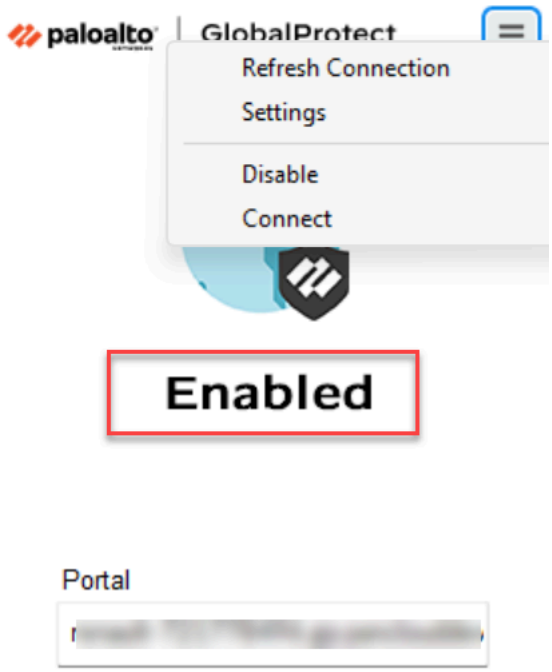
1. Desconecte la aplicación GlobalProtect con la opción **Disconnect (Desconectar)** del menú de tres barras. Al desconectar la aplicación, se desconecta la conexión de túnel (VPN).



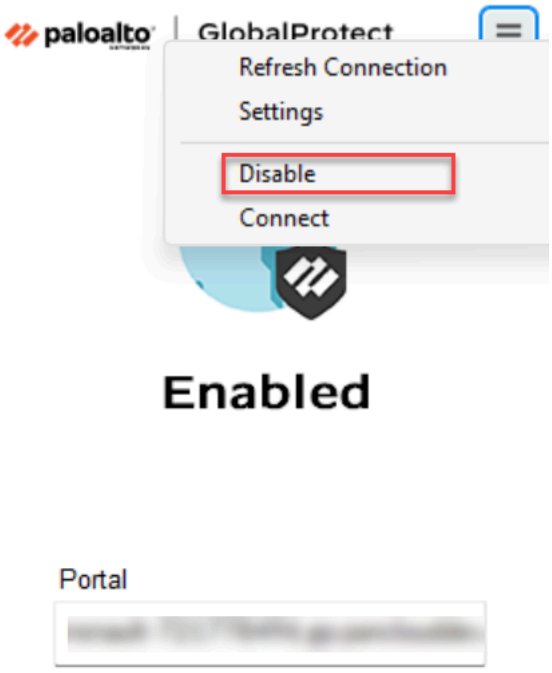
Después de desconectar la aplicación, la conexión VPN se desconecta, pero el modo proxy está habilitado. La aplicación seguirá conectada a través del modo proxy y la aplicación muestra el estado como **Enabled (Habilitado)**.

*Si desea volver a conectar la conexión de túnel (VPN), puede utilizar la opción **Connect (Conectar)** del menú de tres barras.*

 ©2025 Palo Alto Networks, Inc.

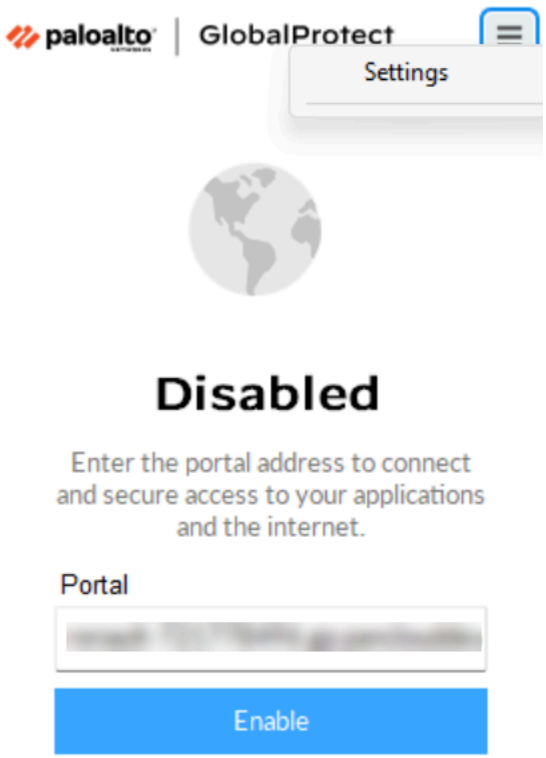


2. Deshabilite la aplicación GlobalProtect con la opción **Disable (Deshabilitar)** del menú de tres barras. Después de deshabilitar la aplicación, tanto la conexión de túnel como la de proxy se desconectan.



La aplicación se deshabilitará y mostrará el estado como **Disabled (Deshabilitado)**.

 ©2025 Palo Alto Networks, Inc.



GlobalProtect en modo túnel y proxy (Panorama)

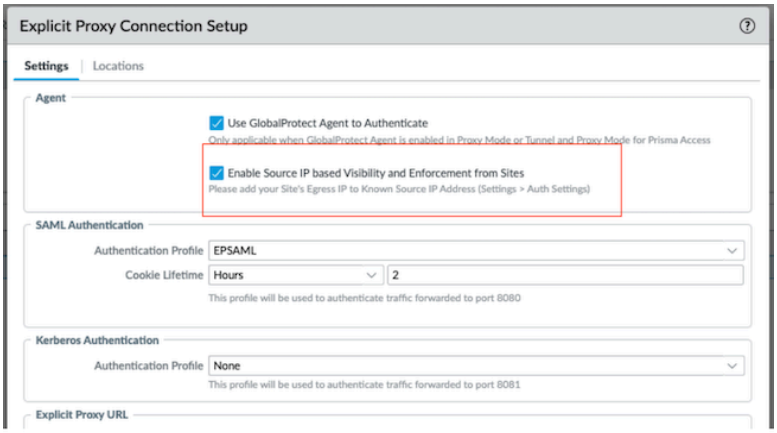
Si convierte una implementación de Prisma Access (Managed by Panorama) de inquilino único a varios inquilinos, solo el primer inquilino (el inquilino que migró) admite esta característica. Además, en este primer inquilino, debe configurar las reglas de la política en el Explicit_Proxy_Device_Group predefinido en lugar de en un grupo de dispositivos personalizado. Los inquilinos posteriores que cree para la implementación de varios inquilinos después de la primera no admiten esta característica.

STEP 1 | Habilite la funcionalidad de Proxy basado en agentes para usuarios móviles.

1. Habilitar el proxy explícito.
    1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: proxy explícito)**.
    2. Seleccione **Configure (Configurar)** la configuración explícita del proxy para especificar un **Explicit Proxy URL (URL de proxy explícito**.
2. Seleccione **Use GlobalProtect app to Authenticate (Utilizar la aplicación GlobalProtect para autenticarse)** para habilitar la funcionalidad de proxy basado en agente, y

 ©2025 Palo Alto Networks, Inc.

opcionalmente **Enable Source IP based Visibility and Enforcement from Sites (Habilitar la visibilidad y el cumplimiento de los sitios basados en IP de origen)**.



3. Introduzca la URL del **PAC (Proxy Auto-Configuration) File (Archivo PAC (configuración automática de proxy)**. Asegúrese de introducir un puerto de 8080 en el archivo PAC.
   - La Declaración proxy en el archivo PAC debe usar el FQDN de Prisma Access que configuró anteriormente.
   - El archivo PAC debe configurarse para excluir las puertas de enlace de GlobalProtect (*.gp.gpcoudservice.com).
4. Seleccione la opción **Connection Name (Nombre de la conexión)** para la configuración de proxy explícito que ha configurado.
5. Seleccione las **Locations (Ubicaciones)** y las regiones en las que desea implementar el proxy explícito para usuarios móviles.

   Prisma Access añade un nodo proxy en cada ubicación que usted seleccione. El proxy explícito es compatible con un subconjunto de todas las ubicaciones de Prisma Access. Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a sus usuarios o en el mismo país que sus usuarios. Si una ubicación no está disponible en el país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a los usuarios móviles.

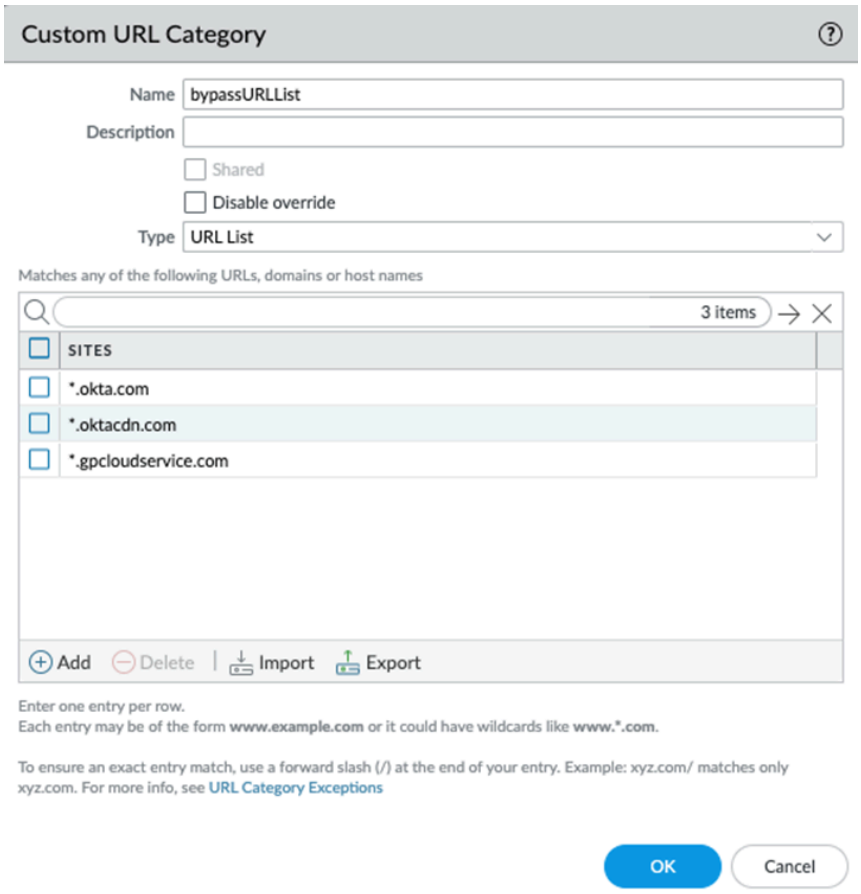
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Omita los proveedores de identidad (IDP).

Se autentican todas las solicitudes al proxy. Sin embargo, si está pasando flujos de IDP a través del proxy, debe omitirlos para que la autenticación se realice correctamente.

En este ejemplo, estamos omitiendo el portal de GlobalProtect y Okta, pero personalícelos según los IDP que utiliza.

1. Con el **Explicit_Proxy_Device_Group** seleccionado, seleccione **Object (Objeto)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y cree una categoría de URL personalizada.
2. En la categoría de URL personalizada, añada todos los dominios FQDN que se deben omitir de la autenticación EP.



3. Seleccione **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)** > **Explicit Proxy (Proxy explícito)** > **Settings (Configuración)** > **Authentication Settings (Configuración de autenticación)** y adjunte la categoría de URL personalizada.



4. Confirmar y enviar al **Explicit_Proxy_Device_Group**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure el Portal de GlobalProtect.

En el modo Túnel y proxy, el método de conexión establecido solo se aplica al tráfico tunelizado a través de GlobalProtect. La funcionalidad de proxy basada en agentes proporcionará seguridad de Internet siempre activa. Incluso si establece un método de conexión bajo demanda, todo el tráfico a Internet seguirá manteniendo la comunicación proxy para una seguridad en Internet siempre activa, incluso cuando los usuarios desconecten la aplicación GlobalProtect.

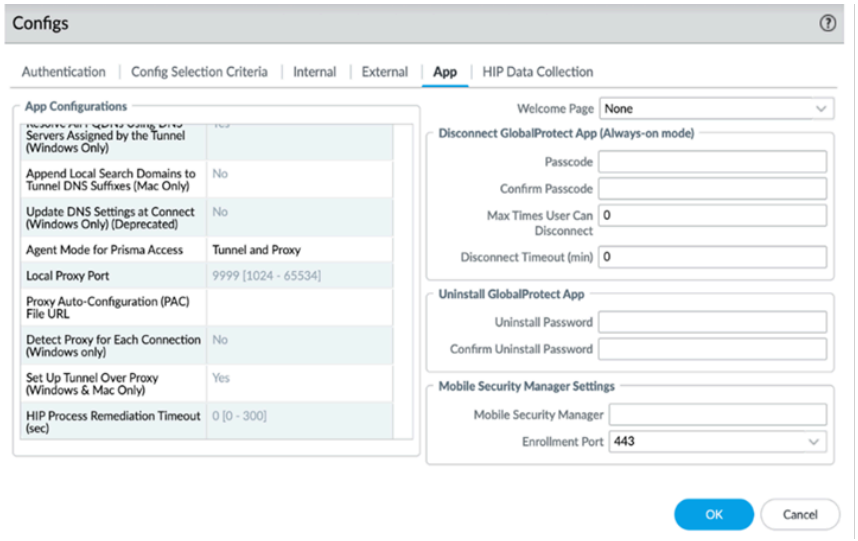
1. En la sección de Incorporación, haga clic en **Configure (Configurar)**.
2. En la pestaña **General**, especifique el **Portal Name Type (Tipo de nombre del portal)**:

   Use Default Domain— (Usar dominio predeterminado:) Si selecciona esta opción, el nombre de host del portal utiliza el nombre de dominio predeterminado: .gpcloudservice.com. En este caso, simplemente introduzca un nombre de host de Portal para añadir al nombre de dominio predeterminado. Prisma Access creará automáticamente los certificados necesarios y se publicará el nombre de host en los servidores DNS públicos.

   Use Company Domain (Utilizar dominio de la empresa): seleccione esta opción si desea que el dominio en el nombre de host del portal coincida con el nombre de dominio de su empresa (por ejemplo, myportal.mydomain.com).
3. Seleccione un **Authentication Profile (Perfil de autenticación)** que especifica cómo Prisma Access debe autenticar a los usuarios móviles o crear uno nuevo.
4. (Opcional) Seleccione un **Authentication Override Certificate (Certificado de anulación de autenticación)** para cifrar las cookies seguras que los usuarios móviles utilizan para autenticarse en el portal y la puerta de enlace.
   1. Habilitar el modo túnel y proxy en 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 la pestaña **Agent (Agente)**, seleccione **App (Aplicación)**.
      4. En el área de App Configurations (Configuraciones de la aplicación), establezca el **Agent Mode for Prisma Access (Modo de agente para Prisma Access)** en **Tunnel and**

 ©2025 Palo Alto Networks, Inc.

Proxy (Túnel y proxy) para enviar el tráfico de internet al proxy explícito de Prisma Access y el tráfico de aplicaciones privadas a la VPN.



2. Realizar configuraciones opcionales.
   1. (Opcional) Configure el puerto proxy local. El intervalo de puertos es de 1024 a 65534 y el puerto predeterminado es 9999. Si el puerto predeterminado no está disponible, GlobalProtect intentará otros 10 puertos en el rango de 9999 a 10009 y utilizará el puerto que esté disponible. También puede elegir su propio número de puerto dentro del rango.
   2. (Opcional) Configure la URL del archivo de configuración automática de proxy (PAC) si desea enviar una URL de PAC personalizada para la configuración del proxy al endpoint. La URL de PAC se envía al endpoint una vez que el usuario se conecta. Cuando el usuario desconecta la aplicación GlobalProtect, las configuraciones del proxy de endpoint se desactivan automáticamente y vuelven a la configuración anterior.
   3. (Opcional) Habilite Allow User to Rediscover Network (Permitir que el usuario redescubra la red) si desea que el usuario compruebe si hay nuevas configuraciones en el portal.
   4. (Opcional) Configure GlobalProtect App Config Refresh Interval (hours) [Intervalo de actualización de configuración para la aplicación de GlobalProtect (horas)]. De forma predeterminada, el cliente de GlobalProtect actualiza la configuración del portal almacenada en caché cada 24 horas. Puede cambiar el intervalo de actualización en función de los requisitos de su empresa.
3. En la configuración de túnel dividido, excluya el FQDN del proxy explícito y el FQDN del archivo PAC.

STEP 4 | Habilite la seguridad de internet Siempre activa mediante la configuración de los siguientes ajustes:

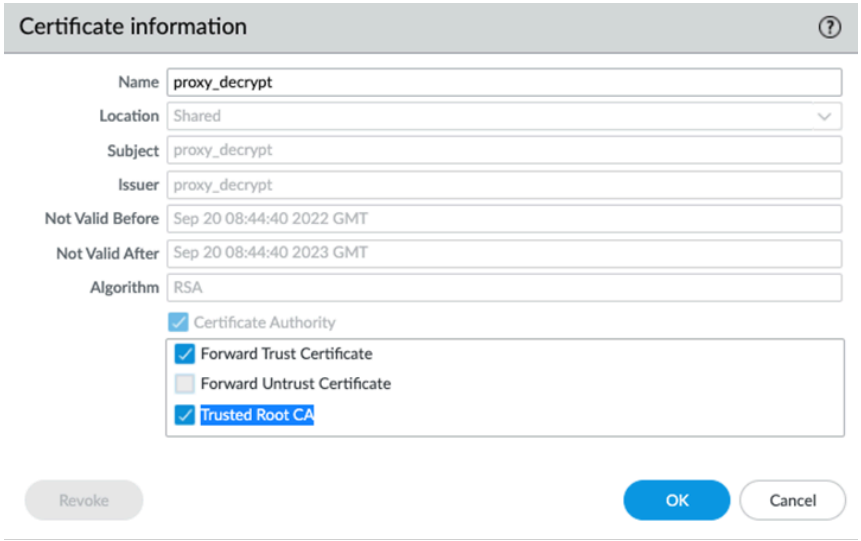
1. Establezca Permitir que el usuario deshabilite GlobalProtect en **Disallow (Prohibir)**, **Allow with Passcode (Permitir con código de acceso)**o **Allow with Ticket (Permitir con ticket de incidencia)**.
2. Establezca Permitir al usuario cerrar sesión desde la aplicación de GlobalProtect en **No**.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Configurar la política de descifrado para el tráfico de proxy explícito.

Si habilita el descifrado, asegúrese de que el certificado de descifrado también esté configurado como una CA raíz de confianza.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión del certificado)** > **Certificates (Certificados)** y cree un certificado que sea una CA raíz de confianza y un certificado de reenvío fiable.



2. Crea una regla de descifrado en**Explicit_Proxy_Device Group** con proxy de reenvío SSL.

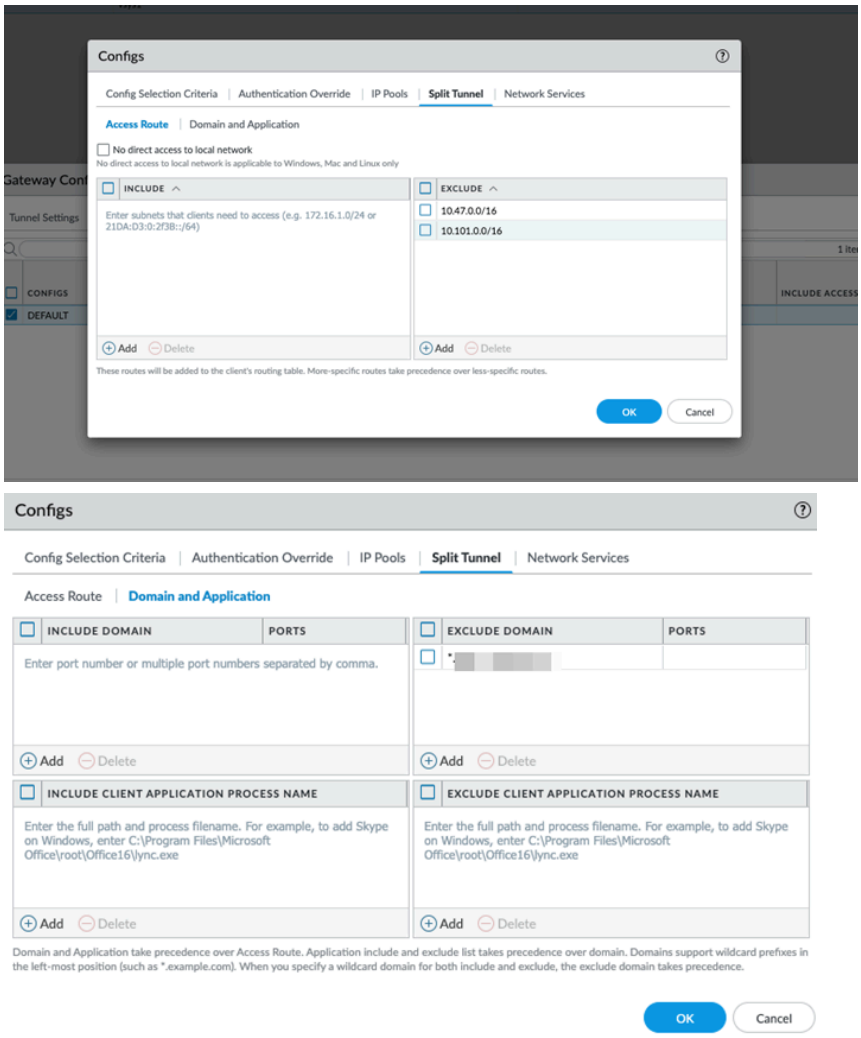
STEP 6 | Configure las reglas de la política de seguridad para el tráfico de proxy explícito.

- Seleccione **Manage (Gestionar)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **..**
- Siga las Prácticas recomendadas de la política de seguridad de puerta de enlace de Internet.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Configure el túnel dividido en Panorama.

1. Seleccione **Network (Plantillas)** > **Mobile User Template (Plantilla de usuario móvil)** > **Gateways (Puertas de enlace)** > **GlobalProtect_ExternalGateway** > **Agent (Agente)** > **Client Settings (Configuración del cliente)** > **Split (Dividir)**.
2. Configure el túnel en función de rutas y dominios.



STEP 8 | (Opcional) Configura la aplicación GlobalProtect en modo túnel y proxy en una red de ruta no predeterminada.

- (Opcional) Alojar un archivo PAC internamente y añadir el FQDN de proxy explícito de Prisma Access como proxy en el archivo PAC, o hospede el archivo PAC en un Perfil de reenvío y añada rutas en su red para Direcciones IP del servicio PAC.
- Verifique que la URL del portal de GlobalProtect y las URL de IDP se estén redirigiendo al Proxy explícito de Prisma Access.
- Establezca rutas al FQDN de proxy explícito o a las direcciones IP en los dispositivos perimetrales para permitir que los usuarios accedan a Internet a través del proxy explícito.
- (Opcional) Añada registros DNS para resolver el FQDN de proxy explícito de Prisma Access a una dirección IP interna si los usuarios no pueden resolver dominios públicos en la red de

 ©2025 Palo Alto Networks, Inc.

sucursal y añada NAT de destino para la dirección IP interna al FQDN de proxy explícito o a la dirección IP.

- Para permitir que los usuarios accedan a aplicaciones privadas directamente cuando están en la oficina:
  - **Acceso directo**: habilita la detección del host interno y mantiene la lista de puertas de enlace internas vacía.

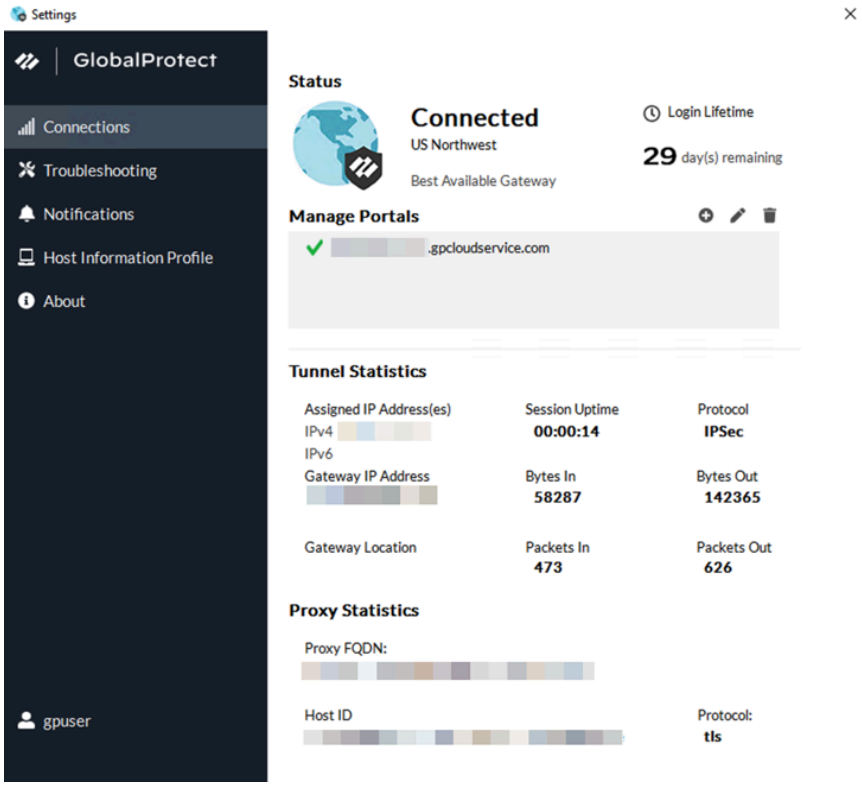
STEP 9 | **Commit (Confirmar)** los cambios en Panorama y **Commit and Push (Confirmar y enviar)** los cambios de configuración a los **Mobile Users (Usuarios móviles)** y **Explicit Proxy (Proxy explícito)** de Prisma Access .

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Verifique y solucione problemas de la implementación del proxy de agente.

1. Verifique la información sobre su conexión de red en la pestaña **Connections (Conexiones)** de la aplicación GlobalProtect en **Settings (Configuración)**.

   1. Abra la aplicación GlobalProtect.
   2. Seleccione **Settings (Configuración)** para abrir el panel de configuración de GlobalProtect y, a continuación, seleccione **Connections (Conexiones)**.



2. Consultar y recopilar los logs de GlobalProtect

   Consulte el log de PanGPS para verificar la configuración del modo proxy en el portal de GlobalProtect.

   Puede verificar que el modo proxy está configurado buscando el siguiente evento en el log de PanGPS:

   ```
   OnProxyAgentMode: modo híbrido
   ```

   Para ver los logs de GlobalProtect en Panorama, seleccione **Monitor (Supervisar)** > **Logs (Logs)** y:

   - **Protección global**, para logs de autenticación
   - **Traffic (Tráfico)** y **Decryption (Descifrado)** para los logs de acceso de usuarios

Desconecte y deshabilite el modo de túnel y proxy con el método de conexión siempre activo

A partir de la versión 6.3.1 de GlobalProtect, cuando se configura **Tunnel and Proxy (Túnel y proxy)** para la aplicación GlobalProtect junto con el modo **Always-On (Siempre activo)**

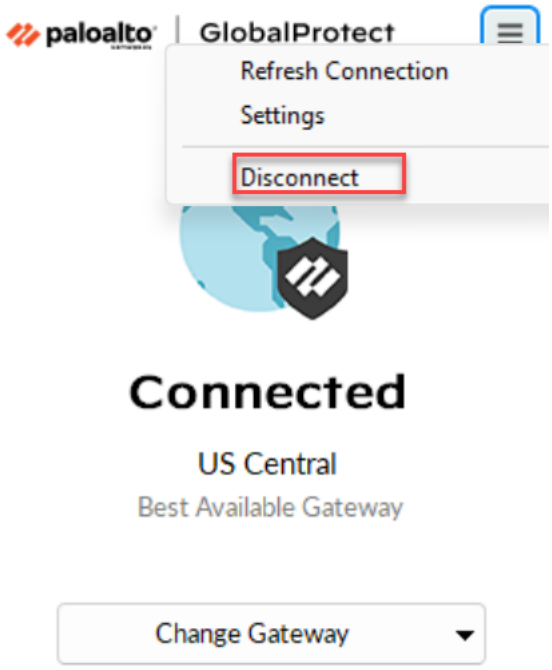
 ©2025 Palo Alto Networks, Inc.

como método de conexión, y desea desconectar el modo de túnel y proxy, debe realizar los siguientes pasos:

1. Desconecte la aplicación GlobalProtect para desconectar la conexión de túnel (VPN). Al desconectar la aplicación, la conexión de túnel (VPN) se desconecta y la aplicación seguirá conectada a través del modo proxy.
2. Deshabilite la aplicación GlobalProtect para desconectar el modo Túnel y proxy. Al deshabilitar la aplicación, tanto el modo de túnel como el de proxy se desconectarán y la aplicación ya no estará conectada.

Para desconectar y deshabilitar la aplicación GlobalProtect configurada con **Tunnel and Proxy (Túnel y proxy)** (modo híbrido) y el método de conexión **Always-On (Siempre activo)**, debe:

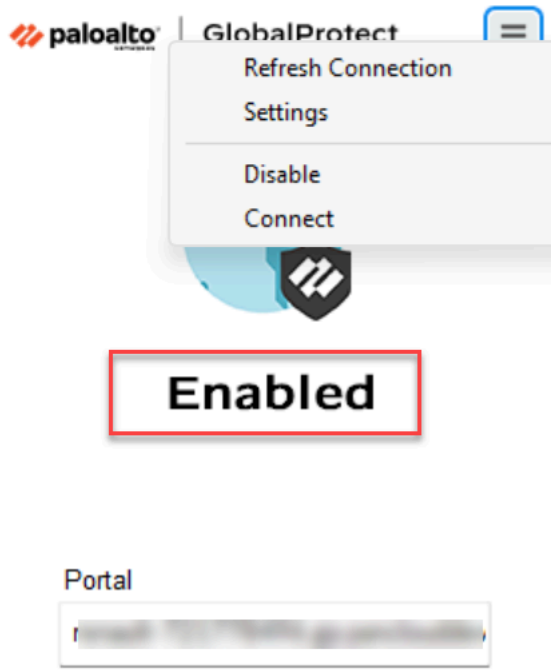
1. Desconecte la aplicación GlobalProtect con la opción **Disconnect (Desconectar)** del menú de tres barras. Al desconectar la aplicación, se desconecta la conexión de túnel (VPN).



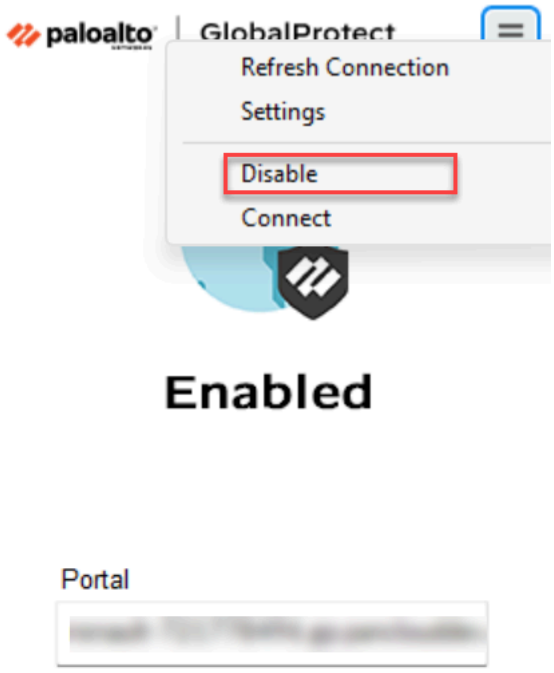
Después de desconectar la aplicación, la conexión VPN se desconecta, pero el modo proxy está habilitado. La aplicación seguirá conectada a través del modo proxy y la aplicación muestra el estado como **Enabled (Habilitado)**.

*Si desea volver a conectar la conexión de túnel (VPN), puede utilizar la opción **Connect (Conectar)** del menú de tres barras.*

 ©2025 Palo Alto Networks, Inc.

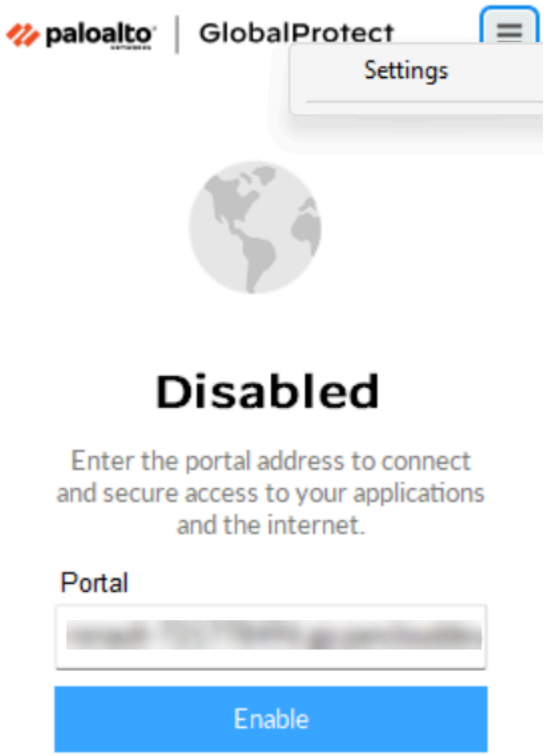


2. Deshabilite la aplicación GlobalProtect con la opción **Disable (Deshabilitar)** del menú de tres barras. Después de deshabilitar la aplicación, tanto la conexión de túnel como la de proxy se desconectan.



La aplicación se deshabilitará y mostrará el estado como **Disabled (Deshabilitado)**.

 ©2025 Palo Alto Networks, Inc.



Visibilidad y aplicación de direcciones IP privadas para tráfico proxy basado en agentes

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 5.2 • Versión 6.3.1 de la aplicación GlobalProtect para Windows o macOS • Plano de datos 10.2.4 de Prisma Access • Licencia de usuario móvil de Prisma Access • Versión 5.2.0 del complemento de Panorama

Los usuarios que se conectan al proxy explícito de Prisma Access a través del agente de GlobalProtect desde las sucursales, pueden aprovechar las Direcciones IP privadas de endpoints para el registro de logs o para aplicar la ejecución basada en direcciones IP.

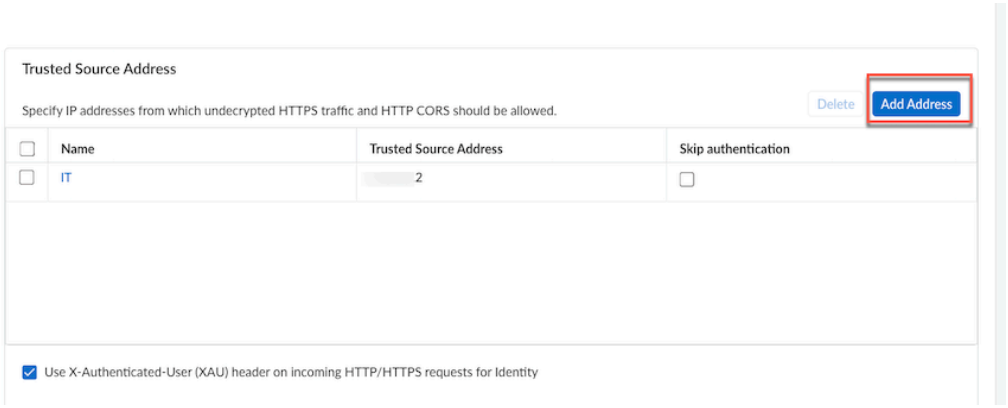
- Strata Cloud Manager
- Panorama

Visibilidad y cumplimiento de direcciones IP privadas para tráfico proxy basado en agentes (Strata Cloud Manager)

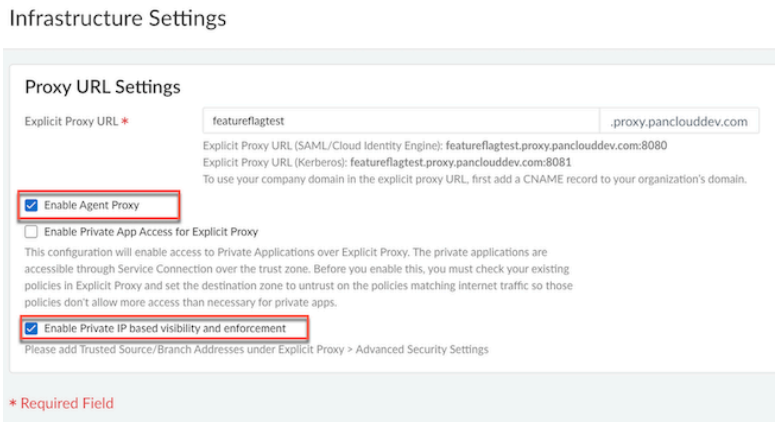
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Habilite la funcionalidad de proxy basada en agente (modo Proxy o modo Túnel y proxy) para usuarios móviles.

STEP 2 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Advanced Security Settings (Configuración de seguridad avanzada)** y haga clic en el icono de configuración. En **Trusted Source Address (Dirección de fuente fiable)**, añada la dirección IP de salida de la sucursal.



STEP 3 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Infrastructure Settings (Configuración de infraestructura)**. En **Proxy URL Settings (Configuración URL de proxy)**, habilite **Enable Source IP based visibility and enforcement (Habilitar visibilidad y aplicación basadas en IP de origen)** y haga clic en **Save (Guardar)**.



STEP 4 | (Opcional) Configure las reglas de seguridad con la dirección IP de origen del endpoint.

STEP 5 | **Push Config (Enviar configuración)** a **Explicit Proxy (Proxy explícito)**.

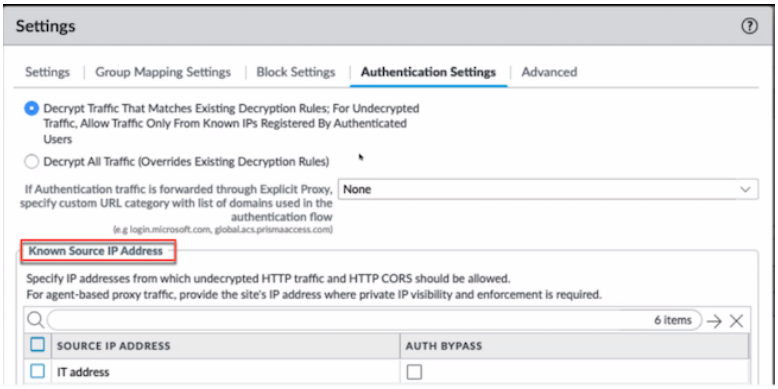
Visibilidad y cumplimiento de direcciones IP privadas para tráfico proxy basado en agentes (Panorama)

STEP 1 | Habilite la funcionalidad de Proxy basada en agentes (modo Proxy y modo Túnel y proxy) para usuarios móviles.

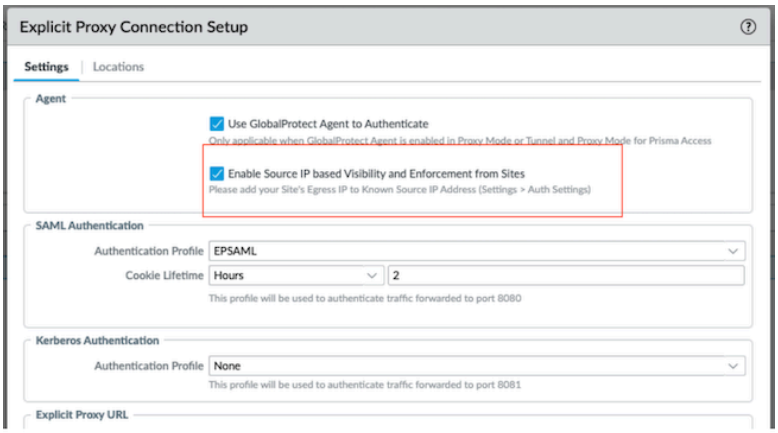
STEP 2 | Vaya a **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)** > **Explicit Proxy (Proxy explícito)** > **Settings (Configuración)** >

 ©2025 Palo Alto Networks, Inc.

Authentication Settings (Configuración de autenticación) y añada la dirección IP de salida de la sucursal en **Known Source IP Address (Dirección IP de Fuente Conocida)**.



STEP 3 | Vaya a **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: proxy explícito)**. En **Agent (Agente)**, habilite **Enable Source IP based Visibility and Enforcement from Sites (Habilitar la visibilidad y el cumplimiento de los sitios basados en IP de origen)**, y haga clic en **OK (Aceptar)**.



STEP 4 | (Opcional) Configure las reglas de seguridad con la dirección IP de origen del endpoint.

STEP 5 | Confirmar y enviar al **Explicit_Proxy_Device_Group**.

Autenticación SAML para Proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	Licencia de Prisma Access

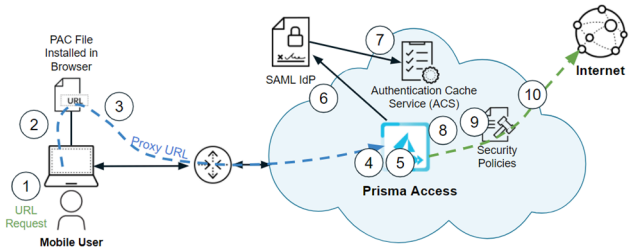
Obtenga información sobre cómo funciona el Proxy explícito con SAML y cómo configurarlo.

- Cómo el Proxy explícito con SAML procesa el tráfico
- Configure el proxy explícito con SAML

 ©2025 Palo Alto Networks, Inc.

Cómo el Proxy explícito con SAML procesa el tráfico

Así es como funciona el proxy explícito con SAML. Siga para ver el camino que toma el tráfico:



STEP 1 | El usuario móvil navega por Internet o accede a la aplicación SaaS introduciendo la URL o la dirección IP mediante un navegador web.

STEP 2 | El navegador en el endpoint de los usuarios móviles comprueba el archivo PAC.

Este archivo PAC especifica que la URL o la solicitud de SaaS deben ir al proxy explícito de Prisma Access.

STEP 3 | El cliente HTTPS (el navegador en el endpoint del usuario móvil) reenvía la solicitud de URL a la URL del proxy.

STEP 4 | El tráfico se redirige al proxy explícito y el proxy descifra el tráfico.

STEP 5 | El proxy inspecciona el tráfico y comprueba la cookie de autenticación configurada por el proxy explícito de Prisma Access.

La cookie contiene información que identifica al usuario móvil y utiliza la cookie para autenticar al usuario.

STEP 6 | Si, tras la inspección de la cookie, Prisma Access determina que el usuario no está autenticado, redirige al usuario para la autenticación.

STEP 7 | Después de que el IdP autentique al usuario, Prisma Access almacena el estado de autenticación del usuario en el Servicio de caché de autenticación (ACS). El período de validez de la autenticación se basa en el valor de la **Cookie Lifetime (Vida útil de la cookie)** especificado durante la configuración de proxy explícito.

STEP 8 | El proxy explícito comprueba la presencia y validez de nuestra cookie. Si la cookie no está presente o no es válida, el usuario es redirigido a ACS. Una vez que ACS confirma la autenticación del usuario, el usuario se redirige de nuevo al proxy explícito con un token. A continuación, el proxy valida ese token y establece la cookie para ese dominio para ese usuario.

STEP 9 | Prisma Access aplica la instauración de seguridad en función de las reglas de política de seguridad que ha configurado el administrador.

STEP 10 | Si la URL no está bloqueada por las reglas de la política de seguridad, Prisma Access envía la solicitud de URL a Internet.

STEP 11 | (Opcional) Configure Conectividad de proxy explícito en GlobalProtect para seguridad de Internet siempre activa. Habilite esta funcionalidad para lograr una seguridad permanente

 ©2025 Palo Alto Networks, Inc.

para el tráfico de Internet, al tiempo que proporciona acceso bajo demanda a aplicaciones privadas a través de GlobalProtect o una VPN de terceros.

Configure el proxy explícito con SAML

Siga estos pasos para configurar el proxy explícito con autenticación SAML.

- Strata Cloud Manager
- Panorama

Configurar el Proxy explícito con SAML (Strata Cloud Manager)

STEP 1 | Configurar Proxy explícito.

STEP 2 | (Opcional) Configure la autenticación para proxy explícito de Cloud Identity Engine.

STEP 3 | Configure reglas de política de seguridad

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **ámbito de la configuración: Proxy explícito** > **Security Services (Servicios de Seguridad)** > **Security Policy (Política de Seguridad)**.
2. Personalice las reglas de la política predeterminada de acuerdo con sus necesidades y las prácticas recomendadas de seguridad de la política de puerta de enlace de Internet.

   *Con Prisma Access 5.1 y un plano de datos de PAN-OS 10.2.10 o una versión posterior, solo necesitará la regla de política de seguridad **Allow Web Access to Known Users (Permitir acceso web a usuarios conocidos)**.*

STEP 4 | Envíe sus cambios de configuración.

Configurar proxy explícito con SAML (panorama)

STEP 1 | Configurar Proxy explícito.

STEP 2 | (Opcional) Configure la autenticación para proxy explícito de Cloud Identity Engine.

STEP 3 | Dependiendo de la versión de su Prisma Access y la versión de su plano de datos, configure una sola regla de políticas o varias.

Requisitos de la versión	Configuración
Prisma Access 5.1 o una versión posterior y un plano de datos de PAN-OS 10.2.10 o una versión posterior.	Configure una Security policy rule (Regla de política de seguridad) para el tráfico de usuarios de autenticación previa. 1. Seleccione **Explicit_Proxy_Device_Group**. 2. Crear un filtro de aplicaciones mediante la etiqueta **Web App (Aplicación web)**. 3. Seleccione **Policies (Políticas)** > **Pre Rules (Reglas previas)** > **Add (Añadir)**.

 ©2025 Palo Alto Networks, Inc.

Requisitos de la versión	Configuración
	4. Crear la regla. 1. **Add (Añadir)** la regla. 2. Dale un nombre descriptivo. Por ejemplo **`allow-pre-auth`** 3. En la pestaña **App (Aplicación)**, seleccione **Add (Añadir)** el filtro de aplicación **Web App (Aplicación web)**. 4. En la pestaña **Source (Fuente)**, seleccione **Add (Añadir) known-user (usuario-conocido)**.
Todas las demás Prisma Access y versiones de plano de datos.	Configure reglas de la política de seguridad de acuerdo a sus necesidades y procedimientos recomendados de la política de seguridad de puerta de enlace de Internet.

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

Configurar Proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si desea habilitar la visibilidad y aplicación basadas en la IP de origen privada en el Proxy explícito en su entorno de Prisma Access, póngase en contacto con su equipo de cuentas para obtener más información.	• Licencia de Prisma Access

Utilice Proxy explícito para proteger a los usuarios móviles redirigiendo el tráfico del navegador a Prisma Access.

Directrices de incorporación: utilice las siguientes directrices al licenciar e incorporar su implementación de proxy explícito:

- El proxy explícito admite un subconjunto de ubicaciones de Prisma Access.
- No puede añadir ubicaciones que estén marcadas con dos asteriscos; estas son zonas locales y no son compatibles con Prisma Access.
- Si tiene una licencia local o de evaluación para Prisma Access para Usuarios y tiene una implementación de Usuarios móviles: GlobalProtect así como una implementación de Usuarios móviles: Proxy explícito, puede implementar un máximo de cinco ubicaciones para cada una (cinco ubicaciones como máximo para Usuarios móviles: GlobalProtect y cinco

 ©2025 Palo Alto Networks, Inc.

ubicaciones como máximo para Usuarios móviles: Proxy explícito). Si tiene una licencia mundial (Worldwide), no hay restricciones sobre el número máximo de ubicaciones.

- Proxy explícito admite la multitenencia en las siguientes condiciones: si tiene una implementación de Prisma Access no multiinquilino existente y la convierte en una implementación multiinquilino, solo el primer inquilino (el inquilino que migró) admite Proxy explícito. Los inquilinos posteriores que cree para la implementación de varios inquilinos después de la primera no admiten el Proxy explícito.
- Al incorporar una implementación de proxy explícito, Palo Alto Networks recomienda que toda la configuración se realice en un solo navegador. Sin embargo, puede añadir políticas de seguridad desde múltiples navegadores o sesiones de navegador.
- Las acciones de filtrado de URL de **continue (continuar)** o **override (anular)** no son compatibles y no funcionan con Proxy explícito.

Aprenda cómo configurar un proxy explícito.

- Strata Cloud Manager
- Panorama

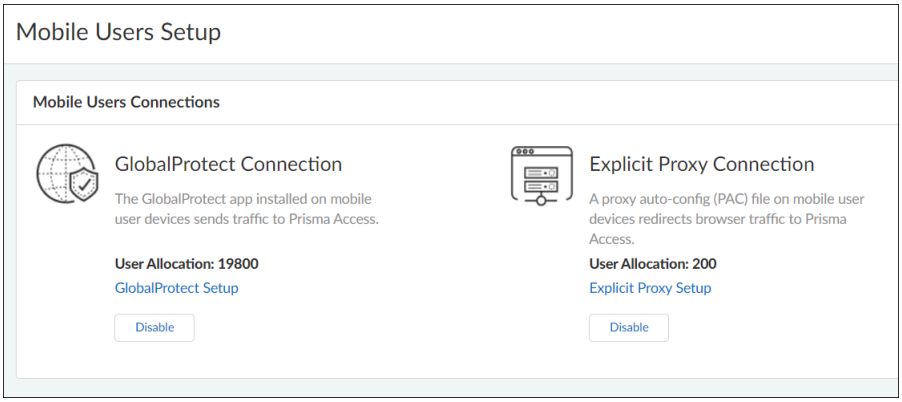
Cloud Management

Configure una conexión de proxy explícito para usuarios móviles; con proxy explícito, un archivo de configuración automática de proxy (PAC) en los dispositivos de usuario móvil redirige el tráfico del navegador a Prisma Access.

Antes de comenzar, asegúrese de revisar las directrices del proxy explícito.

STEP 1 | Habilitar proxy explícito y asignar usuarios

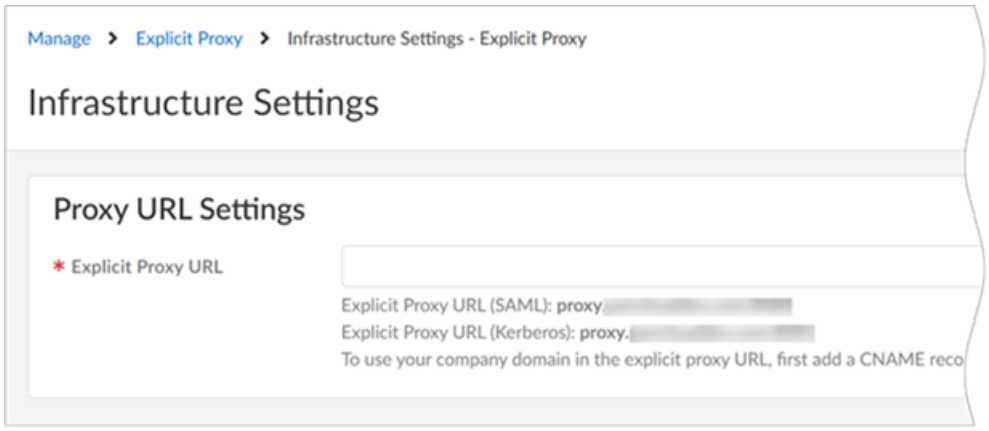
Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** para comenzar a configurar el proxy explícito. Al habilitar el proxy explícito, se le pedirá que especifique el número de usuarios móviles que usarán este tipo de conexión.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada la configuración de proxy que los usuarios móviles usarán para conectarse a Prisma Access

Vaya a la **Infrastructure Settings (Configuración de la infraestructura)**.



1. Especifique una dirección URL de proxy explícita.

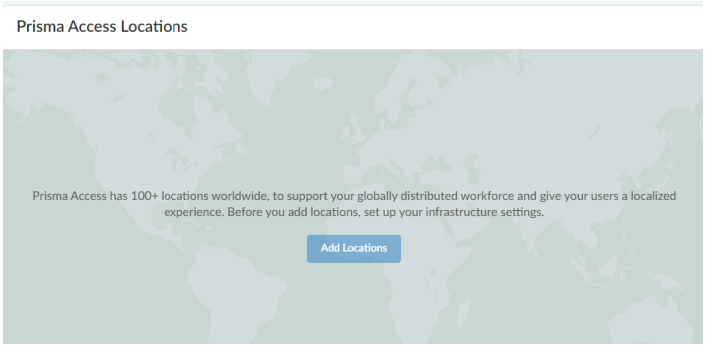
   De forma predeterminada, el nombre es *proxyname*.proxy.prismaaccess.com, donde *proxyname* es el subdominio que especifique, y utiliza el puerto 8080. Para usar el dominio de su empresa en la URL de proxy explícito, primero añada un registro CNAME al dominio de su organización.

   Puede utilizar los tipos de autenticación SAML o Kerberos para autenticar a los usuarios móviles.
2. (Opcional) Seleccione **Enable Agent Proxy (Habilitar proxy de agente)** para habilitar la funcionalidad de proxy basada en agente.

   Habilite esta funcionalidad para configurar el proxy explícito en Proxy Mode (Modo proxy) o Tunnel and Proxy Mode (Modo de túnel y proxy).
3. Utilice reglas de reenvío para crear un archivo PAC que cumpla con sus requisitos o cargue su propio archivo PAC en un perfil de reenvío.

STEP 3 | Seleccione la ubicación de Prisma Access a la que se conectarán los usuarios móviles

Añada las ubicaciones de Prisma Access en las que desea admitir usuarios móviles.



El mapa muestra las ubicaciones de Prisma Access.

Para obtener la mejor experiencia de usuario, si limita el número de ubicaciones, elija las ubicaciones más cercanas a sus usuarios o en el mismo país que sus usuarios. Si una ubicación

 ©2025 Palo Alto Networks, Inc.

no está disponible en el país donde residen los usuarios de dispositivos móviles, elija la ubicación más cercana a sus usuarios para obtener el mejor rendimiento.

Deberá habilitar las ubicaciones de proxy explícito en al menos dos regiones para garantizar la redundancia regional.

STEP 4 | Autenticar usuarios móviles.

Configure la **User Authentication (Autenticación de usuario)** para que solo los usuarios legítimos tengan acceso a sus servicios y aplicaciones.

SAML y Kerberos son los protocolos de autenticación compatibles. Prisma Access admite PingOne, Azure AD y Okta como proveedores de autenticación SAML, pero debe poder usar cualquier proveedor que admita SAML 2.0 como proveedor de identidad (IdP) SAML. Más información sobre cómo Permitir que los usuarios móviles se autentiquen en Prisma Access.

STEP 5 | Revise las reglas de seguridad de procedimientos recomendados que están activadas de forma predeterminada

Prisma Access aplica las reglas de política de seguridad de procedimientos recomendados de forma predeterminada. Estas reglas permiten a los usuarios navegar de forma segura por sitios generales de Internet. Los usuarios son:

- Bloqueado para visitar sitios web malos conocidos en función de la URL
- Bloqueado para cargar o descargar archivos que se sabe que son maliciosos
- Protegido de amenazas desconocidas y nunca antes vistas
- Protegido contra virus, spyware (ataques de comando y control) y vulnerabilidades

Después de pasar por la configuración inicial, puede revisar y actualizar estas reglas predeterminadas para satisfacer las necesidades de su empresa.

STEP 6 | Verifique que la ubicación de los usuarios móviles esté activa

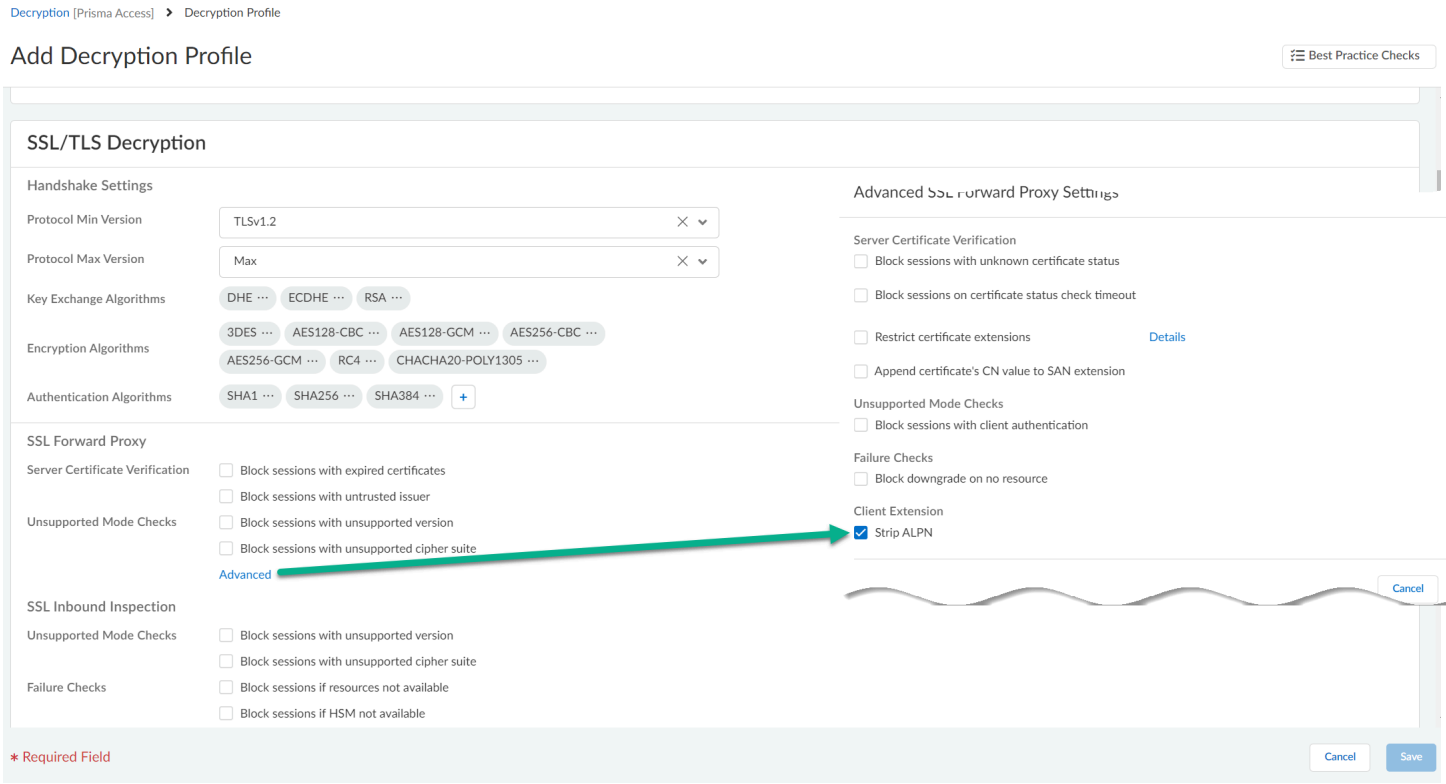
Una vez que haya enviado su configuración inicial a Prisma Access, Prisma Access comenzará a aprovisionar su entorno de usuario móvil. Esto puede tardar hasta 15 minutos. Cuando sus ubicaciones de usuario móvil estén en funcionamiento, podrá verificarlas en las páginas de configuración de usuarios móviles, el Resumen general y en Insights.

*También puede validar su configuración seleccionando **Manage (Gestionar)** > **Service Servicio (Configuración del servicio)** > **Mobile Users (Usuarios móviles)** y edite la configuración de infraestructura para confirmar que se ha configurado una puerta de enlace en cada una de las ubicaciones aprovisionadas.*

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Habilitación del descifrado para el tráfico de proxy explícito

- Establezca la versión máxima de TLS admitida en 1.2.
- Establezca **Strip ALPN (Quitar ALPN)** (Configuración avanzada de proxy de reenvío SSL) porque el proxy explícito no es compatible con HTTP/2 nativo y debe eliminar los encabezados ALPN.



STEP 8 | Descargue el CA raíz e instálelo en su endpoint para el descifrado SSL.

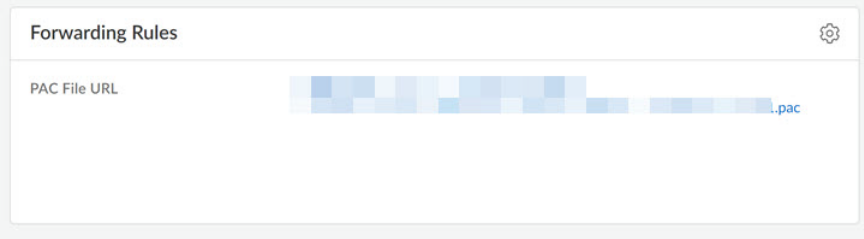
©2025 Palo Alto Networks, Inc.

STEP 9 | **Edit the PAC file content (Editar el contenido del archivo PAC).**

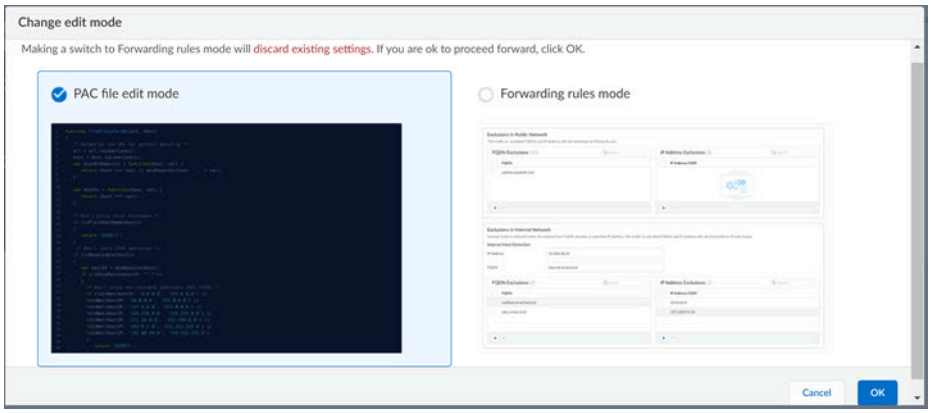
Utilice Perfiles de reenvío para gestionar archivos PAC.

Edite un archivo de configuración automática de proxy (PAC) para un proxy explícito que cumpla con sus requisitos. La aplicación GlobalProtect realiza un proxy del tráfico a Prisma Access basado en las reglas de reenvío y la lógica del archivo PAC.

Vaya a las **Forwarding Rules (Reglas de reenvío)**:



1. Descargue el archivo PAC y personalícelo para que satisfaga sus necesidades. A continuación, impórtalo de nuevo aquí y le daremos la URL de la ubicación en la que Prisma Access aloja el archivo PAC.
2. Edite el archivo PAC usando el modo **PAC File Editor (Editor de archivos PAC)** o **Forwarding rules mode (Modo de reglas de reenvío)**.
3. El modo **PAC File Editor (Editor de archivos PAC)** está seleccionado de forma predeterminada. Haga clic en **OK (Aceptar)** para editar en el modo de edición de archivos PAC.
4. Seleccione **Forwarding rules mode (Modo de reglas de reenvío)** y haga clic en **OK (Aceptar)** para editar en el modo de reglas de reenvío. Al cambiar al modo de reglas de reenvío, se descarta la configuración existente.



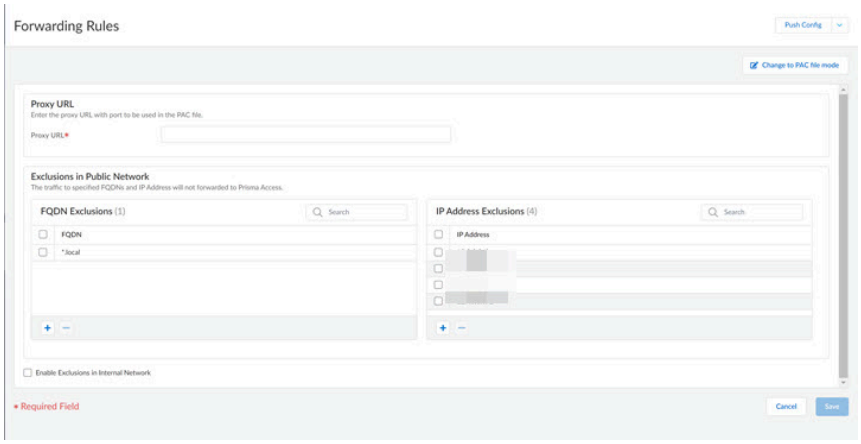
- Especifique la **Explicit Proxy URL (URL del Proxy explícito)** con el puerto que se utilizará en el archivo PAC.

  De forma predeterminada, el nombre es proxyname .proxy.prismaaccess.com, donde proxyname es el subdominio que especifique, y utiliza el puerto 8080.
- Configure **Exclusions in Public Network (Exclusiones en la red pública)** cuando los usuarios móviles del Proxy explícito se conectan a Prisma Access desde una red pública.

 ©2025 Palo Alto Networks, Inc.

- Configure **FQDN Exclusions (Exclusiones de FQDN)** y **IP Address Exclusions (Exclusiones de direcciones IP)**. Los FQDN y las direcciones IP excluidos no se reenviarán desde Prisma Access.

- **Enable Exclusions in Internal Network (Habilitar exclusiones en la red interna)** para configurar exclusiones para direcciones IP o FQDN específicos cuando los usuarios móviles de proxy explícito se conectan a Prisma Access en la red interna.
  - Especifique las siguientes exclusiones para tener diferentes exclusiones de tráfico cuando el usuario esté en la red interna.
    - Introduzca la **IP Address (Dirección IP)** (IPv4) de un host al que solo se tenga acceso desde la red interna.
    - Introduzca el **FQDN** que se resuelve en la dirección IP que introduzca.
  - Configure exclusiones para los FQDN y direcciones IP específicos. El tráfico a los FQDN y direcciones IP especificados no se reenviará desde Prisma Access.
- **Save (Guardar)** los cambios.

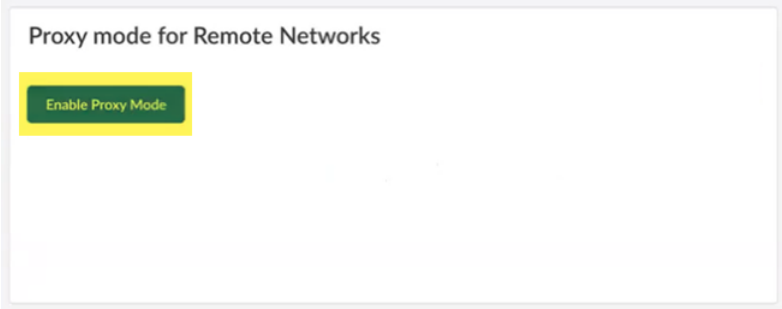


STEP 10 | Configure la **Advanced Security Settings (Configuración de seguridad avanzada)**.

- Si desea reenviar el tráfico al proxy explícito desde sus sucursales a través de un túnel IPSec seguro, deberá **Enable Proxy Mode (Habilitar el modo proxy)** y recuperar las direcciones

 ©2025 Palo Alto Networks, Inc.

IP de difusión por proximidad si desea utilizar Proxy explícito junto con una red remota de Prisma Access.



Esta solución utiliza direcciones de difusión por proximidad con un túnel IPSec de red remota para permitir que el proxy explícito se utilice para usuarios y dispositivos en un sitio de red remoto o una ubicación de sucursal.

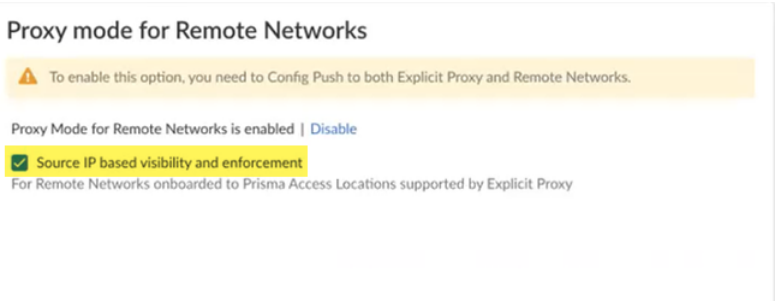
- Solo implementaciones en modo proxy Si el modo proxy está habilitado en las redes remotas, añada una política para permitir el tráfico enlazado a IP de difusión por proximidad y unidifusión en redes remotas. Si ha habilitado la **Source IP visibility and enforcement (Visibilidad y aplicación de IP de origen)**, utilice el campo de **Source IP (IP de origen)** en las políticas de seguridad en el Proxy explícito para asegurar el tráfico. Necesita políticas adicionales en las redes remotas.

 ©2025 Palo Alto Networks, Inc.

- (Opcional) Si habilita el modo de proxy, para aprovechar las direcciones IP privadas de los sistemas de las ubicaciones de las sucursales que reenvían el tráfico al proxy explícito, seleccione **Visibilidad y aplicación basadas en IP de origen**.

  Esta funcionalidad tiene estos requisitos:

  - Un plano de datos de Prisma Access de 10.2.4 como mínimo
  - Una implementación de Prisma Access (Managed by Panorama) con un complemento Cloud Services versión 4.1 como mínimo
  - Las direcciones IP de origen solo se muestran para las ubicaciones de red remota que son compatibles con el proxy explícito.



- Especifique **Block Sources (Bloquear origen)**.

  Añada cualquier tráfico de dirección IP de origen que deba bloquearse a la lista **Block Source Address (Bloquear dirección de origen)**.

  Especifique una dirección, un grupo de direcciones o una EDL.

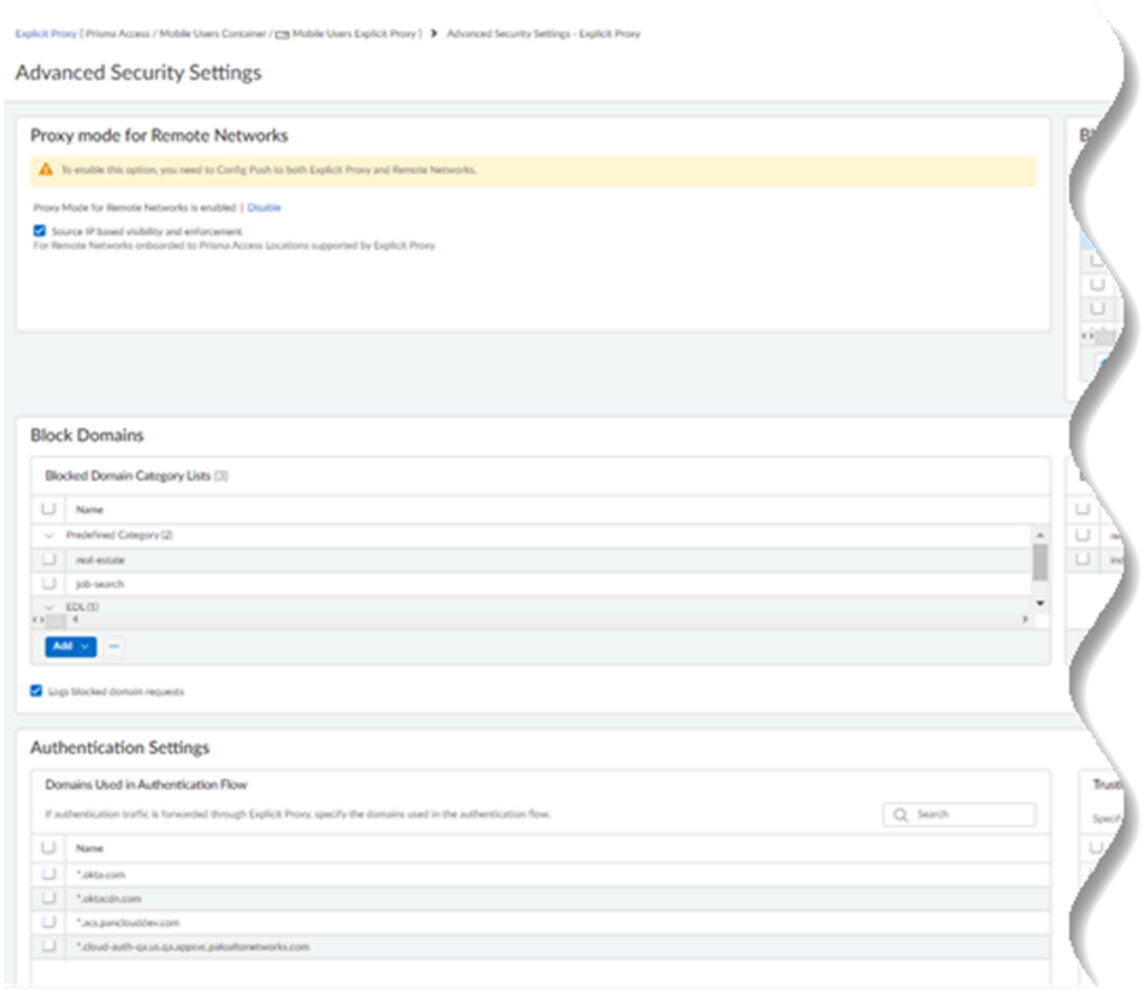
  Para excluir las entradas de la lista de direcciones IP de la aplicación, seleccione **Add Exception (Añadir excepción)** y seleccione las direcciones IP que desea excluir para que no se bloqueen.
- Especifique los **Blocked Domains (Dominios bloqueados)**.

  Especifique los dominios o las categorías de dominios de los sitios web malintencionados o de los sitios web a los que no desea que accedan los usuarios. Prisma Access impide que los usuarios accedan a las direcciones URL y direcciones IP especificadas en esta área cuando los usuarios inician un HTTP GET (para solicitudes no cifradas) o HTTP CONNECT (para

 ©2025 Palo Alto Networks, Inc.

solicitudes cifradas). Los usuarios reciben una página de bloqueo cuando intentan acceder a sitios web bloqueados.

- Si desea eximir los dominios que se incluyen en una lista de categorías de dominios bloqueados, especifíquelos en la casilla **Exception List (Lista de excepciones)**.

  Todos los dominios que se introduzcan están exentos de ser bloqueados, incluso si aparecen en una categoría de dominio que haya bloqueado.
- El proxy explícito requiere descifrado para autenticar a los usuarios. Introduzca los **Domains used in the authentication flow (Dominios utilizados en el flujo de autenticación)**.
- 

- Introduzca las direcciones IP desde las que se pueda permitir el tráfico de uso compartido de recursos (CORS) de origen cruzado (CORS) HTTPS o HTTP sin descifrar la **Trusted Source Address (Dirección de origen de confianza)**.
- Para omitir la autenticación de las direcciones de origen de confianza que haya introducido, seleccione **Skip authentication (Omitir la autenticación**.

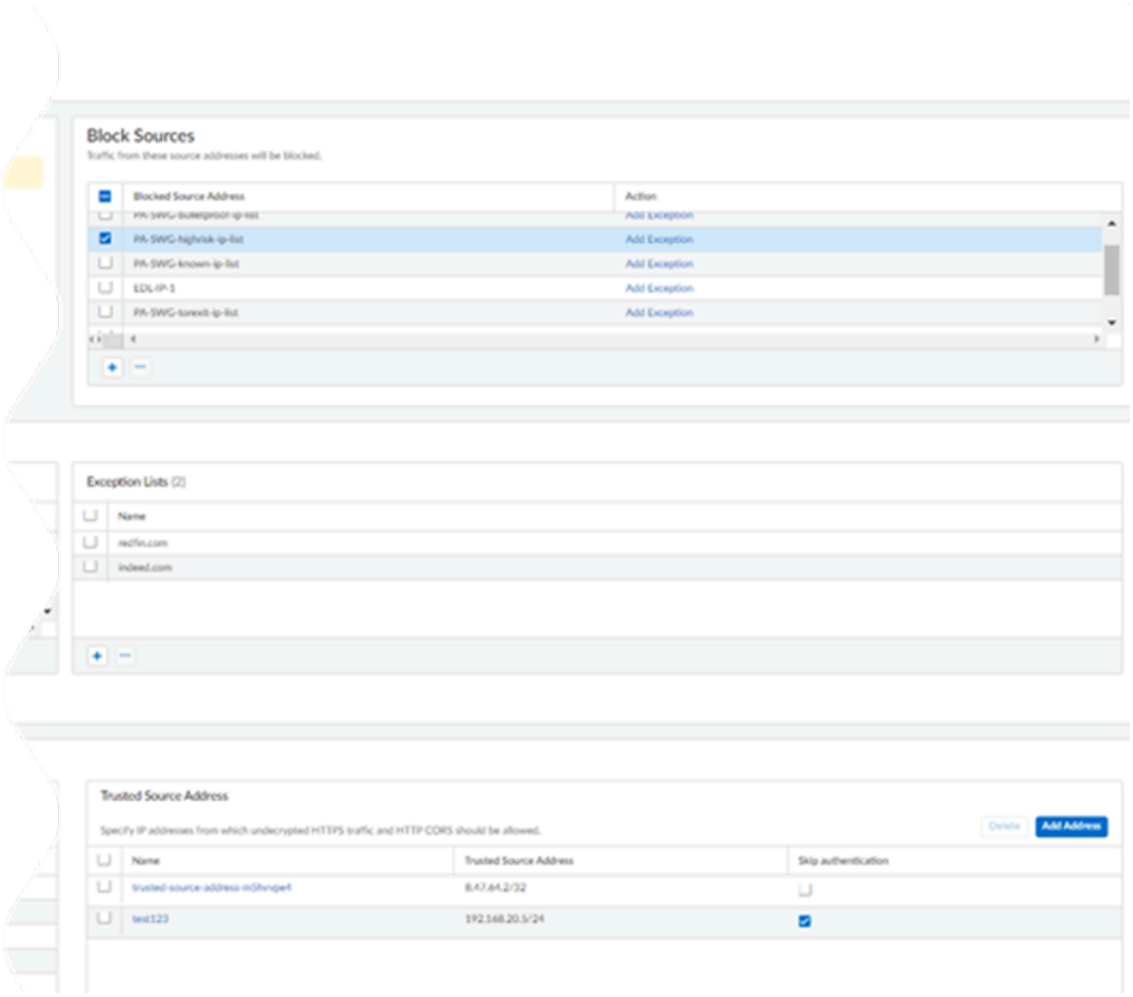
  Puede usar **Skip authentication (Omitir la autenticación)** con **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)** para omitir la autenticación

 ©2025 Palo Alto Networks, Inc.

de sistemas sin periféricos que no pueden autenticarse, configurar políticas de seguridad y obtener visibilidad del tráfico en Prisma Access Proxy explícito.

Puede añadir direcciones IP o subredes. Se admite un máximo de 100.000 direcciones IP después de expandir las subredes.

Si selecciona **Skip authentication (Omitir la autenticación)** para omitir la autenticación de un objeto de dirección y más adelante desea habilitar la autenticación anulando la selección **Skip authentication (Omitir la autenticación)** para ese objeto de dirección, los cambios pueden tardar hasta 24 horas en surtir efecto después de Confirmar y enviarlos.

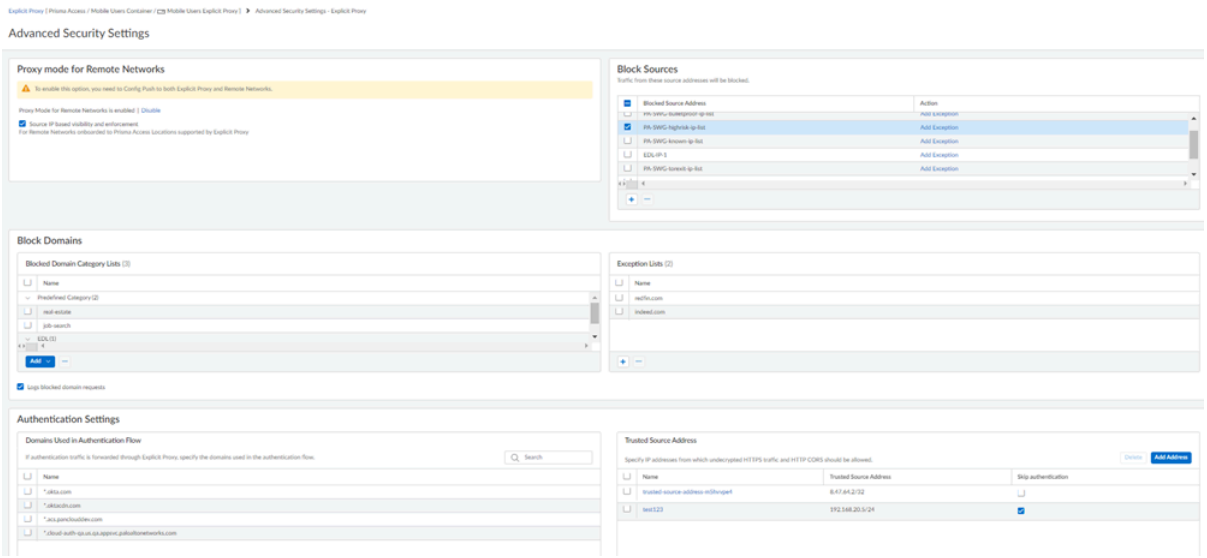
- 

- Si tiene una implementación de proxy explícito y ha añadido una lista de direcciones IP de origen de confianza, puede **Use X-Authenticated-User (XAU) headers on incoming HTTP/HTTPS requests for identity (Usar de encabezados X-Authenticated-User (XAU) en las solicitudes HTTP/HTTPS entrantes para la identidad)**. Utilice esta funcionalidad para

 ©2025 Palo Alto Networks, Inc.

permitir que los usuarios que hayan iniciado sesión desde otro proxy utilicen encabezados XAU para la autenticación.

*Debe hacer clic en **Save (Guardar)** para que la configuración de XAU surta efecto.*



Configurar un proxy explícito (Panorama)

Para proteger a los usuarios móviles con un proxy explícito, complete los siguientes pasos.

Antes de configurar el proxy explícito, revise la lista de comprobación de planificación) y conozca cómo configurar el archivo PAC del proxy explícito.

STEP 1 | Configurar la autenticación para proxy explícito.

SAML y Kerberos son los tipos de autenticación admitidos.

Utilice las siguientes pautas al configurar la autenticación SAML para el IdP y en Panorama:

- **Directrices de Panorama:**
  - Configure un **SAML Identity Provider (Proveedor de identidad SAML)** y un **Authentication Profile (Perfil de autenticación)** para Prisma Access. El perfil de autenticación que creará lo especificará en un paso posterior.
  - Asegúrese de configurar el perfil de autenticación en **Explicit_Proxy_Template**.
  - Utilice **mail (correo)** como atributo de usuario en el perfil del servidor IdP y en el **Authentication Profile (Perfil de autenticación)** en Panorama.
  - El proxy explícito no admite la **Sign SAML Message to IdP (Firma de mensajes SAML al IdP)** en el perfil del servidor del proveedor de identidad SAML.
  - Cuando configure Cloud Identity Engine para recuperar información de asignación de usuarios y grupos, utilice **mail (correo)** o **userPrincipalName** como **SamAccountName** en la asignación de grupos.
  - Al configurar la **Group Mapping Settings (Configuración de asignación de grupos)** durante la configuración de proxy explícito, use el mismo atributo de directorio para

 ©2025 Palo Alto Networks, Inc.

el nombre de usuario principal y el correo electrónico, o Prisma Access no refleja con precisión el número de usuarios. Por ejemplo, dado el siguiente perfil de usuario:

```
sAMAccountName: muser Netbios: example userPrincipalName:
 muser@example.com mail: mobile.user@example.com
```

Si, en la configuración de Cloud Identity Engine, utiliza un **Primary Username (Nombre de usuario principal)** de `userPrincipalName` y un **E-mail (Correo electrónico)** de `mail (correo)`, la información del usuario que Strata Logging Service devuelve en los logs de tráfico y la información del usuario que el ACS devuelve en los logs de autenticación serán diferentes. En este ejemplo, ACS envía el atributo de **mail (correo)** (mobile.user@example.com) a los logs de autenticación y Strata Logging Service envía el atributo **userPrincipalName** (muser@example.com) a los logs de tráfico. Como resultado de esta falta de coincidencia, su recuento de usuarios no será preciso en los campos **Current Users (Usuarios actuales)** y **Users (Last 90 days) [Usuarios (últimos 90 días)]** al verificar el estado de Proxy explícito en la página Estado (**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)**. Por este motivo, utilice el mismo atributo de directorio para el **Primary Username (Nombre de usuario principal)** y el **E-mail (Correo electrónico)** [por ejemplo, **mail (correo)**] al especificar la **Group Mapping Settings (Configuración de asignación de grupos)**.

- Al utilizar Panorama para gestionar Prisma Access, Cloud Identity Engine no completa automáticamente la información de usuarios y grupos en las reglas de política de seguridad.

- **Directrices de idP:**
  - Utilice las siguientes URL al configurar SAML:

    URL del **Servicio de consumidor de aserciones SAML**: **`https://global.acs.prismaaccess.com/saml/acs`**

    URL de **ID de entidad**: **`https://global.acs.prismaaccess.com/saml/metadata`**
  - Si utiliza Okta como IdP, utilice **EmailAddress** para la configuración de **Name ID Format (Formato de ID de nombre)**.
  - Introduzca una URL de inicio de sesión única de `https://global.acs.prismaaccess.com/saml/acs`.
  - No se admite el cierre de sesión único (SLO).
  - Para solucionar problemas de autenticación del IdP, utilice las capacidades de supervisión y resolución de problemas del IdP. El ACS no registra errores de autenticación de IdP.
  - Al crear un **Authentication Profile (Perfil de autenticación)** para el IdP SAML, en la pestaña **Advanced (Avanzado)**, seleccione **all (todos)** en la **Allow List (Lista de permitidos)** o el proxy explícito no podrá recuperar la asignación de grupos.

 ©2025 Palo Alto Networks, Inc.

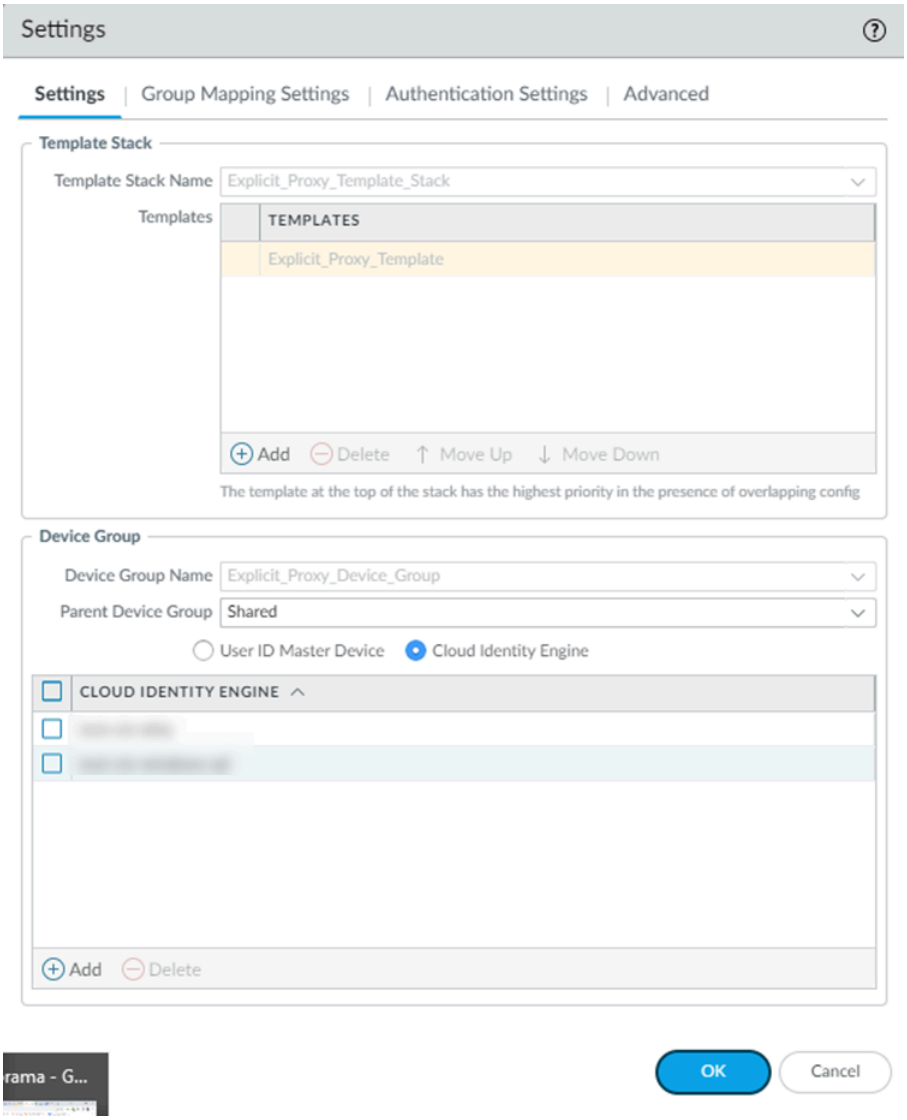
STEP 2 | Configure la configuración de proxy explícito.

1. Select **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** y haga clic en el icono de engranaje para editar la **Settings (Configuración)** de proxy explícito.
2. En la pestaña **Settings (Configuración)**, edite las siguientes configuraciones:
   - (Opcional) Verifique los nombres de la plantilla y de la pila de plantillas.

     Por defecto, Prisma Access crea una nueva pila de plantillas **Explicit_Proxy_Template_Stack** y una nueva plantilla **Explicit_Proxy_Template**. Asegúrese de utilizar esta plantilla al crear y editar la configuración de su **Device (Dispositivo)** en Panorama.
   - En la sección Grupo de dispositivos, seleccione el **Parent Device Group (grupo de dispositivos principal)** que contiene las configuraciones que desea enviar para el proxy explícito, o deje el grupo de dispositivos principal como **Shared (Compartido)** para usar la jerarquía compartida del grupo de dispositivos de Prisma Access. El **Device Group Name (Nombre del grupo de dispositivos)** no se puede cambiar.
   - (Opcional) Si ha configurado un cortafuegos de nueva generación como dispositivo principal o añadió un perfil de Cloud Identity Engine para rellenar la información de usuario y grupo en las políticas de seguridad, seleccione el dispositivo maestro de User-ID o Cloud Identity Engine; luego, seleccione el perfil Dispositivo principal o el perfil de Cloud Identity Engine que creó.

 ©2025 Palo Alto Networks, Inc.

- En la sección Asignación de licencia, especifique la cantidad de usuarios móviles que desea asignar para el proxy explícito.



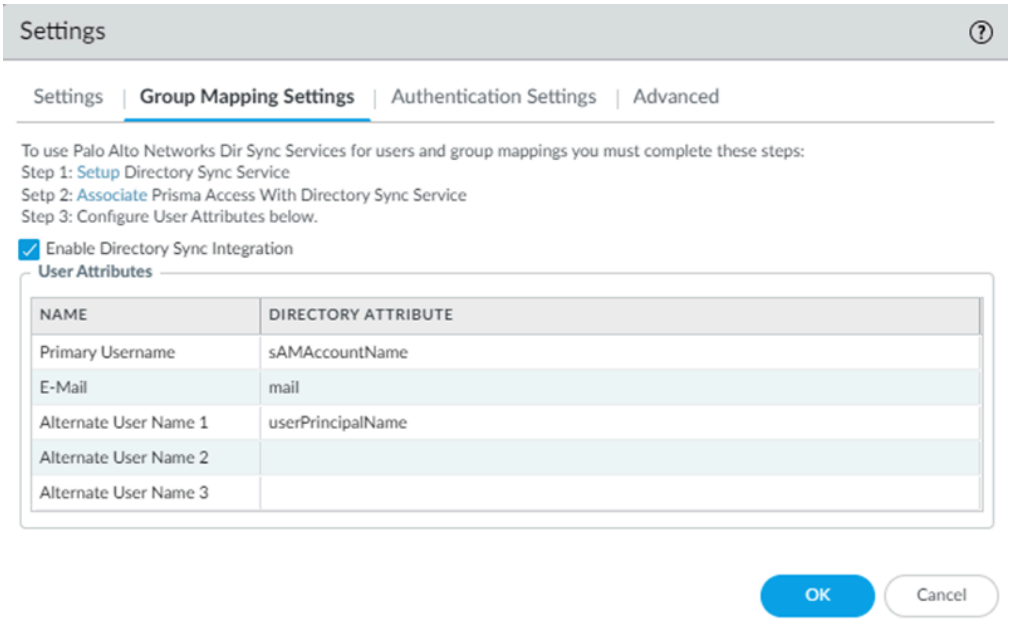
3. En la pestaña **Group Mapping Settings (Configuración de asignación de grupos)**, deberá **Enable Directory Sync Integration (Habilitar la integración de sincronización de**

 ©2025 Palo Alto Networks, Inc.

directorios) (ahora conocida como Cloud Identity Engine) para configurar Prisma Access para utilizar Cloud Identity Engine para recuperar información de usuarios y grupos.

Utilice Cloud Identity Engine para completar la información de asignación de usuarios y grupos para una implementación de proxy explícito.

Introduzca el **mail (correo)** para el atributo de directorio en el campo **Primary Username (Nombre de usuario principal)** y el **mail (correo)** para el campo **E-Mail (Correo electrónico)**.



4. Haga clic en **OK (Aceptar)** cuando haya terminado.

STEP 3 | (Opcional) Configure los ajustes de BGP.

Utilice la configuración de bloqueo para bloquear el acceso a un destino de Internet en la etapa de resolución de DNS.

Para restringir el acceso al Proxy explícito a direcciones IP de origen específicas, también puede utilizar objetos especiales. Estos objetos de dirección, grupos de direcciones y listas dinámicas externas (EDL) que utilizan nombres específicos permiten las direcciones IP que usted especifica para el tráfico de Internet y bloquean cualquier otra dirección IP.

STEP 4 | En la pestaña **Authentication Settings (Configuración de autenticación)**, configure las ajustes de descifrado, X-Authenticated-User (XAU) y autenticación.

1. Configure sus ajustes para el tráfico descifrado.
   - Seleccione **Decrypt Traffic That Matches Existing Decryption rules; For Undecrypted Traffic, Allow Traffic Only From Known IPs Registered By Authenticated Users (Descifrar tráfico que coincida con las reglas de descifrado existentes; para tráfico**

 ©2025 Palo Alto Networks, Inc.

no descifrado, permitir tráfico solo desde direcciones IP conocidas registradas por usuarios autenticados) para configurar las siguientes reglas de descifrado:

- El tráfico que coincida con las reglas de política de descifrado que haya configurado con una **Action (Acción)** para **Decrypt (Descifrar)** o **Decrypt and Forward (Descifrar y reenviar)** se descifrará.

  Si un usuario accede a un sitio HTTPS no cifrado y aún no se ha autenticado en el Proxy explícito desde esa dirección IP, el usuario queda bloqueado. Sin embargo, el usuario puede acceder a un sitio descifrado, completar la autenticación y luego acceder a sitios no descifrados.
- Se permite el tráfico no cifrado desde direcciones IP desde las que el usuario móvil ya se ha autenticado.

El proxy explícito requiere descifrado para autenticar a los usuarios. Introduzca los dominios que se pueden descifrar en una categoría de URL personalizada; luego, especifique esas categorías en **If Authentication traffic is forwarded through Explicit Proxy, specify the domains used in the authentication flow (Si el tráfico de autenticación se reenvía a través de proxy explícito, especifique los dominios utilizados en el flujo de autenticación)**.

Añada únicamente los dominios necesarios para la autenticación a la categoría de URL personalizada que especifique, incluidos todos los FQDN de IdP y ACS. Debe añadir URL de autenticación a la categoría URL personalizada, incluso si las ha añadido a una política de descifrado.

- Para permitir que se descifre todo el tráfico, seleccione **Decrypt All traffic (Overrides Existing Decryption Rules) [Descifrar todo el tráfico (anula las reglas de descifrado existentes)]**.

  Si selecciona este botón de opción, asegúrese de que:

  - No tiene excepciones en su política de descifrado.
  - Está aplicando restricciones basadas en la dirección IP de origen en su política de seguridad.

  No seguir estas recomendaciones permite el abuso del Proxy explícito como un proxy abierto que puede usarse de forma generalizada como servicio de reenvío para realizar ataques de denegación de servicio.

  - Tiene al menos un certificado de proxy de reenvío SSL especificado como **Forward Trust Certificate (Certificado de confianza de reenvío)**.

    Si no tiene un certificado de confianza de reenvío, cree uno en Panorama; luego, vaya a **Commit and Push (Confirmar y enviar)** sus cambios a Prisma Access. Si

 ©2025 Palo Alto Networks, Inc.

no dispone de un certificado de confianza de reenvío, se producirá un error de confirmación cuando confirme los cambios de Proxy explícito.

2. (Opcional) Introduzca cualquier dirección IP desde la cual se debe permitir el tráfico HTTP o HTTP Cross-Origin Resource Sharing (CORS) sin cifrar hacia la **Trusted Source Address Auth Bypass (Omisión de autenticación de dirección de fuente fiable)**.

   Añada las direcciones IP a los objetos de dirección basados en direcciones IP y luego **Add (añadir)** para añadir los objetos de dirección en el campo.

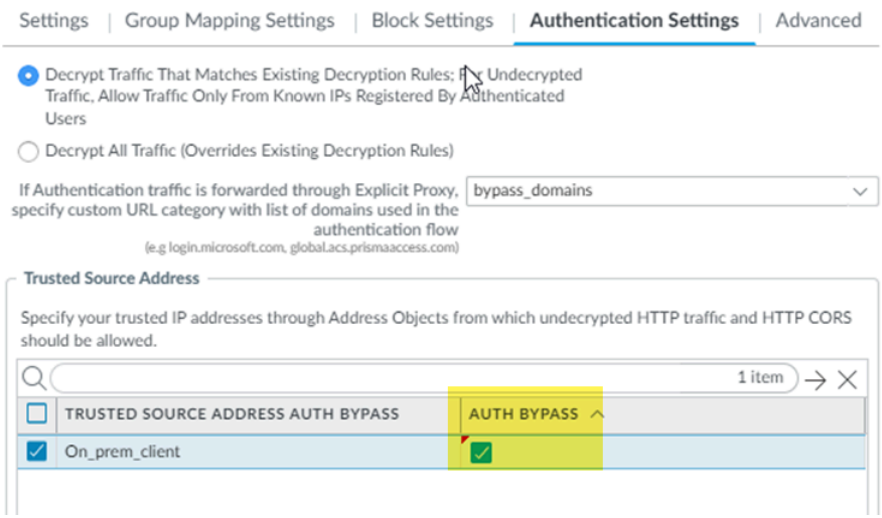
   Introduzca un máximo de 100,000 entradas. Asegúrese de que el objeto de dirección utilice únicamente direcciones IP.

3. (Opcional) Para omitir la autenticación de cualquier dirección de fuente fiable que haya introducido, seleccione **Auth Bypass (Omitir autenticación)**.

   Puede usar **Auth Bypass (Omitir autenticación)** con **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)** para omitir la autenticación de sistemas sin cabeza que no pueden autenticar, configurar políticas de seguridad y obtener visibilidad del tráfico en el Proxy explícito de Prisma Access.

   Puede añadir direcciones IP o subredes. Se admiten un máximo de 100,000 direcciones IP después de expandir las subredes.

   Si selecciona **Auth Bypass (Omisión de autenticación)** para omitir la autenticación de un objeto de dirección y más adelante desea habilitar la autenticación anulando la selección **Auth Bypass (Omisión de autenticación)** para ese objeto de dirección, el cambio puede tardar hasta 24 horas en surtir efecto después de realizarlo y confirmar y enviar sus cambios.



4. (Opcional) Para permitir que las direcciones IP de la fuente fiable utilicen XAU para la identidad, seleccione **Use X-Authenticated-User (XAU) header on incoming HTTP/**

 ©2025 Palo Alto Networks, Inc.

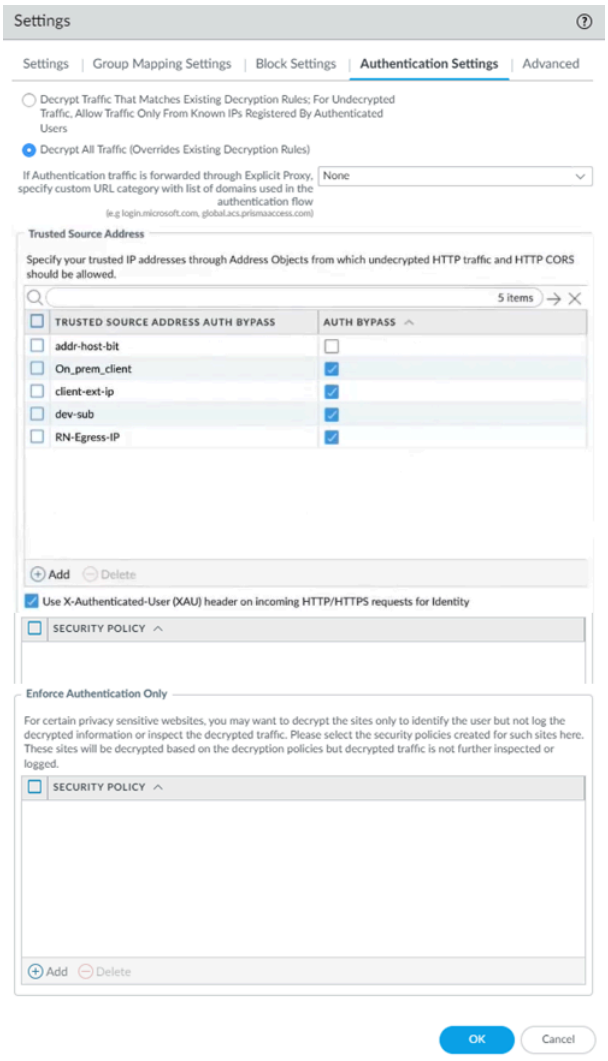
HTTPS requests for Identity (Usar el encabezado X-Authenticated-User (XAU) en las solicitudes HTTP/HTTPS entrantes para la identidad).

Seleccione esta opción si está usando encadenamiento de proxy desde un proxy de terceros a un proxy explícito, los usuarios se han autenticado en ese proxy y el proxy usa encabezados XAU.

Los encabezados XAU son los únicos encabezados HTTP compatibles con la ingesta de encabezados de proxy explícito. Los encabezados X-Forwarded-For (XFF) no son compatibles.

5. (Opcional) Especifique la configuración para sitios web sensibles a la privacidad creando reglas de políticas de seguridad para esos sitios y luego especificando la **Security Policy (Política de seguridad)** o las políticas para esos sitios en el área **Authentication Only (Solo autenticación)**.

   Para cualquier sitio web que especifique en la **Security Policy (Política de seguridad)** o en las políticas que añada, Proxy explícita descifra los sitios web según las políticas de descifrado, pero no inspecciona ni registra el tráfico descifrado.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Configure la configuración **Advanced (Avanzado)**.

1. Si desea reenviar el tráfico al proxy explícito desde sus sucursales a través de un túnel IPSec seguro, deberá **Enable Proxy Mode (Habilitar el modo proxy)** y recuperar las direcciones IP de difusión por proximidad si desea utilizar Proxy explícito junto con una red remota de Prisma Access.

   Esta solución utiliza direcciones de difusión por proximidad con un túnel IPSec de red remota para permitir que el proxy explícito se utilice para usuarios y dispositivos en un sitio de red remoto o una ubicación de sucursal.
2. (Opcional) Para aprovechar las direcciones IP privadas de los sistemas en sus ubicaciones de sucursales que están reenviando tráfico al Proxy explícito, seleccione la **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)**.

   Esta funcionalidad tiene estos requisitos:

   - Un plano de datos de Prisma Access de 10.2.4 como mínimo
   - Una implementación de Prisma Access (Managed by Panorama) con un complemento Cloud Services de 4.1 como mínimo
   - Las direcciones IP de origen solo se muestran para las direcciones IP de una red remota después de haber configurado una implementación de Proxy explícito de redes remotas y solo las direcciones de origen en ubicaciones de redes remotas que son compatibles con Proxy explícito.
3. Solo implementaciones en modo proxy Si el modo proxy está habilitado en las redes remotas, añada una política para permitir el tráfico enlazado a IP de difusión por proximidad y unidifusión en redes remotas. Si ha habilitado la **Source IP visibility and enforcement (Visibilidad y aplicación de IP de origen)**, utilice el campo de **Source IP (IP de origen)** en las políticas de seguridad en el Proxy explícito para asegurar el tráfico. Necesita políticas adicionales en las redes remotas.
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Haga clic en **Configure (Configurar)** para configurar el proxy explícito.

1. Especifique un **Explicit Proxy FQDN (FQDN de proxy explícito)**.

   De forma predeterminada, el nombre es *proxyname*.proxy.prismaaccess.com, donde *proxyname* es el subdominio que especifique, y utiliza el puerto 8080. Si desea utilizar el nombre de dominio de su organización en la URL de proxy explícita (por ejemplo, thisproxy.proxy.mycompany.com), introduzca un registro CNAME del dominio de su organización.

   Por ejemplo, para asignar una URL de proxy llamada thisproxy.prismaaccess.com a un proxy llamado thisproxy.proxy.mycompany.com, deberá añadir un CNAME de thisproxy.proxy.prismaaccess.com al registro CNAME en el dominio de su organización.
2. (Opcional) Seleccione **Use GlobalProtect Agent to Authenticate (Usar agente de GlobalProtect para autenticar)** para habilitar la funcionalidad de proxy basada en agente.

   Habilite esta funcionalidad para configurar el proxy explícito en Proxy Mode (Modo proxy) o Tunnel and Proxy Mode (Modo de túnel y proxy). También debe seleccionar

 ©2025 Palo Alto Networks, Inc.

esta casilla de verificación para habilitar la **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)**.

3. Especifique un **Authentication Profile (Perfil de autenticación)** y **Cookie Lifetime (Vida útil de la cookie)**.

   - Especifique el **Authentication Profile (Perfil de autenticación)** SAML que utilizó en el Paso 1 o añada un perfil de autenticación**New (Nuevo)** para usar con Prisma Access.

     Debe configurar la autenticación SAML, incluida la configuración de un **SAML Identity Provider (Proveedor de identidad SAML)** (IdP) y un **Authentication Profile (Perfil de autenticación)**, para utilizar un proxy explícito.

   - (Opcional) Especifique una **Cookie Lifetime (Vida útil de la cookie)** para la cookie que almacena las credenciales de autenticación de los usuarios.

     Prisma Access almacena en caché las credenciales del usuario y las almacena en forma de cookie. Para cambiar el valor, especifique el tiempo a utilizar en Segundos, Minutos, Horas o Días.

     Para evitar problemas con los usuarios que no pueden descargar archivos grandes antes de que expire la duración de la cookie, o la cookie expire cuando los usuarios están accediendo a un solo sitio web durante un largo período de tiempo, Palo Alto Networks recomienda que configure una Cookie Lifetime (Vida útil de la cookie) de al menos un día. Si los usuarios de Proxy explícito tienen un problema de caducidad de la duración de la cookie, pueden navegar a un sitio web diferente para volver a autenticarse en ACS y actualizar la cookie de ACS.

     Si está descargando un archivo y la descarga del archivo demora más que el **Cookie Lifetime (Tiempo de vida útil de la cookie)**, la descarga del archivo finalizará cuando expire el valor de vida útil. Por este motivo, considere utilizar una **Cookie Lifetime (Vida útil de la cookie)** más larga si descarga archivos grandes que tardan mucho tiempo en descargarse.

STEP 7 | Seleccione las **Locations (Ubicaciones)** y las regiones asociadas con esas ubicaciones donde desea implementar su Proxy explícito para usuarios móviles. Prisma Access añade un nodo proxy en cada ubicación que seleccione.

El proxy explícito es compatible con un subconjunto de todas las ubicaciones de Prisma Access. Ver Directrices de la configuración de proxy explícito para la lista de ubicaciones.

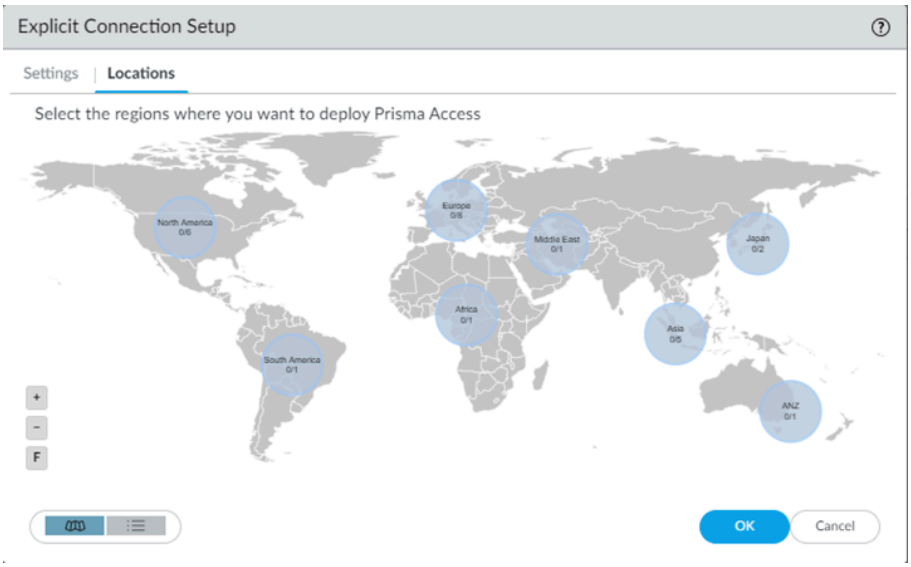
La pestaña **Locations (Ubicaciones)** muestra un mapa. Al resaltar el mapa se muestran las regiones globales (América, Europa y Asia Pacífico) y las ubicaciones disponibles dentro de

 ©2025 Palo Alto Networks, Inc.

cada región. Seleccione una región y luego seleccione las ubicaciones que desea implementar en cada región.

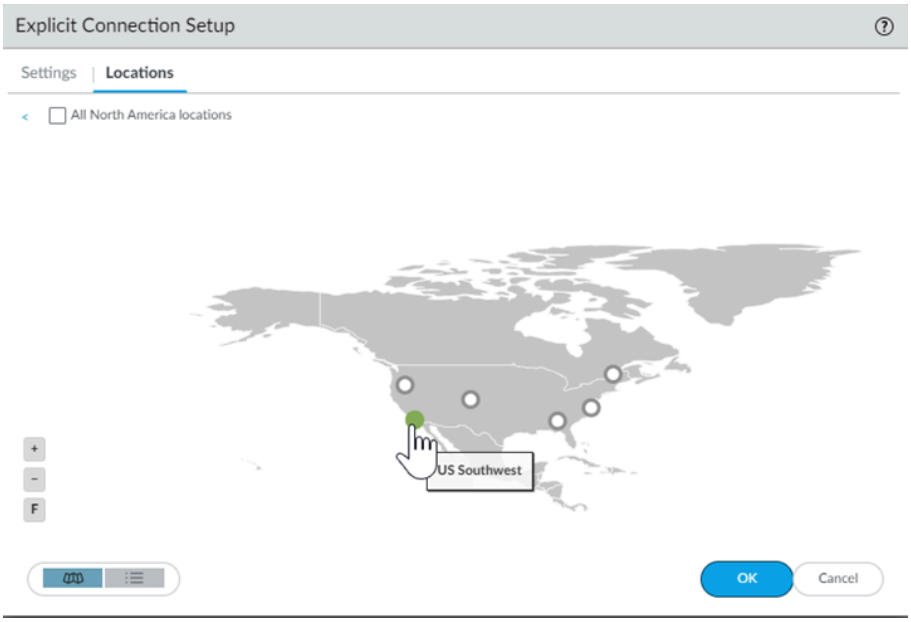
Deberá habilitar las ubicaciones de proxy explícito en al menos dos regiones para garantizar la redundancia regional.

1. Haga clic en la pestaña **Location (Ubicaciones)** y seleccione una región.



2. Seleccione una o más ubicaciones de proxy explícito dentro de la región seleccionada usando el mapa.

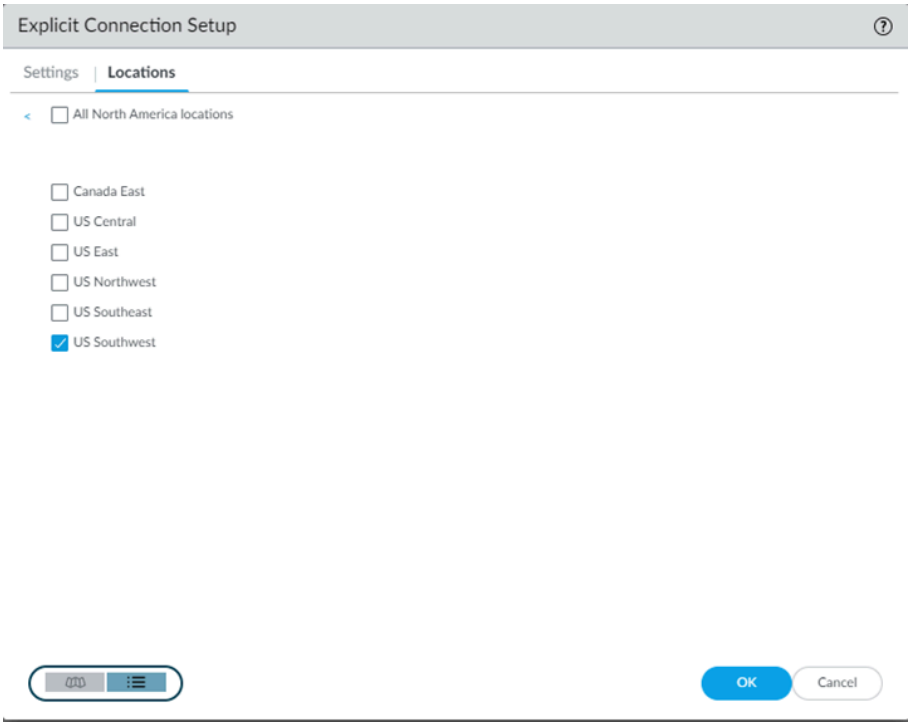
   Al pasar el cursor sobre una ubicación, ésta se resalta. Los círculos blancos indican una ubicación disponible; los círculos verdes indican que ha seleccionado esa ubicación.



   Además de la vista del mapa, puede ver una lista de regiones y ubicaciones. Elija entre la vista de mapa y la vista de lista en la esquina inferior izquierda. En la vista de lista, la lista muestra regiones ordenadas por columnas, con todas las ubicaciones ordenadas por

 ©2025 Palo Alto Networks, Inc.

región. Puede seleccionar **All (Todos)** los sitios dentro de una región (parte superior del cuadro de diálogo).



3. Haga clic en **OK (Aceptar)** para añadir las ubicaciones.

STEP 8 | Configure reglas de política de seguridad para aplicar las políticas de seguridad de su organización.

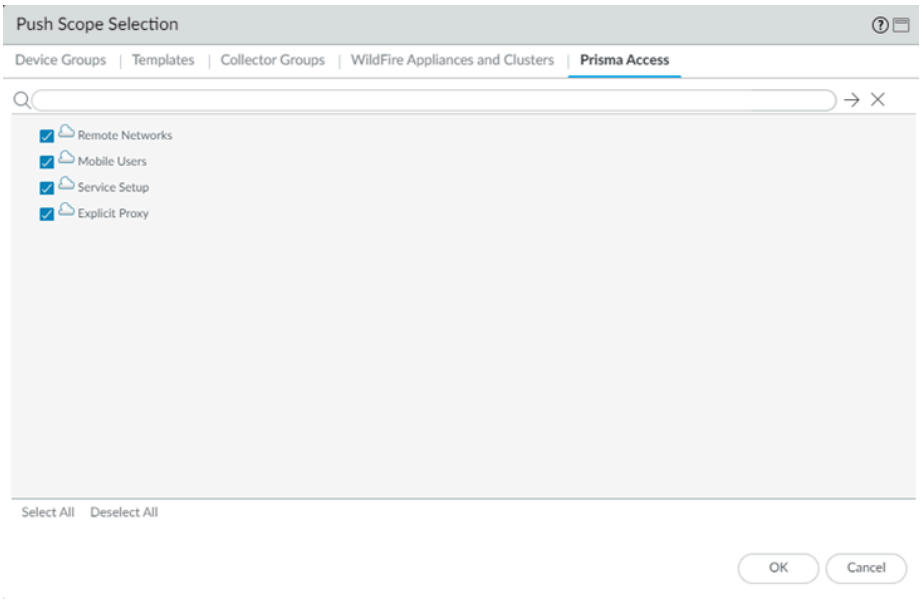
Para realizar los cambios de configuración necesarios y controlar las URL a las que los usuarios móviles pueden acceder desde el proxy explícito, utilice políticas de seguridad. Utilice las siguientes pautas y requisitos al configurar sus políticas de seguridad:

- En función de sus objetivos comerciales, cree políticas de seguridad para aplicaciones SaaS y de Internet autorizadas utilizando App-ID y grupos de usuarios que necesitan acceso a esas aplicaciones.
- Adjunte perfiles de seguridad a todas las reglas de política de seguridad para poder prevenir amenazas conocidas y desconocidas siguiendo las prácticas recomendadas de perfiles de seguridad.

©2025 Palo Alto Networks, Inc.

STEP 9 | Realice sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Deberá **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access**, asegúrese de que **Proxy explícito** esté seleccionado en el **Push Scope (Ámbito de envío)**, luego haga clic en **OK (Aceptar)**.



3. Haga clic en **Commit and Push (Confirmar y enviar)**.

STEP 10 | Seleccione el archivo PAC que desea utilizar con Proxy explícito.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)** > **Explicit Proxy (Proxy explícito)**.

   Asegúrese de introducir un puerto 8080 en el archivo PAC.
2. Seleccione el **Connection Name (Nombre de conexión)** para la configuración de proxy explícito que acaba de configurar.
3. Introduzca el **PAC (Proxy Auto-Configuration) File [Archivo PAC (configuración automática de proxy)]** que se utilizará para el proxy explícito.

   Asegúrese de comprender cómo funcionan los archivos PAC y cómo modificarlos antes de cargarlos en Prisma Access.



   Browse (Examinar) y cargar el archivo.

   Prisma Access le proporciona un archivo PAC de muestra; puede **Download sample PAC file (Descargar un archivo PAC de muestra)**, cambiar los valores y cargar ese archivo. Consulte Configurar su archivo PAC de proxy explícito para conocer los requisitos y las pautas del archivo PAC, así como una descripción del contenido del archivo PAC de muestra.

 ©2025 Palo Alto Networks, Inc.

Autenticación Kerberos para implementaciones de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Implementaciones de Prisma Access Mobile: Proxy explícito compatibles con la autenticación Kerberos. Si tiene servidores, dispositivos IoT o máquinas sin periféricos que no pueden autenticarse mediante SAML, puede usar la autenticación Kerberos en su lugar.

Si la implementación utiliza SAML y Kerberos para la autenticación, puede configurar ambos tipos de autenticación en una única implementación de proxy explícito. De esta manera, puede autenticar a los usuarios móviles con SAML mientras autentica servidores, dispositivos IoT o máquinas sin cabeza con Kerberos. El proxy explícito de Prisma Access procesa la autenticación en función del puerto utilizado para el tráfico de autenticación:

- Si el tráfico de autenticación usa el puerto 8080, el proxy explícito usa la autenticación SAML.
- Si el tráfico de autenticación usa el puerto 8081, el proxy explícito usa la autenticación Kerberos.

Si solo se configura un puerto, el puerto que no está configurado utiliza el mismo perfil de autenticación que el puerto configurado.

El inicio de sesión único de Kerberos solo está disponible para los endpoints y los sistemas que tienen acceso a la infraestructura de Kerberos. Los endpoints y sistemas sin acceso a la infraestructura de Kerberos deben usar el SSO de SAML.

- Requisitos y recomendaciones para la implementación de Kerberos para implementaciones de proxy explícito
- Cree un keytab de Kerberos.
- Configure la autenticación Kerberos para implementaciones de proxy explícito

Requisitos y recomendaciones para la implementación de Kerberos para implementaciones de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licencia de Prisma Access ☐ Versión mínima de plano de datos requerida: PAN-OS 10.1.3 o versiones posteriores

Antes de crear una keytab de Kerberos para implementar Kerberos en una implementación de proxy explícito, asegúrese de que la implementación de Kerberos tenga los siguientes requisitos y requisitos previos:

©2025 Palo Alto Networks, Inc.

- Actualice el plano de datos a PAN-OS 10.1.3 o versiones posteriores.
- Asegúrese de que tiene una cuenta de Kerberos que pueda usar para que Prisma Access autentique los servidores o dispositivos.

  Se requiere una cuenta para crear un keytab de Kerberos, que es un archivo que contiene el nombre principal y la contraseña de Kerberos cifrada.
- Asegúrese de que los servidores y los endpoints estén unidos a un dominio, lo que permite a los usuarios y equipos conectarse de forma segura a su dominio de trabajo mediante sus credenciales de red de trabajo.
- Asegúrese de reenviar el tráfico de autenticación Kerberos al puerto 8081 en el archivo PAC de los usuarios móviles o en la configuración de proxy en el endpoint o los servidores.

  El proxy explícito usa el puerto 8081 para la autenticación Kerberos y el puerto 8080 para la autenticación SAML.
- Asegúrese de que el administrador de Kerberos tenga la capacidad de crear y exportar keytabs.
- Asegúrese de que tiene las direcciones IP de salida de la sucursal o ubicación del campus donde se encuentran los servidores, los dispositivos IoT o los equipos sin periféricos.

  Estas direcciones IP se añaden a la lista de direcciones en las que confía el proxy explícito.
- Siga las prácticas recomendadas para la autenticación y creación de usuarios de Kerberos.

  Es responsabilidad del administrador de la cuenta de Kerberos seguir los procedimientos recomendados para proteger su entorno de Kerberos y evitar que las contraseñas se vean

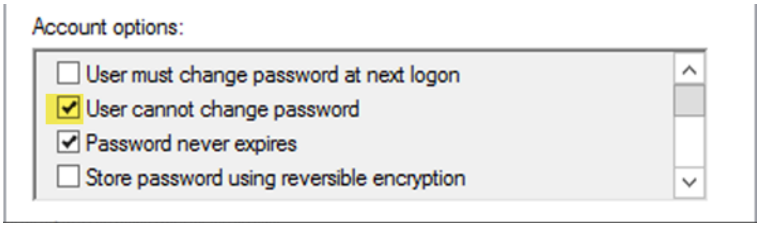
 ©2025 Palo Alto Networks, Inc.

comprometidas. Use los siguientes procedimientos recomendados al crear las cuentas de usuario, la contraseña y los ServicePrincipalNames (SPN).

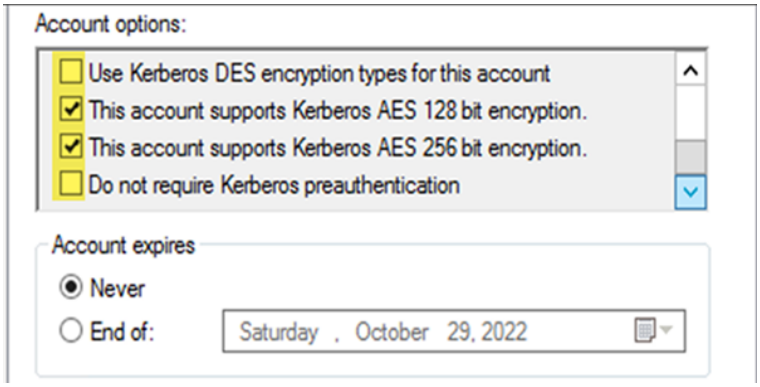
Prácticas recomendadas para la creación de cuentas de usuario de Kerberos:

- No reutilice las cuentas de usuario administrador.

  Cree un nombre de cuenta único para la cuenta de Kerberos que se usará con Prisma Access Proxy explícito.
- No comparta esta cuenta con ningún otro servicio; utilice una cuenta de usuario dedicada para Prisma Access Proxy explícito.
- Asegúrese de que el usuario no pueda cambiar la contraseña de la cuenta Kerberos.

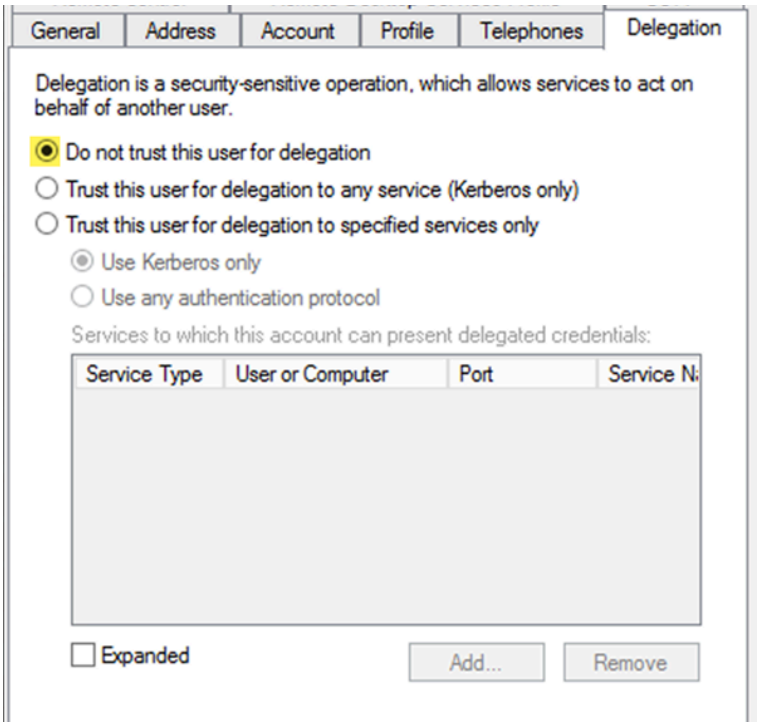


- Al seleccionar las opciones de la cuenta Kerberos, anule la selección **Use Kerberos DES encryption types for this account (Usar tipos de cifrado Kerberos DES para esta cuenta)** y **Do not require Kerberos preauthentication (No requiere autenticación previa de Kerberos)**.
- Habilite el cifrado AES-128 y AES-256 bits.

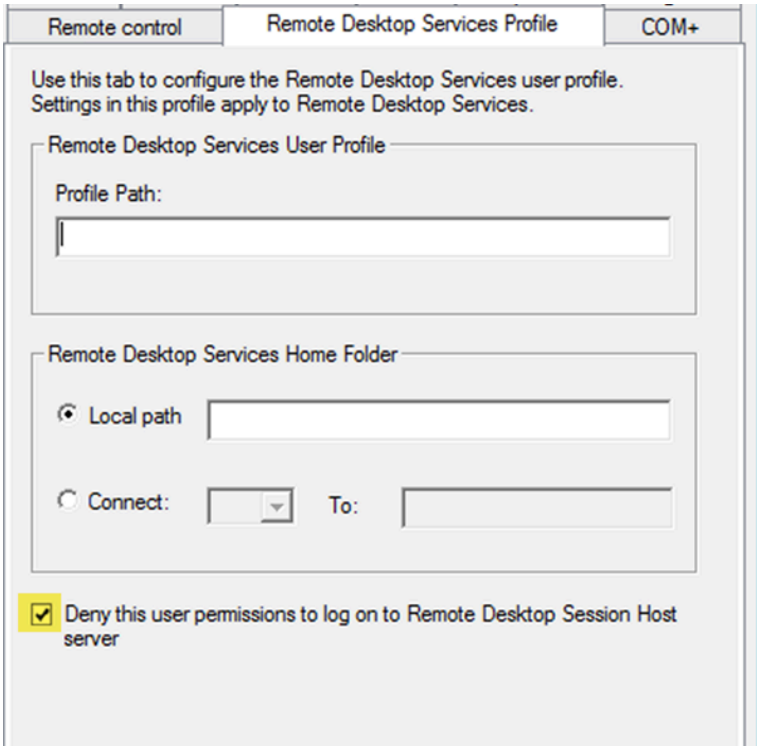


- Deshabilite la delegación para los usuarios.

 ©2025 Palo Alto Networks, Inc.

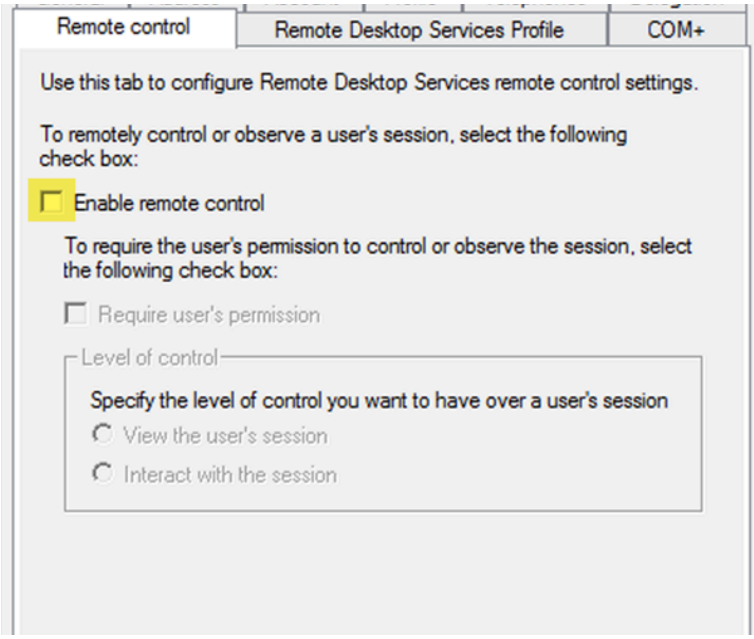


- Impida la capacidad de iniciar sesión en una sesión de escritorio remoto.

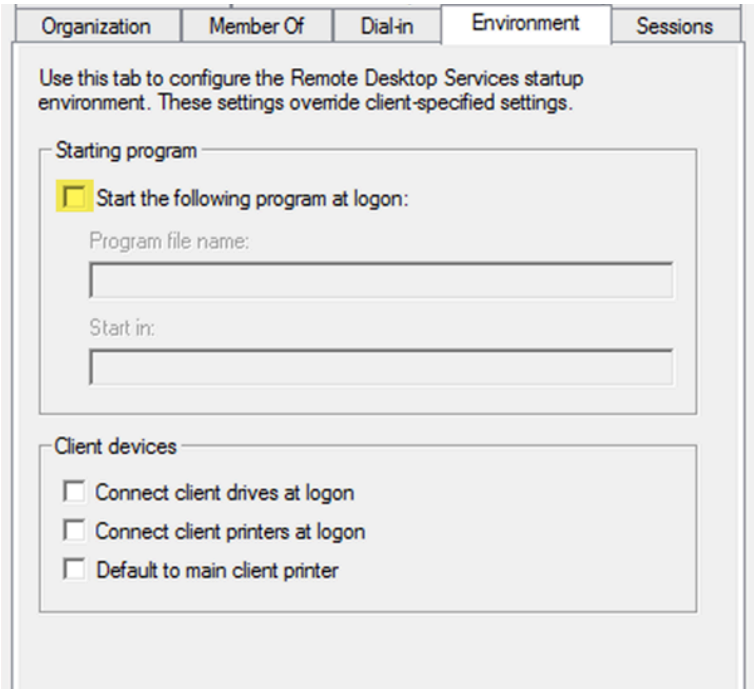


- No habilite el control remoto.

 ©2025 Palo Alto Networks, Inc.



- No permita que los usuarios inicien programas al iniciar sesión.



- Puede especificar usuarios o grupos de usuarios en la lista de permitidos del perfil de autenticación que cree para limitar la autenticación solo a los usuarios o equipos que tengan necesidades empresariales legítimas.

Prácticas recomendadas de SPN y Keytab:

- Asegúrese de que el SPN no esté asociado a varias cuentas de usuario, lo que podría provocar errores de SPN duplicados.
- RC4-HMAC-NT utiliza un hash NTML débil. Siga las políticas y directrices de seguridad de su organización para incluir o excluir el cifrado RC5.

 ©2025 Palo Alto Networks, Inc.

- Los cifrados DES-CBC-CRC y DES-CBC-MD5 han quedado obsoletos y no son compatibles con Prisma Access.
- Cambie la contraseña del SPN de forma regular. Siga las políticas y directrices de seguridad de su organización para el cambio periódico de contraseñas.
- Siga las prácticas de su organización para la complejidad de las contraseñas (por ejemplo, cree las contraseñas de SPN de forma verdaderamente aleatoria que no sean legibles ni que se puedan adivinar).
- Si cambia la contraseña del usuario del servicio o cambia cualquier otro atributo, actualice y vuelva a generar la nueva keytab y cárguela en Prisma Access.
- Si incorpora una nueva región de PA, debe generar una nueva keytab para esa región, como se muestra en los pasos siguientes.

En el siguiente ejemplo de salida se muestra una cuenta que se creó con los procedimientos recomendados de Kerberos.

```
PS C:\Users\Administrator> Get-ADUser example -Properties "*"
 AccountNotDelegated : True AllowReversiblePasswordEncryption :
 False CannotChangePassword : True CN : example Deleted :
 DoesNotRequirePreAuth : False Enabled : True GivenName :
 PrismaAccess EP Service User KerberosEncryptionType :
 {AES128, AES256} msDS-SupportedEncryptionTypes : 24 Name :
 example PasswordExpired : False PasswordNeverExpires : True
 PasswordNotRequired : False PrincipalsAllowedToDelegateToAccount :
 {} ProtectedFromAccidentalDeletion : True SamAccountName :
 example servicePrincipalName : {HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM} ServicePrincipalNames :
 {HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-east-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-south-1.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM}
 SmartcardLogonRequired : False TrustedForDelegation :
 False TrustedToAuthForDelegation : False UseDESKeyOnly :
 False UserPrincipalName : HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM
```

Cree un keytab de Kerberos.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licencia de Prisma Access ☐ Versión mínima de plano de datos requerida: PAN-OS 10.1.3 o versiones posteriores

Después de revisar los requisitos y recomendaciones para implementar Kerberos para Proxy explícito, está listo para crear un keytab de Kerberos.

 ©2025 Palo Alto Networks, Inc.

Para un rendimiento óptimo, el archivo keytab debe ser de menos de 60 KB de tamaño.

STEP 1 | Configure su implementación de Proxy explícito.

STEP 2 | Obtenga el FQDN, los FQDN de proxy y los CNAME de DNS que se requieren para configurar su autenticación Kerberos.

La autenticación Kerberos utiliza la información recuperada del script de la API de Prisma Access para crear y configurar los keytabs de Kerberos. El script de la API recupera la siguiente información:

- **ep_geo_lb_fqdn**: el FQDN del proxy explícito utilizado en la configuración del equilibrador de carga de red del proxy explícito. Este FQDN es idéntico a la **Explicit Proxy URL (URL del Proxy explícito)** en la interfaz de usuario de Prisma Access en **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración)** > **Explicit Proxy (Proxy explícito)** > **Infrastructure Settings (Configuración de Infraestructura)** > **Explicit Proxy URL (URL de proxy explícito)**.
- **ep_geo_lb_cname**: el CNAME DNS para el inquilino del Proxy explícito.
- **ep_regional_fqdn**: los FQDN utilizados para las ubicaciones del Proxy explícito incorporadas.

  El Proxy explícito asigna a cada ubicación una dirección IP pública para el equilibrador de carga de red; el ep_regional_fqdn es el FQDN asociado con esa dirección IP. Si varias ubicaciones comparten la misma dirección IP pública, esas ubicaciones utilizan el mismo FQDN regional.

1. Genere una clave API para usar como parte de un comando curl.
   - En Prisma Access (Managed by Strata Cloud Manager), seleccione, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)** > **Generate New API Key (Generar nueva clave de API)**.
   - En Panorama Managed Prisma Access, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** > **Generate API Key (Generar Clave API)**
2. Cree un archivo .txt e introduzca las siguientes opciones de comando en el archivo:

   ```
   { "serviceType": "swg_proxy", "location": "deployed",
    "addrType": "network_load_balancer" }
   ```

3. Introduzca el siguiente comando para recuperar los FQDN necesarios para utilizar la autenticación Kerberos:

   ```
   curl -X POST --data @option.txt -H header-api-key:Current-
   API-Key "https://api.prod.datapath.prismaaccess.com/
   getPrismaAccessIP/v2"
   ```

   Donde `option.txt` es el archivo .txt que creó en un paso anterior y `Current-API-Key` es la clave API de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

4. Tome nota de los FQDNs.

   Hay al menos un **ep_geo_lb_fqdn**, un **ep_geo_lb_cname** y un **ep_regional_fqdn** por ubicación incorporada.

STEP 3 | Cree un nuevo usuario para el servicio de Prisma Access Proxy explícito en el Active Directory (AD) de su organización introduciendo el siguiente comando:

```
New-ADUser -Name "USER_NAME" -GivenName "USER_GIVEN_NAME"
 -SamAccountName "USER_SAMACCOUNTNAME" -UserPrincipalName
 "USER_NAME@DNS_DOMAIN_NAME" -Path "X_500_PATH" –AccountPassword
 (ConvertTo-SecureString “PASSWORD” -AsPlainText -force) -Enabled
 $true -KerberosEncryptionType RC4,AES128,AES256
```

Donde:

- *USER_NAME* es el nombre del objeto de usuario.
- *USER_GIVEN_NAME* es el nombre del usuario.
- *USER_SAMACCOUNTNAME* es el nombre del Administrador de cuentas de seguridad (SAM) del usuario.
- *USER_NAME@DNS_DOMAIN_NAME* es el nombre principal de usuario (UPN) del usuario.
- *X_500_PATH* es la ruta X.500 de la OU o contenedor donde se crea el nuevo objeto (por ejemplo, `DC=EXAMPLE,DC=COM.`)
- *PASSWORD* es la contraseña que se debe usar para la cuenta.

El siguiente ejemplo de CLI tiene un nombre de usuario de `example`, un nombre de SAM de `example`, un nombre de `PrismaAccess EP Service User`, una UPN de `example@exmp.com`, una ruta de `DC=EXMP,DC=COM` y una contraseña de Ex@mple123:

```
New-ADUser -Name "example" -GivenName "PrismaAccess EP
 Service User" -SamAccountName "example" -UserPrincipalName
 "example@exmp.com" -Path "DC=EXMP,DC=COM" –AccountPassword
 (ConvertTo-SecureString “Ex@mple123” -AsPlainText -force) -Enabled
 $true -KerberosEncryptionType RC4,AES128,AES256
```

El comando anterior especifica un tipo de cifrado RC4, que utiliza un hash NTLM débil. Siga las políticas y directrices de seguridad de su organización para incluir o excluir RC4 en este comando.

STEP 4 | Introduzca el siguiente comando para evitar que la contraseña caduque y para evitar que se cambie:

```
Get-ADUser USER_NAME|Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$true
```

Siga las políticas y directrices de seguridad de su organización en cuanto a la caducidad y las políticas de rotación.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Introduzca el siguiente comando para mostrar la cuenta de usuario recién creada:

```
Get-ADUser USER_NAME -property msDS-KeyVersionNumber
```

STEP 6 | Asocie los SPN y exporte archivos keytab para usar con la autenticación Kerberos en su AD de Windows.

Un archivo keytab permite que el Proxy explícito valide los tokens de autenticación Kerberos proporcionados durante los flujos de tráfico de usuarios, servidores, dispositivos IoT u otras máquinas sin periféricos. Durante la creación del archivo keytab, el Proxy explícito requiere que los valores que recupera utilizando la API en un paso anterior estén asociados como ServicePrincipalNames (SPNs) con la cuenta de usuario que creó en el paso siguiente.

Utilice los valores **ep_geo_lb_fqdn**, **ep_geo_lb_cname**, and **ep_regional_fqdn**. Estos valores permiten que el Proxy explícito autentique los flujos de tráfico hacia cualquiera de esos dominios de proxy.

1. Genere y exporte un keytab utilizando el valor **ep_geo_lb_fqdn** como el nombre principal del servicio (SPN) introduciendo los siguientes comandos:

   ```
   ktpass -princ HTTP/ep_geo_lb_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_1.keytab
   ```

   Donde:

   - *ep_geo_lb_fqdn* es el valor **ep_geo_lb_fqdn** devuelto por el script de la API de Proxy explícito.
   - *REALM* es el dominio (por ejemplo, `EXMP.COM`).

     En la mayoría de los casos, entra en el dominio utilizando letras mayúsculas.
   - *DOMAIN\USER_NAME* es el nombre de inicio de sesión a nivel de dominio (por ejemplo, `EXMP\example`).
   - *PASSWORD* es la contraseña que se debe usar para el keytab. Esta contraseña no tiene que coincidir con la contraseña del usuario, pero debe coincidir con el valor que cree para los SPN **ep_geo_lb_cname** y **ep_regional_fqdn** en los siguientes pasos.
   - *KEYTAB_NAME_1* es el nombre del keytab. El nombre del keytab debe ser único para este SPN.

   Asegúrese de seguir las prácticas recomendadas para crear SPN y contraseñas.

   El siguiente ejemplo de CLI tiene un *ep_geo_lb_fqdn* de `example.proxy.prismaaccess.com`, un *REALM* de `EXMP.COM`, un

 ©2025 Palo Alto Networks, Inc.

DOMAIN\USER_NAME de EXMP\example, una *PASSWORD* de Ex@exmp123 y un nombre de keytab exportado de exmp1.keytab:

```
ktpass -princ HTTP/example.proxy.prismaaccess.com@EXMP.COM -
mapuser EXMP\example -ptype KRB5_NT_PRINCIPAL -crypto all -
pass Ex@mple123 -out exmp1.keytab
```

2. Genere y exporte un keytab utilizando el valor **ep_geo_lb_cname** como el SPN introduciendo los siguientes comandos:

```
ktpass -princ HTTP/ep_geo_lb_cname@REALM -
mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
 -pass PASSWORD -out KEYTAB_NAME_2.keytab
```

Donde:

- *ep_geo_lb_cname* es el valor **ep_geo_lb_cname** devuelto por el script de la API de Proxy explícito.
- *REALM* es el dominio por ejemplo, EXMP.COM
- *DOMAIN\USER_NAME* es el nombre de inicio de sesión a nivel de dominio (por ejemplo, EXMP\example).
- *PASSWORD* es la contraseña que se debe usar para el keytab. Esta contraseña debe coincidir con las contraseñas SPN **ep_geo_lb_fqdn** y **ep_regional_fqdn**.
- *KEYTAB_NAME_2* es el nombre del keytab que desea exportar. Este nombre deberá ser diferente de los otros nombres de keytab SPN que crea.

El siguiente ejemplo de CLI tiene un *ep_geo_lb_cname* de prisma-abcde12345.proxy.prismaaccess.com, un *REALM* de EXMP.COM, un *DOMAIN\USER_NAME* de EXMP\example, una *PASSWORD* de Ex@mple123 y un nombre de keytab exportado de exmp2.keytab:

```
ktpass -princ HTTP/prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
```

 ©2025 Palo Alto Networks, Inc.

```
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp2.keytab
```

3. Genere y exporte un keytab utilizando el valor **ep_regional_fqdn** como el SPN introduciendo los siguientes comandos:

   ```
   ktpass -princ HTTP/ep_regional_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_3.keytab
   ```

   Donde:

   - *ep_regional_fqdn* es el valor **ep_regional_fqdn** devuelto por el script de la API de Proxy explícito.
   - *REALM* es el dominio (por ejemplo, `EXMP.COM`).
   - *DOMAIN\USER_NAME* es el nombre de inicio de sesión a nivel de dominio (por ejemplo, `EXMP\example`).
   - *PASSWORD* es la contraseña que se debe usar para el keytab. Esta contraseña debe coincidir con las contraseñas SPN **ep_geo_lb_fqdn** y **ep_geo_lb_cname**.
   - *KEYTAB_NAME_3* es el nombre del keytab que desea exportar. Este nombre deberá ser diferente de los otros nombres de keytab SPN que crea.

   El siguiente ejemplo de CLI tiene un *ep_regional_fqdn* de `us-west-2.prisma-abcde12345.proxy.prismaaccess.com`, un *REALM* de `EXMP.COM`, un *DOMAIN\USER_NAME* de `EXMP\example`, una *PASSWORD* de `Ex@mple123`, y un nombre de keytab exportado de `exmp3.keytab`:

   ```
   ktpass -princ HTTP/us-west-2.prisma-
   abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
   \example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
    -out exmp3.keytab
   ```

4. (Opcional) Si tiene ubicaciones adicionales que utilizan diferentes valores de **ep_regional_fqdn**, y desea crear keytabs para esas ubicaciones, genere y exporte uno o más keytabs adicionales repitiendo el Paso 6.c, utilizando el valor de **ep_regional_fqdn** para esas ubicaciones.

   Crea un nombre de keytab único para cada **ep_regional_fqdn** único. Por ejemplo, si el **ep_regional_fqdn** para otra ubicación es `us-east-2.prisma-abcde12345.proxy.prismaaccess.com`, introduzca el siguiente ejemplo de CLI con un nombre de archivo keytab exportado único:

   ```
   ktpass -princ HTTP/us-east-2.prisma-
   abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
   \example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
    -out exmp4.keytab
   ```

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Elimine los cifrados no compatibles con los keytabs creados introduciendo los siguientes comandos de `ktutil` en Ubuntu.

La siguiente salida del sistema proporciona ejemplos para limpiar varios cifrados:

```
slot KVNO Principal ---- ----
 ---------------------------------------------------------------------
 1 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (des-cbc-crc) 2 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (des-cbc-md5) 3 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (arcfour-hmac) 4 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (aes256-cts-hmac-sha1-96) 5 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (aes128-cts-hmac-
sha1-96)
```

```
# display all keytabs, get the key entry numbers to remove DES-
CBC-MD5 and DES-CBC-CRC. # Also, enable or disable RC4-HMAC based
 on your organization's policy. for i in `ls keytab_name*.keytab`;
 do echo $i; klist -Kte -k $i; done # cleanup unsupported
 ciphers # entry #1 is typically des-cbc-crc # entry #2 is
 typically des-cbc-md5 # entry #3 is typically arcfour-hmac ktutil
 rkt KEYTAB_NAME_1.keytab delent 2 delent 1 wkt new1.keytab quit
 ktutil rkt KEYTAB_NAME_2.keytab delent 2 delent 1 wkt new2.keytab
 quit ktutil rkt KEYTAB_NAME_3.keytab delent 2 delent 1 wkt
 new3.keytab quit
```

Where *KEYTAB_NAME_1*.keytab, *KEYTAB_NAME_2*.keytab, and *KEYTAB_NAME_3*.keytab are the keytabs you created in the previous step.

STEP 8 | (Opcional) Si has creado más keytabs para otras regiones, elimine los cifrados no compatibles en esos keytabs introduciendo el comando `ktutil` anterior, sustituyendo *KEYTAB_NAME_1*.keytab con el nombre del keytab que utilizó para la región o regiones y especificando un archivo de salida diferente (por ejemplo, `new4.keytab`, `new5.keytab`, etc.).

STEP 9 | Fusione los keytabs que creó introduciendo el siguiente comando `ktutil`, donde new1.keytab, new2.keytab y new3.keytab son los keytabs que creó en el paso anterior. Asegúrese de incluir todos los keytabs específicos de la región en este comando:

```
ktutil rkt new1.keytab rkt new2.keytab rkt new3.keytab # if you
 created any additional region-specific keytab files, add them
 here. wkt papxv1.keytab quit
```

Cuando esté completo, utilice el keytab que creó (`papxv1.keytab` en este ejemplo) como el keytab para usar con el Proxy explícito.

 ©2025 Palo Alto Networks, Inc.

Configure la autenticación Kerberos para implementaciones de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

- Strata Cloud Manager
- Panorama

Configurar la autenticación de Kerberos para implementaciones de proxy explícito (Strata Cloud Manager)

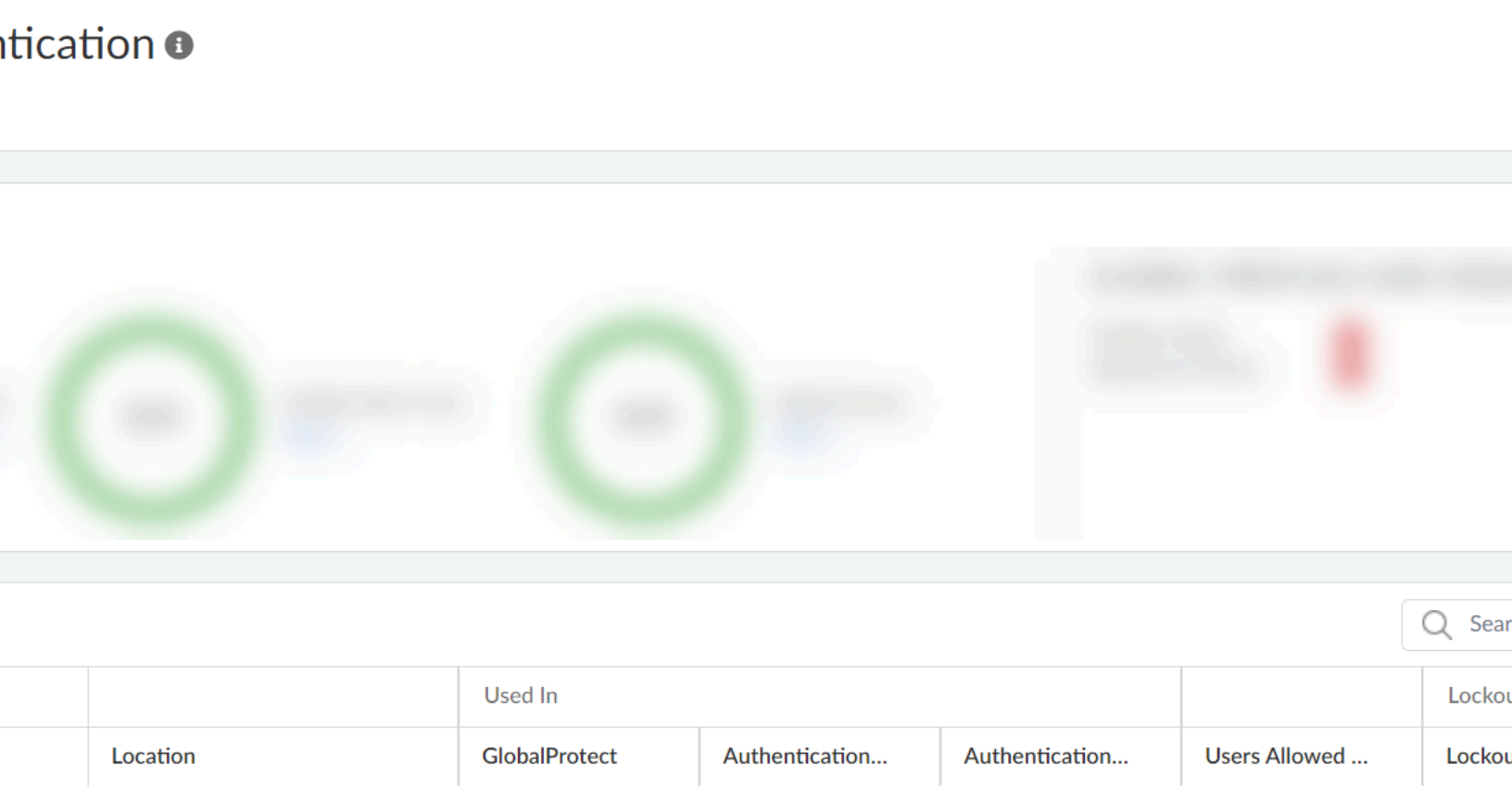
STEP 1 | Configure un perfil de autenticación Kerberos.

El perfil define cómo se conecta el proxy explícito al servidor Kerberos para la autenticación de usuarios móviles.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication**

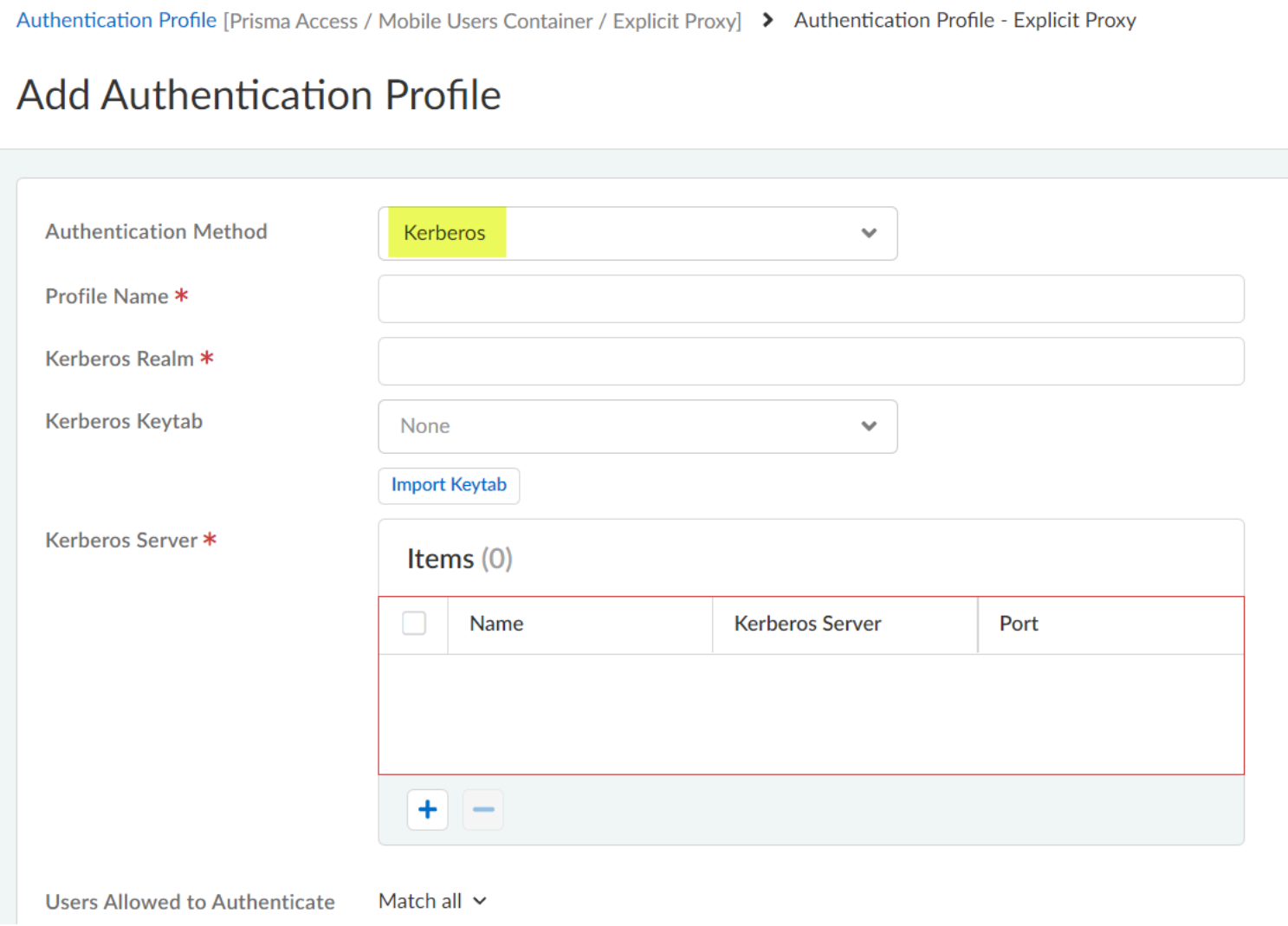
 ©2025 Palo Alto Networks, Inc.

(Autenticación) > Authentication Profiles (Perfiles de autenticación) y **Add Profile (Añadir perfil)**.



2. Seleccione el **Authentication Method (Método de autenticación). Kerberos**.

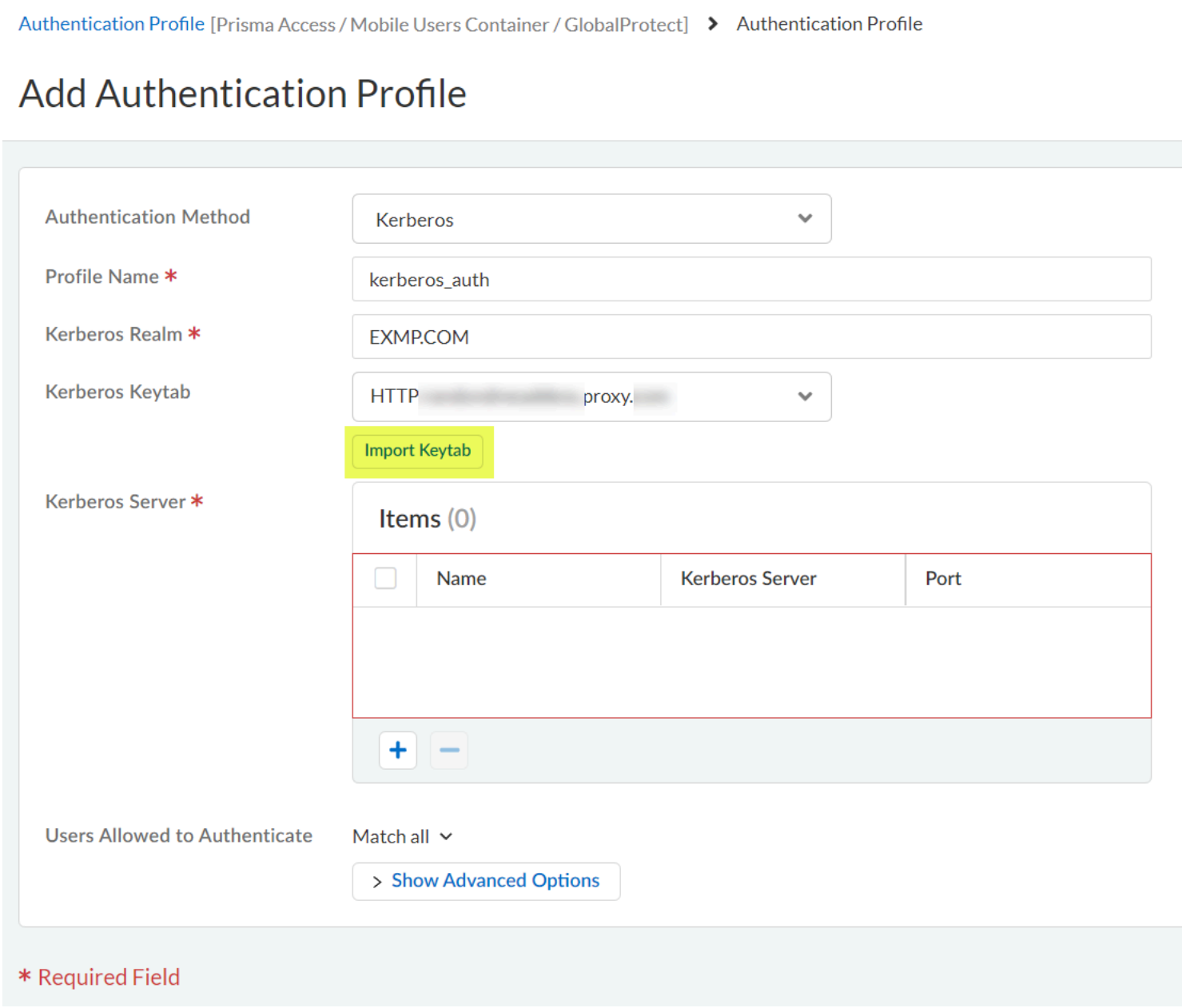
©2025 Palo Alto Networks, Inc.



3. Introduzca el **Profile Name (Nombre del perfil)** para identificar el perfil del servidor.

   El perfil de autenticación especifica el perfil de servidor que debe utilizar el portal o las puertas de enlace cuando autentican a los usuarios.
4. 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, el nombre de la cuenta de usuario user@EXMP.COM tiene el EXMP.COM de dominio.
5. Importe el archivo **Kerberos Keytab (Keytab de Kerberos)** [**Import Keytab (Importar Keytab)**] que creó anteriormente.

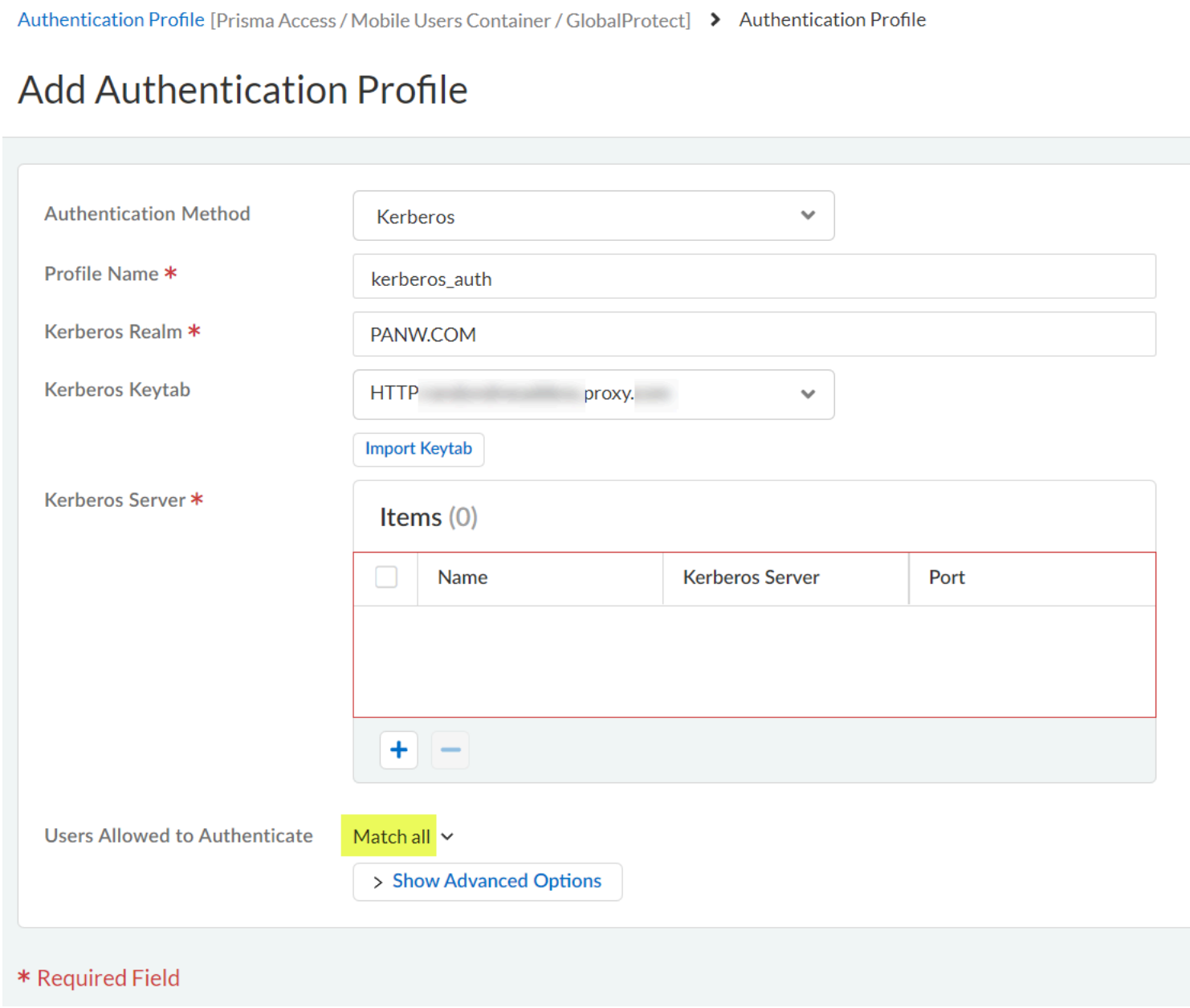
 ©2025 Palo Alto Networks, Inc.



6. Añada **Users Allowed to Authenticate (Usuarios autorizados a autenticarse)** con este perfil.
   - Para seleccionar todos los usuarios, **Match all (Hacer coincidir todo)**.
   - Si usa Cloud Identity Engine para rellenar la lista de usuarios, seleccione los usuarios de una lista o seleccione **all (todos)** para permitir que todos los usuarios se autentiquen.
   - Para añadir usuarios locales que puedan iniciar sesión con Kerberos, seleccione **Add Local User (Añadir usuario local)**, añada el **Name (Nombre)** y cree una **Password (Contraseña)**.

©2025 Palo Alto Networks, Inc.

- Al configurar la autenticación de usuario y la asignación de usuarios, use un formato de userPrincipalName (UPN); no se admiten otros formatos (como samAccountName).
- Los nombres de usuario de caracteres Unicode no son compatibles.

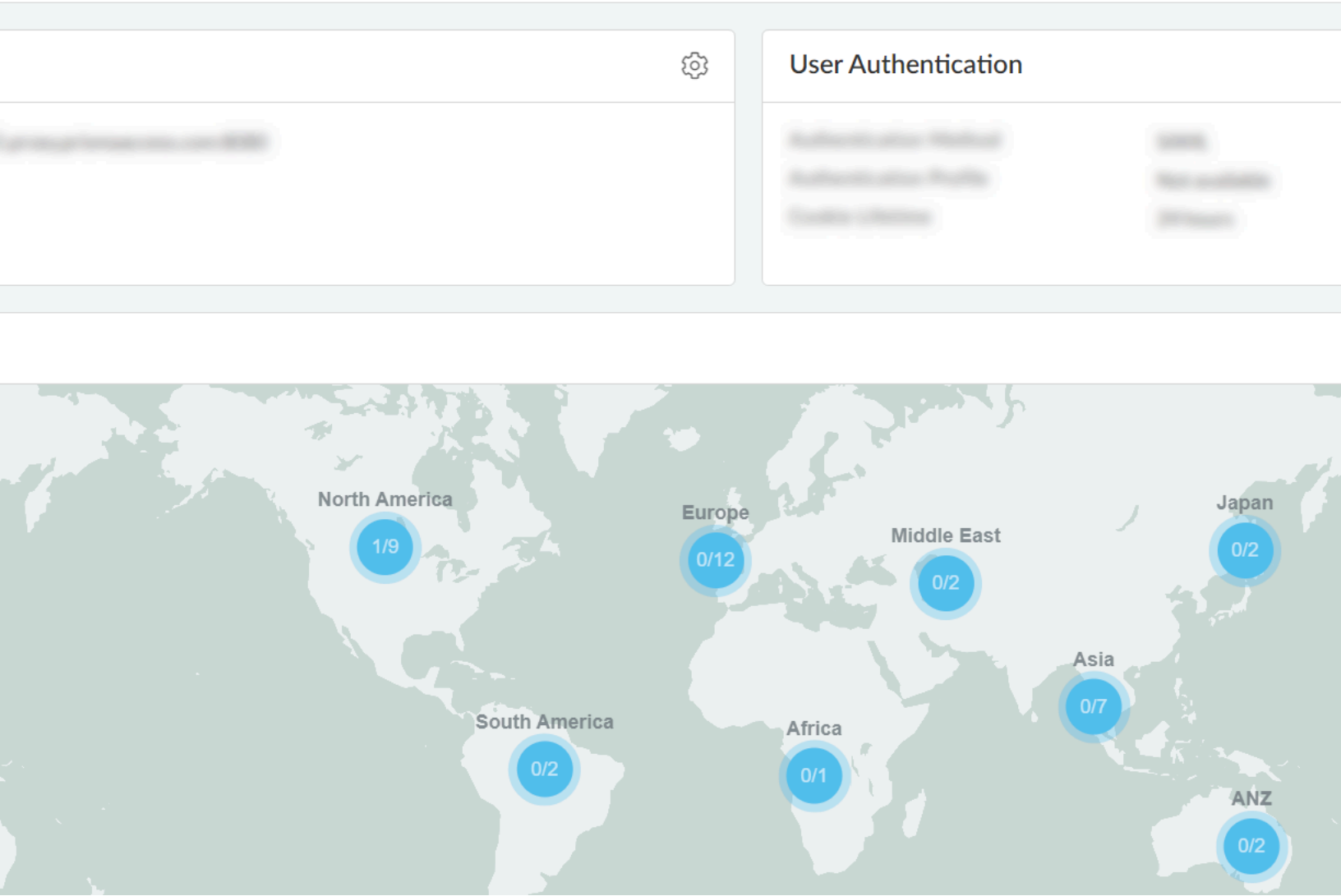


7. Haga clic en **Save (Guardar)** para guardar sus cambios.

 ©2025 Palo Alto Networks, Inc.

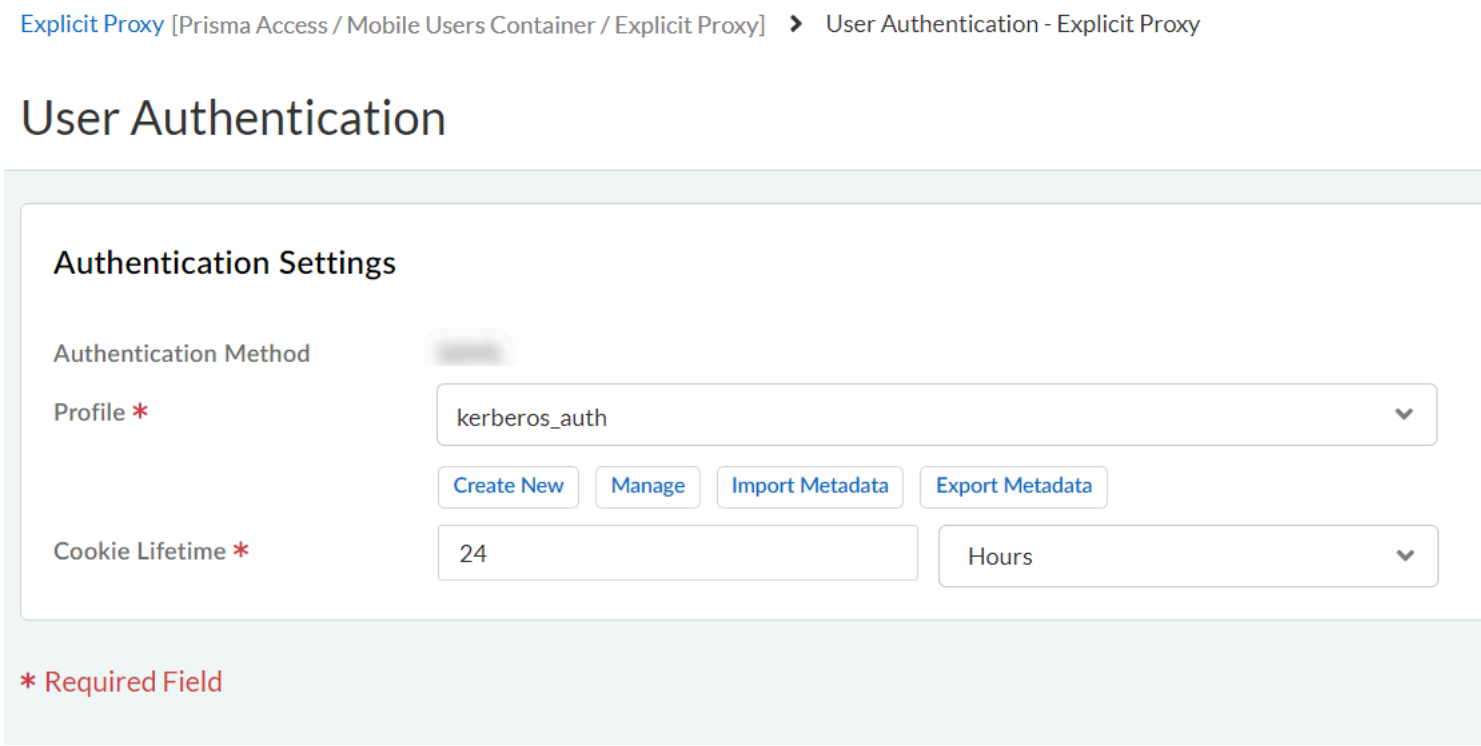
STEP 2 | Asocie el perfil de autenticación a un método de autenticación.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **User Authentication (Autenticación de usuario)**.



2. Seleccione el **Connection Name (Nombre de la conexión)**.
3. Seleccione un **Authentication Method (Método de autenticación)** de **Kerberos** y seleccione el **Profile (Perfil)** de Kerberos que usted creó.

 ©2025 Palo Alto Networks, Inc.



4. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 3 | (Opcional) Añada las direcciones IP de salida de la sucursal o ubicación del campus donde se encuentran los usuarios, servidores, dispositivos IoT o máquinas sin periféricos a la lista de direcciones de proxy explícito de confianza.

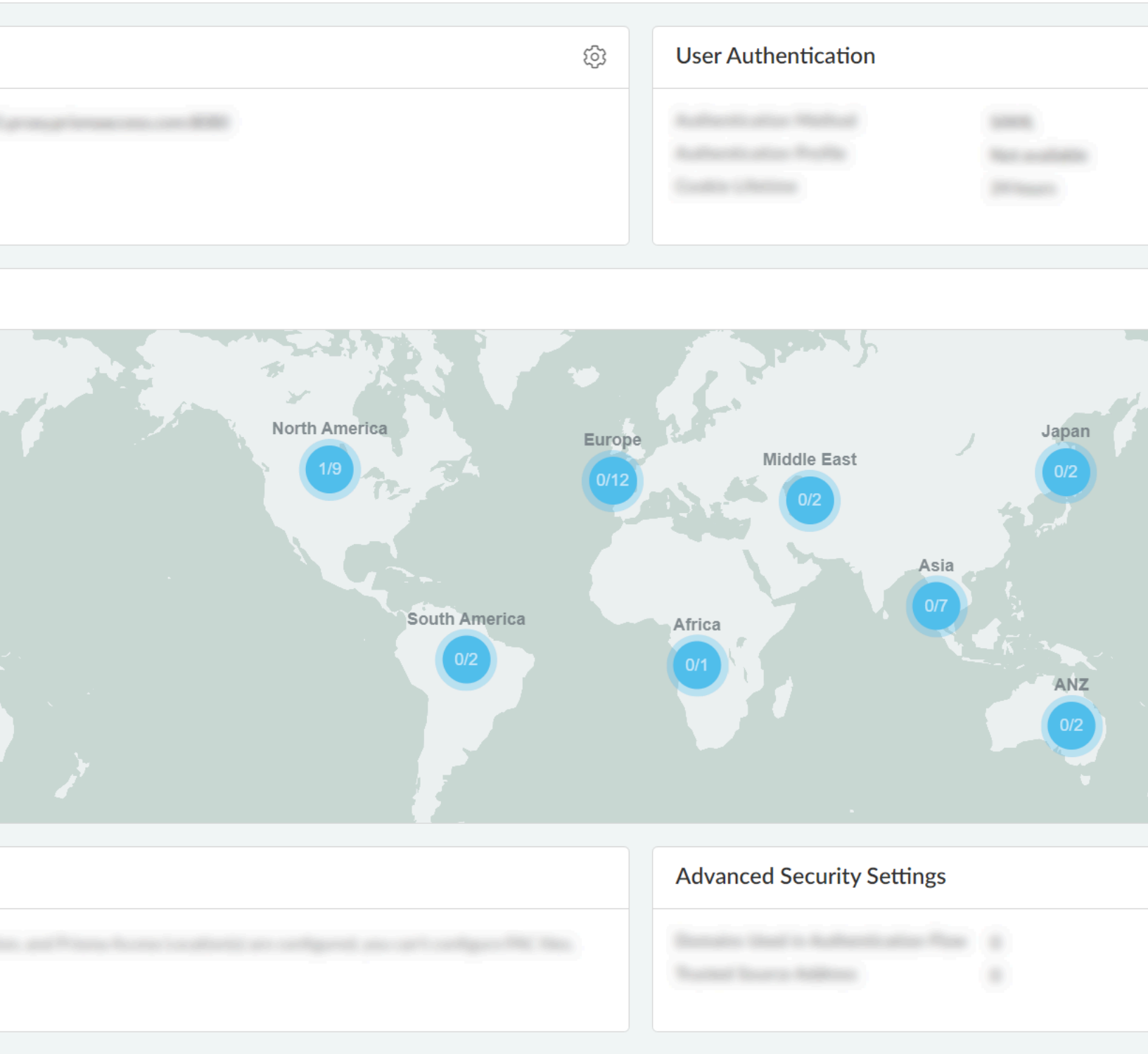
Debe hacer esto solo si lo desea **Skip Authentication (Omitir autenticación)** para direcciones IP específicas o **Use X-Authenticated User (XAU) header on incoming HTTP/HTTPS requests for**

©2025 Palo Alto Networks, Inc.

identity (Usar el encabezado de usuario autenticado X (XAU) en las solicitudes HTTP/HTTPS entrantes para la identidad).

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Advanced Security Settings (Configuración de seguridad avanzada)**.

 ©2025 Palo Alto Networks, Inc.

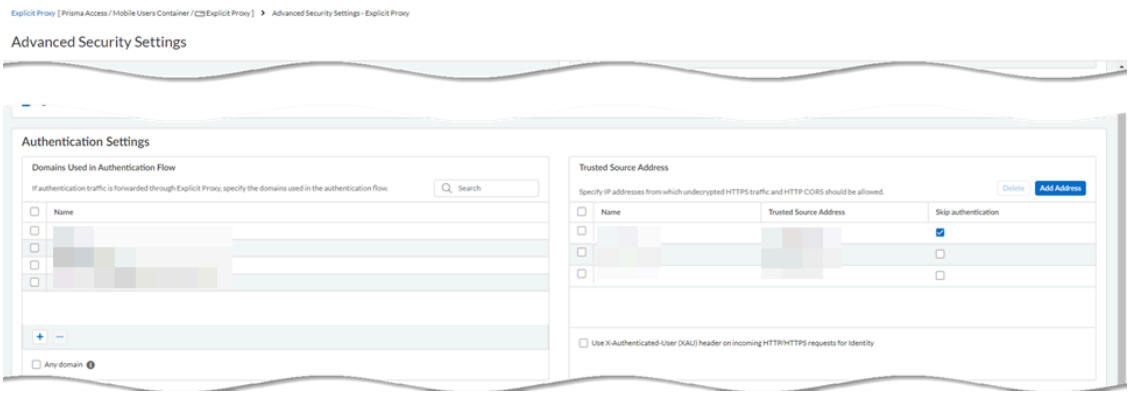


2. Deberá **Add Address (Añadir dirección)** (uno o más) al campo **Trusted Source Address (Dirección de fuente fiable)**.

©2025 Palo Alto Networks, Inc.

Si no añade las direcciones IP del endpoint de salida a la lista de confianza, el proxy explícito obliga a los usuarios y equipos a autenticarse con SAML y Kerberos.

Introduzca un máximo de 100.000 direcciones IP.



3. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 4 | Cree una regla de política de permitir todo para la autenticación de usuarios.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** > **Add Rule (Añadir regla)** > **Pre Rules (Reglas previas)** > **.**
2. Nombre de la regla.
3. Establezca todos los criterios de coincidencia requeridos en **Any (Cualquier)**.
4. Establezca Usuarios en **Known (Conocido)**
5. Establezca Acción en **Allow (Permitir)**.
6. Seleccione **Save (Guardar)** la regla.

STEP 5 | Envíe sus cambios de configuración.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Compruebe que la autenticación Kerberos funciona con Prisma Access mediante la visualización de los logs de tráfico y autenticación.

1. (Solo tráfico descifrado) Vaya a **Activity (Actividad)** > **Log Viewer (Visor de logs)** > **Firewall/Traffic (Cortafuegos/tráfico)** y compruebe que la autenticación Kerberos está funcionando.

   *Si está utilizando Strata Cloud Manager, vaya a **Incidents and Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)** > **Firewall/Traffic (Cortafuegos/Tráfico)**.*

   El tráfico descifrado muestra el nombre de usuario en los registros de tráfico.

2. (Solo tráfico sin descifrar) Vaya a **Activity (Actividad)** > **Log Viewer (Visor de logs)** > **Firewall/Authentication (Cortafuegos/Autenticación)** y compruebe que la autenticación Kerberos funciona correctamente.

   *Si está utilizando Strata Cloud Manager, vaya a **Incidents and Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)** > **Firewall/Authentication (Cortafuegos/autenticación)**.*

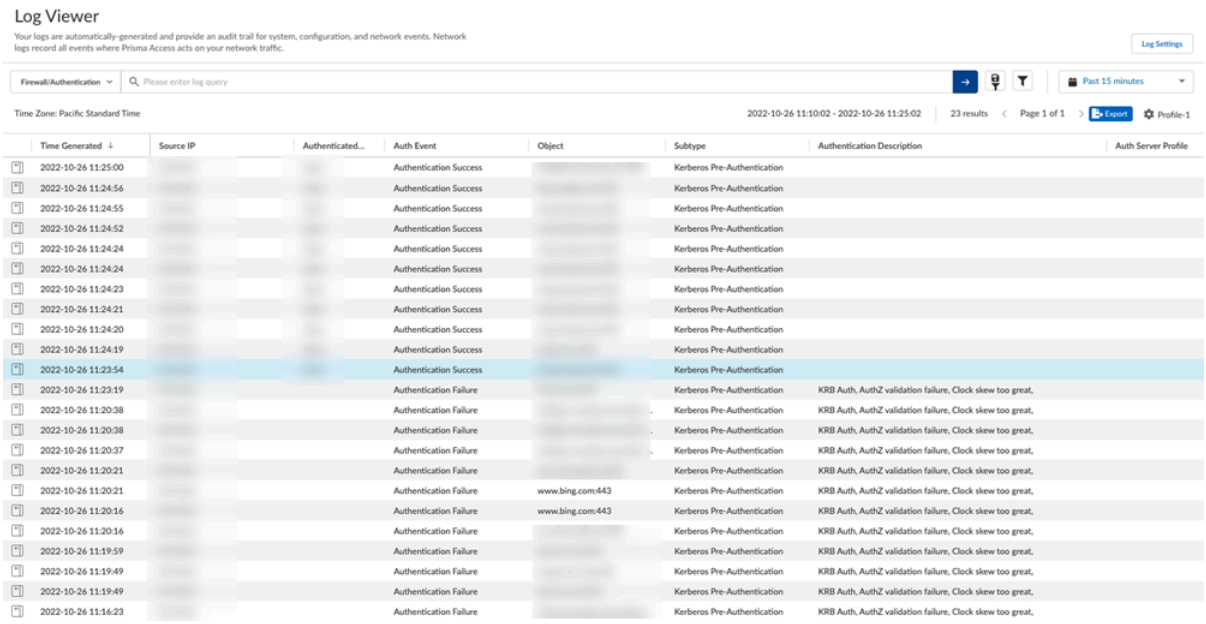
   Los siguientes campos proporcionan más información sobre el evento de autenticación:

   - **Object (Objeto)**: el sitio web al que el usuario intentaba acceder antes de ser redirigido a Kerberos para autenticarse.
   - **Auth Event (Evento de autenticación)**: el estado del intento de autenticación.

     Authentication Success (Éxito de la autenticación) indica que el evento de autenticación se ha realizado correctamente; **Authentication Failure (Fallo de autenticación)** indica que se ha producido un error en el intento y genera un log.
   - **Authentication Description (Descripción de la autenticación)**: si se produjo un error en el intento de autenticación, información adicional sobre el tipo de error.

     Por ejemplo **user not allowed (usuario no permitido)** indica que el usuario o grupo no puede usar Kerberos para autenticarse, posiblemente porque no se agregó a la carpeta **Allow List (Lista de permitidos)** en el perfil de autenticación.

 ©2025 Palo Alto Networks, Inc.



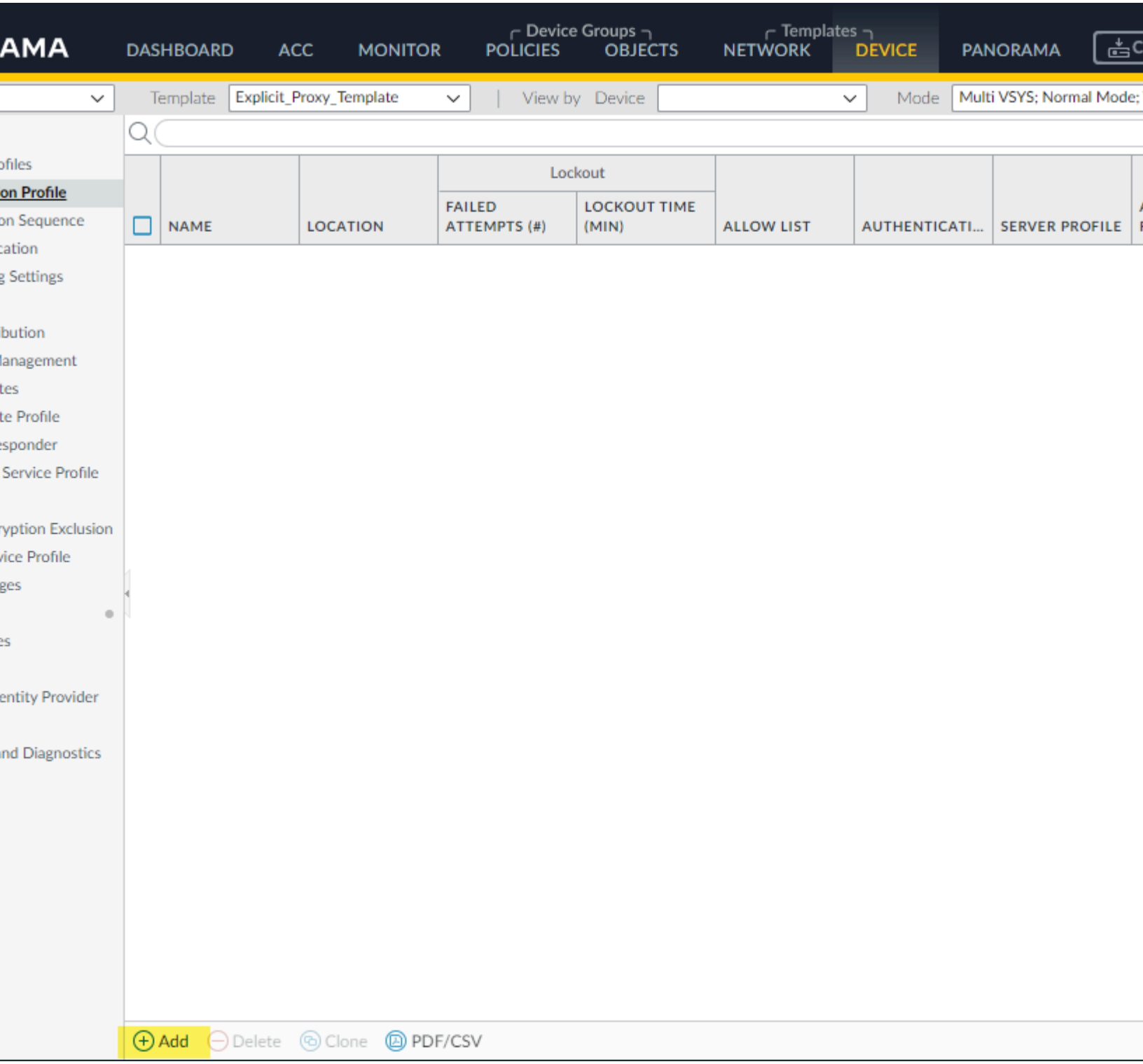
Configurar la autenticación de Kerberos para implementaciones de proxy explícito (Panorama)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configure un perfil de autenticación Kerberos.

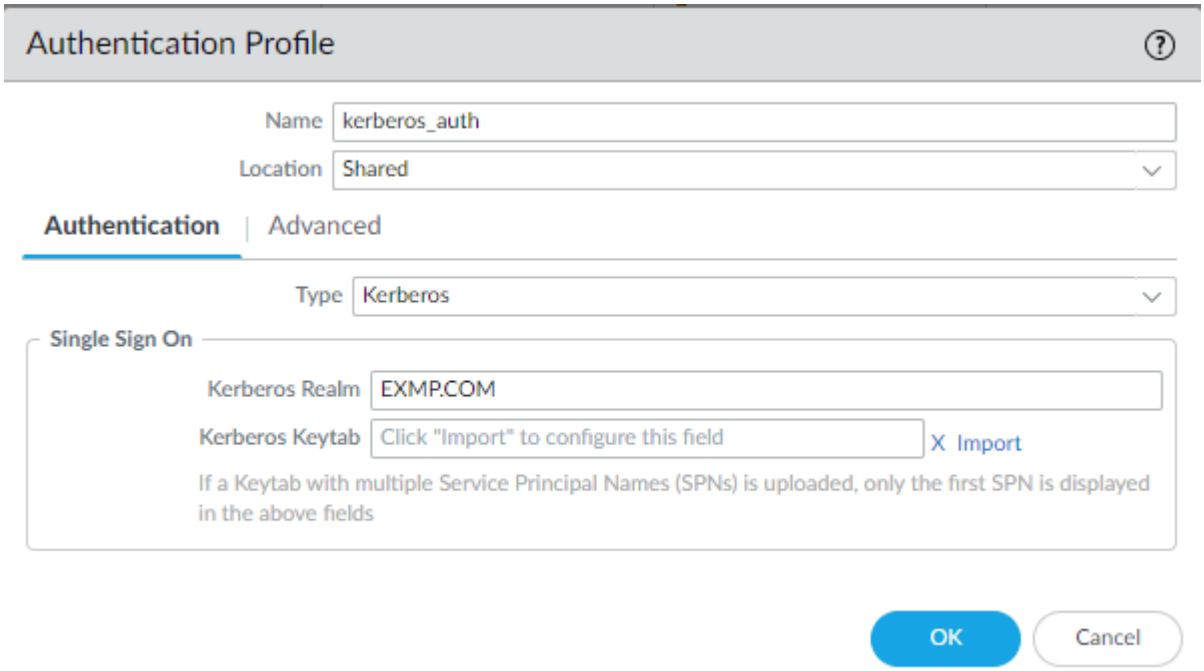
El perfil define cómo se conecta el proxy explícito al servidor Kerberos para la autenticación de usuarios móviles.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** > **+ Add (Añadir +)**.

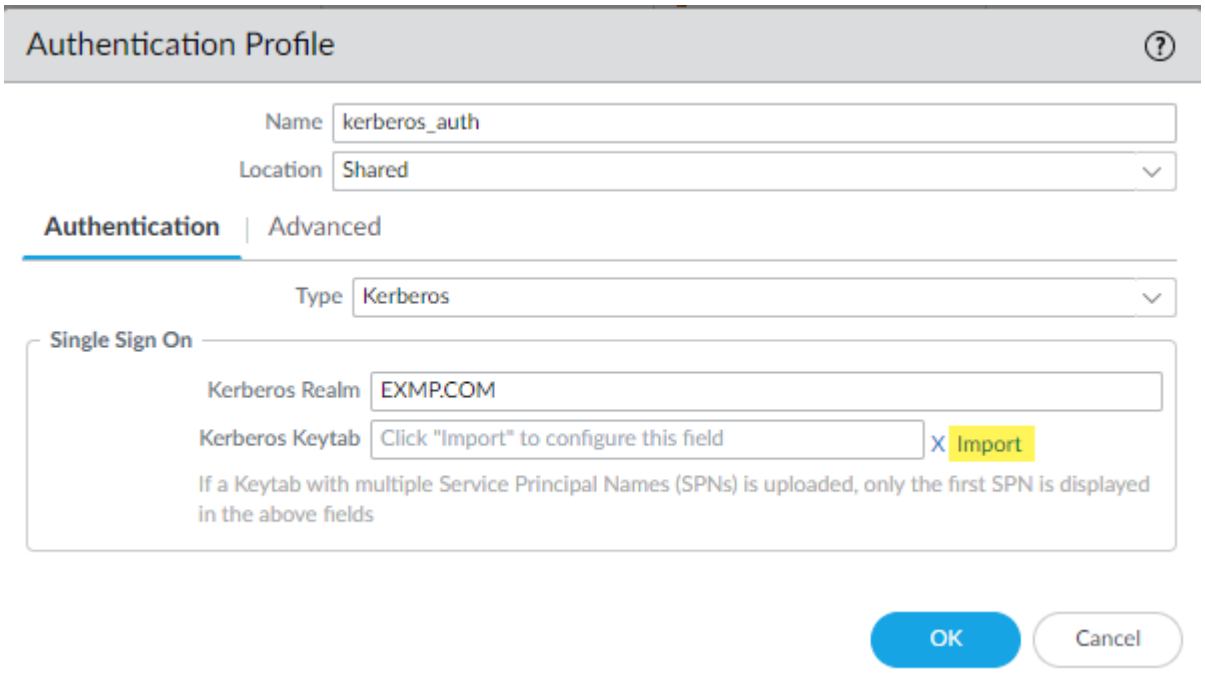


 ©2025 Palo Alto Networks, Inc.

2. Seleccione el **Type (Tipo)**. **Kerberos**.



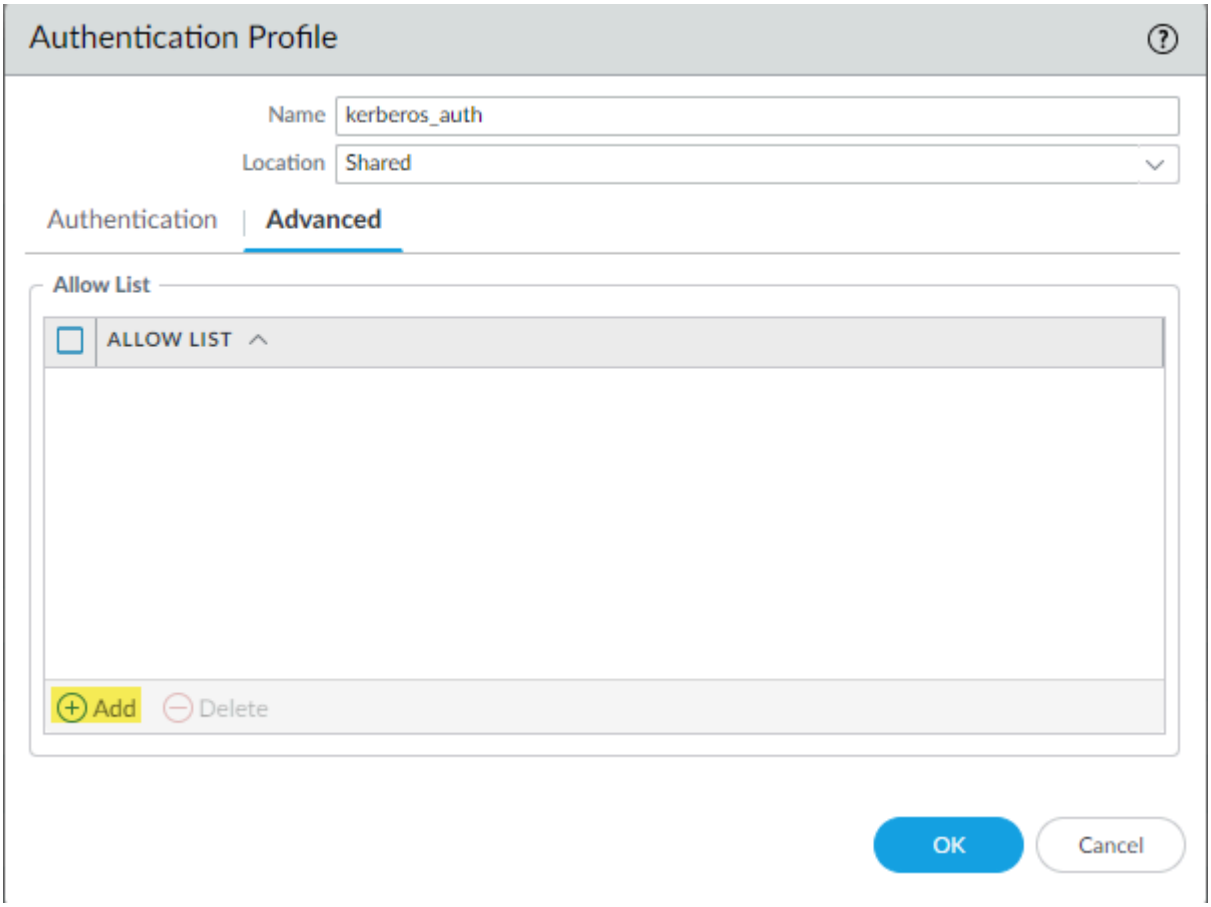
3. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
4. Introduzca el **Kerberos Realm (Dominio Kerberos)** (hasta 127 caracteres) para especificar la parte del nombre de host del nombre de inicio de sesión del usuario. Por ejemplo, el nombre de la cuenta de usuario user@EXMP.COM tiene el EXMP.COM de dominio.
5. Deberá **Import (Importar)** la Keytab de Kerberos creada anteriormente.



6. Añada usuarios autorizados a autenticarse con este perfil.

 ©2025 Palo Alto Networks, Inc.

- Seleccione **Advanced (Avanzado)** > **+ Add (Añadir +)**
- Para seleccionar todos los usuarios, seleccione **all (todo)**.
- Si usa Cloud Identity Engine para rellenar la lista de usuarios, seleccione los usuarios de una lista o seleccione **all (todos)** para permitir que todos los usuarios se autentiquen.
- Para añadir usuarios locales que puedan iniciar sesión con Kerberos, escriba sus nombres de usuario.
  - Al configurar la autenticación de usuario y la asignación de usuarios, use un formato de userPrincipalName (UPN); no se admiten otros formatos (como samAccountName).
  - Los nombres de usuario de caracteres Unicode no son compatibles.



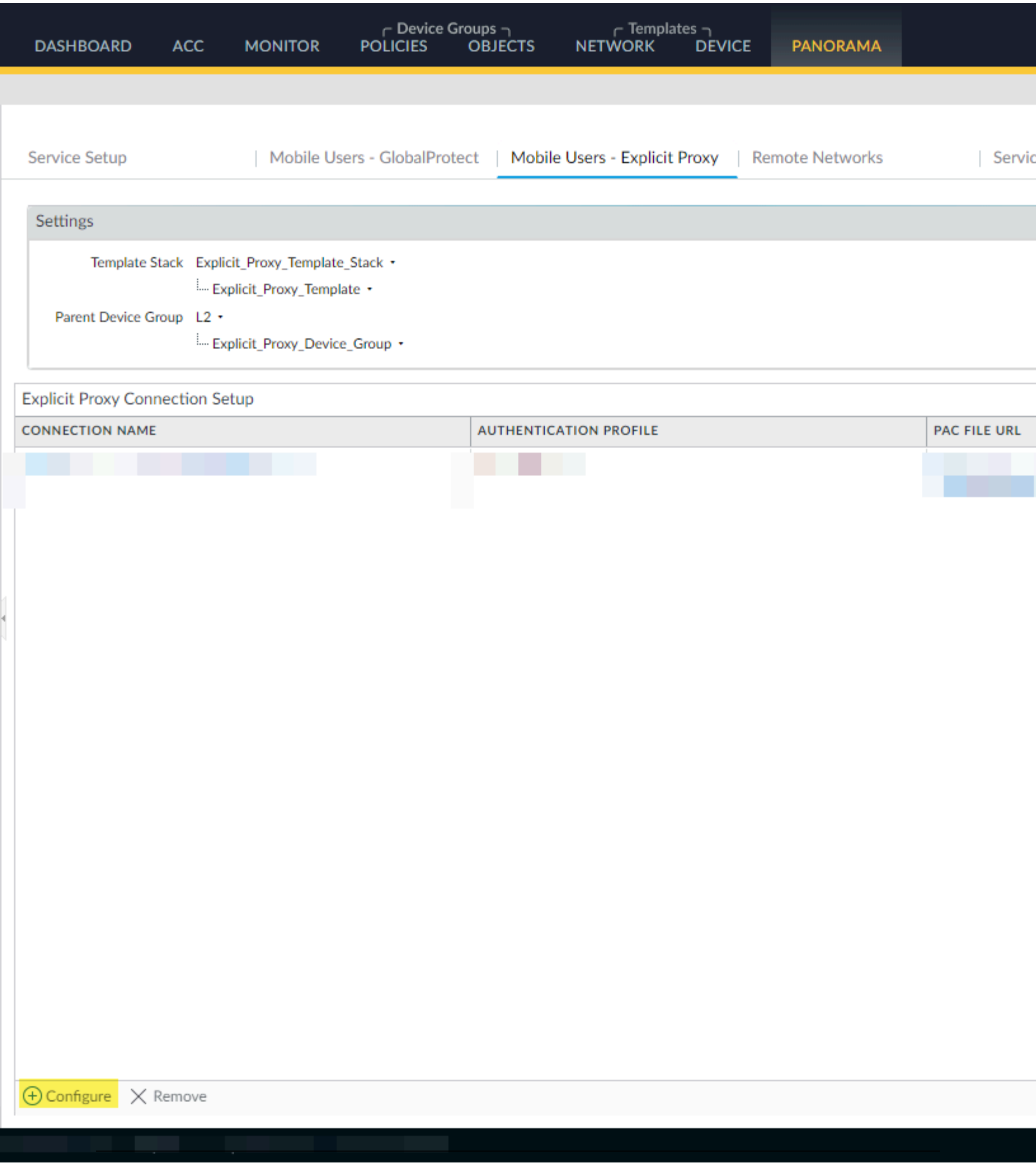
7. Haga clic en **Save (Guardar)** para guardar sus cambios.

©2025 Palo Alto Networks, Inc.

STEP 2 | Asocie el perfil de autenticación a un método de autenticación.

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **+ Configure (Configurar +)**.

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

2. Establezca el **Explicit Proxy FQDN (FQDN de proxy explícito)**.
3. Seleccione el **Profile (Perfil)** Kerberos que creó.
4. Seleccione **OK (Aceptar)** para guardar los cambios.

STEP 3 | (Opcional) Añada las direcciones IP de salida de la sucursal o ubicación del campus donde se encuentran los usuarios, servidores, dispositivos IoT o máquinas sin periféricos a la lista de direcciones de proxy explícito de confianza.

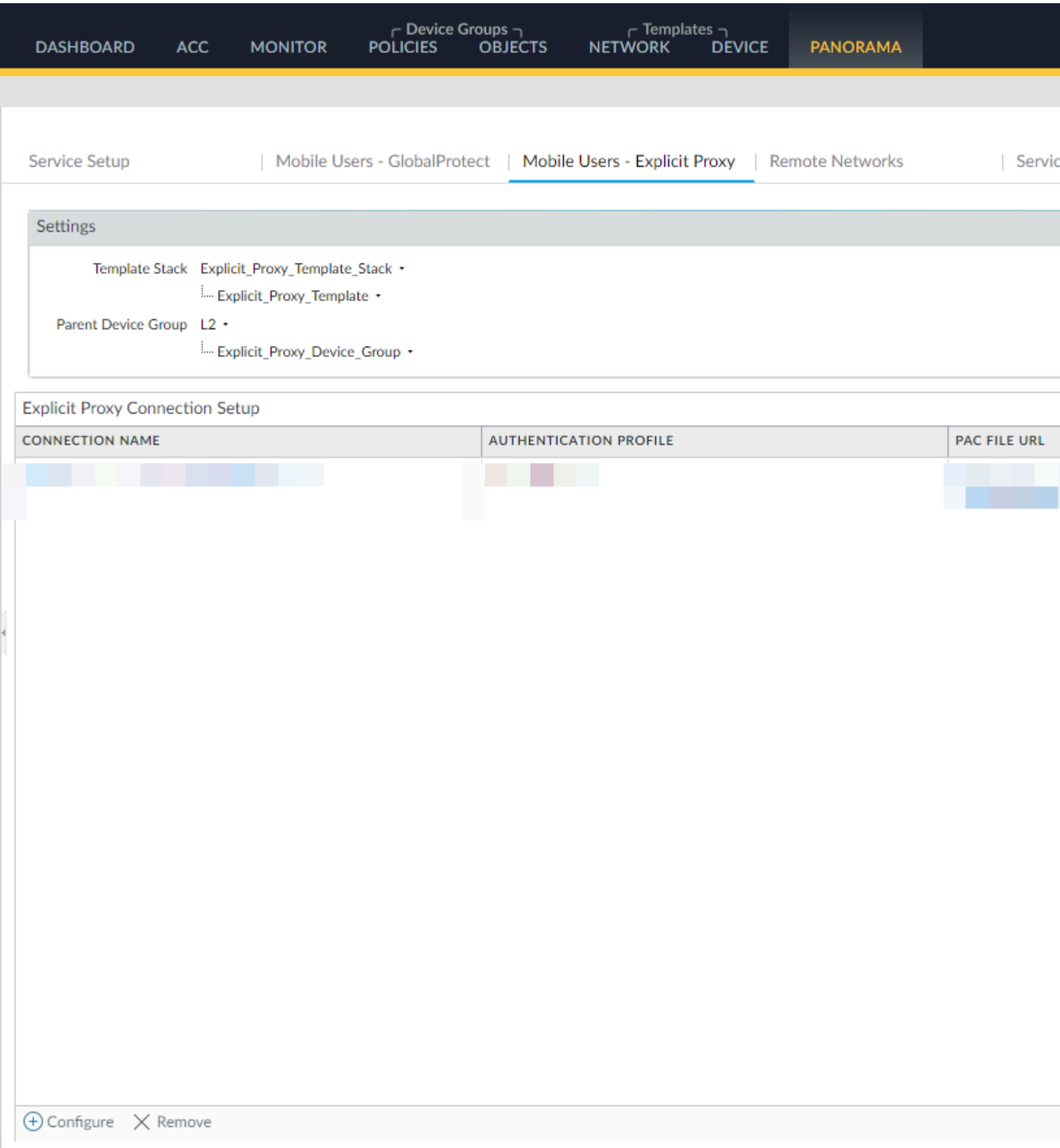
Debe hacer esto solo si lo desea **Skip Authentication (Omitir autenticación)** para direcciones IP específicas o **Use X-Authenticated User (XAU) header on incoming HTTP/HTTPS requests for**

 ©2025 Palo Alto Networks, Inc.

identity (Usar el encabezado de usuario autenticado X (XAU) en las solicitudes HTTP/HTTPS entrantes para la identidad).

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Settings gear (Engranaje de configuración)** > **Authentication Settings (Configuración de autenticación)**.

 ©2025 Palo Alto Networks, Inc.



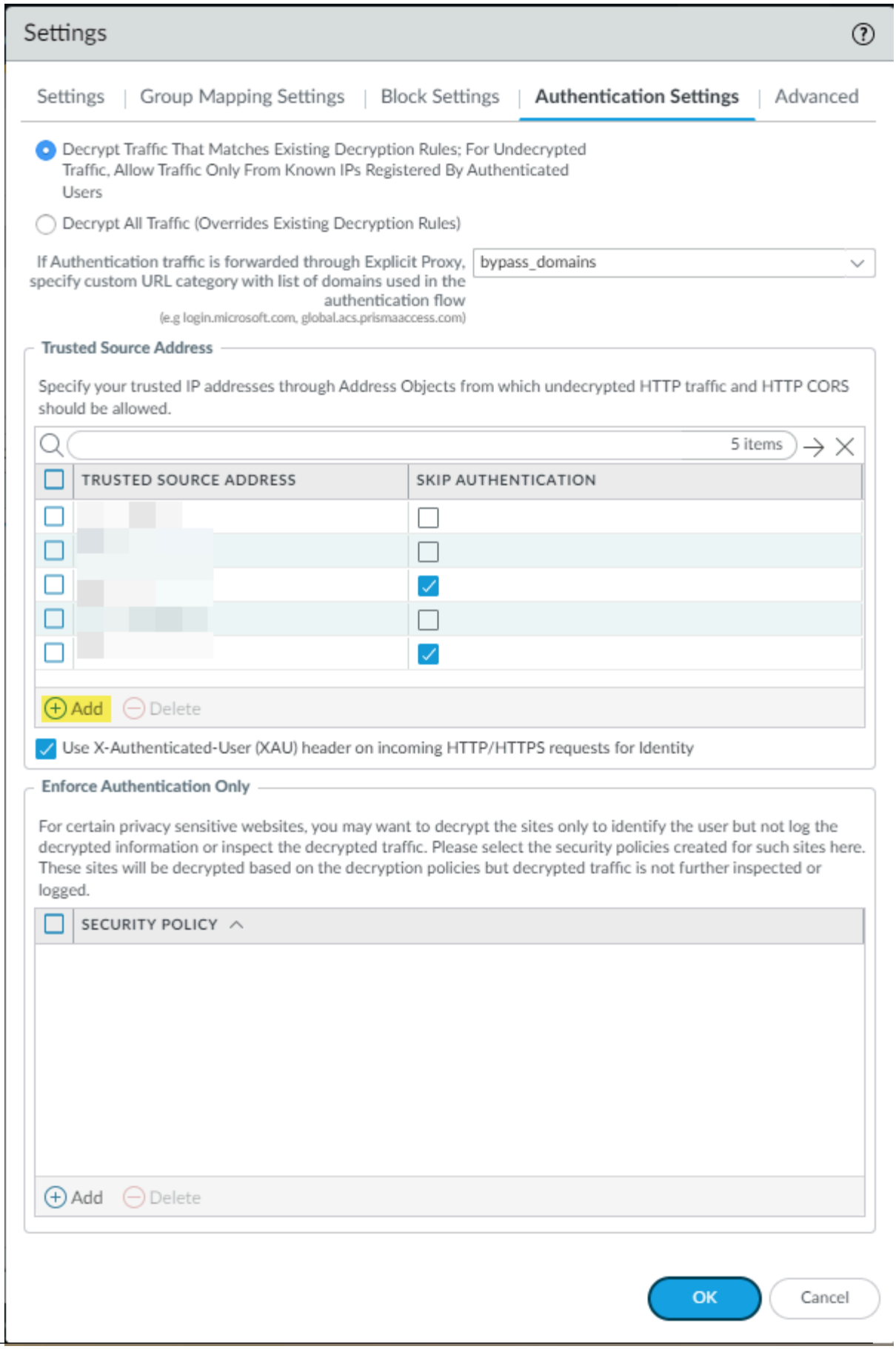
 ©2025 Palo Alto Networks, Inc.

2. Seleccione **Add (Añadir)** direcciones al campo **Trusted Source Address (Dirección de fuente fiable)**.

   Si no añade las direcciones IP del endpoint de salida a la lista de confianza, el proxy explícito obliga a los usuarios y equipos a autenticarse con SAML y Kerberos.

   Introduzca un máximo de 100.000 direcciones IP.

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

3. Seleccione **OK (Aceptar)** para guardar los cambios.

STEP 4 | Cree una regla de política de permitir todo para la autenticación de usuarios.

1. Seleccione **Policies (Políticas)** > **Pre Rules (Reglas previas)** > **+ Add (Añadir +)**.
2. Nombre de la regla.
3. Seleccionar **Source (Fuente)**
4. Establezca Usuario de origen en **known-user (usuario-conocido)**
5. Establezca todos los demás valores necesarios en **Any (Cualquier)**.
6. Seleccione **OK (Aceptar)** para guardar la regla.

STEP 5 | Confirme y envíe sus cambios de configuración.

STEP 6 | Compruebe que la autenticación Kerberos funciona con Prisma Access mediante la visualización de los logs de tráfico y autenticación.

1. (Solo tráfico descifrado) Vaya a **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** y compruebe que la autenticación Kerberos está funcionando.

   El tráfico descifrado muestra el nombre de usuario en los registros de tráfico.

2. (Solo tráfico sin descifrar) Vaya a **Monitor (Supervisar)** > **Logs** > **Authentication (Autenticación)** y compruebe que la autenticación Kerberos funciona correctamente.

   Los siguientes campos proporcionan más información sobre el evento de autenticación:

   - **Object (Objeto)**: el sitio web al que el usuario intentaba acceder antes de ser redirigido a Kerberos para autenticarse.
   - **Auth Event (Evento de autenticación)**: el estado del intento de autenticación.

     Authentication Success (Éxito de la autenticación) indica que el evento de autenticación se ha realizado correctamente; **Authentication Failure (Fallo de autenticación)** indica que se ha producido un error en el intento y genera un log.
   - **Authentication Description (Descripción de la autenticación)**: si se produjo un error en el intento de autenticación, información adicional sobre el tipo de error.

     Por ejemplo **user not allowed (usuario no permitido)** indica que el usuario o grupo no puede usar Kerberos para autenticarse, posiblemente porque no se agregó a la carpeta **Allow List (Lista de permitidos)** en el perfil de autenticación.

Cloud Identity Engine Autenticación para implementaciones de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

Utilice Cloud Identity Engine para proporcionar tanto identificación de usuario como autenticación de usuario para usuarios móviles en una implementación de Prisma Access: Proxy explicito.

Cloud Identity Engine proporciona identificación y autenticación de usuarios para una solución centralizada basada en la nube en entornos de red locales, basados en la nube o híbridos. Cloud Identity Engine le permite escribir políticas de seguridad en función de usuarios y grupos, y ayuda a proteger sus redes mediante la aplicación de acciones de seguridad basadas en el comportamiento.

Al sincronizar de forma continua la información de sus directorios, ya sean locales, basados en la nube o híbridos, garantiza que la información de usuario sea precisa y esté actualizada y que la aplicación de políticas continúe en función de las asignaciones, incluso si el proveedor de identidades en la nube no está disponible temporalmente.

- Autenticación del Cloud Identity Engine para Implementaciones de Proxy Explícito (Strata Cloud Manager)
- Autenticación del Cloud Identity Engine para Implementaciones de Proxy Explícito (Panorama)

Autenticación del Cloud Identity Engine para Implementaciones de Proxy Explícito (Strata Cloud Manager)

Cloud Identity Engine proporciona tanto identificación de usuario como autenticación de usuario para usuarios móviles en una implementación de Prisma Access: Proxy explicito. Cloud Identity Engine se integra con el Servicio de caché de la autenticación (ACS) de proxy explícito y utiliza proveedores de identidad SAML (IdP) para proporcionar autenticación a los usuarios móviles del proxy explícito.

Para configurar la autenticación para una implementación de Proxy explícito de usuarios móviles utilizando el Cloud Identity Engine, complete los siguientes pasos.

STEP 1 | En Prisma Access (Managed by Strata Cloud Manager), configure el Proxy explícito para su inquilino.

Antes de configurar el Proxy Explícito, tenga en cuenta cómo funciona el proxy explícito y las pautas a seguir cuando lo configure.

Si tiene varios inquilinos, configure el Proxy explícito para cada uno de sus inquilinos que lo requieran.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Inicie sesión en el hub y, desde la aplicación de Cloud Identity Engine, configure un tipo de autenticación y un proveedor de autenticación.

Puede ver aplicaciones en el hub por inquilino o por cuenta de soporte.

1. Configura un tipo de autenticación SAML en Cloud Identity Engine.

   La guía de Inicio del Cloud Identity Engine tiene los procedimientos que necesita para configurar un IdP SAML en Cloud Identity Engine:

   - Configurar Azure como un IdP en Cloud Identity Engine
   - Configurar Okta como un IdP en Cloud Identity Engine
   - Configurar PingOne como un IdP en Cloud Identity Engine
   - Configurar PingFederate como un IdP en Cloud Identity Engine
   - Configurar Google como un IdP en Cloud Identity Engine

   No configure el cierre de sesión único, no es compatible.
2. Configure un perfil de autenticación en Cloud Identity Engine y seleccione los usuarios y grupos que pueden utilizar este método de autenticación.

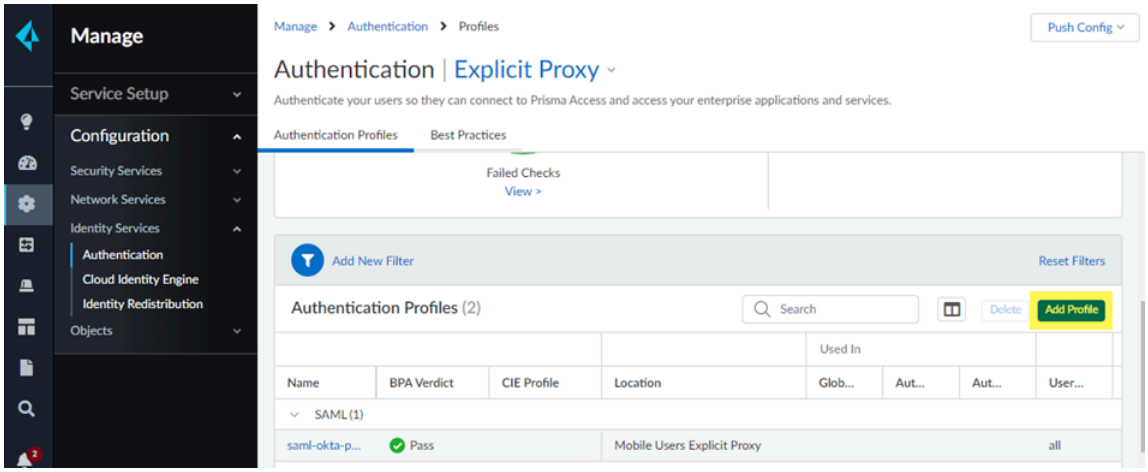
   Especifica este perfil cuando crea un perfil de autenticación en Prisma Access (Managed by Strata Cloud Manager) en un paso posterior.

STEP 3 | Vuelva a Prisma Access (Managed by Strata Cloud Manager) y cree un perfil de autenticación para usar con el Motor de autenticación en la nube.

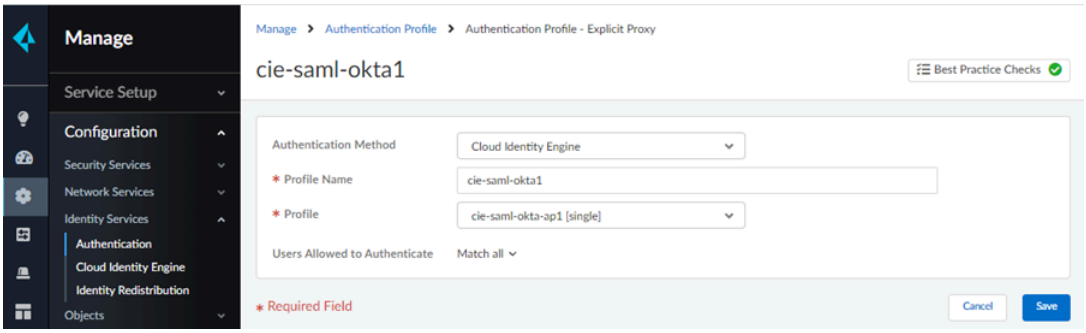
1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication**

 ©2025 Palo Alto Networks, Inc.

(Autenticación), establezca el ámbito en **Explicit Proxy (Proxy explícito)** y añada un perfil de autenticación (**Add Profile (Añadir perfil)**).



2. Seleccione un **Authentication Method (Método de autenticación)** de **Cloud Identity Engine**.
3. Dele al perfil un **Profile Name (Nombre de Perfil)**.
4. Seleccione el perfil de autenticación de Cloud Identity Engine que creó en un paso anterior.

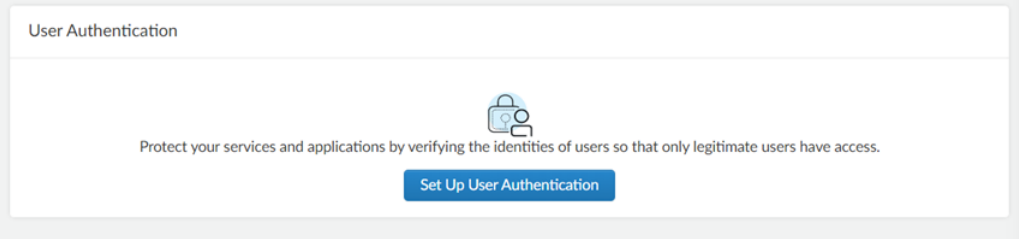


5. Haga clic en **Save (Guardar)** para guardar sus cambios.

©2025 Palo Alto Networks, Inc.

STEP 4 | Configure la autenticación de usuarios en el Proxy explícito.

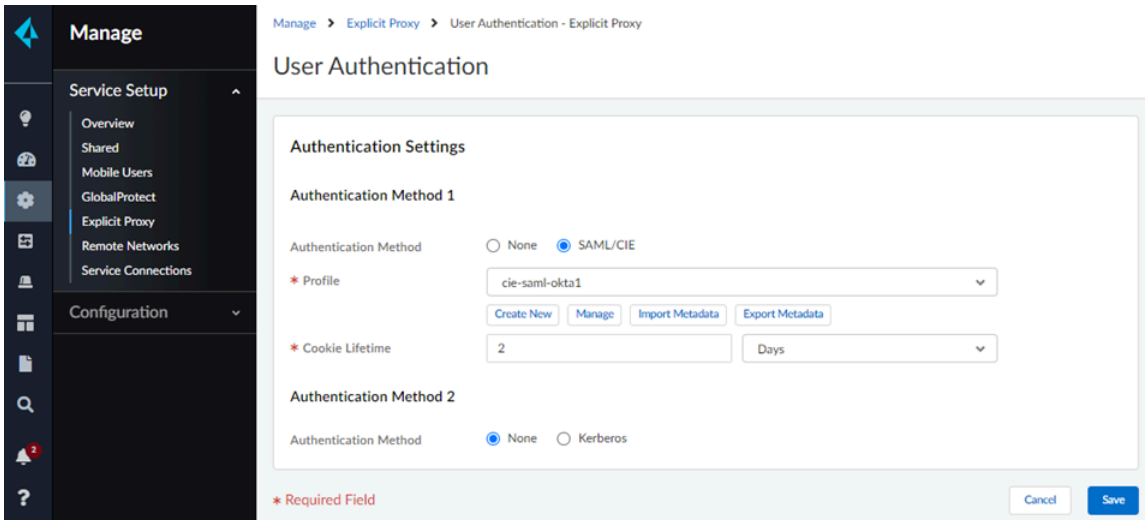
1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración)** > **Explicit Proxy (Proxy explícito)** y **Set Up User Authentication (Configurar la autenticación de usuario)**.



2. Seleccione un **Authentication Method (Método de autenticación)** de **SAML/CIE**.
3. Seleccione el perfil de autenticación que creó en Cloud Managed Prisma Access.
4. Especifique una **duración de la cookie** para la cookie que almacena las credenciales de autenticación de los usuarios.

   Después de que el IdP autentique al usuario, Prisma Access almacena el estado de autenticación del usuario en el Servicio de caché de autenticación (ACS). El período de validez de la autenticación se basa en el valor de la duración de la cookie que especifique aquí.

   Para evitar problemas con los usuarios que no pueden descargar archivos grandes antes de que expire la duración de la cookie, o la cookie expire cuando los usuarios están accediendo a un solo sitio web durante un largo período de tiempo, Palo Alto Networks recomienda que configure una **Cookie Lifetime (Vida útil de la cookie)** de al menos un día. Si los usuarios de Proxy explícito tienen un problema de caducidad de la duración de la cookie, pueden navegar a un sitio web diferente para volver a autenticarse en ACS y actualizar la cookie de ACS.

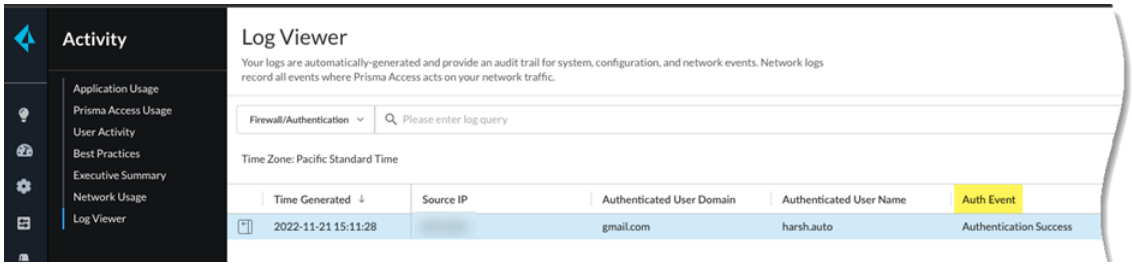


5. Haga clic en **Save (Guardar)** para guardar sus cambios.

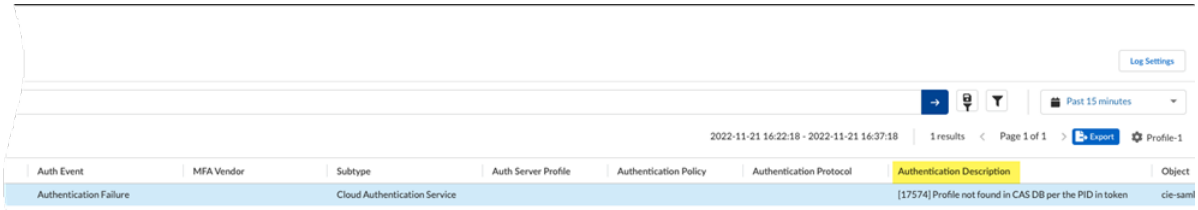
©2025 Palo Alto Networks, Inc.

STEP 5 | Verifique que Cloud Identity Engine esté autenticando correctamente a sus usuarios móviles de Proxy explícito.

1. Desde Prisma Access (Managed by Strata Cloud Manager), seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)** > **Firewall/Authentication (Cortafuegos/autenticación)**.
2. Vea el estado del **Auth Event (Evento de autenticación)**.

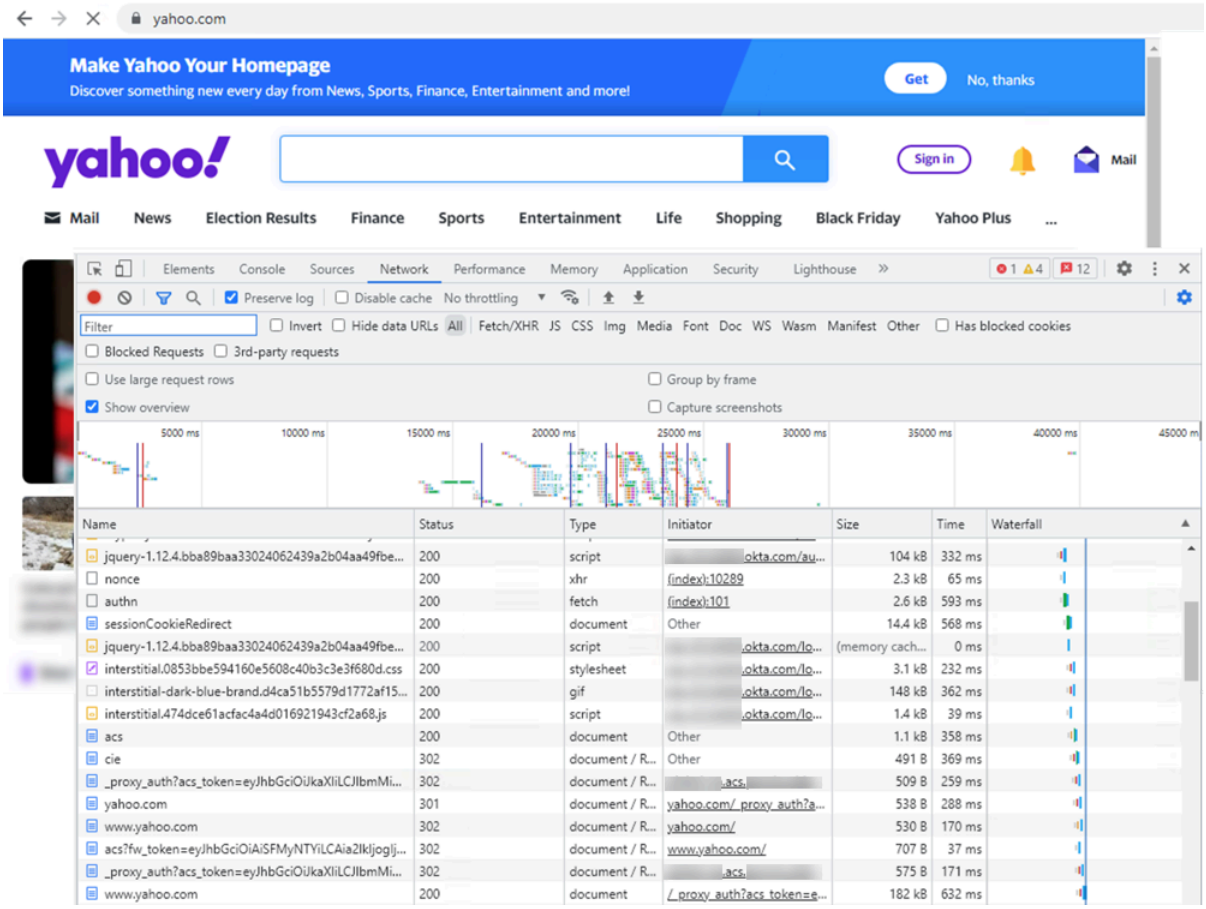


Si la autenticación falla, consulte la **Authentication Description (Descripción de la autenticación)** para obtener más detalles sobre el fallo.



3. Desde el endpoint del usuario móvil, utilice las herramientas de desarrollo para ver el flujo de autenticación de Cloud Identity Engine.

 ©2025 Palo Alto Networks, Inc.



Autenticación del Cloud Identity Engine para Implementaciones de Proxy Explícito (Panorama)

Autenticar usuarios móviles de proxy explícito de Prisma Access (Managed by Panorama) con Cloud Identity Engine

Modo proxy para redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si desea habilitar la visibilidad y aplicación basadas en la IP de origen privada en el Proxy explícito en su entorno de Prisma Access, póngase en contacto con su equipo de cuentas para obtener más información.	• Licencia de Prisma Access Se requiere una licencia de Prisma Access Usuarios móviles y una de Prisma Access Redes remotas para el Modo proxy para redes remotas.

El Modo proxy en redes remotas ayuda a asegurar el tráfico de internet saliente para usuarios y servidores en sus sucursales que necesitan un método de conexión basado en PAC debido a razones de red o cumplimiento.

©2025 Palo Alto Networks, Inc.

Puede usar el Modo proxy para redes remotas para:

- Proteger el tráfico que sale a Internet desde las sucursales que utilizan rutas no predeterminadas.
- Proteger el tráfico dirigido a Internet que sale de sus sucursales sin redirigirlo a un centro de datos o a la sede.
- Conéctese al Prisma Access Proxy explícito a través de direcciones IP privadas.

  Prisma Access le proporciona cuatro direcciones IP anycast a nivel global y una dirección IP unicast por Red remota, que utiliza para redirigir el tráfico al Proxy explícito.
- Aplique controles de seguridad y obtenga visibilidad basada en la IP de origen para los sistemas en la sucursal.
- Omitir la autenticación para servidores basados en la dirección IP de origen.
- Conéctese a Prisma Access desde su sucursal a través de un túnel IPSec.
- Si necesita más de 1000 Mbps de ancho de banda, puede crear una conexión de red remota de alto ancho de banda utilizando múltiples conexiones de red remota y especificar las direcciones de unicast y anycast del proxy explícito en cada conexión.

El siguiente diagrama muestra una Red remota que se ha configurado para un sitio que no tiene una ruta predeterminada configurada. Para proteger a los usuarios y dispositivos sin cabeza en el sitio utilizando Proxy explícito, el administrador ha realizado los siguientes cambios de configuración:

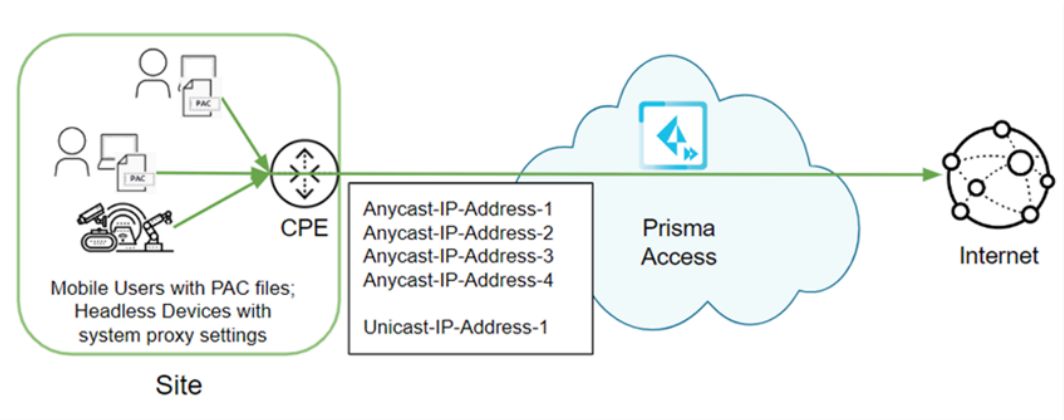
- Ha incorporado ubicaciones de redes remotas y ubicaciones de proxy explícito y ha recuperado las direcciones IP anycast y unicast que Prisma Access toma de su subred de infraestructura.

  También puede crear un nombre de host para el tráfico dirigido por el Proxy explícito y añadir las direcciones IP unicast y anycast del Proxy explícito a ese nombre de host.
- Se configuró el CPE para reenviar el tráfico de Proxy explícito a estas direcciones anycast y unicast.

  Utilice las direcciones IP anycast en el archivo PAC para que Prisma Access seleccione cualquier túnel de Red remota incorporado para redirigir el tráfico al Proxy explícito. Utilice la dirección unicast para que Prisma Access envíe tráfico a través de un túnel de Red remota específico. En este ejemplo, puede usar direcciones de anycast o unicast, ya que el tráfico solo pasa a través de un túnel IPSec de Red remota.
- Ha especificado estas direcciones IP en los archivos PAC de los endpoints de los usuarios y en la configuración del proxy del sistema de los dispositivos sin cabeza.

Después de que se complete la configuración, Prisma Access reenvía el tráfico del túnel de la Red remota al Proxy explícito.

 ©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

Modo proxy en Redes remotas (Strata Cloud Manager)

Para proteger a los usuarios en redes remotas utilizando Proxy explícito en Cloud Managed Prisma Access, complete los siguientes pasos.

STEP 1 | Configure su configuración de Proxy explícito y añada las ubicaciones de Proxy explícito que desea añadir.

STEP 2 | Incorpore sus redes remotas si aún no lo ha hecho.

Deberá habilitar Redes remotas de Prisma Access en las ubicaciones que son compatibles con Proxy explícito.

STEP 3 | **Push Config (Enviar configuración)**, asegurándose de que **Mobile Users—Remote Workforce (Usuarios Móviles: Fuerza laboral remota)** y **Remote Networks (Redes remotas)** estén seleccionados en el ámbito de **Push (Envío)**.

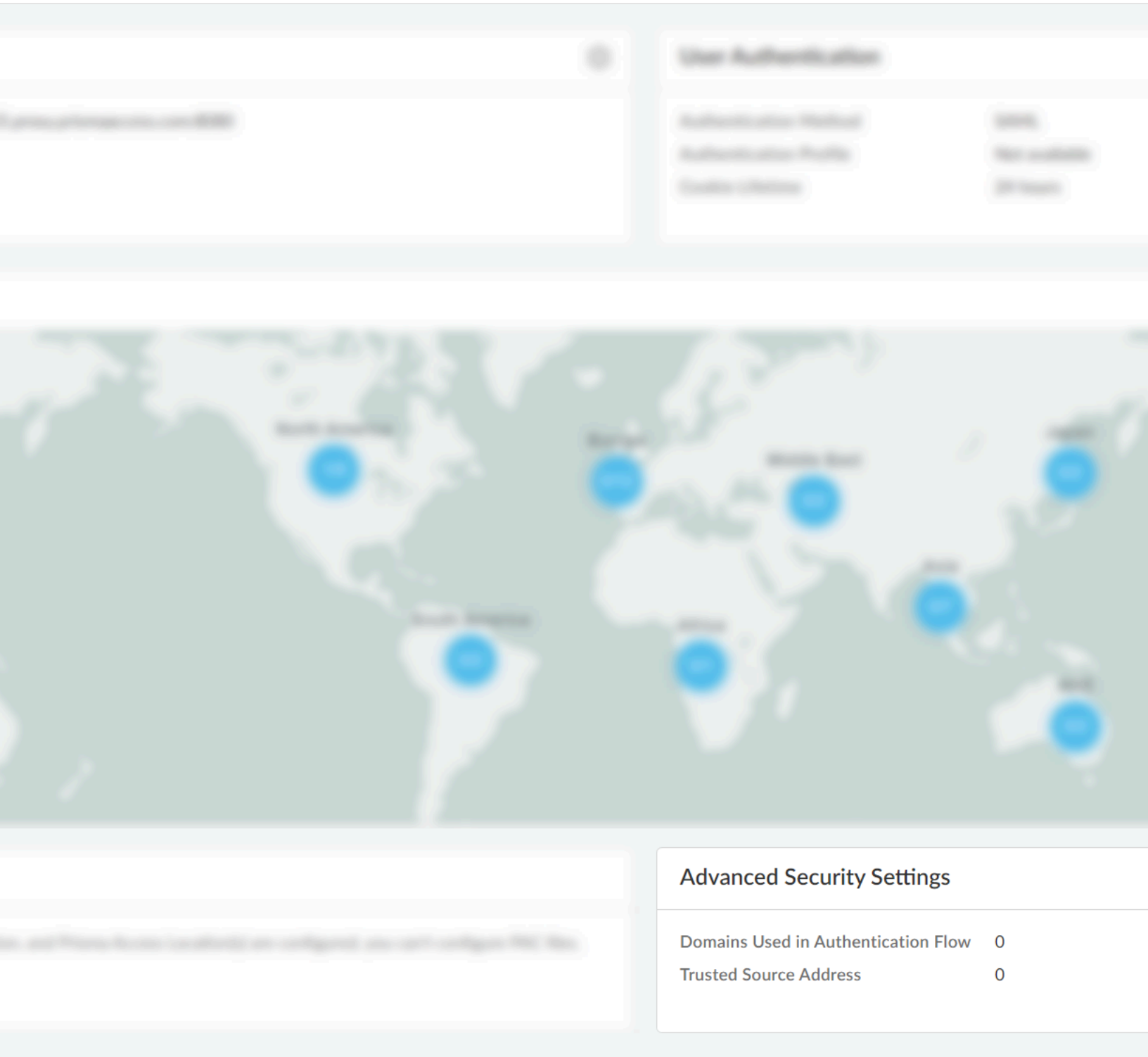
La operación push recupera y realiza una difusión por proximidad, Anycast, de las direcciones que necesita para integrar el Proxy explícito con la red remota.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Obtenga las direcciones IP anycast que utiliza para su implementación de Proxy explícito/red remota.

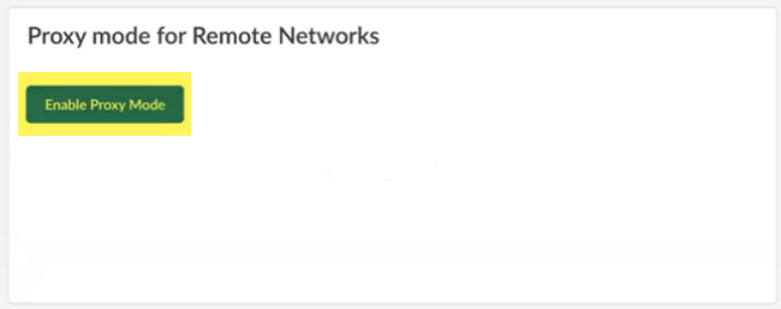
1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Advanced Security Settings (Configuración de seguridad avanzada)**.

 ©2025 Palo Alto Networks, Inc.



2. **Habilitar el modo proxy.**

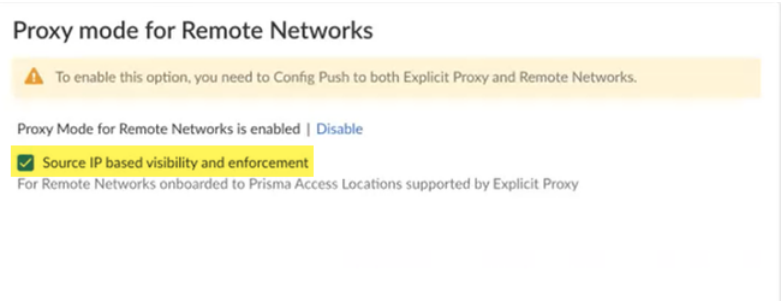
©2025 Palo Alto Networks, Inc.



3. Para aprovechar las direcciones IP de origen de los sistemas en sus ubicaciones de sucursales que están reenviando tráfico al Proxy explícito, seleccione la **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)**.

   Esta funcionalidad tiene estos requisitos:

   - Un plano de datos de Prisma Access mínimo de 10.2.4
   - Debe utilizar solo ubicaciones de red remotas compatibles con Proxy explícito.



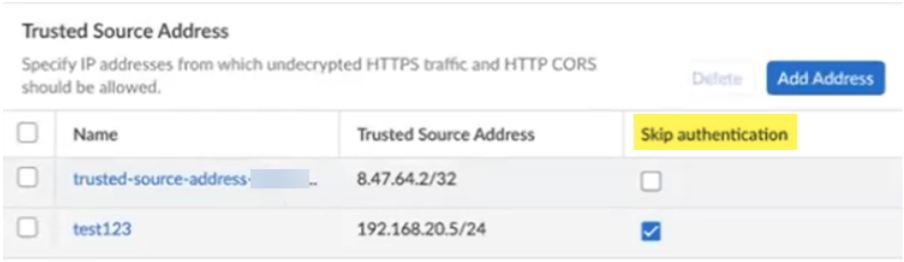
4. Añada una política para permitir el tráfico destinado a direcciones IP anycast y unicast en redes remotas. Si ha habilitado la **Source IP visibility and enforcement (Visibilidad y aplicación de IP de origen)**, utilice el campo de **Source IP (IP de origen)** en las políticas de seguridad en el Proxy explícito para asegurar el tráfico. Necesita políticas adicionales en las redes remotas.
5. (Opcional) Para omitir la autenticación de cualquier dirección de origen fiable que haya introducido, especifique las direcciones IP que deberían omitir la autenticación en el área de **Trusted Source Address (Dirección de fuente fiable)** y seleccione **Skip authentication (Omitir autenticación)**.

   Puede usar **Skip authentication (Omitir autenticación)** con **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)** para omitir la

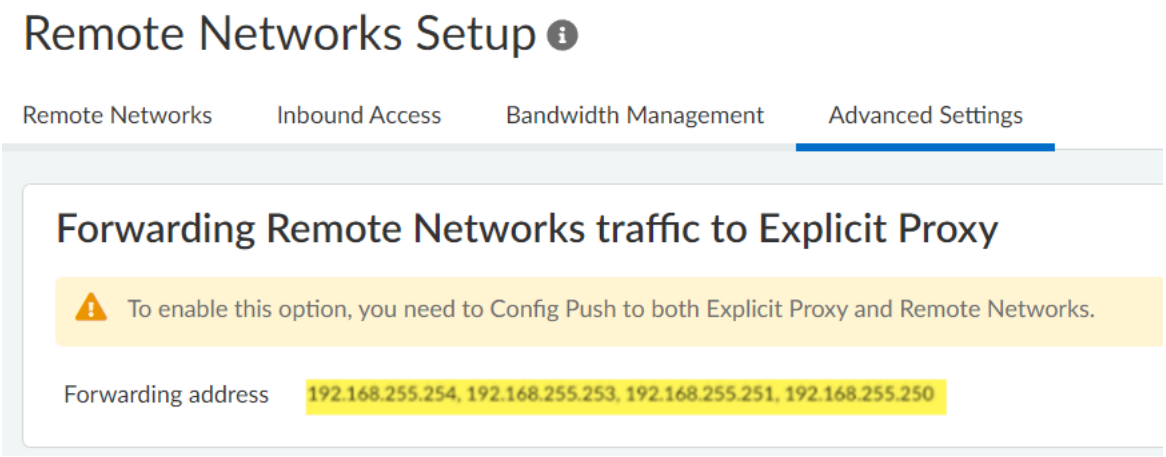
 ©2025 Palo Alto Networks, Inc.

autenticación de sistemas sin cabeza que no pueden autenticar, configurar políticas de seguridad y obtener visibilidad del tráfico en el Proxy explícito de Prisma Access.

Puede añadir direcciones IP o subredes. Se admiten un máximo de 100,000 direcciones IP después de expandir las subredes.



6. Vaya a **Workflows (Flujos de trabajo)** > **Prisma AccessSetup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)**.
7. **Push Config (Enviar configuración)**, asegurándose de que **Mobile Users—Remote Workforce (Usuarios Móviles: Fuerza laboral remota)** y **Remote Networks (Redes remotas)** estén seleccionados en el ámbito de **Push (Envío)**.
8. Vaya a **Advanced Settings (Configuración Avanzada)** en la Configuración de redes remotas y encuentre las direcciones IP anycast utilizadas para reenviar tráfico al Proxy explícito.



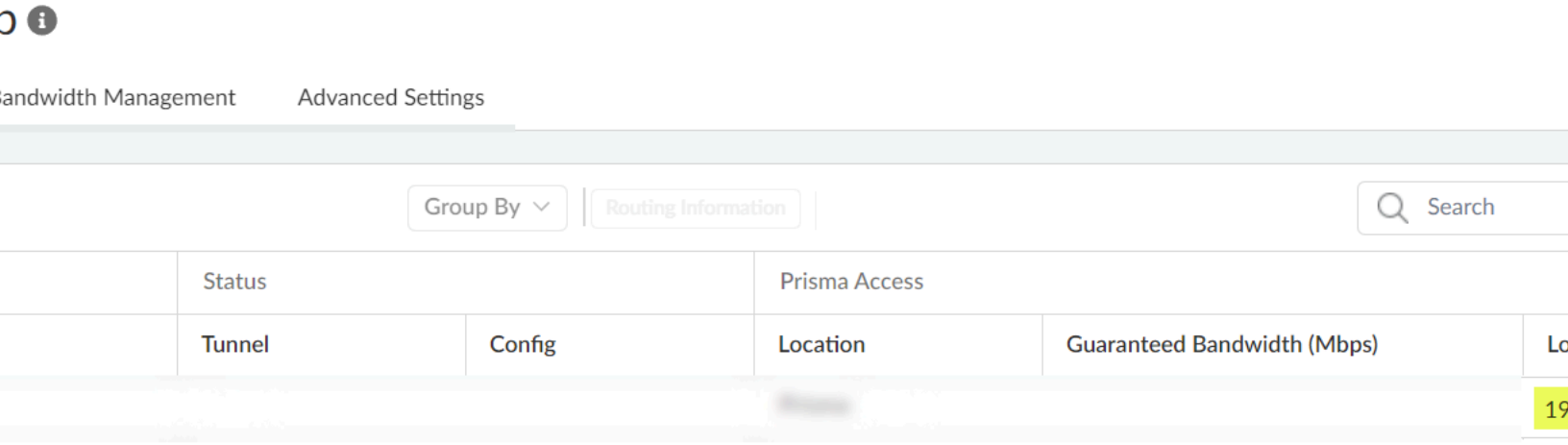
 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Encuentre la dirección unicast que va a usar para su implementación de Proxy explícito/red remota.

Utilice la dirección IP unidifusión en el archivo PAC solo si desea dirigir el tráfico a un Proxy explícito en una red remota específica. Si desea utilizar todas las Redes remotas implementadas para redirigir el tráfico al Proxy explícito, utilice las direcciones anycast.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma AccessSetup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)**.
2. Tome nota de la dirección **Loopback IP (IP de bucle invertido)**.

   Si tiene direcciones IPv4 e IPv6, toma nota de la dirección IPv4.



Modo proxy en Redes remotas (Panorama)

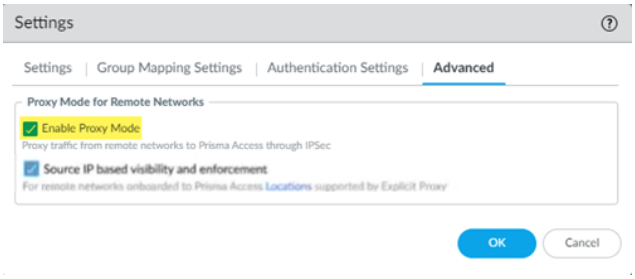
Para proteger a los usuarios en redes remotas mediante proxy explícito en Prisma Access (Managed by Panorama) Access, complete los siguientes pasos.

STEP 1 | Configure su implementación de Proxy explícito e incorpore las ubicaciones de proxy explícito que desee añadir.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Recupere las direcciones IP anycast que utiliza para su implementación de proxy explícito/red remota.

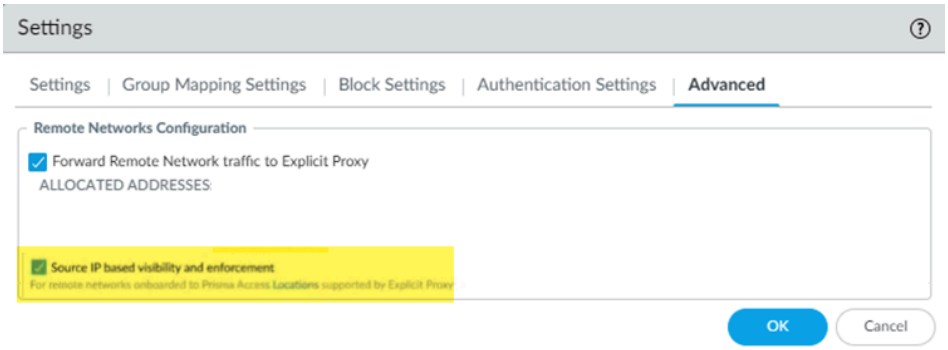
1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: proxy explícito)**.
2. Seleccione el icono de engranaje para editar la **Settings (Configuración)**.
3. Seleccione **Enable Proxy Mode (Habilitar el modo proxy)**.



4. Para aprovechar las direcciones IP privadas de los sistemas en sus ubicaciones de sucursales que están reenviando tráfico al Proxy explícito, seleccione la **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)**.

   Esta funcionalidad tiene estos requisitos:

   - Un plano de datos de Prisma Access de 10.2.4 como mínimo
   - Una implementación de Prisma Access (Managed by Panorama) con un complemento Cloud Services mínimo de 4.1
   - Debe utilizar únicamente ubicaciones de red remotas compatibles con Proxy explícito.



5. Añada una política para permitir el tráfico destinado a direcciones IP anycast y unicast en redes remotas. Si ha habilitado la **Source IP visibility and enforcement (Visibilidad y aplicación de IP de origen)**, utilice el campo de **Source IP (IP de origen)** en las políticas de seguridad en el Proxy explícito para asegurar el tráfico. Necesita políticas adicionales en las redes remotas.
6. (Opcional) En **Authentication Settings (Configuración de autenticación)**, introduzca cualquier dirección IP desde la cual se debe permitir el tráfico HTTP o HTTP Cross-

 ©2025 Palo Alto Networks, Inc.

Origin Resource Sharing (CORS) sin cifrar a la **Trusted Source Address Auth Bypass (Omisión de autenticación de dirección de fuente fiable**.

Añada las direcciones IP a los objetos de dirección basados en direcciones IP y luego **Add (añadir)** para añadir los objetos de dirección en el campo.

Introduzca un máximo de 100,000 entradas. Asegúrese de que el objeto de dirección utilice únicamente direcciones IP.

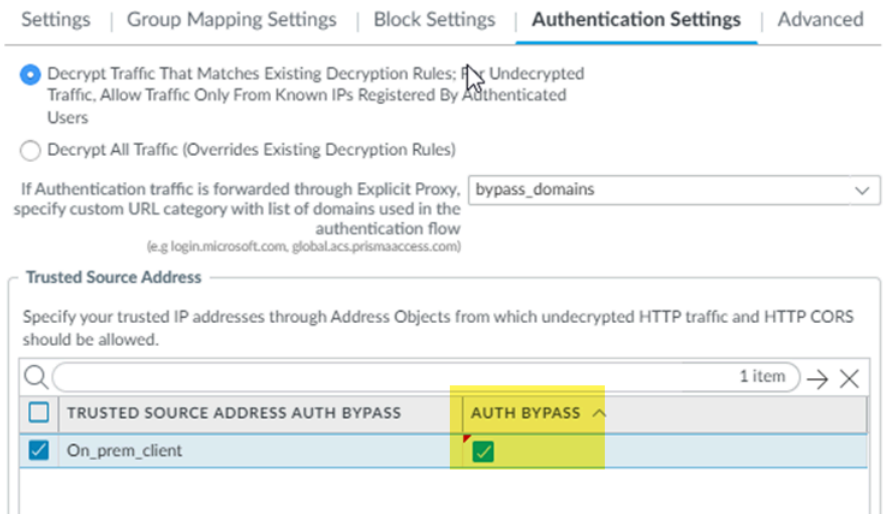
7. (Opcional) Para omitir la autenticación de cualquier dirección de fuente fiable que haya introducido, seleccione **Auth Bypass (Omitir autenticación)**.

   Puede usar **Auth Bypass (Omitir autenticación)** con **Source IP based visibility and enforcement (Visibilidad y aplicación basadas en IP de origen)** para omitir la

 ©2025 Palo Alto Networks, Inc.

autenticación de sistemas sin cabeza que no pueden autenticar, configurar políticas de seguridad y obtener visibilidad del tráfico en el Proxy explícito de Prisma Access.

Puede añadir direcciones IP o subredes. Se admiten un máximo de 100,000 direcciones IP después de expandir las subredes.



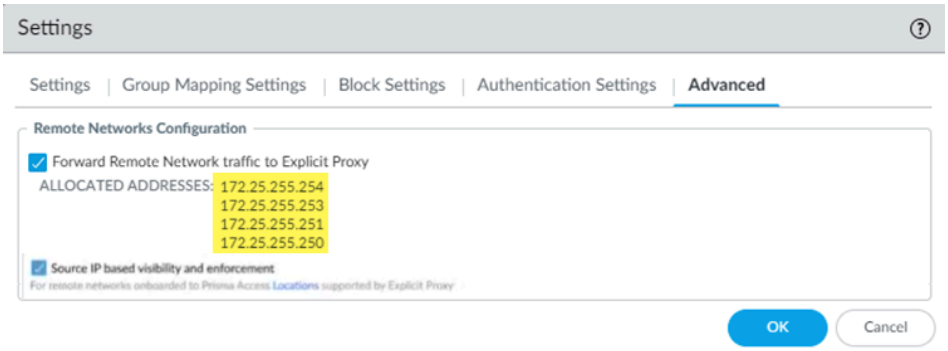
8. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.
9. Integre sus ubicaciones de red remotas si aún no lo ha hecho.

   Deberá habilitar Redes remotas de Prisma Access en las ubicaciones que son compatibles con Proxy explícito.
10. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
11. Deberá **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access** , asegúrese de que **Prisma Access for networks (Prisma Access para redes)** se selecciona en **Push Scope (Ámbito de envío)**, luego haga clic en **OK (Aceptar)**.
12. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

    Debe realizar una confirmación y un envío para sus redes remotas para Prisma Access para recuperar las direcciones IP utilizadas en una implementación de red remota/proxy explícito.
13. Vuelva a la **Settings (Configuración)** de proxy explícito [**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** > **Settings (Configuración)** > **Advanced (Avanzado)**]

©2025 Palo Alto Networks, Inc.

y tome nota de las **ALLOCATED ADDRESSES (DIRECCIONES ASIGNADAS)** que se muestran en **Networks Configuration (Configuración de redes remotas)**.



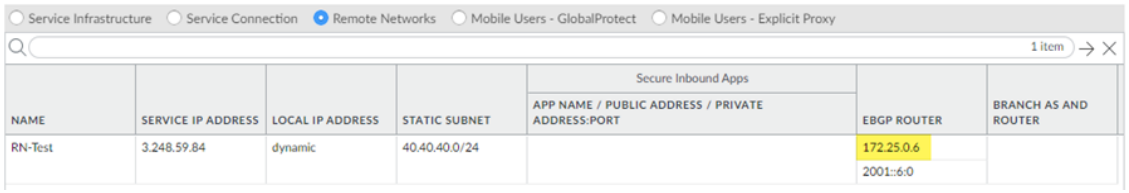
STEP 3 | (Opcional) Busque la dirección de unidifusión que utiliza para su implementación de red remota/proxy explícito.

Utilice la dirección IP unidifusión en el archivo PAC solo si desea dirigir el tráfico a un Proxy explícito en una red remota específica. Si desea utilizar todas las Redes remotas implementadas para redirigir el tráfico al Proxy explícito, utilice las direcciones anycast.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)**.
2. Tome nota de la dirección del **EBGP Router (enrutador EBGP)**.

   Si tiene direcciones IPv4 e IPv6, toma nota de la dirección IPv4.

   Esta dirección también se conoce como dirección de bucle invertido. Si ha realizado cambios de configuración que cambiaron la dirección del enrutador EBGP, puede recuperar la dirección IP de bucle invertido utilizando la API heredada de Prisma Access.



STEP 4 | Asegúrese de que el CPE de su red esté configurado correctamente para que los endpoints reenvíen tráfico al proxy explícito a través de las direcciones IP de unidifusión y anycast.

Cómo el proxy explícito identifica a los usuarios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

©2025 Palo Alto Networks, Inc.

El proxy explícito identifica a los usuarios en los logs de tráfico en función de cómo se autentican los usuarios con el proxy, como se muestra en la tabla siguiente.

Tipo de autenticación	Identificación de usuarios en logs de tráfico
Usuarios que inician sesión mediante la autenticación y el descifrado SAML	El nombre de usuario.
Usuarios que inician sesión desde otro proxy que usa encabezados X-Authenticated-User (XAU)	Información del encabezado XAU El proxy explícito solo permite que el tráfico de direcciones IP específicas utilice XAU para la autenticación. Crea un objeto de dirección y especifica las direcciones IP en las que se permite la autenticación de XAU; a continuación, añada el objeto de dirección en el campo **Trusted Source Address (Dirección de origen de confianza)** durante la configuración del proxy explícito.
Solicitudes autenticadas de uso compartido de recursos entre orígenes (CORS)	El usuario `swg-authenticated-ip-user`. Parte del tráfico proviene de usuarios autenticados cuyos navegadores no pueden enviar cookies ni realizar redireccionamientos de autenticación, como las solicitudes de CORS. En tales casos, el Proxy explícito añade el atributo `swg-authenticated-ip-user` a los logs de tráfico.
Tráfico sin descifrar (si ha permitido que el proxy explícito permita el tráfico sin descifrar de direcciones IP en las que los usuarios se han autenticado previamente)	El usuario `swg-authenticated-ip-user`. Puede especificar el proxy explícito para permitir el tráfico sin descifrar desde las direcciones IP en las que los usuarios se han autenticado; para ello, especifique **Decrypt traffic that matches existing decryption rules; for undecrypted traffic, allow traffic only from known IPs registered by authenticated users (Descifrar el tráfico que coincida con las reglas de descifrado existentes; para el tráfico sin descifrar, permita el tráfico solo desde direcciones IP conocidas registradas por usuarios autenticados)** al configurar el proxy explícito. En estas configuraciones, Proxy explícito añade `swg-authenticated-ip-user` a los logs de tráfico.
Tráfico de los dominios para los que has elegido omitir la autenticación	El usuario *swg-known-auth-bypass*. Cuando configure el Proxy explícito, puede optar por omitir la autenticación de dominios específicos. El nombre de usuario para el tráfico de estos dominios

©2025 Palo Alto Networks, Inc.

Tipo de autenticación	Identificación de usuarios en logs de tráfico
	aparecerá en los registros como *swg-conocido-auth-bypass*.

Perfiles de reenvío de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de usuarios móviles de Prisma Access

Los perfiles de reenvío de proxy explícito le permiten emplear varios archivos PAC para definir qué tráfico reenviar a Prisma Access. Los perfiles de reenvío también le dan la opción de crear reglas de reenvío fáciles de usar en lugar de lidiar con la complejidad de crear y mantener un archivo PAC.

- Usar perfiles de reenvío para definir varios archivos PAC
- Definir qué tráfico reenviar al proxy explícito con reglas de reenvío
- Adjuntar perfiles de reenvío a la configuración de aplicaciones de GlobalProtect

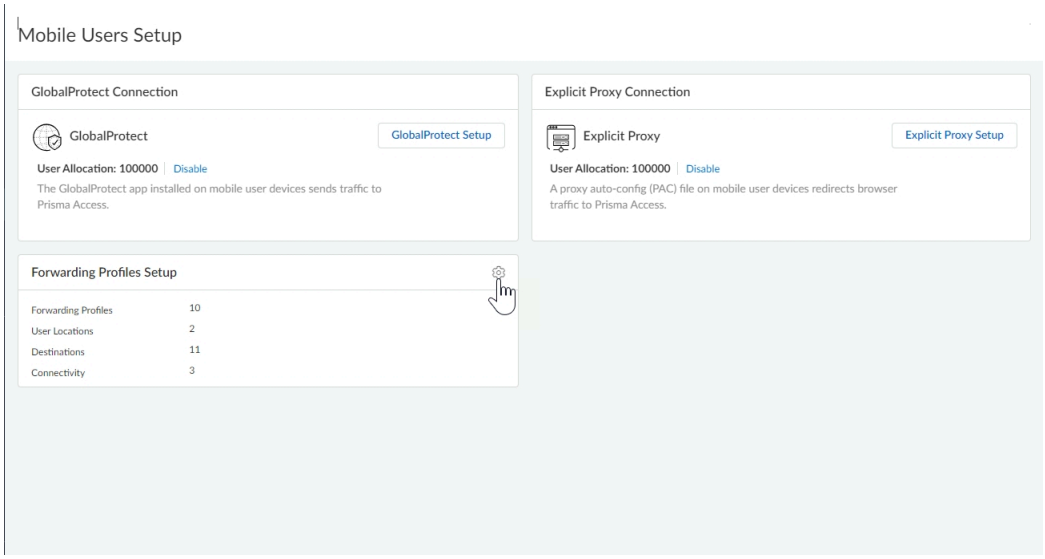
Usar perfiles de reenvío para definir varios archivos PAC

Los perfiles de reenvío le permiten usar varios archivos PAC en su implementación simultáneamente para que pueda definir qué tráfico reenviar a Prisma Access.

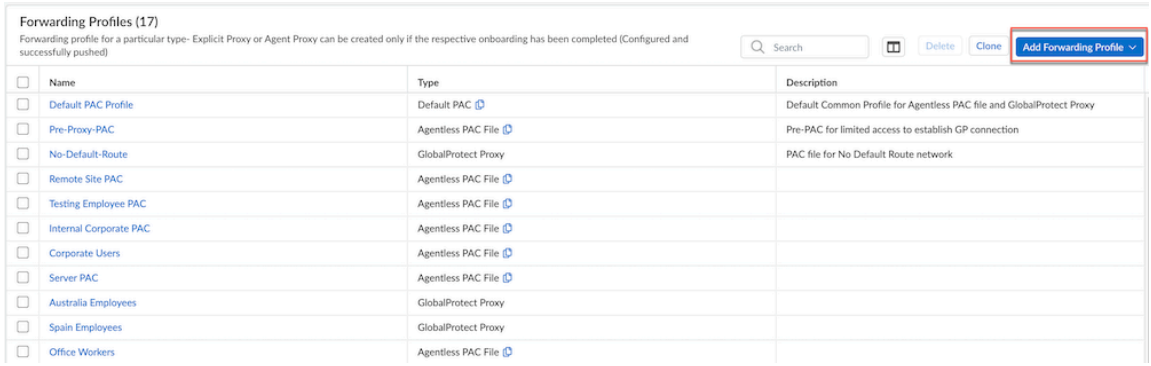
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Cree un perfil de reenvío de logs.

1. De Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** > **Forwarding Profiles Setup (Configuración de perfiles de reenvío)**.



2. **Add Forwarding Profile (Añadir perfil de reenvío)**.



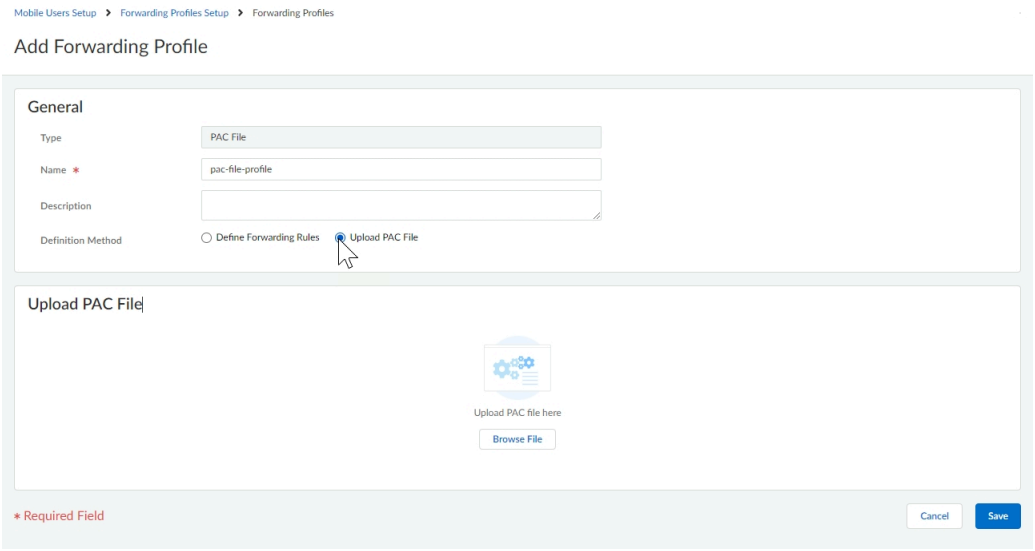
STEP 2 | Seleccione **PAC File (Archivo PAC)**.

El **PAC File (Archivo PAC)** es para Proxy explícito de Prisma Access. **GlobalProtect Proxy (Proxy de GlobalProtect)** es para usar GlobalProtect en modo proxy.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cargar un archivo PAC.

1. Seleccione **Upload PAC File (Cargar archivo PAC)** para cargar un archivo PAC existente o crear un archivo PAC utilizando las directrices de archivo PAC.



2. **Browse file (Examinar archivo)** para buscar en su sistema de archivos el archivo PAC.
3. Seleccione **Save (Guardar)** el perfil.

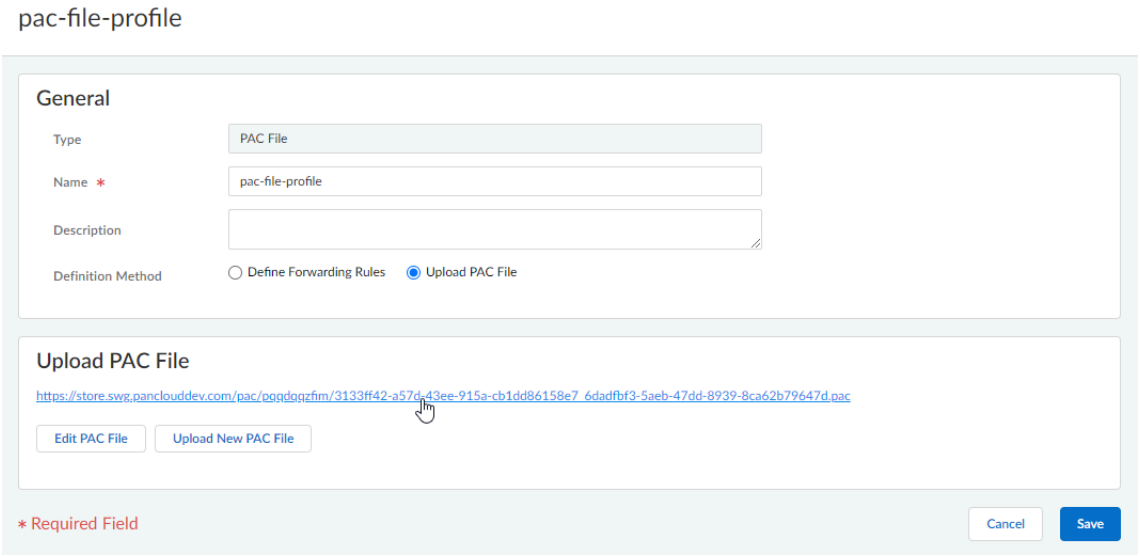
STEP 4 | Repita los dos pasos anteriores para crear otro perfil de reenvío con un archivo PAC diferente.

Ambos archivos PAC ahora están operando en su implementación simultáneamente.

STEP 5 | Recupere la URL del archivo PAC.

1. Vuelva al perfil al que cargó el archivo PAC.

   Debería ver la URL donde está alojado el archivo PAC.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Edite el archivo PAC.

Para realizar cambios rápidamente en el archivo PAC, puede editarlo directamente dentro de la interfaz web

1. Desde el Perfil de reenvío, deberá **Edit PAC File (Editar archivo PAC)**.
2. Haga cambios y dele a **Save (Guardar)**.



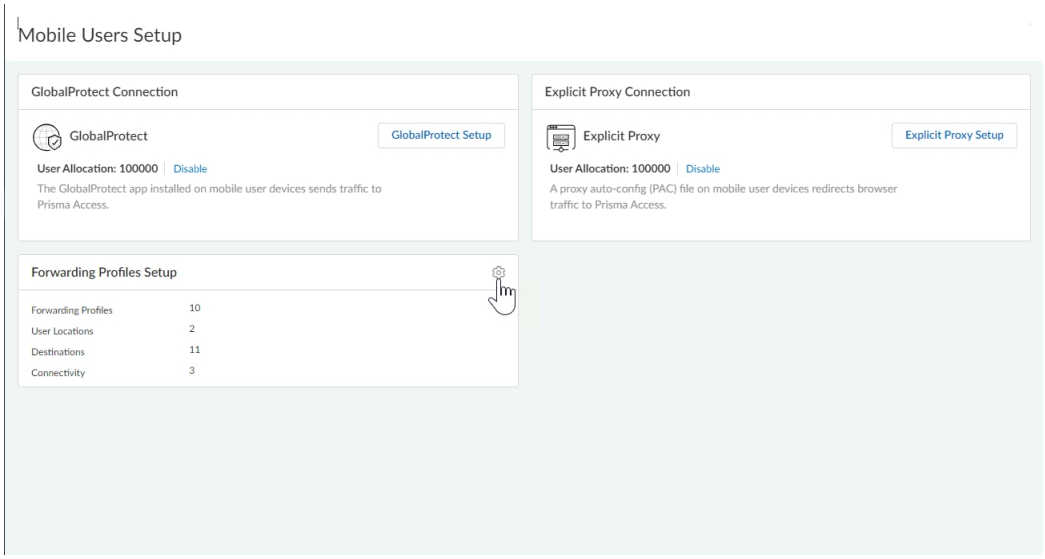
Definir qué tráfico reenviar al proxy explícito con reglas de reenvío

En lugar de crear su propio archivo PAC desde cero, puede crear reglas de reenvío simples para generar un archivo PAC.

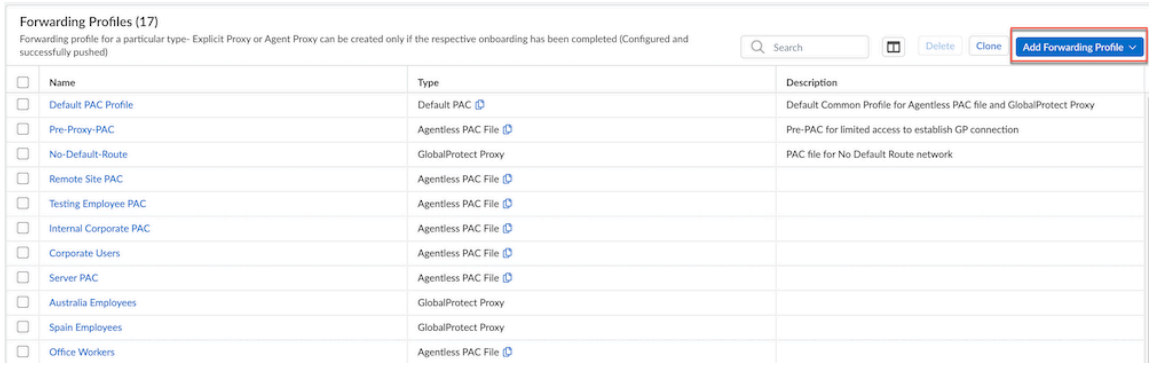
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Cree un perfil de reenvío de logs.

1. De Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** > **Forwarding Profiles Setup (Configuración de perfiles de reenvío)**.



2. **Add Forwarding Profile (Añadir perfil de reenvío)**.



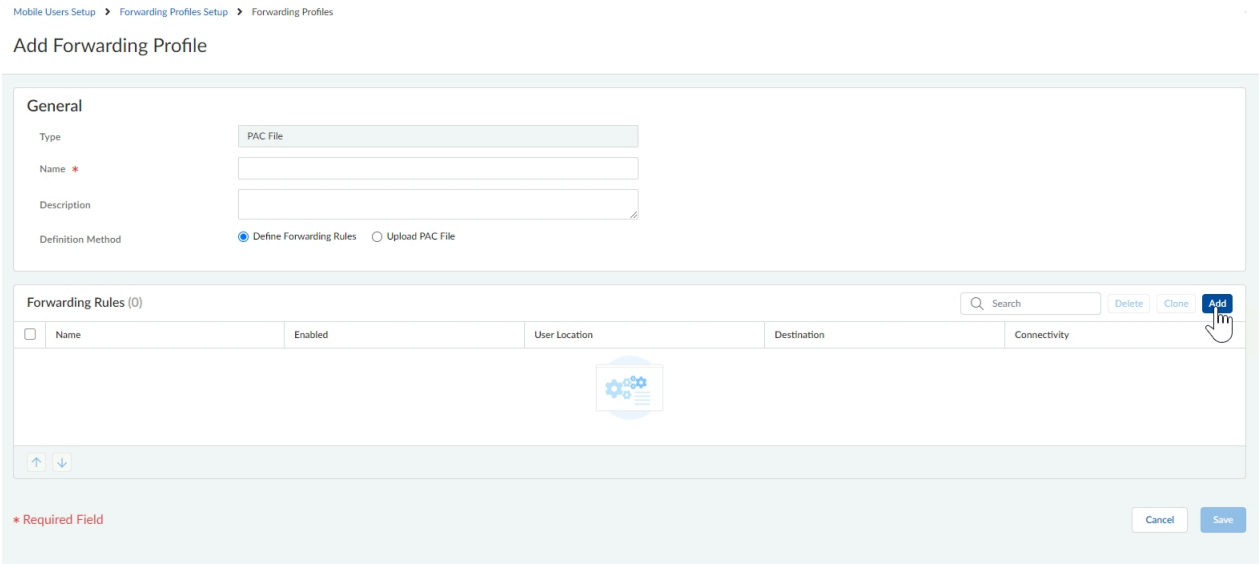
STEP 2 | Seleccione **PAC File (Archivo PAC)**.

El **PAC File (Archivo PAC)** es para Proxy explícito de Prisma Access. **GlobalProtect Proxy (Proxy de GlobalProtect)** es para usar GlobalProtect en modo proxy.

©2025 Palo Alto Networks, Inc.

STEP 3 | Añadir una regla de reenvío.

1. Seleccione **Add (Añadir)**.



2. Complete los campos requeridos:

Nombre	Nombre del perfil.
Ubicaciones de los usuarios	Ubicación de los usuarios para los que está creando la regla de reenvío. Puede crear ubicaciones personalizadas desde **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** > **Forwarding Profiles Setup (Configuración de perfiles de reenvío)** > **User Locations (Ubicaciones de usuario)**. *No puede usar caracteres comodín al configurar ubicaciones de usuario personalizadas basadas en la dirección IP.*
Destinos	Destino del tráfico web. Puede seleccionar entre destinos predefinidos o puede crear destinos personalizados a partir de **Workflows (Flujos de trabajo)** > **Prisma AccessSetup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** > **Forwarding Profiles Setup (Configuración de perfiles de reenvío)** > **Destinations (Destinos)**.

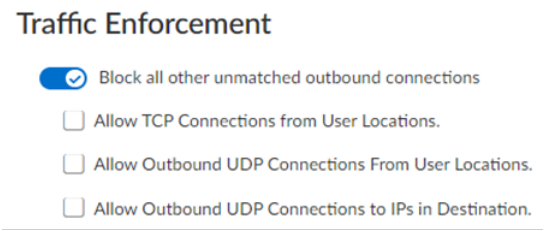
©2025 Palo Alto Networks, Inc.

Conectividad	**Direct (Directo)** hace que el tráfico pase por alto el proxy. **Global Proxy (Proxy global)** hace que el tráfico pase a través del proxy.

3. Seleccione **Add (Añadir)** cuando termine.
4. Habilite la **Traffic Enforcement (Instauración de tráfico)** si desea bloquear todo el tráfico saliente (como UDP) que no coincida con las reglas de reenvío. Esta opción requiere la versión 6.3.1 del agente GlobalProtect y está deshabilitada de forma predeterminada. Si tiene aplicaciones que necesitan que permita conexiones UDP, puede añadir estas excepciones utilizando objetos de **Ubicación de usuario** o **Destino**.

   Puede personalizar sus acciones de bloque de la siguiente manera:

   - Bloquee todas las conexiones salientes UDP desde los endpoints.
   - Permitir TCP de ubicaciones específicas. Por ejemplo, puede permitir todo el tráfico TCP desde su oficina.
   - Permitir UDP de ubicaciones específicas. Por ejemplo, puede permitir todo el tráfico TCP desde su oficina.
   - Si algunas aplicaciones necesitan conexiones UDP, puede permitir conexiones UDP salientes a destinos específicos.

5. Seleccione **Save (Guardar)** para guardar el perfil con la regla de reenvío que creó.

   El perfil aparece en la lista de Perfiles de reenvío. Al abrirlo, verá una URL del archivo PAC generado a partir de la regla. **View PAC file (Ver archivo PAC)** para ver su contenido.

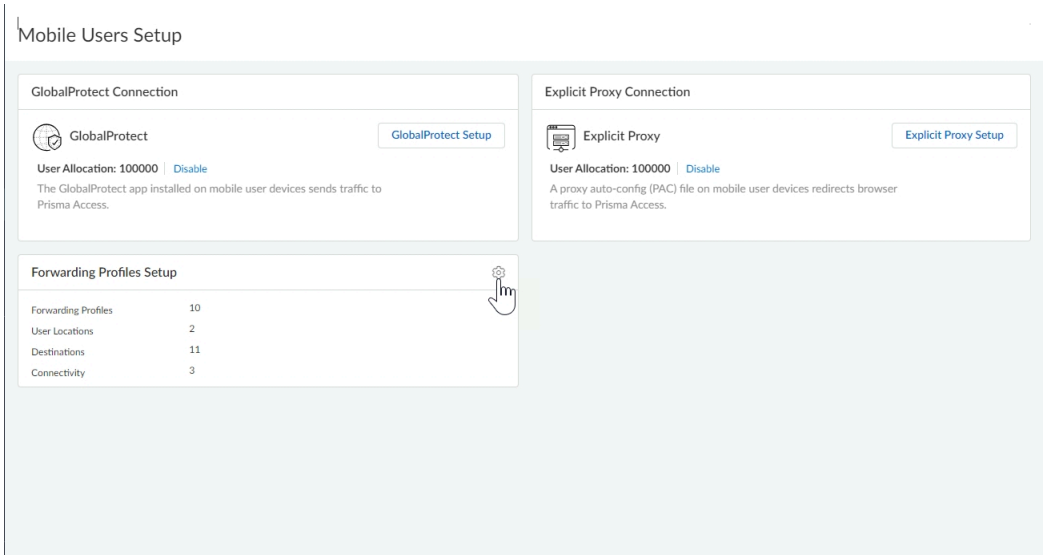
Adjuntar perfiles de reenvío a la configuración de aplicaciones de GlobalProtect

Puede utilizar Perfiles de reenvío para simplificar la configuración de su proxy de aplicación de GlobalProtect.

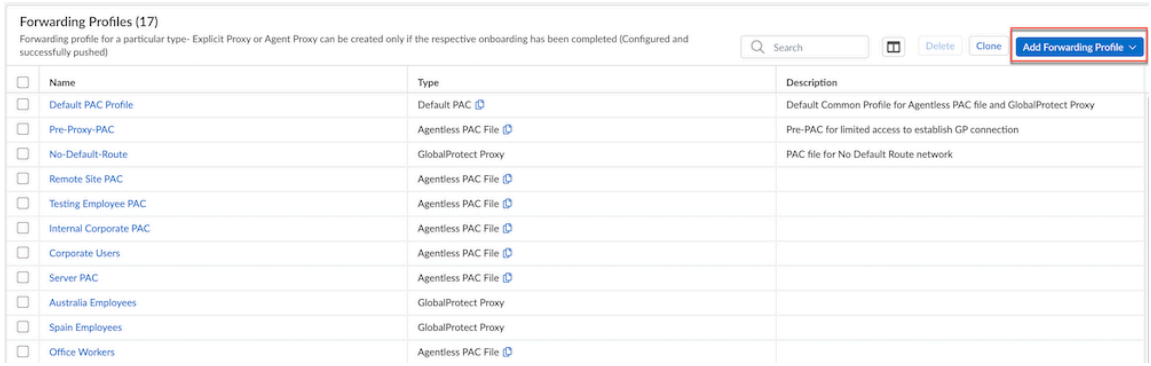
©2025 Palo Alto Networks, Inc.

STEP 1 | Cree un perfil de reenvío de logs.

1. De Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** > **Forwarding Profiles Setup (Configuración de perfiles de reenvío)**.



2. **Add Forwarding Profile (Añadir perfil de reenvío)**.



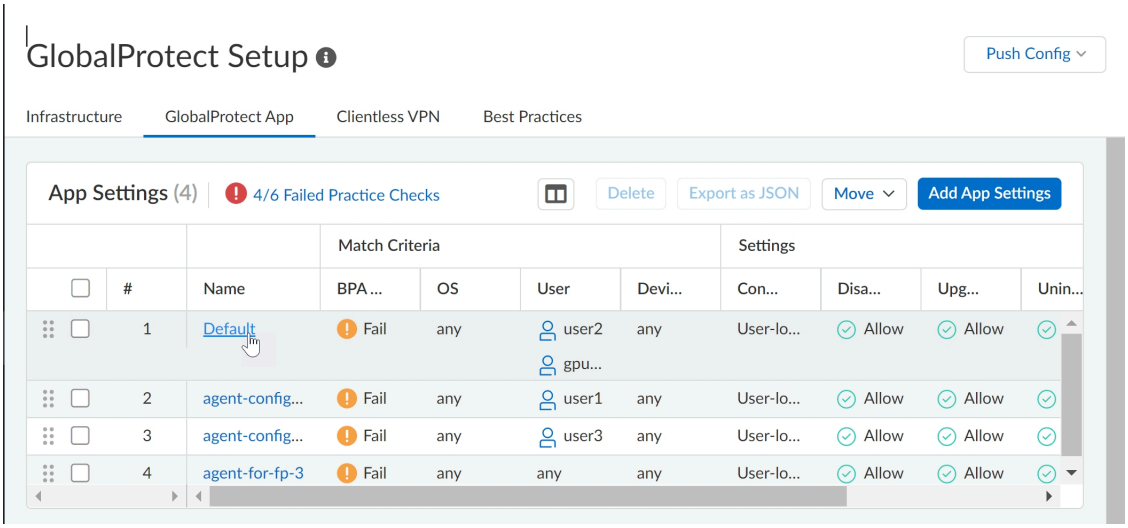
STEP 2 | Seleccione **Proxy de GlobalProtect**.

STEP 3 | Para configurar el perfil de reenvío, cargue un archivo PAC o cree reglas de reenvío.

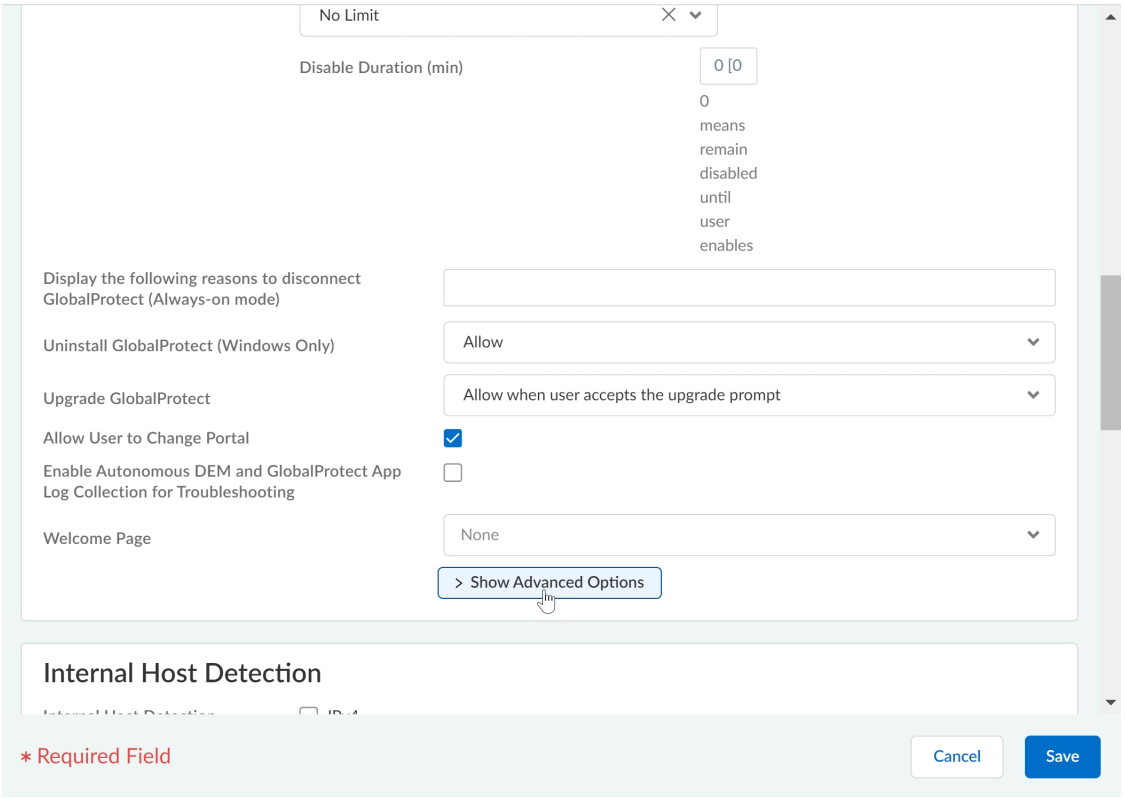
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Añada el perfil de reenvío a la configuración del proxy de GlobalProtect app.

1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Aplicación de GlobalProtect)**.
2. Seleccione un archivo de configuración.



3. En Configuración de aplicaciones, **Show Advanced Options (Mostrar opciones avanzadas)**.

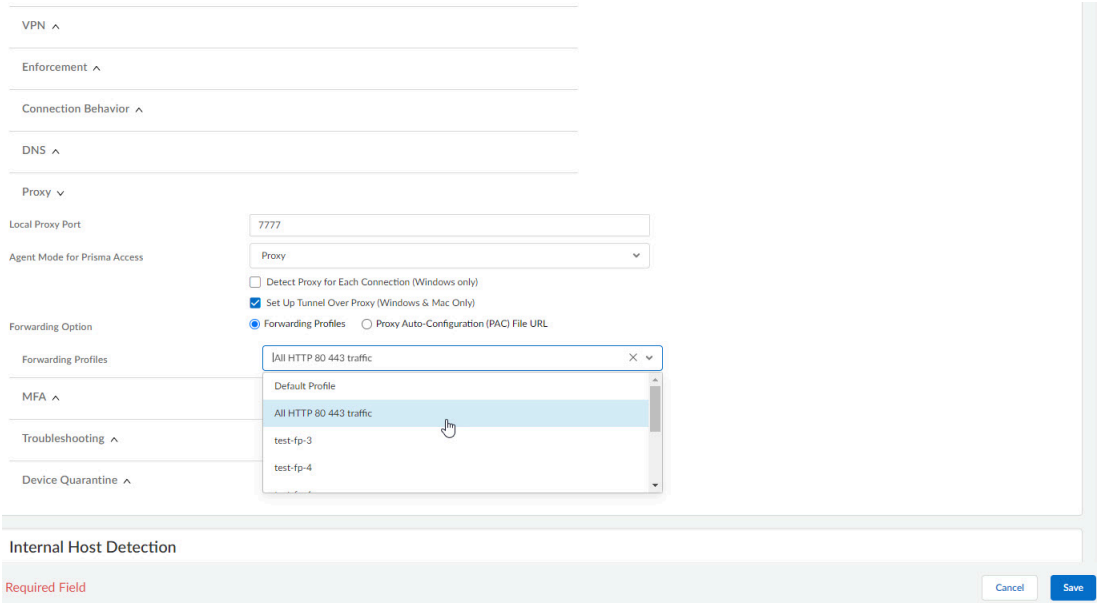


4. Expanda la configuración de **Proxy**.
5. Seleccione el **Proxy** o el **Tunnel and Proxy (Túnel y proxy)** según su modo de agente de GlobalProtect

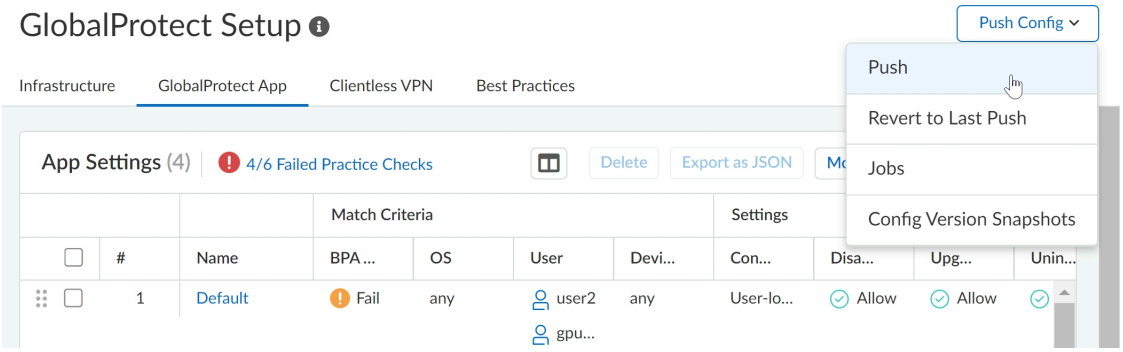
 ©2025 Palo Alto Networks, Inc.

*No puede añadir un perfil de reenvío si selecciona el modo **Tunnel (Túnel)**.*

6. Seleccione **Forwarding Profiles (Perfiles de reenvío)** y elija el Perfil de reenvío que desea utilizar.



7. Haga clic en **Save (Guardar)** para guardar sus cambios.
8. Seleccione **Push Config (Enviar configuración)** > **Push (Enviar)**.



Directrices del archivo PAC

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

Directrices para el archivo PAC (Strata Cloud Manager)

Use las siguientes directrices y requisitos al configurar el archivo PAC para usarlo con el Proxy explícito:

- Tenga en cuenta que si está utilizando el Agente de GlobalProtect en modo Proxy, el agente distribuirá el archivo PAC a sus hosts. El agente accede al archivo PAC a través de HTTPS. El archivo PAC es público.
- Los archivos PAC dirigen el tráfico de usuarios al proxy explícito.
- Solo puede alojar un archivo PAC para su uso con Prisma Access y el archivo PAC de proxy explícito se hospeda en Estados Unidos. Si necesita un acceso alternativo a archivos PAC fuera de los Estados Unidos, puede alojar el archivo PAC en su empresa.
- Para acceder al archivo PAC, asegúrese de que los endpoints puedan acceder a las siguientes direcciones IP:
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

  Si tiene una red de ruta no predeterminada, debe añadir rutas para que estas direcciones IP accedan al archivo PAC.
- Solo se admite el formato de texto ASCII para los archivos PAC. Palo Alto Networks recomienda crear y guardar el archivo PAC en un editor de texto como VI o Vim.
- Después de crear la configuración de proxy explícito y confirmar y enviar los cambios, cargue el archivo PAC o especifique la configuración de PAC en el editor de archivos PAC.
- Debe tener al menos una URL de proxy explícito en la `declaración "PROXY foo.proxy.prismaaccess.com:8080";` de vuelta que comienza para el tráfico que entra en Prisma Access Utilice un dominio configurado que se utilice al enviar los cambios o utilice una dirección IPv4 válida o una palabra clave DIRECT, como `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` o `PROXY 1.2.3.4:8080`, etc.
- Si no se omite el proxy, debe proporcionar una palabra clave PROXY. Se requiere una instrucción de proxy válida si no se ha configurado ninguna palabra clave `DIRECT` para la derivación de proxy.
- Si se encuentra una instrucción PROXY válida antes de una instrucción PROXY no válida, el Proxy explícito omite la verificación de validez en todas las instrucciones PROXY después de la primera. Por ejemplo, un archivo PAC con la instrucción válida `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` seguida de la instrucción `PROXY no válida foo.proxy.prismaacess.com:8080` se consideraría válido ya que el proxy explícito omite la comprobación de validez de `foo.proxy.prismaacess.com:8080`.
- Si está utilizando una instrucción PROXY para que el tráfico ACS omita el proxy de Prisma Access, la instrucción PROXY no debe usar la URL de proxy explícito. En esta configuración, el proxy explícito proporciona un mensaje de error, pero le permite cargar el archivo PAC.

©2025 Palo Alto Networks, Inc.

Puede dirigir el tráfico de ACS a otros servidores proxy mediante un FQDN o una dirección IPv4 válidos, o directamente a Internet, mediante la palabra clave `DIRECT`.

- Solo se admiten direcciones IPv4 en las instrucciones PROXY. No utilice direcciones IPv6 en las declaraciones de PROXY.
- El tamaño máximo de un archivo PAC es de 750 KB.
- Si el tráfico de ACS/IdP necesita pasar por el proxy explícito, añada esos dominios a una lista de omisión de autenticación y una Regla de política Sin descifrado.
- Si configura el proxy explícito en un entorno de ruta predeterminado, debe excluir los FQDN del portal, la puerta de enlace y SAML. Puede usar el archivo PAC para omitir los FQDN.
- No es posible eliminar un archivo PAC después de haberlo cargado. Sin embargo, puede cargar un nuevo archivo PAC o editarlo en el editor de archivos PAC para sobrescribir el existente.

Proxy explícito proporciona un archivo PAC de ejemplo que puede modificar y usar como archivo PAC para la implementación de proxy explícito. El archivo PAC de ejemplo que Prisma Access proporciona contiene los siguientes datos:

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

Si desea utilizar el archivo PAC predeterminado que Prisma Access proporciona, opcionalmente puede modificar los campos del archivo PAC como se describe en la tabla siguiente.

Texto	Descripción
`var resolved_ip = dnsResolve(host); ... return "DIRECT";`	Si no modifica los datos de este archivo, los siguientes nombres de host y direcciones IP omiten el proxy explícito: • `if (isPlainHostName(host)`: omite el proxy explícito para los nombres de host que no contienen puntos (por ejemplo, http://intranet). • `shExpMatch(host, "*.local") ||`: omite el proxy para cualquier nombre de host que esté alojado en la red interna (localhost). • `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip,`

 ©2025 Palo Alto Networks, Inc.

Texto	Descripción
	`"172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`: omite el proxy explícito para cualquier dirección IP que se encuentre en el rango de direcciones IP privadas o de bucle invertido.
`if (url.substring(0,4) == "ftp:" ) return "DIRECT";`	Omite el proxy explícito para las sesiones FTP.
`if (shExpMatch(host, "*.okta.com ") || shExpMatch(host, "*.oktacd n.com")) return "DIRECT";`	Omite el proxy explícito para el IdP de SAML. Asegúrese de añadir todos los FQDN utilizados por el IdP. Si utiliza Okta como el IdP utilizado para la autenticación SAML, introduzca **`*.okta.com`** y **`*.oktacdn.com`**.
`if (shExpMatch(host, "*.acs.pri smaaccess.com")) return "DIRECT ";`	Omite el proxy explícito para el Servicio de caché de autenticación (ACS) de Prisma Access. En lugar de usar un comodín, puede añadir el **ACS FQDN** para su implementación. Encuentre este FQDN en **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** > **ACS FQDN**.
`return "PROXY foo.proxy.prismaac cess.com:8080"`	Omite el proxy explícito para la dirección URL del proxy explícito. Debe tener al menos una URL de proxy explícito en la `declaración "PROXY foo.proxy.prismaaccess.com:8080";` de vuelta para el tráfico que entra en Prisma Access Utilice un dominio configurado que se utilice al enviar los cambios o utilice una dirección IPv4 válida o una palabra clave DIRECT, como `PROXY paloaltonetworks-245139.proxy.prismaaccess.c` o `PROXY 1.2.3.4:8080`.

©2025 Palo Alto Networks, Inc.

Directrices para el archivo PAC (Panorama)

Use las siguientes directrices y requisitos al configurar el archivo PAC para usarlo con el Proxy explícito:

- Tenga en cuenta que si está utilizando el Agente de GlobalProtect en modo Proxy, el agente distribuirá el archivo PAC a sus hosts. El agente accede al archivo PAC a través de HTTPS. El archivo PAC es público.
- Los archivos PAC dirigen el tráfico de usuarios al proxy explícito.
- Solo puede alojar un archivo PAC para su uso con Prisma Access y el archivo PAC de proxy explícito se hospeda en Estados Unidos. Si necesita un acceso alternativo a archivos PAC fuera de los Estados Unidos, puede alojar el archivo PAC en su empresa.
- Para acceder al archivo PAC, asegúrese de que los endpoints puedan acceder a las siguientes direcciones IP:
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36
- Solo se admite el formato de texto ASCII para los archivos PAC. Palo Alto Networks recomienda crear y guardar el archivo PAC en un editor de texto como VI o Vim.
- Cargue el archivo PAC después de crear la configuración de proxy explícito y confirmar y enviar los cambios. Después de cargar el archivo PAC, no se requiere una operación de confirmación y envío.
- Debe tener al menos una URL de proxy explícito en la `declaración "PROXY foo.proxy.prismaaccess.com:8080";` de vuelta que comienza para el tráfico que entra en Prisma Access Utilice un dominio configurado que se utilice al enviar los cambios o utilice una dirección IPv4 válida o una palabra clave DIRECT, como `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` o `PROXY 1.2.3.4:8080`, etc.
- Si no se omite el proxy, debe proporcionar una palabra clave PROXY. Se requiere una instrucción de proxy válida si no se ha configurado ninguna palabra clave `DIRECT` para la derivación de proxy.
- Si se encuentra una instrucción PROXY válida antes de una instrucción PROXY no válida, el Proxy explícito omite la verificación de validez en todas las instrucciones PROXY después de la primera. Por ejemplo, un archivo PAC con la instrucción válida `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` seguida de la instrucción `PROXY no válida foo.proxy.prismaacess.com:8080` se consideraría válido ya que el proxy explícito omite la comprobación de validez de `foo.proxy.prismaacess.com:8080`.
- Si está utilizando una instrucción PROXY para que el tráfico ACS omita el proxy de Prisma Access, la instrucción PROXY no debe usar la URL de proxy explícito. En esta configuración, el proxy explícito proporciona un mensaje de error, pero le permite cargar el archivo PAC. Puede dirigir el tráfico de ACS a otros servidores proxy mediante un FQDN o una dirección IPv4 válidos, o directamente a Internet, mediante la palabra clave `DIRECT`.

 ©2025 Palo Alto Networks, Inc.

- Solo se admiten direcciones IPv4 en las instrucciones PROXY. No utilice direcciones IPv6 en las declaraciones de PROXY.
- El tamaño máximo de un archivo PAC es de 256 KB.
- Si el tráfico de ACS/IdP necesita pasar por el proxy explícito, añada esos dominios a una lista de omisión de autenticación y una Regla de política Sin descifrado.
- Si configura el proxy explícito en un entorno de ruta predeterminado, debe excluir los FQDN del portal, la puerta de enlace y SAML. Puede usar el archivo PAC para omitir los FQDN.
- No es posible eliminar un archivo PAC después de haberlo cargado. Sin embargo, puede cargar un nuevo archivo PAC para sobrescribir el existente.
- Si cambia la URL de Proxy explícito en Prisma Access pero no cambia el archivo PAC para reflejar el cambio, el cambio no se aplicará. Debe cargar un nuevo archivo PAC especificando la nueva URL de proxy explícito.

Proxy explícito proporciona un archivo PAC de ejemplo que puede modificar y usar como archivo PAC para la implementación de proxy explícito. El archivo PAC de ejemplo que Prisma Access proporciona contiene los siguientes datos:

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

Si desea utilizar el archivo PAC predeterminado que Prisma Access proporciona, opcionalmente puede modificar los campos del archivo PAC como se describe en la tabla siguiente.

Texto	Descripción
`var resolved_ip = dnsResolve(host); ... return "DIRECT";`	Si no modifica los datos de este archivo, los siguientes nombres de host y direcciones IP omiten el proxy explícito: • `if (isPlainHostName(host)`: omite el proxy explícito para los nombres de host que no contienen puntos (por ejemplo, http://intranet). • `shExpMatch(host, "*.local") ||`: omite el proxy para cualquier nombre de host que esté alojado en la red interna (localhost). • `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0")`

 ©2025 Palo Alto Networks, Inc.

Texto	Descripción
	`|| isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`: omite el proxy explícito para cualquier dirección IP que se encuentre en el rango de direcciones IP privadas o de bucle invertido.
`if (url.substring(0,4) == "ftp:" ) return "DIRECT";`	Omite el proxy explícito para las sesiones FTP.
`if (shExpMatch(host, "*.okta.com") || shExpMatch(host, "*.oktacdn.com")) return "DIRECT";`	Omite el proxy explícito para el IdP de SAML. Asegúrese de añadir todos los FQDN utilizados por el IdP. Si utiliza Okta como el IdP utilizado para la autenticación SAML, introduzca **`*.okta.com`** y **`*.oktacdn.com`**.
`if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";`	Omite el proxy explícito para el Servicio de caché de autenticación (ACS) de Prisma Access. En lugar de usar un comodín, puede añadir el **ACS FQDN** para su implementación. Encuentre este FQDN en **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** > **ACS FQDN**.
`return "PROXY foo.proxy.prismaaccess.com:8080"`	Omite el proxy explícito para la dirección URL del proxy explícito. Debe tener al menos una URL de proxy explícito en la `declaración "PROXY foo.proxy.prismaaccess.com:8080";` de vuelta para el tráfico que entra en Prisma Access Utilice un dominio configurado que se utilice al enviar los cambios o utilice una dirección IPv4 válida o una palabra clave DIRECT, como `PROXY paloaltonetworks-245139.proxy.prismaaccess.c` o `PROXY 1.2.3.4:8080`.

©2025 Palo Alto Networks, Inc.

Prácticas recomendadas para Proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Utilice las Prácticas recomendadas al implementar su implementación de Proxy explícito para un rendimiento óptimo y una experiencia de usuario ideal:

- **Prácticas recomendadas generales para el implementación de Proxy explícita**:
  - Implemente Proxy explícito en al menos dos regiones para obtener redundancia.
  - Si todos sus usuarios están detrás de un dispositivo NAT y si el Proxy explícito ve la dirección IP del dispositivo NAT como la dirección IP de origen, debería asignar una dirección IP de NAT por cada 500 usuarios móviles.
  - Utiliceperfiles de reenvío para configurar un archivo PAC.
- **Prácticas recomendadas para archivos PAC**: al configurar el archivo PAC, omita todas las URL de SAML, CIE y el Servicio de caché de autenticación (ACS).
- **Prácticas recomendadas de Autenticación SAML**:
  - Establezca la **vida útil de la cookie** de autenticación SAML en 24 horas para tener la mejor experiencia del usuario sin interrupciones en la autenticación.
  - Si ha configurado GlobalProtect en modo proxy o GlobalProtect en modo túnel y proxy, establezca la **Cookie Lifetime (Vida útil de la Cookie)** en el portal de GlobalProtect en 12 horas.
- **Prácticas recomendadas de Autenticación Kerberos**: el archivo keytab debe ser de menos de 60 KB.
- **Prácticas recomendadas de reglas de políticas de seguridad**: utilice las prácticas recomendadas de reglas de políticas de seguridad estableciendo la **Action (Acción)** en las políticas en **Deny (Denegar)** en lugar de **Drop (Descartar)** o **Reset (Restablecer)**. Esta acción ayuda a liberar los recursos rápidamente dentro del Nodo de procesamiento de seguridad de proxy explícito (EP-SPN) para un rendimiento óptimo.
- **Prácticas recomendadas de descifrado**: configure al menos una política de descifrado y un certificado de descifrado.
- **Prácticas recomendadas para la dirección IP de origen**: para restringir el acceso a Proxy explícito, a direcciones IP de origen específicas, utilice objetos especiales que incluyen Objetos de dirección, Grupos de dirección y Listas dinámicas externas (EDLs).

Supervisar y solucionar problemas de proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	• Licencia de Prisma Access

©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	

Aprenda a supervisar y solucionar problemas de su implementación de Proxy explícito de Prisma Access.

- Strata Cloud Manager
- Panorama

Supervisar y solucionar problemas de proxy explícito (Strata Cloud Manager)

Supervise los detalles de implementación del proxy explícito de Prisma Access para ayudarle a solucionar cualquier problema.

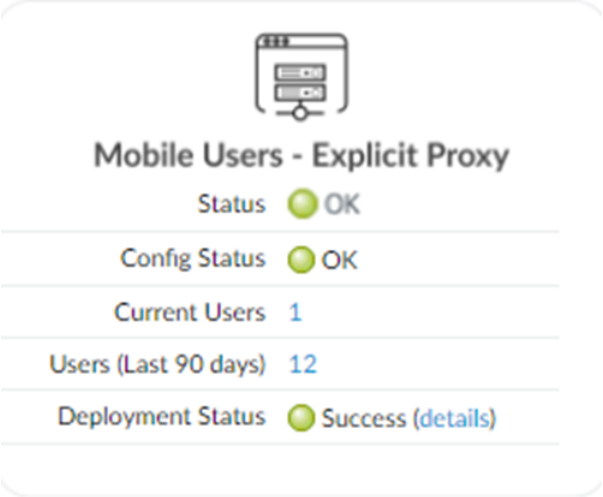
- Haga clic en **Monitor (Supervisar)** > **Users (Usuarios)** y seleccione Método de conexión de **Explicit Proxy (Proxy explícito)**.
- Seleccione **Monitor (Supervisar)** > **Users (Usuarios)** y seleccione el método de conexión como **Explicit Proxy (Proxy explícito)** para ver los usuarios móviles que se conectan a los servicios de seguridad de Prisma Access a través de proxy explícito en un navegador web en sus dispositivos
- Seleccione **Monitor (Supervisar) > Prisma Access locations (Ubicaciones de Prisma Access) > Explicit Proxy Mobile Users (Usuarios móviles de proxy explícito)** para ver una visión general del estado de todas sus ubicaciones de Prisma Access para usuarios móviles.
- Compruebe los logs de tráfico (**Incidentes y Alertas > Visor de logs** y seleccione el tipo de log **Tráfico**) y los logs de autenticación (**Incidentes y Alertas > Visor de logs** y seleccione el tipo de log **Autenticación**) para solucionar problemas relacionados con la autenticación.

Supervisar y solucionar problemas de proxy explícito (Panorama)

Después de haber configurado el Proxy explícito para usuarios móviles, controle el estado y solucione cualquier problema verificando el estado de su implementación de Prisma Access de proxy explícito.

 ©2025 Palo Alto Networks, Inc.

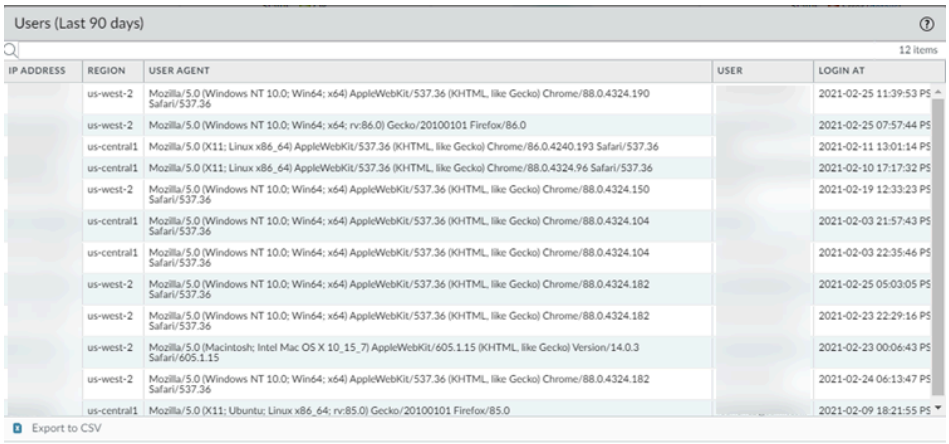
- Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** para ver el estado del Proxy explícito.



Los campos **Status (Estado)** y **Config Status (Estado de configuración)** de los usuarios móviles indican si la conexión entre Prisma Access y sus usuarios móviles está **OK (Aceptar)**, no puede obtener el estado del túnel [**Warning (Advertencia)**], o los usuarios móviles no pueden conectarse al Proxy explícito (**Error**).

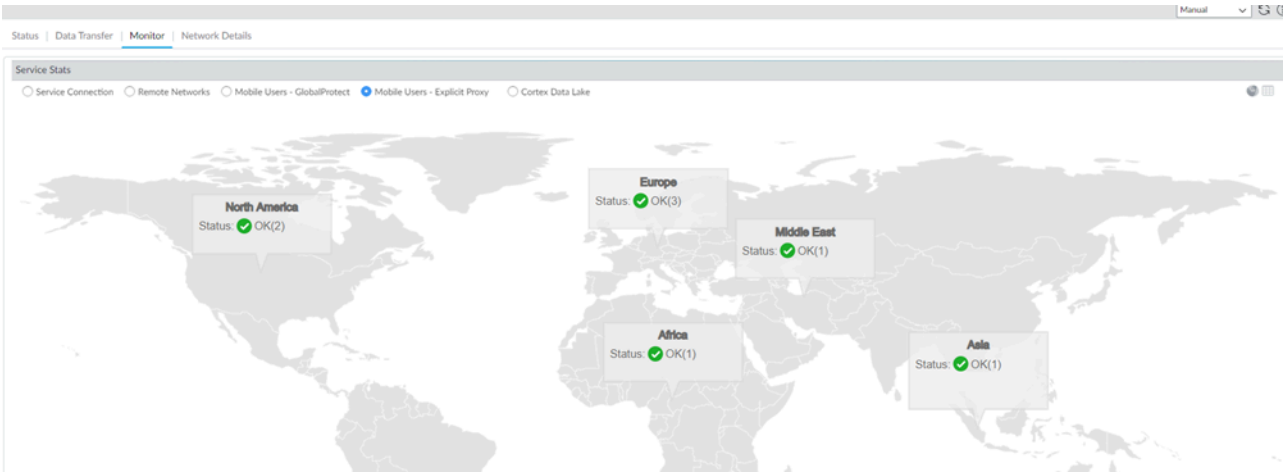
Haga clic en el hipervínculo junto a **Current Users (Usuarios actuales)** y **Users (Last 90 days) [Usuarios (últimos 90 días)]** para obtener más información sobre los usuarios móviles.

- **Current Users (Usuarios actuales)**: el número actual de usuarios autenticados que han navegado por el tráfico en los últimos cinco minutos.
- **Users (Last 90 days) (Usuarios (últimos 90 días)]**: el número de usuarios únicos autenticados de Proxy explícito durante los últimos 90 días.

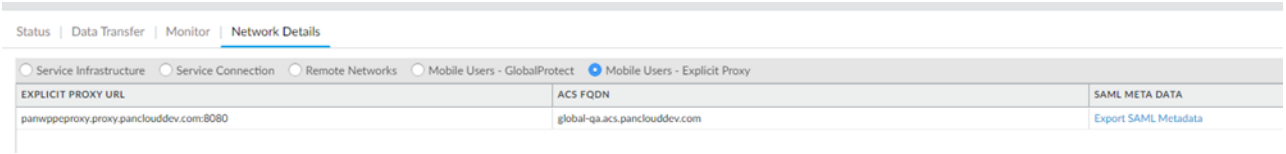


 ©2025 Palo Alto Networks, Inc.

- Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Mobile Users—Explicit Proxy (Mobile Users: Explicit Proxy)** para visualizar un mapa que muestra las ubicaciones de Proxy explícito implementadas.



- Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de red)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** para ver los siguientes detalles:



  - **Explicit Proxy URL (URL de proxy explícito)**: la URL utilizada para el proxy explícito.
  - **ACS FQDN (FQDN de ACS)**: el FQDN del ACS.
  - **SAML Meta Data (Metadatos SAML)**: los metadatos del perfil de autenticación utilizados por SAML. Puede **Export SAML Metadata (Exportar metadatos SAML)** para guardar el archivo de metadatos.
- Para solucionar problemas relacionados con la autenticación, verifique los logs de tráfico [**Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**] y logs de autenticación [**Monitor (Supervisar)** > **Logs** > **Authentication (Autenticación)**]. El proxy explícito muestra las siguientes direcciones IP y ubicaciones en los logs:
  - **Direcciones IP**: si los usuarios móviles omiten el FQDN de ACS en el archivo PAC, la dirección IP que se muestra en la columna **Source (Origen)** en los logs de tráfico y en la columna **IP Address (Dirección IP)** en los logs de autenticación, cuando se visualizan en **Explicit_Proxy_Device_Group**, será la misma que la dirección IP del usuario móvil. Si los usuarios no omiten el FQDN de ACS en el archivo PAC, la dirección IP de origen es la dirección IP pública del cortafuegos en la nube de proxy explícito donde se realizan las redirecciones a ACS.
  - **Ubicaciones**: si los usuarios móviles omiten el FQDN de ACS en el archivo PAC, el nombre de la región que se muestra en la columna **Region (Región)** en **Authentication Logs (Logs de autenticación)**, **Current Users (Usuarios actuales)** y **Users (Last 90 days) [Usuarios (últimos 90 días)]** es una de las cinco regiones (us-west-2, us-east-1, eu-west-2, eu-west-3, ap-south-1) donde está implementado el ACS, y muestra la región donde el proxy explícito está realizando las redirecciones desde el navegador del cliente. Si los usuarios no omiten

 ©2025 Palo Alto Networks, Inc.

el FQDN de ACS en el archivo PAC, el nombre de la región que se muestra en la columna **Region (Región)** en **Authentication Logs (Logs de autenticación)**, **Current Users (Usuarios actuales)** y **Users (Last 90 days) [Usuarios (últimos 90 días)]** es una de las cinco regiones (us-west-2, us-east-1, eu-west-2, eu-west-3, ap-south-1) donde está implementado el ACS, y muestra la región donde el proxy explícito está realizando las redirecciones desde el cortafuegos de Proxy explícito.

Configuración de bloques para proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Licencia de Prisma Access

Para habilitar esta funcionalidad, póngase en contacto con su representante de cuentas o socio de Palo Alto Networks, quien se pondrá en contacto con el equipo de ingeniería de fiabilidad del sitio (SRE) y enviará una solicitud.

Cuando los usuarios acceden a un destino de Internet mediante Proxy explícito, la resolución DNS para el destino de Internet se realiza mediante Proxy explícito. Para bloquear el acceso a un destino de Internet en la etapa de resolución DNS, puede usar la configuración de bloqueo. Puede bloquear en función de las categorías de seguridad de DNS, las categorías de filtrado de URL o las listas dinámicas externas (EDL).

En el caso de los dominios que bloquee, Prisma Access bloquea los dominios y los usuarios reciben una página de bloqueo durante la solicitud HTTP GET (para sitios web no cifrados) o la solicitud HTTP Connect (para sitios web cifrados), lo que significa que los dominios se bloquean durante la solicitud de conexión inicial. Al bloquear el acceso al sitio, se muestra al usuario una página de bloqueo después de guiarlo a través del flujo de autenticación, y el nombre de usuario se captura para posteriores flujos de trabajo forenses y del Centro de operaciones de seguridad (SOC).

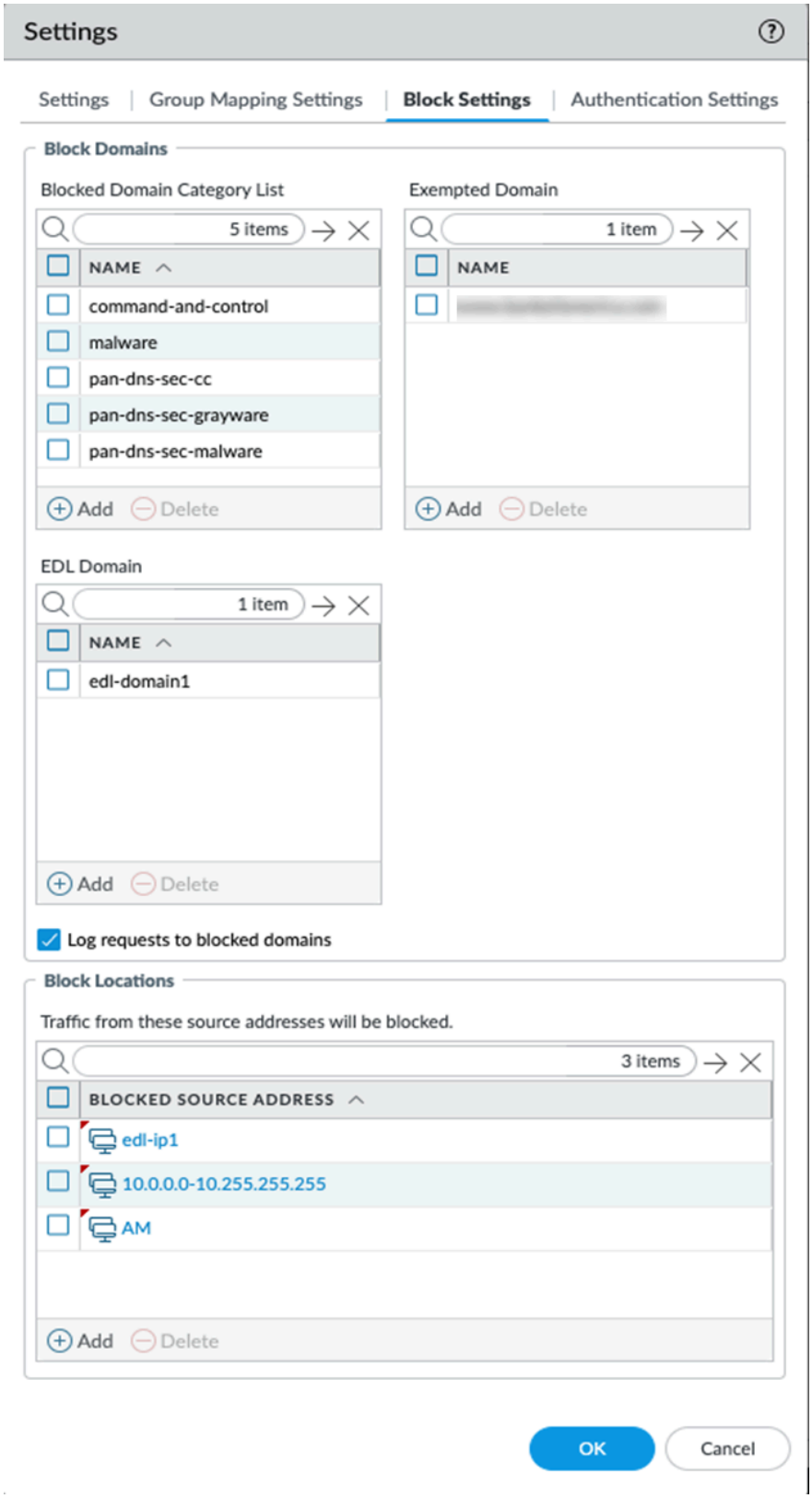
Si está usando Prisma Access (Managed by Strata Cloud Manager), consulte el paso 8 en Configuración de proxy explícito. Para configurar la configuración en bloque de Panorama Manage Prisma Access, complete los siguientes pasos.

STEP 1 | Configure **Block Settings (Configuración de bloques)** para bloquear dominios o categorías de dominios.

Especifique los dominios o las categorías de dominios de los sitios web malintencionados o de los sitios web a los que no desea que accedan los usuarios. Prisma Access evita que los usuarios accedan a las URL y direcciones IP que especifique en esta área cuando los usuarios inician un HTTP GET (para solicitudes no cifradas) o HTTP CONNECT (para solicitudes

 ©2025 Palo Alto Networks, Inc.

cifradas). Los usuarios reciben una página de bloqueo cuando intentan acceder a sitios web bloqueados.



 ©2025 Palo Alto Networks, Inc.

1. En **Blocked Domain Category List (Lista de categorías de dominios bloqueados)**, introduzca las categorías predefinidas para bloquear.

   Categorías de URL personalizadas no son compatibles.
2. En **EDL Domain (Dominio EDL)**, introduzca listas dinámicas externas (EDL) basado en dominios para bloquear.

   Solo puede seleccionar las EDL que tengan un tipo de EDL de **Dynamic Domain Lists (Listas de dominios dinámicos)**; listas de IP dinámicas y listas de URL dinámicas no están permitidas.
3. Si desea eximir a los dominios que se incluyen en un **Blocked Domain Category List (Lista de categorías de dominios bloqueados)**, especifíquelos como un **Exempted Domain (Dominio exento)**.

   Todos los dominios que se introduzcan están exentos de ser bloqueados, incluso si aparecen en una categoría de dominio que haya bloqueado.

   - Puede introducir un máximo de 100 dominios.
   - La longitud máxima del registro de dominio es de 256 caracteres.

STEP 2 | Seleccione las direcciones IP que desea bloquear en el área **Blocked Source Address (Dirección de origen bloqueada)**.

Puede **Add (Añadir)** direcciones, grupos de direcciones, EDL basadas en direcciones IP o direcciones IP basadas en regiones y países.

Utilice las siguientes directrices de direcciones IP:

- Utilice EDL con un **Type (Tipo)** de **IP List (Lista de IP)** o **Predefined IP List (Lista de IP predefinida)** solamente.
- Utilice objetos de dirección con un tipo de **IP Range (Rango de IP)** o **IP Netmask (Máscara de red IP)** solamente.
- Los grupos de direcciones con pertenencia a objetos dinámicos no son compatibles.
- No utilice regiones personalizadas en objetos de dirección IP; en su lugar, utilice regiones predefinidas.

STEP 3 | Seleccione **Log requests to blocked domains (Registrar solicitudes de log a dominios bloqueados)** para que Prisma Access registre las solicitudes de dominio bloqueadas.

Dado que los registros de dominio bloqueados pueden generar un gran número de tráfico de botnets, tenga cuidado al habilitar el registro de logs o utilícelo solo con fines de resolución de problemas. Si restringe el uso del proxy (por ejemplo, si restringe el uso a direcciones IP específicas), es posible que pueda habilitar el registro de logs sin restricciones.

Utilice objetos especiales para restringir el tráfico de Internet proxy explícito a direcciones IP específicas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	• Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	

El proxy explícito le proporciona objetos de dirección especiales, grupos de direcciones y listas dinámicas externas (EDL) para restringir el acceso al proxy explícito a direcciones IP de origen específicas. Cuando crea uno o más de estos objetos especiales utilizando los siguientes nombres exactos, Proxy explícito da permiso a las direcciones IP de origen que usted especifica y bloquea cualquier otra dirección IP:

- **Objeto de dirección**: seleccione **Objects (Objetos)** > **Addresses (Direcciones)** en el Explicit_Proxy_Device_Group y cree un objeto llamado **Dirección de origen permitido de proxy explícito de Palo Alto Networks**.
- **Grupo de direcciones**: seleccione **Objects (Objetos)** > **Address Groups (Grupos de direcciones)** en Explicit_Proxy_Device_Group y cree un objeto llamado **Palo Alto Networks Explicit Proxy Allowed Source Address Group (Grupo de direcciones de origen permitido por proxy explícito de Palo Alto Networks)**.
- **Lista dinámica externa (EDL)**: seleccione **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)** en Explicit_Proxy_Device_Group y cree una EDL denominada **Lista de origen permitido de proxy explícito de Palo Alto Networks** y cree una EDL con un tipo de **Lista de IP**.

Puede especificar direcciones IP como direcciones IP de salida de sucursales.

No se permite el uso de comodines (como *.*) para omitir la autenticación de proxy explícito para una gran cantidad de dominios, a menos que restrinja el tráfico de origen a direcciones IP de origen específicas mediante uno de estos objetos especiales.

Utilice objetos de dirección, grupos de direcciones o EDL de forma separada o conjunta; por ejemplo, puede crear solo un grupo de direcciones sin crear un objeto de dirección o EDL.

Acceda a su centro de datos usando proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ (Para el Conector ZTNA y Colo-Connect) Prisma Access versión 5.2.1 ☐ (Para conexiones de servicio) Prisma Access versión 5.0 ☐ (Para acceso a aplicaciones privadas y de socios) GlobalProtect app versión 6.2 para Windows o macOS

Puede usar conexiones de servicio, Conector ZTNA o colo-connect para acceder a recursos en su centro de datos, como listas dinámicas externas o aplicaciones privadas y asociadas, sin dejar de beneficiarse de una conexión de Proxy explícito.

 ©2025 Palo Alto Networks, Inc.

Las siguientes direcciones IP RFC 6598 no son compatibles con el acceso a aplicaciones privadas a través de proxy explícito a través de conexiones de servicio, Colo-Connect o ZTNA Connector:

- *100.64.0.0/15*
- *100.88.0.0/15*
- *100.72.0.0/15*

Los conectores ZTNA existentes que utilizan estas direcciones IP en los bloques IP de la aplicación del conector ZTNA o los bloques IP del conector no pueden utilizar el navegador de Prisma Access o el agente GlobalProtect en modo proxy a través de proxy explícito. Debe comunicarse con su representante de Palo Alto Networks para migrar sus direcciones IP a un bloque diferente.

- Strata Cloud Manager
- Panorama

Acceda a su centro de datos mediante un proxy explícito (Strata Cloud Manager)

STEP 1 | Configure una conexión de servicio, Colo-Connect o Conector ZTNA en Prisma Access, en función de sus necesidades.

STEP 2 | Configure la configuración DNS.

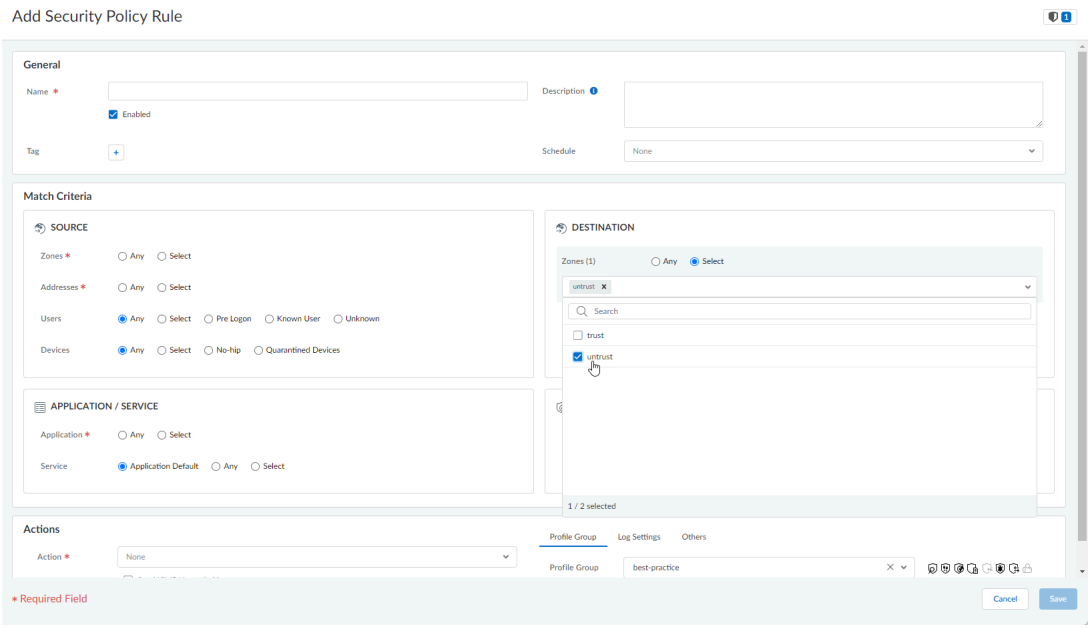
STEP 3 | Asegúrese de que las **zones (zonas)** de **DESTINATION (DESTINO)** para el tráfico con destino a Internet estén configuradas para **untrust (no fiable)** en lugar de **any (ninguna)**.

Si no se realiza este paso, se podría producir un acceso no deseado a su centro de datos.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**, establezca el **Configuration Scope (Alcance de configuración)** en **Prisma Access** > **Mobile Users Container (Contenedor de usuarios móviles)** > **Explicit Proxy (Proxy explicito)**, a continuación, seleccione **Security Policy (Política de seguridad)** > **Security Services (Servicios de seguridad)**.
2. Abra una regla para el tráfico con destino a Internet.

©2025 Palo Alto Networks, Inc.

3. Asegúrese de que las **Zones (Zonas)** en **DESTINATION (DESTINO)** está establecida en **untrust (no fiable)**.



4. Repita todas sus reglas de tráfico en Internet.

STEP 4 | Habilite el acceso a aplicaciones privadas.

- Habilite el acceso a aplicaciones privadas mediante Prisma Access Browser.

  1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Infrastructure Settings (Configuración de infraestructura)** y **Enable (Habilitar)** Prisma Access Browser. En **Proxy URL Settings (Configuración de URL de proxy**, seleccione **Enable Private App Access for Explicit Proxy (Habilitar acceso privado a aplicaciones para proxy explícito)**.

- Habilite el acceso a aplicaciones privadas mediante un navegador normal.

  1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Infrastructure Settings (Configuración de infraestructura)** > **Enable Agent Proxy (Habilitar proxy de agente)** > **Enable Private App Access for Explicit Proxy (Habilitar acceso de aplicación privada para proxy explícito)**.

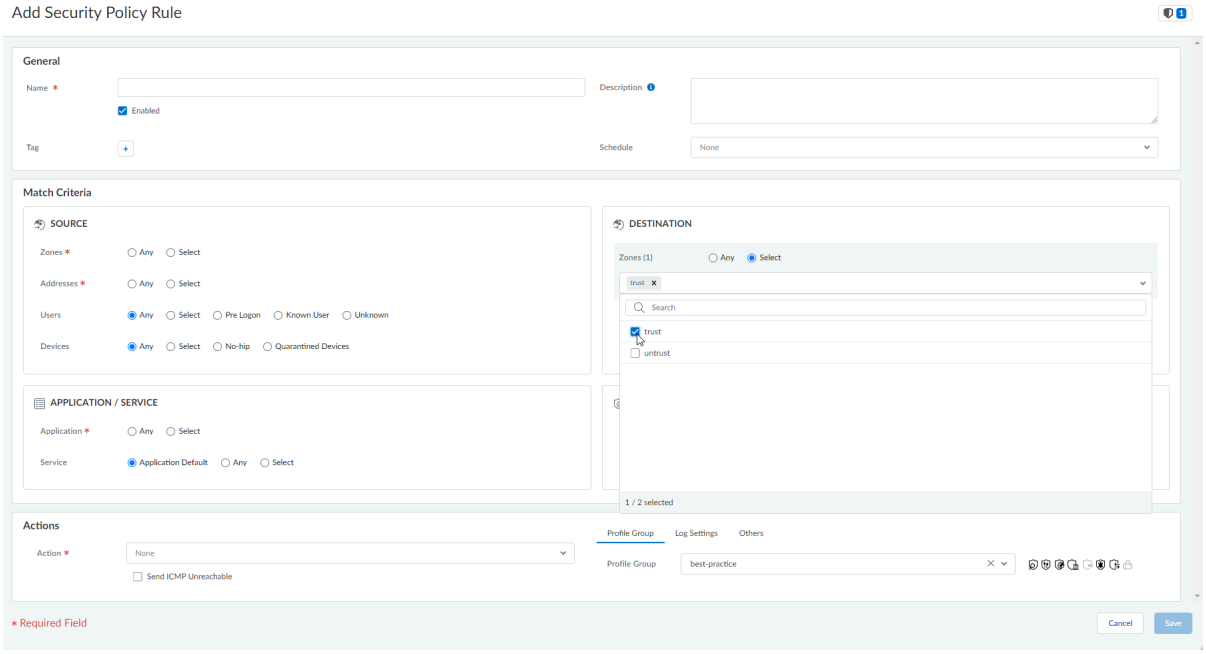
STEP 5 | Cree reglas de política de seguridad para los recursos del centro de datos a los que desea acceder.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**, establezca el **Configuration Scope (Alcance de configuración)** en **Prisma Access** > **Mobile Users Container (Contenedor de usuarios móviles)** > **Explicit Proxy (Proxy explicito)**, a continuación, seleccione **Security Policy (Política de seguridad)** > **Security Services (Servicios de seguridad)**.

 ©2025 Palo Alto Networks, Inc.

2. Cree reglas de políticas de seguridad.

En las reglas para el acceso al centro de datos, asegúrese de que las **Zones (Zonas)** en `DESTINATION (DESTINO)` estén configuradas como **trust (fiable)**.



STEP 6 | Si habilita el acceso a aplicaciones privadas bajo proxy explícito, seleccione **Push Config (Enviar configuración)** para guardar los cambios de configuración después de incorporar el Conector ZTNA.

Acceda a su centro de datos mediante un proxy explícito (Panorama)

STEP 1 | Configure una conexión de servicio, Colo-Connect o Conector ZTNA en Prisma Access, en función de sus necesidades.

STEP 2 | Configure la configuración DNS.

STEP 3 | Configurar asignación de zonas.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users - Explicit Proxy (Usuarios móviles: proxy explícito)** > **Zone Mapping (Asignación de zonas)**
2. Añada las zonas que utilizará para acceder a los recursos de su centro de datos a **Trusted Zones (Zonas de confianza)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Asegúrese de que la `Destination ZONE (ZONA de destino)` en las reglas de política para el tráfico enlazado a Internet, se establece en una zona de no confianza en lugar de `any` (cualquiera).

> *Si no se realiza este paso, se podría producir un acceso no deseado a su centro de datos.*

1. Seleccione **Policies (Políticas)**.
2. Establezca el `Grupo de dispositivos` en **Explicit_Proxy_Device_Group**.
3. Cambie la `Destination ZONE (ZONA de destino)` de `any` (cualquiera) a una de las zonas de no confianza que configuró en un paso anterior.

STEP 5 | Habilite el acceso a aplicaciones privadas.

- Habilite el acceso a aplicaciones privadas mediante Prisma Access Browser.
  1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users - Explicit Proxy (Usuarios móviles: proxy explícito)** > **Settings (Configuración)** > **Advanced (Avanzado)** > **Enable Prisma Access Browser (Habilitar Prisma Access Browser)** > **Enable Private Application Access (Habilitar el acceso a aplicaciones privadas)**

- Habilite el acceso a aplicaciones privadas mediante un navegador normal.
  1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users - Explicit Proxy (Usuarios móviles: proxy explícito)** > **Settings (Configuración)** > **Advanced (Avanzado)** > **Use GlobalProtect Agent to Authenticate (Utilizar agente de GlobalProtect para autenticarse)** > **Enable Private Application Access (Habilitar el acceso a aplicaciones privadas)**

STEP 6 | Cree reglas de política de seguridad para los recursos del centro de datos a los que desea acceder.

1. Seleccione **Policies (Políticas)**.
2. Establezca el `Grupo de dispositivos` en **Explicit_Proxy_Device_Group**.
3. Cree reglas de políticas de seguridad.

   En las reglas para el acceso al centro de datos, asegúrese de utilizar las zona de **Trusted (Confianza)** que configuró en un paso anterior.

Integración de Office 365 basada en aplicaciones con proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de usuario móvil

 ©2025 Palo Alto Networks, Inc.

Aprenda a integrar la versión basada en navegador de Office 365 con Proxy explícito.

- Strata Cloud Manager
- Panorama

Integración de Office 365 basada en aplicaciones con Proxy explícito (Panorama)

Prisma Access Proxy explícito admite la versión basada en navegador de Office 365 (M365), incluyendo Office Online (office.com). Siga estos pasos para integrar la versión basada en navegador de Office 365 con Proxy explícito.

Aunque el Proxy explícito no admite la versión basada en aplicaciones de Office 365, puede seguir estas pautas para usar el Proxy explícito con las políticas basadas en aplicaciones de Office 365.

Configurar la integración de Office 365 basada en navegador con Prisma Access Proxy explícito

Si utiliza la versión basada en navegador de Office 365, complete la siguiente tarea para integrar Office 365 con Proxy explícito.

STEP 1 | (Opcional) si desea utilizar restricciones basadas en inquilinos (restringir el control de acceso a Office 365 solo para un cierto número de inquilinos), utilice la inserción de encabezados HTTP con una categoría de URL personalizada para permitir que inquilinos específicos accedan a Office 365.

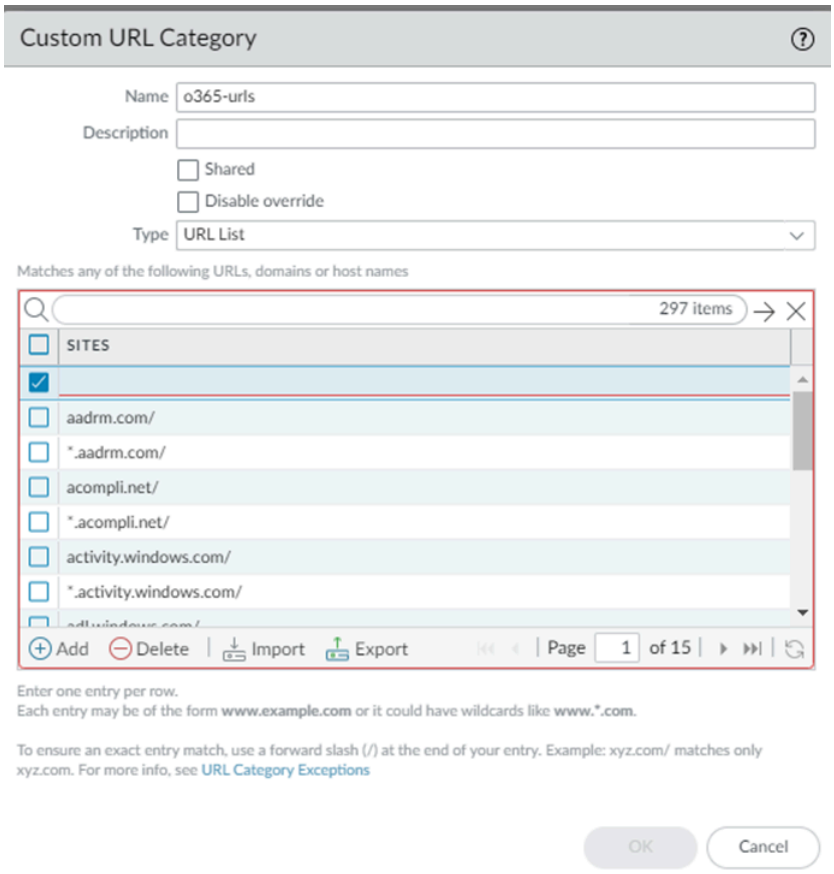
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada políticas de descifrado para las URL que se utilizan para Office 365.

1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría URL personalizada.

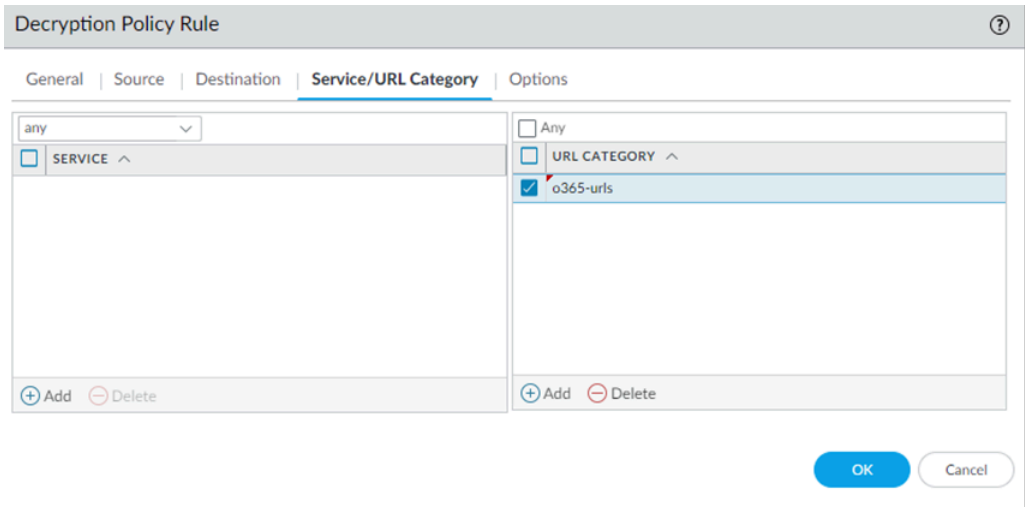
   Asegúrese de que está en el **Explicit_Proxy_Device_Group**.
2. Especifique un **Type (Tipo)** de **URL Lista (Lista de URL)**.
3. Elija **Add (Añadir)** la lista de sitios para habilitar la integración de Office 365.

   Para simplificar la carga de las URL, puede copiar la lista de URL de Office 365 en https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url, guardar esas URL en un archivo e **Import (Importar)** el archivo a la categoría de URL personalizada.



4. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** > **Pre Rules (Reglas previas)** y haga clic en **Add (Añadir)** para añadir una regla de política de seguridad.
5. Especifique la **URL Category (Categoría de URL)** que creó.

 ©2025 Palo Alto Networks, Inc.



6.

STEP 3 | Agregue políticas de descifrado para las capacidades de Protección de Datos y Amenazas, como la Prevención de Pérdida de Datos Empresarial (DLP empresarial), WildFire, Threat Prevention (Prevención de amenazas) o SaaS Security.

STEP 4 | Utilice el Servicio de alojamiento EDL para crear una lista dinámica externa.

STEP 5 |

Configurar la integración de Office 365 basada en aplicaciones con proxy explícito

El Proxy explícito no admite la versión completa basada en cliente (app) de Office 365, porque Office 365 utiliza puertos y protocolos no web y certificados anclados, lo que impide el uso de la descifrado. Si necesita asegurar el tráfico de las aplicaciones cliente de Office 365, puede utilizar una de las siguientes capacidades de Prisma Access para hacerlo:

- Implemente una implementación de Usuarios móviles: GlobalProtect con Proxy explícito y use las opciones de túnel dividido de GlobalProtect para enrutar el tráfico de las aplicaciones de Office 365 al túnel de GlobalProtect, mientras especifica que otro tráfico de internet se envíe al túnel de GlobalProtect, directamente a internet o al Proxy explícito, según su archivo PAC y las opciones de inclusión y exclusión del túnel de GlobalProtect.
- Si su organización requiere que el tráfico destinado a Internet pase a través de un Proxy explícito, o si su red no tiene una ruta predeterminada, puede implementar una Implementación de Red remota con Proxy explícitoImplementación de Red remota con Proxy explícito. En esta implementación, el Proxy explícito le proporciona una lista de direcciones Anycast y unicast, y configura su CPE para enrutar el tráfico a través de esas direcciones hacia la red remota y, desde allí, hacia el Proxy explícito y hacia internet.

  Para usar Office 365 con este tipo de implementación, especifique reglas de archivo PAC para permitir que Office 365 no web pase directamente a Internet.
- Si no puede implementar GlobalProtect o una Red remota de Prisma Access en su entorno, puede configurar el archivo PAC del Proxy explícito para omitir el tráfico de Office 365. Utilice la lista de URL para omitir.

 ©2025 Palo Alto Networks, Inc.

Lista de URL para habilitar la integración de Office 365 con el proxy explícito de Prisma Access

Una opción que puede usar para integrar aplicaciones de Office 365 que no son de navegador con el Proxy explícito es especificar las URL relacionadas con Office 365 y omitir esas URL en el archivo PAC del Proxy explícito. Utilice uno de los siguientes métodos para obtener la lista de URL que se deben omitir:

- Utilice la URL EDL del Servicio de alojamiento EDL de Palo Alto Networks para aplicaciones de Microsoft 365.

  El uso del servicio de alojamiento alivia la carga operativa de asegurar el tráfico hacia sus aplicaciones SaaS al utilizar una URL de fuente como fuente de EDL. Cuando un proveedor de SaaS añade un nuevo endpoint para una aplicación SaaS, la URL de fuente correspondiente se actualiza.

  Para las URL de Microsoft 365 a nivel mundial, utilice la URL https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url. Se proporcionan otras URL para IPv4 e IPv6 y para aplicaciones específicas de países y gubernamentales.
- Recupere la lista de direcciones IP y URL de Office 365 proporcionadas por Microsoft en https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges. Microsoft also provides an Office 365 IP address and URL web service at https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-service.

Configurar el encadenamiento de proxy con Blue Coat Proxy

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access.

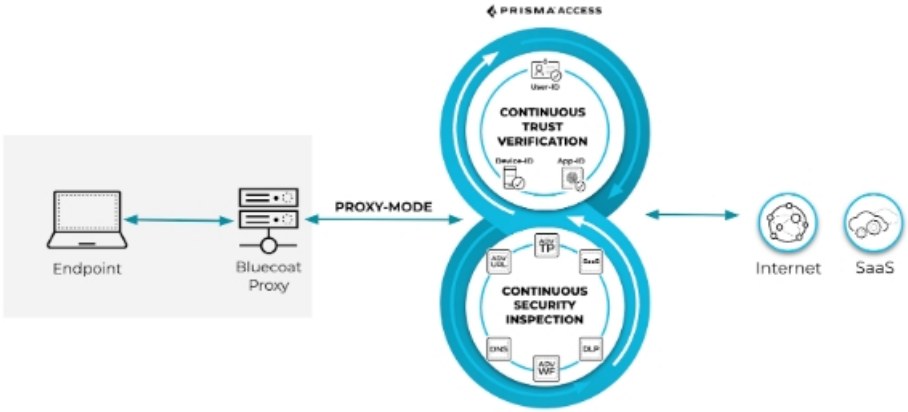
El encadenamiento proxy crea una ruta de Internet multisalto al conectar en cascada varios servidores proxy para una capa adicional de seguridad o para ceñirse al cumplimiento. Cada servidor reenvía su tráfico al siguiente, llegando finalmente a Internet. Esta técnica utiliza la infraestructura de red existente y permite conectarse a un proxy ascendente para una comunicación HTTP y HTTPS segura. La integración preserva la configuración del navegador del usuario al tiempo que mejora la seguridad y el control.

Por qué las empresas utilizan la función de encadenamiento proxy:

1. Privacidad y anonimato mejorados al ofrecer protección multicapa y evitar las restricciones geográficas.
2. Seguridad y control mediante el filtrado de contenido malicioso, spam e intentos de phishing mediante la adición de una capa adicional de seguridad a la experiencia de navegación del usuario.
3. Las empresas pueden utilizar el encadenamiento proxy para hacer cumplir las reglas internas de política restringiendo el acceso a ciertos sitios web o servicios en función de las funciones o ubicaciones de los usuarios.
4. En lugar de implementar un nuevo sistema, el encadenamiento proxy le permite utilizar su infraestructura de red existente conectándose a un servidor proxy ascendente para tareas específicas. Esta puede ser una solución rentable y eficiente.

 ©2025 Palo Alto Networks, Inc.

Obtenga más información sobre cómo funciona Prisma Access Explicit Proxy.



Este es el escenario en el que los clientes desean encadenar el tráfico desde la Blue Coat proxy local al proxy explícito de Prisma Access. La Blue Coat proxy local autentica a los usuarios y pasa el nombre de usuario al proxy explícito de Prisma Access mediante la inserción de encabezados X-Authenticated-User (XAU) en la Blue Coat proxy.

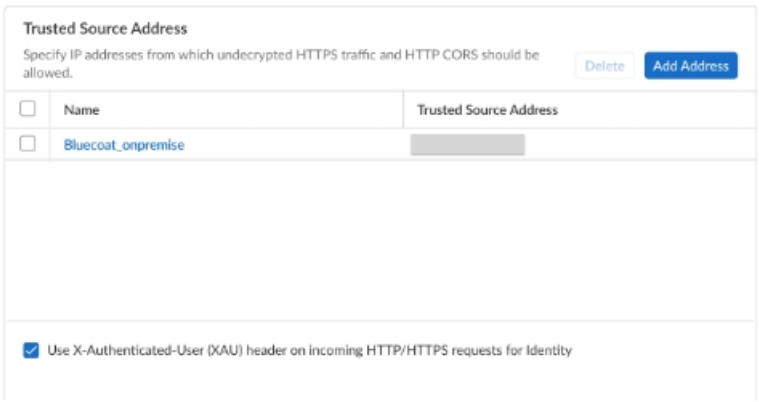
La ruta estática y la NAT de destino para las direcciones IP del proxy explícito son necesarias en redes sin ruta predeterminada.

STEP 1 | Configure Prisma Access.

1. Configurar Proxy explícito.
2. Añadir la proxy explícita de Blue Coat como una dirección de origen fiable.
   1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Advanced Security Settings (Configuración de seguridad avanzada)** > **Add Address (Añadir dirección)**.
   2. Introduzca la dirección IP del proxy explícito Blue Coat.

      Puede añadir direcciones IP o subredes.

   3. Seleccione el **Use X-Authenticated-User (XAU) header on incoming HTTP/HTTPS requests for Identity (Encabezado X-Authenticated-User (XAU) en las solicitudes HTTP/HTTPS entrantes para la identidad)**.

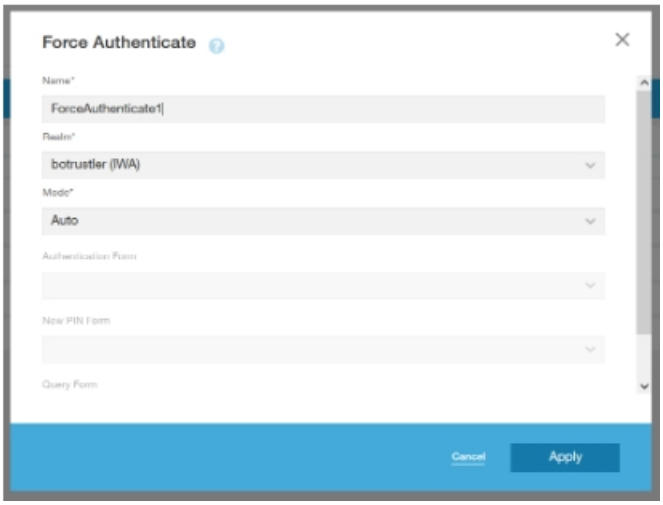


 ©2025 Palo Alto Networks, Inc.

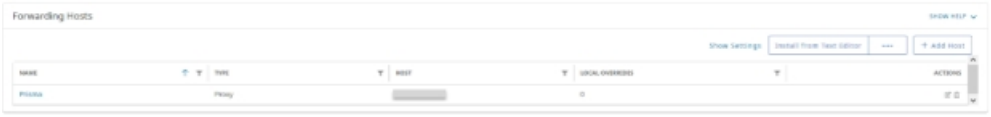
STEP 2 | Realice la configuración en Blue Coat Proxy.

1. Aplicar autenticación.



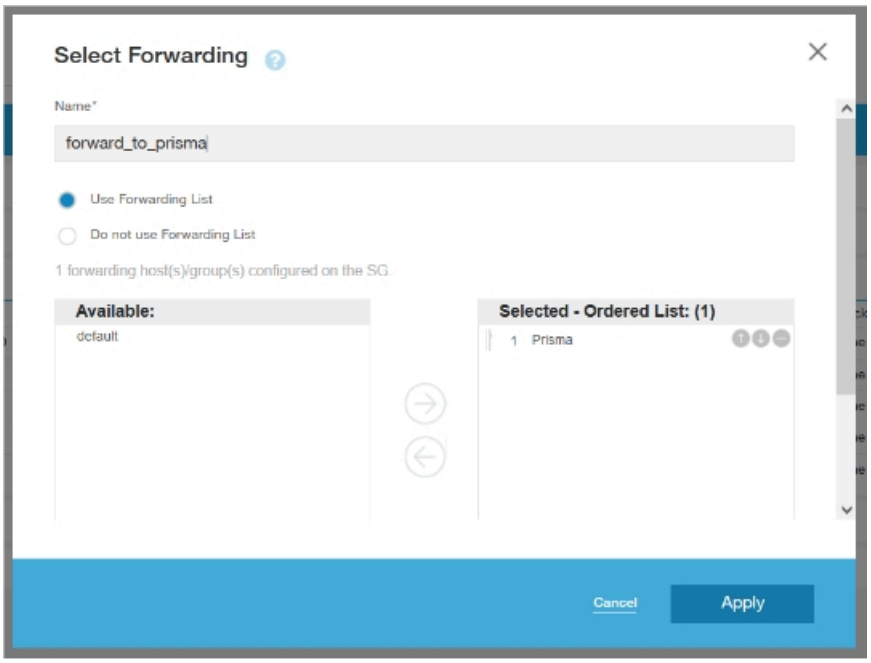


2. Configure la capa de reenvío.



1. Obtener la dirección IP del proxy explícito de Prisma Access.
    1. en Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Infrastructure Settings (Configuración de infraestructura)**.
    2. Copie el FQDN de proxy.

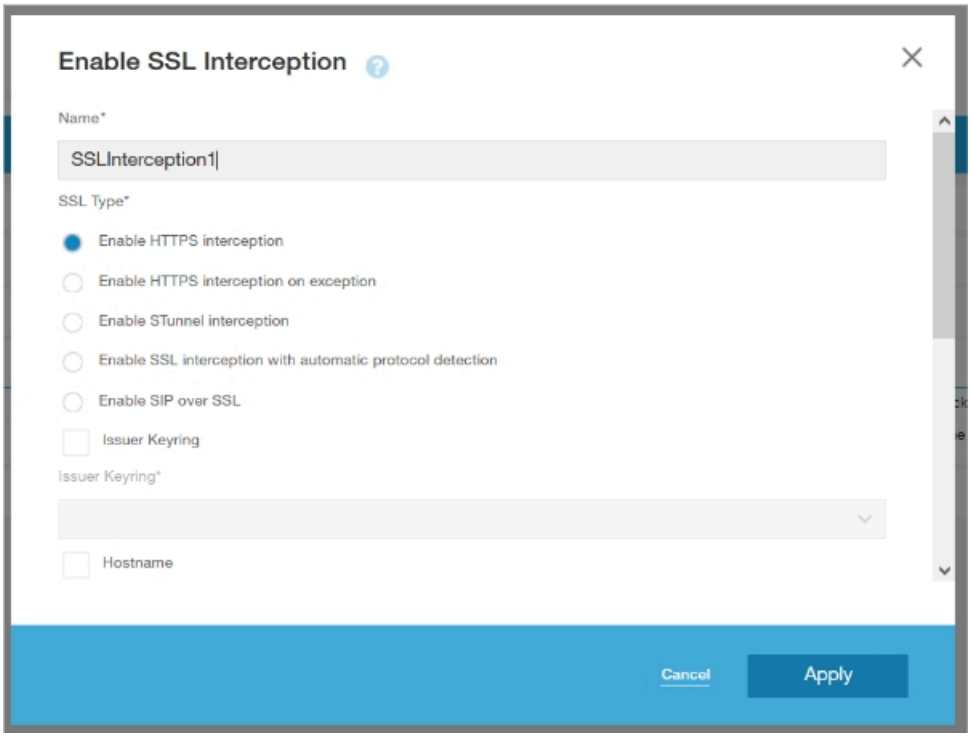
 ©2025 Palo Alto Networks, Inc.





2. Habilite el descifrado HTTPS para la inserción de encabezados.

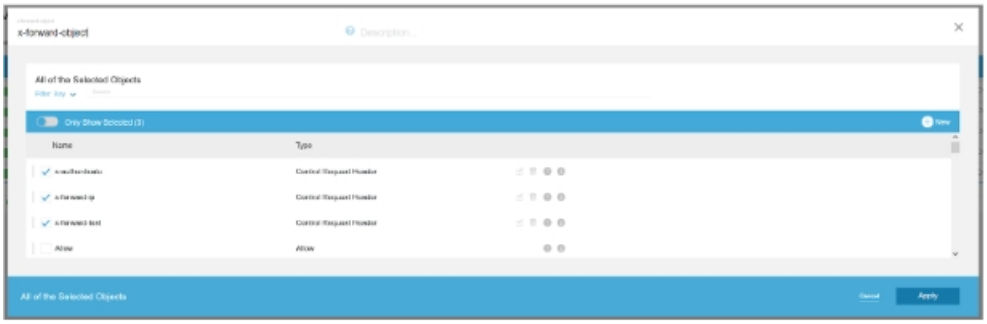
   El descifrado es obligatorio para la inserción del encabezado.

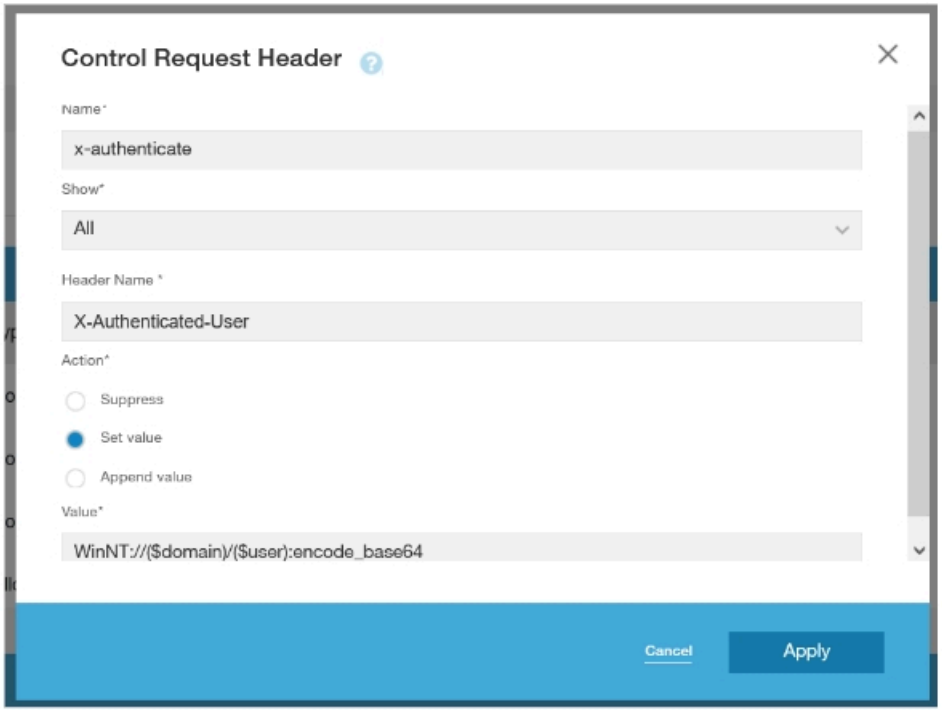


 ©2025 Palo Alto Networks, Inc.

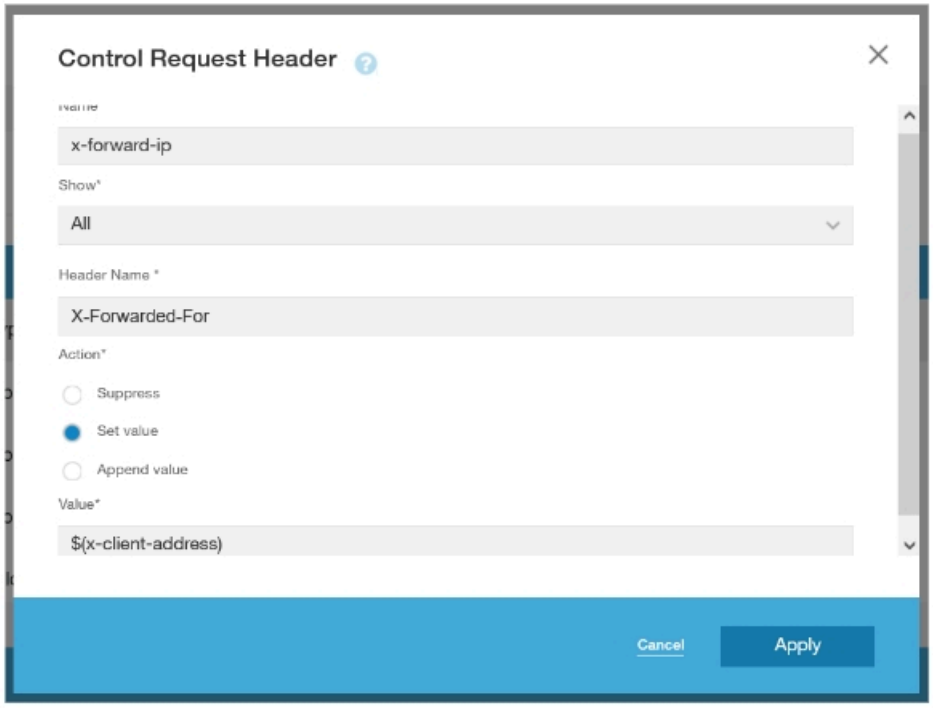


3. Configure el reenvío de encabezados.





 ©2025 Palo Alto Networks, Inc.



La dirección IP del cliente recibida a través del encabezado XFF simplemente se registra y no se puede aprovechar para la política.

4. Establezca la codificación del valor de encabezado en base64:

```
define action Encode_All_XFF set( request.x_header.X-
Authenticated-User, "$(user:encode_base64)" ) end define action
 x-authenticate set( request.x_header.X-Authenticated-User,
 "WinNT://($$domain)/($$user):encode_base64" ) end
```

STEP 3 | Verifique la configuración.

1. En Strata Cloud Manager, seleccione **Incidents and Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**
2. Compruebe las columnas `X-Forwarded-For` y `Usuarios` para verificar que la información de usuario y dirección IP es visible en Prisma Access.

STEP 4 | Considere estos puntos:

1. La Blue Coat proxy requiere autenticación y descifrado para insertar información de encabezado XAU.
2. El valor del encabezado del usuario autenticado X debe estar en formato Base64.
3. Proxy explícito de Prisma Access puede ver la identidad de usuario para el tráfico descifrado.

 ©2025 Palo Alto Networks, Inc.

Utilizar un proxy explícito con GlobalProtect (o una VPN de terceros)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

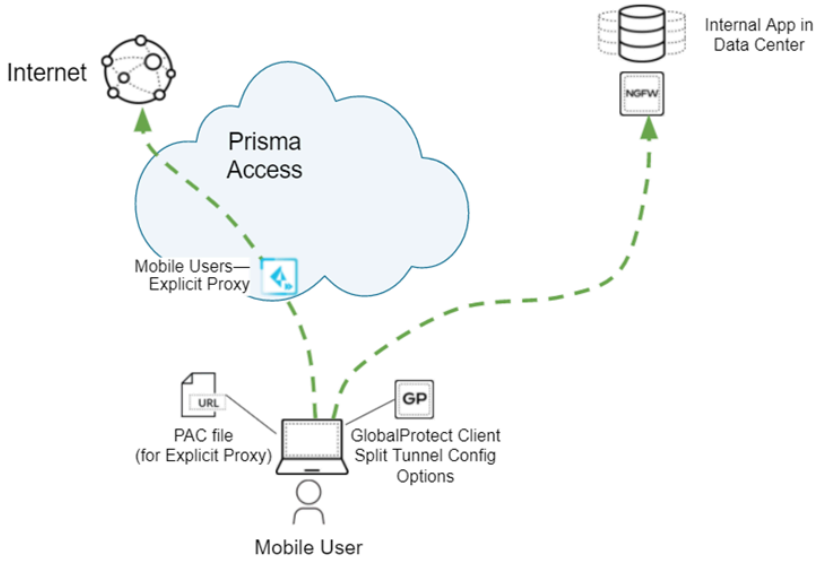
Puede combinar Proxy explícito con GlobalProtect o una VPN de terceros:

- **Proxy explícito y GlobalProtect**
  - Utilice GlobalProtect en modo de túnel dividido para proporcionar acceso seguro solo a aplicaciones privadas.
  - Utilice un proxy explícito para proteger aplicaciones públicas, incluyendo el tráfico de internet y aplicaciones SaaS externas.
- **Proxy explícito y VPN de terceros**

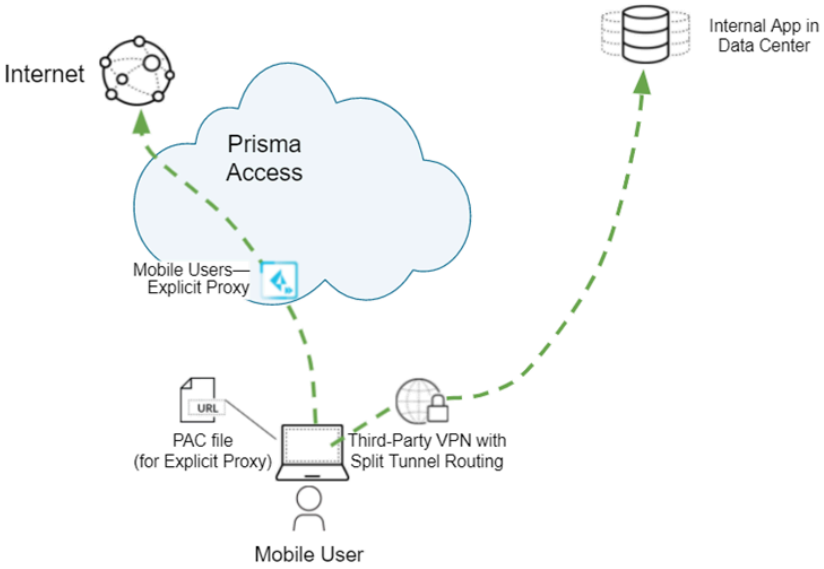
  Si utiliza un cliente VPN para acceder al centro de datos y a aplicaciones privadas, puede seguir usando ese cliente para proteger el acceso a aplicaciones privadas mientras utiliza un proxy explícito y un archivo PAC para proteger el acceso a aplicaciones públicas. Puede implementar Proxy explícito en una ubicación cercana a sus usuarios móviles, lo que elimina la necesidad de enviar tráfico a su centro de datos para la seguridad web.

La siguiente imagen muestra una implementación que utiliza una puerta de enlace GlobalProtect junto con un proxy explícito. GlobalProtect enruta el tráfico mediante el cliente GlobalProtect al cortafuegos de nueva generación de Palo Alto Networks. Para configurar esta implementación, se crea una configuración de túnel dividido en GlobalProtect, lo que permite proteger las aplicaciones privadas con GlobalProtect y las aplicaciones públicas con Proxy explícito. Una vez completada la configuración, los usuarios móviles se conectan a las aplicaciones privadas en el centro de datos de su organización mediante GlobalProtect y se conectan a las aplicaciones privadas basadas en Internet mediante Proxy explícito.

 ©2025 Palo Alto Networks, Inc.



Si tiene una VPN de terceros, puede usarla para conectarse a aplicaciones privadas en el centro de datos, mientras protege las aplicaciones públicas mediante Proxy explícito, como se muestra en la siguiente imagen.



Comenzar:

- Cómo funciona
- Proxy explícito: directrices
- Proxy explícito y GlobalProtect: Configúralo
- Proxy explícito con VPN de terceros

 ©2025 Palo Alto Networks, Inc.

Requisitos para utilizar un proxy explícito con GlobalProtect o una VPN de terceros

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Antes de comenzar su configuración, asegúrese de seguir los requisitos y recomendaciones necesarios para implementar Proxy explícito con GlobalProtect o con una VPN de terceros:

- Para usar Proxy explícito con GlobalProtect, debe implementar GlobalProtect (ya sea una implementación de Usuarios móviles: GlobalProtect o una implementación de GlobalProtect independiente que use puertas de enlace y portales de GlobalProtect).

  Usted configura una configuración de túnel dividido en GlobalProtect. Los ejemplos de esta sección muestran cómo se divide el tráfico según un dominio (URL) o una aplicación; sin embargo, también es posible dividir el tráfico según la ruta de acceso.

  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.
- Para utilizar un proxy explícito con una VPN de terceros, debe implementar la solución VPN.
- Haga una lista de las aplicaciones que desea proteger con la implementación de Usuarios móviles: GlobalProtect o VPN de terceros.

  Por ejemplo, si está configurando Proxy explícito con GlobalProtect, debe configurar GlobalProtect para proteger todo el acceso a aplicaciones o recursos privados, mientras configura el archivo PAC de Proxy explícito para proteger aplicaciones públicas o aplicaciones SaaS. Los ejemplos de configuración en esta sección hacen que GlobalProtect resuelva los dominios internos y que Explicit Proxy resuelva los dominios externos.
- Configure la autenticación para Proxy explícito y GlobalProtect o la VPN de terceros.
  - Para el proxy explícito, debe utilizar la autenticación SAML. Siga las directrices para configurar SAML en una implementación de proxy explícito, incluidas las URL que se utilizarán para el inicio de sesión de SAML.
  - Para implementaciones de Usuarios móviles: GlobalProtect, si usa la autenticación SAML con Okta como proveedor de identidad (IdP), consulte el procedimiento que utiliza para configurar la autenticación SAML con Okta en la Guía de integración de Prisma Access (gestionado por Panorama).
  - Para implementaciones independientes de GlobalProtect, puede configurar la autenticación SAML en PAN-OS.
  - Para una VPN de terceros, consulte la documentación del producto correspondiente a esa VPN.

  Palo Alto Networks recomienda que utilice el navegador predeterminado en el endpoint de cada usuario móvil para la autenticación SAML, de modo que pueda aprovechar el inicio de sesión único (SSO) editando la configuración del portal como se muestra en Configurar Proxy explícito.

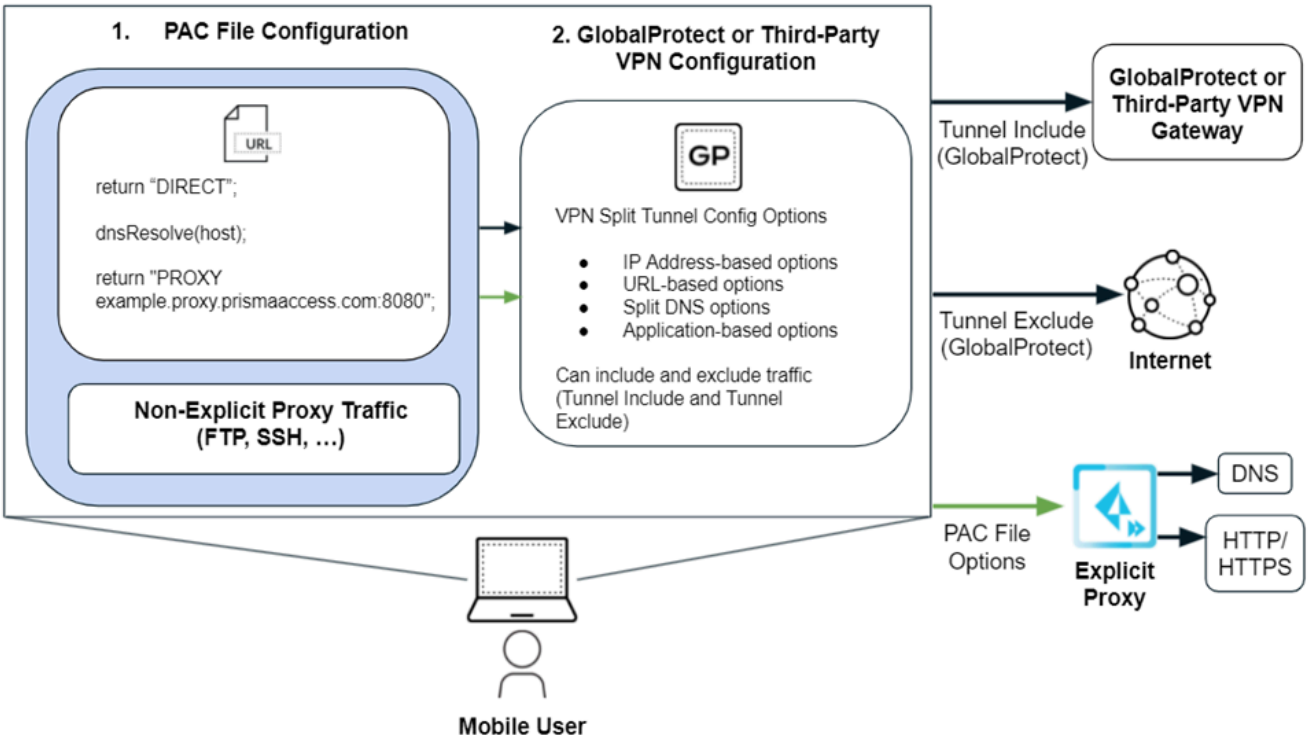
©2025 Palo Alto Networks, Inc.

- Debe asegurarse de que los navegadores utilizados por los usuarios móviles respeten la configuración del archivo PAC.

Proxy explícito y GlobalProtect: Cómo funciona

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Antes de decidir qué aplicaciones o tráfico debe proteger con Proxy explícito y qué aplicaciones debe proteger con GlobalProtect o con una VPN de terceros, debe comprender cómo GlobalProtect y Prisma Access toman sus decisiones de reenvío en función de la configuración de proxy explícito y VPN. Los ejemplos de esta sección asumen que ya ha implementado Explicit Proxy y GlobalProtect en la red de su organización, y que ha configurado las opciones de túnel dividido de GlobalProtect. En la siguiente figura se muestra el proceso.



Cuando un usuario móvil solicita un recurso o una aplicación privada o basada en Internet, la solicitud se evalúa mediante el archivo PAC de proxy explícito en el endpoint.

- Una función `return "DIRECT";` en el archivo PAC hace que el tráfico especificado en la expresión omita el procesamiento de proxy explícito.

  Proxy explícito le proporciona un archivo PAC de muestra que utiliza la función `return "DIRECT";` con direcciones IP y URL. Consulte Configurar su archivo PAC de proxy explícito para ver el contenido del archivo PAC y una descripción de cómo usarlo.

©2025 Palo Alto Networks, Inc.

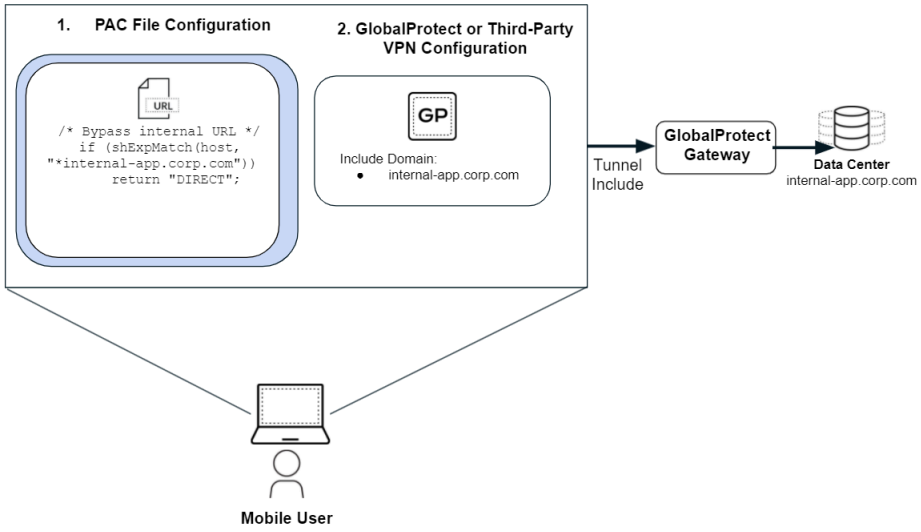
- Una función `dnsresolve(host)` en el archivo PAC obliga al endpoint a realizar una consulta DNS para resolver un nombre de host en una dirección IP. A continuación, esta consulta sigue la política de VPN (por ejemplo, túnel dividido o DNS dividido) para reenviar la solicitud DNS al servidor DNS de destino.

  El archivo PAC proporcionado con el proxy explícito utiliza `dnsresolve(host)`, `return"DIRECT";` y direcciones IP privadas juntas en una expresión. Si, después de una búsqueda de DNS, la dirección IP devuelta se incluye con las direcciones IP privadas de la expresión, el tráfico asociado a la dirección IP privada omite el procesamiento de proxy explícito.
- El tráfico que se especifica en el archivo PAC como `return"PROXY sitename:8080";` se reenvía al proxy explícito.

Una vez que la solicitud web se evalúa en función de las condiciones del archivo PAC, se envía a GlobalProtect o la configuración de VPN de terceros en el endpoint para su procesamiento y el tráfico se evalúa en la aplicación GlobalProtect para las opciones de configuración de túnel dividido. Puede dividir el tráfico en función del dominio (URL) o la aplicación o la subred. Si ha configurado split DNS (DNS dividido) en GlobalProtect, el tráfico también se evalúa en función de esas opciones de DNS.

Una vez procesado el tráfico, se envía a GlobalProtect, directamente a Internet o al Proxy explícito, en función del archivo PAC y el procesamiento de la VPN.

En la siguiente imagen se muestra un usuario móvil que intenta acceder a un recurso privado mediante la dirección URL **`internal-app.corp.com`**.



- El archivo PAC tiene la siguiente configuración para permitir que **`internal-app.corp.com`** omita el proxy explícito.

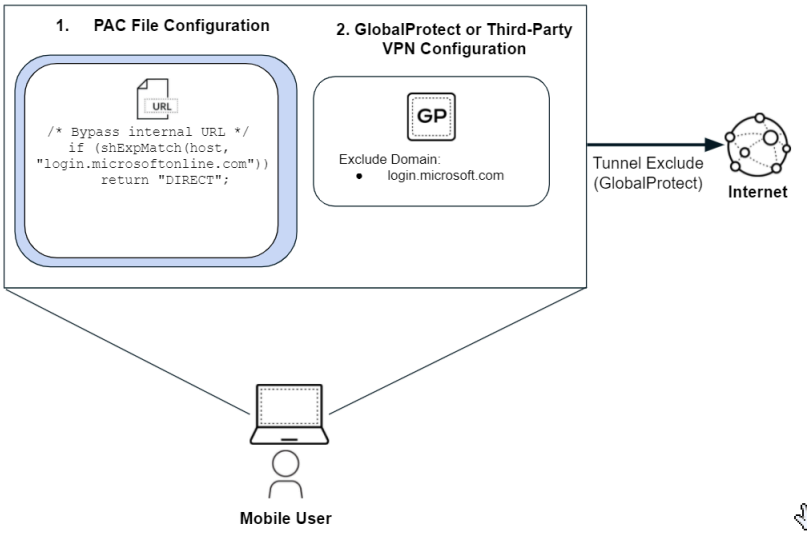
```
    /* Bypass internal URL */ if (shExpMatch(host, "*internal-
app.corp.com")) return "DIRECT";
```

- Cuando el usuario móvil solicita **`internal-app.corp.com`** desde su navegador, el navegador evalúa las condiciones en el archivo PAC. En base a esa evaluación, el navegador no reenvía la solicitud al proxy y la envía directamente a la aplicación GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

- GlobalProtect señala que **internal-app.corp.com** se enumera en **Include Domain (Incluir dominio)** y lo envía a través del túnel VPN.
- GlobalProtect envía la solicitud al recurso en **internal-app.corp.com** en base a las opciones de configuración de GlobalProtect.

Es posible que desee configurar algunos recursos, como los recursos de inicio de sesión, para que no utilicen el proxy explícito o la VPN de GlobalProtect o de terceros para el procesamiento. En la ilustración siguiente se muestra un usuario que inicia sesión en Microsoft Online introduciendo **login.microsoftonline.com** desde su navegador.



- El archivo PAC tiene la siguiente configuración para permitir que **internal-app.corp.com** omita el tráfico de proxy explícito.

```
   /* Bypass internal URL */ if (shExpMatch(host,
"login.microsoftonline.com")) return "DIRECT";
```

- Cuando el usuario móvil solicita **login.microsoftonline.com** desde su navegador, el archivo PAC evalúa la solicitud del archivo PAC en el endpoint del usuario móvil y, a continuación, la envía a la configuración VPN de GlobalProtect (GlobalProtect en este caso) para su procesamiento.
- La aplicación GlobalProtect señala que **login.microsoftonline.com** se enumera en **Exclude Domain (Excluir dominio)**.
- GlobalProtect omite la VPN y envía la solicitud directamente a Internet, en función de las opciones de configuración de GlobalProtect.

Proxy explícito y GlobalProtect: Configúralo

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	• Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	

Para que sus usuarios móviles se conecten de forma segura, puede combinar un proxy explícito con GlobalProtect o una VPN de terceros.

- Proxy explícito y GlobalProtect
  - Utilice GlobalProtect en modo de túnel dividido para proporcionar acceso seguro solo a aplicaciones privadas.
  - Utilice un proxy explícito para proteger aplicaciones públicas, incluyendo el tráfico de internet y aplicaciones SaaS externas.
- Proxy explícito y VPN de terceros
  - Utiliza un cliente VPN para acceder al centro de datos y a aplicaciones privadas, y para asegurar el acceso a aplicaciones privadas.
  - Utilice un proxy explícito y un archivo PAC para asegurar el acceso a aplicaciones públicas.

Antes de decidir qué aplicaciones o tráfico debería proteger con un proxy explícito y con GlobalProtect o con una VPN de terceros, debe comprender cómo GlobalProtect y Prisma Access toman sus decisiones de reenvío en función de la configuración de proxy explícito y VPN.

Cuando un usuario móvil solicita un recurso o aplicación privada o basada en internet, la solicitud se envía al archivo PAC del proxy explícito que está instalado en el endpoint.

- El tráfico que se especifica en el archivo PAC como return "DIRECT"; omite el procesamiento de proxy explícito. La resolución DNS (host) utilizada con return "DIRECT"; permite que la IP especificada pase por el procesamiento de proxy explícito.
- El tráfico que se especifica en el archivo PAC como "PROXY sitename:8080"; se reenvía a un proxy explícito.

Una vez procesado el tráfico, se envía a GlobalProtect, directamente a Internet o al proxy explícito, en función del archivo PAC y el procesamiento de la VPN.

El archivo PAC tiene la configuración para permitir que "internal-app.corp.com" evite el proxy explícito. Cuando el usuario móvil solicita "internal-app.corp.com" desde su navegador, el navegador evalúa las condiciones en el archivo PAC. GlobalProtect señala que "internal-app.corp.com" está enumerado en Incluir dominio y lo envía a través del túnel VPN. GlobalProtect envía la solicitud al recurso en "internal-app.corp.com" en base a las opciones de configuración de GlobalProtect.

- Strata Cloud Manager
- Panorama

Proxy explícito y GlobalProtect: Configurarlo (Strata Cloud Manager)

Para implementar GlobalProtect—Usuarios móviles con proxy explícito, complete los siguientes pasos.

Estos pasos de configuración hacen las siguientes suposiciones sobre su entorno de red; si su entorno de red es diferente, la configuración podría ser diferente:

 ©2025 Palo Alto Networks, Inc.

- Los usuarios móviles pueden acceder y resolver el nombre de host del portal GlobalProtect, los FQDN de la puerta de enlace, la URL del proxy explícito y la URL del archivo PAC.

  Aquí es donde puede encontrar esta información:

  - **FQDNs de la puerta de enlace de GlobalProtect** y **Nombre de host del portal**

    # Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** y edite la **Infrastructure Settings (Configuración de infraestructura)**.
  - **URL de proxy explícito** y **URL de archivo PAC**

    # Vaya a **Workflows (Flujos de trabajo)** > **Prisma AccessSetup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícita)** > **Infrastructure (Infraestructura)** y edite la **Infrastructure Settings (Configuración de la infraestructura)**.
- Los usuarios móviles pueden resolver dominios internos desde GlobalProtect.

STEP 1 | Decida qué aplicaciones quiere enviar a GlobalProtect y qué aplicaciones quiere enviar a Proxy explícito.

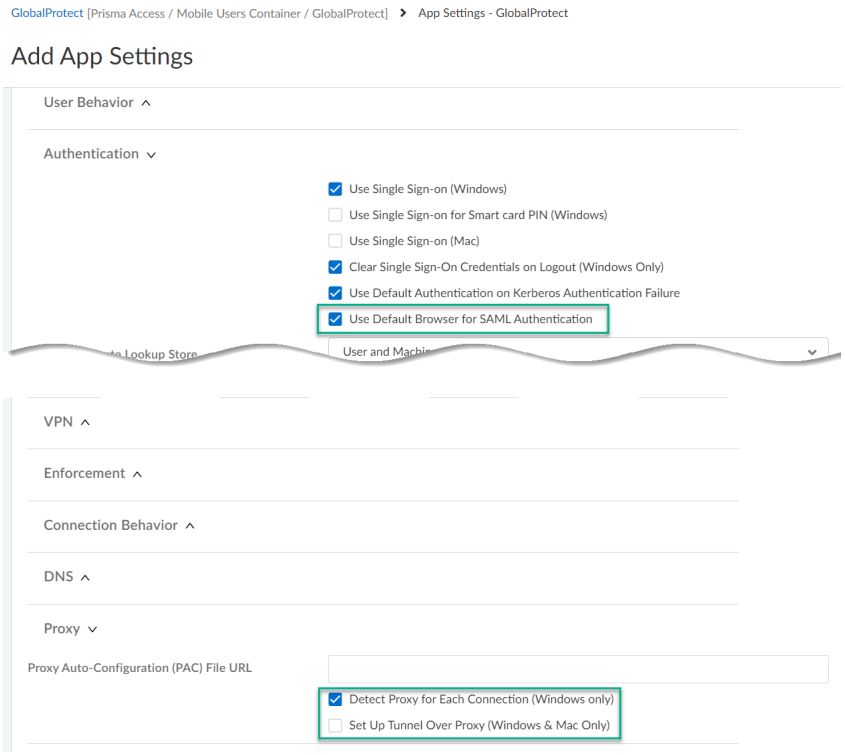
Los siguientes pasos dirigen las aplicaciones privadas alojadas en su centro de datos a GlobalProtect y las solicitudes a Internet y aplicaciones SaaS públicas a Explicit Proxy.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Modificar configuración del portal de GlobalProtect

Vaya a **GlobalProtect** > **App Settings (Ajustes de la aplicación)** > **App Configuration (Configuración de la aplicación)** > **Advanced Settings (Configuración avanzada)**

1. En la configuración del **Proxy**
   - Marque **Detect Proxy for Each Connection (Detectar proxy para cada conexión)**
   - Retire la marca de **Set Up Tunnel Over Proxy (Windows & Mac Only) [Configurar túnel sobre proxy (solo Windows y Mac)]**
2. En configuración de **Authentication (Autenticación)**:
   - Marque **Use Default Browser for SAML Authentication (Usar navegador predeterminado para la autenticación SAML)**



STEP 3 | Cree un túnel dividido en GlobalProtect que le permita dirigir el tráfico interno a GlobalProtect.

Vaya a **GlobalProtect** > **Tunnel Settings (Configuración de túnel)** > **Split Tunneling (Túnel dividido)**. Configure un túnel dividido según el dominio (FQDN), las rutas de acceso o las aplicaciones.

STEP 4 | Configure el archivo PAC para excluir los dominios que especificó para el túnel dividido de GlobalProtect.

Para descargar el archivo PAC para poder editarlo, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Infrastructure (Infraestructura)** >

 ©2025 Palo Alto Networks, Inc.

Explicit Proxy (Proxy explícito) > **Infrastructure Settings (Configuración de infraestructura)** > **Proxy Auto Configuration (Configuración automática de proxy)**.

El siguiente ejemplo muestra un archivo PAC con la URL que aloja aplicaciones privadas (internal-app.corp.com) sin pasar por el proxy interno. Los parámetros del siguiente archivo PAC son todos valores de ejemplo:

- El nombre de host del portal es `splittunnel.gpcloudservice.com`.
- Las puertas de enlace de usuarios móviles están contenidas en el FQDN comodín `*examplegateways.gw.gpcloudservice.com`.
- La URL del archivo PAC es `https://pacfileurl.pac`.
- `internal-app.corp.com` aloja las aplicaciones privadas que están protegidas por Usuarios móviles: GlobalProtect.
- Okta se utiliza para la autenticación SAML.
- El URL de Proxy explícito es `example.proxy.prismaacess.com`.

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

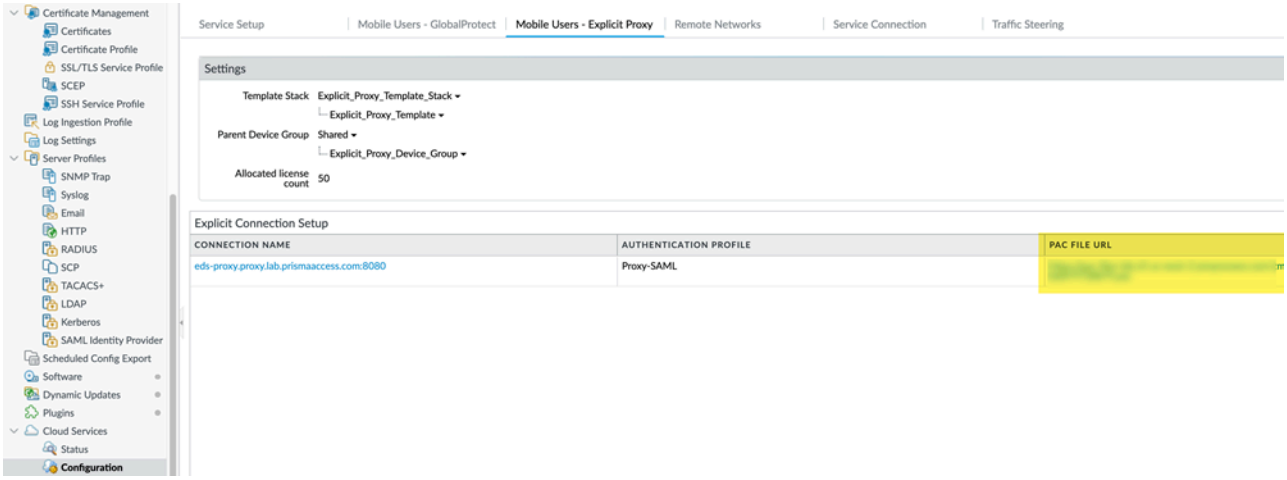
Proxy explícito y GlobalProtect: Configurarlo (Panorama)

Para implementar GlobalProtect—Usuarios móviles con proxy explícito, complete los siguientes pasos.

Estos pasos de configuración hacen las siguientes suposiciones sobre su entorno de red; si su entorno de red es diferente, la configuración podría ser diferente:

 ©2025 Palo Alto Networks, Inc.

- Los usuarios móviles pueden acceder y resolver el nombre de host del portal GlobalProtect, los FQDN de la puerta de enlace, la URL del proxy explícito y la URL del archivo PAC.
  - Para encontrar los FQDN de la puerta de enlace, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)** > **Gateways (Puertas de enlace)**.
  - Para encontrar el **PAC File URL (URL del archivo PAC)**, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** > **PAC File URL (URL del archivo PAC)**.



- Los usuarios móviles pueden resolver dominios internos desde GlobalProtect.

STEP 1 | Planifique la implementación de Usuarios móviles: Proxy explícito y su implementación de GlobalProtect (ya sea la implementación de Usuarios móviles: Proxy explícito o la implementación independiente de GlobalProtect).

STEP 2 | Decida qué aplicaciones quiere enviar a GlobalProtect y qué aplicaciones quiere enviar a Proxy explícito.

Los siguientes pasos dirigen las aplicaciones privadas alojadas en su centro de datos a GlobalProtect y las solicitudes a Internet y aplicaciones SaaS públicas a Explicit Proxy.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | En el Panorama que gestiona Prisma Access, configure la configuración del portal GlobalProtect.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)**.

   Asegúrese de que está en la **Mobile_User_Template** del menú desplegable de **Template (Plantilla)**.
2. Seleccione **GlobalProtect_Portal** para editar la configuración del portal de Prisma Access.
3. Seleccione la pestaña **Agent (Agente)** y seleccione la configuración **DEFAULT (PREDETERMINADA)** del agente o seleccione **Add (Añadir)** una nueva.
4. Seleccione la pestaña **App (Aplicación)**.
5. Realiza los siguientes cambios en la configuración de la aplicación:
   - En **Detect Proxy for Each Connection (Detectar proxy para cada conexión)**, seleccione **Yes (Sí)**
   - En **Set Up Tunnel Over Proxy (Windows & Mac Only) [Configurar túnel sobre proxy (solo Windows y Mac)]**, seleccione **No**.
   - En **Use Default Browser for SAML Authentication (Usar navegador predeterminado para la autenticación SAML**, seleccione **Yes (Sí)**.

STEP 4 | Cree un túnel dividido en GlobalProtect que le permita dirigir el tráfico interno a GlobalProtect.

El siguiente ejemplo utiliza un túnel dividido para dirigir el tráfico según el dominio (FQDN); también podría configurar un túnel dividido según la ruta de acceso del tráfico.

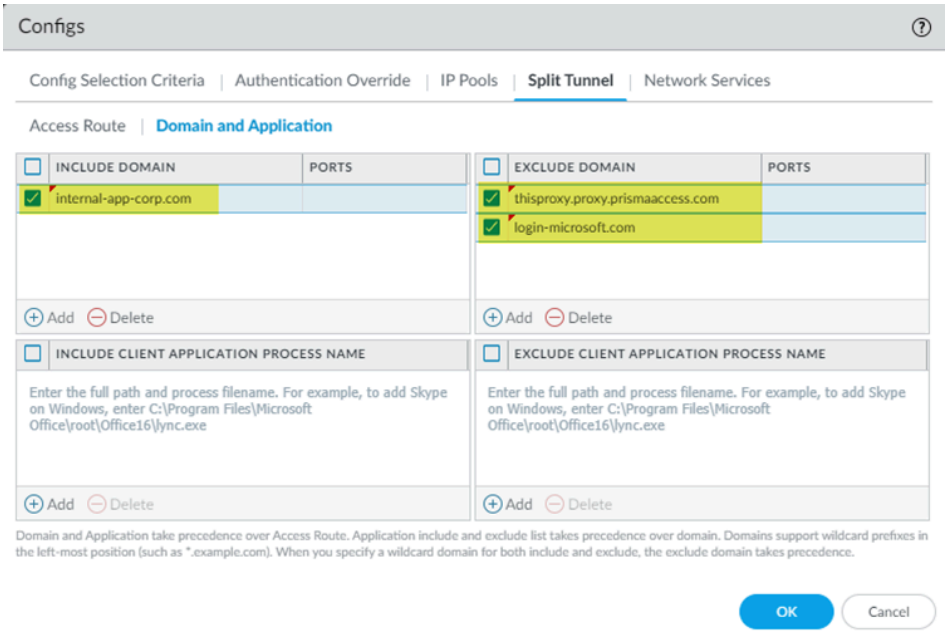
1. Mientras aún esté en la configuración del agente de GlobalProtect [**Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > **GlobalProtect External Gateway**

 ©2025 Palo Alto Networks, Inc.

(Puerta de enlace de GlobalProtect)], seleccione **Agent (Agente)** > **Client Settings (Configuración de cliente)**.

2. Seleccione la configuración **DEFAULT (PREDETERMINADA)** o elija **Add (Añadir)** para añadir una nueva.
3. Seleccione **Split Tunnel (Túnel dividido)** > **Domain and Application (Dominio y aplicación)**.
4. Deberá **Add (Añadir)** la opción **Include Domain (Incluir dominio)** y, opcionalmente, los **Ports (Puertos)** a utilizar con el dominio.

   Este ejemplo utiliza internal-app.corp.com como la URL que usa para alojar aplicaciones en su centro de datos. Usted añade esta URL y la URL de autenticación SAML en el **Exclude Domain (Excluir dominio)**.



5. Haga clic en **OK (Aceptar)** para guardar los cambios.
6. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 5 | Configure el archivo PAC para excluir los dominios que incorporó para el túnel dividido.

El siguiente ejemplo muestra un archivo PAC con la URL que aloja aplicaciones privadas (internal-app.corp.com) sin pasar por el proxy interno. Los parámetros del siguiente archivo PAC son todos valores de ejemplo:

- El nombre de host del portal es `splittunnel.gpcloudservice.com`.
- Las puertas de enlace de usuario móvil [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Mobile Users—GlobalProtect**

©2025 Palo Alto Networks, Inc.

(Usuarios móviles: GlobalProtect) > **Gateways (Puertas de enlace)**] están contenidas en el FQDN comodín `*examplegateways.gw.gpcloudservice.com`.

- La **PAC File URL (URL del archivo PAC)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)** > **PAC File URL (URL del archivo PAC)**] es `https://pacfileurl.pac`.
- `internal-app.corp.com` está alojando las aplicaciones privadas protegidas por Usuarios Móviles: GlobalProtect.
- Okta se está utilizando para la autenticación SAML.
- La URL del proxy explícito es `example.proxy.prismaaccess.com`.

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

Proxy explícito con VPN de terceros

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Para utilizar las VPN de terceros con proxy explícito, debe poder realizar los siguientes cambios en su red:

- Debe configurar su VPN de terceros para realizar túneles divididos para dirigir el tráfico de Internet al proxy explícito.

  Para obtener ayuda con la configuración de su VPN de terceros, comuníquese con su proveedor de VPN de terceros.
- modificar el archivo PAC para que el Proxy explícito omita cualquiera de los siguientes componentes VPN:
  - Cualquier dirección IP asociada con la VPN de terceros
  - Cualquier URL de inicio de sesión requerida para la VPN de terceros

 ©2025 Palo Alto Networks, Inc.

En el ejemplo siguiente, configuró el archivo PAC para que el proxy explícito omita recursos internos utilizando direcciones IP privadas, así como flujos de tráfico de autenticación.

```
++++++++++++++++ function FindProxyForURL(url, host) { if
 (isPlainHostName(host) || shExpMatch(host, "*.local")
 || isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
 isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
 return "DIRECT"; /* Bypass SAML for AnyConnect Azure */
 if (shExpMatch(host, "login.microsoftonline.com")) return
 "DIRECT"; if (shExpMatch(host, "login.windows.net")) return
 "DIRECT"; if (shExpMatch(host, "login.microsoft.com"))
 return "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

Optimización de direcciones IP para usuarios de proxy explícito: Implementaciones de proxy

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si desea utilizar esta función en su entorno de Prisma Access, póngase en contacto con su equipo de cuenta para obtener más información.	• Prisma Access 5.2 • Plano de datos 10.2.4 de Prisma Access • Complemento Panorama versión 5.2.0

La optimización de direcciones IP es un conjunto de mejoras de la arquitectura que reducen el número total de direcciones IP en la implementación, lo que simplifica los flujos de trabajo de listas de permitidos, al tiempo que mejora la resiliencia y permite una incorporación más rápida de los inquilinos de Prisma Access.

Persistencia de la dirección IP

Con la adherencia, o persistencia, de la dirección IP, puede proteger las aplicaciones SaaS y los sitios web que requieren que las sesiones de usuario mantengan la misma dirección IP de salida de Prisma Access durante toda la sesión de usuario.

Simplifique la incorporación de aplicaciones SaaS

Añadir una ubicación de Prisma Access o experimentar un evento de escalado en una ubicación existente de Prisma Access podría llevar a que se asignen nuevas direcciones IP a sus implementaciones de proxy explícito. Es una práctica recomendada recuperar las nuevas direcciones IP de salida y puerta de enlace y añadirlas a una lista de permitidos de las aplicaciones SaaS. La optimización de direcciones IP reduce el número de direcciones IP que tiene que gestionar en implementaciones grandes.

Resolución de problemas

 ©2025 Palo Alto Networks, Inc.

Si desea orientar aplicaciones específicas para la optimización de direcciones IP, puede añadirlas a la categoría URL o a la lista dinámica externa (EDL). Después de configurar los objetos especiales, solo los dominios incluidos en estos objetos obtendrán la optimización de la dirección IP.

Panorama: configure la categoría de URL como **PANW EP IP Affinity URL List** o EDL como **Lista de afinidad IP de PANW EP**. Evite entradas comodín, por ejemplo **.*** o dominios de nivel superior como **.com**.

Strata Cloud Manager: admite la lista de URL **PANW EP IP Affinity URL List**.

Resolución de DNS para implementaciones de Usuarios móviles: Proxy explícito

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Si desea utilizar esta función en su entorno de Prisma Access, póngase en contacto con su equipo de cuenta para obtener más información.	☐ Licencia de Prisma Access ☐ Prisma Access versión 5.2.0

Prisma Access le permite especificar servidores DNS para resolver tanto los dominios internos de su organización como los dominios externos. Prisma Access realiza un proxy de la solicitud DNS en función de la configuración de sus servidores DNS. Proxy explícito admite las siguientes funcionalidades de DNS:

- Uso de un navegador de terceros con proxy explícito
- Uso de un servidor DNS por región con Prisma Access Browser

- *El proxy DNS para la configuración de proxy explícito tiene prioridad sobre las configuraciones de servidores DNS internos definidas en la**Prisma Access Setup (Configuración de Prisma Access)**.*
- *Después de habilitar el proxy DNS para Proxy explícito, debe migrar la configuración de DNS existente desde **Prisma Access Setup (Configuración de Prisma Access)** > **Internal DNS Servers (Servidores DNS internos)** a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Infrastructure Settings (Configuración de infraestructura)** > **DNS Proxy (Proxy DNS)***

Configurar la configuración de DNS

Para configurar los ajustes del proxy DNS, complete los siguientes pasos:

 ©2025 Palo Alto Networks, Inc.

1. Añadir una regla de servidor DNS de proxy explícito.
   1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Infrastructure Settings (Configuración de infraestructura)** > **Explicit Proxy (Proxy explícita)**.
   2. Haga clic en el icono de configuración y vaya a **Client DNS (DNS del cliente)**.
   3. **Add Region (Añadir región)** y asignarle un nombre único.
   4. Seleccione una región o ubicación, o seleccione**Worldwide (Mundial)**.

      Si especifica múltiples configuraciones proxy con una mezcla de configuraciones Worldwide (mundial) y teatro; Prisma Access utiliza las configuraciones para el grupo de ubicaciones, luego teatro, luego mundial (Worldwide). Prisma Access evalúa las reglas de arriba a abajo en la lista.
   5. Añada la dirección IP del servidor DNS.

2. Elija si desea o no que Prisma Access proceda a **Resolve internal domains (Resolver dominios internos)**; si lo hace, deberá **Add (Añadir)** una o más **Internal Domain Resolve Rules (Reglas internas de resolución de dominio)**.

3. Elija **Add (Añadir)** y defina las **Internal Domain Resolve Rules (Reglas de resolución de dominio interno)**.

   *Actualmente, las **Internal Domain Resolve Rules (Reglas de resolución de dominio interno)** solo son compatibles con Prisma Access Browser y Proxy de agente.*
4. Añada un **Name (Nombre)** único para la regla y una dirección IP personalizada en **Primary DNS (DNS primario)** y **Secondary DNS (DNS secundario)**.
5. Seleccione **Prisma Access Default (Predeterminado de Prisma Access)** para utilizar el servidor DNS de Prisma Access predeterminado para resolver dominios internos. Si desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios que desea resolver en las **Domain Lists (Lista de dominios)**.
6. Si tiene un servidor DNS **Custom (Personalizado)** que pueda acceder a sus dominios internos, especifique las direcciones IP del servidor **Primary DNS (DNS primario)** y **Secondary DNS (DNS secundario)**.

7. Si desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios que desea resolver en las **Domain Lists (Listas de dominios)**. Especifique un asterisco delante del dominio; por ejemplo, *.acme.com. Haga clic en **Save (Guardar)**
8. Debe **Push Config (Enviar configuración)** para guardar y enviar sus cambios en la configuración.

 ©2025 Palo Alto Networks, Inc.

Ver asignaciones de usuarios a direcciones IP o grupos de usuarios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Licencia de Prisma Access

Prisma Access Insights le permite ver la asignación de usuarios a direcciones IP o de usuarios a grupos para usuarios móviles en tiempo real. Para redes remotas y conexiones de servicio, puede ver las asignaciones de usuarios a grupos de usuarios.

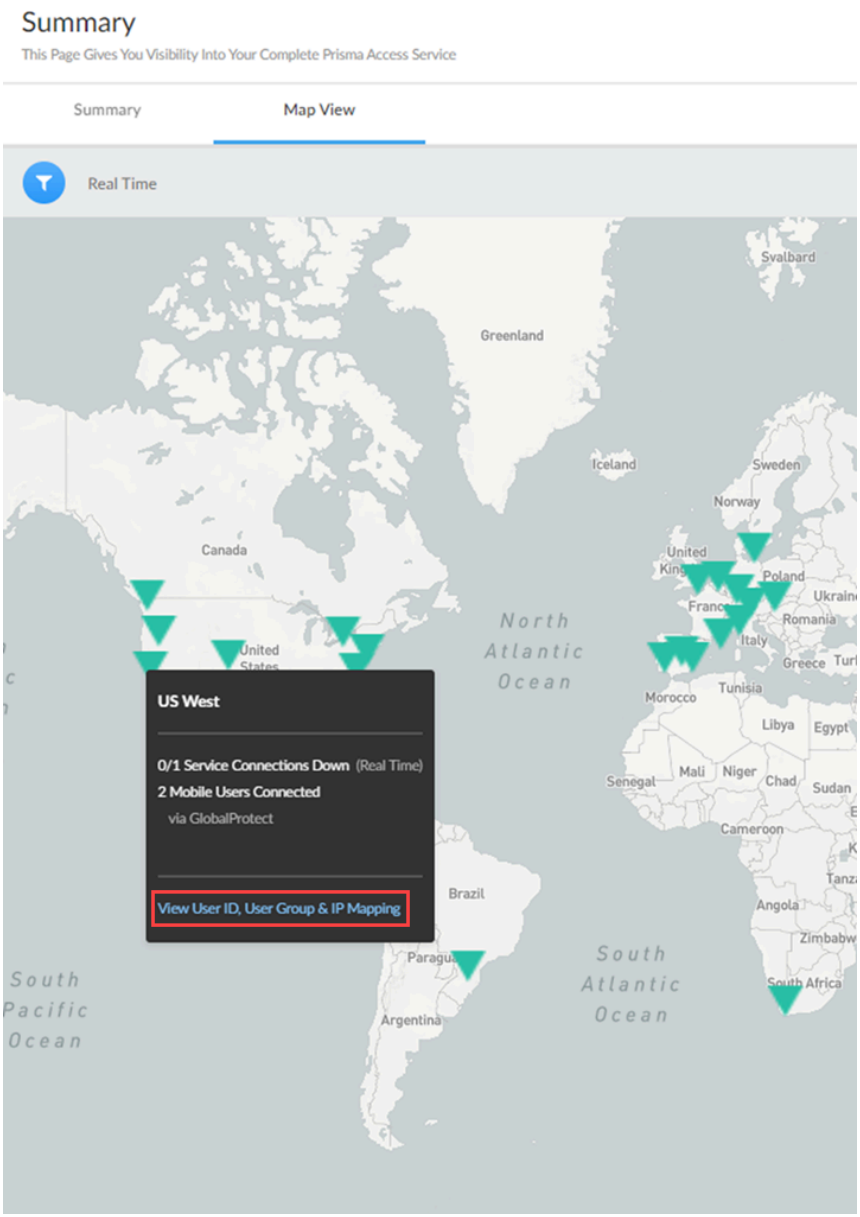
Los triángulos invertidos en el mapa están codificados por colores para indicar el estado de ubicación de Prisma Access:

- Verde: Todas las instancias están activas.
- Rojo: Todas las instancias están inactivas.
- Amarillo: Las instancias son una combinación de activo, inactivo y desconocido, y pueden requerir su atención.
- Gris: Todos las instancias son desconocidos.

STEP 1 | Desde el panel **Summary (Resumen)**, seleccione la **Map View (Vista de mapa)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Pase el puntero del ratón sobre una ubicación hasta que aparezca un cuadro de diálogo emergente.



STEP 3 | Seleccione **View User ID, User Groups & IP Mapping (Ver ID de usuario, grupos de usuarios y asignación de IP)** en el cuadro de diálogo. El cuadro de diálogo **UserID and User Group Distribution Check (Comprobación de distribución de UserID y grupo de usuarios)** se abre.

STEP 4 | Seleccione el **Prisma Access Location (Ubicación de Prisma Access)** y **Node Type (Tipo de nodo)**. El **Prisma Access Location filter (Filtro de ubicación de Prisma Access)** no se tiene

 ©2025 Palo Alto Networks, Inc.

en cuenta cuando el **Node Type (Tipo de nodo)** es **Mobile Users (GlobalProtect) [Usuarios móviles (GlobalProtect)]**.

Para redes remotas y conexiones de servicio, solo puede ver las asignaciones de ID de usuario a grupos de usuarios.

1. Seleccione una **Prisma Access Location (Ubicación de Prisma Access)** Si la ubicación de Prisma Access que seleccione no tiene ninguna red remota o conexión de servicio asociada, verá un mensaje "No hay datos disponibles" en el campo **Remote Networks Site (Sitio de redes remotas)** o **Service Connections Site (Sitio de conexiones de servicio)**, según sea el caso, y los botones **Show User Groups (Mostrar grupos de usuarios)** y **Export to CSV (Exportar a CSV)** no estarán habilitados.
2. En **Node Type (Tipo de nodo)**, seleccione Redes remotas o Conexiones de servicio.
3. Desde el campo **Remote Networks Site (Sitio de redes remotas)** o **Service Connections Site (Sitio de conexiones de servicio)**, seleccione el sitio desde el cual desea recuperar los datos.
4. En Ver, seleccione si desea ver a qué grupos de usuarios pertenece un ID de usuario (Usuario) o qué usuarios forman parte de un grupo particular (Grupo) asociado con el sitio.
   - Si selecciona **User (Usuario)**, introduzca el **User ID (ID de usuario)** del usuario (por ejemplo, saas\testuser3) para obtener la asignación del ID de usuario al grupo de usuarios, luego seleccione **Show User Groups (Mostrar grupos de usuarios)**. Una lista de todos los grupos a los que pertenece el ID de usuario se muestra en **User ID-IP Mappings (Asignaciones de IP de ID de usuario)**.

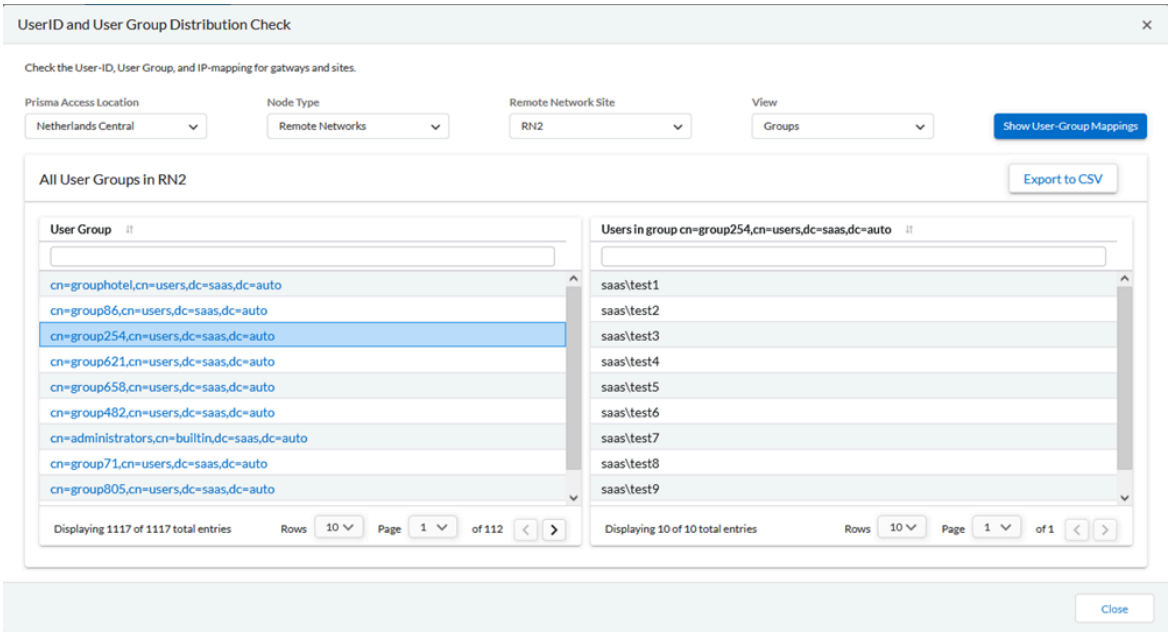
     Puede buscar un grupo específico escribiendo el nombre del grupo o una cadena contenida dentro del nombre del grupo que desea encontrar introduciéndolo en el cuadro de texto **User Group (Grupo de usuarios)** . Si busca un grupo que no existe, verá un mensaje de error que dice: "No hay datos disponibles". También puede ordenar la lista de grupos alternando el icono de flechas junto a **User Group (Grupo de usuarios)**. Puede seleccionar el número de entradas que desea mostrar, así como desplazarse por las páginas haciendo clic en las flechas hacia adelante y hacia atrás.

     Si selecciona **Groups (Grupos)**, al seleccionar **Show User-Group Mappings (Mostrar asignaciones de grupos de usuarios)** se muestran todos los grupos que están disponibles en el sitio en **All User Groups in (Todos los grupos de usuarios en) *<selected_site>***. Si selecciona un grupo, todos los usuarios que pertenecen al grupo se muestran en el panel derecho. El botón **Export to CSV (Exportar a CSV)** se activa y puede exportar todos los usuarios que pertenecen a ese grupo a un archivo CSV. El archivo CSV exportado contiene todas las entradas del grupo, incluso si no se muestran en la interfaz de usuario en el momento de la exportación.

     Puede buscar un grupo específico escribiendo el nombre del grupo o una cadena contenida dentro del nombre del grupo que desea encontrar introduciéndolo en el cuadro de texto **User Group (Grupo de usuarios)** . Si busca un grupo que no existe, verá un mensaje de error que dice: "No hay datos disponibles". También puede ordenar la lista de grupos alternando el icono de flechas junto a **User Group (Grupo de usuarios)**.

 ©2025 Palo Alto Networks, Inc.

Puede seleccionar el número de entradas que desea mostrar, así como desplazarse por las páginas seleccionando las flechas hacia adelante y hacia atrás.



Node Type (Tipo de nodo): Mobile Users (GlobalProtect) [Usuarios móviles: GlobalProtect]

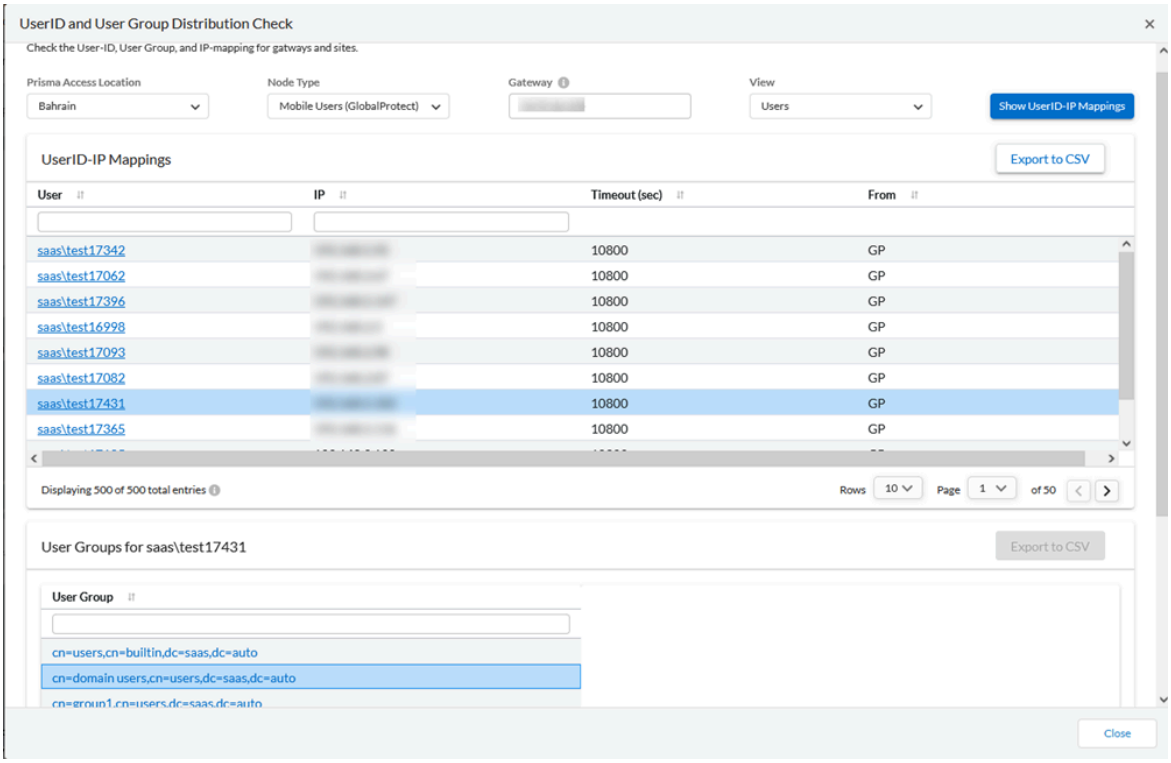
Puede ver la asignación de ID de usuario a IP, así como la asignación de ID de usuario a grupo de usuarios. El filtro **Prisma Access Location (Ubicación de Prisma Access)** no se tiene en cuenta cuando el **Node Type (Tipo de nodo)** seleccionado es **Mobile Users (GlobalProtect) [Usuarios móviles (GlobalProtect)]**. En cambio, Prisma Access Insights utiliza la dirección IP de la puerta de enlace de GlobalProtect para buscar los datos.

1. Introduzca una dirección de puerta de enlace IP de GlobalProtect en el cuadro de texto **Gateway (Puerta de enlace)**.
2. Seleccione si desea **View (Ver)** datos de asignación de ID de usuario a IP de usuario [**Users (Usuarios)**] o de asignación de ID de usuario a grupo de usuarios [**Groups (Grupos)**] para usuarios que están conectados a su puerta de enlace GlobalProtect especificada.

   Si seleccionó **Users (Usuarios)**, seleccione **Show UserID-IP Mappings (Mostrar asignaciones de UserID-IP)**. Se muestra una tabla con la asignación del ID de usuario a su IP de usuario junto con el **Timeout (Tiempo de espera)**, que muestra durante cuánto tiempo (en segundos) es válida la entrada del ID de usuario a la IP de usuario. Al seleccionar un usuario en particular, se muestran los grupos a los que pertenece dicho usuario. Al seleccionar un grupo se muestran todos los usuarios que pertenecen a ese grupo. También habilita el botón **Export to CSV (Exportar a CSV)**, que le permite exportar todos los usuarios de

 ©2025 Palo Alto Networks, Inc.

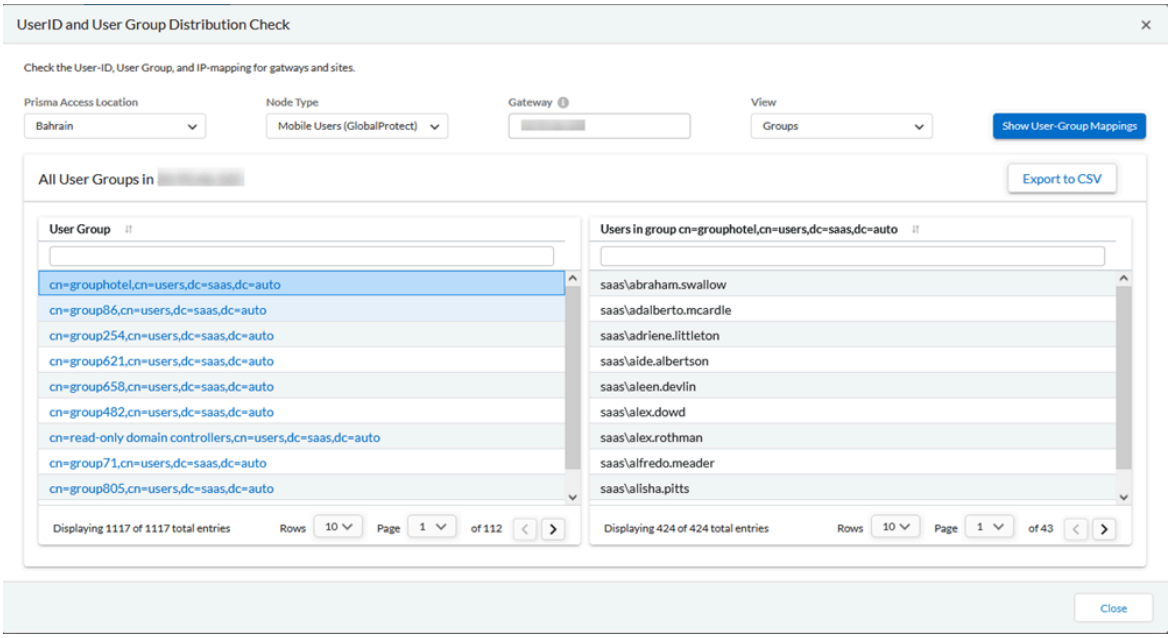
ese grupo independientemente de cualquier vista filtrada que se muestre en la interfaz de usuario.



Si seleccionó **Groups (Grupos)**, seleccione **Show User-Group Mappings (Mostrar asignaciones de grupos de usuarios)**. En **User Group (Grupo de usuarios)** aparece una lista de todos los grupos de usuarios que pertenecen a esa puerta de enlace de GlobalProtect. Al seleccionar un grupo de usuarios, se muestran todos los usuarios que pertenecen a ese grupo en el panel derecho. También habilita el botón **Export to CSV (Exportar a CSV)**, que

 ©2025 Palo Alto Networks, Inc.

le permite exportar todos los usuarios de ese grupo independientemente de cualquier vista filtrada que se muestre en la interfaz de usuario.



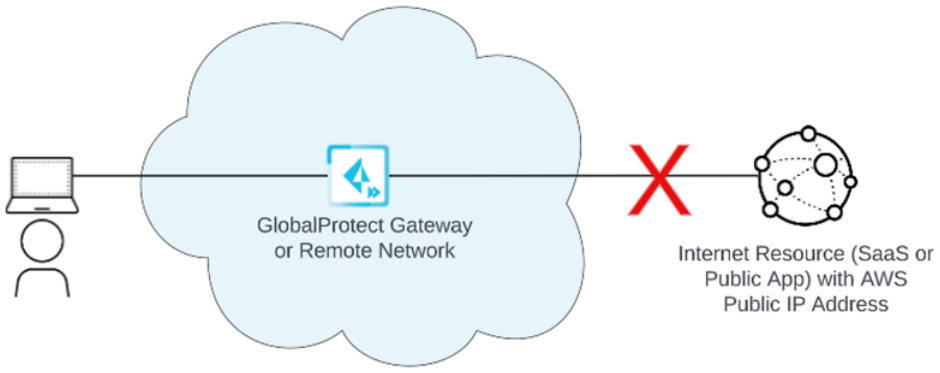
 ©2025 Palo Alto Networks, Inc.

Reportar problemas de acceso al sitio de usuario móvil

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Algunos sitios web como stubhub.com, ticketmaster.com o dollartree.com bloquean el tráfico del rango de direcciones IP de la nube de AWS. Cuando los usuarios protegidos por Prisma Access intentan acceder a estos sitios web, se les puede negar el acceso con el siguiente mensaje en el navegador web:

```
Acceso denegado. You don't have permission to access
 "http://www.dollartree.com/" on this server. Reference
 #18.7f955b8.1509600370.44eb7c8
```



Para informar de este problema, introduzca https://reportasite.gpcloudservice.com/ desde un navegador web y proporcione la URL del sitio web que es inaccesible. Después de 24-48 horas, regrese a https://reportasite.gpcloudservice.com/ e introduzca la misma URL para ver su estado.

Palo Alto Networks le proporciona la dirección IP que utiliza la URL; en algunos casos, debe añadir esta dirección IP a las listas de permisos de su organización para evitar el bloqueo del tráfico. Si tiene URL que se redirigen, añada estas direcciones IP a sus listas de permisos:

- 65.154.226.160
- 154.59.126.110
- 66.232.36.110

Proceso de redirección de URL de Prisma Access

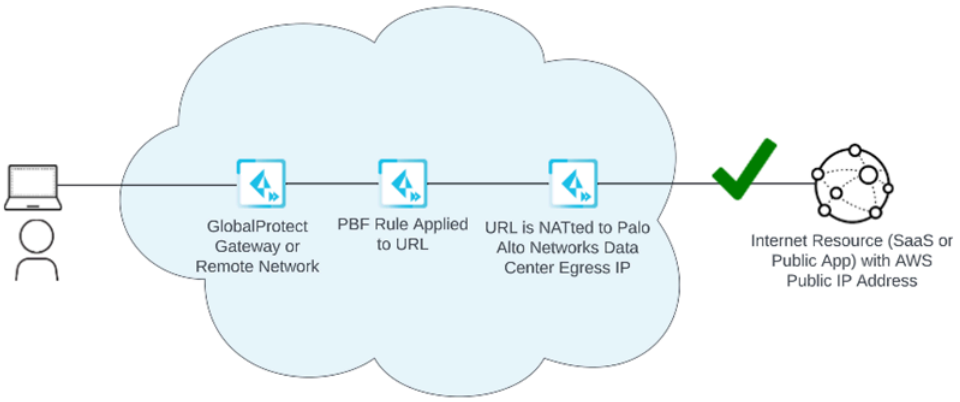
Algunos sitios web bloquean el tráfico de un rango de direcciones IP en la nube. Cuando los usuarios protegidos por Prisma Access intentan acceder a estos sitios web, se les impide el acceso. Con el fin de garantizar que se restablezca el acceso a estos sitios web, Palo Alto Networks revisa todos los sitios que se informan y, si se encuentra un problema de acceso, clasifica el sitio y añade

©2025 Palo Alto Networks, Inc.

una política de salida que hace NAT de la dirección IP a una a la que se pueda acceder. Palo Alto Networks revisa minuciosamente los sitios para determinar su reputación y solo se añaden sitios web con una reputación prístina a la regla de salida, mientras que los demás son rechazados, utilizando este proceso:

1. Usted nos notifica la URL con problemas de acceso usando https://reportasite.gpcloudservice.com/.
2. La automatización de la Ingeniería de fiabilidad del sitio (SRE) revisa la URL.
3. Si SRE determina que la URL es segura, se aplica una regla de reenvío basado en políticas (PBF) a la URL y su dominio padre.
4. El tráfico se enruta a través de Prisma Access desde la puerta de enlace de GlobalProtect o red remota a un hub de procesamiento de URL, donde se aplica la regla PBF al dominio, y desde el hub a un centro de datos de Palo Alto Networks.
5. A medida que el tráfico sale del centro de datos, la URL es sometida a NAT de origen hacia la dirección IP del centro de datos.

Como resultado de estas acciones, el tráfico hacia y desde las aplicaciones SaaS no se pierde porque la dirección IP del centro de datos tiene una reputación limpia.



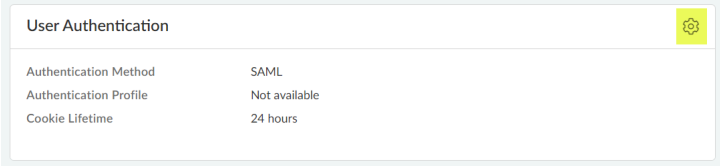
 ©2025 Palo Alto Networks, Inc.

Habilite usuarios móviles para autenticarse en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Puede autenticar a los usuarios móviles en Prisma Access utilizando cualquiera de los tipos de autenticación. Siga estos pasos para configurar la autenticación para los usuarios móviles de GlobalProtect o Proxy explícito.

STEP 1 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** y vaya a la configuración de Usuarios móviles: GlobalProtect o de Explict Proxy (Proxy explícito), y **Set Up User Authentication (Configurar la autenticación de usuario)**.



STEP 2 | Seleccione su **Authentication Method (Método de autenticación)** de los tipos de autenticación compatibles.

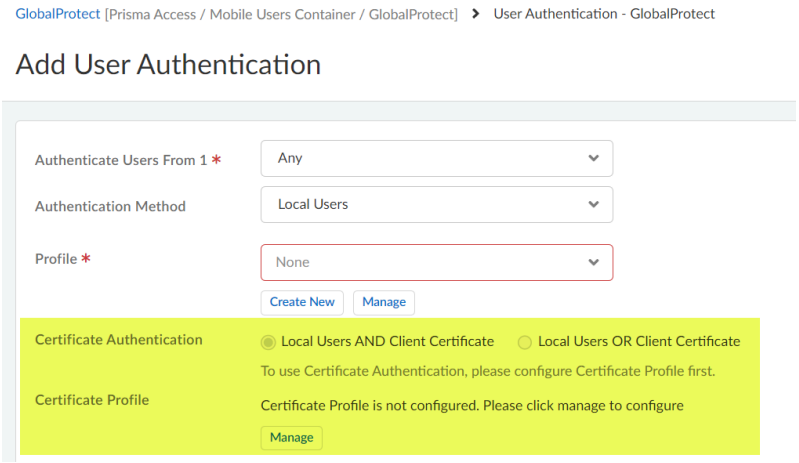
Si aún no ha integrado Prisma Access con sus servicios de autenticación, le explicamos cómo hacerlo.

STEP 3 | Elija el **Profile (Perfil)** de autenticación que configuró para habilitar Prisma Access para conectarse al servicio que desea utilizar para autenticar a los usuarios.

- Especifique el **Profile (Perfil)** de autenticación SAML si usó SAML en el Paso 2, o cree un nuevo perfil de autenticación SAML para usar con Prisma Access.
- Especifique el **Profile (Perfil)** de autenticación CIE si utilizó CIE en el Paso 2, o cree un nuevo perfil de autenticación CIE para usar con Prisma Access.
- Especifique el**Profile (Perfil)** de la autenticación Kerberos si usó Kerberos en el Paso 2, o cree un nuevo perfil de autenticación Kerberos para usar con Prisma Access.

©2025 Palo Alto Networks, Inc.

STEP 4 | Especifique la configuración de autenticación de certificados:



- **Autenticación del certificado**

  Para mejorar la seguridad, use un certificado (además del servicio de autenticación) para obtener nombres de usuario y autenticar a los usuarios en Prisma Access. Para autenticar al usuario en base a un certificado de cliente, uno de los campos del certificado, tal como el campo Subject Name, debe identificar el nombre de usuario. Los usuarios móviles que se autentican correctamente a través de la autenticación de certificado de cliente no tienen la opción de cerrar sesión en la aplicación GlobalProtect.

  Con Prisma Access, puede optar por exigir a los usuarios móviles que pasen la autenticación de certificados y la autenticación basada en el tipo de autenticación, o conceder acceso a los usuarios móviles siempre que hayan superado correctamente solo una de esas comprobaciones.

- **Perfil del certificado**

  Utilice un perfil de certificado opcional para verificar los certificados que los usuarios móviles presentan a Prisma Access 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. Dado que el certificado forma parte de la autenticación para el usuario móvil, debe implementar previamente los certificados utilizados en los perfiles de certificado para los usuarios antes de su inicio de sesión inicial. El perfil de certificado especifica qué campo de certificado contiene el nombre de usuario (Asunto o Asunto Alt). 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 debe contener los campos correspondientes, que se usarán como el nombre de usuario cuando la aplicación de GlobalProtect se autentique con Prisma Access.

©2025 Palo Alto Networks, Inc.

STEP 5 | Especifique una **Cookie Lifetime (Vida útil de la cookie)** para la cookie que almacena las credenciales de autenticación de los usuarios.

Después de que el IdP autentique al usuario, Prisma Access almacena el estado de autenticación del usuario en el Servicio de caché de autenticación (ACS). El período de validez de la autenticación se basa en el valor de la **vida útil de la cookie** que especifique aquí.

Para evitar problemas con los usuarios que no pueden descargar archivos grandes antes de que expire la duración de la cookie, o la cookie expire cuando los usuarios están accediendo a un solo sitio web durante un largo período de tiempo, Palo Alto Networks recomienda que configure una Cookie Lifetime (Vida útil de la cookie) de al menos un día. Si los usuarios de Proxy explícito tienen un problema de caducidad de la duración de la cookie, pueden navegar a un sitio web diferente para volver a autenticarse en ACS y actualizar la cookie de ACS.

Soporte de autenticación y características

Estos son los servicios con los que se integra Prisma Access para proporcionar autenticación, y las características a tener en cuenta cuando está planificando la configuración de su autenticación:

Soporte de autenticación:

- Cloud Identity Engine
- SAML
- TACACS+
- RADUIS
- LDAP
- Kerberos
- MFA
- Autenticación de base de datos local

Aspectos destacados de la característica de autenticación:

- SSO
- Portal de autenticación
- Secuencia de autenticación

Soporte de autenticación

Cloud Identity Engine	Para implementar Cloud Identity Engine para la autenticación de usuarios, configure un proveedor de identidad (IdP) basado en SAML 2.0, un certificado de cliente y una cadena de entidad de certificación (CA) o ambos. Después de especificar cómo desea autenticar a sus usuarios, configure su perfil de autenticación para definir su política de seguridad de autenticación y, opcionalmente,

 ©2025 Palo Alto Networks, Inc.

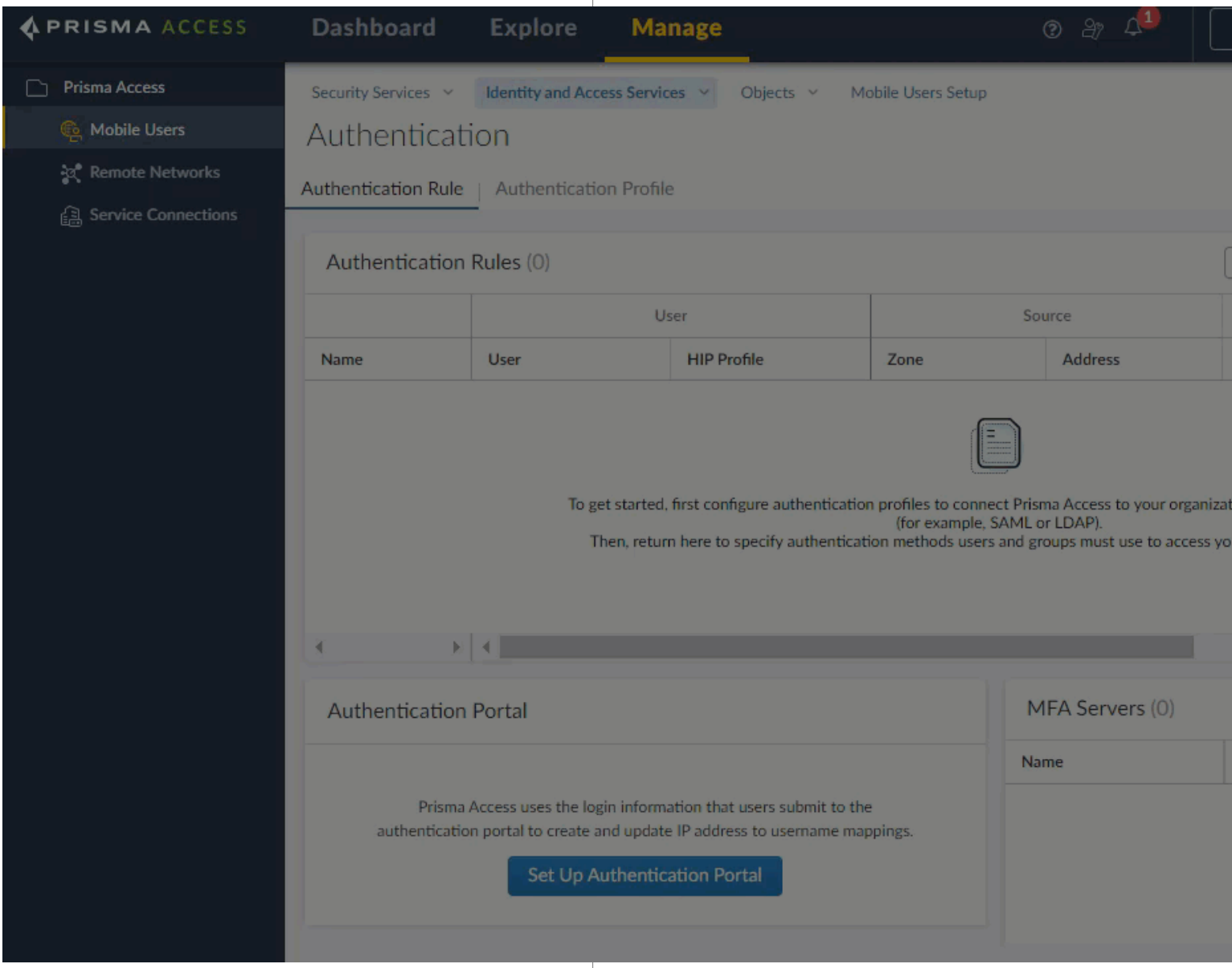
	configure la política de autenticación en su cortafuegos o Panorama.
SAML	Si sus usuarios acceden a los servicios y aplicaciones externos a su red, puede utilizar SAML para integrar Prisma Access con un proveedor de identidad (IdP) que controla el acceso a los servicios y aplicaciones externos e internos. El inicio de sesión único (SSO) de SAML permite un inicio de sesión para acceder a varias aplicaciones y es útil en entornos donde cada usuario accede a varias aplicaciones y la autenticación de cada uno impediría la producción de usuario. En este caso, el inicio de sesión único (SSO) de SAML permite que un inicio de sesión acceda a varias aplicaciones. De igual modo, el cierre de sesión único (single logout, SLO) de SAML le permite a un usuario finalizar sesiones de varias aplicaciones cerrando la sesión de una sola sesión. SSO funciona para usuarios móviles que acceden a aplicaciones a través de la aplicación GlobalProtect o usuarios en redes remotas que acceden a aplicaciones a través del Portal de autenticación. SLO está disponible para los usuarios de la aplicación GlobalProtect. *No puede utilizar los perfiles de autenticación de SAML en las secuencias de autenticación.*
TACACS+	El sistema de control de acceso del controlador de acceso a terminales (Terminal Access Controller Access-Control System Plus, TACACS+) es una familia de protocolos que permiten la autenticación y la autorización mediante un servidor centralizado. TACACS + cifra nombres de usuario y contraseñas, lo que lo convierte en una opción más segura que RADIUS, que solo cifra contraseñas. TACACS + es más fiable dado que utiliza TCP, mientras que RADIUS utiliza UDP.
RADIUS	El servicio de autenticación remota telefónica de usuario (RADIUS) es un protocolo de red ampliamente admitido que brinda autenticación y autorización centralizadas. También puede añadir un servidor RADIUS

 ©2025 Palo Alto Networks, Inc.

	a Prisma Access para implementar la autenticación multifactor.
LDAP	El protocolo ligero de acceso a directorios (LDAP) es un protocolo estándar para acceder a directorios de información. Puede utilizar LDAP para autenticar a los usuarios que accedan a aplicaciones o servicios a través del Portal de autenticación.
Kerberos	Kerberos es un protocolo de autenticación que permite un intercambio seguro de información entre las partes utilizando claves únicas (denominadas vales) para identificar a las partes. Con Kerberos, puede autenticar a los usuarios que acceden a las aplicaciones a través del Portal de autenticación. Si el SSO de Kerberos está habilitado, el usuario solo debe iniciar sesión durante el acceso inicial a su red (como iniciar sesión en Microsoft Windows). Tras este inicio de sesión inicial, el usuario podrá acceder a cualquier servicio basado en el explorador de la red sin tener que iniciar sesión de nuevo hasta que venza la sesión con SSO. Para usar Kerberos, primero necesita una cuenta de Kerberos para Prisma Access que autenticará a los usuarios. Se requiere una cuenta para crear un keytab de Kerberos, que es un archivo que contiene el nombre principal y una contraseña con hash del cortafuegos o Panorama. El proceso de SSO requiere un keytab. El SSO de Kerberos se encuentra disponible solo para los servicios y las aplicaciones internas de su entorno de Kerberos. Para habilitar el SSO para los servicios y las aplicaciones externas, utilice SAML.
MFA	La autenticación multifactor (MFA) le ofrece una forma de implementar múltiples desafíos de autenticación de diferentes tipos (estos se llaman *factores*) para proteger sus servicios y aplicaciones más sensibles. Por ejemplo, es posible que desee una autenticación más sólida para los documentos financieros clave que para los motores de búsqueda. Prisma Access tiene una lista integrada de proveedores de MFA compatibles que se

 ©2025 Palo Alto Networks, Inc.

actualiza automáticamente a medida que se añaden nuevos proveedores:



Autenticación de base de datos local

Cree una base de datos que se ejecute localmente en Prisma Access e incluya cuentas de usuario (nombres de usuario y contraseñas o contraseñas hash) y grupos de usuarios. Este tipo de autenticación es útil para la creación de cuentas de usuario que reutilizan las credenciales de las cuentas Unix existentes en casos donde solo conoce las contraseñas con hash, no las contraseñas en texto normal. En el caso de las cuentas que utilizan contraseñas en texto normal, también puede realizar el paso Defina la complejidad de la contraseña y la

 ©2025 Palo Alto Networks, Inc.

	configuración del vencimiento. Este método de autenticación está disponible para los usuarios que acceden a servicios y aplicaciones a través del Portal de autenticación o la aplicación GlobalProtect.

Aspectos destacados de la característica de autenticación

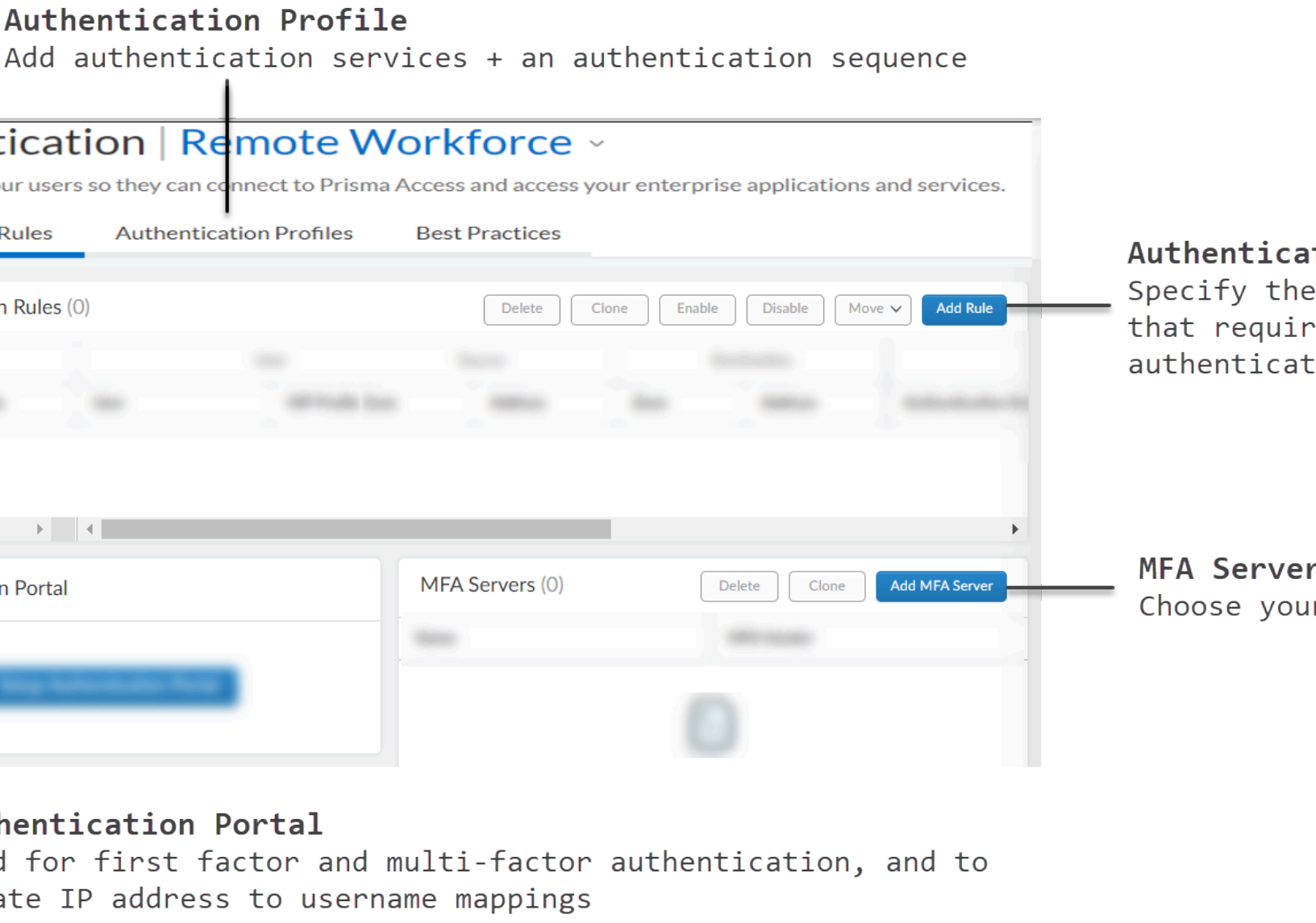
SSO	Si utiliza SAML o Kerberos, puede implementar el inicio de sesión único (SSO), que permite a los usuarios autenticarse solo una vez para acceder a varios servicios y aplicaciones. SAML y Kerberos admiten el SSO.
Portal de autenticación	Redirija las solicitudes web que coinciden con una regla de autenticación a una página de inicio de sesión de Prisma Access donde se les solicita que se autentiquen. Prisma Access utiliza la información que el usuario envía a este portal de autenticación para crear o actualizar asignaciones de direcciones IP a nombres de usuario. Esto es especialmente útil para las redes remotas, de modo que continúe supervisando y haciendo cumplir el tráfico basado en un usuario (o grupo). Cuando un usuario inicia tráfico web (HTTP o HTTPS) que coincide con una regla de autenticación, Prisma Access solicita al usuario que se autentique a través del portal de autenticación. Prisma Access crea o actualiza la asignación de la dirección IP al nombre de usuario en función de la información que el usuario envía al portal. Esto garantiza que conozca exactamente quién accede a sus aplicaciones y datos más delicados desde un sitio de red remoto.
Secuencia de autenticación	Si utiliza varios tipos de autenticación para diferentes propósitos, puede establecer una secuencia de autenticación para clasificar sus perfiles. Prisma Access verifica cada perfil en función de su clasificación hasta que uno autentica correctamente al usuario.

©2025 Palo Alto Networks, Inc.

Configurar la autenticación

Para establecer la autenticación con Prisma Access, primero añada sus servicios de autenticación a Prisma Access. A continuación, especifique el tráfico para el que desea requerir autenticación. Desarrolle en base a estos ajustes para añadir más funciones de autenticación, como MFA, secuencias de autenticación o habilite Prisma Access para crear y actualizar la dirección IP a las asignaciones de nombres de usuario.

Así es cómo empezar: todos los ajustes que necesita para habilitar la autenticación con Prisma Access están en un único lugar: **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)**. Seleccione el ámbito de configuración de **Prisma Access**.



 ©2025 Palo Alto Networks, Inc.

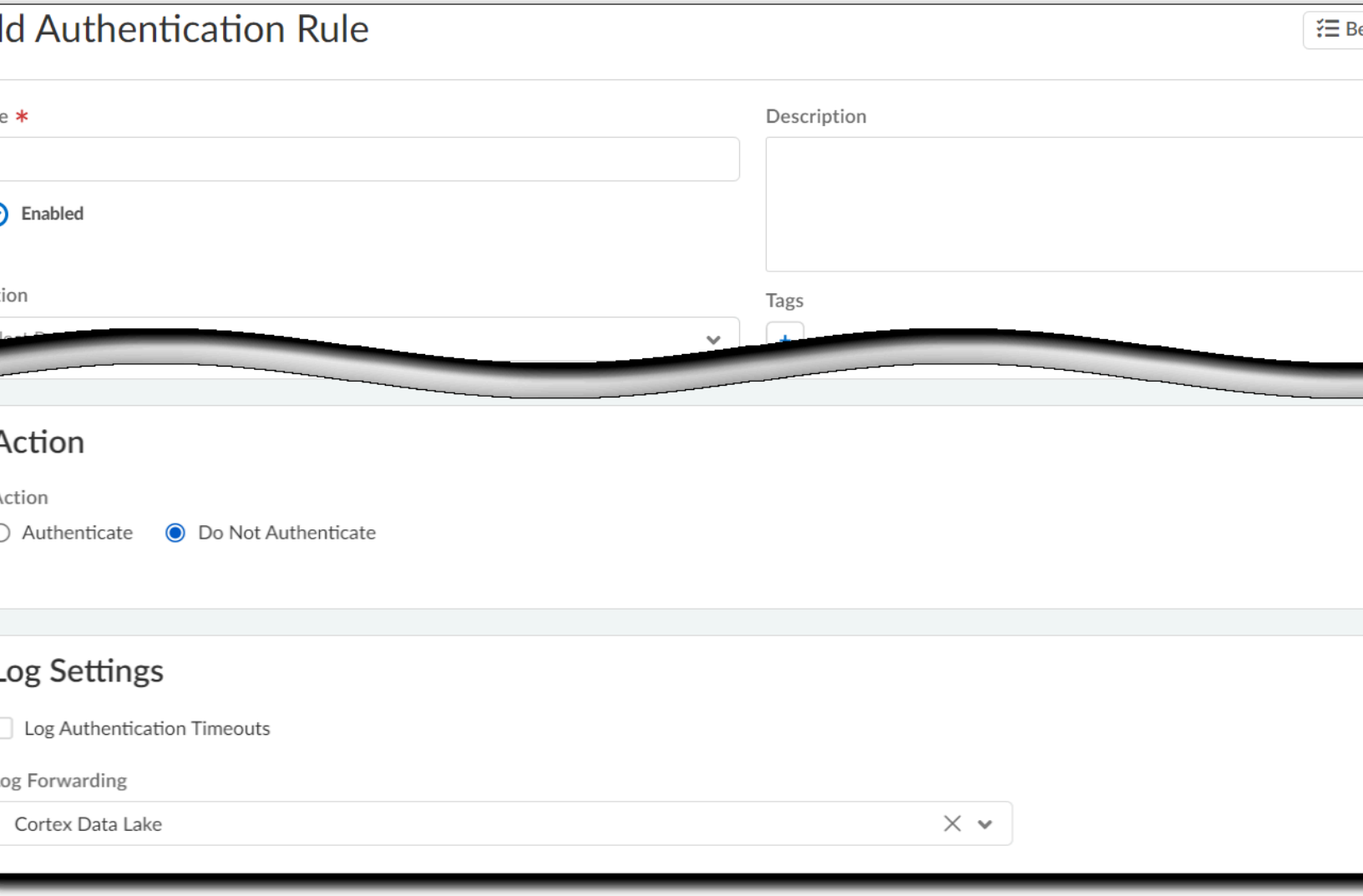
- **Reglas de autenticación** Aquí es donde especifica el tráfico para el que desea requerir autenticación

  Parte de la configuración de una regla de autenticación incluye añadir un perfil de autenticación a la regla. Cuando Prisma Access detecta tráfico que coincide con una regla de autenticación, aplica los métodos y configuraciones de autenticación definidos en el perfil de autenticación al tráfico coincidente. El perfil es lo que define cómo se requerirá que los usuarios se autentiquen.

  1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)** > **Authentication Rule (Regla de autenticación)** y **Add Authentication Rule (Añadir regla de autenticación)**. Seleccione el ámbito de configuración de **Prisma Access**
  2. Defina los usuarios, servicios y categorías de URL que requieren autenticación.

 ©2025 Palo Alto Networks, Inc.

3. Establezca la acción de regla en **Authenticate (Autenticación)** y elija el **Profile (Perfil)** que define el método de autenticación que desea utilizar para el tráfico que coincida con esta regla.



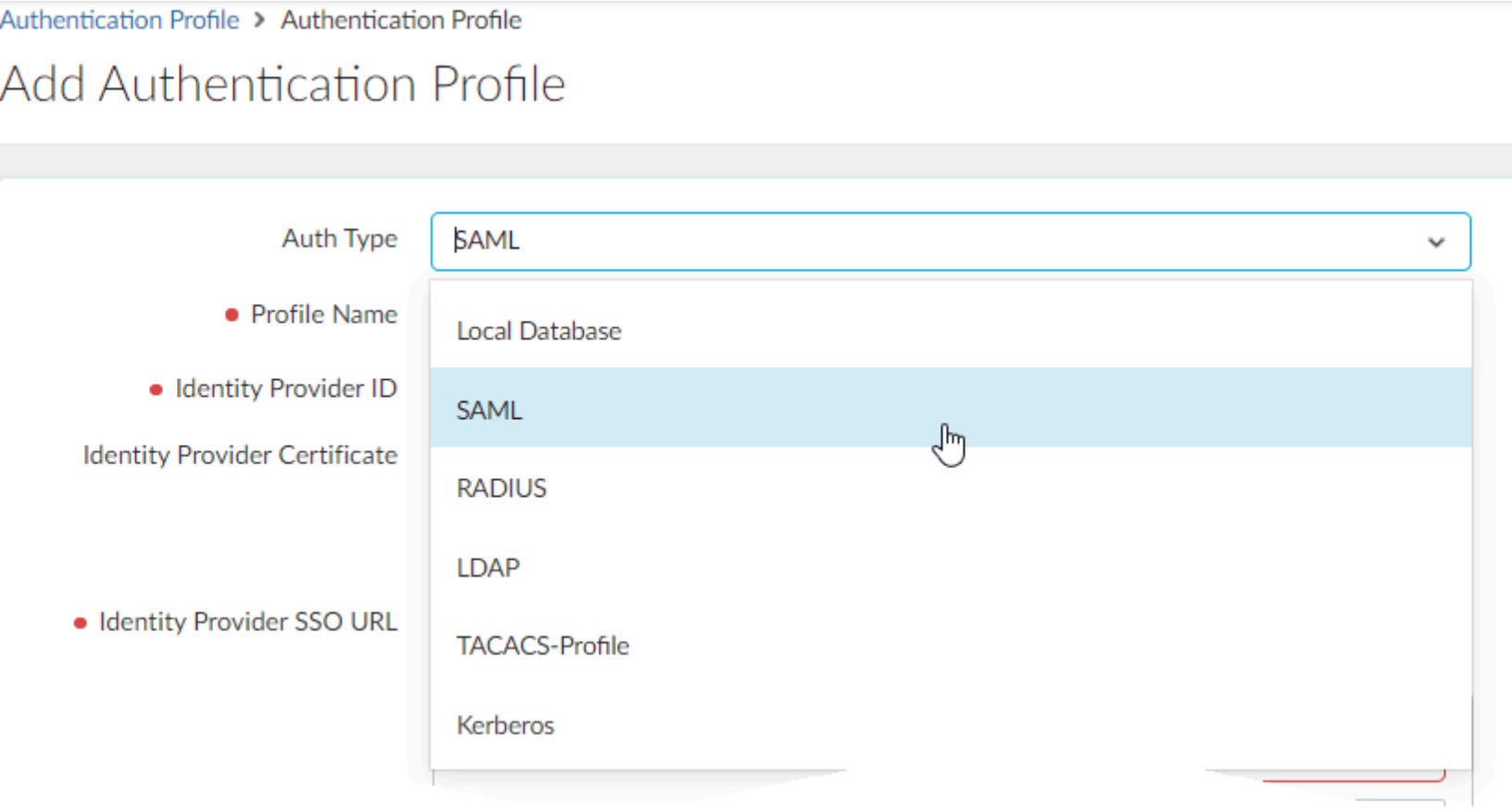
 ©2025 Palo Alto Networks, Inc.

- **Perfil de autenticación** Añada sus servicios de autenticación aquí y defina la configuración de autenticación

  Conecte Prisma Access a los servicios que desea utilizar para autenticar usuarios (SAML, TACACS+, RADIUS, LDAP o Kerberos) y defina la configuración de autenticación (por ejemplo, establezca un límite para los intentos fallidos de inicio de sesión).

  > *Si está utilizando un servicio de autenticación local, primero debe crear una conexión de servicio para conectar el servicio de autenticación local a Prisma Access. Luego, regrese aquí para configurar su perfil de autenticación.*

  Vaya a **Manage (Gestionar)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)** > **Authentication Profile (Perfil de autenticación)** > **Add Profile (Añadir perfil)** y empiece por establecer el perfil en **Auth Type (Tipo de autenticación)**. Seleccione el ámbito de configuración de **Prisma Access**

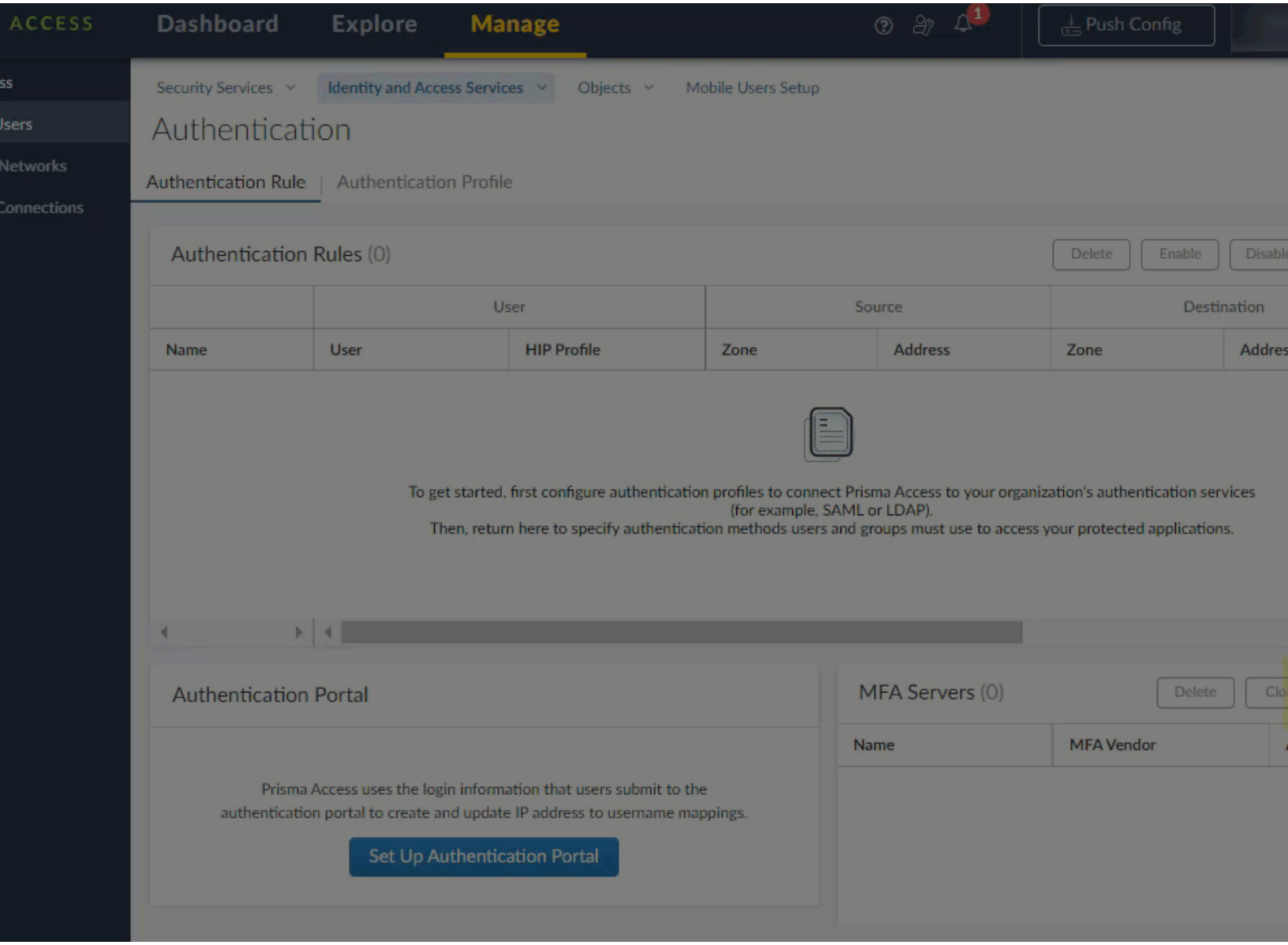


  Se le pedirá que añada detalles sobre el servicio de autenticación que seleccionó para permitir que Prisma Access se conecte al servicio y lea las credenciales de usuario y los permisos de rol. En el perfil se proporcionan ajustes adicionales para personalizar la autenticación, que pueden variar según el tipo de autenticación que esté configurando.

 ©2025 Palo Alto Networks, Inc.

- **Servidores MFA** Especifique el proveedor de MFA que está utilizando

  Para utilizar varios métodos para autenticar a los usuarios en aplicaciones sensibles, comience añadiendo los proveedores de MFA que desea utilizar (**Add MFA Server (Añadir servidor MFA**). Prisma Access proporciona una lista de proveedores de MFA para que usted pueda elegir.



- **Portal de autenticación**: configure el portal de autenticación (anteriormente conocido como *Portal cautivo*) para usuarios en sitios de red remotos y habilite Prisma Access para crear asignaciones de direcciones IP a nombres de usuario

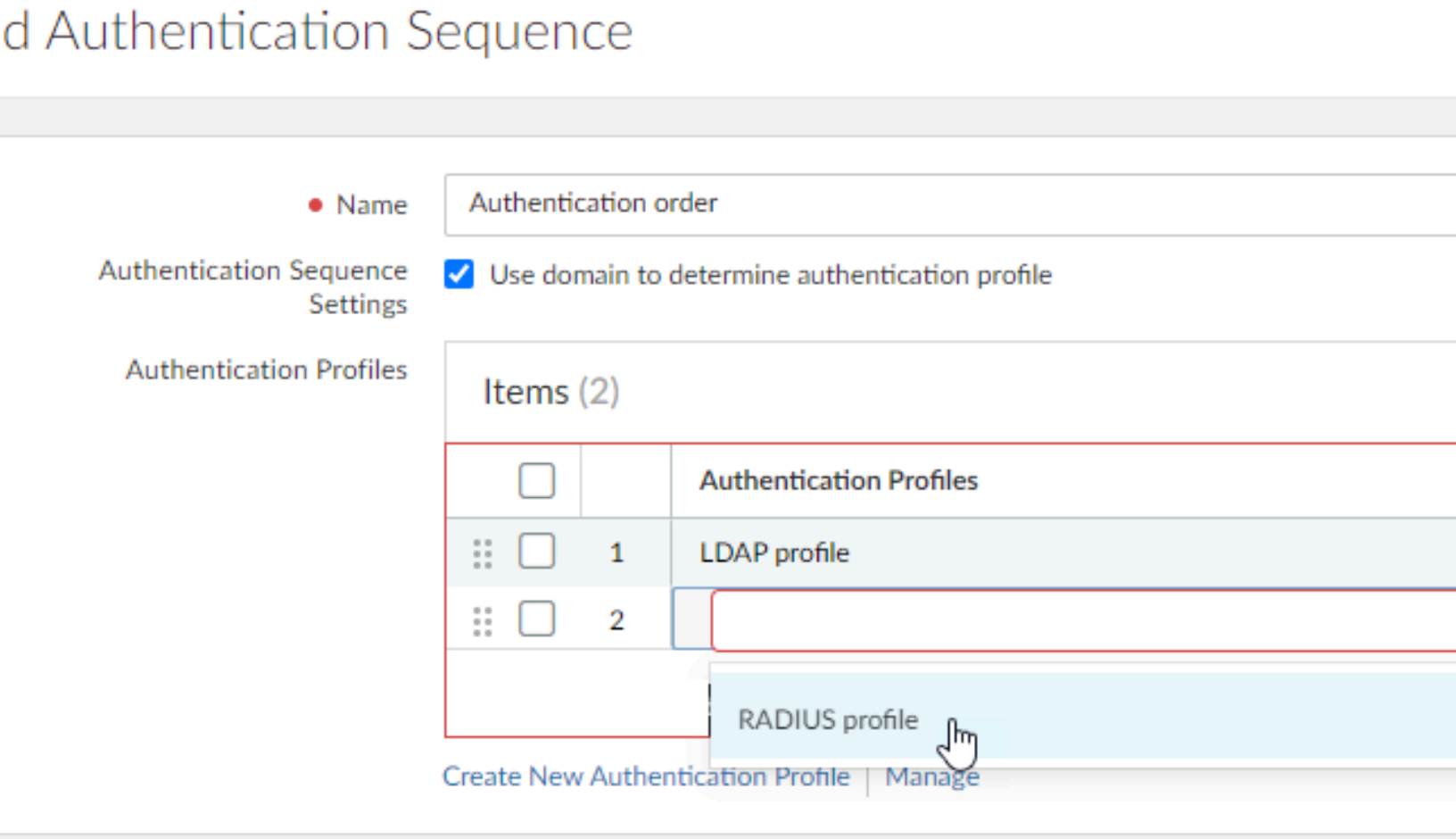
  Para la autenticación de un único factor (login y contraseña), los usuarios en sitios de red remotos deben autenticarse a través del portal de autenticación. Si la autenticación tiene éxito, Prisma Access muestra una página de inicio de sesión de MFA para cada factor de autenticación adicional que se requiere. Prisma Access utiliza las credenciales que envían los usuarios para crear y actualizar las asignaciones de direcciones IP a nombres de usuario. Esto

 ©2025 Palo Alto Networks, Inc.

significa que siempre sabrá quién en un sitio de red remoto está accediendo a contenido web y aplicaciones empresariales.

- **Secuencia de autenticación** Clasifique los perfiles de autenticación en el orden en que desee que Prisma Access los pruebe

  Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Authentication (Autenticación)** > **Authentication profile (Perfil de autenticación)** > **Add Authentication sequence (Añadir secuencia de autenticación)**. Seleccione el ámbito de configuración de **Prisma Access**. Prisma Access comprueba cada uno de ellos en secuencia hasta que uno autentica correctamente al usuario.



 ©2025 Palo Alto Networks, Inc.

Permitir a los usuarios móviles acceder a los recursos corporativos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Licencia de Prisma Access

Para habilitar Prisma Access y permitir el acceso a Internet solo para los usuarios, no es necesario configurar ningún servicio de red porque Prisma Access proporciona un grupo de direcciones IP predeterminado y un servidor DNS predeterminado en la nube.

Sin embargo, si desea que sus usuarios móviles puedan acceder a recursos internos en su sede, centros de datos o en sitios de red remotos que ha incorporado a Prisma Access, tendrá que:

- ❑ definir los grupos de direcciones IP que Prisma Access utiliza para asignar direcciones IP a sus usuarios móviles,
- ❑ establecer la infraestructura de servicios de Prisma Access,
- ❑ y, permitir el acceso a su sede o centros de datos, incorporar conexiones de servicio.

Si desea que sus usuarios móviles se conecten a sitios de red remotos, debe configurar al menos una conexión de servicio, incluso si no planifica usar la conexión para proporcionar acceso a sus ubicaciones de centros de datos o de la sede. Aunque todas las sucursales están completamente en malla, las conexiones de usuarios móviles no lo están. La creación de una conexión de servicio establece la arquitectura hub-and-spoke (concentrador y radio) necesaria para permitir que el tráfico de usuarios móviles se enrute a las redes de sucursales. En este caso, puede configurar mínimamente la conexión de servicio de la siguiente manera:

- Cuando incorpora la conexión de servicio, utiliza una ubicación de Prisma Access cercana a los usuarios móviles.
- Cuando configure el túnel IPSec primario para la conexión de servicio, configure la autenticación de peers IPSec y la configuración del túnel mediante valores de marcador de posición.
- Cuando habilite el enrutamiento y la QoS para la conexión de servicio, añada subredes IP de marcador de posición.

  Dado que Prisma Access no enruta ningún tráfico a través de este túnel, solo asegúrese de que la subred IP que utiliza no entre en conflicto o se solape con otras subredes configuradas y conectadas a Prisma Access.

STEP 1 | Vaya a **Manage (Gestionar)** > **Mobile Users (Usuarios móviles)** > **Mobile Users Setup (Configuración de usuarios móviles)** y edite **Infrastructure Settings (Configuración de infraestructura)** para ajustar la configuración de red de los usuarios móviles.

©2025 Palo Alto Networks, Inc.

STEP 2 | Revise o ajuste el **Client IP Pool (Grupo de direcciones IP cliente)** que Prisma Access utiliza para asignar direcciones IP a usuarios móviles.

- De forma predeterminada, todos los usuarios móviles disponen de un grupo de direcciones IP **Worldwide (mundial)**.
- Puede **Customize per region (Personalizar por región)** para usar un grupo de direcciones IP dedicado a regiones o ubicaciones. Para las regiones o ubicaciones que no especifican un grupo de direcciones IP, Prisma Access utiliza el grupo de direcciones IP mundial.

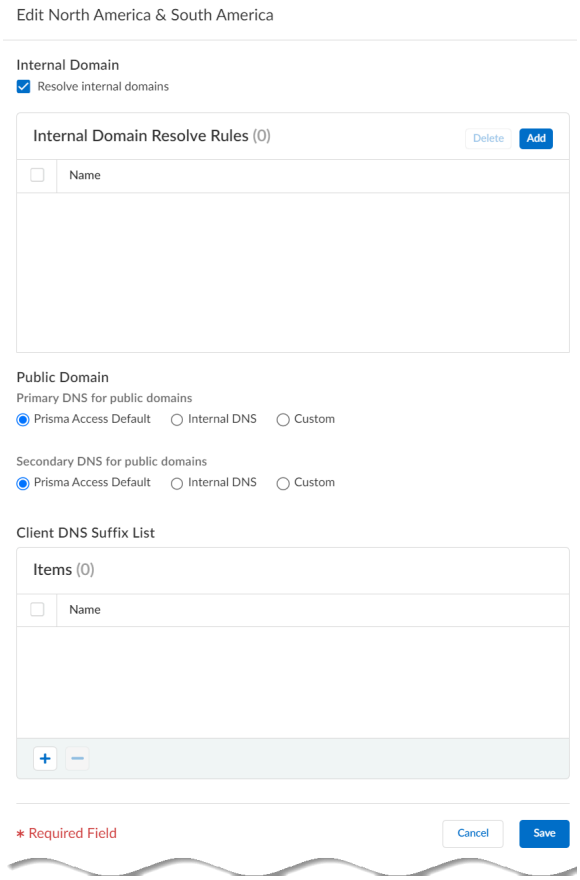
Los grupos de direcciones IP que defina deben cumplir los siguientes requisitos:

- ❑ Como práctica recomendada, defina grupos de direcciones IP compatibles con RFC 1918 para evitar conflictos de direcciones IP.
- ❑ Asegúrese de que los grupos de direcciones IP que defina no se solapen con otras direcciones IP que utilice internamente.
- ❑ Asegúrese de que los grupos de direcciones IP que defina no se solapen con el grupo de direcciones IP de infraestructura que está utilizando para Prisma Access.
- ❑ No especifique ninguna subred que se solape con 169.254.0.0/16 y el rango de subredes 100.64.0.0/10, porque Prisma Access reserva esas direcciones IP y subredes para su uso interno.
- ❑ Asegúrese de designar un grupo de direcciones IP que permita suficiente cobertura para todos los usuarios móviles de su organización, según las siguientes directrices:
- ❑ Si planifica usar un grupo de direcciones de Worldwide implementado en una o dos regiones, el grupo de direcciones IP mínimo requerido es /23 (512 direcciones IP).
- ❑ Si planifica utilizar un grupo de direcciones de ámbito mundial implementado en tres o más regiones, el grupo de direcciones IP mínimo requerido es /19 (8.192 direcciones IP), ya sea en un solo grupo de direcciones IP o en varios grupos.
- ❑ Si planifica definir grupos de direcciones IP por región, el tamaño mínimo de grupo en cualquier región es /23 (512 direcciones IP).
- ❑ No es necesario asignar un grupo de direcciones IP en regiones donde no se planea implementar Prisma Access. Por ejemplo, seleccione las regiones Este de los Estados Unidos (N. Virginia), Este de los Estados Unidos (Ohio) y Oeste de los Estados Unidos (N. California), regiones solo cuando incorpore Prisma Access para los usuarios, debe especificar un grupo de direcciones IP solo para la región de las Américas. Sin embargo, tenga en cuenta que los usuarios de otras regiones no podrán conectarse a Prisma Access.
- ❑ Si planifica definir una combinación de agrupaciones regionales y mundiales, asegúrese de asignar al menos 512 direcciones IP por región. Por ejemplo, para una implementación de tres regiones, puede especificar 1.024 direcciones en la región de Europa y 512 direcciones en todo el mundo.
- ❑ Como práctica recomendada, designe grupos de direcciones IP para que tenga al menos una dirección IP para cada usuario móvil único de su organización de forma que puedan iniciar sesión simultáneamente. Si designa un grupo de direcciones IP que tiene un número menor de direcciones IP que el número de usuarios con licencia, Prisma Access mostrará un mensaje de advertencia. Sin embargo, si tiene un grupo limitado de direcciones IP y no espera que todos los usuarios inicien sesión al mismo tiempo, puede omitir el mensaje y usar un grupo de tamaño más pequeño.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Añada la configuración de **Client DNS (DNS de cliente)**: puede usar la configuración predeterminada de **Worldwide (Mundial)** o personalizarla según la región.

Seleccione la región para la que desea personalizar la configuración DNS:



Marque la opción de usar esta configuración DNS para **Resolve internal domains (Resolver dominios internos)** y, opcionalmente **Use the internal DNS Server for resolving public domains too (Utilice también el servidor DNS interno para resolver dominios públicos)**. Si no selecciona esta opción, Prisma Access utiliza su DNS predeterminado en la nube para resolver solicitudes de dominios públicos.

El proxy DNS en Prisma Access envía las solicitudes a los servidores DNS que usted especifique. La dirección de origen en la solicitud DNS es la primera dirección IP en el grupo de IP que asigna a la región. Para garantizar que sus solicitudes de DNS puedan llegar a los servidores, deberá asegurarse de permitir el tráfico desde todas las direcciones en su grupo de direcciones IP de usuarios móviles a sus servidores DNS.

STEP 4 | Si desea que sus usuarios móviles puedan acceder a los recursos en sus redes de la sede o del centro de datos, o en otras ubicaciones de sucursal, debe configurar la configuración de infraestructura de Prisma Access para habilitar la red troncal.

Vaya a **Manage (Gestionar)** > **Prisma Access** > **Prisma Access Setup (Configuración de Prisma Access)**.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Para que los usuarios móviles puedan acceder a los recursos de su sede o centros de datos, cree conexiones de servicio para conectar estos sitios a Prisma Access.

Vaya a **Manage (Gestionar)** > **Service Connections (Conexiones de servicio)** > **Service Connections Setup (Instalación de conexiones de servicio)**.

STEP 6 | Cuando esté listo, debe **Push Config (Enviar configuración)** a Prisma Access para guardar la configuración del usuario móvil.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Redes remotas de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

A medida que su negocio crece y sus ubicaciones de oficina se distribuyen geográficamente, Prisma Access para redes le permite incorporar rápidamente sus ubicaciones de red remotas y ofrecer la mejor seguridad para sus usuarios. Ofrece una opción conveniente que elimina la complejidad en la configuración y gestión de dispositivos en cada ubicación remota. El servicio proporciona una forma eficiente de añadir fácilmente nuevas ubicaciones de red remotas y minimizar los desafíos operativos para garantizar que los usuarios en estas ubicaciones estén siempre conectados y seguros. Y permite gestionar la política de forma central desde Panorama para una seguridad coherente y optimizada para sus ubicaciones de red remotas.

Para conectar sus ubicaciones de red remotas a Prisma Access, puede utilizar el cortafuegos de nueva generación de Palo Alto Networks o un dispositivo de terceros compatible con IPSec, incluyendo SD-WAN, que puede establecer un túnel IPSec al servicio.

Además de la conectividad del túnel IPSec, Prisma SD-WAN le permite usar un CloudBlade que incorpora como una red remota para integrar el controlador de Prisma SD-WAN y los dispositivos ION con Prisma Access.

Lista de verificación de planificación para redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Antes de comenzar a incorporar redes remotas, asegúrese de tener listos los siguientes elementos de configuración para asegurarse de que podrá habilitar correctamente el servicio y hacer cumplir la política para los usuarios en sus ubicaciones de red remotas:

- ❑ **¿Solicitar acceso a recursos corporativos?**

  Si su red remota requiere acceso a la infraestructura o recursos en su sede o un centro de datos, cree una conexión de servicio de Prisma Access con el sitio corporativo. Si la ubicación remota de la red es autónoma y no necesita acceder a la infraestructura en otras ubicaciones, no necesita hacerlo.

- ❑ **Prisma Access Ubicaciones**

  Cuando los usuarios de su sucursal se conectan a Prisma Access, la ubicación de Prisma Access que elija determina el idioma en el que se publica el contenido de Internet. Para obtener la mejor experiencia del usuario, seleccione la región y la ubicación en el mismo condado que su sucursal para garantizar la mejor experiencia para sus usuarios. Si una ubicación no está disponible en el mismo país que su sucursal, elija una ubicación que use el mismo idioma que la mayoría de los usuarios del sitio.

  Pocas ubicaciones están marcadas como **Local Zones (Zonas locales)**. Estas ubicaciones proporcionan ubicaciones de cómputo de Prisma Access cerca de grandes centros de población e industria.

- ❑ **Subredes IP**

  Para que Prisma Access enrute el tráfico a sus redes remotas, deberá proporcionar información de enrutamiento para las subredes que desea que Prisma Access proteja. Puede hacerlo de varias maneras. Puede definir una ruta estática para cada subred en el sitio de red remoto o configurar BGP entre las ubicaciones de conexión de su servicio y Prisma Access, o utilizar una combinación de ambos métodos. Si configura ambas rutas estáticas y habilita BGP, las rutas estáticas tienen prioridad. Si bien puede ser conveniente utilizar rutas estáticas, si solo tiene unas pocas subredes en sus ubicaciones de red remotas, en una implementación grande con redes remotas con subredes superpuestas, BGP le permitirá ampliar más fácilmente.

- ❑ **Modelo de ancho de banda agregado**: el ancho de banda para sus ubicaciones de redes remotas se asigna a un nivel agregado por ubicación de cómputo. Cada ubicación que incorpora tiene una ubicación de cómputo correspondiente para la cual se asigna ancho de banda. Asigna ancho de banda por ubicación de cómputo, en lugar de por ubicación. Este método se conoce como el *modelo de ancho de banda agregado*.

  El modelo de ancho de banda agregado está disponible para todas las implementaciones nuevas. Si tiene una implementación existente que asignó ancho de banda por ubicación,

 ©2025 Palo Alto Networks, Inc.

puede migrar de asignar ancho de banda por ubicación a asignar ancho de banda por ubicación de cómputo.



Antes de migrar al modelo de ancho de banda agregado, debe revisar Planifique su migración al nuevo modelo.

Todas las ubicaciones incorporadas comparten el ancho de banda asignado para esa ubicación de cómputo. Por ejemplo, necesita incorporar cuatro oficinas sucursales utilizando redes remotas en las ubicaciones de Singapur, Tailandia y Vietnam. Todas estas ubicaciones se asignan a la ubicación de cómputo del sudeste asiático. Si asignas 200 Mbps de ancho de banda a la ubicación de cómputo del sudeste asiático, Prisma Access divide los 200 Mbps de ancho de banda entre las cuatro oficinas sucursales que incorporó en esa ubicación. Si también añade una ubicación en Hong Kong, notará que Hong Kong se corresponde con la ubicación de cómputo de Hong Kong, y necesitaría añadir ancho de banda a esa ubicación de cómputo. Especifique un ancho de banda mínimo de 50 Mbps por ubicación de cómputo.

Prisma Access asigna dinámicamente el ancho de banda según la carga o la demanda por ubicación. Usando el ejemplo anterior donde los cuatro sitios utilizan colectivamente hasta 200 Mbps, si uno o más sitios no están utilizando tanto ancho de banda como los otros sitios, Prisma Access proporciona más ancho de banda para las ubicaciones que están más en demanda, dándole un uso más eficiente del ancho de banda asignado. Además, si uno de los sitios se cae, Prisma Access redistribuye el ancho de banda entre los otros sitios que aún están activos en esa ubicación de cómputo.

Las ubicaciones marcadas como **Local Zones (Zonas locales)** admiten un ancho de banda máximo de 500 Mbps para redes remotas. Para soportar un ancho de banda de 1 Gbps póngase en contacto con la asistencia de Palo Alto Networks. Estas ubicaciones proporcionan ubicaciones de cómputo de Prisma Access cerca de grandes centros de población e industria; sin embargo, también tienen algunas limitaciones. Para añadir una zona local, póngase en contacto con su representante de Palo Alto Networks.

- Si tiene problemas para acceder a las URL, informe del problema del sitio web a la asistencia de Palo Alto Networks.
- **Directrices de tamaño y consideraciones de asignación de ancho de banda**

  Al calcular la cantidad de ancho de banda que necesita en un sitio, considere que el uso del ancho de banda incluye tanto el tráfico de salida como el de entrada para la conexión de red remota (es decir, el ancho de banda asignado es la suma de la entrada y la salida), y todas las ubicaciones que integran comparten el ancho de banda asignado para esa ubicación de cómputo. Para ayudarle a determinar cuánta ancho de banda necesita un sitio específico, considere el ancho de banda disponible de su ISP en cada ubicación.
- **Subredes superpuestas**

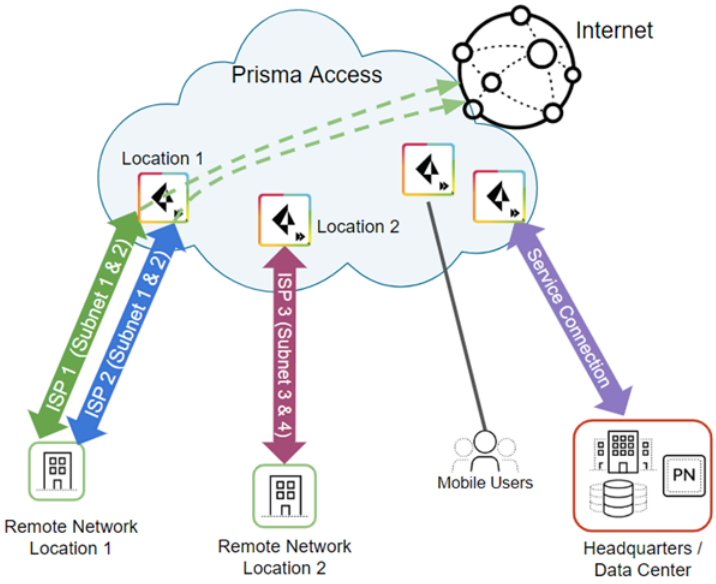
  Generalmente, no puede tener ninguna subred superpuesta dentro de una instancia de Prisma Access. Es decir, las subredes para todas las ubicaciones de red remotas, sus conexiones de servicio y su Prisma Access para grupos de direcciones IP de usuarios móviles no se pueden superponer. Sin embargo, en algunas circunstancias no puede evitar tener subredes superpuestas, por ejemplo, si ha adquirido una empresa que usa subredes que se superponen con sus subredes existentes. En algunos casos, es posible que desee configurar dos regiones

 ©2025 Palo Alto Networks, Inc.

con subredes superpuestas por diseño; por ejemplo, si desea crear una red de invitados independiente en un comercio minorista con reglas de políticas diferentes.

Prisma Access le permite incorporar ubicaciones de red remotas con subredes superpuestas, pero solo se admite el flujo de tráfico vinculado a Internet desde sucursales que tienen subredes superpuestas. Las sucursales que no tienen subredes superpuestas en el mismo inquilino reciben funcionalidad completa de Prisma Access. Consulte la tabla en la siguiente imagen para obtener más detalles.

Traffic Flow	Supported?
Remote Network to Internet	Yes
Remote Network to Remote Network (Overlapping Subnets)	No
Remote Network to Remote Network (No Overlapping Subnets)	Yes
Remote Network to HQ (Overlapping Subnets)	No
Remote Network to HQ (No Overlapping Subnets)	Yes
HQ to Remote Network (Overlapping Subnets)	No
Mobile Users to and from Remote Network (Overlapping Subnets)	No
Mobile Users to and from Remote Network (No Overlapping Subnets)	Yes



Sin embargo, tenga en cuenta que los sitios con subredes superpuestas tienen las siguientes limitaciones:

- No hay tráfico de red remota a red remota entrante. Las otras ubicaciones de red remotas no sabrían dónde enrutar el tráfico porque varias ubicaciones de red remotas enrutan a las mismas subredes. Sin embargo, los usuarios y servicios de cualquier ubicación remota de la red pueden acceder a los recursos de otras ubicaciones remotas de la red siempre que no haya subredes superpuestas en el sitio y que cualquier sitio pueda acceder a Internet a través de la infraestructura de Prisma Access.
- El tráfico de sus conexiones de servicio no puede acceder a recursos en ninguna ubicación de red remota con subredes superpuestas porque no sabría a qué ubicación de red remota enrutar el tráfico. Sin embargo, las ubicaciones de red remotas con subredes superpuestas pueden acceder a recursos desde conexiones de servicio.
- Los usuarios móviles no pueden acceder a los recursos en las ubicaciones de red remotas con subredes superpuestas, de nuevo debido a las limitaciones de enrutamiento entrante.

Si administra Prisma Access utilizando Strata Cloud Manager, vaya a ***Workflows (Flujos de trabajo) > Prisma Access Setup (Configuración de Prisma Access) > Remote Networks (Redes remotas) > Advanced Settings (Configuración avanzada)****. Edite la configuración de* ***Overlapped Subnets (Subredes superpuestas)*** *para habilitar las subredes superpuestas. Si está utilizando Panorama para gestionar Prisma Access, vaya a* ***Panorama > Cloud Services (Servicios en la nube) > Configuration (Configuración) > Remote Networks (Redes remotas)*** *y marque* ***Overlapped Subnets (Subredes superpuestas)****.*

 ©2025 Palo Alto Networks, Inc.

- **Nodos de terminación IPSec**: asigna un *nodo de terminación IPSec* a la red remota durante la incorporación. Puede especificar un máximo de 500 sitios de red remotos (para Prisma Access 5.0 y versiones posteriores) o 400 sitios de red remotos (para versiones de Prisma Access anteriores a 5.0) por nodo de terminación IPSec. Asigne más de 500 Mbps a la ubicación de cómputo que corresponde al nodo de terminación IPSec para admitir el número máximo de redes remotas permitidas.

  Puede tener un máximo de 200 nodos de terminación IPSec en una ubicación de cómputo. Cada nodo de terminación IPSec puede proporcionarle un máximo de 1.000 Mbps de ancho de banda. Si asigna más de 1.000 Mbps de ancho de banda a una ubicación de cómputo, Prisma Access le proporciona un nodo de terminación IPSec adicional.

  - **Nodos de terminación IPSec y actualizaciones de versiones anteriores a 3.2**: antes de 3.2, se asignaba un nodo de terminación IPSec por cada 500 Mbps de ancho de banda asignado en una ubicación de cómputo. Si tiene una implementación de red remota anterior a 3.2 y actualiza a una versión que sea 3.2.1 o posterior, y si las ubicaciones de red remotas tienen más de 500 Mbps asignados a su ubicación de cómputo correspondiente, cada red remota asociada con el nodo de terminación IPSec puede admitir hasta 1.000 Mbps de ancho de banda. Después de actualizar a 3.2 o posterior, Prisma Access implementa un nodo de terminación IPSec por cada 1.000 Mbps de ancho de banda asignado. Para las redes remotas existentes, Prisma Access puede aumentar el ancho de banda de una red remota mediante un mecanismo de escalado automático que se activa cuando el consumo de ancho de banda en la red remota requiere capacidad adicional. Consulte Cambios en el comportamiento predeterminado en las notas de la versión de Prisma Access (Panorama gestionado) para obtener más detalles.

    La asignación actual de nodo de terminación IPSec a red remota después de la actualización a 3.2 no cambia, y el número de nodos de terminación IPSec permanece igual. Los nodos de terminación IPSec se añaden o eliminan solo cuando aumenta o disminuye el ancho de banda para una ubicación de cómputo existente o cuando incorpora nuevas ubicaciones de cómputo para redes remotas.
- **Conexión de servicio**: si las ubicaciones de red remotas requieren acceso a la infraestructura de la sede corporativa para autenticar a los usuarios o habilitar el acceso a los activos de red críticos, debe crear una conexión de servicio para que la sede y las ubicaciones de red remotas estén conectadas. Si la ubicación de red remota es autónoma y no necesita acceder a la infraestructura en otras ubicaciones, no necesita configurar la conexión de servicio (a menos que sus usuarios móviles necesiten acceso).
- **Plantilla**: Prisma Access crea automáticamente una pila de plantillas (Remote_Network_Template_Stack) y una plantilla de nivel superior (Remote_Network_Template) para Prisma Access para redes. Para Incorporar y configurar redes remotas, deberá configurar la plantilla de nivel superior desde cero o aprovechar la configuración existente, si ya está ejecutando un cortafuegos de redes Palo Alto en las instalaciones. La plantilla requiere la configuración para establecer el túnel IPSec y la configuración de intercambio de claves de Internet (IKE) para la negociación de protocolos entre la ubicación de red remota y Prisma Access para redes, zonas a las que puede hacer referencia en la política de seguridad y un perfil de reenvío de logs para que pueda reenviar logs desde el Prisma Access para redes remotas al Strata Logging Service.
- **Configuraciones de túneles IPSec**: si tiene una plantilla existente que contiene configuraciones de túneles IPSec, monitorización de túneles y perfil criptográfico IPSec, puede añadir esa plantilla a Remote_Network_Template_Stack para simplificar el proceso de creación

 ©2025 Palo Alto Networks, Inc.

de los túneles IPSec. O bien, puede editar la Remote_Network_Template que se crea automáticamente y crear las configuraciones IPSec necesarias para crear el túnel IPSec de regreso al sitio corporativo. Prisma Access también le proporciona un conjunto de plantillas IPSec predefinidas para algunos dispositivos de red comúnmente utilizados y una plantilla genérica para cualquier dispositivo que no esté incluido en las plantillas predefinidas. Asegúrese de seguir las recomendaciones del túnel IPSec cuando configure el túnel de red remoto.

- **Determinar el método de enrutamiento (estático o dinámico)**: para que Prisma Access enrute el tráfico a sus redes remotas, debe proporcionar información de enrutamiento para las subredes que desea proteger mediante Prisma Access. Puede hacerlo de varias maneras. Puede definir una ruta estática para cada subred en el sitio de red remoto o configurar BGP entre las ubicaciones de conexión de su servicio y Prisma Access, o utilizar una combinación de ambos métodos. Si configura ambas rutas estáticas y habilita BGP, las rutas estáticas tienen prioridad. Si bien puede ser conveniente utilizar rutas estáticas, si solo tiene unas pocas subredes en sus ubicaciones de red remotas, en una implementación grande con muchas redes remotas con subredes superpuestas, BGP le permitirá ampliar más fácilmente.
- **Grupo de dispositivos primario**:Prisma Access para las redes requiere que especifique un grupo de dispositivos primarios que incluirá su política de seguridad, perfiles de seguridad y otros objetos de política (como grupos de aplicaciones y objetos y grupos de direcciones), así como la política de autenticación para que Prisma Access para redes pueda imponer de forma coherente la política para el tráfico que se enruta a través del túnel IPSec a Prisma Access para redes. Deberá definir reglas y objetos de políticas en Panorama o utilizar un grupo de dispositivos existente para proteger a los usuarios en la ubicación remota de la red.

  Si usa un grupo de dispositivos existente que hace referencia a zonas, asegúrese de añadir la plantilla correspondiente que define las zonas a Remote_Network_Template_Stack. Al hacerlo, podrá completar la asignación de zonas cuando Incorpore y configure redes remotas.

 ©2025 Palo Alto Networks, Inc.

Asignar ancho de banda de red remota

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Se utilizan redes remotas para proteger ubicaciones de redes remotas, como sucursales, y usuarios en esas sucursales.

Las redes remotas están medidas, lo que significa que se asigna una cantidad específica de ancho de banda a la ubicación de cómputo y hay un coste asociado con este ancho de banda asignado.

A medida que se prepara para conectar redes remotas a Prisma Access, necesitará saber cuántos sitios incorporará junto con los requisitos de ancho de banda para cada uno.

Obtenga información sobre cómo asignar ancho de banda de red remota.

- Strata Cloud Manager
- Panorama

Asignar ancho de banda de red remota (Strata Cloud Manager)

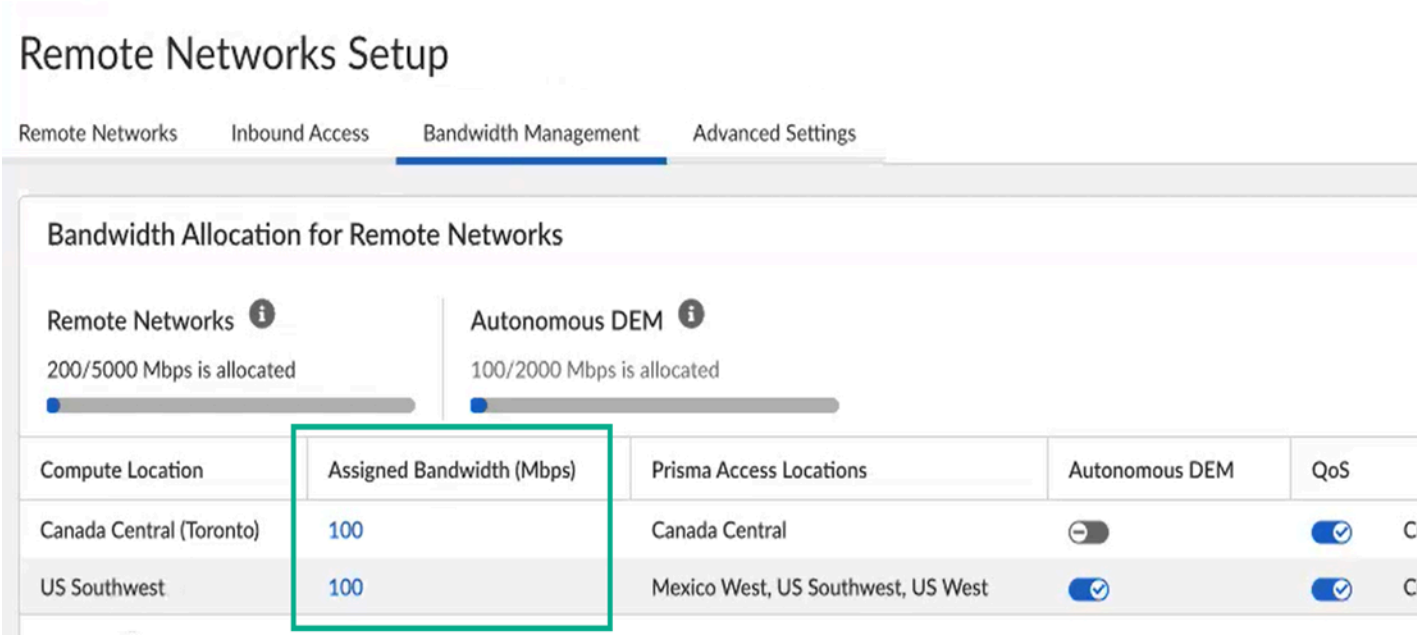
Al menos dos ubicaciones de Prisma Access (a menudo más) que están geográficamente cerca unas de otras se agrupan en *ubicaciones de cómputo*. Este es el nivel en el que asigna ancho de banda, en lugar de asignar ancho de banda para ubicaciones de Prisma Access individuales o para sitios de red remotos específicos. Significa que Prisma Access puede asignar dinámicamente ancho de banda a sitios en una ubicación de cómputo según la carga o la demanda.

Por ejemplo, necesita incorporar cuatro oficinas sucursales utilizando redes remotas en las ubicaciones de Singapur, Tailandia y Vietnam. Todas estas ubicaciones se asignan a la ubicación de cómputo del sudeste asiático. Si asignas 200 Mbps de ancho de banda a la ubicación de cómputo del sudeste asiático, Prisma Access divide los 200 Mbps de ancho de banda entre las cuatro oficinas sucursales que incorporó en esa ubicación. Si también añade una ubicación en Hong Kong, notará que Hong Kong se corresponde con la ubicación de cómputo de Hong Kong, y necesitaría añadir ancho de banda a esa ubicación de cómputo. Especifique un ancho de banda mínimo de 50 Mbps por ubicación de cómputo.

Prisma Access asigna dinámicamente el ancho de banda según la carga o la demanda por ubicación. Usando el ejemplo anterior donde los cuatro sitios utilizan colectivamente hasta 200 Mbps, si uno o más sitios no están utilizando tanto ancho de banda como los otros sitios, Prisma Access proporciona más ancho de banda para las ubicaciones que están más en demanda, dándole un uso más eficiente del ancho de banda asignado. Además, si uno de los sitios se cae, Prisma Access redistribuye el ancho de banda entre los otros sitios que aún están activos en esa ubicación de cómputo.

Para comenzar vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración)** > **Remote Networks (Redes remotas)** > **Bandwidth Management (Gestión de ancho de bandas**.

 ©2025 Palo Alto Networks, Inc.



Considera el ancho de banda que necesita cada sitio, cuando asigna ancho de banda según la ubicación.

Para ayudarle a determinar cuánta ancho de banda necesita un sitio específico, considere el ancho de banda disponible de su ISP en cada ubicación. Al calcular la cantidad de ancho de banda que necesita en un sitio, considere que el uso de ancho de banda incluye tanto el tráfico de salida como el de entrada para la conexión de red remota.

El acceso seguro entrante para sitios de red remotos y la Calidad de servicio (QoS) para redes remotas no son compatibles cuando asigna ancho de banda entre ubicaciones.

Asignar ancho de banda de red remota (Panorama)

Para configurar una implementación de red remota de Prisma Access que asigna ancho de banda por ubicación de cómputo, complete los siguientes pasos.

Si necesita incorporar muchas redes remotas (hasta 1000), puede incorporar una red remota mediante el siguiente procedimiento, luego exportar la configuración de la red remota a un archivo CSV, añadir las otras redes remotas que desea incorporar al archivo CSV y luego importar el archivo CSV para guardar la configuración en Prisma Access.

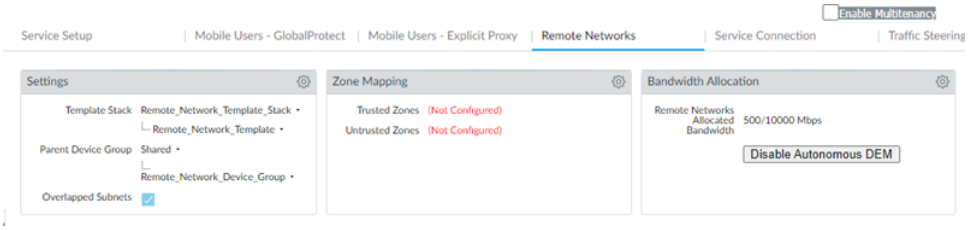
STEP 1 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Asigne ancho de banda a las ubicaciones que desea incorporar haciendo clic en el icono de engranaje en el área **Bandwidth Allocation (Asignación de ancho de banda)**.

Asigna ancho de banda a un nivel agregado por ubicación de cómputo. Consulte Redes remotas de Prisma Access para obtener más detalles.

*Si ha eliminado Autonomous DEM como licencia complementaria, o si elimina Autonomous DEM para redes remotas de su licencia, seleccione **Disable Autonomous DEM (Deshabilitar Autonomous DEM)**. Si elimina Autonomous DEM para redes remotas y no deshabilita Autonomous DEM, recibirá un error al confirmar.*



Si tiene una implementación de redes remotas existente que actualmente incorpora redes remotas por ubicación, una ventana emergente aparecerá que le preguntará si desea migrar al modelo de ancho de banda agregado. Haga clic en **Migrate (Migrar)** para continuar o en **Cancel (Cancelar)** para cancelar la migración.

*La migración al modelo de ancho de banda agregado es permanente e irreversible. Antes de migrar, revise la lista de verificación previa a la migración. Debe **Commit and Push (Confirmar y enviar)** sus cambios para que surtan efecto.*

La **Service IP Address (Dirección IP del servicio)** (el la dirección IP pública utilizada en el lado de Prisma Access del túnel IPSec para la conexión de red remota) no cambia cuando migra su implementación al modelo de ancho de banda agregado y no se requiere ninguna reconfiguración de su túnel IPSec.

STEP 3 | Introduzca la **Bandwidth Allocation (Asignación de ancho de banda)** que desea para cada **Compute Location (Ubicación de cómputo)** asociada con las **Prisma Access Locations (Ubicaciones de PA)** a las que desea incorporarse.

Para verificar la cantidad de ancho de banda introducido, seleccione la marca de verificación junto a la cantidad de ancho de banda; para cancelar la cantidad, seleccione **x**.

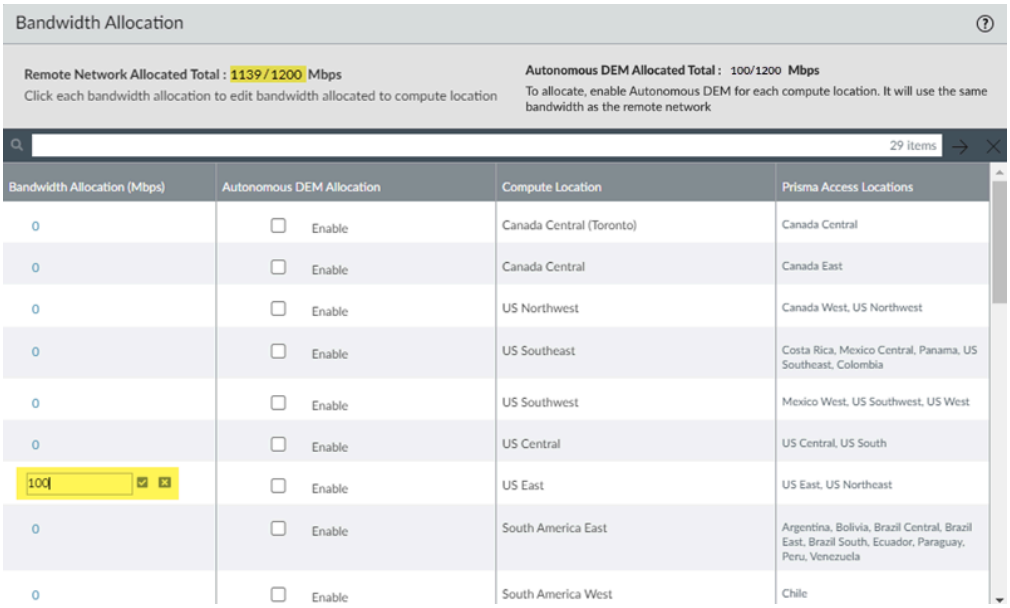
Especifique un ancho de banda mínimo de 50 Mbps y un ancho de banda máximo del ancho de banda máximo restante con licencia.

STEP 4 | (Opcional, solo implementaciones con licencias de Autonomous DEM para redes remotas) **Enable (Habilitar) Autonomous DEM Allocation (Asignación de Autonomous DEM)** para la ubicación de cómputo para la cual asignó ancho de banda.

Si habilita Autonomous DEM para la ubicación de cómputo, la cantidad de ancho de banda utilizada por la licencia de Autonomous DEM es la misma que el ancho de banda que especifica para la ubicación de cómputo. El **Autonomous DEM Allocated Total (Número total asignado de Autonomous DEM)** muestra cuánto ancho de banda utiliza Autonomous DEM y cuánto queda. Consulte la guía de Autonomous DEM para obtener más información.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Espere a que el ancho de banda se refleje en el campo **Allocated Total (Total asignado)** en la parte superior de la página; luego, haga clic en **OK (Aceptar)**.



STEP 6 | (Opcional) Si desea configurar su red remota para proporcionar acceso entrante seguro a ubicaciones de red remotas, haga clic en la pestaña **Inbound Access Remote Networks (Redes remotas de acceso entrante)** y siga el flujo de trabajo para configurar el acceso entrante seguro para una red remota.

STEP 7 | Seleccione **Add (Añadir)** para añadir una red remota y especifique un **Name (Nombre)**.

No puede cambiar el nombre de la ubicación de red remota después de introducirla. Asegúrese de conocer el esquema de nombres para sus redes remotas antes de comenzar la incorporación.

STEP 8 | (Opcional, solo implementaciones de BGP) Cree una configuración para que su conexión de red remota pueda usar hasta cuatro túneles IPSec para su tráfico [**ECMP Load Balancing (Equilibrio de carga ECMP)**].

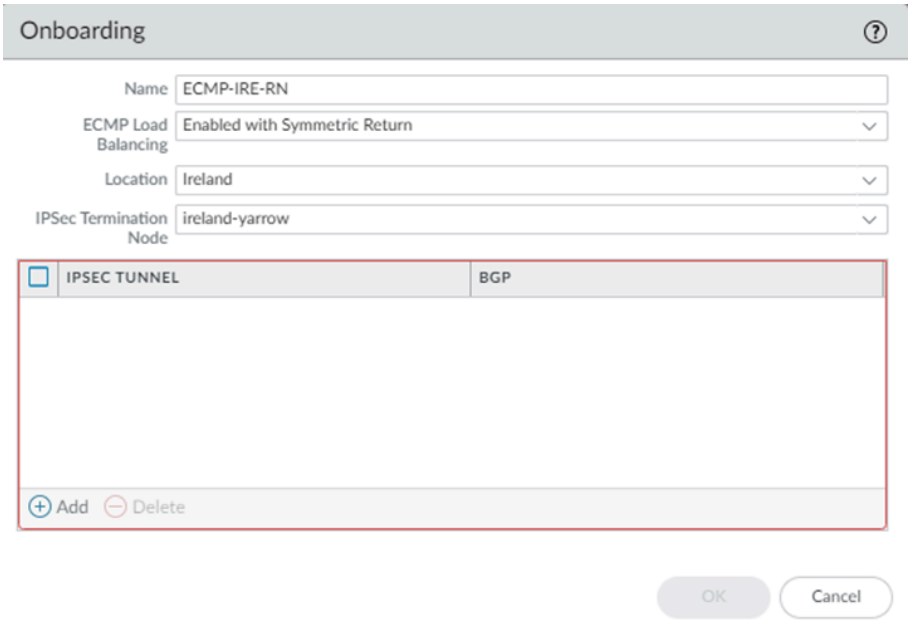
Las rutas estáticas (se requiere BGP) no son compatibles y, si tiene QoS configurado, no puede cambiar la ratio de asignación para los enlaces ECMP. Si su implementación utiliza un túnel IPSec para su conexión de red remota o utiliza rutas estáticas, seleccione **None (Ninguna)** para **ECMP Load Balancing (Equilibrio de carga ECMP)** y continúe con el Paso 11.

1. Seleccione una de las opciones para habilitar o deshabilitar el equilibrio de carga ECMP.
   - **None (Ninguno)**: no utilice el equilibrio de carga ECMP (utilice un único túnel de red remota para esta conexión de red remota). Esta es la única opción que puede elegir para las rutas estáticas; BGP es necesario para el equilibrio de carga de ECMP.
   - **Enabled with Symmetric Return (Habilitado con retorno simétrico)**: especifique hasta cuatro túneles IPSec para esta conexión de red remota y fuerce a Prisma Access

 ©2025 Palo Alto Networks, Inc.

a utilizar el mismo enlace para el tráfico de retorno que el utilizado para enviar el tráfico.

Seleccione esta opción si utiliza uno o más túneles como túnel de respaldo para usarlos solo si uno de los túneles principales deja de funcionar. Si un enlace falla, Prisma Access utiliza uno de los otros túneles para enviar y recibir tráfico simétricamente.



2. Seleccione **Add (Añadir)** para añadir un túnel IPSec para la conexión de red remota y especifique los siguientes valores:

   - **Enable (Habilitar)**: habilita BGP para el túnel IPSec.

     Esta selección no es configurable; debe habilitar BGP para configurar ECMP.

   - **Summarize Mobile User Routes before advertising (Resumir las rutas de los usuarios móviles antes de anunciarse)**: realiza un resumen para reducir el número de anuncios de subred IP de usuarios móviles a través de BGP a los equipos de las instalaciones del cliente (CPE).

     De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred especificada. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube

 ©2025 Palo Alto Networks, Inc.

(puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

Si habilita el resumen de ruta para una ubicación que usa ECMP, debe habilitar el resumen de ruta en todos los enlaces a esa ubicación o recibirá un error durante la confirmación.

Prisma Access establece la cadena de comunidad para las rutas de usuarios móviles agregadas en `0xFFFE:0xFFF0`.

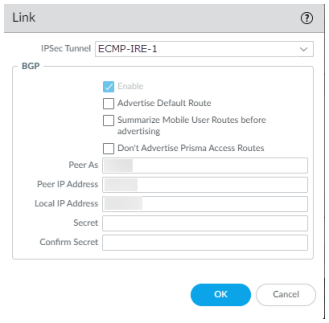
- **Advertise Default Route (Publicitar ruta predeterminada)**: Prisma Access origina un anuncio de ruta predeterminado para la red remota utilizando eBGP.

  Asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.

- **Don't Advertise Prisma Access Route (No anunciar ruta de Prisma Access)**: impide que el peer BGP de Prisma Access reenvíe rutas a la red de su organización.

  Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

  Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.



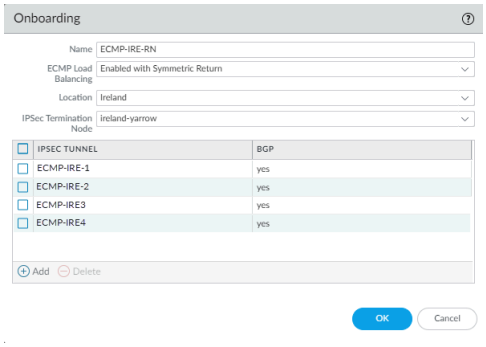
- **Peer AS (AS de peers)**: especifique el sistema autónomo (AS) al que pertenece el cortafuegos, el enrutador virtual o el enrutador BGP en su red remota.
- **Peer IP Address (Dirección IP del peer)**: introduzca la dirección IP asignada como ID del enrutador eBGP en la red remota para la que está configurando esta conexión.
- **Local IP Address (Dirección IP local)** (opcional): introduzca una dirección que Prisma Access utiliza como su dirección IP local para BGP. Especifique la dirección IP que se utilizará en el lado de Prisma Access del túnel.

  Especificar una **Local Address (Dirección local)** es útil cuando el dispositivo en el otro lado de la conexión (como una puerta de enlace privada virtual de Amazon Web Service (AWS)) requiere una dirección IP local específica para que el intercambio de BGP se realice correctamente. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP de la subred de infraestructura o las subredes de la red remota.

 ©2025 Palo Alto Networks, Inc.

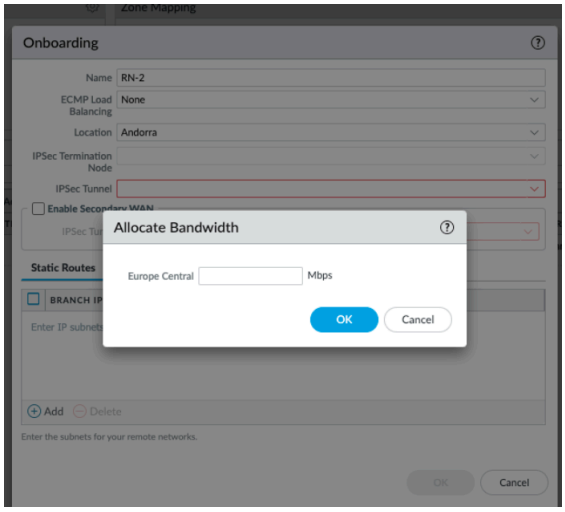
- **Secret (Secreto)** y **Confirm Secret (Confirmar secreto)** (opcional): introduzca y confirme una frase de contraseña para autenticar las comunicaciones entre peers de BGP.

3. Repita el paso anterior para añadir hasta cuatro túneles para usar con la conexión de red remota.



STEP 9 | Seleccione la **Location (Ubicación)** en la que Prisma Access implementará la infraestructura necesaria para proteger su ubicación de red remota. Esta región debe estar ubicada geográficamente cerca de la ubicación de su red remota.

Si aún no ha asignado ancho de banda para la ubicación de cómputo a la que se asigna la ubicación, Prisma Access le solicita que introduzca el ancho de banda para esa ubicación de cómputo.



STEP 10 | Seleccione el **IPSec Termination Node (Nodo de terminación IPSec)** que desea utilizar para esta red remota.

Prisma Access utiliza este nodo para asociar ubicaciones de red remotas con ubicaciones de cómputo.

STEP 11 | (Solo enrutamiento estático o implementaciones de un único túnel) Seleccione o añada una nueva configuración de **IPSec Tunnel (Túnel IPSec)** para acceder al cortafuegos, enrutador o dispositivo SD-WAN en la ubicación corporativa:

- Seleccione una de las plantillas IPSec predefinidas en Remote_Network_Template o, si añadió una plantilla a Remote_Network_Template_Stack (o modificó la

 ©2025 Palo Alto Networks, Inc.

Remote_Network_Template predefinida) que incluye una configuración de túnel IPSec, seleccione ese **IPSec Tunnel (Túnel IPSec)** en el menú desplegable. Tenga en cuenta que el túnel que está creando para cada conexión de red remota conecta Prisma Access al dispositivo compatible con IPSec en cada sucursal.

Utilice las siguientes pautas cuando configure un túnel IPSec:

- Las direcciones de peers en la configuración de IKE Gateway deben ser únicas para cada túnel. Sin embargo, puede reutilizar algunos de los otros elementos de configuración comunes, como los perfiles criptográficos.
- El túnel IPSec que seleccione de una plantilla debe utilizar el intercambio automático de claves e IPv4 únicamente.
- Los nombres del túnel IPSec, la puerta de enlace IKE y el perfil criptográfico no pueden superar los 31 caracteres.
- Si incorpora varias redes remotas en la misma ubicación con peers IKE dinámicos, debe usar el mismo perfil criptográfico IKE para todas las configuraciones de red remota.

- Para crear una nueva configuración de túnel IPSec, haga clic en **New IPSec Tunnel (Nuevo túnel IPSec)**, asígnele un **Name (Nombre)** y configure los ajustes de Puerta de enlace IKE, el Perfil criptográfico IPSec y Supervisión de túneles.
  - Si el dispositivo compatible con IPSec en su sucursal utiliza VPN basada en políticas, en la pestaña **Proxy IDs (ID de proxy)**, elija **Add (Añadir)** un ID de proxy que coincida con la configuración configurada en su dispositivo IPSec local para garantizar que Prisma Access pueda establecer correctamente un túnel IPSec con su dispositivo local.
- Deje seleccionado **Enable Replay Protection (Activar protección de reproducción)** para detectar y neutralizar ataques de reproducción.
- Marque **Copy TOS Header (Copiar encabezado de TOS)** para copiar el encabezado del tipo de servicio (type of service, ToS) del encabezado de la IP interna en el encabezado de la IP externa de los paquetes encapsulados a fin de conservar la información original del TOS.
- Para habilitar la supervisión de túnel para la conexión de servicio, seleccione **Tunnel Monitor (Supervisión de túnel)**.
  - Introduzca una dirección **Destination IP (IP de destino)**.

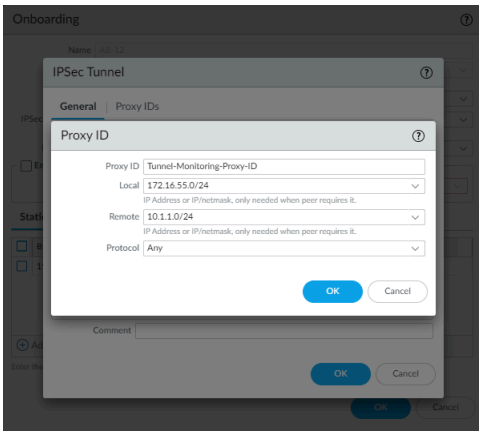
    Especifique una dirección IP en la ubicación de su sucursal a la que Prisma Access pueda enviar solicitudes de ping ICMP para la supervisión del túnel IPSec. Asegúrese de que

 ©2025 Palo Alto Networks, Inc.

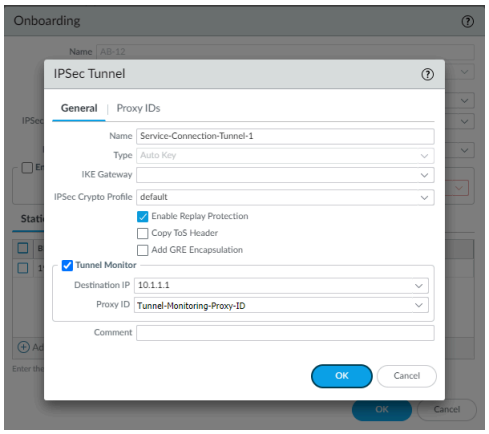
el ICMP pueda acceder a esta dirección desde toda la subred de la infraestructura de Prisma Access.

- Si utiliza la supervisión de túnel con un dispositivo de peer que utiliza varios ID de proxy, especifique un **Proxy ID (ID de proxy)** o añada un **New Proxy ID (ID de proxy nuevo)** que permita el acceso desde la subred de la infraestructura a la ubicación de su sucursal.

  La siguiente figura muestra un ID de proxy con la subred de la infraestructura del servicio (172.16.55.0/24 en este ejemplo) como la subred IP **Local (Local)** y la subred de la ubicación de la sucursal (10.1.1.0/24 en este ejemplo) como la subred **Remote (Remota)**.



  La siguiente figura muestra el ID de proxy que creó aplicándose a la configuración del monitor de túnel mediante su especificación en el campo **Proxy ID (ID de proxy)**.



Debe configurar en su CPE una ruta estática a la dirección IP del monitor de túnel para que funcione la supervisión del túnel. Para encontrar la dirección IP de destino que se utilizará para la supervisión del túnel desde la ubicación de su sucursal hasta Prisma Access, seleccione ***Panorama*** *>* ***Cloud Services (Servicios en la nube)*** *>* ***Status (Estado)*** *>* ***Network Details (Detalles de red)****, haga clic en el botón* ***Service Infrastructure (Infraestructura de servicios)*** *y encuentre la* ***Tunnel Monitor IP Address (Dirección IP de la supervisión del túnel)****.*

 ©2025 Palo Alto Networks, Inc.

STEP 12 | Si tiene un enlace WAN secundario en esta ubicación, seleccione **Enable Secondary WAN (Habilitar WAN secundaria)**.

Asegúrese de crear un túnel IPSec único para la WAN secundaria de cada red remota; Prisma Access no es compatible con la reutilización del mismo túnel IPSec para WAN secundarias en múltiples redes remotas.

La configuración de una WAN secundaria no se admite en las siguientes implementaciones:

- Si su WAN secundaria está configurada en modo activo-activo con el túnel IPSec primario.
- Si el equipo de las instalaciones del cliente (CPE) está configurado en una configuración de enrutamiento multipath de igual coste (ECMP) con el túnel IPSec primario y secundario.

Si utiliza rutas estáticas, el tiempo de conmutación por error del túnel es inferior a 15 segundos desde el momento de la detección, dependiendo de su proveedor de WAN.

Si configura el enrutamiento de BGP y ha habilitado la supervisión del túnel, el tiempo de espera predeterminado más corto para determinar que un índice de parámetro de seguridad (SPI) está fallando es el monitor del túnel, que elimina todas las rutas a un par cuando detecta un fallo del túnel durante 15 segundos consecutivos. De esta forma, el monitor de túnel determina el comportamiento de las rutas BGP. Si no configura la supervisión del túnel, el temporizador de mantenimiento determina el tiempo que el túnel estará inactivo antes de eliminar la ruta. Prisma Access utiliza el valor BGP HoldTime predeterminado de 90 segundos según lo definido por RFC 4271, que es el tiempo máximo de espera antes de que Prisma Access elimine una ruta para un SPI inactivo. Si el dispositivo peer BGP tiene un tiempo de espera configurado más corto, el temporizador de espera BGP utilizará el valor más bajo.

Cuando el túnel secundario se instala correctamente, la ruta secundaria tiene prioridad hasta que el túnel principal vuelva a subir. Si tanto la ruta primaria como la secundaria están activas, la ruta principal tiene prioridad.

Si utiliza un peer BGP diferente para la conexión secundaria (de respaldo), Prisma Access no respeta los atributos del discriminador de salidas múltiples (MED) anunciados por el CPE. Esta advertencia se aplica si utiliza varios peers BGP en conexiones de red remotas o en conexiones de servicio.

STEP 13 | Habilite el enrutamiento a las subredes o direcciones IP individuales en el sitio de red remoto a las que sus usuarios necesitarán acceder.

Prisma Access utiliza esta información para dirigir las solicitudes al sitio apropiado. Las redes de cada sitio no pueden superponerse entre sí ni con los grupos de direcciones IP que usted designó para la infraestructura del servicio o para Prisma Access para grupos de IP de usuarios. Puede configurar **Static Routes (Rutas estáticas)**, **BGP**o una combinación de ambas.

- Para configurar **Static Routes (Rutas estáticas)**:

  1. En la pestaña **Static Routes (Rutas estáticas)**, haga clic en **Add (Añadir)** e introduzca la dirección de subred (por ejemplo, 172.168.10.0/24) o la dirección IP individual de un recurso, como un servidor DNS (por ejemplo, 10.32.5.1/32) al que sus usuarios remotos necesitarán acceder.

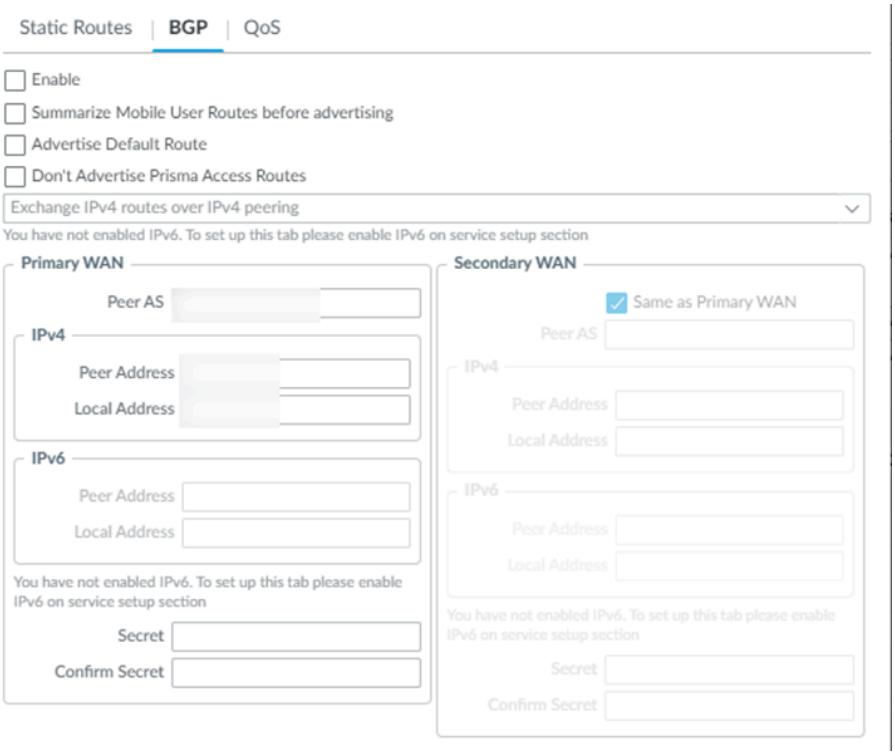
 ©2025 Palo Alto Networks, Inc.

2. Repita esto para todas las subredes o direcciones IP que Prisma Access necesitará acceso a esta ubicación.



- Para configurar **BGP**:

1. Seleccione la pestaña **BGP**.
2. (Opcional) Seleccione las opciones **ECMP Load Balancing (Equilibrio de carga ECMP)**. Consulte el paso 8.
3. Si selecciona **None (Ninguno)** para **ECMP Load Balancing (Equilibrio de carga de ECMP)**, introduzca las opciones de BGP.



4. Para habilitar BGP para la conexión de red remota, seleccione **Enable (Habilitar)**.

   Cuando habilita BGP, Prisma Access establece el valor de tiempo de vida útil (TTL) para BGP externo (eBGP) en 8 para acomodar cualquier salto adicional que pueda ocurrir entre la infraestructura de Prisma Access y el equipo de las instalaciones de su cliente (CPE) que finaliza la conexión eBGP.
5. Para reducir el número de anuncios de subred IP de usuarios móviles a través de BGP a los equipos de las instalaciones del cliente (CPE) resumiéndolos, seleccione **Summarize**

 ©2025 Palo Alto Networks, Inc.

Mobile User Routes before advertising (Resumir rutas de usuarios móviles antes de anunciar).

De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred especificada. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

Prisma Access establece la cadena de comunidad para las rutas de usuarios móviles agregadas en `0xFFFE:0xFFF0`.

6. Para permitir que Prisma Access anuncie una ruta predeterminada para la red remota usando eBGP, seleccione **Advertise Default Route (Anunciar ruta predeterminada)**.

   Si selecciona **Advertise Default Route (Anunciar ruta predeterminada)**, asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría generar problemas de enrutamiento en su red.

   Debe publicar sus rutas predeterminadas antes de realizar esta selección para publicitarlas. Además, asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.

7. Para evitar que el peer de BGP en el cortafuegos Prisma Access reenvíe rutas a la red de su organización, seleccione **Don't Advertise Prisma Access Routes (No anunciar rutas de Prisma Access)**.

   Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

   Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.

8. Introduzca el **Peer AS (AS de peer)**, que es el sistema autónomo (AS) al que pertenece el cortafuegos, el enrutador virtual o el enrutador BGP en su red remota.
9. Introduzca la dirección IP asignada como ID de enrutador del enrutador eBGP en la red remota para la que está configurando esta conexión como **Peer Address (Dirección de peer)**.
10. (Opcional) Introduzca una dirección que Prisma Access utiliza como su dirección IP local para BGP.

    Especificar una **Local Address (Dirección local)** es útil cuando el dispositivo en el otro lado de la conexión (como una puerta de enlace privada virtual de Amazon Web Service (AWS)) requiere una dirección IP local específica para que el intercambio de BGP se

 ©2025 Palo Alto Networks, Inc.

realice correctamente. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP de la subred de infraestructura o las subredes de la red remota.

*Debe configurar una ruta estática en su CPE a la **Local Address (Dirección local)**de BGP.*

11. (Opcional) Introduzca y confirme una frase de contraseña para autenticar las comunicaciones entre peers de BGP.
12. (Opcional) Si configuró una **Secondary WAN (WAN secundaria)** y necesita cambiar la **Peer Address (Dirección del peer)** o la **Local Address (Dirección local)** para el peer BGP secundario (copia de seguridad), anule la marca de **Same as Primary WAN (Igual que la WAN principal)** e introduzca un peer único y, opcionalmente, una dirección IP local para la WAN secundaria.

    Si utiliza redes IPv6 en su implementación de red remota, puede configurar direcciones **IPv6** así como también direcciones **IPv4** . También debe habilitar la red IPv6 a nivel global en su Infraestructura de Prisma Access antes de poder utilizar el direccionamiento IPv6.

    En algunas implementaciones (por ejemplo, cuando se usa BGP para conectarse con una puerta de enlace VPN de AWS), el peer BGP para la WAN primaria y secundaria puede ser diferente. En esos escenarios, puede optar por configurar un par BGP diferente para la WAN secundaria.

    *Para implementaciones de BGP con WAN secundarias, Prisma Access establece los túneles primario y secundario en un estado **UP (Activo)** pero sigue el comportamiento normal de respaldo activo BGP para el tráfico de red. Prisma Access establece el túnel principal como activo y envía y recibe tráfico únicamente a través de ese túnel; si el túnel principal falla, Prisma Access detecta el fallo utilizando reglas BGP, establece el túnel secundario como activo y utiliza solo el túnel secundario para enviar y recibir tráfico.*

STEP 14 | (Opcional) Habilite **QoS** para la ubicación y especifique un **QoS Profile (Perfil de QoS)**.

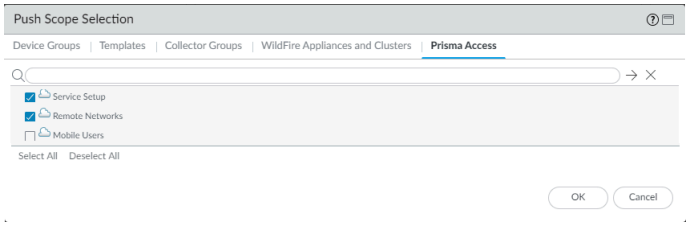
Puede especificar las opciones de QoS y la configuración general según la ubicación de computación en **Settings (Configuración)**; sin embargo, puede habilitar o deshabilitar QoS o cambiar el perfil de QoS según la ubicación aquí.

STEP 15 | Confirme los cambios de configuración en Panorama y envíe la configuración a Prisma Access para redes.

1. Haga clic en **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.
2. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**. Haga clic en **Edit Selections (Editar selecciones)** > **Prisma Access** y seleccione ambos Prisma Access

 ©2025 Palo Alto Networks, Inc.

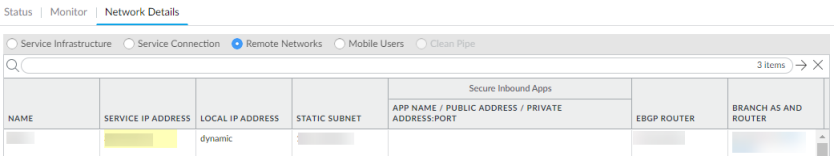
para redes y Prisma Access para la configuración del servicio para enviar la configuración al servicio.



3. Haga clic en **OK (Aceptar)** y **Push (Enviar)**.

STEP 16 | Configure el dispositivo compatible con IPSec en la ubicación de red remota para configurar una conexión IPSec con Prisma Access para redes.

1. Busque la **Service IP Address (Dirección IP del servicio)** para esta conexión de red remota seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de red)**, haciendo clic en el botón de opción **Remote Networks (Redes remotas)** y visualizando el campo **Service IP Address (Dirección IP del servicio)**. Prisma Access para la infraestructura de redes se ha asignado este dirección IP para la conexión de red remota de Prisma Access y debe configurarla como la dirección IP del peer para configurar el túnel IPSec entre la ubicación de red remota y Prisma Access para redes.



2. Verifique la **Local IP address (dirección IP local)** del dispositivo en la ubicación de red remota en la página **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de red)** > **Remote Networks (Redes remotas)**. Si está realizando NAT en la ubicación de red remota, la **Local IP address (Dirección IP local)** muestra la dirección IP del dispositivo después de NAT.

STEP 17 | Para proteger el tráfico en la ubicación de red remota, debe crear reglas de política de seguridad.

1. Seleccione **Policies (Políticas)**.
2. Seleccione el **Device Group (Grupo de dispositivos)** en el que desea añadir reglas de política. Puede seleccionar Remote_Network_Device_Group o el grupo de dispositivos principal que seleccionó para definir políticas para proteger la ubicación de la red remota.
3. Cree reglas de políticas de seguridad. Asegúrese de no definir reglas de política de seguridad para permitir el tráfico de cualquier zona a cualquier zona. En las reglas de la política de seguridad, utilice las zonas que definió en su plantilla.

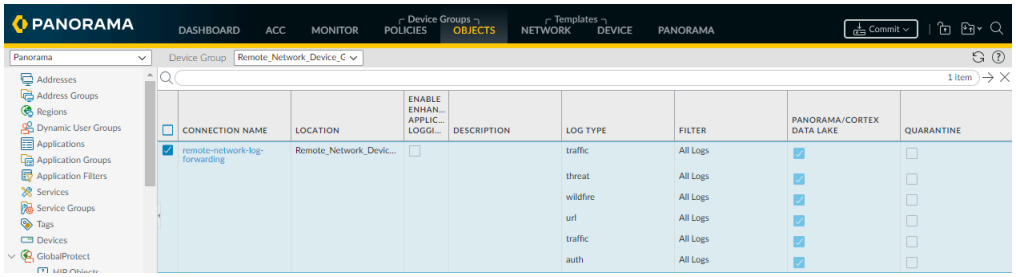
   Si a un usuario de su red se le niega el acceso a un sitio web, informe los problemas de acceso al sitio web antes de abrir un ticket de incidencia con Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

STEP 18 | Habilite el registro de logs para Strata Logging Service. Debe crear y adjuntar un perfil de reenvío de logs a cada regla de política para la cual desea reenviar logs.

1. Seleccione **Objetos > Reenvío de logs**.
2. Seleccione el **Device Group (Grupo de dispositivos)** en el que añadió las reglas de política, por ejemplo, Remote_Network_Device_Group.
3. **Add (Añadir)** perfil de reenvío de logs En la lista de coincidencia del perfil de reenvío de logs, seleccione **Add (Añadir)** para añadir cada **Log Type (Tipo de log)** que desea reenviar.
4. Seleccione **Panorama/Strata Logging Service (Servicio de registro de logs de Panorama/Strata)** como método de reenvío para habilitar Prisma Access para reenviar los logs a Strata Logging Service. Podrá supervisar los logs y generar informes desde Panorama. Strata Logging Service proporciona una integración perfecta para almacenar logs sin tener que enviarlos de regreso a su Panorama en la sede central, y Panorama puede consultar Strata Logging Service según sea necesario.

   El siguiente ejemplo permite el reenvío de logs de tráfico, prevención de amenazas, envío de WildFire, filtrado de URL, filtrado de datos y autenticación a Strata Logging Service.



5. Seleccione **Policies (Políticas) > Security (Seguridad)** y modifique la regla de políticas. Seleccione **Actions (Acciones)** y seleccione el perfil de Reenvío de logs que ha creado.

STEP 19 | Confirme todos sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Deberá **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access** , asegúrese de que **Prisma Access for networks (Prisma Access para redes)** se selecciona en **Push Scope (Ámbito de envío)**, luego haga clic en **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 20 | Verifique el estado de la red remota.

Consulte Compruebe si la red remota está conectada a Prisma Access para obtener más detalles.

 ©2025 Palo Alto Networks, Inc.

Planifique su migración al nuevo modelo

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Ancho de banda para nuevas implementaciones de redes remotas de Prisma Access se asignan a un nivel agregado por ubicación de cómputo, también conocido como *modelo de ancho de banda agregado*. La asignación de ancho de banda a nivel de ubicación de cómputo le ofrece más flexibilidad para asignar su ancho de banda de red remota con licencia, porque Prisma Access asigna dinámicamente el ancho de banda para cada ubicación según la carga o la demanda.

Si tiene una implementación existente que asigna ancho de banda por ubicación de Prisma Access, puede migrar al modelo de ancho de banda agregado. También puede migrar su implementación de QoS de red remota. Al migrar, todas las redes remotas utilizan el modelo de ancho de banda agregado.

Utilice la siguiente lista de verificación para planificar la migración al modelo de ancho de banda agregado:

- ❑ Tenga en cuenta los siguientes componentes de red remota que permanecen sin cambios después de la migración:
  - No hay cambios en el plano de datos. El tráfico continúa fluyendo a través del plano de datos de Prisma Access sin ningún cambio en la configuración existente.
  - La migración no afecta a los túneles existentes.

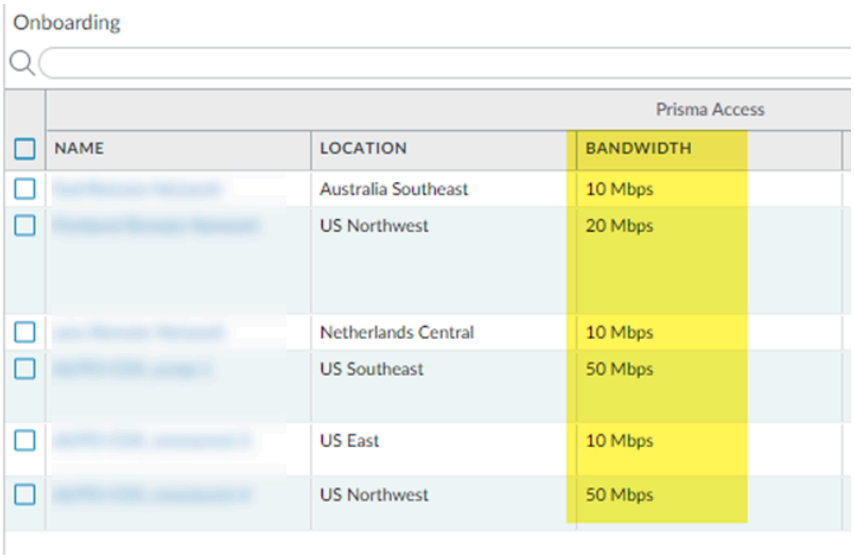
    No es necesario reconfigurar los parámetros de su túnel IPSec. Las puertas de enlace IKE, los perfiles de cifrado IKE e IPSec y las configuraciones de túnel IPSec permanecen sin cambios.
  - La red remota **Service IP Address (Dirección IP del servicio)** (el las direcciones IP públicas utilizadas en el lado del túnel IPSec de Prisma Access para la conexión de red remota no cambia para cada red remota cuando migra su implementación al modelo de ancho de banda agregado.
- ❑ Prisma Access asigna nodos de terminación IPSec y asigna ancho de banda a redes remotas durante una migración al modelo de ancho de banda agregado. Debe comprender cómo funciona este modelo antes de migrar.

  *Si desea reasignar una red remota existente a otro nodo de terminación IPSec después de la migración, Prisma Access asigna otra **Service IP Address (Dirección IP del servicio)** a la red remota después de confirmar y enviar sus cambios. En este caso, necesitará reconfigurar su CPE para que apunte a la nueva dirección IP del túnel de red remota.*

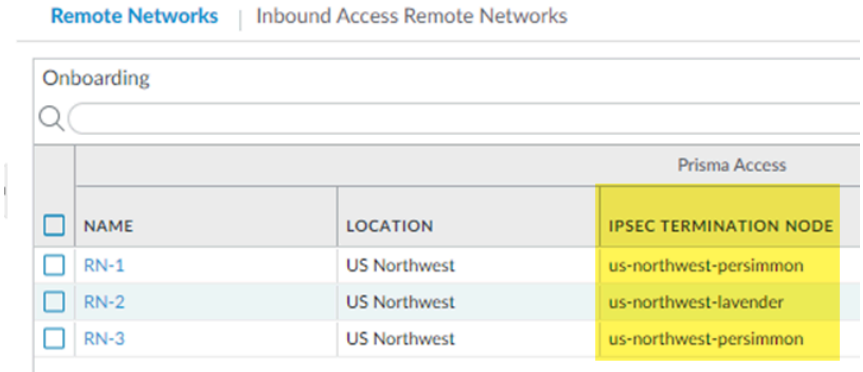
 ©2025 Palo Alto Networks, Inc.

- Si tiene una configuración no compatible, no verá la pestaña Asignación de ancho de banda ni verá el banner para migrar. Las siguientes configuraciones no son compatibles con la migración al modelo de ancho de banda agregado:
  - Una red remota con un ancho de banda de **1000 Mbps**.
  - Una integración de Prisma SD-WAN CloudBlade con Prisma Access que tiene una versión anterior a la 3.0.
  - Una configuración de red remota que proporciona acceso entrante seguro a aplicaciones en un sitio de red remoto anterior a la versión 2.1 Innovation.

  Si tiene y usa QoS con sus redes remotas, asegúrese de seguir las pautas de migración de QoS antes de migrar.
- Si no está seguro de qué modelo utiliza su implementación, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.
  - Si ve un campo de **Bandwidth (Ancho de banda)** en el área Redes remotas, está asignando ancho de banda por ubicación de Prisma Access y puede migrar al modelo de ancho de banda agregado.

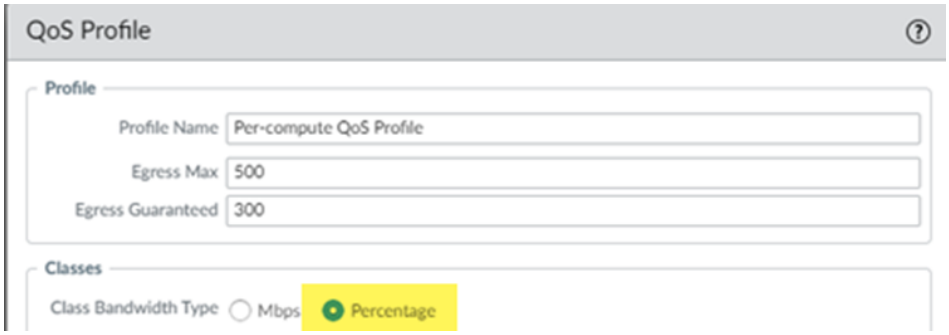


  - Si ve un **IPSec Termination Node (Nodo de terminación IPSec)**, ya ha migrado al modelo de ancho de banda agregado.



 ©2025 Palo Alto Networks, Inc.

- Después de migrar al modelo de ancho de banda agregado, el cambio es permanente y no puede volver a tener una implementación que asigne ancho de banda por ubicación de Prisma Access.
- Debe tener un mínimo de 50 Mbps de ancho de banda disponible para migrar al modelo de ancho de banda agregado.
- Si desea implementar QoS después de la migración, conozca las diferencias sobre la configuración de QoS para una implementación de ancho de banda agregado.
  - Asegúrese de utilizar un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)** en lugar de **Mbps** en sus perfiles de QoS. Prisma Access no admite tipos de ancho de banda de **Mbps** en perfiles de QoS para implementaciones que asignan ancho de banda por ubicación de cómputo.



  - Comprenda cómo especificar una relación de ancho de banda garantizada y cómo personalizar el ancho de banda por sitio.

    Al utilizar una relación de ancho de banda garantizada, puede asignar un porcentaje del ancho de banda total asignado en la ubicación de cómputo. Prisma Access divide el ancho de banda garantizado en partes iguales por la cantidad de nodos de terminación IPSec en la ubicación de cómputo.

    Al personalizar el ancho de banda por sitio, puede aplicar una relación de asignación para los sitios en un solo nodo de terminación IPSec y especificar perfiles de QoS por sitio en la **Settings (Configuración)** de red remota. Como alternativa, puede especificar un perfil de QoS durante la configuración de la red remota seleccionando la red remota y especificando un perfil de QoS en la pestaña **QoS**.
- Si ha configurado sus redes remotas para proporcionar acceso entrante seguro a sus ubicaciones de red remotas, todas las funciones de acceso entrante existentes son compatibles, como habilitar un enlace WAN secundario [**Enable Secondary WAN (Habilitar WAN secundaria)**], BGP, QoS y opciones de NAT de origen. Tampoco hay cambios en el ancho de banda que consumen las direcciones IP públicas. Prisma Access asigna (5 direcciones IP toman 150 Mbps de su asignación de licencia de red remota y 10 direcciones IP toman 300 Mbps).

  Si necesita configurar el acceso entrante después de migrar, utilice el procedimiento de acceso entrante específico del modelo de ancho de banda agregado.

 ©2025 Palo Alto Networks, Inc.

- Palo Alto Networks recomienda que tome nota de su configuración de ancho de banda existente y del ancho de banda total con licencia antes de migrar.

  A pesar de que Prisma Access migra su ancho de banda durante la migración; debe tener en cuenta su configuración actual como práctica recomendada y realizar cualquier ajuste al ancho de banda de la ubicación de cómputo después de migrar.

  - Verifique su configuración de ancho de banda existente seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y tome nota del **Bandwidth (Ancho de banda)** existente que está disponible para cada conexión de red remota.
  - Vaya a **Panorama** > **Licenses (Licencias)** y verifique su ancho de banda total autorizado en Mbps para redes remotas. Esta información se incluye en **Prisma Access Net Capacity (Capacidad neta)** o **GlobalProtect Cloud Service for Mobile Users (GlobalProtect Cloud Service para usuarios móviles**, según su tipo de licencia.

Después de migrar, tome nota de las siguientes diferencias en su implementación:

- Incorpore todas las nuevas redes remotas mediante el procedimiento de incorporación de red remota de ancho de banda agregado.
- Cuando visualiza las estadísticas de uso de ancho de banda, las visualiza a nivel de nodo de terminación por IPSec.

Asignación de ancho de banda para una implementación de ancho de banda agregado migrado

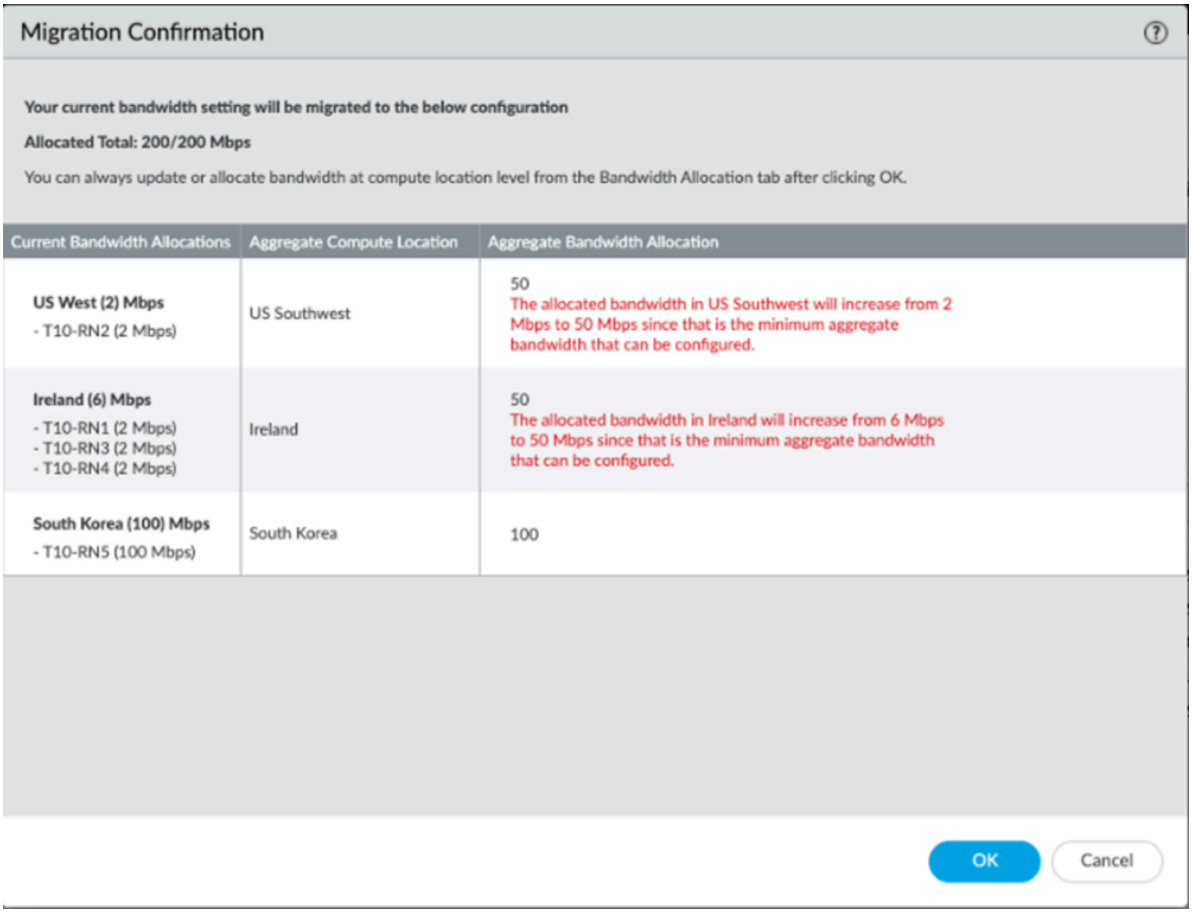
Si tiene una implementación que asigna ancho de banda por ubicación de Prisma Access, Prisma Access realiza los siguientes cambios cuando migra al modelo de ancho de banda agregado:

- Prisma Access suma el ancho de banda de todas las ubicaciones en una ubicación de cómputo determinada y asigna el ancho de banda sumado a esa ubicación de cómputo.

  Por ejemplo, tiene tres ubicaciones (**Location 1**, **Location 2** y **Location 3**) en las ubicaciones México Oeste, EE. UU. Suroeste y EE. UU. Oeste, y cada ubicación existente tiene 50 Mbps de ancho de banda. Dado que cada ubicación se encuentra en la ubicación de cómputo de EE. UU. Suroeste, Prisma Access suma el ancho de banda de las tres ubicaciones y asigna 150 Mbps de ancho de banda a la ubicación EE. UU suroeste.
- Si todas las ubicaciones en una ubicación de cómputo tienen un ancho de banda total de menos de 50 Mbps, Prisma Access aumentará el ancho de banda a 50 Mbps para esa ubicación

 ©2025 Palo Alto Networks, Inc.

de cómputo. Prisma Access le proporciona las ubicaciones que requieren el aumento del ancho de banda durante el proceso de migración.



- Prisma Access utiliza nodos de terminación IPSec en implementaciones de ancho de banda agregado. Durante la migración, Prisma Access proporciona un nodo de terminación IPSec por ubicación de cómputo por cada 1000 Mbps de ancho de banda asignado. Por ejemplo, si asigna 1500 Mbps de ancho de banda en una ubicación de cómputo, Prisma Access proporciona esa ubicación con dos nodos de terminación IPSec.

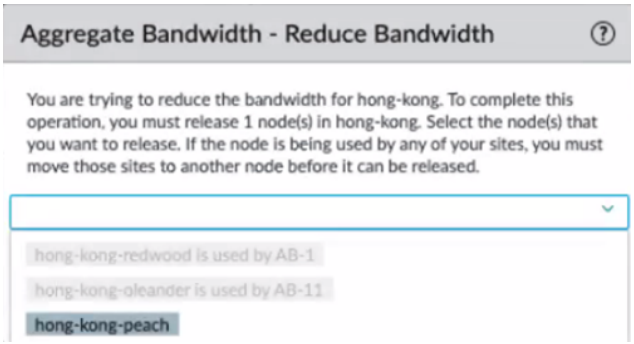
  Usted asigna nodos de terminación IPSec a una red remota durante la incorporación de la red remota. En una migración de ancho de banda agregado, Prisma Access asocia los nodos de terminación IPSec a las redes remotas durante la migración. La siguiente lista proporciona algunos ejemplos de asociación de nodos de terminación IPSec para una migración:

  - Si tiene cuatro redes remotas que están en la misma ubicación de cómputo y esas ubicaciones tienen 50 Mbps de ancho de banda cada una, Prisma Access asigna 200 Mbps de ancho de banda a esa ubicación de cómputo, proporciona un único nodo de terminación IPSec a esa ubicación de cómputo y asocia ese nodo de terminación IPSec a las cuatro redes remotas.
  - Si tiene tres redes remotas en la misma ubicación de procesamiento con 100 Mbps cada una, Prisma Access asigna 300 Mbps de ancho de banda a esa ubicación de cómputo, proporciona un único nodo de terminación IPSec a esa ubicación de cómputo y asocia ese nodo de terminación IPSec a las tres redes remotas.

 ©2025 Palo Alto Networks, Inc.

- Si tiene siete redes remotas en la misma ubicación de cómputo, con dos redes remotas que tienen 500 Mbps y cinco redes remotas que tienen 100 Mbps cada una, Prisma Access asigna 1500 Mbps de ancho de banda a esa ubicación de cómputo. Debido a que el ancho de banda total asignado en esa ubicación de cómputo es mayor a 1000 Mbps, Prisma Access asigna dos nodos de terminación IPSec y realiza las siguientes asociaciones:
  - A las dos redes remotas de 500 Mbps se les asigna un nodo de terminación IPSec (un nodo por cada red remota de 1000 Mbps).
  - A las cinco redes remotas de 100 Mbps se les asigna un nodo de terminación IPSec.

  Después de migrar, puede cambiar la asociación del nodo de terminación IPSec para aumentar el ancho de banda de una ubicación. Por ejemplo, dada una ubicación de cómputo con dos nodos de terminación IPSec, podría reasignar un solo nodo de terminación IPSec a una sola ubicación y reasignar el otro nodo de terminación IPSec a las ubicaciones restantes, lo que efectivamente proporciona a la ubicación que no comparte un nodo de terminación IPSec con más ancho de banda.
- Si reduce el ancho de banda lo suficiente, es posible que tenga que liberar un nodo de terminación IPSec. Por ejemplo, si reduce el ancho de banda en una ubicación de procesamiento de 1500 Mbps a 800 Mbps, necesitará eliminar uno de los nodos de terminación IPSec existentes. Si ubicaciones existentes están utilizando alguno de esos nodos, debe reasignar el nodo de terminación IPSec antes de eliminarlo.



Directrices para la migración de QoS

Si utiliza QoS con su actual implementación de red remota de Prisma Access y asigna ancho de banda por ubicación, puede migrar a una implementación de ancho de banda agregado mientras aún conserva sus políticas y perfiles de QoS existentes.

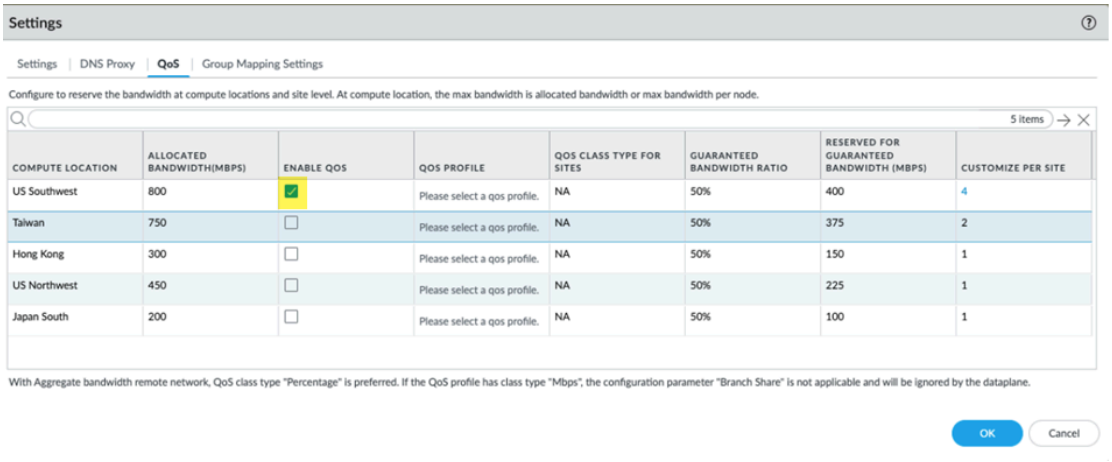
Al utilizar el modelo de ancho de banda agregado, se asigna ancho de banda a un nivel agregado por ubicación de cómputo y Prisma Access asigna dinámicamente el ancho de banda según la carga o la demanda por ubicación.

Después de la migración, la pestaña **QoS** muestra la configuración de QoS en la configuración de red remota [**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** > **Settings (Configuración)**]. Cualquier ubicación de cómputo que se asigne a las ubicaciones que tengan QoS habilitado tiene la opción **Enable QoS (Habilitar QoS)** seleccionada; cualquier ubicación de cómputo que se asigne a ubicaciones que no tengan QoS habilitado no tienen la opción **Enable QoS (Habilitar QoS)** seleccionada.

La siguiente captura de pantalla muestra una muestra de una pestaña de QoS después de la migración. Una red remota en la ubicación EE. UU. Oeste tiene QoS habilitado, y ninguna otra

 ©2025 Palo Alto Networks, Inc.

ubicación tiene QoS habilitado. Dado que la ubicación EE. UU. Oeste se asigna a la ubicación de cómputo EE. UU. Suroeste, la pestaña **QoS** muestra QoS habilitada para la ubicación de cómputo EE. UU. Suroeste

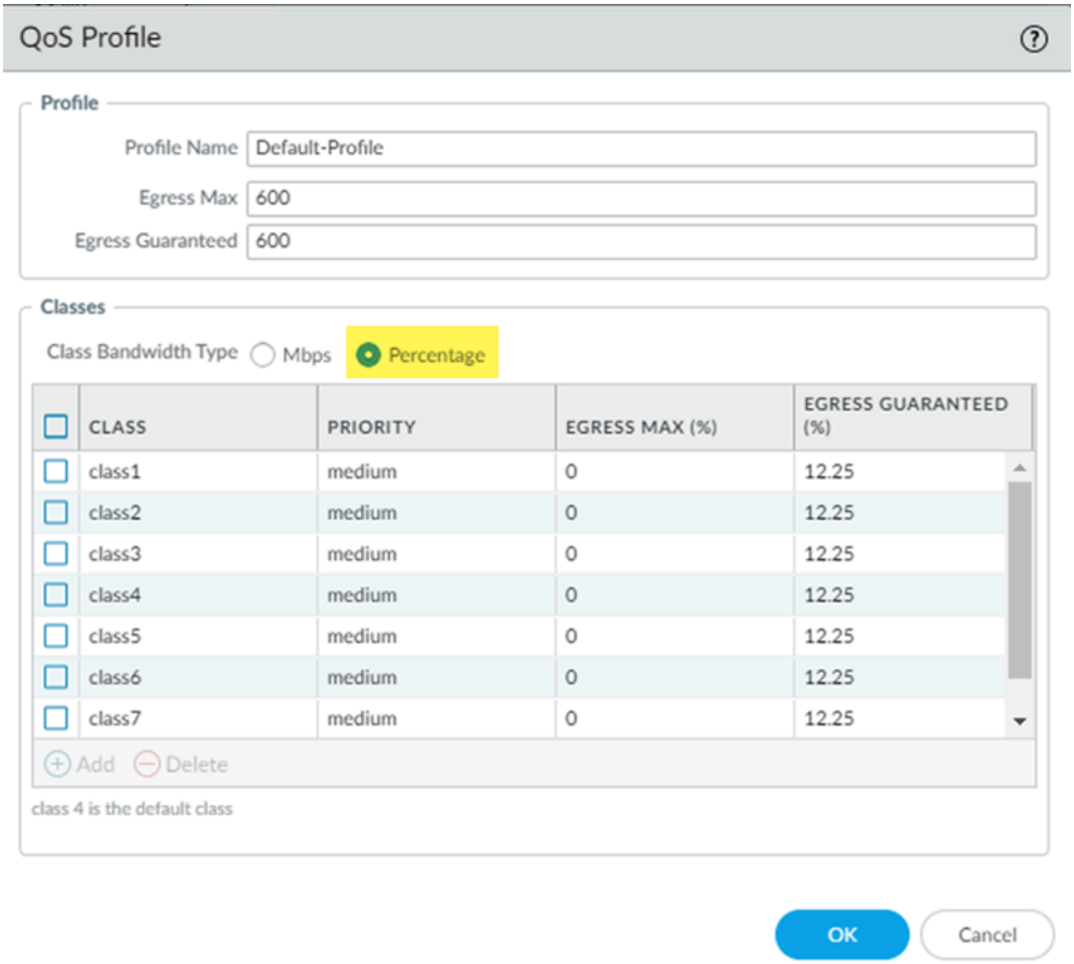


Palo Alto Networks hace las siguientes recomendaciones y requisitos para QoS en una implementación de ancho de banda agregado.

- Dado que el ancho de banda se comparte entre todas las ubicaciones en una única ubicación de cómputo, deberá cambiar el **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Mbps** a **Percentage (Porcentaje)**. La única ocasión en la que se admite un tipo de ancho de

 ©2025 Palo Alto Networks, Inc.

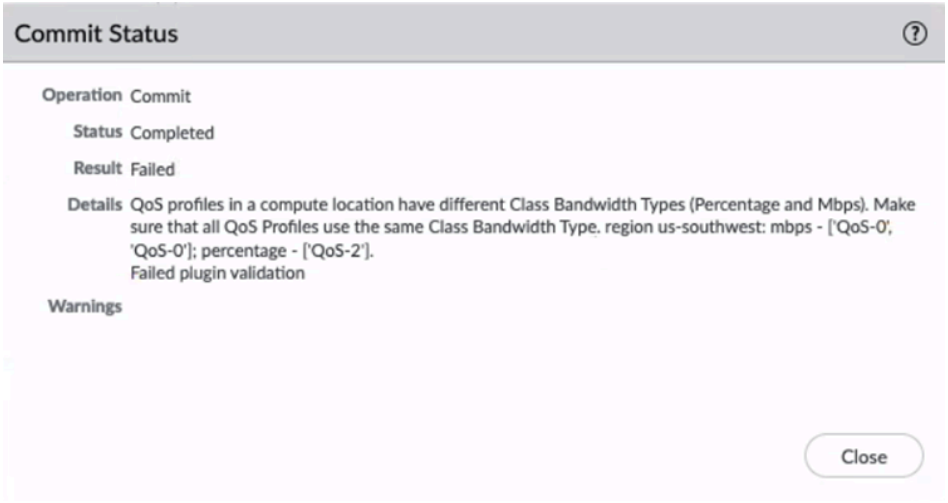
banda de **Mbps** es cuando tiene una implementación existente que asigna ancho de banda por ubicación y luego migra a una implementación de ancho de banda agregado.



- No puede ajustar la asignación de ancho de banda de QoS en función de Mbps en el perfil; para los perfiles que usan un tipo de ancho de banda por **Percentage (Porcentaje)**, puede cambiar el ancho de banda de QoS por ubicación ajustando la Relación de ancho de banda garantizado y personalizando el perfil de QoS por sitio.

©2025 Palo Alto Networks, Inc.

- No puede mezclar tipos de ancho de banda en una ubicación de cómputo; si lo hace, recibirá un mensaje de error durante la confirmación.

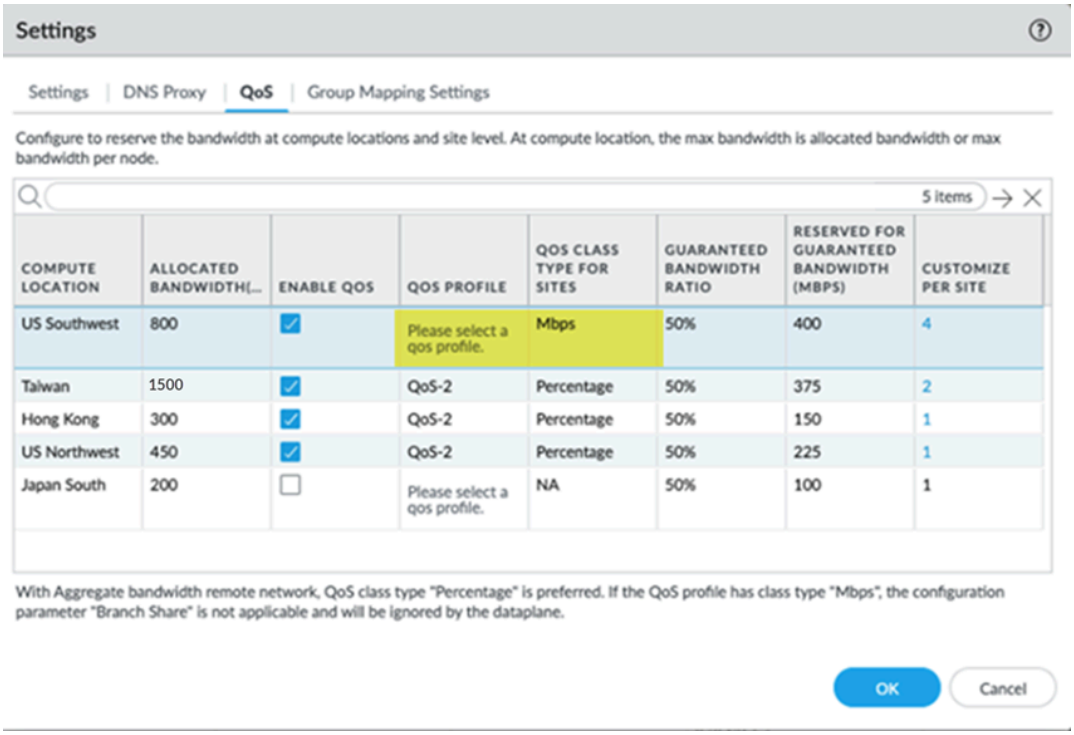


- Si agrega nuevas ubicaciones y esas ubicaciones pertenecen a una nueva ubicación de cómputo, solo podrá crear perfiles que tengan un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)** en la nueva ubicación de cómputo.
- Si conserva perfiles de QoS que tienen un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Mbps**, se ignorarán todos los cambios que realice en la relación de ancho de banda garantizado o personalice el perfil de QoS por sitio.
- Después de la migración, cualquier ubicación que use perfiles de QoS con un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Mbps** muestra un **QoS Class Type For Sites (Tipo de clase de QoS para sitios)** de **Mbps** para su ubicación de cómputo correspondiente en la pestaña **QoS**. Los perfiles de QoS con un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)** muestran un **QoS Class Type For Sites (Tipo de clase de QoS para sitios)** de **Percentage (Porcentaje)**.

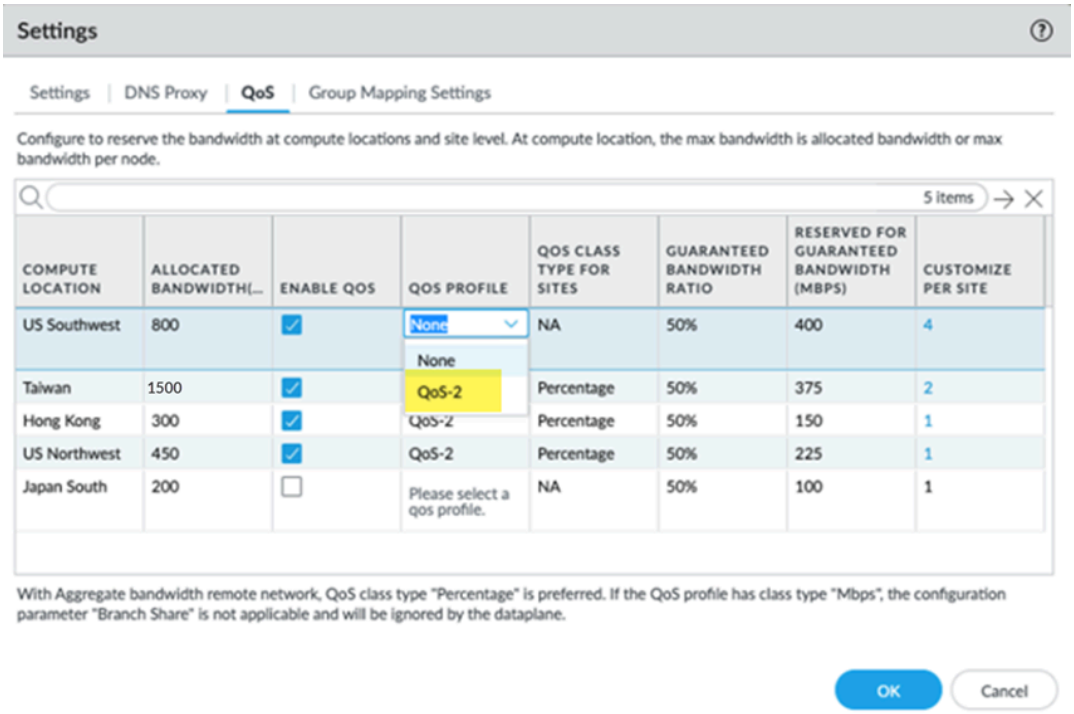
  Además, no puede seleccionar ningún perfil de QoS que tenga un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Mbps**. La siguiente captura de pantalla muestra la ubicación de cómputo de EE. UU. Suroeste utilizando un perfil de QoS con un **Class Bandwidth Type**

 ©2025 Palo Alto Networks, Inc.

(Tipo de ancho de banda de clase) de **Mbps**. Esa opción no se puede seleccionar en el menú desplegable del área **QoS Profile (Perfil de QoS)** .



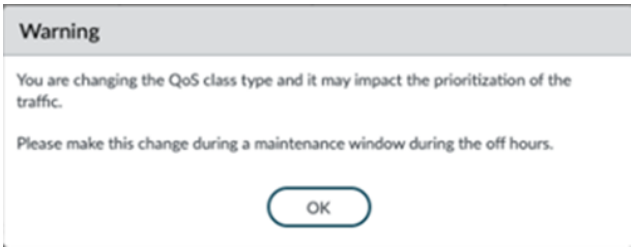
Sin embargo, puede seleccionar un perfil de QoS que utilice un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)** (QoS-2 en este ejemplo).



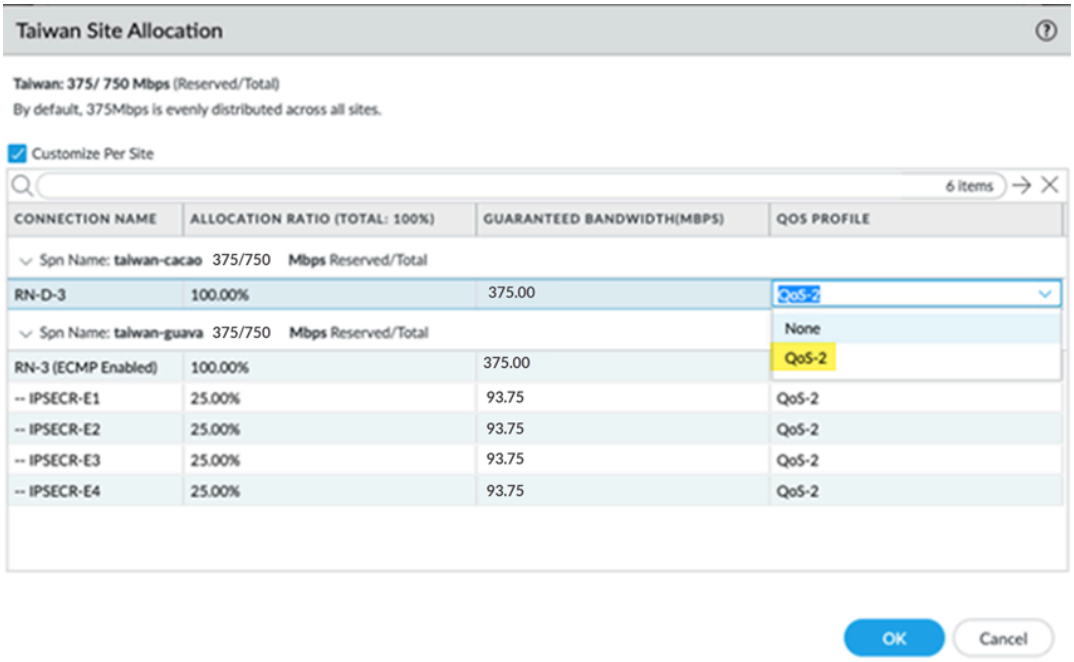
- Si cambia el perfil de QoS para una ubicación de cómputo de un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Mbps** a **Percentage (Porcentaje)**, debe realizar el cambio

 ©2025 Palo Alto Networks, Inc.

durante una ventana de mantenimiento o durante horas de baja actividad. Cambiar el perfil de QoS podría cambiar la priorización del tráfico.



- Solo puede seleccionar perfiles de QoS con un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)** cuando personaliza el perfil de QoS por sitio.



Migrar la configuración de gestión del ancho de banda

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Aprenda cómo migrar su configuración de gestión de ancho de banda.

Si tiene una implementación de red remota de Prisma Access que asigna ancho de banda por ubicación, Prisma Access le permite hacer que su implementación sea más flexible y escalable al migrar a una implementación que asigna ancho de banda por ubicación de cómputo (el modelo de ancho de banda agregado). Después de revisar la lista de comprobación de la planificación de la migración, utilice los siguientes pasos para migrar al modelo de ancho de banda agregado.

©2025 Palo Alto Networks, Inc.

También puede migrar su implementación de QoS de red remota. Al migrar, todas las redes remotas utilizan el modelo de ancho de banda agregado.

Tenga en cuenta lo siguiente antes de migrar su configuración de ancho de banda:

- Los siguientes componentes de red remota permanecen sin cambios después de la migración:
  - El plano de datos de Prisma Access.
  - Sin impacto en túneles existentes.
  - No es necesario reconfigurar los parámetros de su túnel IPSec.
  - Las puertas de enlace IKE, los perfiles de cifrado IKE e IPSec y las configuraciones de túnel IPSec permanecen sin cambios.
  - La **Service IP Address (Dirección IP del servicio)** de la red remota no cambia para cada red remota.
- Prisma Access asigna nodos de terminación IPSec y asigna ancho de banda a redes remotas durante una migración al modelo de ancho de banda agregado.
- Si tiene una configuración no compatible, no verá la pestaña Asignación de ancho de banda ni verá el banner para migrar.
- Si tiene una QoS con sus redes remotas, asegúrese de seguir las pautas de migración de QoS antes de migrar.
- Después de migrar al modelo de ancho de banda añadido, el cambio es permanente y no puede volver a tener una implementación que asigna ancho de banda por ubicación de Prisma Access.
- Debe tener un mínimo de 50 Mbps de ancho de banda disponible para migrar al modelo de ancho de banda agregado.
- Si desea implementar QoS después de la migración, conozca las diferencias sobre la configuración de QoS para una implementación de ancho de banda agregado.
- Una vez migrado, incorpore todas las nuevas redes remotas mediante el procedimiento de incorporación de red remota de ancho de banda agregado.
- Una vez migrado, cuando ve las estadísticas de uso de ancho de banda, las ve a nivel de nodo de terminación por IPSec.
- No utilice la CLI para realizar la migración; utilice únicamente la UI para migrar.
- Strata Cloud Manager
- Panorama

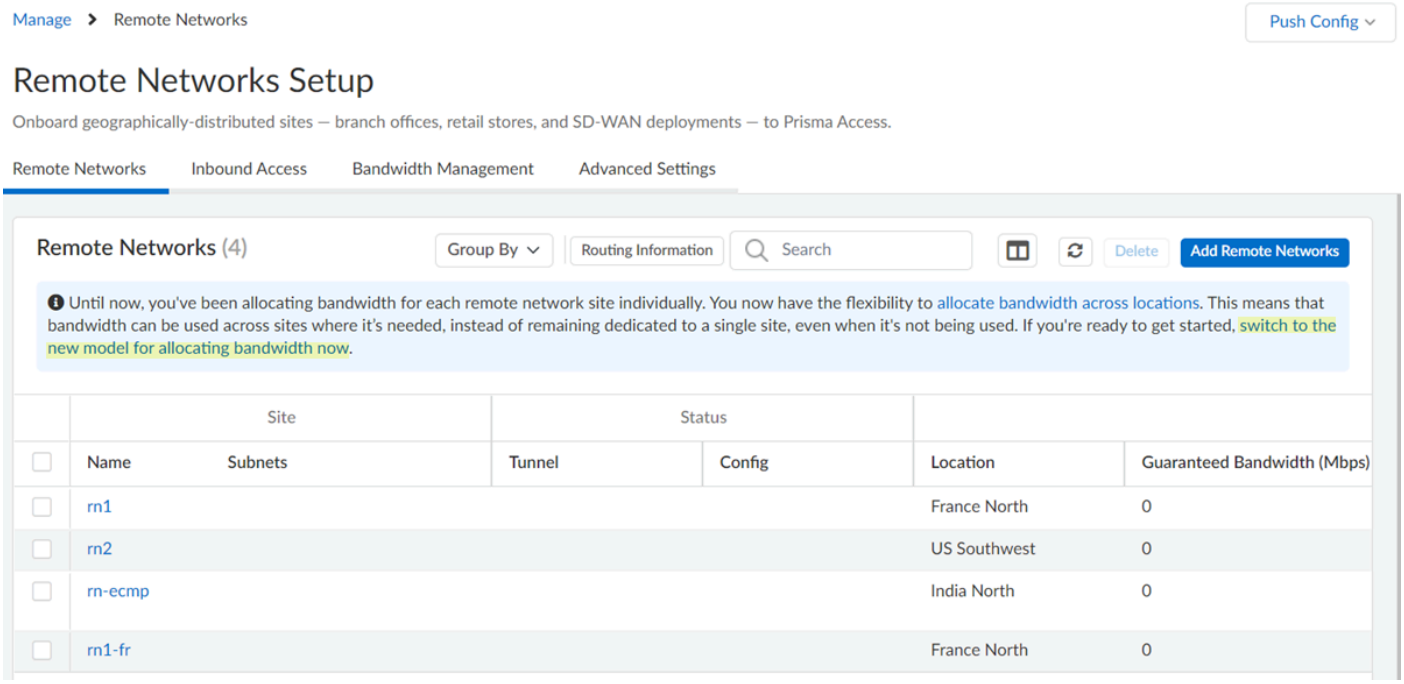
Migrar su configuración de gestión de ancho de banda (Strata Cloud Manager)

Si tiene una implementación de red remota de Prisma Access que asigna ancho de banda por ubicación, Prisma Access le permite hacer que su implementación sea más flexible y escalable al migrar a una implementación que asigna ancho de banda por ubicación de cómputo (el modelo de ancho de banda agregado). Después de revisar la lista de comprobación de la planificación de la migración, utilice los siguientes pasos para migrar al modelo de ancho de banda agregado.

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)**.

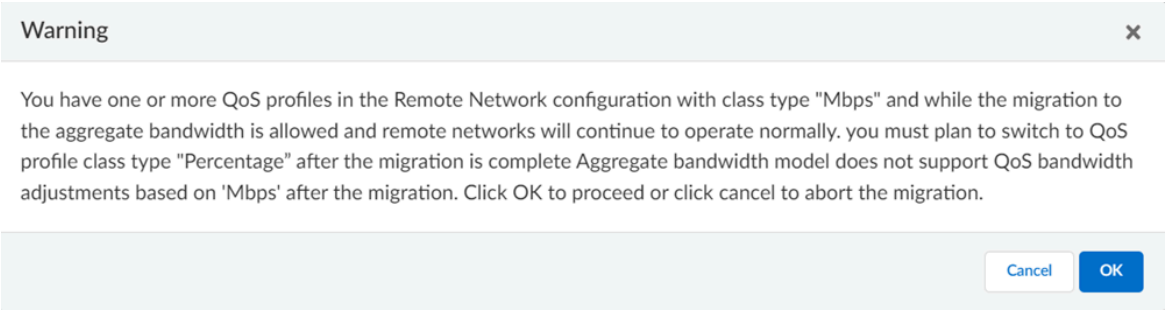
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Cambie ahora al nuevo modelo para asignar ancho de banda.

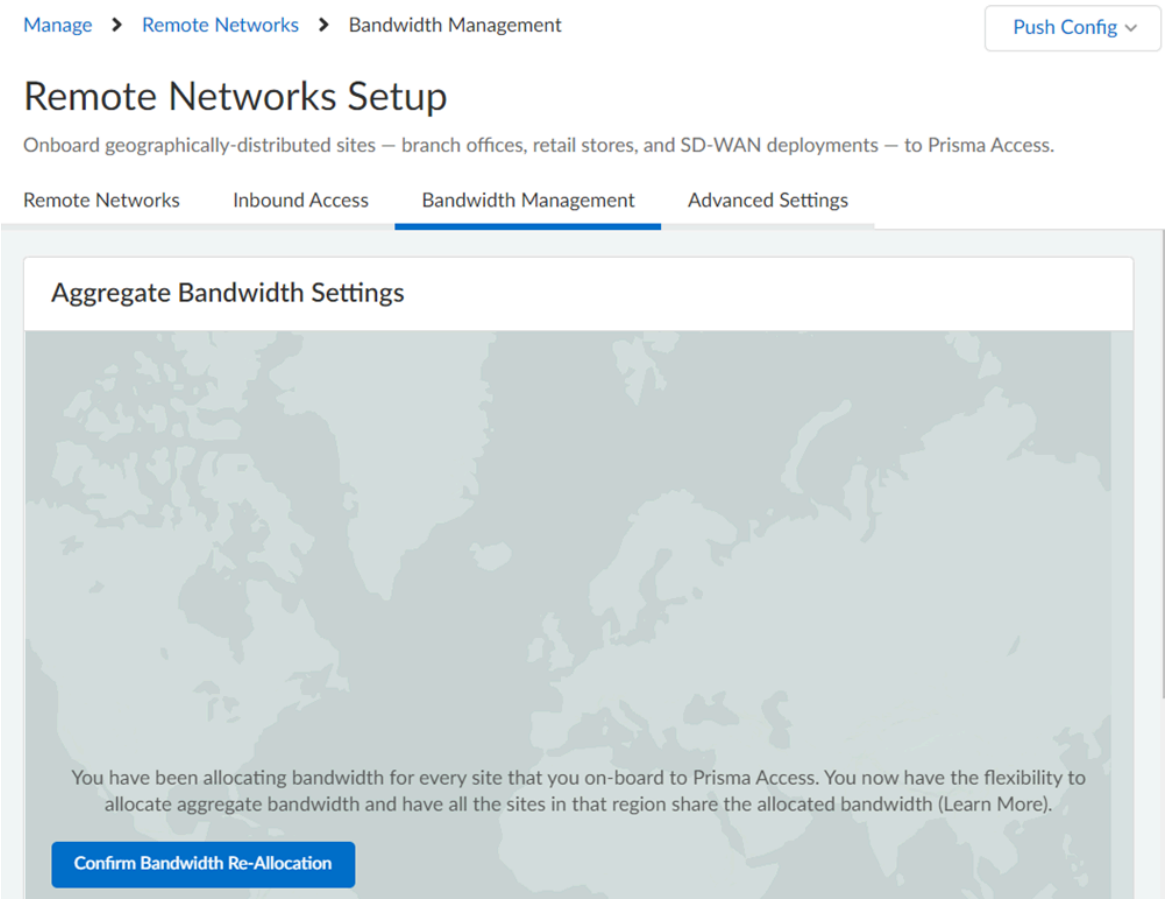


 ©2025 Palo Alto Networks, Inc.

- *Si tiene perfiles de QoS con un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Mbps**, Prisma Access le notifica que debe planificar cambiar estos perfiles a un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)**.*



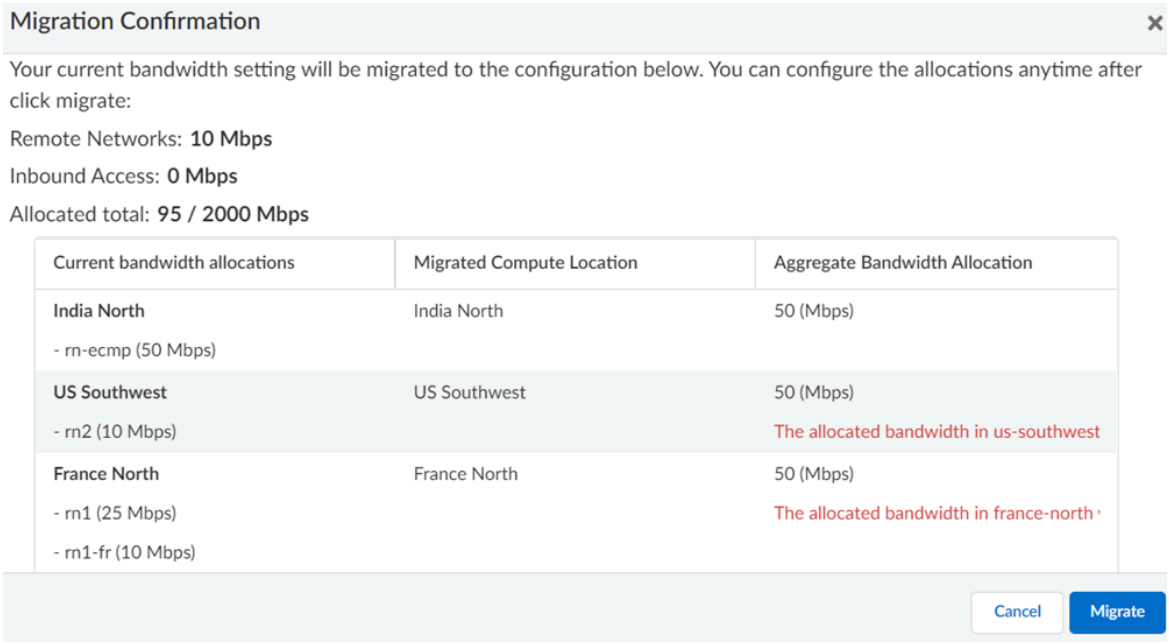
- *Alternativamente, en la pestaña **Bandwidth Management (Gestión de ancho de banda)**, seleccione **Confirm Bandwidth Re-Allocation (Confirmar reasignación de ancho de banda)**.*



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Revise la información y seleccione **Migrate (Migrar)** en la ventana emergente que aparece.

Si todas las ubicaciones en una ubicación de cómputo tienen un ancho de banda total de menos de 50 Mbps, Prisma Access aumentará el ancho de banda a 50 Mbps para esa ubicación de cómputo. Prisma Access le proporciona las ubicaciones que requieren el aumento del ancho de banda durante el proceso de migración.



*La migración al modelo de ancho de banda agregado es permanente e irreversible. Antes de migrar, revise la lista de verificación previa a la migración. Debe **Commit and Push (Confirmar y enviar)** sus cambios para que surtan efecto.*

Prisma Access migra el ancho de banda de red remota asignado al modelo de ancho de banda agregado.

STEP 4 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

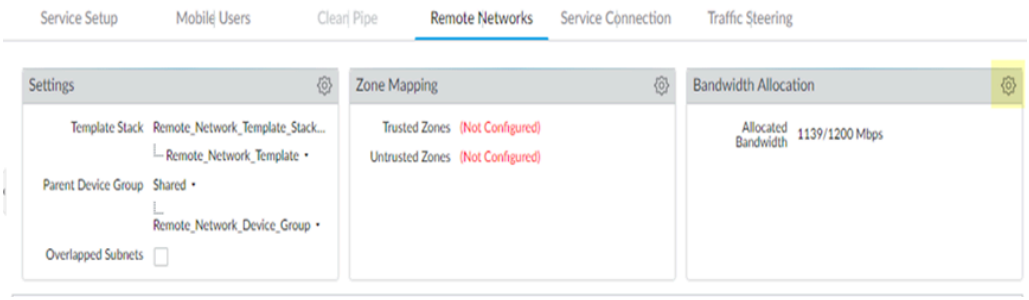
Migrar su configuración de gestión de ancho de banda (Panorama)

Si tiene una implementación de red remota de Prisma Access que asigna ancho de banda por ubicación, Prisma Access le permite hacer que su implementación sea más flexible y escalable al migrar a una implementación que asigna ancho de banda por ubicación de cómputo (el modelo de ancho de banda agregado). Después de revisar la lista de comprobación de la planificación de la migración, utilice los siguientes pasos para migrar al modelo de ancho de banda agregado.

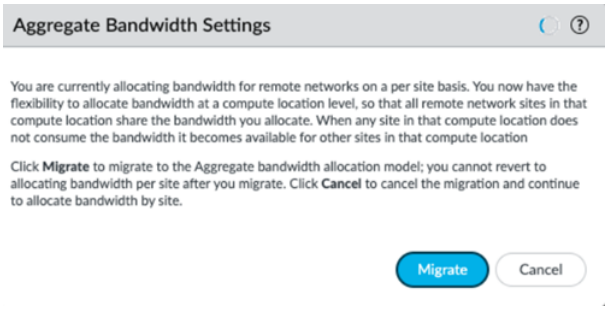
STEP 1 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Edite la configuración haciendo clic en el icono de engranaje en el área **Bandwidth Allocation (Asignación de ancho de banda)**.

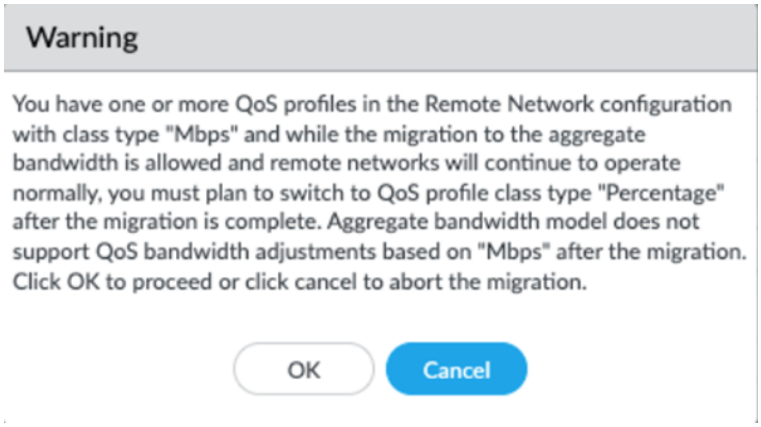


STEP 3 | Seleccione **Migrate (Migrar)** en la ventana emergente que se muestra.



La migración al modelo de ancho de banda agregado es permanente e irreversible. Antes de migrar, revise la lista de verificación previa a la migración. Debe ***Commit and Push (Confirmar y enviar)*** *sus cambios para que surtan efecto.*

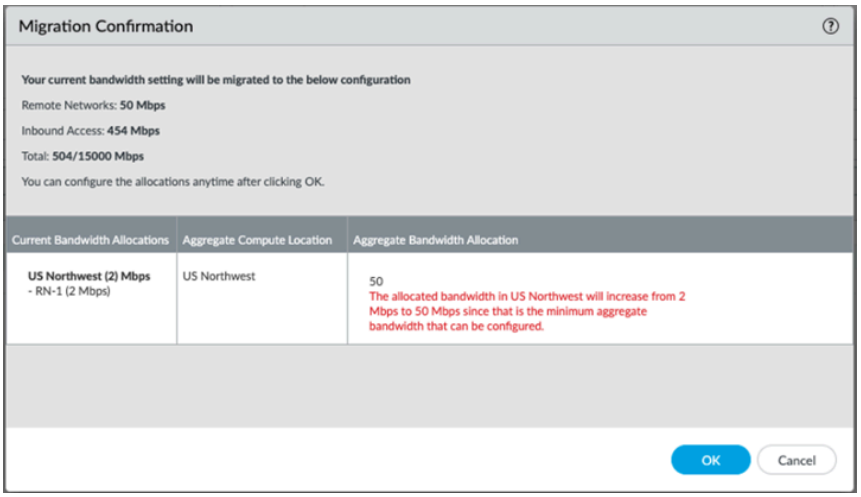
Si tiene perfiles de QoS con un ***Class Bandwidth Type (Tipo de ancho de banda)*** *de* ***Mbps****, Prisma Access le notifica que debe cambiar estos perfiles a un* ***Class Bandwidth Type (Tipo de ancho de banda)*** *de* ***Percentage (Porcentaje)****.*



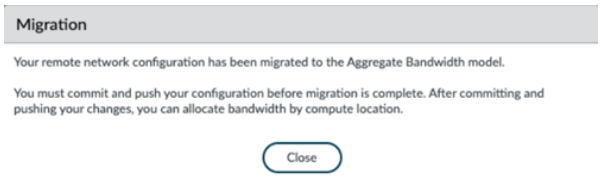
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Revise la información en la ventana **Migration Confirmation (Confirmación de migración)** y, a continuación, haga clic en **OK (Aceptar)**.

Si todas las ubicaciones en una ubicación de cómputo tienen un ancho de banda total de menos de 50 Mbps, Prisma Access aumentará el ancho de banda a 50 Mbps para esa ubicación de cómputo. Prisma Access le proporciona las ubicaciones que requieren el aumento del ancho de banda durante el proceso de migración.



Prisma Access migra el ancho de banda de red remoto asignado al modelo de ancho de banda agregado y muestra una ventana de confirmación. Haga clic en **Close (Cerrar)** para cerrar la ventana.



STEP 5 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

Incorpore una red remota

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Una vez que haya planificado su red remota, puede comenzar el proceso de configuración. Esto incluye la incorporación de la red remota y la conexión del sitio de red remota a Prisma Access y habilitar el enrutamiento y la calidad de servicio para la red remota. Para cada red remota que desee proteger mediante Prisma Access para redes, envíe la configuración de política requerida a Prisma Access e integre cada red remota para que pueda comenzar a enviar tráfico desde el sitio remoto a través del túnel IPSec a Prisma Access. Utilice uno de los siguientes procedimientos para integrar sus redes remotas según su tipo de asignación de ancho de banda:

Aprenda cómo integrar una red remota.

- Strata Cloud Manager
- Panorama

Incorpore una red remota (Strata Cloud Manager)

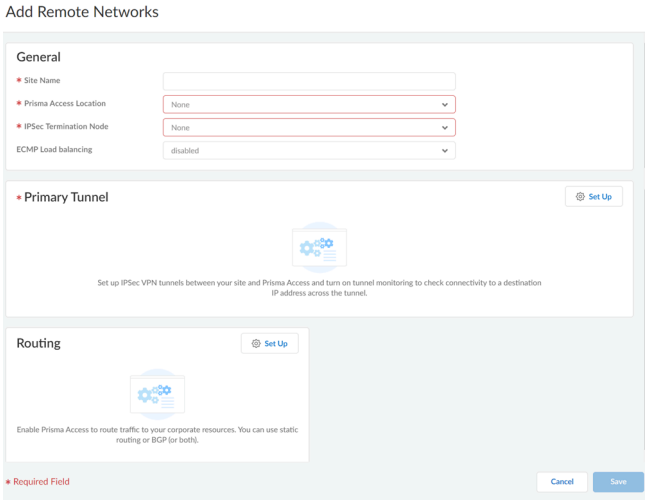
Le mostramos cómo añadir un nuevo sitio de red remoto a Prisma Access. Comenzará especificando la ubicación y definiendo la cantidad de ancho de banda que se asignará a la conexión.

STEP 1 | Iniciar Prisma Access (Managed by Strata Cloud Manager).

STEP 2 | Asegúrese de que ha asignado ancho de banda a la ubicación donde implementará la red remota. Consulte Lista de verificación de planificación para redes remotas.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Vaya a **Workflows (Flujos de trabajo)** > **Setup Prisma Access (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)** > **Add Remote Networks (Añadir redes remotas)**.



STEP 4 | Asigne a la red remota un **Site Name (Nombre de sitio)** descriptivo.

STEP 5 | Seleccione la **Region (Región)** en la que se encuentra el sitio y la **Location (Ubicación)** más cercana de Prisma Access.

STEP 6 | (Solo si planea usar BGP para el enrutamiento dinámico) Habilite el **ECMP Load Balancing (Equilibrio de carga ECMP)** para que el sitio de red remoto pueda usar hasta cuatro túneles IPSec.

Se requiere BGP para el equilibrio de carga ECMP; no se admiten QoS ni rutas estáticas.

Cuando habilita ECMP, el tráfico de red remota se equilibra en carga en los túneles que configura.

STEP 7 | Configure la **Advanced Settings (Configuración avanzada)**.

- (Opcional) Utilice **Static Entries (Entradas estáticas)** para resolver FQDNs a direcciones IP específicas.

  Esta funcionalidad puede ser útil si tiene servicios de internet para invitados en su organización y desea que sus invitados utilicen motores de búsqueda de forma segura, evitando que busquen material potencialmente inapropiado u ofensivo que podría estar en contra de la política de la empresa. Para ello, introduzca un **Name (Nombre)** único para la regla de entrada estática, un **FQDN** y la **Address (Dirección)** IP a la que debe dirigirse la solicitud FQDN.



 ©2025 Palo Alto Networks, Inc.

- Si desea que Prisma Access realice el proxy de las solicitudes DNS, configure valores para **UDP Queries Retries (Reintentos de consultas de UDP)** [el **Interval (Sec) [Intervalo (Seg)]** para reintentar la consulta en segundos y el número de **Attempts (Intentos)** de reintento que debe realizar.

STEP 8 | Conectar un sitio de red remoto a Prisma Access, donde creará un túnel VPN IPSec para conectar el sitio de red remoto a Prisma Access.

STEP 9 | Configure el enrutamiento estático.

1. Si utiliza rutas estáticas para enrutar el tráfico hacia y desde sitios de red remotos, seleccione **Add (Añadir)** para añadir las subredes IP o las direcciones IP que desea proteger en el sitio.

   Si realiza algún cambio en las subredes IP de su sede o red de centro de datos, debe actualizar manualmente las rutas estáticas.

STEP 10 | Configure el enrutamiento dinámico.

1. Para que el enrutamiento dinámico anuncie subredes de la sede central o del centro de datos, seleccione **Enable BGP for Dynamic Routing (Habilitar BGP para enrutamiento dinámico)**.
2. (Opcional) Seleccione un valor de **MRAI Timer (Temporizador MRAI)**.

   El enrutamiento BGP ofrece un temporizador que puede utilizar para adaptar la convergencia del enrutamiento BGP en su red llamada el *Intervalo mínimo de anuncio de ruta (MRAI)*. El MRAI actúa para limitar la velocidad de las actualizaciones según el destino, y los enrutadores BGP esperan al menos el tiempo MRAI configurado antes de enviar un anuncio para el mismo prefijo. Un número menor le proporciona un tiempo de convergencia más rápido pero crea más anuncios en su red. Un número mayor disminuye la cantidad de anuncios que se pueden enviar, pero también puede hacer que la convergencia de enrutamiento sea más lenta. Usted decide el número que desea colocar en su red para lograr el mejor equilibrio entre una convergencia de enrutamiento más rápida y menos anuncios.

   Configure un rango de MRAI de entre 1 y 600 segundos, con un valor predeterminado de 30 segundos.
3. Para reducir la cantidad de anuncios de subred IP de usuarios móviles a través de BGP a su equipo local del cliente (CPE), especifique Prisma Access para resumir las subredes antes de anunciarlas seleccionando **Summarize Mobile User Routes before advertising (Resumir rutas de usuarios móviles antes de anunciarlas)**.

   De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred especificada. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

 ©2025 Palo Alto Networks, Inc.

4. (Opcional) Para que Prisma Access desarrolle un anuncio de ruta predeterminada para la red remota usando eBGP, seleccione **Advertise the Default Route (Anunciar ruta predeterminada)**. Asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.
5. (Opcional) Si configuró una WAN secundaria y necesita cambiar la dirección de peer para el peer de BGP secundario (de respaldo), seleccione **Use different BGP Peer for Secondary Tunnel (Utilizar un par BGP diferente para el túnel secundario)** e introduzca un peer único y, opcionalmente, una dirección IP local para la WAN secundaria.
6. (Opcional) Seleccione **Do Not Export Routes (No exportar rutas)** para evitar que Prisma Access reenvíe rutas a la sede central o al centro de datos.

   Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

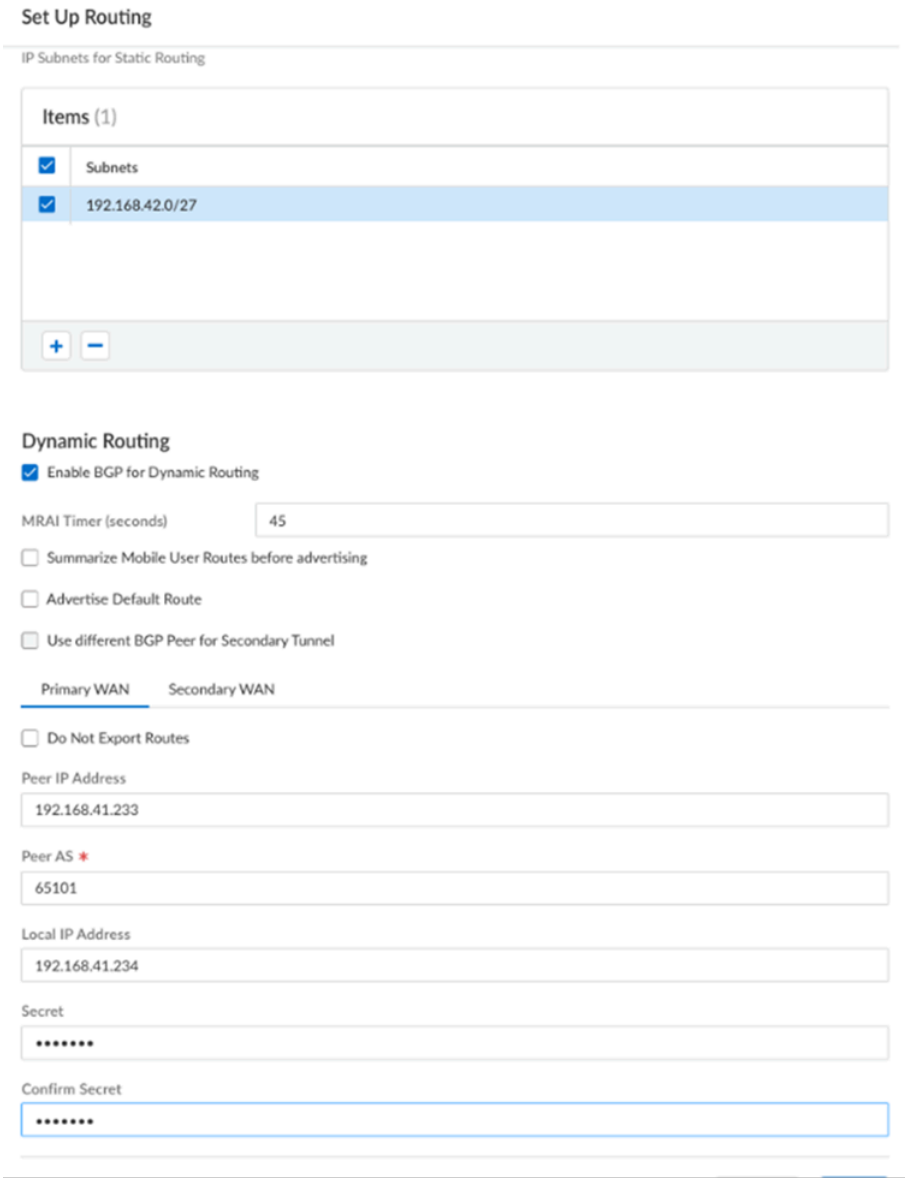
   Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en su equipo local para establecer rutas de regreso a Prisma Access.
7. Introduzca la **Peer IP Address (Dirección IP del peer)** asignada como ID del enrutador eBGP en la red de la sede central o del centro de datos.
8. Introduzca el **Peer AS (AS del peer)**, el sistema autónomo (AS) para su red.

   Utilice un número AS privado BGP compatible con RFC 6996.
9. Introduzca la **Local IP Address (Dirección IP local)** que Prisma Access utiliza como su dirección IP local para BGP.

   Solo se requiere una dirección local si su dispositivo de centro de datos o sede central la requiere para que el intercambio de BGP se realice correctamente. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP en la subred de infraestructura o subredes de la red remota.
10. Introduzca una contraseña **Secret (Secreta)** para autenticar las comunicaciones entre peers de BGP.

 ©2025 Palo Alto Networks, Inc.

11. Seleccione **Confirm Secret (Confirmar secreto)**.



Empezando con la versión Prisma Access 5.2, puede incorporar un máximo de 25.000 redes remotas y 50.000 puertas de enlace IKE por inquilino en una implementación de Prisma Access. Para adaptar esta mejora, se han realizado los siguientes cambios en la interfaz web de Strata Cloud Manager:

- La paginación está habilitada y puede elegir el número de filas que se mostrarán en una página determinada.

- El filtrado está habilitado para redes remotas.

  Después de aplicar el filtrado, puede ordenar el resultado por nombre.

 ©2025 Palo Alto Networks, Inc.

- Se añade un nuevo campo **Group By (Agrupar por)**. Si selecciona un grupo por **Compute Location (Ubicación de cómputo)**, se muestran todos los grupos, pero están contraídos, y el tamaño de página seleccionado se aplica a los grupos. Si selecciona una ubicación de cómputo para expandirla, las filas se muestran en función del tamaño de página seleccionado.

- Cuando las redes remotas se muestran en un menú desplegable, la interfaz web muestra los primeros 500 elementos. Puede encontrar la red remota deseada en la lista escribiendo en el cuadro de texto.

  Además, se muestra el número total de redes remotas.

- A las siguientes páginas adicionales se les ha aplicado la paginación:
  - Túneles IPSec:
  - QoS:
  - Estadísticas de QoS:
  - **Resolución de problemas—Redes remotas** en **External Dynamic Lists (Listas dinámicas externas)**:

Incorpore una red remota (Panorama)

Para configurar una implementación de red remota de Prisma Access que asigna ancho de banda por ubicación de cómputo, complete los siguientes pasos.

Si necesita incorporar muchas redes remotas (hasta 1000), puede incorporar una red remota mediante el siguiente procedimiento, luego exportar la configuración de la red remota a un archivo CSV, añadir las otras redes remotas que desea incorporar al archivo CSV y luego importar el archivo CSV para guardar la configuración en Prisma Access.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y edite la configuración haciendo clic en el icono de engranaje en el área **Settings (Configuración)**.

1. En la sección Plantillas, seleccione **Add (Añadir)** para añadir cualquier plantilla que contenga la configuración que desea enviar a Prisma Access para redes. Por ejemplo, si tiene plantillas existentes que contienen sus configuraciones de zona, túnel IPSec, puerta de enlace IKE o configuraciones de perfil criptográfico, puede añadirlas a la Remote_Network_Template_Stack predefinida para simplificar el proceso de incorporación.

   Puede **Add (Añadir)** más de una plantilla a la pila y, a continuación, ordénelas adecuadamente mediante **Move Up (Desplazar hacia arriba)** y **Move Down (Desplazar hacia abajo)**. Esto es importante porque Panorama evalúa la pila de arriba hacia abajo, dando prioridad a la configuración en las plantillas ubicadas más arriba sobre la misma

 ©2025 Palo Alto Networks, Inc.

configuración especificada en plantillas más abajo en la pila. Tenga en cuenta que no puede mover la plantilla predeterminada de la parte superior de la pila.

Aunque puede añadir plantillas existentes a la pila desde el complemento, no puede crear una nueva plantilla desde el complemento. En su lugar, utilice el flujo de trabajo para Add (Añadir) una nueva plantilla.

2. Seleccione el **Parent Device Group (Grupo de dispositivos principales)** para Prisma Access para redes remotas. Puede seleccionar un grupo de dispositivos existente o usar **Shared (Compartido)**.

   Enviará toda la configuración, incluida la política de seguridad, perfiles de seguridad y otros objetos de política (como grupos y objetos de aplicaciones y grupos de direcciones), objetos y perfiles HIP y política de autenticación, que Prisma Access para redes necesita para aplicar una política coherente a los usuarios de la red remota mediante el método jerarquía de grupos de dispositivos que especifique aquí.

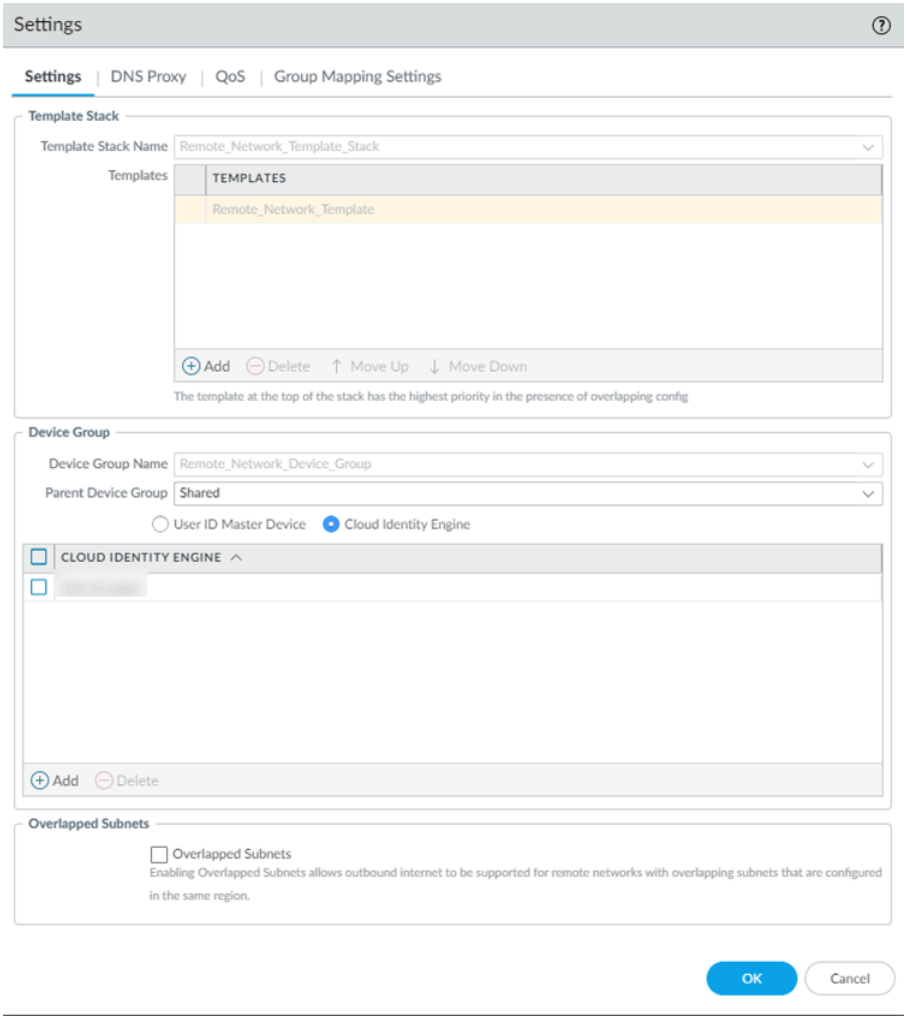
   Todavía no es necesario definir toda la política que insertará en la red remota. En su lugar, configure las opciones para incorporar el sitio remoto. A continuación, puede volver atrás y añadir las plantillas y los grupos de dispositivos con las configuraciones completas para enviar una política coherente a las redes remotas.

3. (Opcional) Si ha configurado un cortafuegos de nueva generación como dispositivo principal o añadió un perfil de Cloud Identity Engine para hacer que la información de usuario y grupo se pueda seleccionar en las políticas de seguridad, seleccione **User-ID Master Device (Dispositivo maestro de User-ID)** o **Cloud Identity Engine**; luego, seleccione el perfil Dispositivo maestro o el perfil de Cloud Identity Engine que creó.

 ©2025 Palo Alto Networks, Inc.

4. Si va a configurar redes remotas que tienen subredes superpuestas, seleccione la opción **Overlapped Subnets (Subredes superpuestas)** para habilitar el acceso saliente a Internet para esas ubicaciones.

   Mientras que la configuración de Ubicaciones de red remotas con subredes superpuestas introduce algunas limitaciones, es aceptable en algunos casos (por ejemplo, si desea añadir una red de invitados en una ubicación de comercio minorista).



STEP 2 | (Opcional) Configure la configuración de **DNS Proxy (Proxy DNS)** de la red remota.

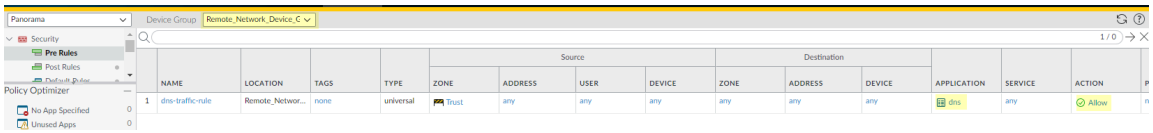
Prisma Access le permite especificar servidores DNS para resolver tanto los dominios internos de su organización como los dominios externos. Si no especifica ninguna configuración, Prisma Access no realiza la proxy de las solicitudes DNS para redes remotas.

1. En el grupo de dispositivos **Remote_Network_Device_Group**, seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir una regla de política

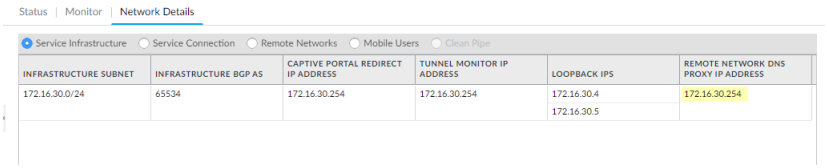
 ©2025 Palo Alto Networks, Inc.

de seguridad con un **Application (Aplicación)** de **DNS** y una **Action (Acción)** de **Allow (Permitir)** para permitir el tráfico DNS.

Sin una regla de política de seguridad para permitir el tráfico DNS, no se produce la resolución DNS.



2. Si configura Prisma Access para que realice el proxy de las solicitudes de DNS de las redes remotas, actualice la configuración de DNS en todos los endpoints de esa red para usar la **Remote Network DNS Proxy IP Address (Dirección IP de proxy DNS de red remota)** de Prisma Access como servidor DNS primario y utilice su servidor DNS como servidor DNS secundario. Puede obtener esta IP de proxy DNS desde **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Infrastructure (Infraestructura de servicios)**.



3. **Add (Añadir)** un o más ajustes de **DNS Proxy (Proxy DNS)**, introduciendo los siguientes valores:

   - Seleccione un **Region (Región)** en el menú desplegable en la parte superior de la ventana.

     Seleccione **Worlwide (Mundial)** para aplicar la configuración de DNS globalmente, seleccione un teatro específico o seleccione la configuración por grupo de ubicaciones (un grupo de ubicaciones que es más pequeño que el teatro). Si añade varios ajustes, primero se utilizan los ajustes del grupo de ubicaciones, luego los ajustes de teatro y, por último, los ajustes mundiales. Prisma Access evalúa las reglas de arriba hacia abajo en la lista.
   - **Add (Añadir)** una o más reglas para configurar los ajustes de DNS para **Internal Domain (Dominio interno)**.
     - Introduzca un **Rule Name (Nombre de regla)** único para la regla.
     - Sí desea que su servidor DNS interno solo resuelva los dominios que especifique, introduzca los dominios que desea resolver en la **Lista de dominios**. Especifique un asterisco delante del dominio; por ejemplo, *.acme.com. Puede especificar un máximo de 1.024 entradas de dominio.
     - Si tiene un **Custom DNS server (Servidor DNS personalizado)** que puede acceder a sus dominios internos, especifique las direcciones IP del servidor **Primary DNS DNS principal** y del servidor **Secondary DNS DNS secundario**, o seleccione **Use Cloud DefaultUsar Cloud Default** para usar el valor predeterminado del servidor DNS de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

- Especifique la configuración de DNS para **Public Domains (Dominios Públicos)**.
  - **Use Cloud Default (Usar el valor predeterminado de la nube)**: utilice el valor predeterminado del servidor DNS de Prisma Access.
  - **Same as Internal Domains (Igual que dominios internos)**: utilice el mismo servidor que utiliza para resolver dominios internos. Cuando selecciona esta opción, el servidor DNS utilizado para resolver dominios públicos es el mismo que el servidor configurado para la primera regla en la sección **Internal Domains (Dominios internos)**.
  - **Custom DNS server (Servidor DNS personalizado)**: si tiene un servidor DNS que puede acceder a sus dominios públicos (externos), introduzca la dirección del servidor DNS principal en ese campo.

  (Opcional) Puede **Add (Añadir)** un **DNS Suffix (Sufijo DNS)** para especificar el sufijo que el cliente deberá usar localmente cuando se introduce un nombre de host no cualificado que no puede resolver, por ejemplo, acme.local. No introduzca un carácter comodín (*) antes del sufijo de dominio (por ejemplo, acme.com). Puede añadir varios sufijos.
- Si quiere que Prisma Access realice la proxy de las solicitudes DNS, configure los valores de Configurar para el uso de consultas UDP [el **Interval (Intervalo)** para volver a intentar la consulta en segundos y el número de reintentos **Attempts (Intentos)** a realizar).

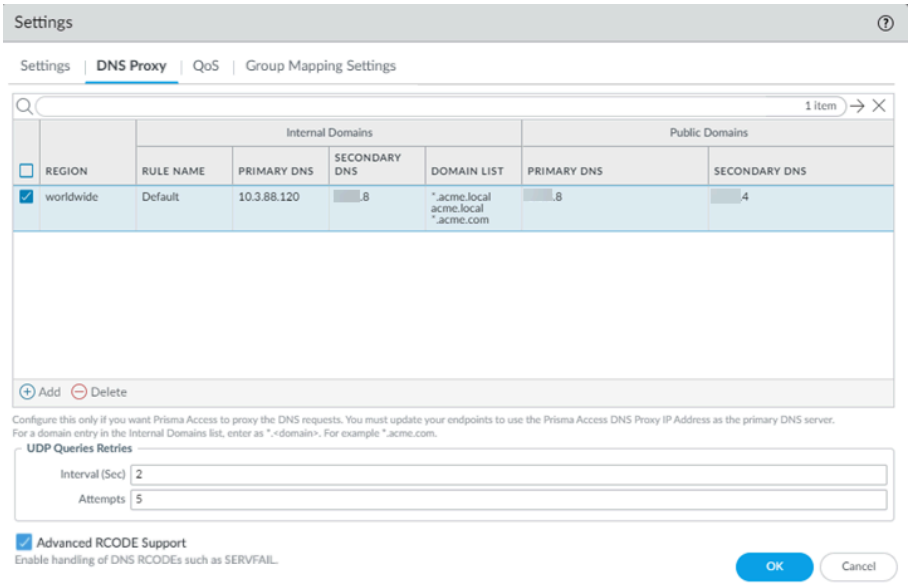
  Si desea que Prisma Access realice el proxy de las solicitudes de DNS de los usuarios de GlobalProtect, debe actualizar los endpoints para utilizar la **Remote Network DNS Proxy IP Address (Dirección IP de proxy DNS de red remota)** como servidor DNS principal [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Infrastructure (Infraestructura de servicios)**].

4. (Opcional) Seleccione Advanced RCODE Support (Compatibilidad avanzada con RCODE) para permitir que el servidor DNS primario falle al servidor DNS secundario si se recibe un código de retorno DNS RCODE 2 (SERVFAIL) y RCODE 5 (REFUSED).

   Un código de respuesta DNS de SERVFAIL hace referencia a un error de comunicación con el servidor DNS primario, y un código de respuesta DNS de REFUSED significa que

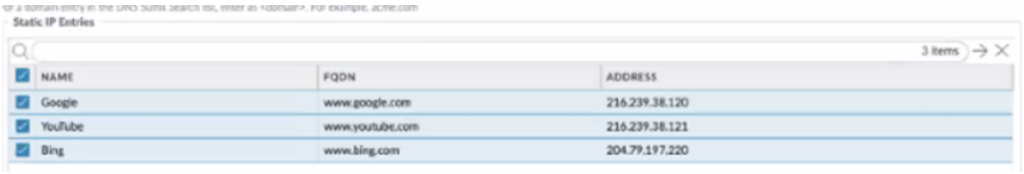
 ©2025 Palo Alto Networks, Inc.

el servidor DNS primario se negó a proporcionar la información solicitada. En ambos casos, el servicio realiza la conmutación por error al servidor DNS secundario.



5. (Opcional) Utilice **Static Entries (Entradas estáticas)** para resolver FQDN en direcciones IP específicas.

   Esta funcionalidad puede ser útil si tiene servicios de Internet para invitados en su organización y desea que sus invitados utilicen los motores de búsqueda de forma segura, lo que les impide buscar material potencialmente inapropiado u ofensivo que podría ir en contra de la política de la empresa. Para ello, introduzca un **Name (Nombre)** único en el caso de la regla de entrada estática, un **FQDN** y la **Address (Dirección)** IP a dónde se debe dirigir la solicitud de FQDN.



STEP 3 | (Opcional) Habilite **QoS** para la implementación de red remota y especifique un **QoS Profile (Perfil de QoS)**, una **Guaranteed Bandwidth Ratio (Relación de ancho de banda garantizada)**, la cantidad de ancho de banda **Reserved for Guaranteed Bandwidth (Mbps) [Reservado para ancho de banda garantizado (Mbps)]** y, opcionalmente, personalice las opciones del sitio por ubicación [**Customize Per Site (Personalizar por sitio)**].

Habilite QoS a nivel de ubicación de cómputo; sin embargo, puede optar por habilitarlo o deshabilitarlo por sitio y especificar un perfil de QoS por sitio cuando añade su red remota en un paso posterior. Antes de configurar QoS, debe comprender cómo funciona QoS para redes remotas que asignan ancho de banda por ubicación de cómputo, incluida la especificación del ancho de banda garantizado y personalización del ancho de banda por sitio.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Configure **Group Mapping Settings (Configuración de asignación de grupos)** para que Prisma Access utilice el componente Directory Sync de Cloud Identity Engine para recuperar información de usuarios y grupos.

Debe configurar Cloud Identity Engine para recuperar información de usuarios y grupos desde su Active Directory (AD) antes de habilitar la asignación de grupos en Prisma Access usando la **Group Mapping Settings (Configuración de asignación de grupos)**.

STEP 5 | Cree nuevas zonas en una de las plantillas de la pila [**Network > Zones> Add (Network > Zonas > Añadir)**] o asigne las zonas a las que se hace referencia en las plantillas existentes que añadió a la pila como de confianza o de no confianza. En Panorama, las reglas de políticas se definen en grupos de dispositivos y las zonas se definen en plantillas. Por lo tanto, debe asegurarse de añadir las plantillas que hacen referencia a las zonas incluidas en las reglas de directiva a la pila de plantillas.

En un cortafuegos de nueva generación de Palo Alto Networks®, la política de seguridad se aplica entre zonas, que se asignan a interfaces físicas o virtuales en el cortafuegos. Pero dado que Prisma Access para redes tiene solo dos zonas, confianza y desconfianza, debe asignar cualquier zona con tráfico vinculado a Internet (incluidas las aplicaciones SaaS autorizadas) como desconfianza y todas las zonas internas como confianza.

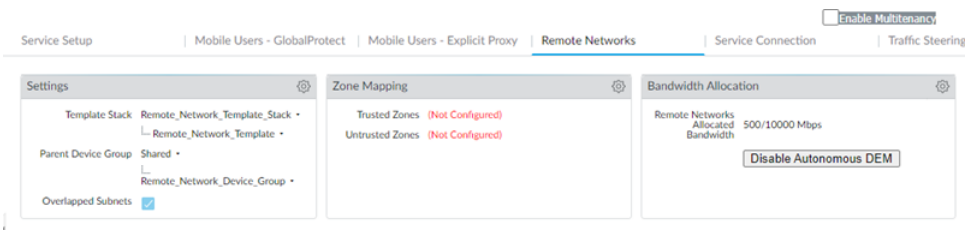
1. (Opcional) Edite la configuración de asignación de zonas.

   De forma predeterminada, todas las zonas de Prisma Access para redes, la pila de plantillas A se clasifican como zonas que no son de confianza. Si aún no ha definido zonas o si las plantillas del Remote_Network_Template_Stack no tienen configuraciones de zona, puede volver y añadirlas cuando inserte la política en Prisma Access para redes.
2. Para cada zona que desee designar como de confianza, selecciónela y haga clic en **Add (Añadir)** para moverla a la lista de **Trusted Zones (Zonas de confianza)**.
3. Haga clic en **OK (Aceptar)** para guardar las asignaciones.

STEP 6 | Asigne ancho de banda a las ubicaciones que desea incorporar haciendo clic en el icono de engranaje en el área **Bandwidth Allocation (Asignación de ancho de banda)**.

El ancho de banda se asigna a un nivel de agregado por ubicación de cómputo. Consulte Redes remotas de Prisma Access para obtener más detalles.

*Si ha eliminado Autonomous DEM como licencia complementaria, o si elimina Autonomous DEM para redes remotas de su licencia, seleccione **Disable Autonomous DEM (Deshabilitar Autonomous DEM)**. Si elimina Autonomous DEM para redes remotas y no deshabilita Autonomous DEM, recibirá un error al confirmar.*



Si tiene una implementación de redes remotas existente que actualmente incorpora redes remotas por ubicación, una ventana emergente aparecerá que le preguntará si desea migrar al

 ©2025 Palo Alto Networks, Inc.

modelo de ancho de banda agregado. Haga clic en **Migrate (Migrar)** para continuar o en **Cancel (Cancelar)** para cancelar la migración.

> *La migración al modelo de ancho de banda agregado es permanente e irreversible. Antes de migrar, revise la lista de verificación previa a la migración. Debe:* ***Commit and Push (Confirmar y enviar)*** *sus cambios para que surtan efecto.*

La **Service IP Address (Dirección IP del servicio)** (el la dirección IP pública utilizada en el lado de Prisma Access del túnel IPSec para la conexión de red remota) no cambia cuando migra su implementación al modelo de ancho de banda agregado y no se requiere ninguna reconfiguración de su túnel IPSec.

STEP 7 | Introduzca la **Bandwidth Allocation (Asignación de ancho de banda)** que desea para cada **Compute Location (Ubicación de cómputo)** asociada con las **Prisma Access Locations (Ubicaciones de Prisma Access)** a las que desea incorporarse.

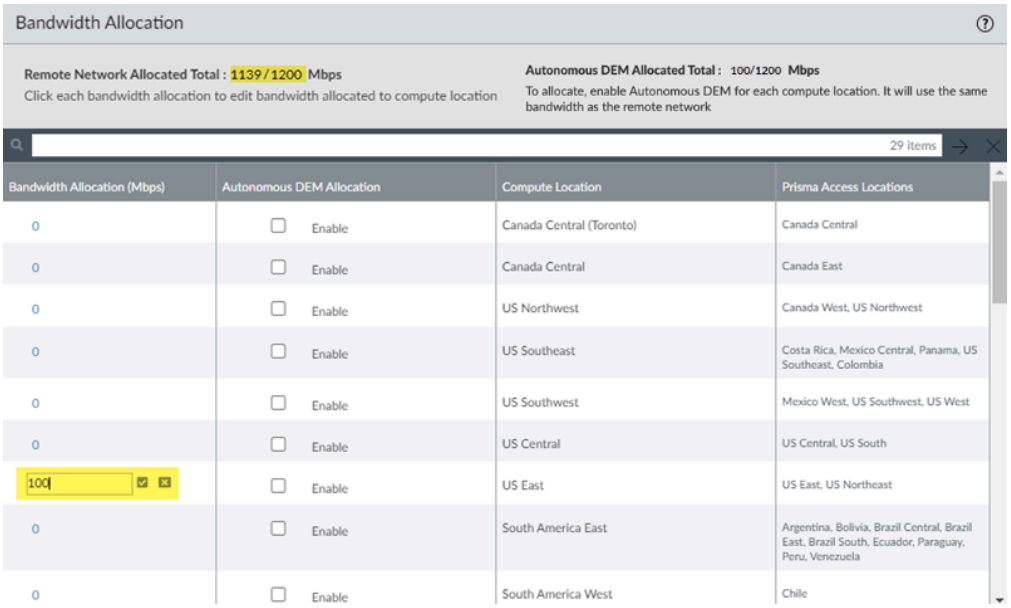
Para verificar la cantidad de ancho de banda introducido, seleccione la marca de verificación junto a la cantidad de ancho de banda; para cancelar la cantidad, seleccione **x**.

Especifique un ancho de banda mínimo de 50 Mbps y un ancho de banda máximo del ancho de banda máximo restante con licencia.

STEP 8 | (Opcional, solo implementaciones con licencias de Autonomous DEM para redes remotas) **Enable (Habilitar) Autonomous DEM Allocation (Asignación de Autonomous DEM)** para la ubicación de cómputo para la cual asignó ancho de banda.

Si habilita Autonomous DEM para la ubicación de cómputo, la cantidad de ancho de banda utilizada por la licencia de Autonomous DEM es la misma que el ancho de banda que especifica para la ubicación de cómputo. El **Autonomous DEM Allocated Total (Número total asignado de Autonomous DEM)** muestra cuánto ancho de banda utiliza Autonomous DEM y cuánto queda. Consulte la guía de Autonomous DEM para obtener más información.

STEP 9 | Espere a que el ancho de banda se refleje en el campo **Allocated Total (Total asignado)** en la parte superior de la página; luego, haga clic en **OK (Aceptar)**.



 ©2025 Palo Alto Networks, Inc.

STEP 10 | (Opcional) Si desea configurar su red remota para proporcionar acceso entrante seguro a ubicaciones de red remotas, haga clic en la pestaña **Inbound Access Remote Networks (Redes remotas de acceso entrante)** y siga el flujo de trabajo para configurar el acceso entrante seguro para una red remota.

STEP 11 | Seleccione **Add (Añadir)** para añadir una red remota y especifique un **Name (Nombre)**.

No puede cambiar el nombre de la ubicación de red remota después de introducirla. Asegúrese de conocer el esquema de nomenclatura de las redes remotas antes de comenzar la incorporación.

STEP 12 | (Opcional, solo implementaciones de BGP) Cree una configuración para que su conexión de red remota pueda usar hasta cuatro túneles IPSec para su tráfico [**ECMP Load Balancing (Equilibrio de carga ECMP)**].

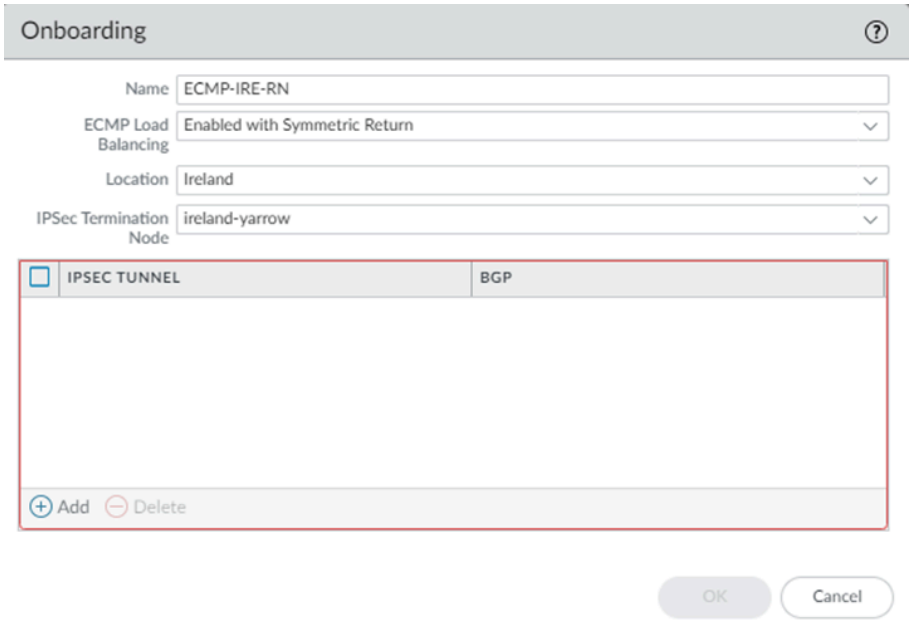
Las rutas estáticas (se requiere BGP) no son compatibles y, si tiene QoS configurado, no puede cambiar la ratio de asignación para los enlaces ECMP. Si su implementación utiliza un túnel IPSec para su conexión de red remota o utiliza rutas estáticas, seleccione **None (Ninguna)** para **ECMP Load Balancing (Equilibrio de carga ECMP)** y continúe con el Paso 15.

1. Seleccione una de las opciones para habilitar o deshabilitar el equilibrio de carga ECMP.
   - **None (Ninguno)**: no utilice el equilibrio de carga ECMP (utilice un único túnel de red remota para esta conexión de red remota). Esta es la única opción que puede elegir para las rutas estáticas; BGP es necesario para el equilibrio de carga de ECMP.
   - **Enabled with Symmetric Return (Habilitado con retorno simétrico)**: especifique hasta cuatro túneles IPSec para esta conexión de red remota y fuerce a Prisma Access a utilizar el mismo enlace para el tráfico de retorno que el utilizado para enviar el tráfico.

     Seleccione esta opción si utiliza uno o más túneles como túnel de respaldo para usarlos solo si uno de los túneles principales deja de funcionar. Si un enlace

 ©2025 Palo Alto Networks, Inc.

falla, Prisma Access utiliza uno de los otros túneles para enviar y recibir tráfico simétricamente.



2. Seleccione **Add (Añadir)** para añadir un túnel IPSec para la conexión de red remota y especifique los siguientes valores:

   - **Enable (Habilitar)**: habilita BGP para el túnel IPSec.

     Esta selección no es configurable; debe habilitar BGP para configurar ECMP.

   - **Summarize Mobile User Routes before advertising (Resumir las rutas de los usuarios móviles antes de anunciarse)**: realiza un resumen para reducir el número de anuncios de subred IP de usuarios móviles a través de BGP a los equipos de las instalaciones del cliente (CPE).

     De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred especificada. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

     Si habilita el resumen de ruta para una ubicación que usa ECMP, debe habilitar el resumen de ruta en todos los enlaces a esa ubicación o recibirá un error durante la confirmación.

     Prisma Access establece la cadena de comunidad para las rutas de usuarios móviles agregadas en `0xFFFE:0xFFF0`.

 ©2025 Palo Alto Networks, Inc.

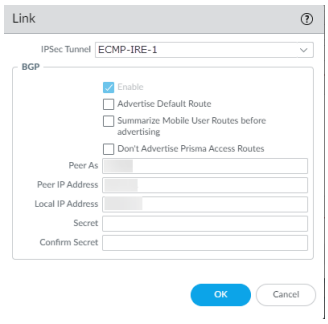
- **Advertise Default Route (Publicitar ruta predeterminada)**: Prisma Access origina un anuncio de ruta predeterminado para la red remota utilizando eBGP.

  Asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.

- **Don't Advertise Prisma Access Route (No anunciar ruta de Prisma Access)**: impide que el peer BGP de Prisma Access reenvíe rutas a la red de su organización.

  Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

  Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.



- (Opcional) Seleccione un valor de temporizador de **MRAI**.

  El enrutamiento BGP ofrece un temporizador que puede usar para adaptar la convergencia de enrutamiento BGP en su red llamado *intervalo mínimo de* publicidad de ruta. El MRAI actúa para limitar la velocidad de las actualizaciones según el destino, y los enrutadores BGP esperan al menos el tiempo MRAI configurado antes de enviar un anuncio para el mismo prefijo. Un número menor le proporciona un tiempo de convergencia más rápido pero crea más anuncios en su red. Un número mayor disminuye la cantidad de anuncios que se pueden enviar, pero también puede hacer que la convergencia de enrutamiento sea más lenta. Usted decide el número a poner en su red para el mejor equilibrio entre una convergencia de enrutamiento más rápida y menos anuncios.

  Configure un rango MRAI de entre 1 y 600 segundos, con un valor predeterminado de 30 segundos.

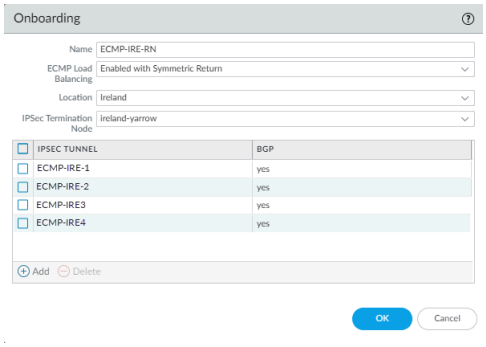
- **Peer AS (AS de peers)**: especifique el sistema autónomo (AS) al que pertenece el cortafuegos, el enrutador virtual o el enrutador BGP en su red remota.
- **Peer IP Address (Dirección IP del peer)**: introduzca la dirección IP asignada como ID del enrutador eBGP en la red remota para la que está configurando esta conexión.

 ©2025 Palo Alto Networks, Inc.

- **Local IP Address (Dirección IP local)** (Opcional): introduzca una dirección que Prisma Access utiliza como su dirección IP local para BGP. Especifique la dirección IP que se utilizará en el extremo del túnel de Prisma Access.

  Especificar una **Local Address (Dirección local)** es útil cuando el dispositivo en el otro lado de la conexión (como una puerta de enlace privada virtual de Amazon Web Service (AWS)) requiere una dirección IP local específica para que el intercambio de BGP se realice correctamente. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP de la subred de infraestructura o las subredes de la red remota.
- **Secret (Secreto)** y **Confirm Secret (Confirmar secreto)** (opcional): introduzca y confirme una frase de contraseña para autenticar las comunicaciones entre peers de BGP.

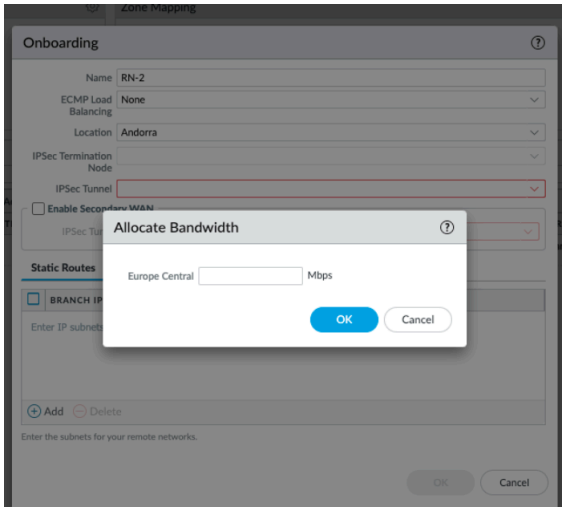
3. Repita el paso anterior para añadir hasta cuatro túneles para usar con la conexión de red remota.



 ©2025 Palo Alto Networks, Inc.

STEP 13 | Seleccione la **Location (Ubicación)** en la que Prisma Access implementará la infraestructura necesaria para proteger su ubicación de red remota. Esta región debe estar ubicada geográficamente cerca de la ubicación de su red remota.

Si aún no ha asignado ancho de banda para la ubicación de cómputo a la que se asigna la ubicación, Prisma Access le solicita que introduzca el ancho de banda para esa ubicación de cómputo.



Las ubicaciones denotadas con dos asteriscos son **Local Zones (Zonas locales)**. Estas ubicaciones colocan los servicios de cómputo, almacenamiento, bases de datos e infraestructura cerca de grandes centros de población e industrias, sin embargo, también tienen algunas limitaciones. Para añadir una zona local, póngase en contacto con su representante de Palo Alto Networks.

STEP 14 | Seleccione el **IPSec Termination Node (Nodo de terminación IPSec)** que desea utilizar para esta red remota.

Prisma Access utiliza este nodo para asociar ubicaciones de red remotas con ubicaciones de cómputo.

STEP 15 | (Solo enrutamiento estático o implementaciones de un único túnel) Seleccione o añada una nueva configuración de **IPSec Tunnel (Túnel IPSec)** para acceder al cortafuegos, enrutador o dispositivo SD-WAN en la ubicación corporativa:

- Seleccione una de las plantillas IPSec predefinidas en Remote_Network_Template o, si añadió una plantilla a Remote_Network_Template_Stack (o modificó la Remote_Network_Template predefinida) que incluye una configuración de túnel IPSec, seleccione ese **IPSec Tunnel (Túnel IPSec)** en el menú desplegable. Tenga en cuenta que el túnel que está creando para cada conexión de red remota conecta Prisma Access al dispositivo compatible con IPSec en cada sucursal.

  Utilice las siguientes pautas cuando configure un túnel IPSec:

  - Las direcciones de peers en la configuración de IKE Gateway deben ser únicas para cada túnel. Sin embargo, puede reutilizar algunos de los otros elementos de configuración comunes, como los perfiles criptográficos.
  - El túnel IPSec que seleccione de una plantilla debe utilizar el intercambio automático de claves e IPv4 únicamente.

 ©2025 Palo Alto Networks, Inc.

    - Los nombres del túnel IPSec, la puerta de enlace IKE y el perfil criptográfico no pueden superar los 31 caracteres.
    - Si incorpora varias redes remotas en la misma ubicación con peers IKE dinámicos, debe usar el mismo perfil criptográfico IKE para todas las configuraciones de red remota.
- Para crear una nueva configuración de túnel IPSec, haga clic en **New IPSec Tunnel (Nuevo túnel IPSec)**, asígnele un **Name (Nombre)** y configure los ajustes de Puerta de enlace IKE, Perfil criptográfico IPSec y Supervisión de túneles.
    - Si el dispositivo compatible con IPSec en su sucursal utiliza VPN basada en políticas, en la pestaña **Proxy IDs (ID de proxy)**, elija **Add (Añadir)** un ID de proxy que coincida con la configuración configurada en su dispositivo IPSec local para garantizar que Prisma Access pueda establecer correctamente un túnel IPSec con su dispositivo local.
- Deje seleccionado **Enable Replay Protection (Activar protección de reproducción)** para detectar y neutralizar ataques de reproducción.
- Marque **Copy TOS Header (Copiar encabezado de TOS)** para copiar el encabezado del tipo de servicio (type of service, ToS) del encabezado de la IP interna en el encabezado de la IP externa de los paquetes encapsulados a fin de conservar la información original del TOS.
- Para habilitar la supervisión de túnel para la conexión de servicio, seleccione **Tunnel Monitor (Supervisión de túnel)**.
    - Introduzca una dirección **Destination IP (IP de destino)**.

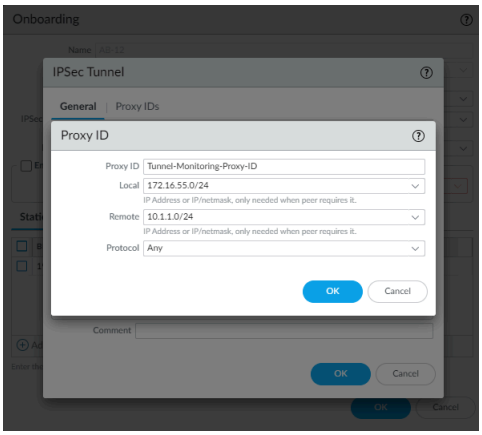
      Especifique una dirección IP en la ubicación de su sucursal a la que Prisma Access pueda enviar solicitudes de ping ICMP para la supervisión del túnel IPSec. Asegúrese de que

 ©2025 Palo Alto Networks, Inc.

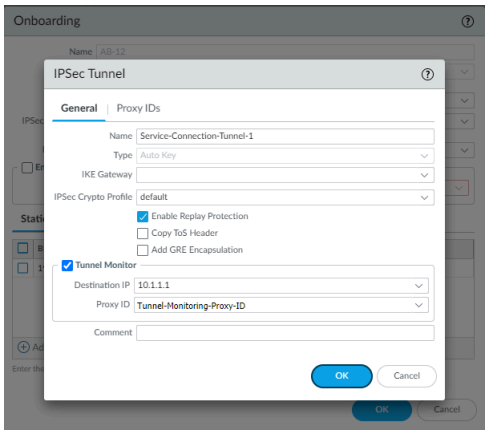
el ICMP pueda acceder a esta dirección desde toda la subred de la infraestructura de Prisma Access.

- Si utiliza la supervisión de túnel con un dispositivo de peer que utiliza varios ID de proxy, especifique un **Proxy ID (ID de proxy)** o añada un **New Proxy ID (ID de proxy nuevo)** que permita el acceso desde la subred de la infraestructura a la ubicación de su sucursal.

  La siguiente figura muestra un ID de proxy con la subred de la infraestructura del servicio (172.16.55.0/24 en este ejemplo) como la subred IP **Local (Local)** y la subred de la ubicación de la sucursal (10.1.1.0/24 en este ejemplo) como la subred **Remote (Remota)**.



  La siguiente figura muestra el ID de proxy que creó aplicándose a la configuración del monitor de túnel mediante su especificación en el campo **Proxy ID (ID de proxy)**.



Debe configurar en su CPE una ruta estática a la dirección IP del monitor de túnel para que funcione la supervisión del túnel. Para encontrar la dirección IP de destino que se utilizará para la supervisión del túnel desde la ubicación de su sucursal hasta Prisma Access, seleccione ***Panorama*** *>* ***Cloud Services (Servicios en la nube)*** *>* ***Status (Estado)*** *>* ***Network Details (Detalles de red)****, haga clic en el botón* ***Service Infrastructure (Infraestructura de servicios)*** *y encuentre la* ***Tunnel Monitor IP Address (Dirección IP de la supervisión del túnel)****.*

 ©2025 Palo Alto Networks, Inc.

STEP 16 | Si tiene un enlace WAN secundario en esta ubicación, seleccione **Enable Secondary WAN (Habilitar WAN secundaria)**.

Asegúrese de crear un túnel IPSec único para la WAN secundaria de cada red remota; Prisma Access no es compatible con la reutilización del mismo túnel IPSec para WAN secundarias en múltiples redes remotas.

La configuración de una WAN secundaria no se admite en las siguientes implementaciones:

- Si su WAN secundaria está configurada en modo activo-activo con el túnel IPSec primario.
- Si el equipo de las instalaciones del cliente (CPE) está configurado en una configuración de enrutamiento multipath de igual coste (ECMP) con el túnel IPSec primario y secundario.

Si utiliza rutas estáticas, el tiempo de conmutación por error del túnel es inferior a 15 segundos desde el momento de la detección, dependiendo de su proveedor de WAN.

Si configura el enrutamiento de BGP y ha habilitado la supervisión del túnel, el tiempo de espera predeterminado más corto para determinar que un índice de parámetro de seguridad (SPI) está fallando es el monitor del túnel, que elimina todas las rutas a un par cuando detecta un fallo del túnel durante 15 segundos consecutivos. De esta forma, el monitor de túnel determina el comportamiento de las rutas BGP. Si no configura la supervisión del túnel, el temporizador de mantenimiento determina el tiempo que el túnel estará inactivo antes de eliminar la ruta. Prisma Access utiliza el valor BGP HoldTime predeterminado de 90 segundos según lo definido por RFC 4271, que es el tiempo máximo de espera antes de que Prisma Access elimine una ruta para un SPI inactivo. Si el dispositivo peer BGP tiene un tiempo de espera configurado más corto, el temporizador de espera BGP utilizará el valor más bajo.

Cuando el túnel secundario se instala correctamente, la ruta secundaria tiene prioridad hasta que el túnel principal vuelva a subir. Si tanto la ruta primaria como la secundaria están activas, la ruta principal tiene prioridad.

Si utiliza un peer BGP diferente para la conexión secundaria (de respaldo), Prisma Access no respeta los atributos del discriminador de salidas múltiples (MED) anunciados por el CPE. Esta advertencia se aplica si utiliza varios peers BGP en conexiones de red remotas o en conexiones de servicio.

STEP 17 | Habilite el enrutamiento a las subredes o direcciones IP individuales en el sitio de red remoto a las que sus usuarios necesitarán acceder.

Prisma Access utiliza esta información para dirigir las solicitudes al sitio apropiado. Las redes de cada sitio no pueden superponerse entre sí ni con los grupos de direcciones IP que usted designó para la infraestructura del servicio o para Prisma Access para grupos de IP de usuarios. Puede configurar **Static Routes (Rutas estáticas)**, **BGP**o una combinación de ambas.

- Para configurar **Static Routes (Rutas estáticas)**:
  1. En la pestaña **Static Routes (Rutas estáticas)**, haga clic en **Add (Añadir)** e introduzca la dirección de subred (por ejemplo, 172.168.10.0/24) o la dirección IP individual de un recurso, como un servidor DNS (por ejemplo, 10.32.5.1/32) al que sus usuarios remotos necesitarán acceder.

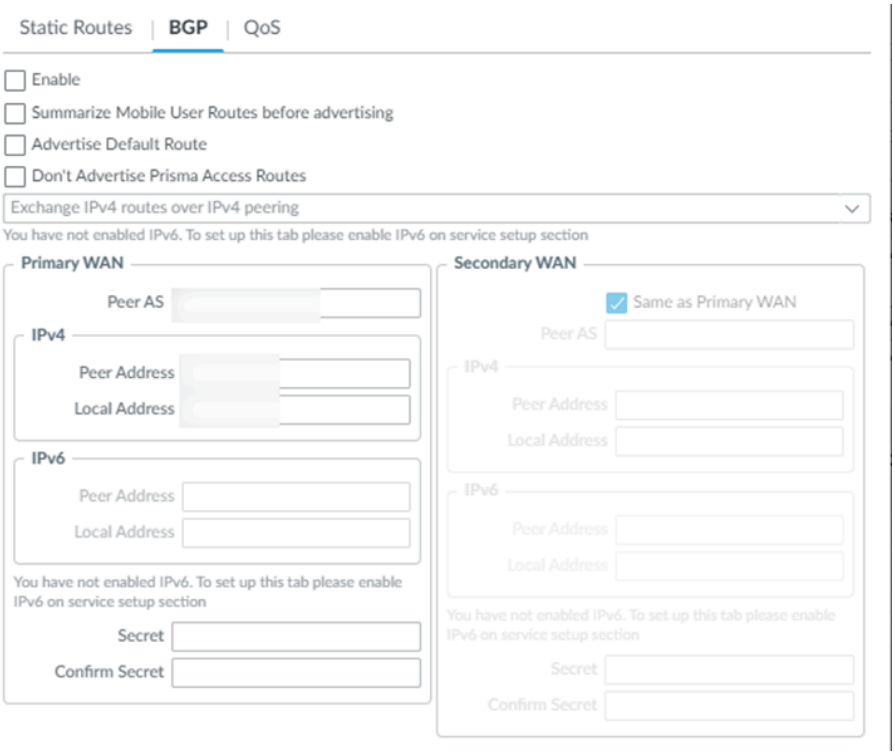
 ©2025 Palo Alto Networks, Inc.

2. Repita esto para todas las subredes o direcciones IP que Prisma Access necesitará acceso a esta ubicación.



- Para configurar **BGP**:

1. Seleccione la pestaña **BGP**.
2. (Opcional) Seleccione las opciones **ECMP Load Balancing (Equilibrio de carga ECMP)**. Consulte el Paso 12.
3. Si selecciona **None (Ninguno)** para **ECMP Load Balancing (Equilibrio de carga de ECMP)**, introduzca las opciones de BGP.



4. Para habilitar BGP para la conexión de red remota, seleccione **Enable (Habilitar)**.

   Cuando habilita BGP, Prisma Access establece el valor de tiempo de vida útil (TTL) para BGP externo (eBGP) en 8 para acomodar cualquier salto adicional que pueda ocurrir entre la infraestructura de Prisma Access y el equipo de las instalaciones de su cliente (CPE) que finaliza la conexión eBGP.
5. Para reducir el número de anuncios de subred IP de usuarios móviles a través de BGP a los equipos de las instalaciones del cliente (CPE) resumiéndolos, seleccione **Summarize**

 ©2025 Palo Alto Networks, Inc.

Mobile User Routes before advertising (Resumir rutas de usuarios móviles antes de anunciar).

De forma predeterminada, Prisma Access anuncia los grupos de direcciones IP de los usuarios móviles en bloques de /24 subredes; si los resume, Prisma Access anuncia el grupo en función de la subred especificada. Por ejemplo, Prisma Access anuncia un grupo de direcciones IP móviles de usuarios públicos de 10.8.0.0/20 utilizando la subred /20, en lugar de dividir el grupo en subredes de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, etc. antes de anunciarlas. Resumir estos anuncios puede reducir el número de rutas almacenadas en las tablas de enrutamiento de CPE. Por ejemplo, puede utilizar el resumen de grupo de IP con puertas de enlace VPN en la nube (puertas de enlace privadas virtuales (VGW) o puertas de enlace de tránsito (TGW)) que pueden aceptar un número limitado de rutas.

Prisma Access establece la cadena de comunidad para las rutas de usuarios móviles agregadas en `0xFFFE:0xFFF0`.

6. Para permitir que Prisma Access anuncie una ruta predeterminada para la red remota usando eBGP, seleccione **Advertise Default Route (Anunciar ruta predeterminada)**.

   Si selecciona **Advertise Default Route (Anunciar ruta predeterminada)**, asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría generar problemas de enrutamiento en su red.

   Debe publicar sus rutas predeterminadas antes de realizar esta selección para publicitarlas. Además, asegúrese de que su red no tenga otra ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.

7. Para evitar que el peer de BGP en el cortafuegos Prisma Access reenvíe rutas a la red de su organización, seleccione **Don't Advertise Prisma Access Routes (No anunciar rutas de Prisma Access)**.

   Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

   Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en el equipo local para establecer rutas de regreso a Prisma Access.

8. Introduzca el **Peer AS (AS de peer)**, que es el sistema autónomo (AS) al que pertenece el cortafuegos, el enrutador virtual o el enrutador BGP en su red remota.
9. Introduzca la dirección IP asignada como ID de enrutador del enrutador eBGP en la red remota para la que está configurando esta conexión como **Peer Address (Dirección de peer)**.
10. (Opcional) Introduzca una dirección que Prisma Access utiliza como su dirección IP local para BGP.

    Especificar una **Local Address (Dirección local)** es útil cuando el dispositivo en el otro lado de la conexión (como una puerta de enlace privada virtual de Amazon Web Service (AWS)) requiere una dirección IP local específica para que el intercambio de BGP se

 ©2025 Palo Alto Networks, Inc.

realice correctamente. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP de la subred de infraestructura o las subredes de la red remota.

*Debe configurar una ruta estática en su CPE a la **Local Address (Dirección local)**de BGP.*

11. (Opcional) Introduzca y confirme una frase de contraseña para autenticar las comunicaciones entre peers de BGP.
12. (Opcional) Si configuró una **Secondary WAN (WAN secundaria)** y necesita cambiar la **Peer Address (Dirección del peer)** o la **Local Address (Dirección local)** para el peer BGP secundario (copia de seguridad), anule la marca de **Same as Primary WAN (Igual que la WAN principal)** e introduzca un peer único y, opcionalmente, una dirección IP local para la WAN secundaria.

    Si utiliza redes IPv6 en su implementación de red remota, puede configurar direcciones **IPv6** así como también direcciones **IPv4** . También debe habilitar la red IPv6 a nivel global en su Infraestructura de Prisma Access antes de poder utilizar el direccionamiento IPv6.

    En algunas implementaciones (por ejemplo, cuando se usa BGP para conectarse con una puerta de enlace VPN de AWS), el peer BGP para la WAN primaria y secundaria puede ser diferente. En esos escenarios, puede optar por configurar un par BGP diferente para la WAN secundaria.

    *Para implementaciones de BGP con WAN secundarias, Prisma Access establece los túneles primario y secundario en un estado **UP (Activo)** pero sigue el comportamiento normal de respaldo activo BGP para el tráfico de red. Prisma Access establece el túnel principal como activo y envía y recibe tráfico únicamente a través de ese túnel; si el túnel principal falla, Prisma Access detecta el fallo utilizando reglas BGP, establece el túnel secundario como activo y utiliza solo el túnel secundario para enviar y recibir tráfico.*

STEP 18 | (Opcional) Habilite **QoS** para la ubicación y especifique un **QoS Profile (Perfil de QoS)**.

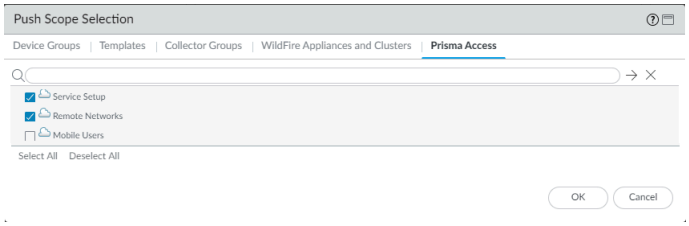
Puede especificar las opciones de QoS y la configuración general según la ubicación de computación en **Settings (Configuración)**; sin embargo, puede habilitar o deshabilitar QoS o cambiar el perfil de QoS según la ubicación aquí.

STEP 19 | Confirme los cambios de configuración en Panorama y envíe la configuración a Prisma Access para redes.

1. Haga clic en **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.
2. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**. Haga clic en **Edit Selections (Editar selecciones)** > **Prisma Access** y seleccione ambos Prisma Access

 ©2025 Palo Alto Networks, Inc.

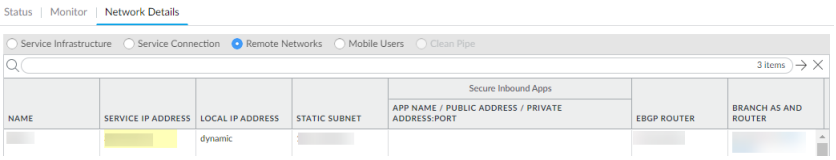
para redes y Prisma Access para la configuración del servicio para enviar la configuración al servicio.



3. Haga clic en **OK (Aceptar)** y **Push (Enviar)**.

STEP 20 | Configure el dispositivo compatible con IPSec en la ubicación de red remota para configurar una conexión IPSec con Prisma Access para redes.

1. Busque la **Service IP Address (Dirección IP del servicio)** para esta conexión de red remota seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de red)**, haciendo clic en el botón de opción **Remote Networks (Redes remotas)** y visualizando el campo **Service IP Address (Dirección IP del servicio)**. Prisma Access para la infraestructura de redes se ha asignado este dirección IP para la conexión de red remota de Prisma Access y debe configurarla como la dirección IP del peer para configurar el túnel IPSec entre la ubicación de red remota y Prisma Access para redes.



2. Verifique la **Local IP address (dirección IP local)** del dispositivo en la ubicación de red remota en la página **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de red)** > **Remote Networks (Redes remotas)**. Si está realizando NAT en la ubicación de red remota, la **Local IP address (Dirección IP local)** muestra la dirección IP del dispositivo después de NAT.

STEP 21 | Para proteger el tráfico en la ubicación de red remota, debe crear reglas de política de seguridad.

1. Seleccione **Policies (Políticas)**.
2. Seleccione el **Device Group (Grupo de dispositivos)** en el que desea añadir reglas de política. Puede seleccionar Remote_Network_Device_Group o el grupo de dispositivos principal que seleccionó para definir políticas para proteger la ubicación de la red remota.
3. Cree reglas de políticas de seguridad. Asegúrese de no definir reglas de política de seguridad para permitir el tráfico de cualquier zona a cualquier zona. En las reglas de la política de seguridad, utilice las zonas que definió en su plantilla.

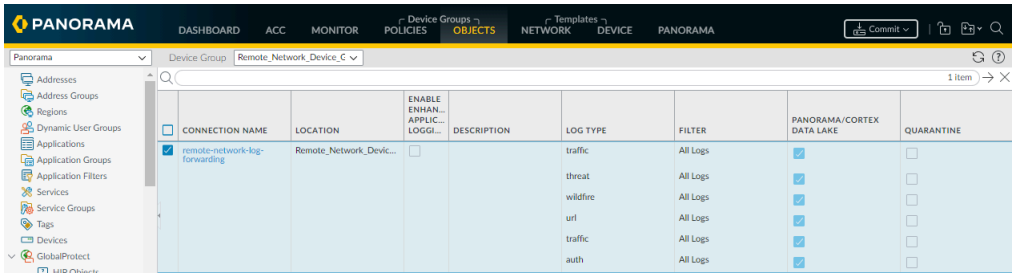
   Si a un usuario de su red se le niega el acceso a un sitio web, informe los problemas de acceso al sitio web antes de abrir un ticket de incidencia con Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

STEP 22 | Habilitar el registro en Strata Logging Service. Debe crear y adjuntar un perfil de reenvío de logs a cada regla de política para la cual desea reenviar logs.

1. Seleccione **Objects (Objetos) > Log Forwarding (Reenvío de logs)**.
2. Seleccione el **Device Group (Grupo de dispositivos)** en el que añadió las reglas de política, por ejemplo, Remote_Network_Device_Group.
3. **Add (Añadir)** un perfil de reenvío de logs En la lista de coincidencia del perfil de reenvío de logs, seleccione **Add (Añadir)** para añadir cada **Log Type (Tipo de log)** que desea reenviar.
4. Seleccione **Panorama/Strata Logging Service (Servicio de registro de logs de Panorama/Strata)** como método de reenvío para habilitar Prisma Access para reenviar los logs a Strata Logging Service. Podrá supervisar los logs y generar informes desde Panorama. Strata Logging Service proporciona una integración perfecta para almacenar logs sin tener que enviarlos de regreso a su Panorama en la sede central, y Panorama puede consultar Strata Logging Service según sea necesario.

   El siguiente ejemplo permite el reenvío de logs de tráfico, prevención de amenazas, envío de WildFire, filtrado de URL, filtrado de datos y autenticación a Strata Logging Service.



5. Seleccione **Policies (Políticas) > Security (Seguridad)** y modifique la regla de políticas. Seleccione **Actions (Acciones)** y seleccione el perfil de Reenvío de logs que ha creado.

STEP 23 | Confirme todos sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Deberá **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access** , asegúrese de que **Prisma Access for networks (Prisma Access para redes)** se selecciona en **Push Scope (Ámbito de envío)**, luego haga clic en **OK (Aceptar)**.
3. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 24 | Verifique el estado de la red remota.

Consulte Verificar el estado de la conexión de red remota para obtener más detalles.

 ©2025 Palo Alto Networks, Inc.

Conectar un sitio de red remoto a Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

Configure túneles VPN IPSec para conectar sus sitios de redes remotas a Prisma Access. Debe crear un túnel IPSec desde su dispositivo IPSec de sucursal a Prisma Access.

El primer túnel que se crea es el túnel principal para el sitio de red remota. A continuación, puede repetir este flujo de trabajo para, opcionalmente, configurar un túnel secundario. Cuando ambos túneles están activos, el túnel primario tiene prioridad sobre el túnel secundario. Si el túnel principal para una sitio de red remota deja de funcionar, la red remota vuelve al túnel secundario hasta que el túnel principal vuelva a funcionar.

Basado en el dispositivo IPSec que utiliza para establecer el túnel, Prisma Access proporciona configuraciones de seguridad IKE e IPSec integradas y recomendadas. Puede usar los ajustes recomendados para comenzar rápidamente o personalizarlos según sea necesario para su entorno.

- Añadir túneles VPN IPSec primarios y secundarios
- Más opciones de IKE
- Más opciones de IPSec

Añadir túneles VPN IPSec primarios y secundarios

STEP 1 | Iniciar Prisma Access

STEP 2 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)** > **Add Remote Networks (Añadir redes remotas)** y **Set Up (Configurar)** el túnel principal. Si ya ha configurado un túnel principal, puede continuar aquí para añadir también un túnel secundario.

1. Asigne un **Name (Nombre)** descriptivo al túnel.
2. Seleccione el **Branch Device Type (Tipo de dispositivo de sucursal)** para el dispositivo IPSec en el sitio de red remoto que está utilizando para establecer el túnel con Prisma Access.
3. Para la **Branch Device IP Address (Dirección IP del dispositivo de sucursal)**, elija usar una dirección **Static IP (IP estática)** que identifique el endpoint del túnel o una dirección IP **Dynamic (Dinámica)**.

   Si establece la **Branch Device IP Address (Dirección IP del dispositivo de sucursal)** como **Dynamic (Dinámica)**, también debe añadir el ID de IKE para el sitio de red remoto [**IKE Local Identification (Identificación local de IKE)**] o para Prisma Access [**IKE Peer Identification (Identificación de peers IKE)**] para permitir que los peers IPSec se autentiquen.

   Dado que no tiene los valores que se van a utilizar para el ID de IKE de Prisma Access [**IKE Peer Identification (Identificación de peers de IKE)**] hasta que la red remota esté

 ©2025 Palo Alto Networks, Inc.

completamente implementada, normalmente querrá establecer el ID de IKE para el sitio de red remota [**IKE Local Identification (Identificación local de IKE)**] en lugar del ID de IKE de Prisma Access.

STEP 3 | **Turn on Tunnel Monitoring (Activar la supervisión de túneles**.

Introduzca una dirección de **Destination IP (IP de destino)** de Supervisión de túnel en la red remota para que Prisma Access la use, determine si el túnel está activo y, si su dispositivo IPSec usa VPN basada en políticas, introduzca el **Proxy ID (ID de proxy)** asociado.

La dirección IP de supervisión de túnel que introduzca se añadirá automáticamente a la lista de redes secundarias de sucursales.

STEP 4 | Elija **Save (Guardar)** la configuración del túnel.

Para continuar:

- Configure y personalice la configuración criptográfica avanzada para IKE e IPSec. Consulte Más opciones de IKE y Más opciones de IPSec.
- Habilitar el enrutamiento para su red remota.

Más opciones de IKE

Según el tipo de dispositivo IPSec que haya seleccionado, Prisma Access proporciona un conjunto recomendado de cifrados y una vida útil de la clave para el proceso de intercambio de claves IKE de fase 1 entre el dispositivo del sitio de red remoto y Prisma Access. Puede utilizar la configuración recomendada o personalizar la configuración según sea necesario para su entorno.

- Seleccione una **IKE Protocol Version (Versión del protocolo IKE)** para su dispositivo IPSec de sucursal y Prisma Access para usar para la negociación IKE.

  Si selecciona **IKEv1 Only Mode (Modo de solo IKEv1)**, Prisma Access solo podrá usar el protocolo IKEv1 para la negociación. Si selecciona **IKEv2 Only Mode (Modo de solo IKEv2)**, Prisma Access solo podrá usar el protocolo IKEv2 para la negociación. Si selecciona el **IKEv2 Preferred Mode (Modo preferido de IKEv2)**, Prisma Access utiliza el protocolo IKEv2 solo si su dispositivo IPSec de sucursal también admite IKEv2. Si su dispositivo IPSec de sucursal no es compatible con IKEv2, Prisma Access recurre al protocolo IKEv1.

 ©2025 Palo Alto Networks, Inc.

- Añada un **IKEv1 Crypto Profile (Perfil criptográfico IKEv1)** para personalizar la configuración criptográfica de IKE que define los algoritmos de cifrado y autenticación utilizados para el proceso de intercambio de claves en la Fase 1 de IKE.

  Prisma AccessPrisma Access utiliza automáticamente un perfil criptográfico IKE predeterminado según el **Branch Device Type (Tipo de dispositivo de sucursal)** que se utiliza para establecer dicho túnel.

  - **Encryption (Cifrado)**: especifique el algoritmo de cifrado utilizado en la negociación de SA de IKE.

    Prisma Access admite los siguientes algoritmos de cifrado: 3des (168 bits), aes-128-cbc (128 bits), aes-192-cbc (192 bits), aes-256-cbc (256 bits) y des (56 bits). También puede seleccionar nulo (sin cifrado).
  - **Authentication (Autenticación)**: especifique el algoritmo de autenticación utilizado en la negociación de SA de IKE.

    Prisma Access es compatible con los siguientes algoritmos de autenticación: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) y md5 (128 bits). También puede seleccionar nulo (sin autenticación).
  - **Grupo DH:**especifique los grupos Diffie-Hellman (DH) utilizados para generar claves simétricas para IKE en la negociación de SA de IKE. El algoritmo Diffie Hellman usa la clave privada de una parte y la clave pública de la otra para crear un secreto compartido, que es una clave cifrada compartida por ambos peers del túnel VPN.

    Prisma Access es compatible con los siguientes grupos DH: grupo 1 (768 bits); grupo 2 (1024 bits—predeterminado); grupo 5 (1536 bits); grupo 14 (2048 bits), grupo 19 (grupo de curva elíptica de 256 bits) y grupo 20 (grupo de curva elíptica de 384 bits). Para mayor seguridad, seleccione el grupo con el número más alto.
  - **Lifetime (Vida útil)**: especifique la unidad y el tiempo durante la cual la clave IKE de fase 1 es válida (el valor predeterminado es 8 horas). Para IKEv1, la asociación de seguridad (SA) no se vuelve a generar activamente antes de que caduque la vida útil de la clave. La nueva clave de IKEv1 de fase 1 se activa solo cuando caduca la SA. Para IKEv2, es necesario volver a introducir la clave de SA antes de que caduque la vida útil de la clave. Si no se vuelve a introducir la clave de la SA al vencimiento, la SA debe comenzar una nueva clave de fase 1.
  - **IKEv2 Authentication Multiple (Autenticación IKEv2 múltiple)**: Especifique el valor que se multiplica por la duración de la clave para determinar el recuento de autenticación (rango: 0 a 50; valor predeterminado: 0). El recuento de autenticaciones es el número de veces que el nodo de procesamiento de seguridad puede regenerar la clave de codificación de SA IKE IKEv2 antes de que deba volver a empezar con la reautenticación IKEv2. El valor predeterminado 0 deshabilita la función de reautenticación.

- Habilite el **IKE Passive Mode (Modo pasivo IKE)** para que Prisma Access solo responda a las conexiones IKE y no las inicie.

- **IKE NAT Traversal (NAT transversal de IKE)** está activado de forma predeterminada.

  Esto significa que la encapsulación UDP se utiliza en los protocolos IKE y UDP, lo que les permite pasar a través de dispositivos de traducción de direcciones de red (NAT) que se encuentran entre los endpoints del túnel IPSec VPN.

 ©2025 Palo Alto Networks, Inc.

Más opciones de IPSec

En base al tipo de dispositivo IPSec que haya seleccionado, Prisma Access proporciona un conjunto recomendado de protocolos IPSec y ajustes clave de vida útil para proteger los datos dentro del túnel IPSec entre su dispositivo de sucursal y Prisma Access en IKE de fase 2 para la asociación de seguridad (SA). Puede utilizar la configuración recomendada o personalizar la configuración según sea necesario para su entorno.

- Personalice el **IPSec Crypto Profile (Perfil criptográfico de IPSec)** para definir cómo se protegen los datos dentro del túnel cuando Auto Key IKE genera automáticamente claves para las SA de IKE durante la fase 2 de IKE.

  Prisma Access configura automáticamente un perfil de cifrado IPSec predeterminado basado en el proveedor de **Branch Device Type (Tipo de dispositivo de sucursal)**. Puede usar el perfil predeterminado o crear un perfil personalizado.

  - **IPSec Protocol (Protocolo IPSec)**: proteja los datos que atraviesan el túnel VPN. El protocolo de carga de seguridad encapsulada (**ESP**) cifra los datos, autentica el origen y verifica la integridad de los datos. El protocolo de encabezado de autenticación **AH** autentica el origen y verifica la integridad de los datos.

    Si utiliza **ESP** como protocolo IPSec, especifique también el algoritmo de **Encryption (Cifrado)** utilizado en la negociación SA de IPSec.

    Prisma Access es compatible con los siguientes algoritmos de cifrado: aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits) y des (56 bits). También puede seleccionar nulo (sin cifrado).

- **Authentication (Autenticación)**: especifique el algoritmo de autenticación utilizado en la negociación de SA de IPSec.

  Prisma Access es compatible con los siguientes algoritmos de autenticación: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) y md5 (128 bits). Si define el Protocolo IPSec en ESP, también podrá seleccionar ninguno (sin autenticación).

- **DH Group (Grupo DH)**: especifique los grupos Diffie-Hellman (DH) para IKE en la negociación de la asociación de seguridad (SA) IPSec.

  Prisma Access es compatible con los siguientes grupos DH: grupo 1 (768 bits); grupo 2 (1024 bits—predeterminado); grupo 5 (1536 bits); grupo 14 (2048 bits), grupo 19 (grupo de curva elíptica de 256 bits) y grupo 20 (grupo de curva elíptica de 384 bits). Para mayor seguridad, seleccione el grupo con el número más alto. Si no desea renovar la clave que crea Prisma Access durante la fase 1 de IKE, seleccione **no-pfs** (sin secreto perfecto hacia adelante). Si selecciona esta opción, Prisma Access reutiliza la clave actual para la negociación SA de IPSec.

- **Lifetime (Vida útil)**: especifique la unidad y el tiempo durante el cual la clave negociada es válida (por defecto es una hora).

- **Lifesize (Tamaño real**: especifique la unidad y el volumen de datos que la clave puede utilizar para el cifrado.

 ©2025 Palo Alto Networks, Inc.

Habilitar el enrutamiento para su red remota

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

Para que Prisma Access enrute el tráfico a sus redes remotas, debe proporcionar información de enrutamiento para las subredes que desea proteger mediante Prisma Access. Puede hacer esto de varias maneras. Puede definir una ruta estática para cada subred en el sitio de red remoto o configurar BGP entre las ubicaciones de conexión de su servicio y Prisma Access, o utilizar una combinación de ambos métodos.

Si configura ambas rutas estáticas y habilita BGP, las rutas estáticas tienen prioridad. Si bien puede ser conveniente utilizar rutas estáticas, si solo tiene unas pocas subredes en sus ubicaciones de red remotas, en una implementación grande con muchas redes remotas con subredes superpuestas, BGP le permitirá ampliar más fácilmente.

- ❑ **Rutas estáticas**: para habilitar rutas estáticas hacia y desde su sitio remoto a Prisma Access, identifique las subredes o direcciones IP individuales en el sitio remoto que desea que Prisma Access asegure (tanto el tráfico entrante como el saliente). Las subredes de cada sitio no deben superponerse entre sí, con los grupos de IP que usted designó para Prisma Access para usuarios, o con la subred de infraestructura.
- ❑ **BGP**: si desea habilitar BGP para enrutar dinámicamente el tráfico hacia y desde su red remota, deberá proporcionar la información de BGP para el enrutador eBGP en su sucursal:
  - ❑ **Número de sistema autónomo (AS) del enrutador de sucursal**: el número AS al que pertenece el enrutador eBGP en la red remota. Esto se llama el **Peer AS (AS del peer)**.
  - ❑ **Router ID (ID de enrutador)**: la dirección IP asignada como el ID de enrutador del enrutador eBGP en la red remota. Esto se llama **Peer Address (Dirección del peer)**.

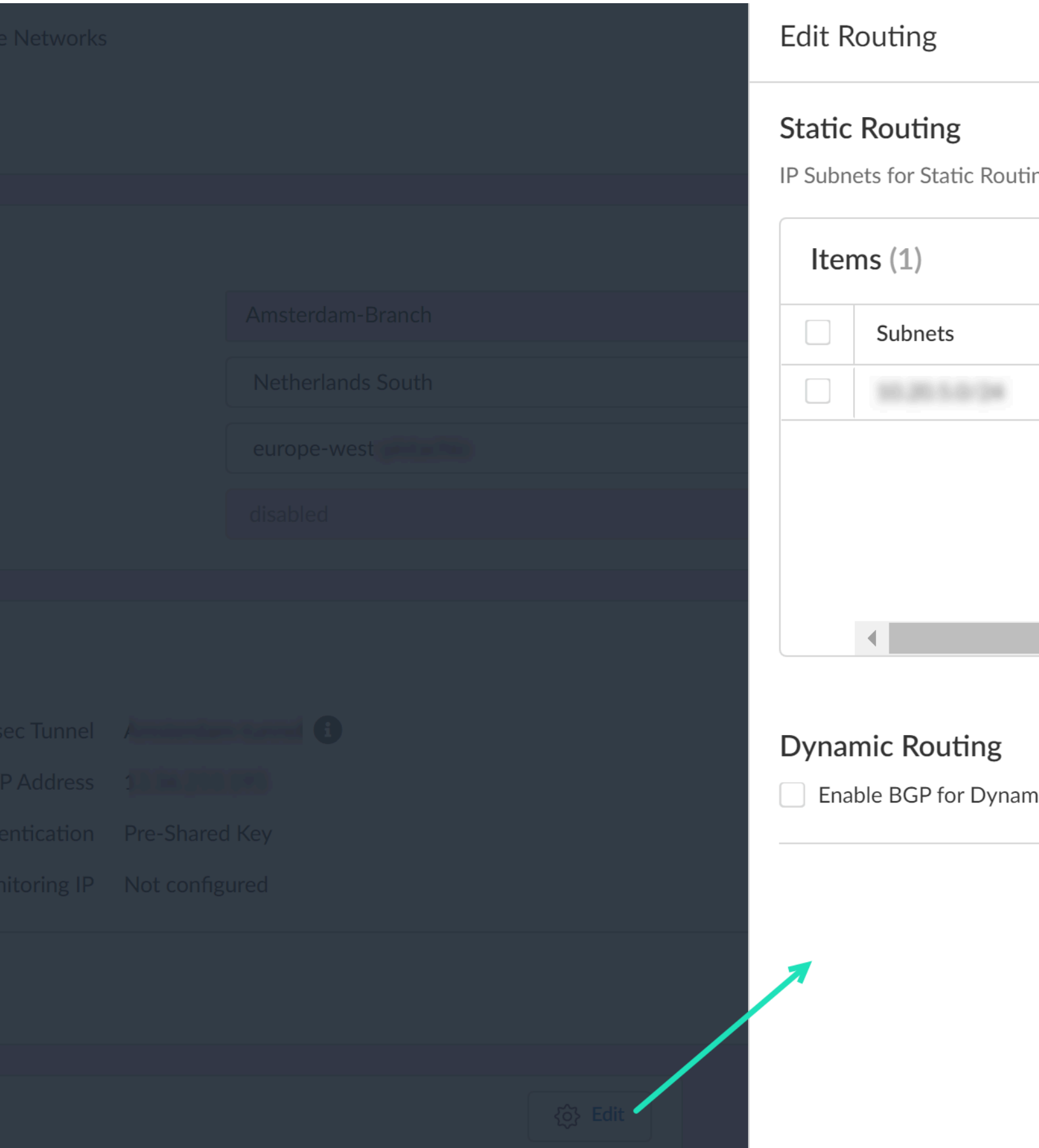
  Si configura rutas estáticas y enrutamiento BGP, las rutas estáticas tienen prioridad.

A continuación se explica cómo configurar los ajustes de enrutamiento para su sitio de red remoto.

 ©2025 Palo Alto Networks, Inc.

- Para añadir o ajustar la configuración de enrutamiento, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)** y añada o edite un sitio de red remota.

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

- Configurar rutas estáticas.

  Si utiliza rutas estáticas para enrutar el tráfico hacia y desde sitios de red remotos, debe **Add (Añadir)** las subredes IP o las direcciones IP que desea proteger en el sitio. Tenga en cuenta que si realiza algún cambio en las subredes IP de su sucursal, deberá actualizar manualmente las rutas estáticas.

- Configurar enrutamiento dinámico.

  Para utilizar el enrutamiento dinámico para anunciar las subredes de su sucursal, deberá **Enable BGP for Dynamic Routing (Deshabilitar BGP para enrutamiento dinámico)** y luego configure los siguientes ajustes:

  - **Do Not Export Routes (No exportar rutas)**: impide que Prisma Access reenvíe rutas a su red remota.

    Por defecto, Prisma Access anuncia toda la información de enrutamiento BGP, incluidas las rutas locales y todos los prefijos que recibe de otras conexiones de servicio, redes remotas y subredes de usuarios móviles. Seleccione esta casilla de verificación para evitar que Prisma Access envíe cualquier anuncio BGP y aún así usar la información BGP que recibe para aprender rutas de otros vecinos BGP.

    Dado que Prisma Access no envía anuncios BGP si selecciona esta opción, debe configurar rutas estáticas en su equipo local para establecer rutas de regreso a Prisma Access.

  - **Peer IP Address (Dirección IP del peer)**: introduzca la Dirección IP del peer asignada como ID del enrutador eBGP en la red remota.
  - **Peer AS (AS de peer)**: introduzca el AS del peer, que es el sistema autónomo (AS) para su red.

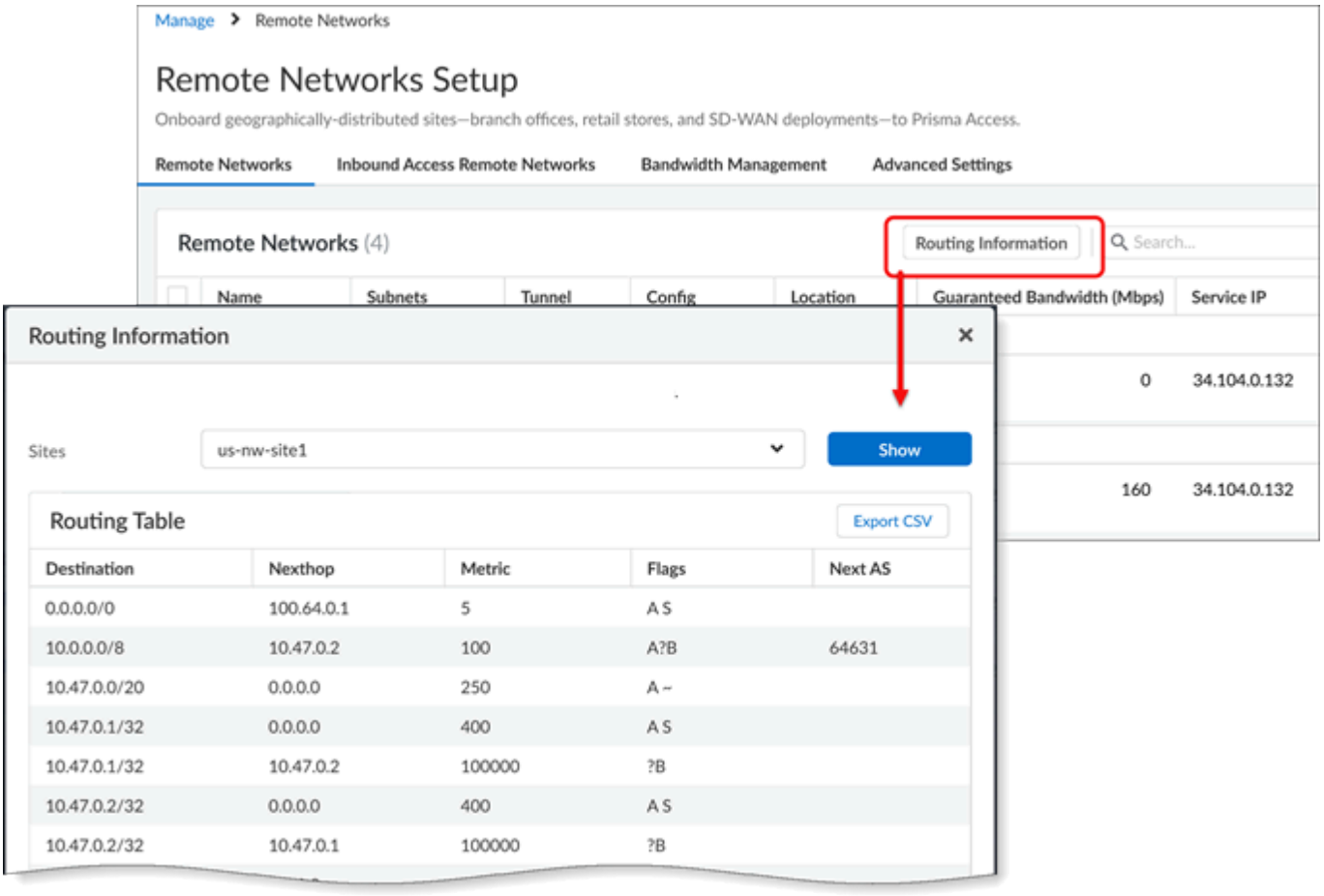
    Debe utilizar un número AS privado BGP compatible con RFC 6996.
  - **Local IP Address (Dirección IP local)**: introduce la dirección IP que Prisma Access utiliza como su dirección IP local para BGP.

    Solo se requiere una dirección local si su dispositivo de sitio remoto la requiere para que el intercambio de BGP sea correcto. Asegúrese de que la dirección que especifique no entre en conflicto ni se superponga con las direcciones IP en la subred de infraestructura o subredes de la red remota.
  - **Secret (Secreto)**: introduzca una contraseña secreta para autenticar las comunicaciones de peers de BGP y luego seleccione **Confirm Secret (Confirmar secreto)**.

Solucionar problemas de conexiones del sitio

Para solucionar problemas, ahora puede ver la tabla de enrutamiento de un sitio de red remoto o un sitio de conexión de servicio. Encuentre el botón **Routing Information (Información de enrutamiento)** en el panel de conexión de servicios o redes remotas.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Integrar varias redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Para agilizar el proceso de incorporación y configuración de redes remotas, tiene la opción de incorporar al menos una red remota y luego exportar esas configuraciones a un archivo de texto de valores separados por comas (CSV). El archivo CSV incluye los valores de la configuración del túnel IPSec y la puerta de enlace IKE para la red que seleccionó para exportar, y luego puede editar estas configuraciones y hacerlas únicas para cada nueva red que desee incorporar. Puede modificar el archivo CSV para incluir 100 nuevas redes remotas y luego volver a importar el archivo CSV para acelerar el proceso de incorporación de nuevas ubicaciones de redes remotas.

El archivo CSV no incluye claves ni contraseñas, como el secreto compartido BGP, la clave precompartida IKE, el ID de proxy, el perfil de cifrado IKE y el perfil de cifrado IPSec. Por lo tanto, todas las claves y contraseñas necesarias para la configuración del túnel IPSec y del portal IKE se heredan de la red que usted selecciona cuando inicia la importación del archivo CSV.

Al utilizar este proceso de importación masiva, debe esperar que Prisma Access implemente la infraestructura necesaria para proteger estas ubicaciones.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** (en la sección Incorporación).

STEP 2 | Seleccione una ubicación y luego seleccione **Export (Exportar)** para exportar la configuración de una red remota que haya incorporado previamente.

Si aún no ha añadido ninguna ubicación, debe **Add (Añadir)** una ubicación y luego descargar su configuración. Debe seleccionar una red remota y hacer clic en **Export (Exportar)**. Se descarga a su equipo un archivo CSV que incluye la configuración.

STEP 3 | (Implementaciones que asignan ancho de banda solo por ubicación de cómputo) Asegúrese de haber asignado ancho de banda para las ubicaciones a incorporar.

Cada ubicación que incorpora tiene una ubicación de cómputo correspondiente para la cual se asigna ancho de banda.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y haga clic en el engranaje en el área **Bandwidth Allocation (Asignación de ancho de banda)**.
2. Verifique el campo **Bandwidth Allocation (Asignación de ancho de banda)** en la tabla que se muestra.

   La tabla en esta área muestra la ubicación de cómputo a la asignación de ubicación de Prisma Access. Debe tener ancho de banda asignado para las ubicaciones de cómputo que estén asociadas con las ubicaciones que desea incorporar. Por ejemplo, para integrar

 ©2025 Palo Alto Networks, Inc.

la ubicación central de Japón, asegúrese de haber asignado ancho de banda en la ubicación de cómputo de Asia Noreste.

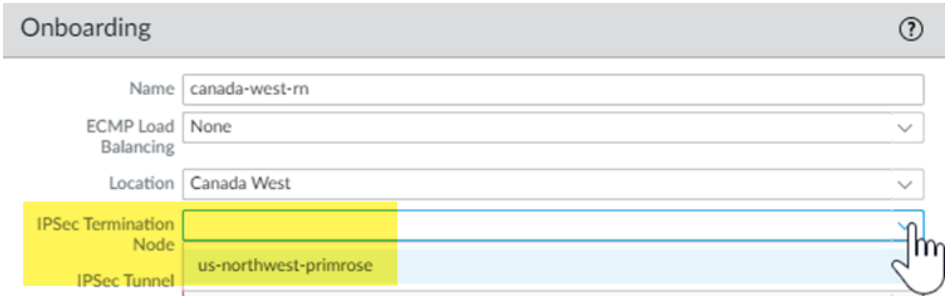
3. Si aún no ha asignado ancho de banda para las ubicaciones de cómputo asociadas con las ubicaciones que desea incorporar, añádalo ahora.

STEP 4 | (Implementaciones que asignan ancho de banda solo por ubicación de cómputo) Busque el **IPSec Termination Node (Nodo de terminación IPSec)** asociado a la ubicación o las ubicaciones que desea incorporar.

Asigna un *nodo de terminación IPSec* a la red remota durante la incorporación e introduce este valor en la columna **spn-name** del archivo CSV. Cada nodo de terminación IPSec puede proporcionar hasta 1000 Mbps de ancho de banda.

Para encontrar el nodo de terminación IPSec, realice una de las siguientes acciones:

- Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, elija **Add (Añadir)** una red remota y seleccione la ubicación que desea incorporar, y tome nota de las opciones de Nodo de terminación IPSec en el área de incorporación.



- Abra una sesión de interfaz de línea de comandos (CLI) con el Panorama que gestiona Prisma Access e introduzca el *nombre de ubicación de cómputo* `show plugins cloud_services remote-networks agg-bandwidth region`, donde *nombre de ubicación de cómputo* es la ubicación de cómputo que está asociada con la ubicación que desea incorporar. El nodo de terminación IPSec se muestra en el campo `spn-name-list`.

STEP 5 | Modifique el archivo CSV para añadir configuración para redes remotas.

Consulte Campos en la tabla de Redes remotas para una descripción de los campos y los posibles valores en este archivo.

Debe cambiar el nombre de las redes enumeradas en el archivo exportado. Si el archivo tiene nombres duplicados la importación fallará.

STEP 6 | **Import (Importar)** el archivo CSV.

La configuración del archivo se muestra en la pantalla. La red remota que seleccionó para importar el archivo servirá como la configuración modelo, y las redes remotas enumeradas en el archivo heredarán las claves y cualquier valor que falte que no tenga que ser único allí.

STEP 7 | Confirmar y enviar sus cambios.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** sus cambios.
2. Haga clic en **OK (Aceptar)** y **Push (Enviar)**.

 ©2025 Palo Alto Networks, Inc.

Campos en la tabla de Redes remotas

La siguiente tabla proporciona una descripción de los campos de la tabla de redes remotas. Los campos marcados como **Y** en la fila **Obligatorio** son campos obligatorios y los campos marcados como **N** son opcionales.

Campo	Descripción	¿Requerido? (S/N)
name	El nombre de la red remota.	S
ancho de banda	(Implementaciones que asignan ancho de banda solo por ubicación) El ancho de banda asignado de la red remota. Los valores aceptables son: • 2 Mbps • 5 Mbps • 10 Mbps • 20 Mbps • 25 Mbps • 50 Mbps • 100 Mbps • 150 Mbps • 300 Mbps • 500 Mbps • 1000 Mbps *La opción de ancho de banda de 1000 Mbps está en modo de vista previa. El rendimiento durante la vista previa se entrega según el mejor esfuerzo y el rendimiento real variará dependiendo de la combinación de tráfico.*	S
región	La ubicación de la red remota. Introduzca las ubicaciones exactamente como aparecen en este documento (por ejemplo, **EE. UU. Oeste**o **Japón Sur**).	S
subredes	Subredes enrutadas estáticamente en el extremo del LAN de la red remota. Separe varias subredes con comas.	N

©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
bgp_peer_as	El número de sistema autónomo (ASN) BGP del dispositivo par de la red remota.	N
bgp_peer_address	La dirección de par BGP del dispositivo par de la red remota.	N
tunnel_name	El nombre de la configuración de túnel de IPSec. Se requiere un valor único.	S
gateway_name	El nombre de la configuración de la puerta de enlace IKE. Se requiere un valor único.	S
peer_ip_address	Introduzca la dirección IP del dispositivo par de Prisma Access.	N
local_id_type	El tipo de ID de IKE que Prisma Access presenta al dispositivo par. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	N
local_id_value	El valor del ID de IKE que Prisma Access presenta al dispositivo par. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	N
peer_id_type	El valor del ID de IKE que el par presenta a Prisma Access. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	N
peer_id_value	El valor del ID de IKE que Prisma Access presenta al dispositivo par. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	N
monitor_ip	La dirección IP de supervisión del túnel que la nube usará para determinar que el túnel IPSec está activo y que la red de pares es accesible. *No es posible exportar un valor de proxy-ID para el monitor de túnel.*	N

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
proxy_ids	Los ID de proxy que están configurados para el par. Para las VPN basadas en rutas, deje este campo en blanco. Especifique el ID de proxy en el siguiente formato de configuración CSV: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	N
sec_wan_enabled	Especifica si habilita o no un túnel IPSec secundario. Los valores aceptables son sí y no.	N
sec_tunnel_name	El nombre de la configuración del túnel IPSec secundario. Se requiere un valor único si especifica un túnel secundario.	N
sec_gateway_name	El nombre de la configuración de la puerta de enlace IKE secundaria. Se requiere un valor único si especifica un túnel secundario.	N
sec_peer_ip_address	La dirección IP del dispositivo par de Prisma Access para el túnel IPSec secundario.	N
sec_local_id_type	El tipo de ID de IKE que Prisma Access presenta al dispositivo par para el túnel IPSec secundario. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	N
sec_local_id_value	El valor del ID de IKE que Prisma Access se presenta al dispositivo par para el túnel IPSec secundario. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	N
sec_peer_id_type	El valor del ID de IKE que el par presenta a Prisma Access para el túnel IPSec secundario. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	N

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
sec_peer_id_value	El valor del ID de IKE que Prisma Access se presenta al dispositivo par para el túnel IPSec secundario. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	N
sec_monitor_ip	La dirección IP de supervisión del túnel que la nube usará para el túnel IPSec secundario para determinar que el túnel IPSec está activo y que la red de peers es accesible. *No es posible exportar un valor de proxy-ID para el monitor de túnel.*	N
sec_proxy_ids	Los ID de proxy que están configurados para el par para el túnel IPSec secundario. Para las VPN basadas en rutas, deje este campo en blanco. Especifique el ID de proxy en el siguiente formato de configuración CSV: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	N
ecmp_link_1_tunnel_name	(Solo implementaciones de ECMP) El nombre de la configuración del túnel IPSec para el túnel ECMP 1. Se requiere un valor único.	
ecmp_link_1_gateway_name	(Solo implementaciones de ECMP) El nombre de la configuración de la puerta de enlace IKE para el túnel ECMP 1. Se requiere un valor único.	
ecmp_link_1_peer_ip_address	(Solo implementaciones de ECMP) La dirección IP del dispositivo par de Prisma Access para el túnel ECMP 1.	
ecmp_link_1_local_id_type	(Solo implementaciones de ECMP) El tipo de ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 1. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados	

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
	harán referencia a los valores del Certificado configurado.	
ecmp_link_1_local_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 1. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_1_peer_id_type	(Solo implementaciones de ECMP) El valor del ID de IKE que el par presenta a Prisma Access para el túnel ECMP 1. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_1_peer_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 1. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_1_monitor_ip	(Solo implementaciones de ECMP) La dirección IP de supervisión del túnel que la nube usará para determinar que el túnel IPSec está activo y que la red de peers es accesible para el túnel ECMP 1. *No es posible exportar un valor de proxy-ID para el monitor de túnel.*	
ecmp_link_1_proxy_ids	(Solo implementaciones de ECMP) Los ID de proxy que se configuran para el par del túnel ECMP 1. Para las VPN basadas en rutas, deje este campo en blanco. Especifique el ID de proxy en el siguiente formato de configuración CSV: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
ecmp_link_1_bgp_peer_as	(Solo implementaciones de ECMP) El número de sistema autónomo (ASN) BGP del dispositivo de red remoto para el túnel ECMP 1.	
ecmp_link_1_bgp_peer_address	(Solo implementaciones de ECMP) La dirección de par BGP del dispositivo par de la red remota para el túnel ECMP 1.	
ecmp_link_2_tunnel_name	(Solo implementaciones de ECMP) El nombre de la configuración del túnel IPSec para el túnel ECMP 2. Se requiere un valor único.	
ecmp_link_2_gateway_name	(Solo implementaciones de ECMP) El nombre de la configuración de la puerta de enlace IKE para el túnel ECMP 2. Se requiere un valor único.	
ecmp_link_2_peer_ip_address	(Solo implementaciones de ECMP) La dirección IP del dispositivo par de Prisma Access para el túnel ECMP 2.	
ecmp_link_2_local_id_type	(Solo implementaciones de ECMP) El tipo de ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 2. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_2_local_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 2. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_2_peer_id_type	(Solo implementaciones de ECMP) El valor del ID de IKE que el par presenta a Prisma Access para el túnel ECMP 2. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_2_peer_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 2. Si utiliza certificados en la red remota a la que importa este archivo,	

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
	todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_2_monitor_ip	(Solo implementaciones de ECMP) La dirección IP de supervisión del túnel que la nube usará para determinar que el túnel IPSec está activo y que la red de peers es accesible para el túnel ECMP 2. *No es posible exportar un valor de proxy-ID para el monitor de túnel.*	
ecmp_link_2_proxy_ids	(Solo implementaciones de ECMP) Los ID de proxy que se configuran para el par del túnel ECMP 2. Para las VPN basadas en rutas, deje este campo en blanco. Especifique el ID de proxy en el siguiente formato de configuración CSV: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_2_bgp_peer_as	(Solo implementaciones de ECMP) El número de sistema autónomo (ASN) BGP del dispositivo de red remoto para el túnel ECMP 2.	
ecmp_link_2_bgp_peer_address	(Solo implementaciones de ECMP) La dirección de par BGP del dispositivo par de la red remota para el túnel ECMP 2.	
ecmp_link_3_tunnel_name	(Solo implementaciones de ECMP) El nombre de la configuración del túnel IPSec para el túnel ECMP 3. Se requiere un valor único.	
ecmp_link_3_gateway_name	(Solo implementaciones de ECMP) El nombre de la configuración de la puerta de enlace IKE para el túnel ECMP 3. Se requiere un valor único.	
ecmp_link_3_peer_ip_address	(Solo implementaciones de ECMP) La dirección IP del dispositivo par de Prisma Access para el túnel ECMP 3.	
ecmp_link_3_local_id_type	(Solo implementaciones de ECMP) El tipo de ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 3. Si utiliza certificados	

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
	en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_3_local_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access se presenta al dispositivo par para el túnel ECMP 3. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_3_peer_id_type	(Solo implementaciones de ECMP) El valor del ID de IKE que el par presenta a Prisma Access para el túnel ECMP 3. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_3_peer_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access se presenta al dispositivo par para el túnel ECMP 3. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_3_monitor_ip	(Solo implementaciones de ECMP) La dirección IP de supervisión del túnel que la nube usará para determinar que el túnel IPSec está activo y que la red de peers es accesible para el túnel ECMP 3. *No es posible exportar un valor de proxy-ID para el monitor de túnel.*	
ecmp_link_3_proxy_ids	(Solo implementaciones de ECMP) Los ID de proxy que se configuran para el par del túnel ECMP 3. Para las VPN basadas en rutas, deje este campo en blanco. Especifique el ID de proxy en el siguiente formato de configuración CSV: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*",	

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
	`"remote":"3.4.5.6/32", "protocol":{"tcp":{"local-port":234,"remote-port":345}}}]`	
ecmp_link_3_bgp_peer_as	(Solo implementaciones de ECMP) El número de sistema autónomo (ASN) BGP del dispositivo de red remoto para el túnel ECMP 3.	
ecmp_link_3_bgp_peer_address	(Solo implementaciones de ECMP) La dirección de par BGP del dispositivo par de la red remota para el túnel ECMP 3.	
ecmp_link_4_tunnel_name	(Solo implementaciones de ECMP) El nombre de la configuración del túnel IPSec para el túnel ECMP 4. Se requiere un valor único.	
ecmp_link_4_gateway_name	(Solo implementaciones de ECMP) El nombre de la configuración de la puerta de enlace IKE para el túnel ECMP 4. Se requiere un valor único.	
ecmp_link_4_peer_ip_address	(Solo implementaciones de ECMP) La dirección IP del dispositivo par de Prisma Access para el túnel ECMP 4.	
ecmp_link_4_local_id_type	(Solo implementaciones de ECMP) El tipo de ID de IKE que Prisma Access presenta al dispositivo par para el túnel ECMP 4. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_4_local_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access se presenta al dispositivo par para el túnel ECMP 4. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del Certificado configurado.	
ecmp_link_4_peer_id_type	(Solo implementaciones de ECMP) El valor del ID de IKE que el par presenta a Prisma Access para el túnel ECMP 4. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_4_peer_id_value	(Solo implementaciones de ECMP) El valor del ID de IKE que Prisma Access se presenta	

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción	¿Requerido? (S/N)
	al dispositivo par para el túnel ECMP 4. Si utiliza certificados en la red remota a la que importa este archivo, todos los tipos importados especificados harán referencia a los valores del certificado de peers.	
ecmp_link_4_monitor_ip	(Solo implementaciones de ECMP) La dirección IP de supervisión del túnel que la nube usará para determinar que el túnel IPSec está activo y que la red de peers es accesible para el túnel ECMP 4. *No es posible exportar un valor de proxy-ID para el monitor de túnel.*	
ecmp_link_4_proxy_ids	(Solo implementaciones de ECMP) Los ID de proxy que se configuran para el par del túnel ECMP 4. Para las VPN basadas en rutas, deje este campo en blanco. Especifique el ID de proxy en el siguiente formato de configuración CSV: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_4_bgp_peer_as	(Solo implementaciones de ECMP) El número de sistema autónomo (ASN) BGP del dispositivo de red remoto para el túnel ECMP 4.	
ecmp_link_4_bgp_peer_address	(Solo implementaciones de ECMP) La dirección de par BGP del dispositivo par de la red remota para el túnel ECMP 4.	
spn-name	(Implementaciones que asignan ancho de banda solo por ubicación de cómputo) El nombre del nodo de terminación IPSec. Este campo es obligatorio para las implementaciones que asignan ancho de banda por ubicación de cómputo.	

 ©2025 Palo Alto Networks, Inc.

Compruebe si la red remota está conectada a Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

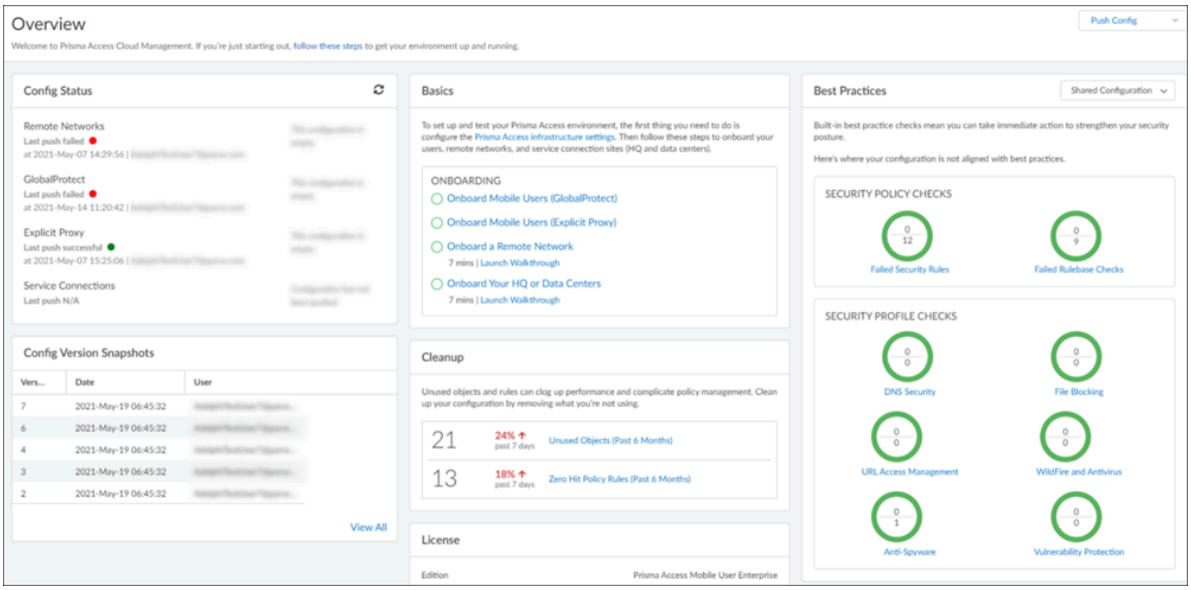
Después de configurar el dispositivo VPN IPSec en la red remota, compruebe el estado del túnel. Cuando verifique el estado de las redes remotas, recuerde lo siguiente:

- Verifique el estado del túnel IPSec en su red remota.
- El paso final al verificar las redes remotas es revisar los logs y asegurarse de que el tráfico fluye a través de Prisma Access. Si hay errores o advertencias, revise los logs del sistema en Prisma Access y logs locales en el dispositivo de red remoto. Resuelva cualquier error o advertencia antes de proceder con la configuración.
- Continúe añadiendo redes remotas según sea necesario.
- Strata Cloud Manager
- Panorama

Compruebe si la red remota está conectada a Prisma Access (Strata Cloud Manager)

Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**, cambie el **Configuration Scope (Ámbito de configuración)** a **Prisma Access** y seleccione **Status Prisma Access Sync Status (Estado de sincronización de Prisma Access)** > **Remote Networks (Redes remotas)**.

©2025 Palo Alto Networks, Inc.



Compruebe si la red remota está conectada a Prisma Access (Panorama)

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** para comprobar que las conexiones de red remotas se han implementado correctamente.

El área de **Deployment Status (Estado de implementación)** le permite ver el progreso de los trabajos de incorporación y implementación antes de que se completen, así como ver más información sobre el estado de los trabajos completados.

STEP 2 | Para mostrar un mapa que muestre las ubicaciones de las redes remotas en las regiones seleccionadas, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (supervisar)** y haga clic en la pestaña **Remote Networks (Redes remotas)**.

STEP 3 | Seleccione una región para obtener más detalles sobre esa región.

STEP 4 | Haga clic en las pestañas debajo del mapa para ver estadísticas adicionales de redes remotas.

Pestaña **Status (Estado)**:

- **Location (Ubicación)**: la ubicación en la que se implementa la red remota.
- **Remote Peer (Par remoto)**: el par con el que la red remota tiene una conexión de túnel IPSec.
- **IPSec Termination Node (Nodo de terminación IPSec)**: el nodo de terminación IPSec asociado con la red remota. Este campo solo se muestra si asigna ancho de banda por ubicación de cómputo.
- **ECMP**: ya sea que haya habilitado **ECMP Load Balancing (Equilibrio de carga ECMP)** en esta conexión de red remota.
- **Config Status (Estado de configuración)**: el estado de su último envío de configuración al servicio. Si ha realizado un cambio localmente y aún no ha enviado la configuración a la nube, el estado se muestra **Out of sync (Fuera de sincronización)**. Pase el cursor sobre

 ©2025 Palo Alto Networks, Inc.

el indicador de estado para obtener información más detallada. Después de confirmar y enviar la configuración a Prisma Access, el estado de configuración cambia a **In sync (Sincronizado)**.

- **BGP Status (Estado de BGP)**: muestra información sobre el estado de BGP entre el cortafuegos o el enrutador en la ubicación de red remota y Prisma Access. Aunque es posible que vea pasar temporalmente el estado a través de los diversos estados de BGP [**idle (inactivo)**, **active (activo)**, **open send (abrir envío)**, **open pend (abrir pendiente)**, **open confirm (abrir confirmación)**], lo más común es que el estado de BGP muestre:
  - **Connect (Conectar)**: el enrutador en la ubicación de red remota está intentando establecer la relación del par BGP con Prisma Access.
  - **Established (Establecido)**: se ha establecido la relación entre pares BGP.

    Este campo también mostrará si la conexión BGP se encuentra en un estado de error:
  - **Advertencia**: no ha habido una actualización de estado de BGP en más de ocho minutos. Esto puede indicar una interrupción en el cortafuegos.
  - **Error**: se desconoce el estado de BGP.
- **Tunnel Status (Estado del túnel)**: el estado de funcionamiento de la conexión entre Prisma Access y la red remota.

Pestaña **Statistics (Estadísticas)**

- **Location (Ubicación)**: la ubicación en la que se implementa la red remota.
- **Remote Peer (Par remoto)**: la ubicación corporativa en la que esta red remota está configurando un túnel IPSec.
- **Ingress Bandwidth (Mbps) [Ancho de banda de entrada (Mbps)]**: El ancho de banda desde la ubicación de red remota hasta Prisma Access.

  Para los campos Ancho de banda de entrada, Ancho de banda máximo de entrada, Ancho de banda de salida y Ancho de banda máximo de salida, cuando el consumo de ancho de banda en una red remota supera el 80 % del ancho de banda asignado, los números se muestran en color rojo.
- **Ingress Peak Bandwidth (Mbps) [Ancho de banda máximo de entrada (Mbps)]**: la carga máxima desde la ubicación de red remota en el servicio en la nube.
- **Egress Bandwidth (Mbps) [Ancho de banda de salida (Mbps)]**: el ancho de banda de Prisma Access en la ubicación de la red remota.
- **Egress Peak Bandwidth (Mbps) [Ancho de banda máximo de salida (Mbps)]**: la carga máxima de Prisma Access en la ubicación de la red remota.

Para buscar estadísticas sobre las ubicaciones de la región, seleccione **Bandwidth Usage (Uso de ancho de banda)**.

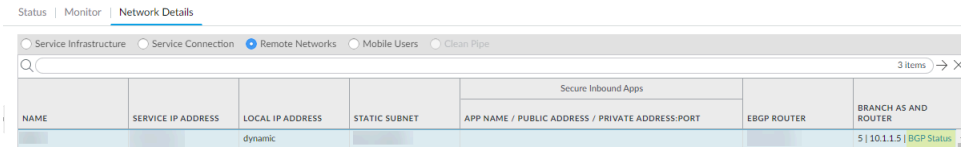
Seleccione la marca de verificación de una ubicación para ver el uso detallado del ancho de banda. En el caso de las implementaciones que asignan ancho de banda por ubicación de cómputo, seleccione un nodo de terminación de IPSec para ver las estadísticas de ese nodo. Prisma Access utiliza el estándar del percentil 95 para recopilar estadísticas, que realiza un seguimiento del ancho de banda en el uso máximo e ignora el 5 por ciento superior de los picos de utilización y las ráfagas grandes.

 ©2025 Palo Alto Networks, Inc.

Verificar el estado de la conexión remota BGP

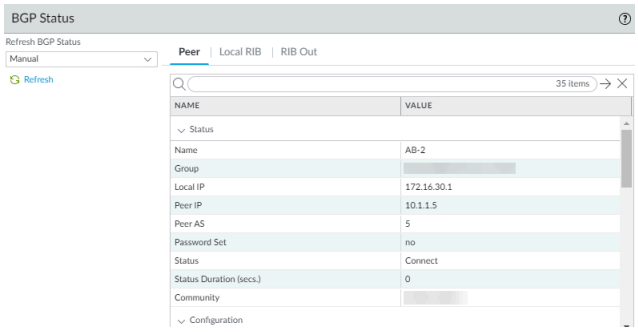
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si has configurado BGP, puede comprobar su estado seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details Detalles de red)** > **Remote Networks (Redes remotas)** > **BGP Status (Estado de BGP)**.

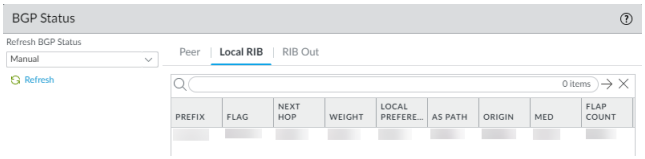


Se muestra el cuadro de diálogo Estado de BGP. Esta tabla le proporciona la siguiente información:

- **Peer**: información de enrutamiento para el peer de BGP, incluido el estado, el número total de rutas, la configuración y las estadísticas y contadores de tiempo de ejecución. El número total de rutas que se muestran en el área **bgpAfiIpv4-unicast Counters (Contadores de bgpAfiIpv4-unicast**, en los campos **Incoming Total (Total entrante)** y **Outgoing Total (Total saliente)**.



- **RIB local**: información de enrutamiento que ha sido recibida de diferentes pares y se almacena en la Base de información de enrutamiento (RIB).



- **Salida de RIB**: información de enrutamiento que Prisma Access anuncia a sus peers a través de mensajes de actualización BGP. Consulte Cómo BGP anuncia los grupos de direcciones IP de usuarios móviles para conexiones de servicio y conexiones de red remotas para un ejemplo de esta tabla y para información sobre cómo BGP utiliza el grupo de direcciones IP que crea para los usuarios móviles.

 ©2025 Palo Alto Networks, Inc.

Configurar la red remota y la conexión de servicio conectada con un enlace WAN

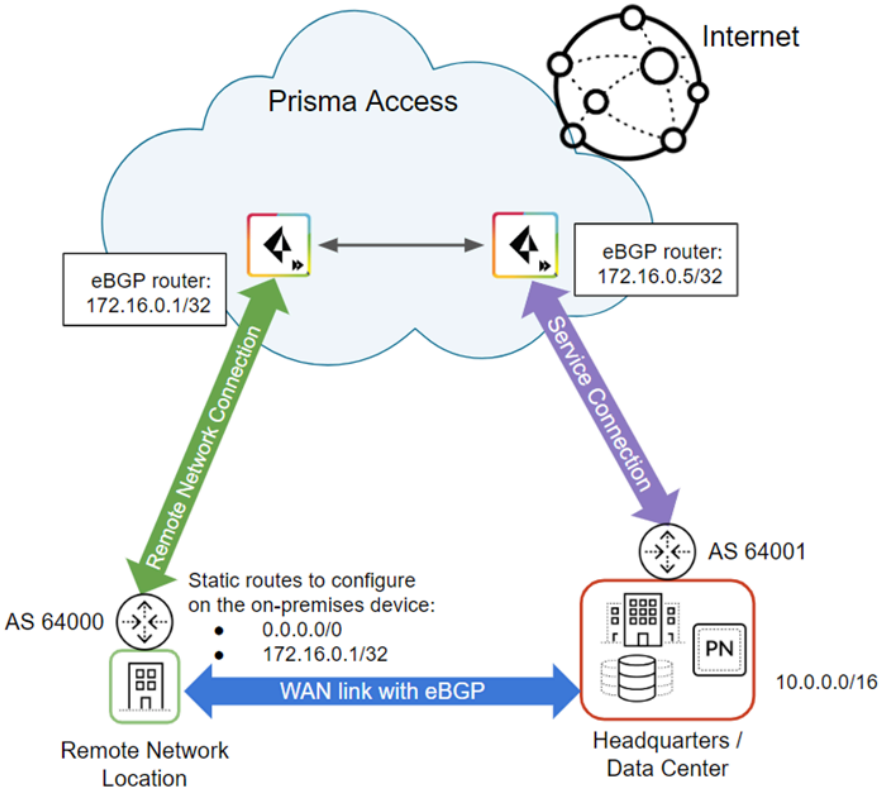
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si tiene una implementación en la que una ubicación de red remota y una sede central o centro de datos con una conexión de servicio están conectadas directamente a través de un enlace WAN, para garantizar un enrutamiento óptimo (con eBGP) debe:

- Añada una ruta estática a la dirección del enrutador eBGP. Además de la ruta predeterminada que envía todo el tráfico a Prisma Access, debe añadir una ruta estática localmente en el dispositivo o enrutador compatible con IPSec en las redes remotas.
- Filtre las rutas que se anuncian desde el dispositivo o enrutador compatible con IPSec en la sede central a los peers de eBGP en otras ubicaciones conectadas directamente. Como práctica recomendada, configure el enrutador BGP en la sede central para anunciar solo las rutas que desea permitir a través del enlace WAN; se asegura de que el enrutador eBGP en la sede central no anuncie las rutas de las que aprende Prisma Access a otras ubicaciones de red remotas protegidas por Prisma Access. En este ejemplo, el router eBGP de la sede central sólo anuncia las rutas que los empleados de la sucursal necesitarán conectar a los servidores (subredes) de la sede central.

En la imagen siguiente se muestra una empresa minorista con dos rutas de acceso a los servidores en la ubicación de la sede central. Una ruta es un enlace WAN que proporciona conectividad directa para los empleados que acceden a los servidores en la sede central, y la otra ruta protege el tráfico generado por otros usuarios en esta ubicación. Por ejemplo, el tráfico generado por los clientes que acceden al sitio web del minorista a través de Wifi o que utilizan el quiosco de la sucursal para comprobar el inventario. Este tráfico se envía a través del túnel a la red remota y a la sede central.

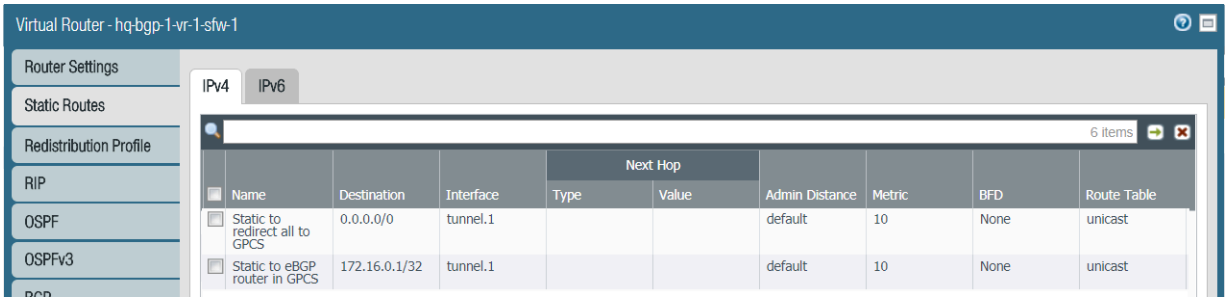
 ©2025 Palo Alto Networks, Inc.



Para configurar esta configuración, cree una conexión de red remota y cree una conexión de servicio para incorporar la red remota y las ubicaciones de la sede. Los detalles a continuación muestran cómo configurar la configuración del enrutador en cada ubicación para garantizar un enrutamiento óptimo:

STEP 1 | Añada las rutas estáticas en el enrutador o en el dispositivo compatible con IPSec local en la ubicación de red remota.

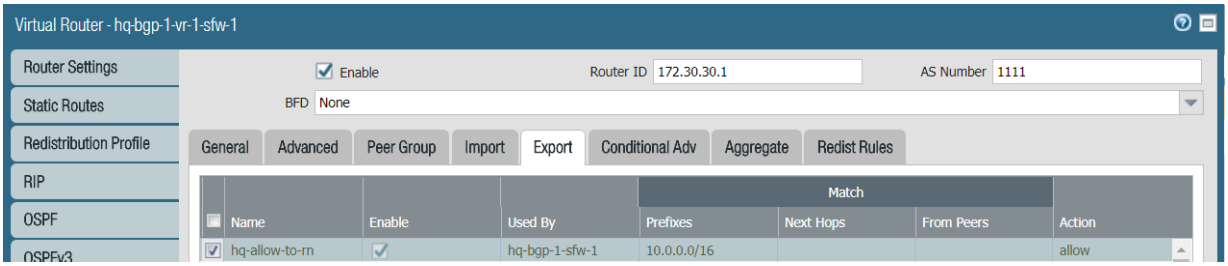
Si tiene un cortafuegos de Palo Alto Networks en el perímetro del enlace WAN, en **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** > **Static Routes (Rutas estáticas)**, seleccione **Add (Añadir)** las rutas estáticas:



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configure las rutas que desea anunciar a otra ubicación conectada directamente a través del enlace WAN.

En este ejemplo, debe configurar esto en la ubicación de la sede. Si tiene un cortafuegos de Palo Alto Networks local en el perímetro del vínculo WAN, puede configurar la redistribución de rutas y configurar las rutas BGP en las que exportar **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** > **BGP**.



 ©2025 Palo Alto Networks, Inc.

QoS para Redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Minimum Required Prisma Access Version: 3.0 Preferred

Nuevas implementaciones de Prisma Access incorporan ancho de banda para redes remotas por ubicación de cómputo. Para utilizar QoS con redes remotas, usted habilita o deshabilita QoS y especifica el ancho de banda garantizado a nivel de ubicación de cómputo. Sin embargo, aún puede personalizar la QoS y el ancho de banda garantizado a nivel de cada ubicación personalizando el ancho de banda por sitio.

Prisma Access divide la ubicación de ancho de banda de cómputo utilizando *nodos de terminación IPSec*. Cada nodo de terminación IPSec puede proporcionarle un máximo de 1.000 Mbps de ancho de banda. Si asigna más de 1,000 Mbps de ancho de banda a una ubicación de cómputo, Prisma Access proporciona nodos de terminación IPSec adicionales.

- Strata Cloud Manager
- Panorama

QoS para redes remotas (Strata Cloud Manager)

Utilice QoS para priorizar el tráfico crítico en sus redes remotas y para establecer anchos de banda máximos y garantizados para sitios de red remotos en una ubicación de cómputo.

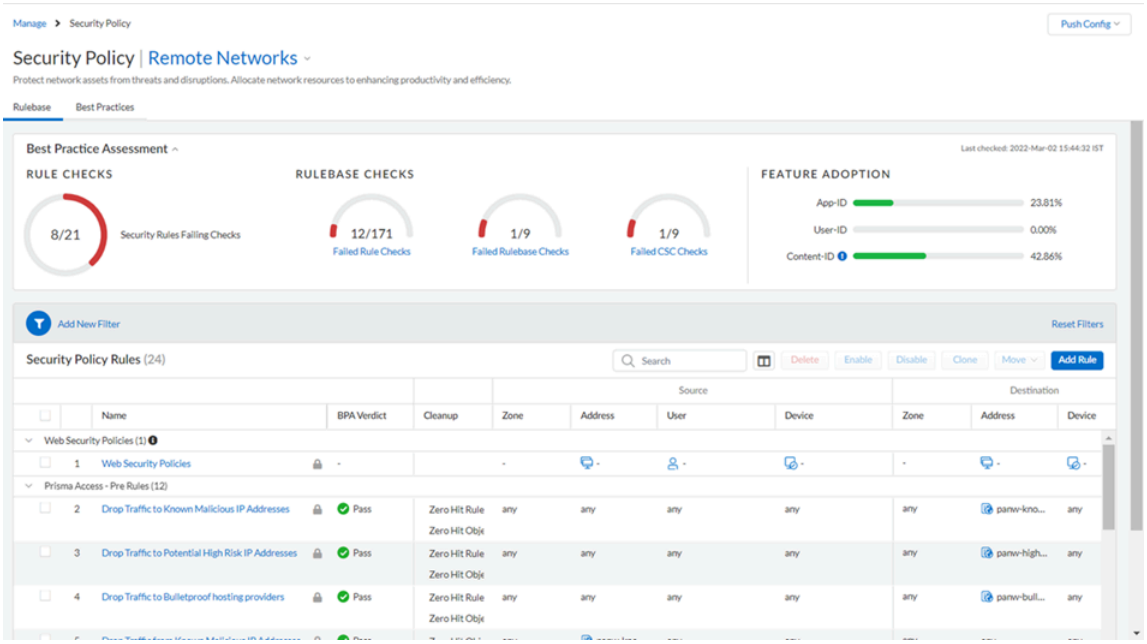
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Marque el tráfico que desea que reciba tratamiento QoS.

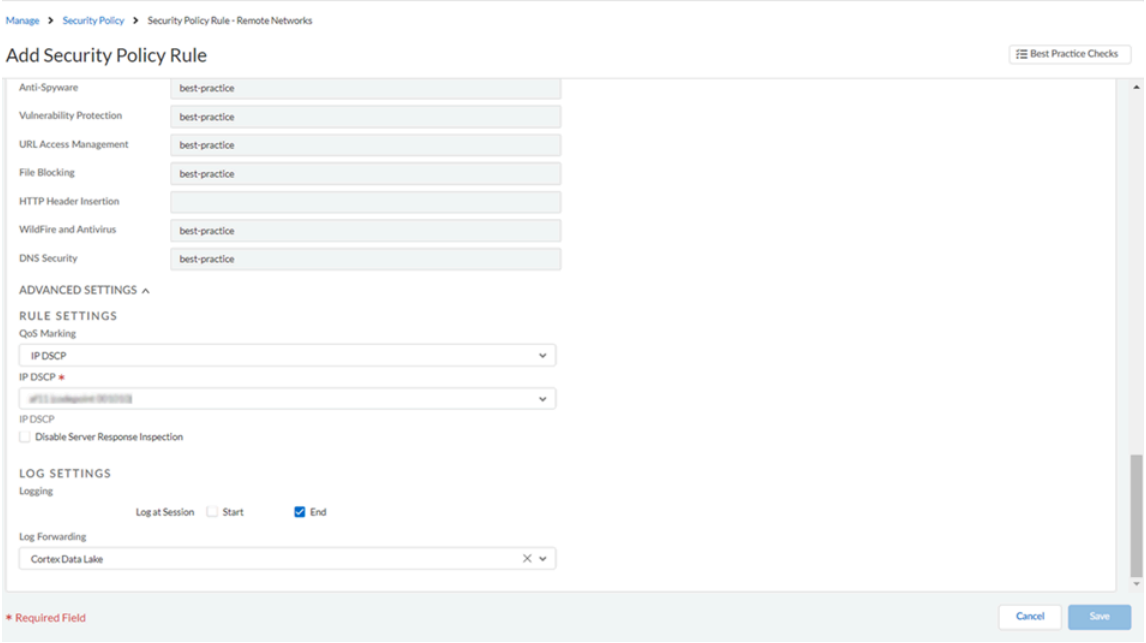
1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de Seguridad)** > **Security Policy (Política de seguridad)**.

   Asegúrese de estar creando la política para redes remotas.

2. **Add Rule (Añadir regla)**.



3. Marque el tráfico entrante asignando un valor DSCP en **Advanced Settings (Configuración avanzada)** y guarde la política.

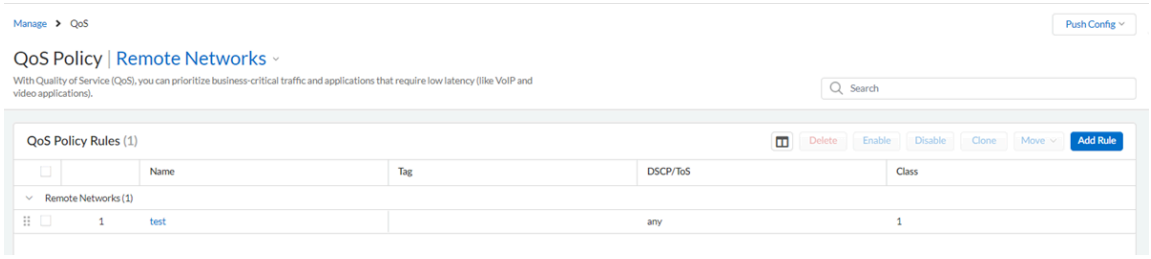


 ©2025 Palo Alto Networks, Inc.

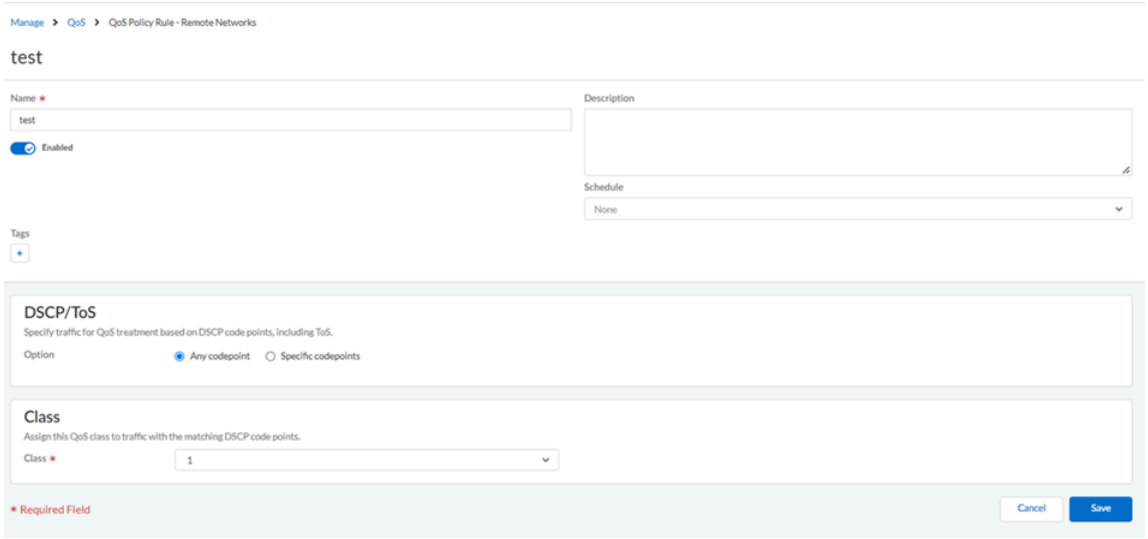
STEP 2 | Añada una o más reglas de política de QoS.

Utilice políticas de QoS para vincular el marcado DSCP a una de las ocho clases disponibles. En los próximos pasos definirá el tratamiento que recibe una clase de QoS. La clase de QoS determina la prioridad y el ancho de banda del tráfico que coincide con una regla de la política de QoS.

1. Seleccione **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **QoS**.
2. **Add Rule (Añadir regla)**.



3. Introduzca valores y guarde la política.



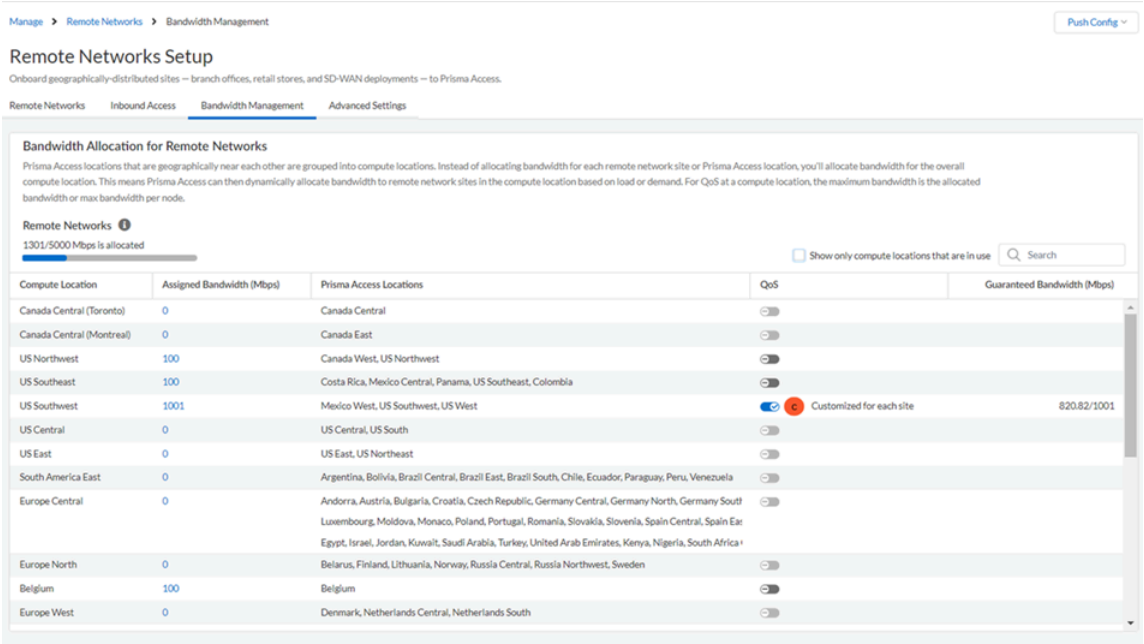
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Habilite QoS para sus ubicaciones de red remotas.

1. Seleccione **Manage (Gestionar)** > **Service Setup (Configuración de servicio)** > **Remote Networks (Redes remotas)** > **Bandwidth Management (Gestión de ancho de banda)**.
2. Determine las ubicaciones de Prisma Access donde desea implementar QoS; luego encuentre la ubicación de cómputo que corresponde a cada ubicación de Prisma Access.

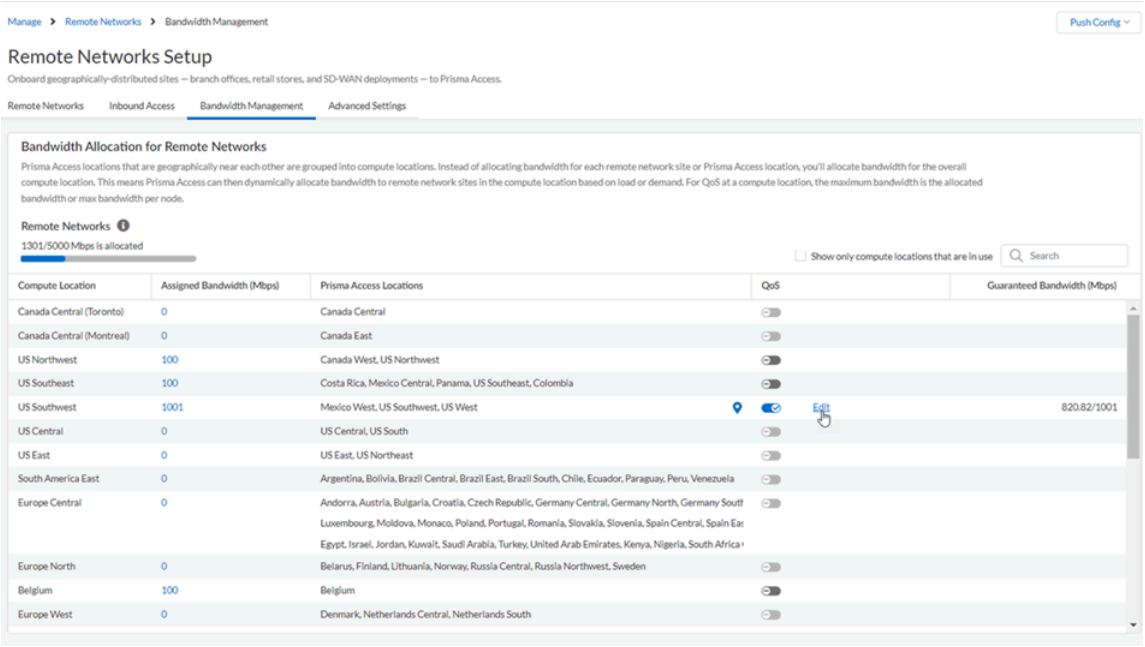
   Cada ubicación de Prisma Access tiene asignado un ancho de banda desde su ubicación de cómputo, y debe conocer el nombre de la ubicación de cómputo para las ubicaciones donde desea asignar QoS.
3. Habilite QoS en un nivel de ubicación de cómputo en la columna **QoS** .

   Cualquier configuración que introduzca se aplicará a todas las ubicaciones que correspondan a esta ubicación de cálculo.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Deberá **Edit (Editar)** la configuración de QoS para la ubicación de cómputo.



1. Seleccione la relación de ancho de banda garantizado, que es una relación basada en el ancho de banda total asignado para la ubicación de cómputo.

   Por ejemplo, si ha asignado un ancho de banda de 1001 Mbps para la ubicación de cómputo del suroeste de EE. UU. e introduce una **Guaranteed Bandwidth Ratio (Relación de ancho de banda garantizada)** del 82 %, el ancho de banda garantizado para esa ubicación de cómputo es 820,82 Mbps.

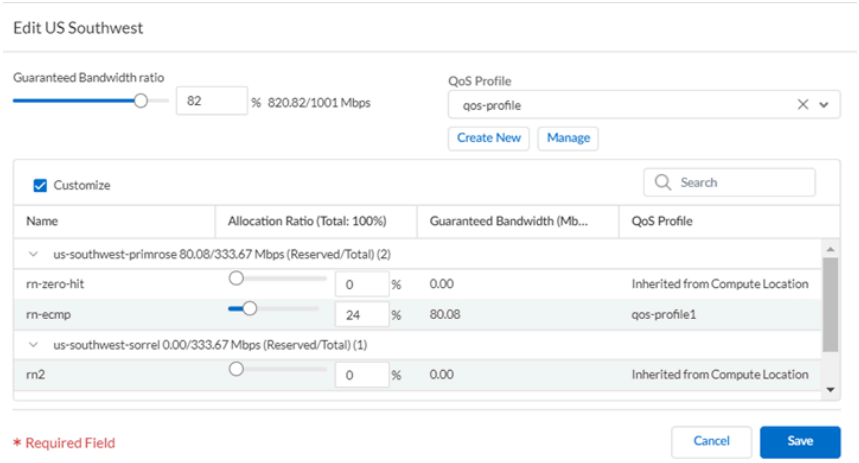
   De forma predeterminada, a cada red remota se le asigna un porcentaje que es igual al número de conexiones. Por ejemplo, dado 4 conexiones en una ubicación de cómputo y un ancho de banda total garantizado de 820,82 Mbps, cada ubicación recibe el 25 % de ese ancho de banda o 205,2 Mbps.

   Si la licencia ADEM impulsada por AIOps está habilitada, entonces la licencia se habilita automáticamente para todas las ubicaciones de cómputo.
2. Deberá **Create New (Crear nuevo)** perfil de QoS o **Manage (Gestionar)** un perfil de QoS existente.

   Utilice perfiles QoS para dar forma al tráfico en el punto de salida.
3. (Opcional) Personalice la configuración de QoS para sitios de red remotos en una ubicación de cómputo. Si tiene varias redes remotas por ubicación de cómputo y desea cambiar la relación de ancho de banda o el perfil de QoS para cada red remota,

 ©2025 Palo Alto Networks, Inc.

seleccione **Personalizar** y cambie la relación de asignación de ancho de banda, el perfil de QoS o ambos.



*Si selecciona **Customize (Personalizar)** y luego incorpora redes remotas adicionales en el mismo nodo de terminación IPSec, los sitios recién incorporados reciben una proporción de asignación de 0, y debe reequilibrar manualmente la proporción de asignación entre los sitios existentes y el sitio recién incorporado.*

STEP 5 | **Save (Guardar)** los cambios.

STEP 6 | **Push (Enviar)** las configuraciones.

QoS para redes remotas (Panorama)

Configurar la Calidad de Servicio en Prisma Access completando la siguiente tarea.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Añada una o más reglas de política de seguridad para redes remotas y usuarios móviles para marcar el tráfico de entrada para QoS.

Utiliza estas políticas para hacer coincidir un flujo de tráfico y asignarle un valor DSCP seleccionado.

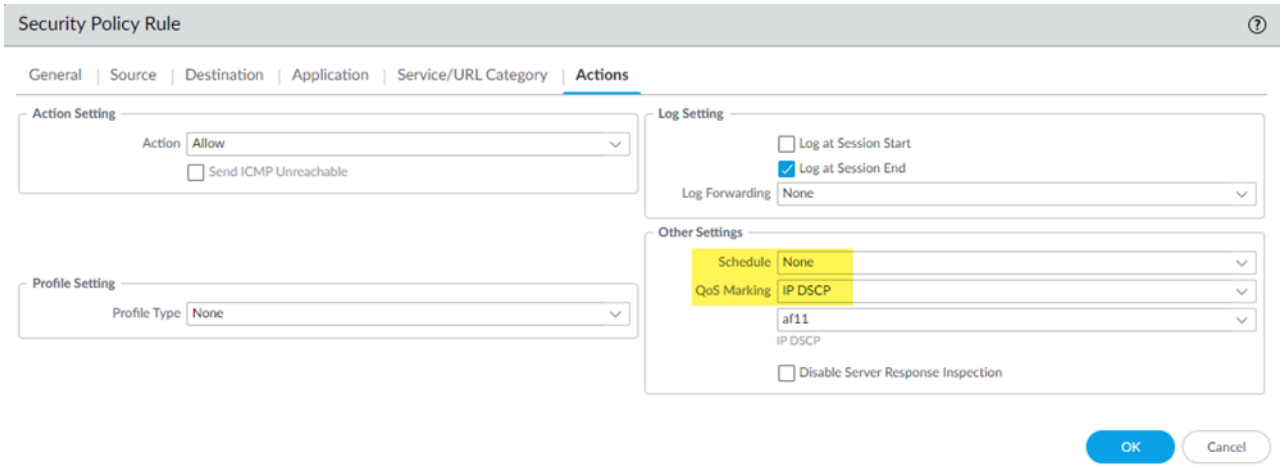
1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)**.

   Alternativamente, selecciona **Policies (Políticas)** > **Security (Seguridad)** > **Post Rules (Reglas posteriores)** para añadir una regla al final del orden de reglas que se evalúa después de una regla previa.

   *Asegúrese de seleccionar el **Device Group (Grupo de dispositivos)** correcto. Para crear una regla de seguridad para una red remota, seleccione el grupo de dispositivos para la red remota (por ejemplo, **Remote_Network_Device_Group**); para usuarios móviles, seleccione el grupo de dispositivos para los usuarios móviles (por ejemplo, **Mobile_User_Device_Group**).*
2. **Add (Añadir)** una regla de política de seguridad.
3. Introduzca un **Name (Nombre)** para la regla.
4. Defina los criterios de coincidencia para los campos de destino en el paquete.

   Consulte Crear una regla de política de seguridad para obtener detalles.
5. Haga clic en **Actions (Acciones)**, luego seleccione un **QoS Marking (Marcado de QoS)** de **IP DSCP (DSCP de IP)** o **IP Precedence (Precedencia de IP)**.
6. Introduzca el valor de QoS en forma binaria o seleccione el valor del menú desplegable.

   La siguiente captura de pantalla muestra una regla de política de seguridad que coincide con el tráfico marcado con un valor **IP DSCP (DSCP de IP)** de **af11**.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Añada una o más reglas de políticas de QoS.

Utilice políticas de QoS para vincular el marcado DSCP a una de las ocho clases disponibles. Use estas clases más tarde cuando cree uno o más perfiles de QoS.

1. Seleccione **Policies (Políticas)** > **QoS** > **Pre Rules (reglas previas)**.

   Alternativamente, utilice Reglas posteriores [**Policies (políticas)** > **QoS** > **Post Rules (Reglas posteriores)**] para añadir una regla al final del orden de reglas que se evalúa después de una regla previa.

   Las conexiones de servicio no admiten las reglas posteriores de QoS; utilice las reglas previas solo con las Conexiones de servicio.

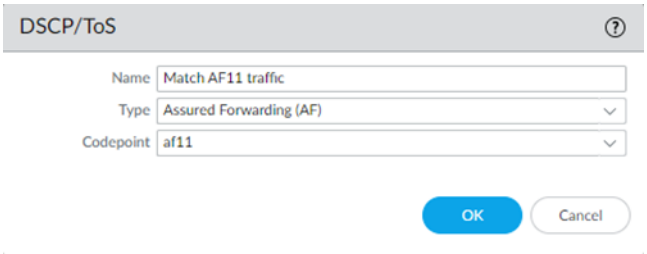
   Asegúrese de seleccionar el **Device group (Grupo de Dispositivos)** correcto para la conexión de servicio (por ejemplo, **Service_Conn_Device_Group**) o conexión de red remota (por ejemplo, **Remote_Network_Device_Group**). Si una regla en un grupo de dispositivos compartidos tiene valores definidos diferentes a los valores en las áreas de

 ©2025 Palo Alto Networks, Inc.

configuración **General**, **DSCP/ToS** y **Other (Otro)**, Prisma Access no aplica la regla en la red remota y la conexión de servicio.

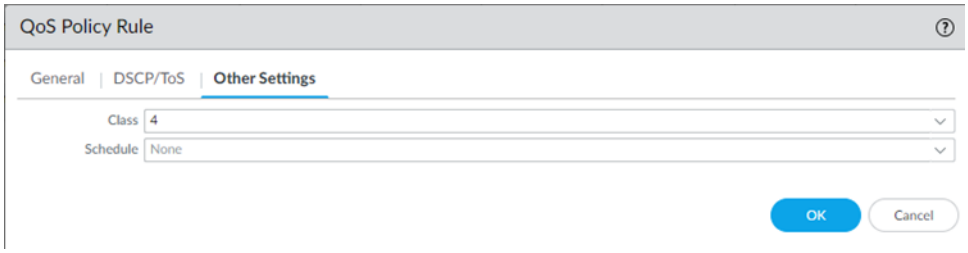
2. **Add (Añadir)** una regla de políticas de QoS.
3. Haga clic en **General** y escriba un nombre para la regla de la política.
4. Haga clic en la pestaña **DSCP/ToS**, luego haga clic en **Codepoints (Puntos de código)** y seleccione **Add (Añadir)** para añadir uno o más nuevos puntos de código.

   Para las implementaciones de Clean Pipe, puede especificar configuraciones adicionales de QoS en la política, como origen, destino o aplicación.
5. Especifique un **Name (Nombre)** para la regla DSCP/ToS, luego seleccione un **Type (Tipo)** y un **Codepoint (Punto de código)**.



   Seleccione la opción **Any (Cualquiera)** (predeterminada) para que la política coincida con el tráfico independientemente del valor Punto de código de servicios diferenciados (DSCP) o la precedencia de IP/tipo de servicio (ToS) definido para el tráfico.
6. Haga clic en la pestaña **Other Settings (Otras configuraciones)**, luego elija la **Class (Clase)** QoS que desea asignar a la regla.

   Las características de clase se definen en el perfil de QoS.
7. Haga clic en **OK (Aceptar)**.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cree uno o más perfiles de QoS para dar forma al tráfico de QoS en la salida para conexiones de servicio y conexiones de red remotas.

Utiliza perfiles para dar forma al tráfico en el punto de salida definiendo clases de QoS y asignándoles un ancho de banda. Debe seleccionar un perfil de QoS existente o crear un nuevo perfil de QoS cuando habilite QoS para Prisma Access.

1. Seleccione la plantilla correcta para el perfil que desea crear (**Remote_Network_Template** o **Service_Conn_Template**); luego, seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **QoS Profile (Perfil de QoS)** y
2. **Add (Añadir)** un perfil.
3. Introduzca un **Name (Nombre)** de perfil.
4. Configure los límites de ancho de banda general para la regla del perfil de QoS.
   - Introduzca un **Egress Max (Máx. de salida)** que represente el máximo rendimiento (en Mbps) para el tráfico que sale de la conexión de servicio o de la conexión de red remota.
     - Para las conexiones de servicio, especifique un número de hasta 1 Gbps (1.000 Mbps).

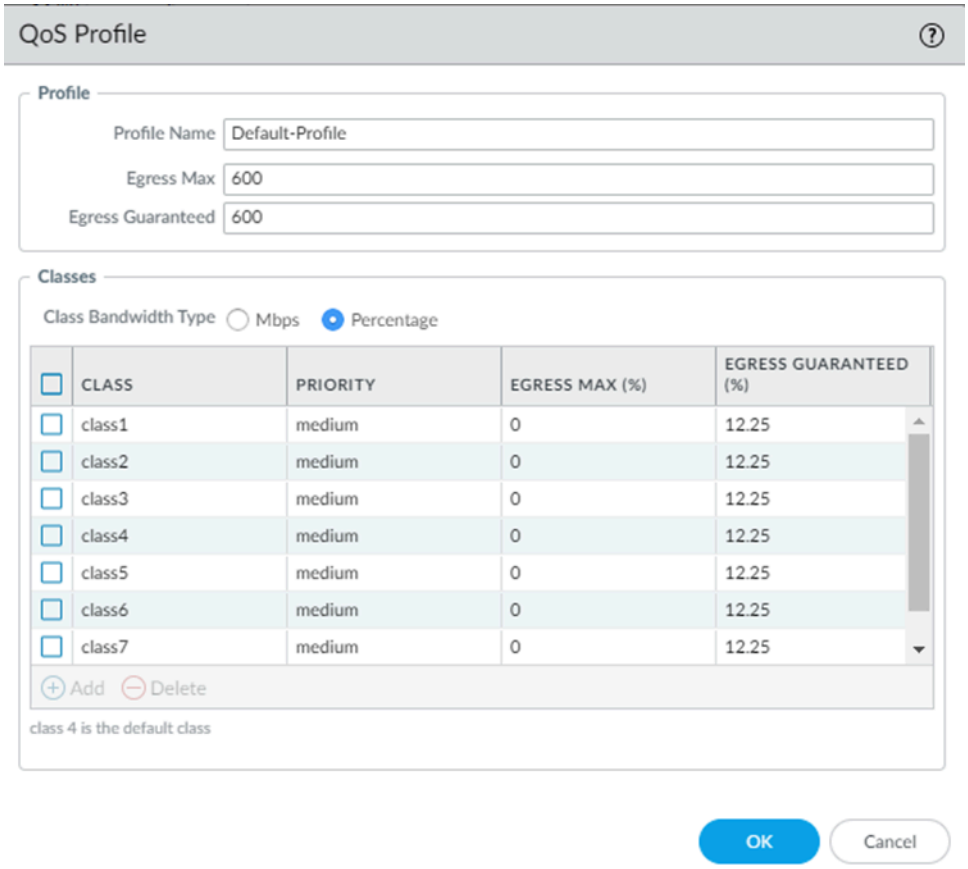
       No introduzca un número mayor de 1 Gbps; Prisma Access calcula el ancho de banda de conexión del servicio por túnel IPSec de conexión de servicio y no de forma acumulativa a través de múltiples túneles.
   - Para conexiones de red remotas, introduzca un valor de **0**.
   - Introduzca un ancho de banda de valor de **Egress Guaranteed (Salida garantizada)** que es el ancho de banda garantizado para este perfil (en Mbps).
     - Para las conexiones de servicio, introduzca un ancho de banda de **Egress Guaranteed (Salida garantizada)** que sea el ancho de banda garantizado para este perfil (en Mbps).

       Todo el tráfico que supere el valor de Egress Guaranteed será la mejor opción pero no estará garantizado. El ancho de banda que está garantizado pero sin usar continúa disponible para todo el tráfico.
     - Para conexiones de red remotas, introduzca un valor de **0**.
5. En la sección Clases, seleccione **Add (Añadir)** para añadir una o más clases y especifique cómo marcar hasta ocho clases individuales de QoS.
   - Para los perfiles de QoS utilizados por redes remotas que asignan ancho de banda por ubicación de cómputo, cambie el **Class Bandwidth Type (Tipo de ancho de banda de clase)** a **Percentage (Porcentaje)** e introduzca porcentajes para los valores de **Egress Max (Máx. de salida)** y **Egress Guaranteed (Salida garantizada)** que introduzca en esta área.
   - Para los perfiles de QoS utilizados por conexiones de servicio o por redes remotas que asignan ancho de banda por ubicación, especifique un tipo de **Mbps**.
   - Seleccione la **Priority (Prioridad)** para la clase:[either **real-time (tiempo real)**, **high (alta)**, **medium (media)** o **low (baja)**].

 ©2025 Palo Alto Networks, Inc.

- Introduzca el **Egress Max (Máx. de salida)** para el tráfico asignado a cada clase de QoS que cree.
  - Para redes remotas que asignan ancho de banda por ubicación de cómputo, introduzca **0**.
  - Para los perfiles de QoS basados en el ancho de banda (utilizados por conexiones de servicio o redes remotas que asignan ancho de banda por ubicación), introduzca un valor en Mbps. El valor Máximo de salida para una clase de QoS debe ser menor o igual que el valor Máximo de salida definido para el perfil de QoS.
- Introduzca el porcentaje o ancho de banda **Egress Guaranteed (Garantizado de salida)** en Mbps para cada clase de QoS. Para los perfiles de QoS para redes remotas, introduzca un porcentaje.

  El ancho de banda garantizado asignado a una clase no está reservado para esa clase; el ancho de banda que no se utiliza continúa permaneciendo disponible para todo el tráfico. Cuando una clase de tráfico supera el ancho de banda garantizado de salida, Prisma Access pasa ese tráfico en base al mejor esfuerzo.
- Introduzca un **Class Bandwidth Type (Tipo de ancho de banda de clase)** para el perfil.



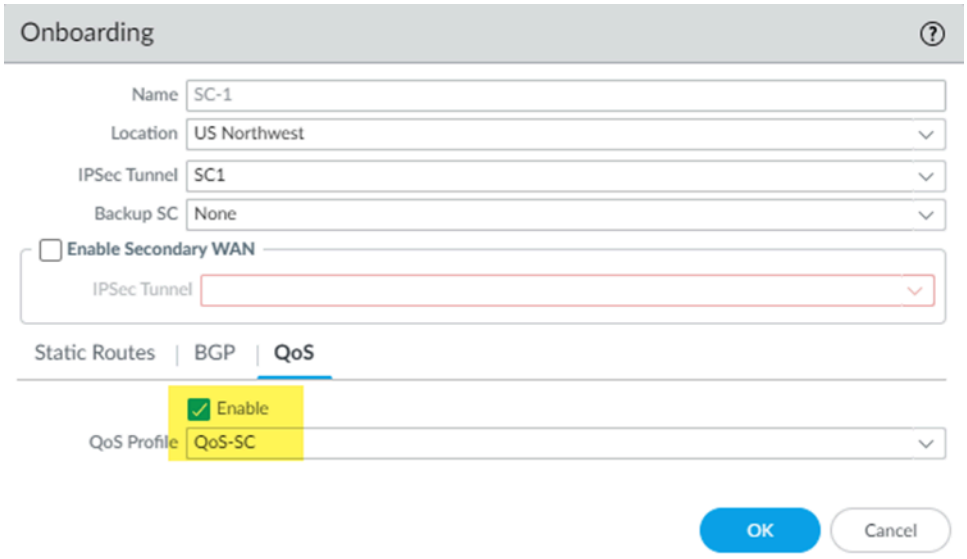
6. Haga clic en **OK (Aceptar)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Conexiones de Servicio Solamente) Habilite QoS para la conexión de servicio y aplique el perfil de QoS a la conexión.

1. Habilite QoS seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicios)**, seleccionando un **Connection Name (Nombre de conexión)**, haciendo clic en la pestaña **QoS** y luego seleccionando **Enable (Habilitar)** para habilitar QoS.

   Si asigna el ancho de banda de su red remota por Redes remotas de Prisma Access en lugar de por ubicación de cómputo, configura QoS de la misma manera que lo hace con las conexiones de servicio. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, seleccione el hiperenlace para un nombre de conexión **Name (Nombre)**, haga clic en la pestaña **QoS** y en **Enable (Habilitar)** QoS. Si asigna ancho de banda por ubicación de cómputo (el método predeterminado), continúe al Paso 5 para configurar QoS para redes remotas.
2. Seleccione un perfil de QoS y haga clic en **OK (Aceptar)**.



STEP 5 | (implementaciones de red remota que asignan ancho de banda solo por ubicación de cómputo) Habilite QoS para sus ubicaciones de red remotas.

1. Determine las ubicaciones de Prisma Access donde desea implementar QoS; luego encuentre la ubicación de cómputo que corresponde a cada lugar.

   Cada ubicación tiene asignado un ancho de banda desde su ubicación de cómputo, y debe conocer el nombre de la ubicación de cómputo para las ubicaciones donde desea asignar QoS. Para obtener una lista de asignación cómputo de ubicación a ubicación, consulte Prisma Access Ubicaciones, o seleccione **Panorama** > **Cloud Services (Servicios en la Nube)** > **Configuración** > **Remote Networks (Redes Remotas)** > **Aggregate Bandwidth (Ancho de banda agregado)** y haga clic en el icono de engranaje; las asignaciones se muestran en las columnas de **Compute Location (Ubicación de cómputo)** y **Prisma Access Location (Ubicación de Prisma Access)**.
2. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** > **Settings (Configuración)**, haga clic en el engranaje para editar la configuración y seleccione **QoS**.

 ©2025 Palo Alto Networks, Inc.

3. **Enable QoS (Habilitar QoS)** a nivel de ubicación de cómputo.

   Cualquier configuración que introduzca se aplicará a todas las ubicaciones que correspondan a esta ubicación de cálculo.

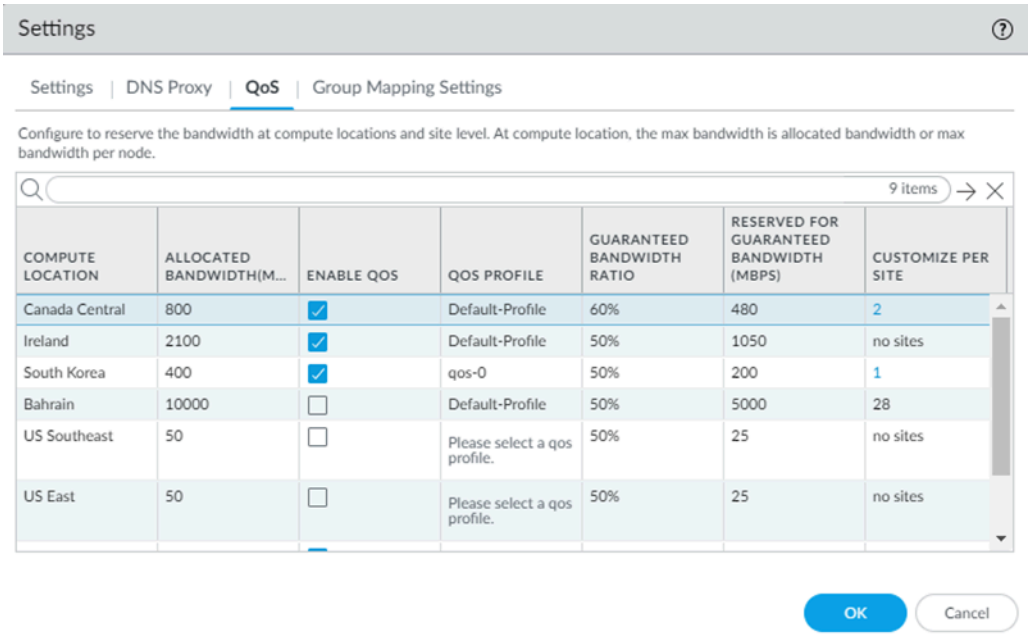
4. Introduzca el **QoS Profile (Perfil QoS)**, la **Guaranteed Bandwidth Ratio (Relación de ancho de banda garantizado)** y **Reserved for Guaranteed Bandwidth (Mbps) [Reservado para ancho de banda garantizado (Mbps)]**.

   - Introduce el **QoS Profile (Perfil de QoS)** que se utilizará con esta ubicación de cómputo.

     Si desea utilizar diferentes Perfiles de QoS por redes remotas, utilice **Customize Per Site (Personalizar por sitio)** como se describe en un paso posterior.
   - Introduzca la Guaranteed Bandwidth Ratio (Relación de ancho de banda garantizado), que es una relación basada en el ancho de banda total asignado para la ubicación de cómputo.

     Por ejemplo, si ha asignado un ancho de banda de 800 Mbps para la ubicación de cómputo de Canadá Central, y introduces una **Guaranteed Bandwidth Ratio (Relación de ancho de banda garantizado)** del **60 %**, el ancho de banda garantizado para esa ubicación de cómputo es de 480 Mbps.
   - Introduzca la cantidad de ancho de banda que está **Reserved for Guaranteed Bandwidth (Mbps) [Reservada para el ancho de banda garantizado (Mbps)]** para el perfil de QoS y la ubicación de cómputo que seleccionó.

   La siguiente captura de pantalla muestra QoS habilitado para las ubicaciones de cómputo de Canadá Central, Irlanda y Corea del Sur.



5. (Opcional) si tiene múltiples conexiones de red remota por ubicación de cómputo y desea cambiar ya sea la proporción de ancho de banda o el perfil de QoS para cada ubicación, incorpore sus ubicaciones de red remota; luego, seleccione **Customize Per**

©2025 Palo Alto Networks, Inc.

Site (Personalizar por sitio) y cambie la proporción de asignación de ancho de banda, el perfil de QoS o ambos.

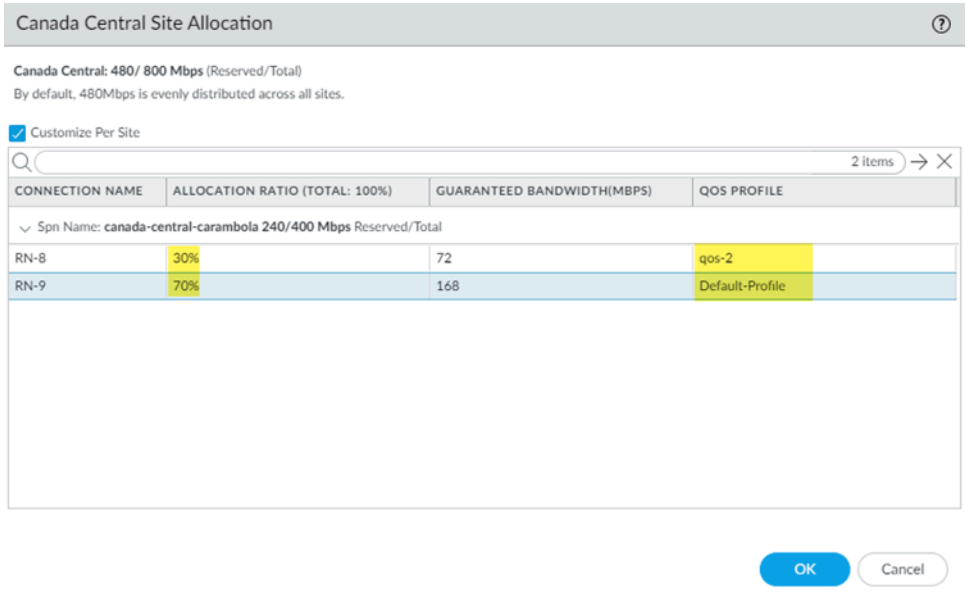
- Para personalizar el ancho de banda garantizado, haga clic en el número en el área **Customize Per Site (Personalizar por sitio)**, seleccione **Customize Per Site (Personalizar por sitio)** y cambie la **Allocation Ratio (Ratio de Asignación)**.

  Por defecto, a cada conexión remota se le asigna un porcentaje que es igual al número de conexiones. Por ejemplo, dado 4 conexiones en una ubicación de cómputo y un ancho de banda total garantizado de 100 Mbps, cada ubicación recibe el 25 % de ese ancho de banda o 25 Mbps.

  *Si selecciona **Customize Per Site (Personalizar por sitio)** y luego incorpora redes remotas adicionales en el mismo nodo de terminación IPSec, los sitios recién incorporados reciben una proporción de asignación de **0**, y debe reequilibrar manualmente la proporción de asignación entre los sitios existentes y el sitio recién incorporado.*

  *Si no selecciona **Customize Per Site (Personalizar por sitio)**, el porcentaje de ancho de banda se reequilibra automáticamente cuando añade redes remotas. Por ejemplo, si no seleccionó **Customize Per Site (Personalizar por sitio)** y tiene cuatro redes remotas incorporadas, cada una de esas redes remotas tiene una proporción de asignación del 25 %. Si añade una quinta red remota, los cinco sitios se reequilibran y reciben un ancho de banda garantizado del 20 %.*

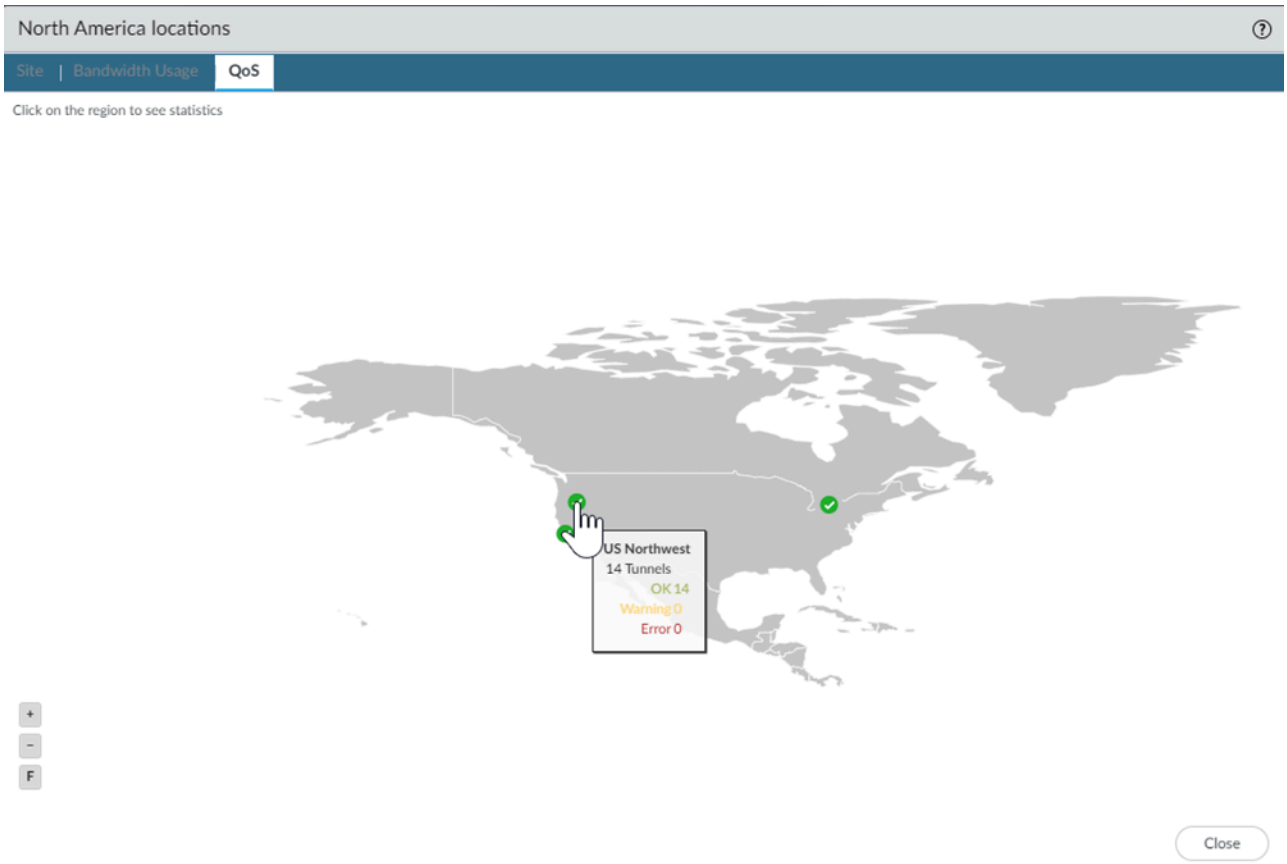
- Si desea especificar un perfil de QoS a nivel de red remota, selecciona un **QsO Profile (Perfil de QoS)** diferente para la red remota.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | Verifique el estado de QoS.

- Para redes remotas, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Remote Networks (redes remotas)**, seleccione una región del mapa, seleccione **QoS**, luego seleccione una ubicación.

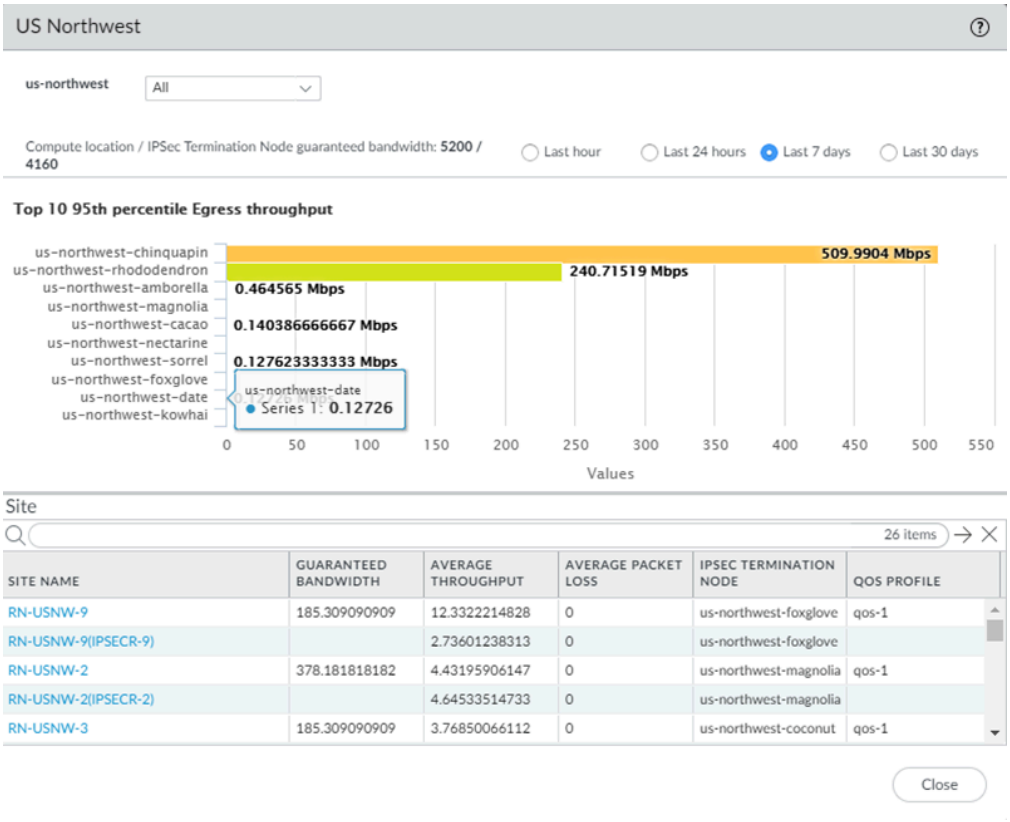


Estadísticas de red remota para los 10 nodos de terminación IPSec que tienen el mayor rendimiento. Prisma Access utiliza el estándar del percentil 95 para recopilar estadísticas,

 ©2025 Palo Alto Networks, Inc.

que rastrea el ancho de banda en la utilización máxima e ignora el 5 por ciento superior de los picos de utilización y las grandes ráfagas.

Seleccione el rango de tiempo [**Last hour (Última hora)**, **Last 24 hours (Últimas 24 horas)**, **Last 7 days (Últimos 7 días)** o **Last 30 days (Últimos 30 días)**] para ver estadísticas de ese período de tiempo.

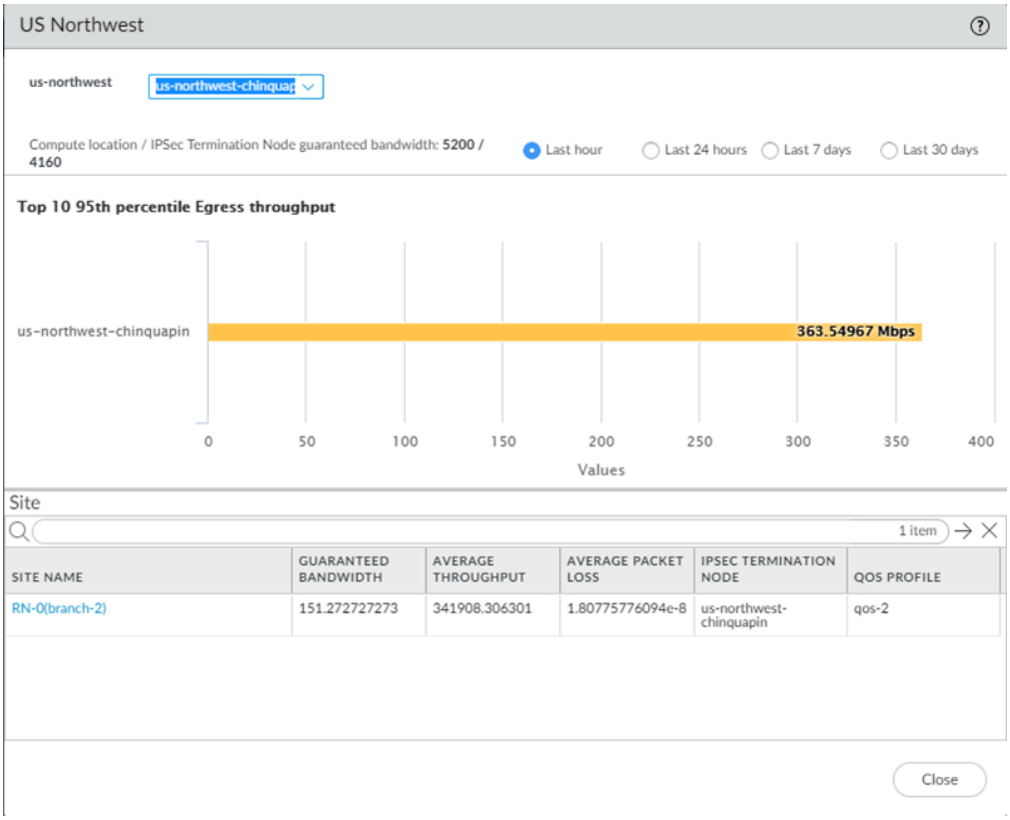


Las redes remotas con el mayor uso de ancho de banda de salida se muestran en el área del **Site (Sitio)**, junto con las estadísticas de las ubicaciones de las redes remotas para el **Guaranteed Bandwidth (Ancho de banda garantizado)**, el **Average Throughput (Rendimiento medio)**, la **Average Packet Loss (Pérdida media de paquetes)** y el **IPSec Termination Node (Nodo de terminación IPSec)** y el **QoS Profile (Perfil QoS)** utilizado por la red remota. También puede **Search (Buscar)** una ubicación.

Para ver las redes remotas asociadas con un nodo de terminación IPSec específico, cambie el menú desplegable en la parte superior de la página de **All (Todos)** a un nodo de

 ©2025 Palo Alto Networks, Inc.

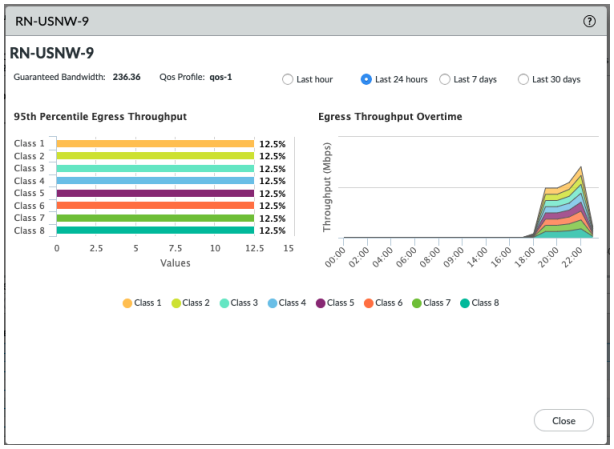
terminación IPSec específico para ver las estadísticas de ese nodo de terminación IPSec y las redes remotas de ese sitio.



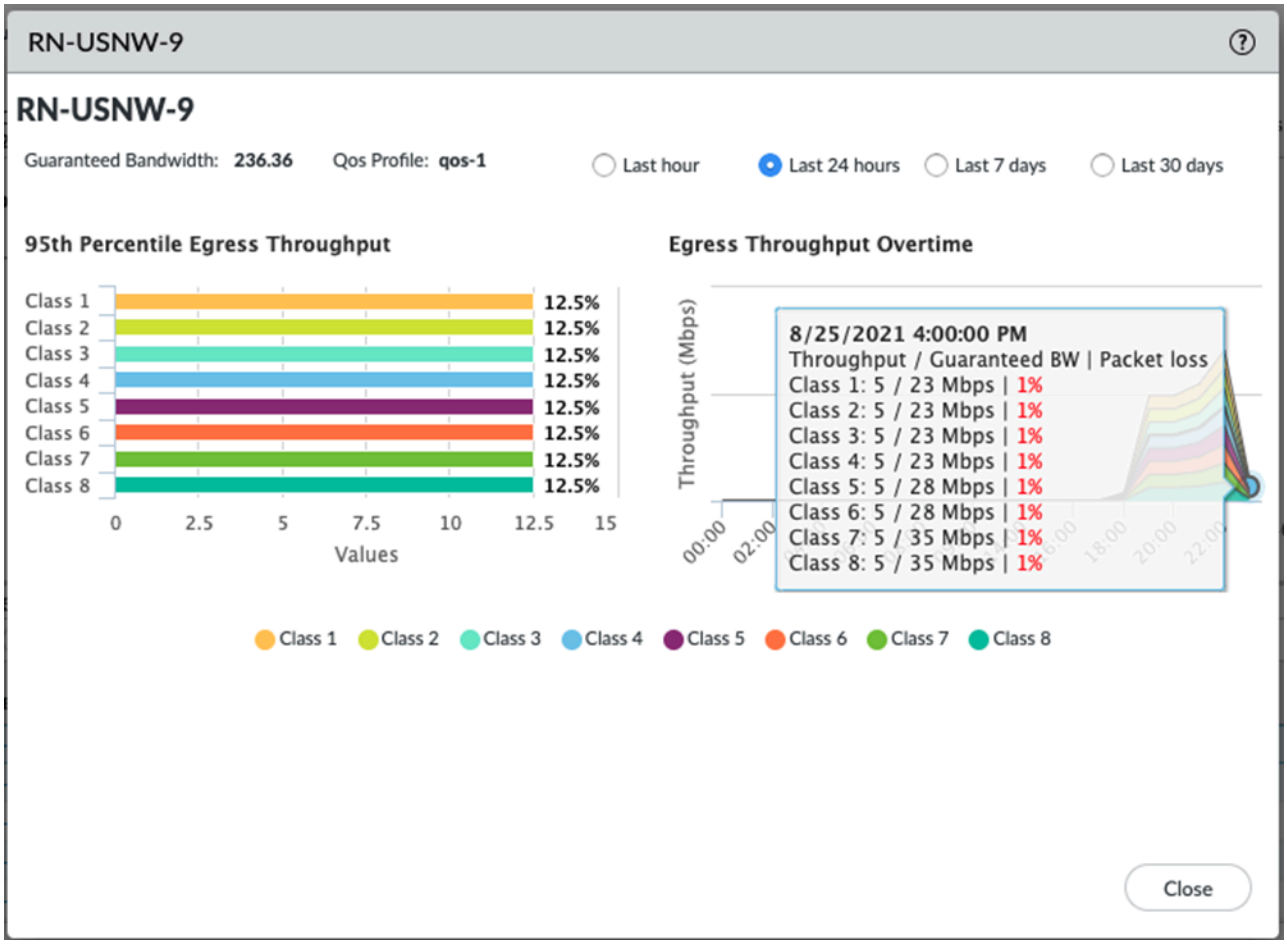
Para ver el tráfico específico de un sitio ordenado por clase de QoS, haga clic en **Site Name (Nombre del sitio)**. El ancho de banda garantizado, el rendimiento de salida y el rendimiento a lo largo del tiempo se muestran para el sitio de red remoto. También puede

 ©2025 Palo Alto Networks, Inc.

ordenar esta información en la última hora, las últimas 24 horas, los últimos 7 días o los últimos 30 días.



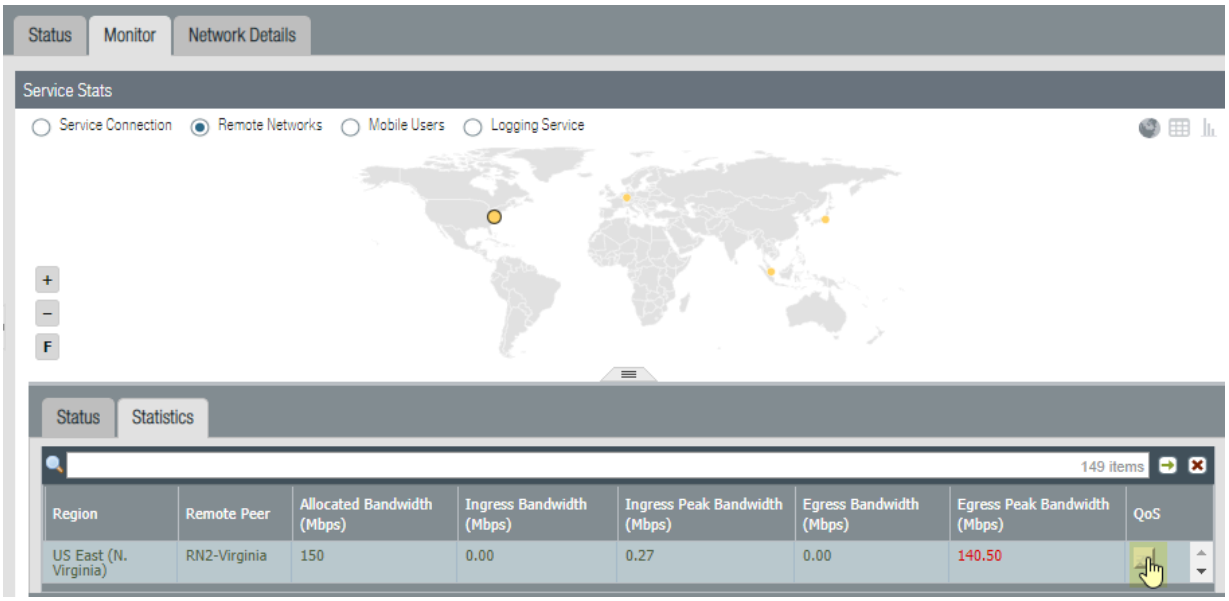
Pasa el ratón sobre el gráfico de la derecha para obtener información detallada sobre un período de tiempo específico.



- Para las conexiones de servicio, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Service Connection (Conexión de servicio)**, seleccione una región y luego **Monitor (Supervisar)** las **Statistics (Estadísticas)**.

Haga clic en **QoS** para ver una página con estadísticas de QoS.

 ©2025 Palo Alto Networks, Inc.

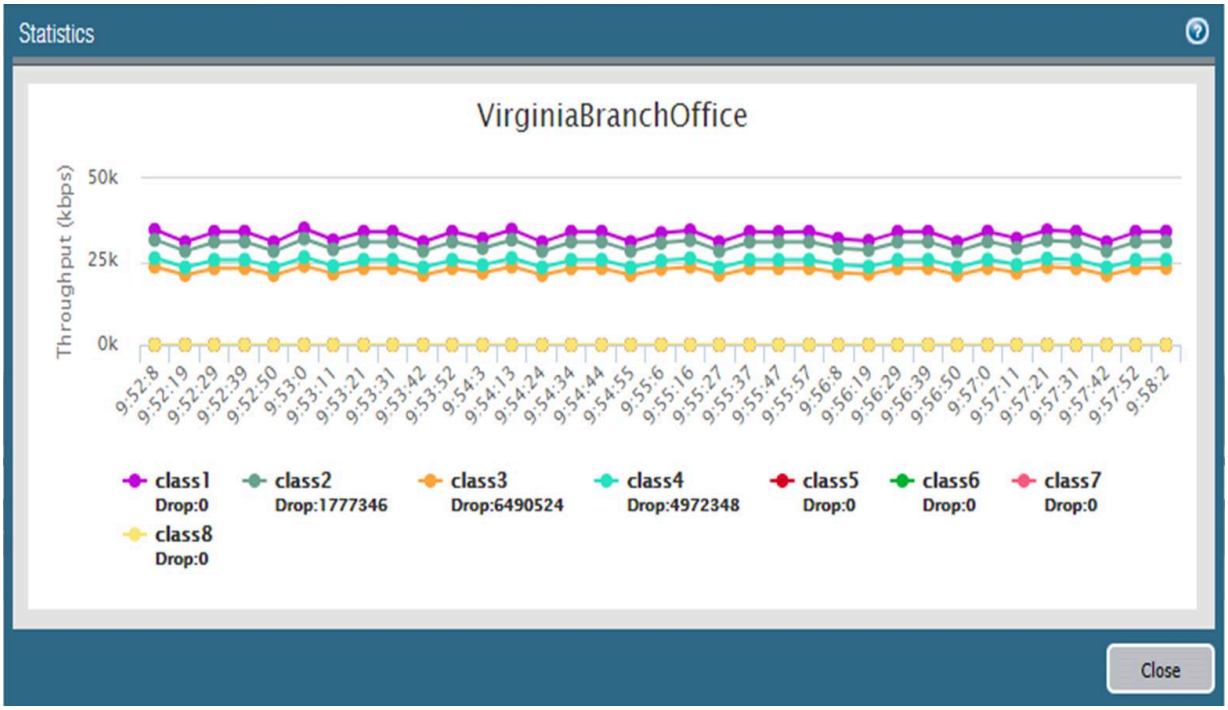


Esta página muestra un gráfico con estadísticas de QoS en tiempo real e históricas, incluyendo el número de paquetes perdidos por clase. Este gráfico muestra solo las conexiones de servicio

 ©2025 Palo Alto Networks, Inc.

o conexiones de red remotas que tienen QoS habilitado, muestra los últimos cinco minutos de la actividad de red de la conexión y se actualiza cada 10 segundos.

La siguiente figura muestra el tráfico que se pasa para las clases 1, 2, 3 y 4. Los datos debajo de la figura muestran el número de paquetes perdidos según la configuración de QoS para las clases 2, 3 y 4.



Cambiar el ancho de banda garantizado

Cambiar el ancho de banda garantizado

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si tiene varias ubicaciones de red remotas asociadas a un nodo de terminación IPSec, puede cambiar el ancho de banda garantizado para cada sitio. En el siguiente ejemplo, desea que la ubicación Este de Canadá reciba más ancho de banda que la ubicación Centro de Canadá; para ello, siga estos pasos.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** > **Settings (Configuración)**.

STEP 2 | Haga clic en el engranaje para editar la configuración y seleccione **QoS**.

STEP 3 | Seleccione **Enable QoS (Habilitar QoS)**, asigne un **QoS Profile (Perfil de QoS)** (**Default-Profile (Perfil predeterminado)** en este ejemplo) y una **Guaranteed Bandwidth Ratio (Relación de ancho de banda garantizada)** a la ubicación de cómputo central de Canadá.

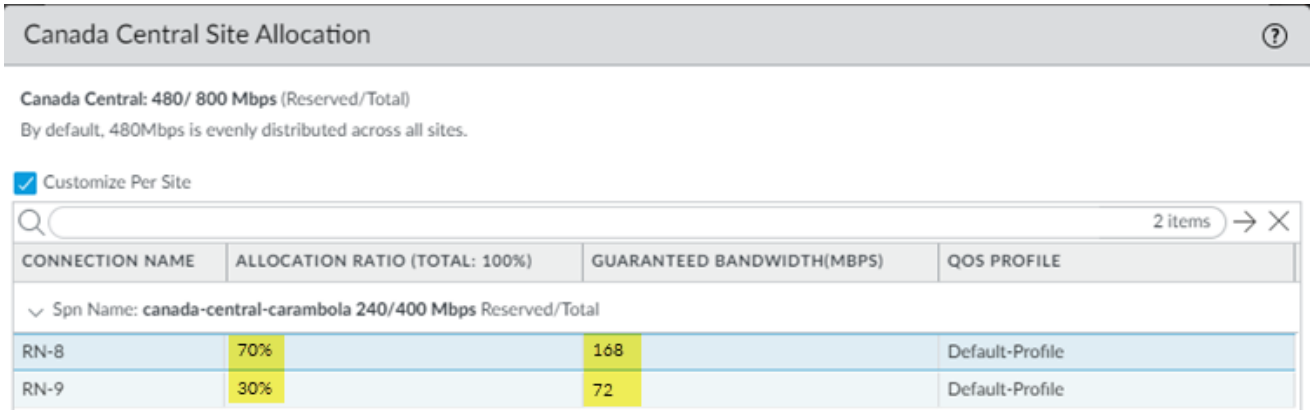
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Customize Per Site (Personalizar por sitio)**, habilite **Customize Per Site (Personalizar por sitio)** y, a continuación, aplique un **Allocation Ratio (Ratio de asignación)** de ancho de banda mayor para la red remota RN-8 (para la ubicación de Canadá Este) que la red remota RN-9 (para la ubicación de Canadá Central).

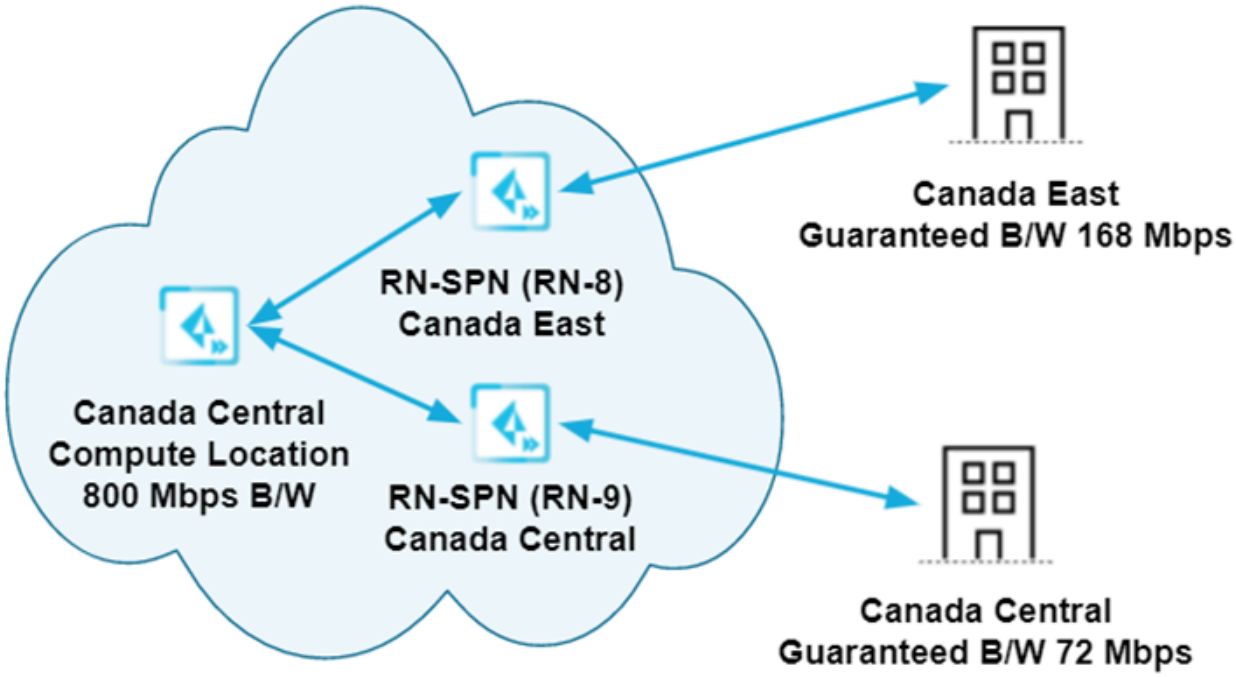
En el ejemplo siguiente se muestra un **Allocation Ratio (Ratio de asignación)** de 70 % para RN-8 y de 30 % para RN-9. El **Guaranteed Bandwidth (Mbps) [Ancho de banda garantizado**

 ©2025 Palo Alto Networks, Inc.

(Mbps)] cambia en consecuencia, mostrando las nuevas cantidades de ancho de banda garantizadas.



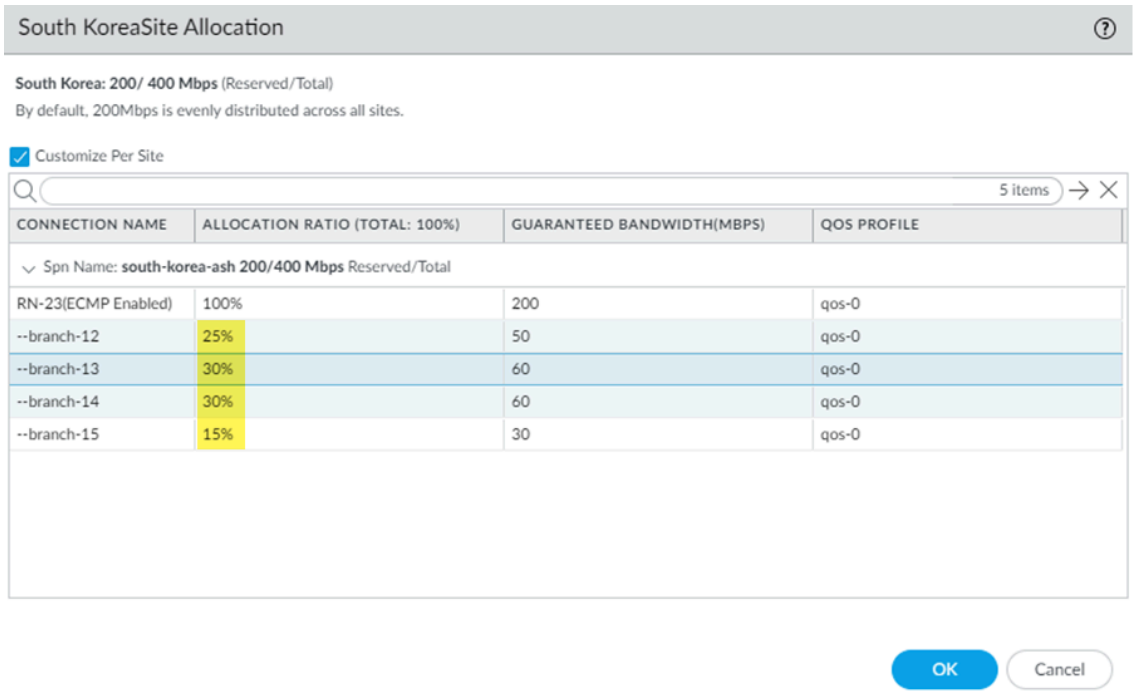
Una vez completada, su configuración tiene la siguiente asignación de ancho de banda garantizada para los dos sitios.



También puede asignar diferentes perfiles de QoS por ubicación de red remota. Para asignar diferentes perfiles, habilite la opción **Customize Per Site (Personalizar por sitio)** y seleccione diferentes perfiles de QoS para cada ubicación de red remota.

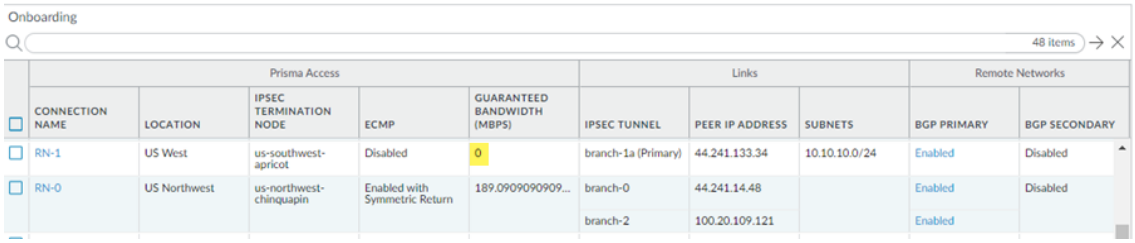
Si tiene una red remota que tiene ECMP habilitado para usar varios túneles IPSec para una sola red remota, puede cambiar la **Allocation Ratio (Ratio de asignación)** para los túneles IPSec que utiliza para esa ubicación de red remota.

 ©2025 Palo Alto Networks, Inc.



STEP 5 | Guarde y confirme los cambios.

Los valores de ancho de banda garantizados se muestran en el área **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Remote Networks (Redes remotas)**, en el área **Guaranteed Mbps (Mbps garantizados)**. Si no especificó un ancho de banda, se muestra como 0.



 ©2025 Palo Alto Networks, Inc.

Redes remotas—Alto rendimiento

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access *Esta es una versión de disponibilidad limitada. Para activar esta funcionalidad, póngase en contacto con su representante de cuentas de Palo Alto Networks.*

A medida que su negocio crece y sus oficinas se distribuyen geográficamente, las redes remotas de Prisma Access le permiten integrar rápidamente sus sucursales y brindar la mejor seguridad de su clase para sus usuarios. Para incorporar una sucursal con un alto ancho de banda, Prisma Access le proporciona una *Red remota de alto rendimiento*.

Para incorporar una red remota de alto rendimiento, debe especificar la ubicación de la sucursal y Prisma Access selecciona la ubicación más cercana al sitio. Opcionalmente, puede configurar una ubicación secundaria (de respaldo) en el sitio para lograr redundancia y resiliencia. La red remota de alto rendimiento utiliza una única dirección IP de servicio por cada 3 Gbps de ancho de banda, lo que elimina la complejidad de configurar y administrar múltiples dispositivos IPSec en cada ubicación remota.

No se admite una ubicación secundaria para implementaciones de Prisma Access (Managed by Panorama).

Una vez que haya planificado su red remota de alto rendimiento, puede comenzar el proceso de configuración, que incluye la incorporación de la red remota de alto rendimiento a Prisma Access y habilitar QoS y el enrutamiento.

Capacidades y directrices de Redes remotas: Alto rendimiento

Una red remota de alto rendimiento le proporciona las siguientes capacidades principales:

- Ancho de banda agregado de hasta 3 Gbps por nodo en una región de cómputo
- Hasta 2 Gbps de ancho de banda por túnel de red remota desde un sitio remoto
- Hasta 500 sucursales remotas por dirección IP de servicio con Prisma SD-WAN e implementaciones de CPE extendidas (de terceros)

Al configurar una red remota de alto rendimiento para una sucursal, tenga en cuenta las siguientes pautas y diferencias entre sitios y redes remotas:

- **Ubicaciones de Prisma Access**: Redes remotas: Alto rendimiento es compatible con un subconjunto de ubicaciones de Prisma Access.
- **Calidad de servicio (QoS)**: para sucursales, Prisma Access Admite QoS a nivel de sitio y el perfil de QoS que seleccione se aplica a todo el sitio.

 ©2025 Palo Alto Networks, Inc.

- **Tasa de información comprometida (CIR)**: para asegurar y confirmar la cantidad de ancho de banda utilizado por sitio, especifique una CIR. Si hay varias redes remotas que comparten ancho de banda en una ubicación de cómputo, la red remota de alto rendimiento recibe al menos el ancho de banda especificado en el CIR cuando hay contención con otros sitios en esa ubicación de cómputo.
- **Nodos de terminación IPSec**: a diferencia de las redes remotas, no es necesario seleccionar un nodo de terminación IPSec durante la incorporación de implementaciones de Prisma Access (Managed by Strata Cloud Manager). Prisma Access equilibra automáticamente la carga de las conexiones de red remotas para maximizar la asignación de ancho de banda a los sitios.

  Aún es necesario seleccionar un nodo de terminación IPSec para las redes remotas incorporadas desde Panorama.
- **Redundancia de ubicación de túnel y cómputo y número máximo de túneles por sitio**: una red remota de alto rendimiento le permite configurar tanto la ubicación como la redundancia IPSec.
  - Redundancia de ubicación (especificar una ubicación **Primary (Principal)** en una ubicación de cómputo y especificar una ubicación **Secondary (Secundaria)** en una ubicación de cómputo separada).

    La configuración de una ubicación secundaria es opcional y la ubicación secundaria debe estar en una ubicación de cómputo diferente a la ubicación principal.
  - Redundancia de túnel IPSec (especificando túneles como **Active/Active (Activo/Activo)** o **Active/Passive (Activo/Pasivo)**).

  Esta tabla le proporciona el número mínimo y máximo de ubicaciones por túnel.

Tipo de implementación de ubicación	Tipo de implementación de túnel	Número mínimo de túneles	Número máximo de túneles
Solo primario	Activo/Pasivo	1	2
Solo primario	Activo/Activo	2	4
Primario y secundario	Activo/Pasivo	2	4
Primario y secundario	Activo/Activo	4	8

- **Asignación de direcciones IP de servicio según el tipo de implementación**: el número de direcciones IP de servicio que recibe depende de si ha configurado sus redes remotas de alto rendimiento en una sola ubicación o si las ha configurado utilizando dos ubicaciones diferentes en una implementación principal y secundaria.
  - Si ha configurado su red remota de alto rendimiento en una única ubicación sin una ubicación secundaria, Prisma Access le proporciona una única dirección IP de servicio.
  - Si configura la redundancia de ubicación de cómputo en una configuración primaria y secundaria, Prisma Access le proporciona dos direcciones IP de servicio (una para la configuración primaria y otra para la secundaria).

  Si configura túneles IPSec en una configuración activa/pasiva, Prisma Access le proporciona una única dirección IP de servicio para ambos túneles (la misma que una configuración de red remota estándar de Prisma Access).

 ©2025 Palo Alto Networks, Inc.

- **Asignación de direcciones IP del servicio según el ancho de banda**: Prisma Access proporciona una única dirección IP o FQDN por cada 3 Gbps de ancho de banda en una ubicación de cómputo.
- **Ancho de banda por ubicación de cómputo**: se asigna ancho de banda por ubicación de cómputo de la misma manera que se asigna ancho de banda para una red remota estándar. Puede planificar y asignar el ancho de banda antes de comenzar la configuración o durante la creación de una red remota de alto rendimiento.
- **Compatibilidad con IPv6**:IPv6 no es compatible con implementaciones de redes remotas de alto rendimiento.

Utilice uno de los siguientes procedimientos para integrar sus redes remotas según su tipo de asignación de ancho de banda:

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

Strata Cloud Manager

Aquí se explica cómo añadir una red remota de alto rendimiento usando Strata Cloud Manager.

STEP 1 | De Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Branch Sites (Sucursales)**.

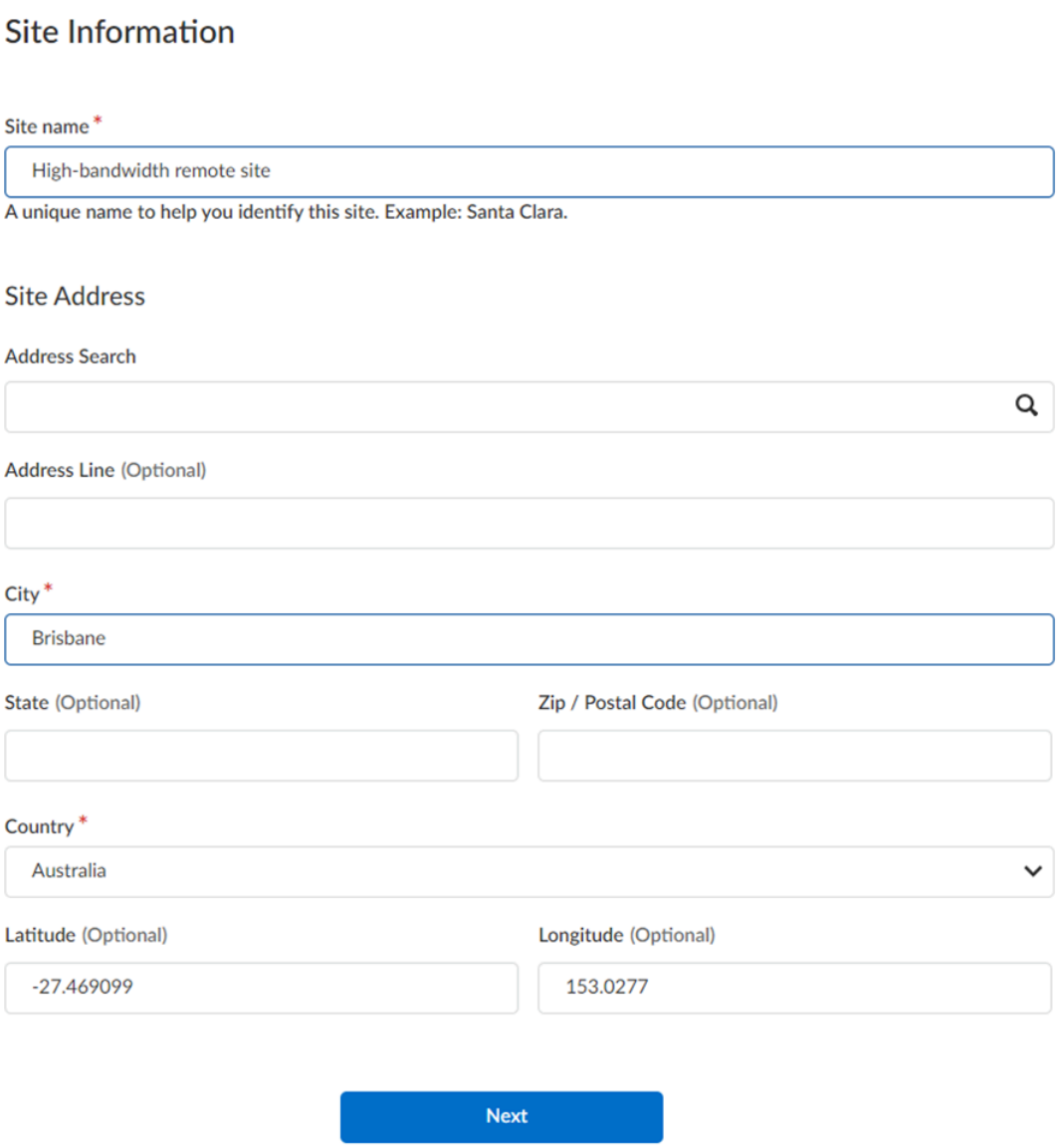
Esta opción indica que el túnel que crea para las sucursales lo finaliza su CPE (un cortafuegos de última generación de Palo Alto Networks o un CPE de terceros).

STEP 2 | **Add Site (Añadir sitio)** y asignar a la red remota un **Site Name (Nombre de sitio)** descriptivo.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Seleccione la **City (Ciudad)** y el **Country (País)** del sitio.

Para búsquedas más precisas, añada una dirección.



STEP 4 | Haga clic en **Next (Siguiente)**.

STEP 5 | Introduzca la **QoS CIR (Committed Information Rate) [CIR (tasa de información comprometida) de QoS]** en Mbps.

Si tiene varias redes remotas que comparten ancho de banda en una ubicación de cómputo, y existe contención de ancho de banda con otros sitios en esa ubicación de cómputo, la red remota de alto rendimiento recibe al menos el ancho de banda especificado en el CIR.

Si configura sitios primarios y secundarios, especifica diferentes regiones de cómputo y la región secundaria obtiene el 20 % del CIR. Por ejemplo, si configura un CIR de 100 Mbps para

 ©2025 Palo Alto Networks, Inc.

un sitio, Prisma Access proporciona al sitio principal un CIR de 100 Mbps y al sitio secundario un CIR de 20 Mbps.

Si el CIR es de 500 Mbps y si todo el ancho de banda restante en la ubicación de cómputo es utilizado por otros sitios, Prisma Access elimina cualquier ancho de banda que supere los 500 Mbps. Sin embargo, si otros sitios no utilizan el ancho de banda, el ancho de banda para la red remota de alto rendimiento puede superar los 500 Mbps hasta el ancho de banda asignado en la ubicación de procesamiento.

Introduzca un CIR mínimo de 1 Mbps y un máximo de 2000 Mbps. No supere el ancho de banda especificado para la región de cómputo.

STEP 6 | Seleccione una **Primary Prisma Access Location (Ubicación principal de Prisma Access**.

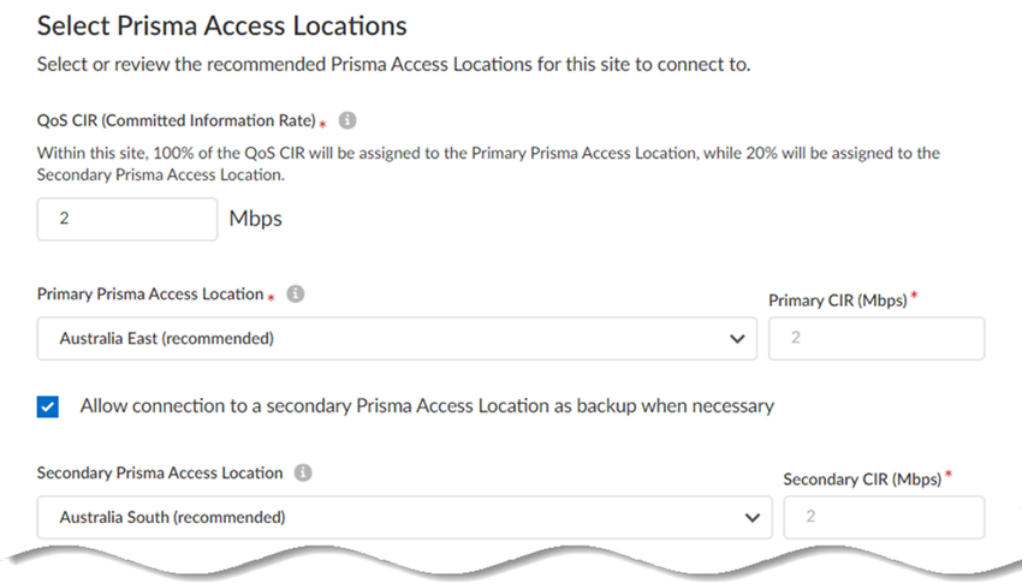
Si se **Recommended (Recomiendan)** varias ubicaciones en la lista, seleccione la ubicación que funcione mejor para su implementación.

STEP 7 | (Opcional) Para crear un sitio secundario (de respaldo), seleccione **Allow connection to a secondary Prisma Access Location as backup when necessary (Permitir la conexión a una ubicación de Prisma Access secundaria como respaldo cuando sea necesario)** y luego seleccione una **Secondary Prisma Access Location (Ubicación de Prisma Access secundaria)**.

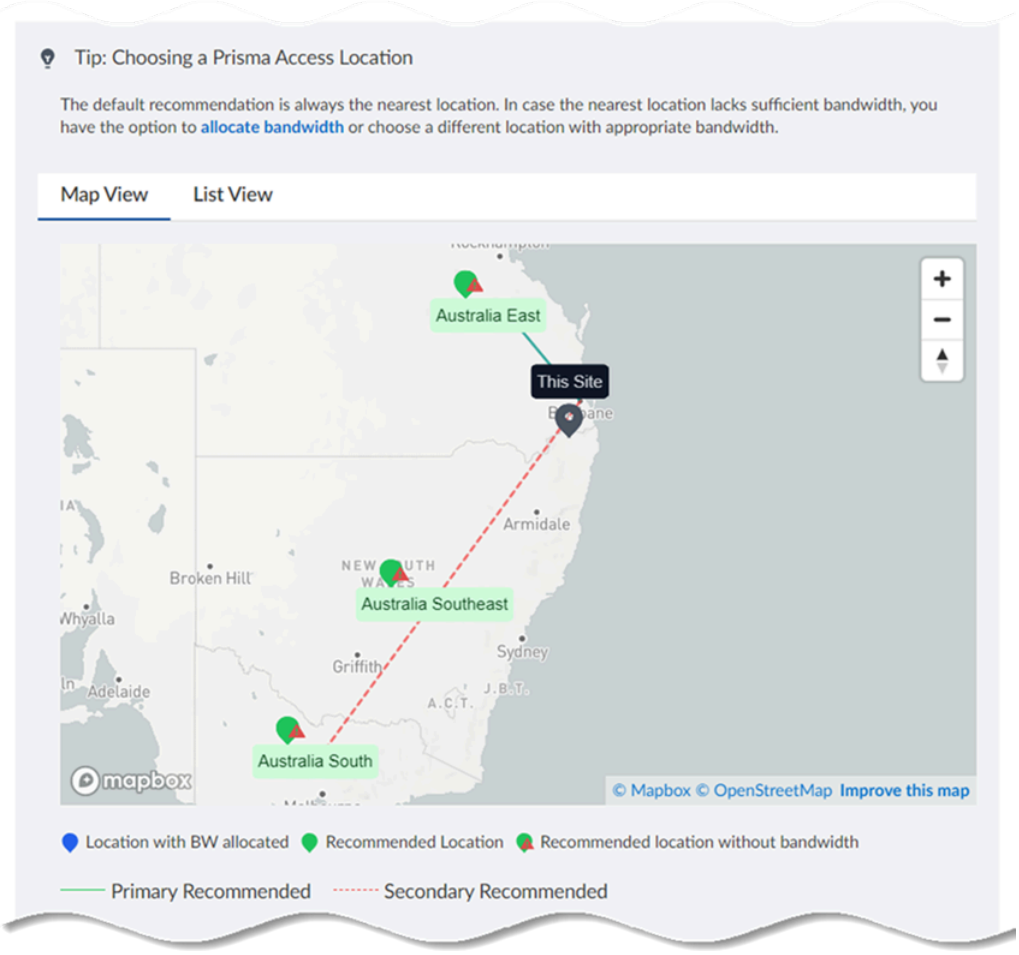
Si selecciona esta opción, Prisma Access rellena previamente la mejor ubicación secundaria o las ubicaciones que se encuentran en una ubicación de cómputo diferente a la ubicación

 ©2025 Palo Alto Networks, Inc.

principal. Si se **recomiendan**varias ubicaciones, seleccione la ubicación que funcione mejor para su implementación.



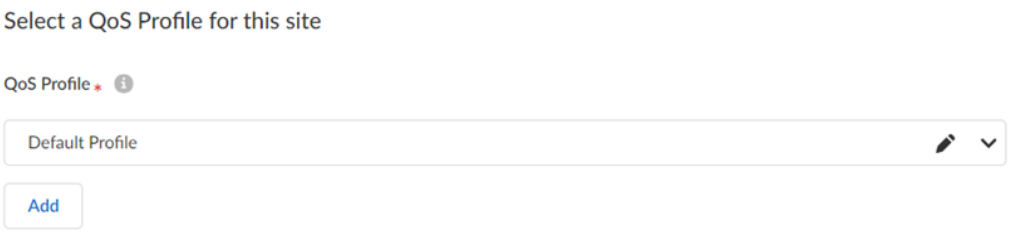
Prisma Access le proporciona un mapa con ubicaciones sugeridas para ayudarle a elegir una.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Seleccione un **QoS Profile (Perfil de QoS)** para usar en este sitio.

Redes remotas: Alto rendimiento que utilizan un único perfil QoS.

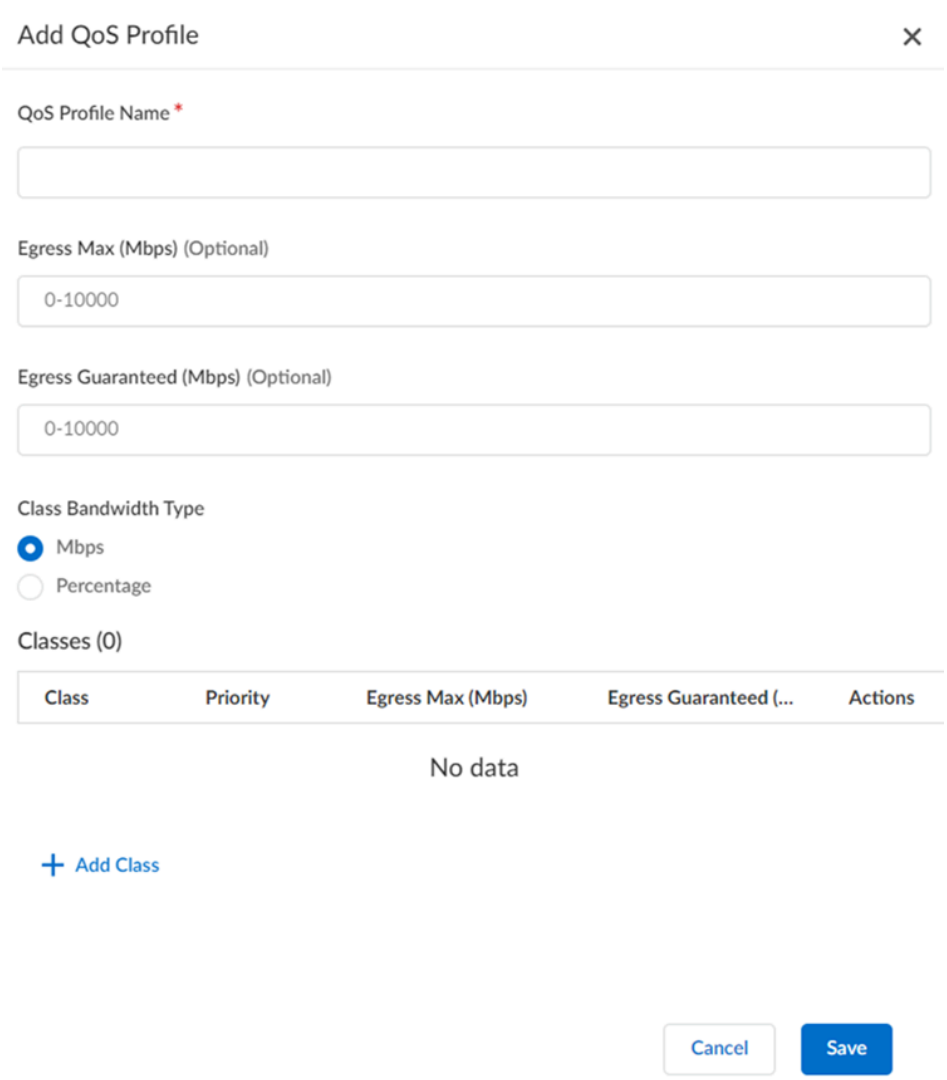


Si aún no ha creado un perfil de QoS, proceda a **Add (Añadir)** un perfil de QoS, especificando los siguientes valores:

- Introduzca un **QoS Profile Name (Nombre de perfil de QoS)** único.
- (Opcional) Introduzca un **Egress Max (Mbps [Máximo de salida (Mbps)]** que represente el rendimiento máximo en Mbps para el tráfico que sale de la conexión de servicio o la conexión de red remota.
- (Opcional) Introduzca un valor de **Egress Guaranteed (Mbps) [Salida garantizada (Mbps)]** que represente el ancho de banda garantizado para este perfil en Mbps.
- Introduzca un **Class Bandwidth Type (Tipo de ancho de banda de clase)** de **Percentage (Porcentaje)** o **Mbps**.

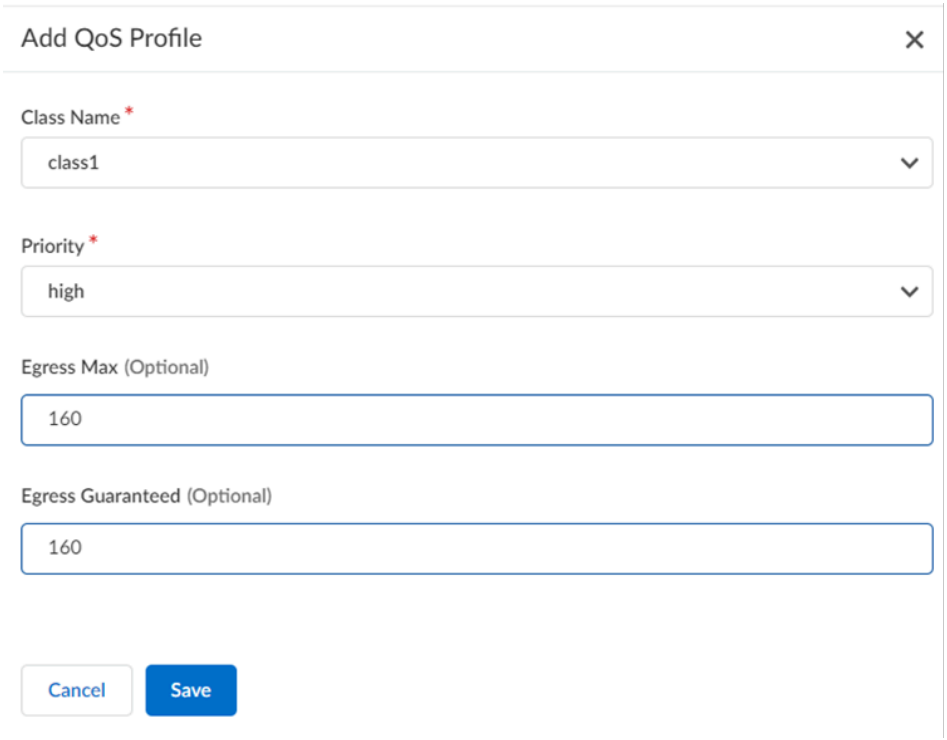
  QoS para Redes remotas: Alto rendimiento no utiliza una relación de ancho de banda garantizada.

 ©2025 Palo Alto Networks, Inc.



- En la sección Clases, seleccione **Add Class (Añadir clase)** y especifique cómo tratar hasta ocho clases de QoS individuales.
  - Introduzca un **Class Name (Nombre de clase)**.
  - Seleccione la **Priority (Prioridad)** para la clase [**real-time (tiempo real)**, **high (alta)**, **medium (media)** o **low (baja)**].
  - Introduzca un **Egress Max (Máx. de salida)** que represente el máximo rendimiento (en Mbps) para el tráfico que sale de la conexión de servicio o de la conexión de red remota.
  - Introduzca un valor de **Egress Guaranteed (Salida garantizada)** que represente el ancho de banda garantizado para este perfil (en Mbps).
- Haga clic en **Save (Guardar)** para guardar sus cambios.

 ©2025 Palo Alto Networks, Inc.

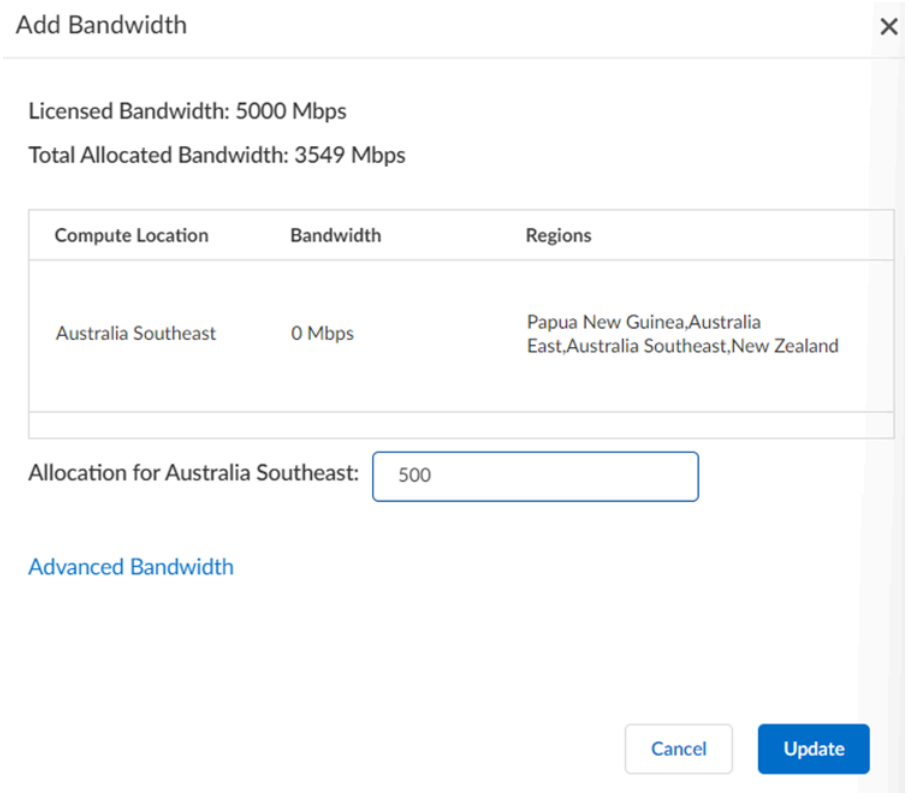


STEP 9 | Si aún no ha asignado ancho de banda, Prisma Access le solicita que **allocate (asigne)** ancho de banda para la ubicación de cómputo asociada con la ubicación que seleccionó. Especifique un ancho de banda mínimo de 50 Mbps por ubicación de cómputo.



 ©2025 Palo Alto Networks, Inc.

STEP 10 | Asigne ancho de banda a las ubicaciones que seleccionó si aún no lo ha hecho; luego seleccione **Update (Actualizar)** para actualizar sus cambios.



STEP 11 | Haga clic en **Next (Siguiente)**.

STEP 12 | Defina **Tunnel & Circuit Settings (Configuraciones de túnel y circuito)**.

1. Seleccione un **Tunnel Mode (Modo de túnel)**: **Active/Active (Activo/Activo)** o **Active/Passive (Activo/Pasivo)**.

   El modo túnel especifica cuántos circuitos de su ISP desea utilizar para la red remota de alto rendimiento.

   - Si selecciona **Active/Active (Activo/Activo)**, Prisma Access utiliza cuatro circuitos ISP para crear dos o cuatro túneles activos.
   - Si selecciona **Active/Passive (Activo/Pasivo)**, Prisma Access utiliza dos circuitos ISP para crear dos túneles activos. Si el túnel activo deja de funcionar, el túnel pasivo se vuelve activo.

2. Seleccione el número de **Internet Circuits (Circuitos de Internet)** a utilizar.

   Prisma Access asigna túneles según la cantidad de circuitos que especifique aquí y si su implementación es Activa/Activa o Activa/Pasiva, como se muestra en la siguiente tabla.

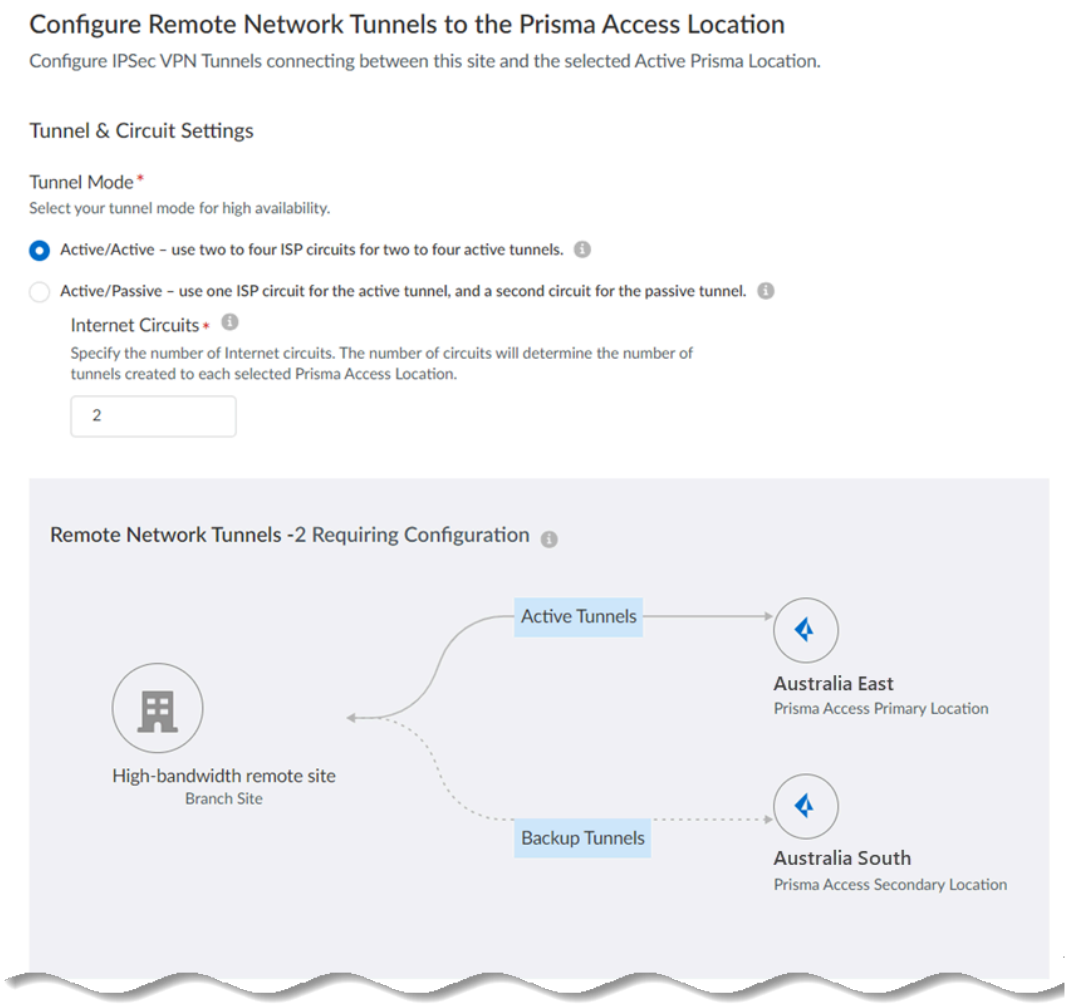
Número de circuitos	Tipo de implementación	Número de túneles
1	Activo/Pasivo	1 (uno para el túnel activo).

 ©2025 Palo Alto Networks, Inc.

Número de circuitos	Tipo de implementación	Número de túneles
2	Activo/Activo	2 (uno por cada túnel activo). Si selecciona ubicaciones primarias y secundarias, Prisma Access crea un túnel activo para la ubicación principal y un túnel activo para la ubicación secundaria.
2	Activo/Pasivo	2 (uno por cada túnel activo). Si selecciona ubicaciones primarias y secundarias, Prisma Access crea un túnel activo y pasivo para la ubicación principal y un túnel activo y pasivo para la ubicación secundaria. Si el túnel activo deja de funcionar, Prisma Access utiliza la misma dirección IP de servicio o FQDN para el túnel pasivo que se vuelve activo.
4	Activo/Activo	4 (uno por cada túnel activo). Si selecciona ubicaciones primarias y secundarias, Prisma Access crea dos túneles activos para la

 ©2025 Palo Alto Networks, Inc.

Número de circuitos	Tipo de implementación	Número de túneles
		ubicación principal y dos túneles activos para la ubicación secundaria.



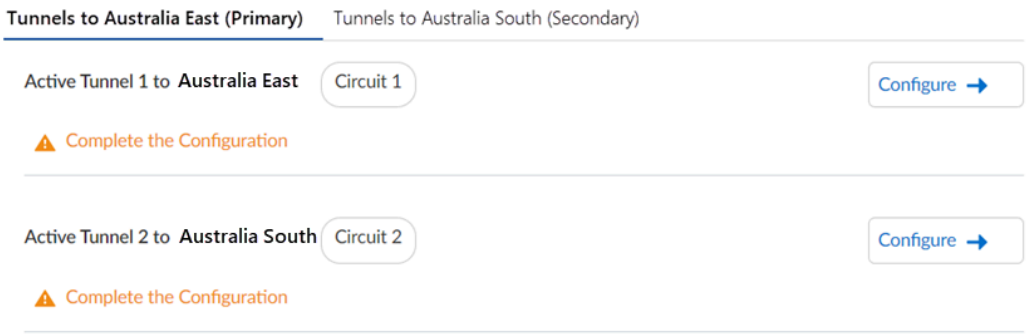
3. (Opcional) **Configure (Configurar)** su configuración del túnel IPSec.

   Prisma Access le proporciona la configuración de túnel IPSec predeterminada. Estas configuraciones determinan las configuraciones de cifrado IPSec e IKE para el túnel de

 ©2025 Palo Alto Networks, Inc.

red remoto. Si desea cambiarlos, seleccione el **Primary Tunnel (Túnel Principal)** y **Edit (Editar)** para modificar su configuración.

Si especifica una ubicación secundaria, Prisma Access rellena automáticamente los valores del túnel principal al túnel secundario; para editar el túnel secundario, seleccione ese túnel y elija **Edit (Editar)** para editar la configuración.



Tome nota de estas configuraciones; deben coincidir con las del CPE que finaliza el túnel IPSec en su sitio.

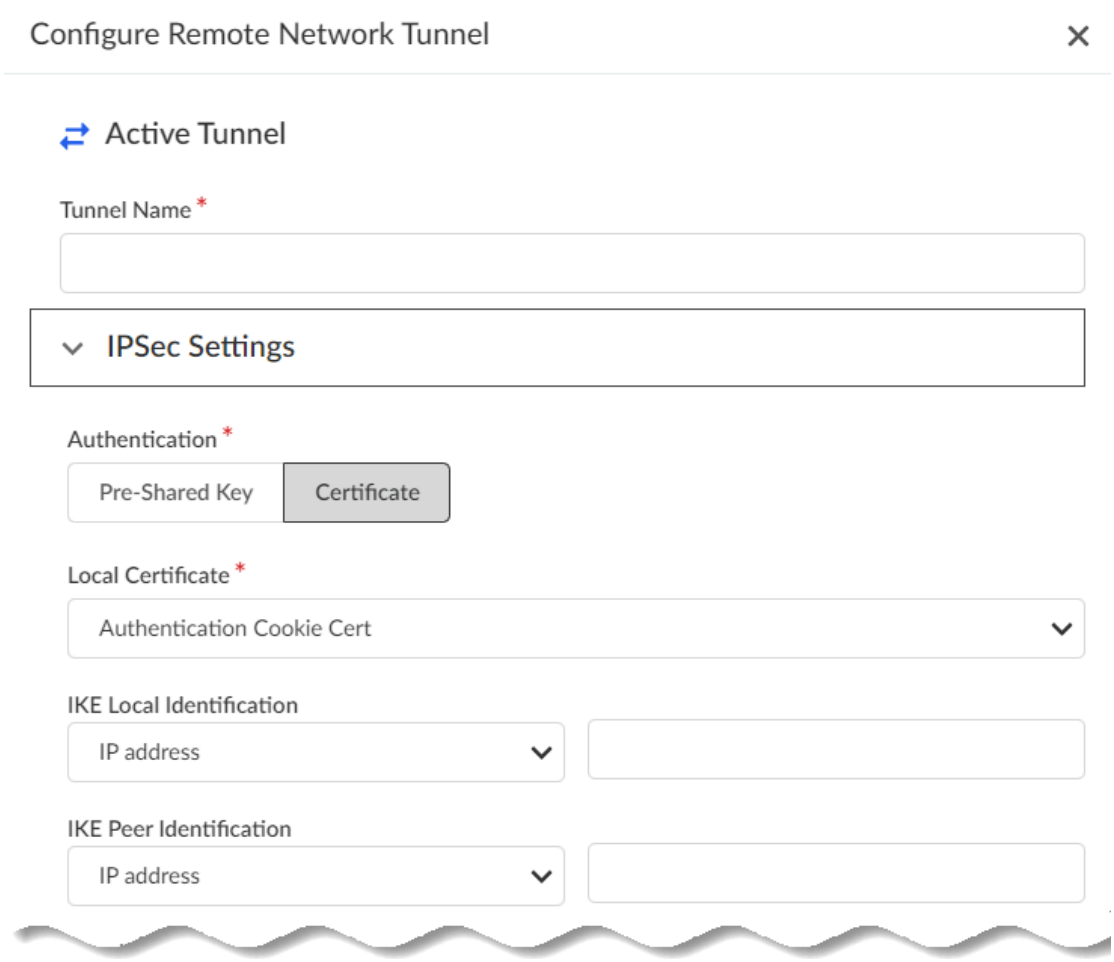
- Dale al túnel activo un **Tunnel Name (Nombre de túnel)**único.
- Especifique la **IPSec Settings (Configuración de IPSec)**.
  - Especifique un tipo de **Authentication (Autenticación)** [ya sea una **Pre-Shared Key (Clave precompartida)** o un **Certificate (Certificado)**].

    Si especifica una **Pre-Shared Key (Clave precompartida)**, introduzca y confirme la **Pre-Shared Key (Clave precompartida)**.

    Si especifica un **Certificate (Certificado)**, introduzca el **Local Certificate (Certificado local)** a utilizar. Este certificado ya debe existir en Strata Cloud Manager.
  - Especifique la **IKE Local Identification (Identificación local de IKE)** [ya sea **IP Address (Dirección IP)**, **Distinguished Name (Subject) [Nombre distintivo (asunto)]**, **User FQDN (email address) [FQDN de usuario (dirección de correo electrónico)]** o **FQDN (hostname) [FQDN (nombre de host)]** .
  - Especifique la **IKE Local Identification (Identificación local de IKE)** (ya sea **IP Address (Dirección IP)**, **Distinguished Name (Subject) [Nombre distintivo (asunto)]**,

 ©2025 Palo Alto Networks, Inc.

User FQDN (email address) [FQDN de usuario (dirección de correo electrónico)] o **FQDN (hostname) [FQDN (nombre de host)]**

- 

- Seleccione el tipo de Comprobación de ID de peer:
  - **Exact (Exacta)**: garantiza que el ajuste local y la carga de trabajo de la ID IKE del peer coincidan a la perfección.
  - **Wildcard (Carácter comodín)**: permite que la identificación de peer coincida siempre que coincidan todos caracteres antes del comodín (*). No es necesario que los caracteres que aparecen después del comodín coincidan.
- (Opcional) Seleccione **Permit peer identification and certificate payload identification mismatch (Permitir identificación de peer y falta de coincidencia de identificación de carga de certificado)** para permitir una asociación de seguridad (SA) IKE correcta

 ©2025 Palo Alto Networks, Inc.

incluso aunque la identificación del peer no coincida con la identificación del peer en el certificado.

- En **Certificate Profile (Perfil de certificados)** seleccione un perfil. Un perfil del certificado contiene información sobre el modo de autenticar la puerta de enlace del peer.
- (Opcional) Seleccione **Enable strict validation of peer's extended key use (Habilitar validación estricta de uso de clave extendida de peer)** para controlar de forma estricta cómo se puede utilizar la clave.
- Seleccione la **Branch Device IP Address (Dirección IP del dispositivo de sucursal)** [**Static (Estática)** o **Dynamic (Dinámica)**].
  - Si selecciona **Static (Estático)**, introduzca la **Static IP Address (Dirección IP estática)** que se utilizará para el túnel IPSec.
  - Especifique **Dynamic (Dinámico)** para obtener la dirección IP automáticamente.
- (Opcional, recomendado) Habilite el **IKE Passive Mode (Modo pasivo IKE)** para que Prisma Access responda a conexiones IKE pero no las inicie.

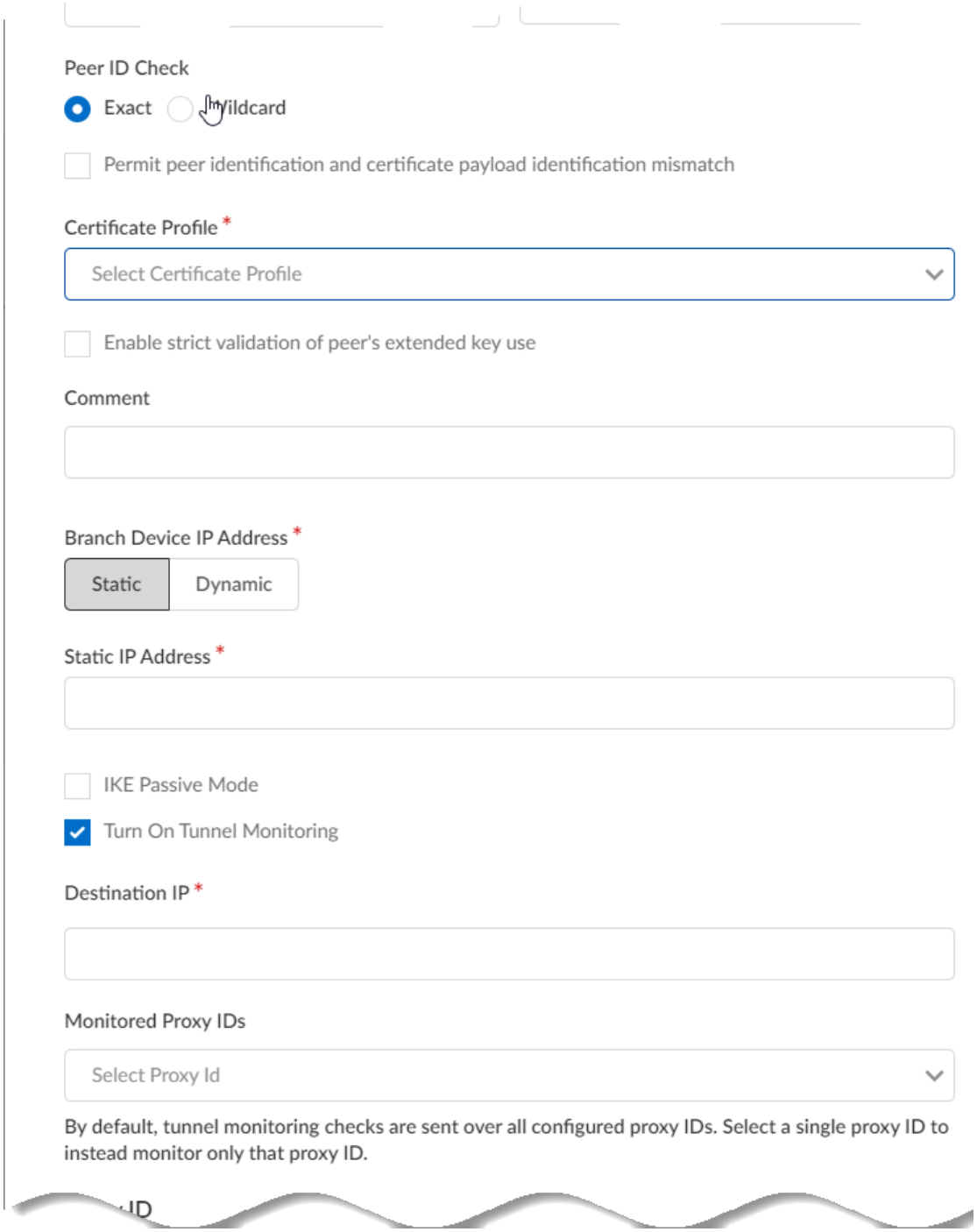
  Si bien no es obligatorio, el **IKE Passive Mode (Modo pasivo IKE)** es la configuración recomendada.
- (Opcional) **Turn on Tunnel Monitoring (Activar la supervisión de túneles)**.

  Introduzca una **Destination IP (IP de destino)** de la supervisión de túnel en la red remota para Prisma Access para determinar si el túnel está activo y, si su dispositivo

 ©2025 Palo Alto Networks, Inc.

IPSec usa VPN basada en políticas, introduzca el **Proxy ID (ID de proxy)** asociado como la **Monitored Proxy ID (ID de proxy supervisada)**.

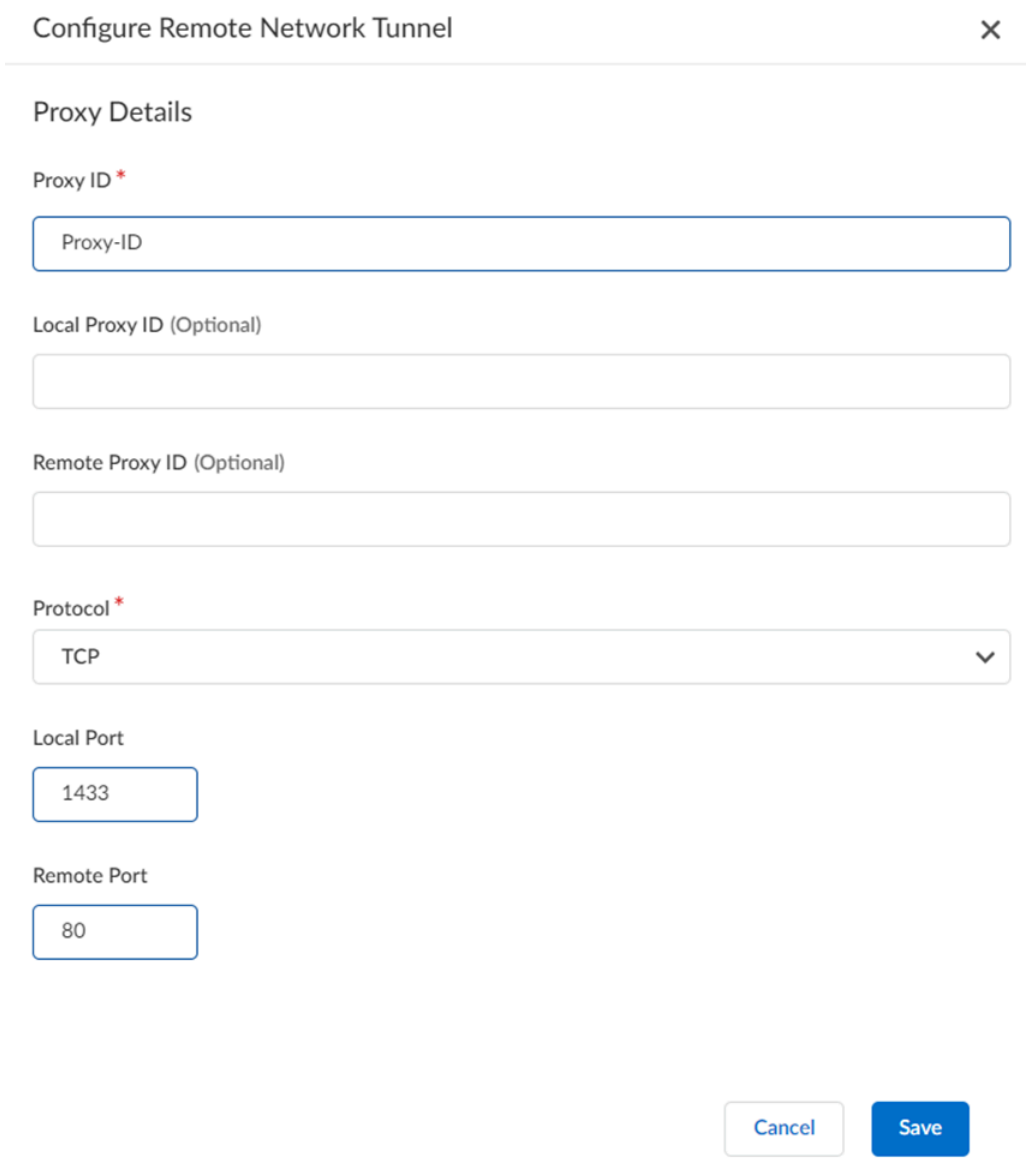
.

- 

- (Opcional) Si necesita un ID de proxy:
  - **Add Proxy ID (Añadir ID de proxy)** e introduzca el **Proxy ID (ID de proxy)**.
  - Opcionalmente, introduzca el **Local Proxy ID (ID del proxy local)** y el **Remote Proxy ID (ID del proxy remoto)**.

 ©2025 Palo Alto Networks, Inc.

- Introduzca el **Protocol (Protocolo)** que se utilizará para el ID del proxy. Introduzca un **Number (Número)**, **TCP**o **UDP**.
- Especifique un **Local Port (Puerto local)** y un **Remote Port (Puerto remoto)** para TCP o UDP, o especifique
- **Save (Guardar)** para guardar sus cambios.



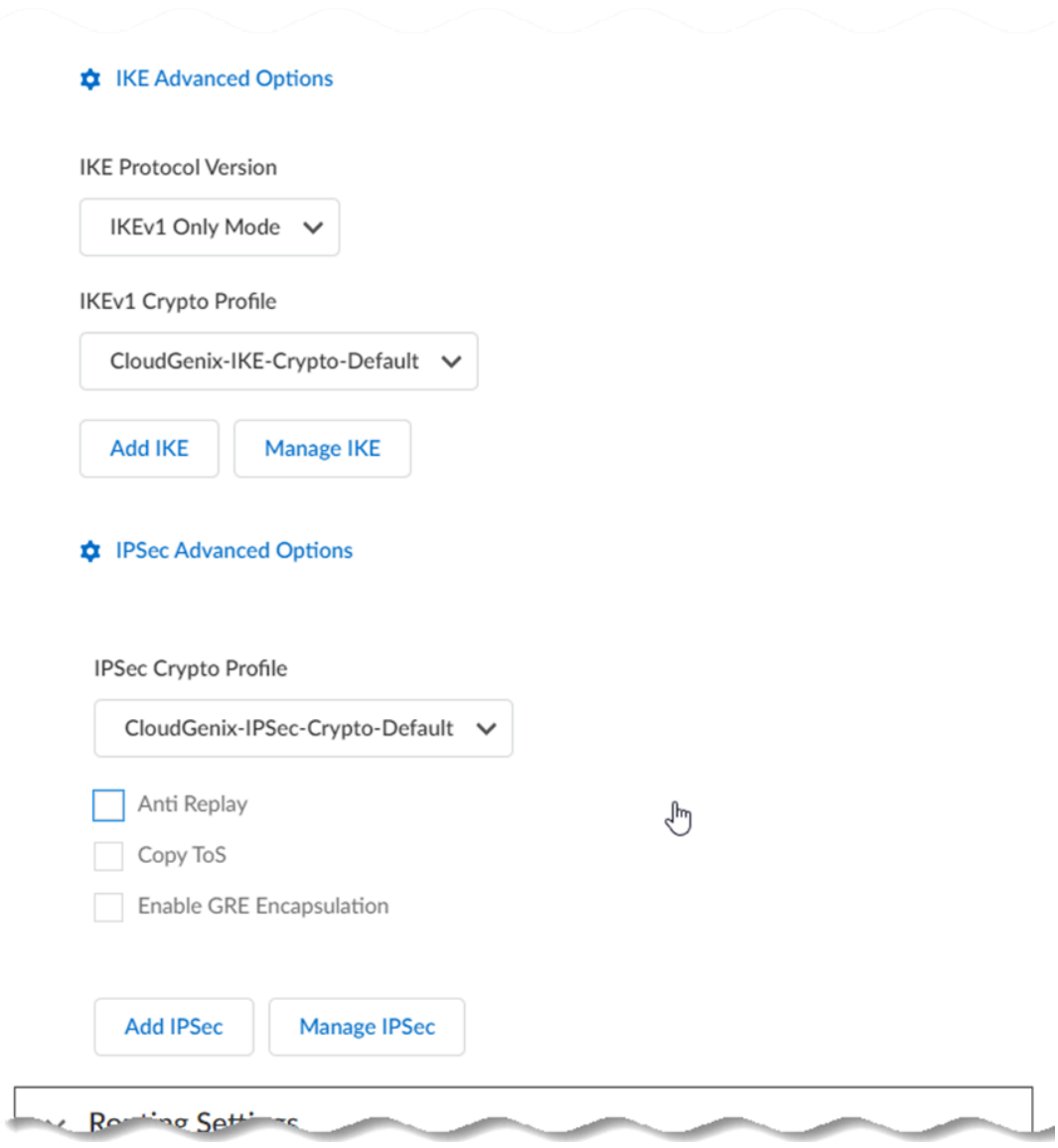
- Especifique **IKE Advanced Options (Opciones avanzadas de IKE)**.
  - Seleccione una **IKE Protocol Version (Versión del protocolo IKE)**.
  - Seleccione un **IKEv1 Crypto Profile (Perfil de cifrado IKEv1)**.

    Para añadir un perfil criptográfico, seleccione **Add IKE (Añadir IKE)**. Para gestionar un perfil IKE existente, seleccione **Manage IKE (Gestionar IKE)** y seleccione el perfil que desea editar.
  - Seleccione un **IKEv2 Crypto Profile (Perfil de cifrado IKEv2)**.

 ©2025 Palo Alto Networks, Inc.

Para añadir un perfil criptográfico, seleccione **Add IKE (Añadir IKE)**. Para gestionar un perfil IKE existente, seleccione **Manage IKE (Gestionar IKE)** y seleccione el perfil que desea editar.

- Especifique las **IPSec Advanced Options (Opciones avanzadas de IPSec)**.
  - Seleccione un **IPSec Crypto Profile (Perfil de cifrado IPSec)**.

    Para añadir un perfil criptográfico, seleccione **Add IPSec (Añadir IPSec)**. Para administrar un perfil IPSec existente, seleccione **Manage IPSec (Gestionar IPSec)** y seleccione el perfil que desea editar.
- 

- Elija su **Routing Settings (Configuración de enrutamiento)**.
  - Seleccione el **Routing Type (Tipo de enrutamiento)** [**Static (Estático)** o **Dynamic (Dinámico)**].

    Si selecciona **Static (Estático)**, debe **Add (Añadir)** las subredes IP o las direcciones IP que desea proteger en el sitio.

 ©2025 Palo Alto Networks, Inc.

Si selecciona **Dynamic (Dinámico)**:

- Introduzca el **Peer AS (AS del peer)**, el sistema autónomo (AS) para su red.

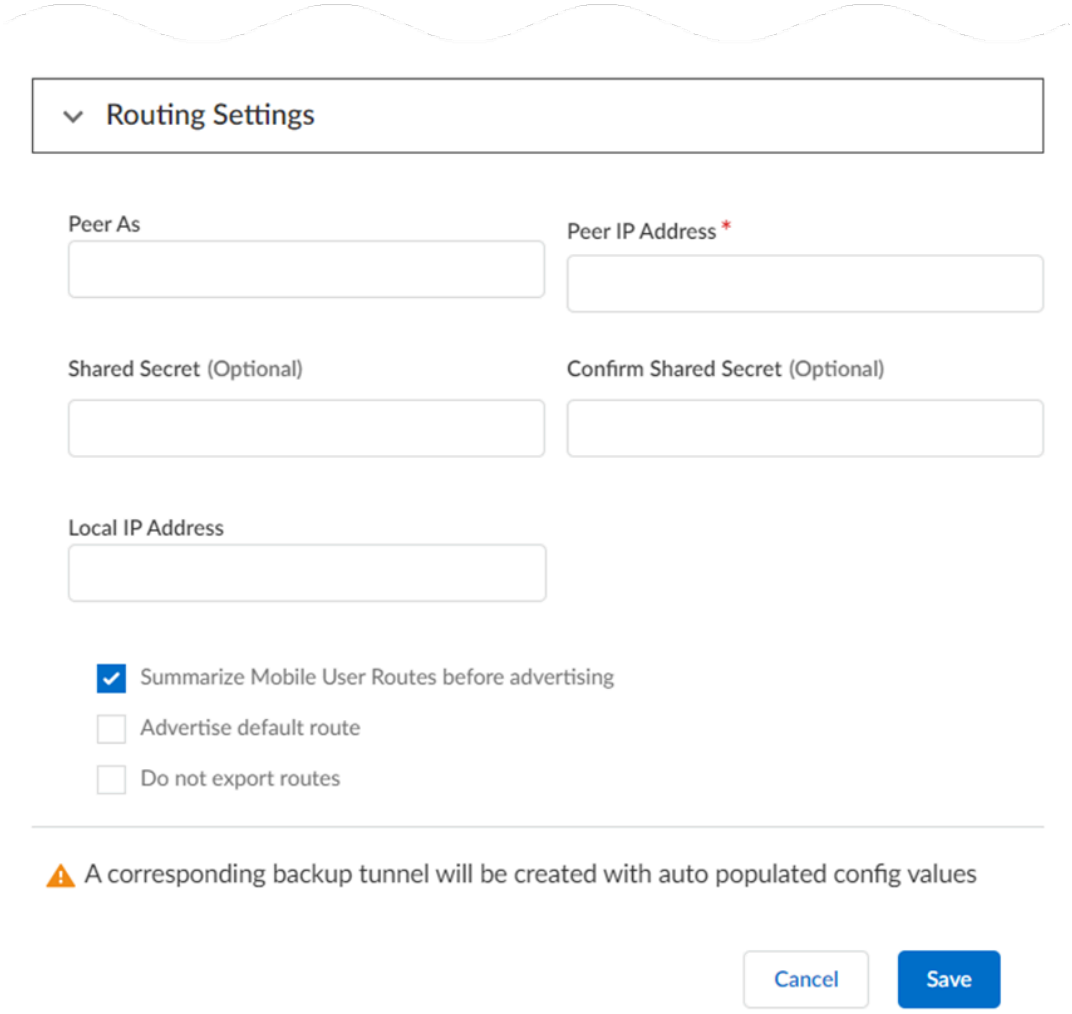
  Utilice un número AS privado de BGP que cumpla con RFC 6996.
- Introduzca la **Peer IP Address (Dirección IP del peer)** asignada como ID del enrutador eBGP en la red de la sede central o del centro de datos.
- (Opcional) Introduzca una contraseña del **Shared Secret (Secreto compartido)** para autenticar las comunicaciones entre pares BGP.
- Introduzca la **Local IP Address (Dirección IP local)** que Prisma Access utiliza como su dirección IP local para BGP.
- (Opcional) Seleccione **Summarize Mobile User Routes before advertising (Resumir las rutas de los usuarios móviles antes de anunciarse)** para reducir la cantidad de anuncios de subredes IP de usuarios móviles a través de BGP a su equipo local del cliente (CPE) al tener Prisma Access resumir las subredes antes de anunciarlas.
- (Opcional) Seleccione **Advertise Default Route (Anunciar ruta predeterminada)** para que Prisma Access genere un anuncio de ruta predeterminado para la red remota utilizando eBGP. Asegúrese de que su red no tenga otra

 ©2025 Palo Alto Networks, Inc.

ruta predeterminada anunciada por BGP, o podría introducir problemas de enrutamiento en su red.

- (Opcional) Seleccione **Do Not Export Routes (No exportar rutas)** para evitar que Prisma Access reenvíe rutas a la sede central o al centro de datos.

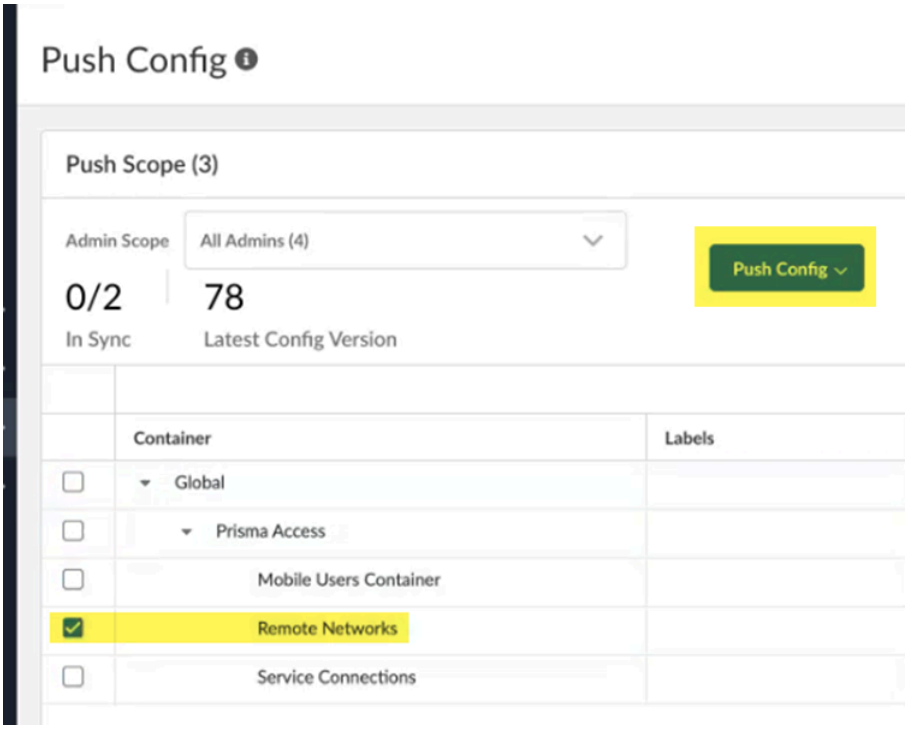
4. **Save (Guardar)** los cambios en el túnel IPSec.



STEP 13 | **Save & Exit (Guardar y salir).**

 ©2025 Palo Alto Networks, Inc.

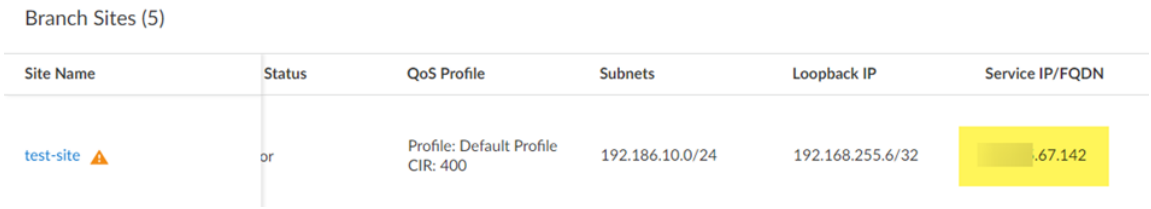
STEP 14 | **Push Configuration (Enviar configuración)** para guardar los cambios de configuración, asegurándose de seleccionar **Remote Networks (Redes remotas)** en el **Push Scope (Ámbito de envío)**.



STEP 15 | Encuentre la dirección **Service IP (IP del servicio)** que especifique en su CPE.

Cuando configura la red remota, utilice la dirección IP del servicio como la dirección IP del par en su CPE para finalizar el túnel IPSec.

1. Vaya a **Workflows (Flujos de trabajo)** > **Prisma SASE Setup (Configuración SASE de Prisma)** > **Branch Site Management (Gestión de la sucursal)** > **Extended CPE Site (Sitio CPE extendido)**.
2. Busque la dirección **IP/FQDN del servicio** .



Panorama

Los pasos para configurar una Red remota: Alto rendimiento son los mismos que para incorporar una Red remota estándar en Prisma Access (Managed by Panorama), incluida la elección de un **IPSec Termination Node (Nodo de terminación IPSec)** durante la incorporación.

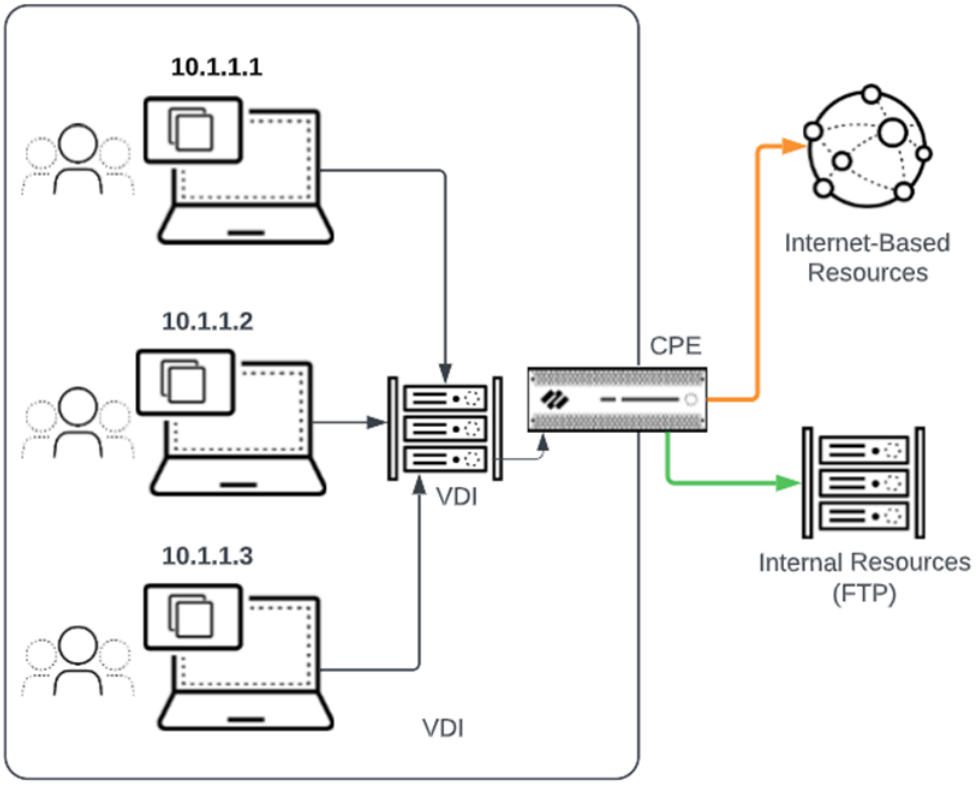
 ©2025 Palo Alto Networks, Inc.

Integre una VDI de escritorio compartido con Prisma Access usando Terminal Server

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

La infraestructura de escritorio virtual (VDI) es una tecnología que utiliza máquinas virtuales para aprovisionar y gestionar escritorios virtuales. VDI implementa entornos de escritorio mediante un servidor gestionado y los implementa a los usuarios finales que lo soliciten. Los usuarios finales acceden a los recursos que necesitan, como las aplicaciones públicas y los recursos basados en Internet o privados, y los recursos disponibles desde una conexión FTP, desde sus escritorios VDI aprovisionados.

Una topología VDI se puede implementar mediante escritorios compartidos o dedicados. Si los escritorios son compartidos, varios usuarios están detrás de una sola dirección IP y los puertos se utilizan para diferenciar a los usuarios.



Si la implementación de VDI utiliza una implementación de escritorio compartido, Prisma Access ofrece una solución que permite a los usuarios finales acceder de forma segura a los recursos de Internet y FTP con un solo inicio de sesión, al tiempo que protege a los usuarios de VDI de su

 ©2025 Palo Alto Networks, Inc.

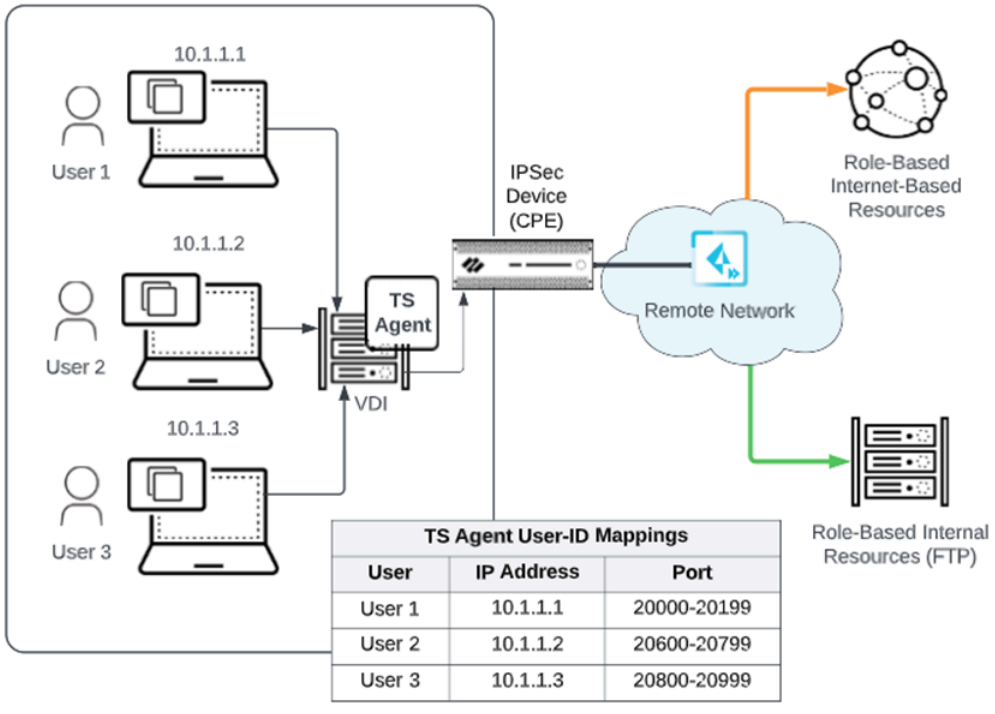
organización y a los recursos internos y externos. Esta solución utiliza el agente TS de Palo Alto Networks que usted instala en los servidores VDI.

El Agente TS es un software de User-ID instalado para resolver el desafío asociado con la identificación de asignaciones de nombre de usuario a dirección IP cuando los usuarios comparten direcciones IP. Una vez instalado el agente TS, se supervisan todos los usuarios que han iniciado sesión y se asigna a los usuarios individuales un conjunto específico de puertos. Cuando Prisma Access recibe este tráfico de red VDI de la VDI, identifica al usuario en función del puerto de origen del usuario. Esta implementación le proporciona una solución basada en la nube que permite a los administradores crear reglas de política de seguridad para que los usuarios finales de VDI controlen su acceso a Internet y a los sitios internos.

Si su red tiene una ruta predeterminada, puede incorporar una o más redes remotas e implementar el agente TS para proteger de manera fácil y sencilla a los usuarios y recursos de su organización.

En esta implementación:

- Especifique un intervalo de puertos en el agente TS para identificar usuarios específicos en servidores de terminales basados en Windows. El agente TS notifica a Prisma Access los rangos de puertos asignados, de modo que Prisma Access pueda aplicar la política basada en usuarios y grupos de usuarios.
- La red remota aplica la seguridad y el control de acceso para FTP y recursos basados en Internet.



TS Agent User-ID Mappings		
User	**IP Address**	**Port**
User 1	10.1.1.1	20000-20199
User 2	10.1.1.2	20600-20799
User 3	10.1.1.3	20800-20999

No puede redistribuir la información de asignación de usuarios recopilada de un agente TS.

Para integrar una VDI mediante el Agente TS y una red remota de Prisma Access en Cloud Managed Prisma Access, complete los siguientes pasos.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Instalar y configurar el Agente TS de Palo Alto Networks en los servidores VDI.

Para asignar a todos sus usuarios, debe instalar el agente de TS en todos los servidores de terminal en los que sus usuarios inicien sesión.

1. En los servidores VDI de Windows, Instale y configure el agente Terminal Server (TS) de Palo Alto Networks.
2. Defina el rango de puertos que el agente TS asigna a los usuarios finales.

   Verifique el recuento de escala compatible para el agente TS desde la Matriz de compatibilidad.
3. (Opcional) Si hay varios servidores VDI, configure un agente TS en cada uno de ellos.

STEP 2 | Incorpore una red remota y conéctela al sitio de la sucursal de VDI en Cloud Managed Prisma Access (si aún no lo has hecho).

STEP 3 | Configure las opciones en el dispositivo IPSec (CPE) de la sucursal para permitir que la red remota se comunique con la VDI.

- Configure los parámetros criptográficos IPSec e IKE para el túnel IPSec que coincidan con los parámetros configurados en Prisma Access.
- Utilice la dirección de **Service IP (IP de servicio)** [**Manage (Gestionar)** > **Remote Networks (Redes remotas)** > **Service IP (IP de servicio)**] como el lado de Prisma Access del túnel IPSec para la red remota.
- Configure una ruta en el dispositivo IPSec para permitir el tráfico VDI al túnel de red remota.
- Configure una ruta en el dispositivo IPSec para permitir el tráfico de red remoto al agente TS a través del túnel.
- Si es necesario, configure una política de seguridad en el dispositivo IPSec para permitir que el tráfico pase por el túnel.

STEP 4 | Configure el Agente TS para permitir la asignación de usuarios en la red remota.

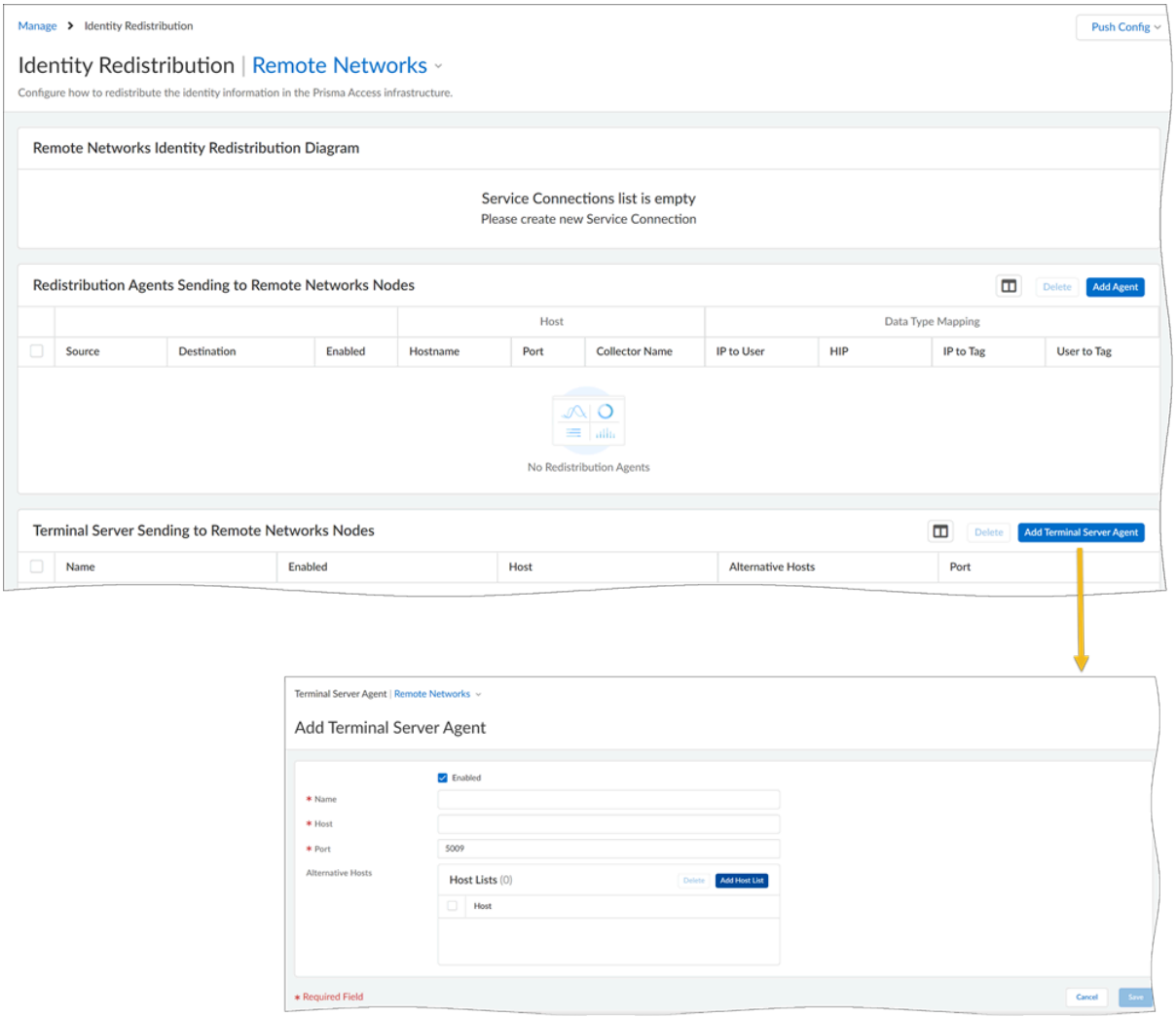
Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Identity Redistribution (Redistribución de identidades)**, establezca el **Configuration Scope (Ámbito de la configuración)** para **Remote Networks (Redes remotas)** y **Add Terminal Server Agent (Añadir agente de Terminal Server)**.

- Confirme que el agente esté **Enabled (Habilitado)**.
- Introduzca un **Name (Nombre)** para el Agente TS.
- Introduzca la dirección IP del **Host** de Windows en el que está instalado el agente TS.
- Introduzca el número de **Port (Puerto)** en el que el agente escucha solicitudes de asignación de usuarios.

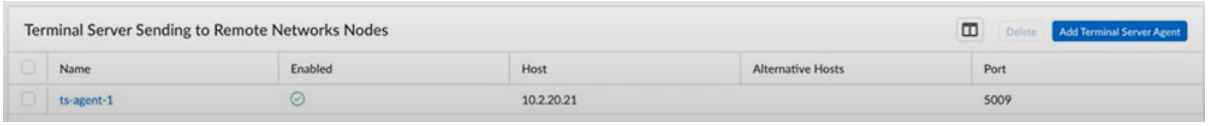
  El puerto está establecido en 5009 de forma predeterminada.

 ©2025 Palo Alto Networks, Inc.

- Haga clic en **Save (Guardar)** para guardar sus cambios.



En el ejemplo siguiente se tiene un agente configurado con la dirección de host 10.2.20.21 y un puerto 5009.

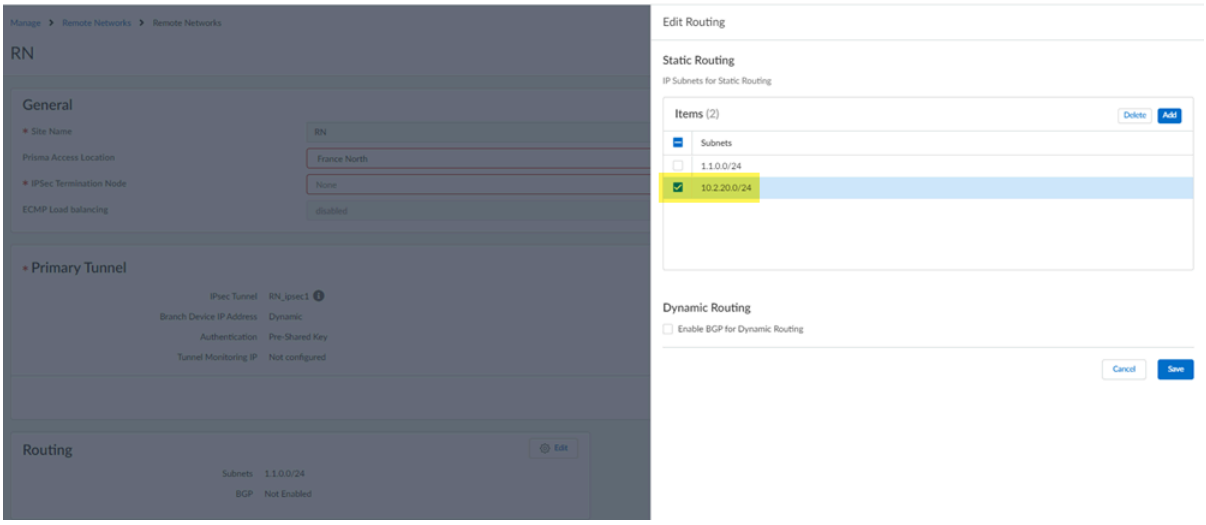


 ©2025 Palo Alto Networks, Inc.

STEP 5 | Permitir el enrutamiento entre la VDI y la red remota de Prisma Access.

1. Vaya a **Manage (Gestionar)** > **Service Setup (Configuración del servicio)** > **Remote Networks (Redes remotas)** > ***remote-network-name*** > **Routing (Enrutamiento)** y **Add (Añadir)** una ruta a la subred VDI.

   La adición de esta subred permite que el agente TS se comunique con la red remota. En la siguiente captura de pantalla de ejemplo, la subred de VDI es 10.2.20.0/24.



2. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)**, establezca el ámbito en **Remote Networks (Redes remotas)** y añada una regla de política de seguridad (**Add Rule [Añadir regla]**) para permitir el tráfico entre la subred VDI y la red remota.

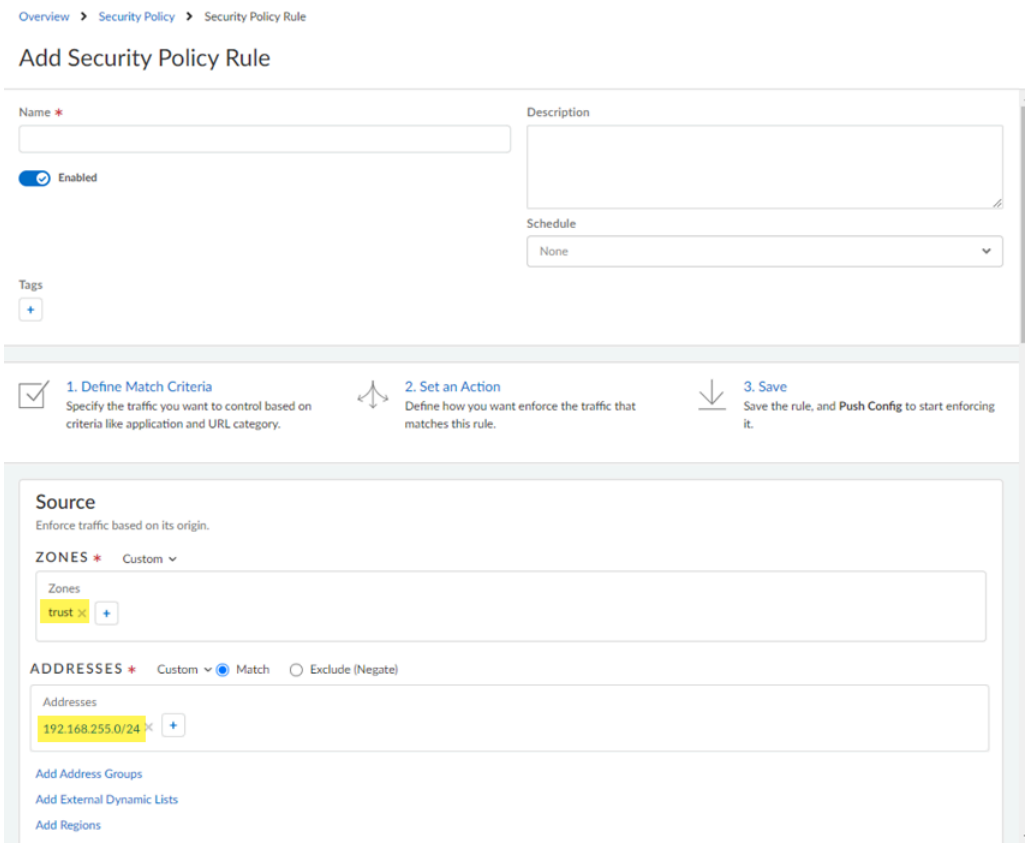
   A los usuarios de redes remotas que se conectan a Prisma Access desde la VDI se les asigna una dirección IP desde la Subred de infraestructura de Prisma Access y debe permitir el enrutamiento entre la subred de infraestructura y la subred de VDI.

   - Asegúrese de que la regla esté **Enabled (Habilitado)**.
   - **Source (Origen)**: establezca los siguientes parámetros:
     - **Zones (Zonas)**: Establézcalo en **Trust (Confianza)**.
     - **Addresses (Direcciones)**: cree un objeto de dirección para la subred de infraestructura [**Manage (Gestionar)** > **Shared (Compartido)** > **Infrastructure**

 ©2025 Palo Alto Networks, Inc.

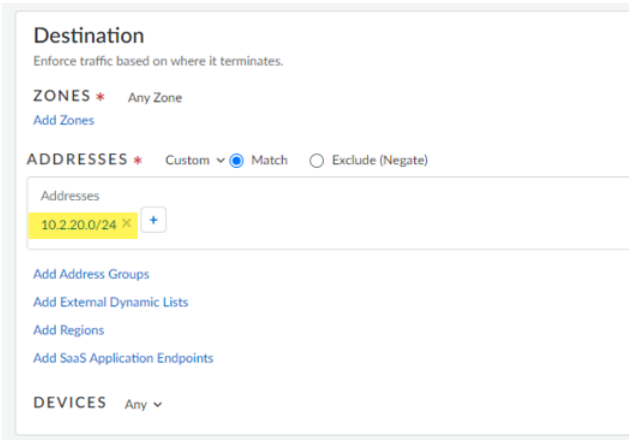
Settings (Configuración de la infraestructura) > **Infrastructure Subnet (Subred de infraestructura)**] y añada el objeto de dirección aquí.

Es preferible un objeto de dirección en lugar de entrar en la subred de infraestructura real, ya que si la subred cambia, puede cambiar el objeto de dirección y el cambio se aplica a todas las configuraciones en las que se utiliza el objeto de dirección.



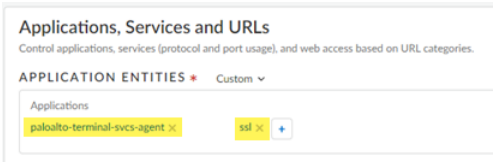
- **Destination (Destino)**: añada el host VDI que ejecuta el agente TS a las **Addresses (Direcciones)**.

  Si ha configurado el agente TS en varios hosts VDI, agréguelos todos aquí.



 ©2025 Palo Alto Networks, Inc.

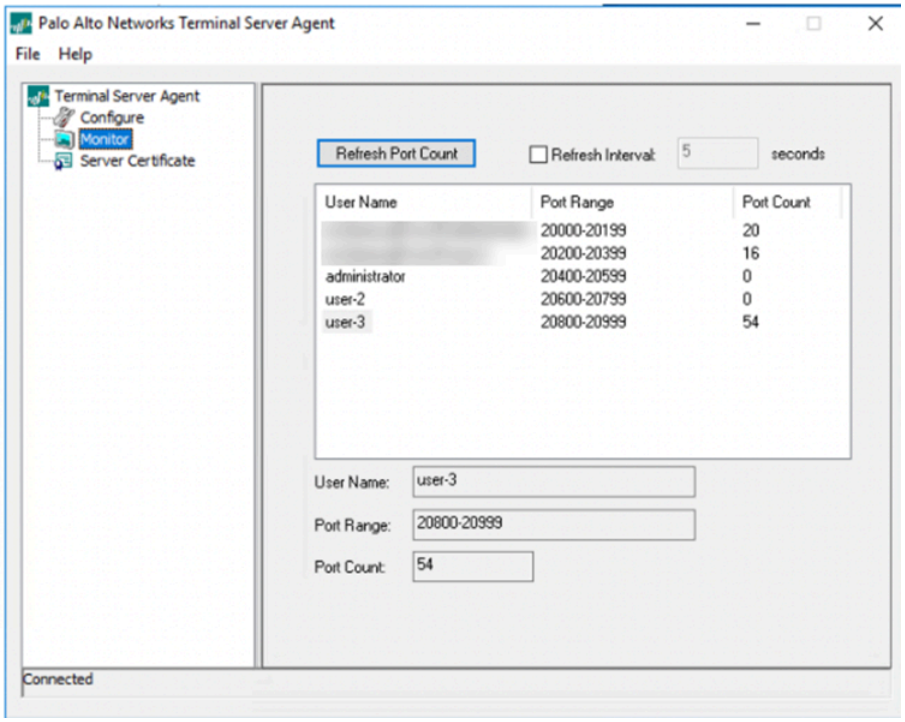
- **Applications, Services and URLs (Aplicaciones, servicios y URL)**: añada **paloalto-terminal-svcs-agent** a las **Application Entities (Entidades de aplicación)**.



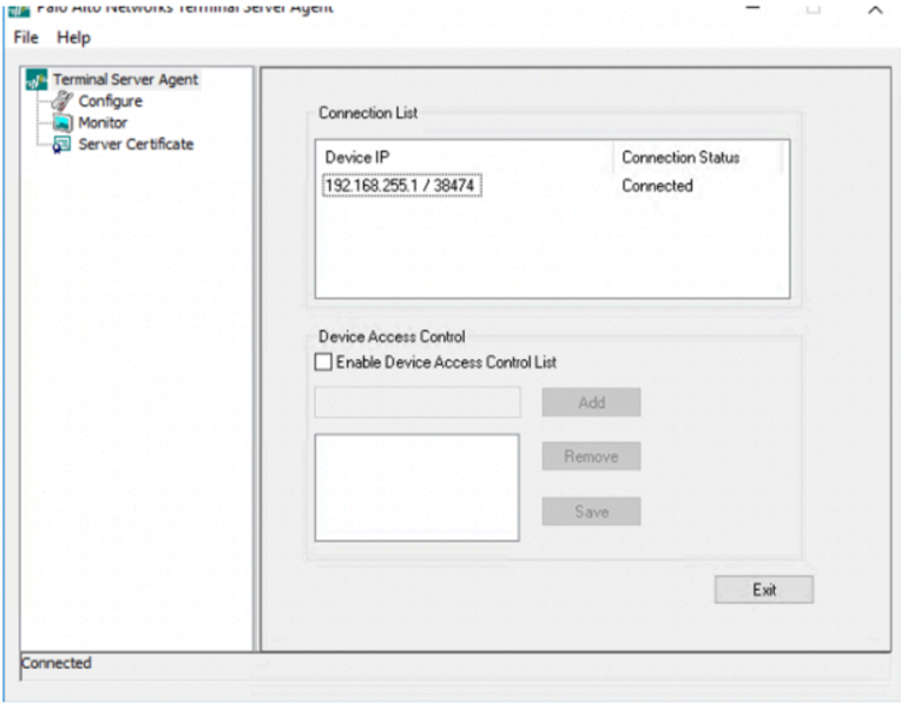
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Compruebe que la implementación funciona correctamente.

1. En el agente TS, deberá **Monitor (Supervisar)** el estado del agente y verificar que el agente TS refleje la asignación correcta del nombre de usuario al puerto.

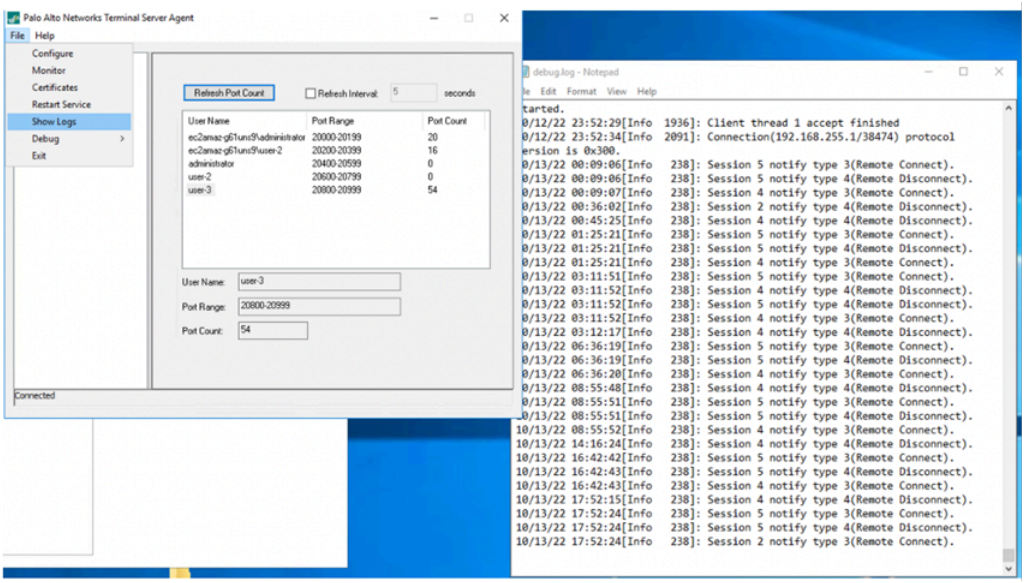


2. Verifique que la dirección IP de la red remota esté conectada al agente TS.

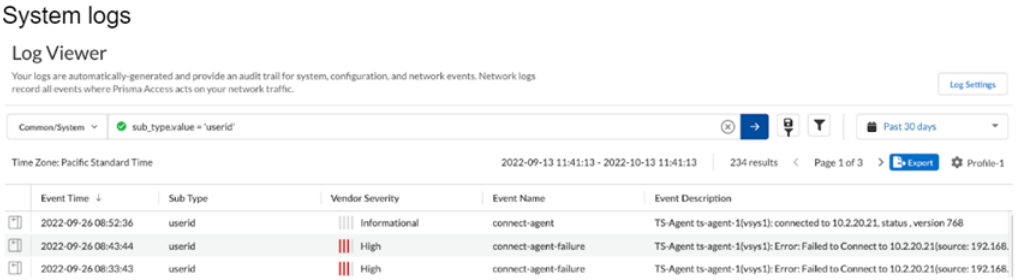


3. Vaya a **File (Archivo)** > **Show Logs (Mostrar logs)** y vea los mensajes de log para el agente TS.

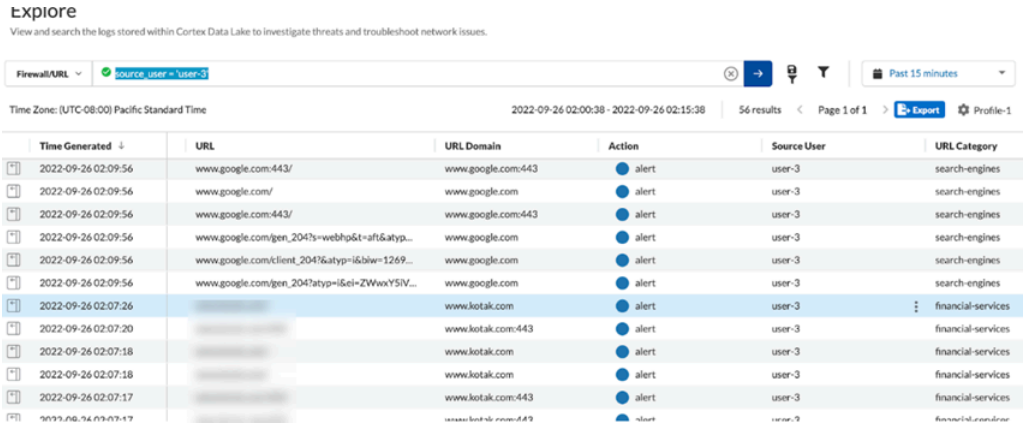
 ©2025 Palo Alto Networks, Inc.



4. En Prisma Access (Managed by Strata Cloud Manager), vaya a **Activity (Actividad)** > **Log Viewer (Visor de logs)** > **Common/System (Común/sistema)** y verifique que las redes remotas puedan conectarse al agente TS.



5. Vaya a **Activity (Actividad)** > **Log Viewer (Visor de logs)** > **Firewall/URL (Cortafuegos/URL)** y verifique que las redes remotas sean capaces de aplicar políticas basadas en identidad.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Supervisión y visibilidad de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Se requiere la licencia de ADEM Observability para acceder a Autonomous DEM.

Prisma Access proporciona las siguientes funciones para obtener información sobre su actividad de seguridad y supervisar su implementación. Estas características proporcionan visibilidad del tráfico de la red y de los usuarios a través de logs, notificaciones de alerta en redes remotas, conexiones de servicio, usuarios móviles y entidades con licencia, y paneles interactivos para brindar una vista integral de los datos sobre las aplicaciones, las amenazas, los usuarios y las suscripciones de seguridad que funcionan en su red. También puede supervisar Prisma Access en el Strata Cloud Manager.

- Logs de Prisma Access

  Sus logs se generan automáticamente y proporcionan una pista de auditoría para el sistema, la configuración y los eventos de red. Los logs de red registran todos los eventos en los que Prisma Access actúa sobre el tráfico de red. Por ejemplo, las entradas se registran cuando Prisma Access bloquea el tráfico según una regla de seguridad, otorga acceso a un usuario según una regla de autenticación o da forma al tráfico según una regla de QoS. Puede ver los logs de Prisma Access en las interfaces de gestión de Strata Cloud Manager y Panorama.
- Paneles e informes de actividad de Prisma Access

  La actividad le brinda una vista integral de lo que sucede en su red, desde los datos de registro de logs hasta los hallazgos clave que puede usar para informar actualizaciones de políticas y cerrar brechas de seguridad empresarial y productividad del usuario.
- Supervisar Prisma Access en Strata Cloud Manager
- Obtenga una visibilidad integral de todo el tráfico de su red y de los productos y suscripciones que gestiona mediante las secciones Monitor (Supervisar) y Workflows (Flujos de trabajo) de Strata Cloud Manager.
- Prisma Access y Autonomous DEM

  Autonomous DEM proporciona visibilidad y conocimientos nativos de extremo a extremo para todo el tráfico de usuarios en su Secure Access Service Edge (Strata Cloud Manager). La funcionalidad de Autonomous DEM está integrada de forma nativa en la aplicación GlobalProtect y Prisma Access, y por lo tanto no requiere que implemente ningún dispositivo o agente adicional. Puede aislar rápidamente la fuente de los problemas de experiencia digital y simplificar su solución.

- Centro de control de Strata Cloud Manager

  El Centro de control es un resumen visual interactivo de los dispositivos IoT, los usuarios, los hosts y el tráfico en su red. Al utilizar los datos de sus suscripciones de seguridad entregadas en la nube y ADEM, el Centro de control muestra información importante sobre las amenazas, la experiencia del usuario y la seguridad de los datos en su red.

  El Centro de control le permite interactuar con los datos y visualizar las relaciones entre eventos en la red para que pueda detectar anomalías o averiguar formas de mejorar su seguridad de red.

 ©2025 Palo Alto Networks, Inc.

Logs de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Un log es un archivo con marca de tiempo generado automáticamente que proporciona un código de seguimiento para los eventos del sistema o eventos de tráfico de red que Prisma Access supervisa. Las entradas de log contienen artefactos, que son las propiedades, actividades o comportamientos asociados con el evento registrado en el log, tales como el tipo de aplicación o la dirección IP de un atacante. Cada tipo de log registra información para un tipo de evento separado. Por ejemplo, Prisma Access puede generar un log de amenazas para registrar el tráfico que coincida con una firma de spyware, vulnerabilidad o virus. Prisma Access (Managed by Strata Cloud Manager) proporciona logs de red (como tráfico, amenazas, URL, archivos, coincidencias HIP), logs de endpoints y logs comunes (sistema y configuración). Puede ver los detalles de cada entrada de log y, en el caso de los logs de amenazas, puede revisar los detalles de las amenazas y ver si hay anulaciones de amenazas vigentes.

- Strata Cloud Manager
- Panorama

Logs de Prisma Access (Strata Cloud Manager)

Si estás usando **Strata Cloud Manager**, vaya a **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.

Prisma Access (Managed by Strata Cloud Manager) proporciona logs de red (tráfico, amenaza, URL, archivo, coincidencia HIP) y logs comunes (sistema y configuración).

Puede ver los detalles de cada entrada de log, y para los logs de amenazas, puede revisar los detalles de la amenaza y ver si hay alguna anulación de amenaza en vigor. Más información

Logs de Prisma Access (Panorama)

También puede ver los logs de Prisma Access en la interfaz de Prisma Access (Managed by Panorama). La infraestructura de Prisma Access reenvía todos los logs a Strata Logging Service. Prisma Access recupera los resultados del log de Strata Logging Service utilizando el complemento de servicios en la nube y proporciona una vista añadida de su red remota y los logs de tráfico de usuarios móviles. Independientemente de la interfaz de gestión que esté utilizando, Prisma Access—Panorama o Strata Cloud Manager—puede ver sus logs en Prisma Access (Managed by Strata Cloud Manager) en **Activity (Actividad)** > **Logs** > **Log Viewer (Visor de logs)**.

Además de los logs de Infraestructura de servicios en la nube de Prisma Access, también puede ver los logs directamente desde el dispositivo de Panorama que gestiona Prisma Access. Para ver los logs, vaya a **Monitor (Supervisar) > Logs (Logs)**. Más información

 ©2025 Palo Alto Networks, Inc.

Logs externos y otros datos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Es posible que ya esté acostumbrado a ver e interactuar con los logs de Prisma Access que se almacenan en el Strata Logging Service de **Activity Logs** > **Logs de actividad**. Pero, ¿sabía que Prisma Access también admite la ingestión de logs y otros datos de una variedad de fuentes externas y de terceros cuando tiene un modelo de licencia Cortex XDR Pro per TB License Data Lake? Una vez que esté configurado, puede usar la aplicación de Strata Logging Service en el hub para ver los logs y configurar el reenvío de logs. Los proveedores compatibles incluyen:

• Activación del recopilador de eventos de Windows	• Corelight Zeek	• PAN IoT Security
• Amazon S3	• ElasticSearch Filebeat	• PingFederate
• Apache Kafka	• Forcepoint DLP	• PingOne para empresas
• AWS	• Fortinet Fortigate	• Prisma Cloud
• AWS CloudTrail y Amazon CloudWatch	• Google Cloud Platform	• Prisma Cloud Compute
• Azure Event Hub	• Google Kubernetes Engine	• Proofpoint Targeted Attack Protection
• Azure Network Watcher	• Google Workspace	• ServiceNow CMDB
• BeyondTrust Privilege Management Cloud	• Microsoft Azure	• DHCP de Windows mediante Elasticsearch Filebeat
• Check Point FW1/VPN1	• Microsoft Office 365	• Jornada laboral
• Cisco ASA	• Okta	• Cortafuegos Zscaler Cloud

Puede usar los logs ingeridos de fuentes de terceros como única fuente de datos o, puede usar esos logs junto con los logs de Prisma Access de Palo Alto Networks y fuentes de datos adicionales.

Con Palo Alto Networks, reduzca su carga operativa y simplifique radicalmente sus operaciones de SOC recopilando, integrando y normalizando datos de todas las fuentes de datos: red, endpoint y nube. Obtenga una visión unificada y perspectivas prácticas para el uso de aplicaciones, patrones de tráfico, amenazas e incidentes en toda su empresa.

©2025 Palo Alto Networks, Inc.

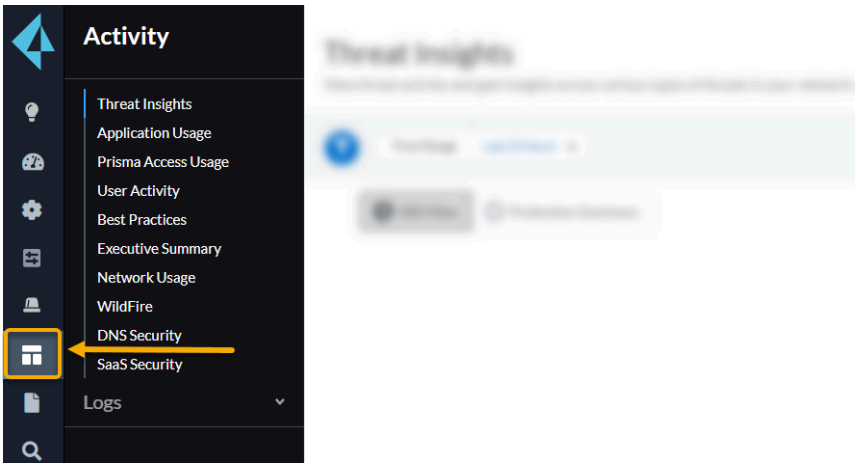
Paneles e informes de actividad de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	❑ Licencia de Prisma Access ❑ Revise las licencias y otros requisitos para los paneles y los informes de actividad

La actividad identifica hallazgos clave que puede utilizar para informar sus actualizaciones de políticas y cerrar brechas de seguridad empresarial y productividad del usuario. La actividad le proporciona:

- Paneles interactivos donde puede explorar datos de las aplicaciones, amenazas, usuarios y suscripciones de seguridad que funcionan en su red.
- Informes que puede compartir sin conexión y programar para actualizaciones periódicas.
- El Visor de logs proporciona una pista de auditoría para eventos del sistema, configuración y red. Puede saltar desde los paneles al Visor de logs para obtener más contexto y profundizar en los datos.
- La búsqueda de artefactos de seguridad le ayuda a buscar artefactos como un hash de archivo, una URL, un dominio o una dirección IP (IPv4 o IPv6) para interactuar con datos solo para ese artefacto. Los resultados de la búsqueda incluyen el historial del artefacto, información sobre amenazas del artefacto y hallazgos de análisis de terceros para el artefacto.

Los usuarios de Prisma Access (Managed by Strata Cloud Manager) y Panorama Managed Prisma Access pueden utilizar la **Activity (Actividad)** en la aplicación Prisma Access (Managed by Strata Cloud Manager). Para comenzar, inicie Prisma Access (Managed by Strata Cloud Manager) y haga clic en la pestaña **Activity (Actividad)** en el panel de navegación izquierdo.



Insights cuenta con respaldo como parte de la certificación Prisma SASE FedRAMP High “en curso”. La actividad cuenta con respaldo como parte de la certificación Prisma SASE FedRAMP High “en curso”.

- Comenzar con la actividad

 ©2025 Palo Alto Networks, Inc.

Ver y supervisar Prisma Access en Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Esta es una función de Prisma Access Insights.

Palo Alto Networks Centro de control de Strata Cloud Manager es una plataforma de seguridad de red impulsada por IA. Con Strata Cloud Manager y el Centro de control de Strata Cloud Manager puede gestionar fácilmente toda su infraestructura de seguridad de red de Palo Alto Networks, sus NGFW y su entorno SASE, desde una única interfaz de usuario optimizada.

Puede obtener visibilidad integral de todo el tráfico de su red y de los productos y suscripciones que gestiona utilizando Activity Insights en el Centro de control y las secciones del Centro de controlMonitor (Supervisar) y Workflows (Flujos de trabajo).

- **View and Monitor Applications (Ver y supervisar aplicaciones)**: vaya a **Activity Insights** > **Applications (Aplicaciones)** para obtener información sobre las aplicaciones que está utilizando.
- **View and Monitor App Acceleration (Ver y supervisar la aceleración de aplicaciones)**: la aceleración de aplicaciones aborda las causas del bajo rendimiento de las aplicaciones y actúa en tiempo real para mitigarlas, mejorando la experiencia del usuario para los usuarios de Prisma Access GlobalProtect y Remote Network. Vaya a **Activity Insights** > **Applications (Aplicaciones)** para ver detalles sobre todas las aplicaciones aceleradas.
- **View Mobile Users (Ver Usuarios móviles):todos los usuarios** proporciona una descripción general de todos los usuarios conectados a las soluciones de seguridad de Palo Alto Networks, que incluyen cortafuegos de nueva generación (NGFW) y Prisma Access. Puede determinar fácilmente el estado de conexión de un usuario a NGFW o Prisma Access, ya sea en una sucursal, una conexión de servicio o una ubicación remota. Vaya a **Activity Insights** > **Insights** > **Users (Usuarios)** para ver información sobre sus **Usuarios agentes**, **Usuarios de proxy sin agente**, **Usuarios de Office** y **Otros usuarios**
- Seleccione **View and Monitor Branch Sites (Ver y supervisar sucursales)**: vaya a **Monitor (Supervisar)** > **Branch Sites (Sucursales)** > **Prisma Access** para ver el estado y la conectividad de sus Redes remotas y el uso de todas sus Redes remotas implementadas en diferentes ubicaciones de Prisma Access. Verá el estado de la conectividad en tiempo real y los detalles de consumo de ancho de banda, junto con otros detalles de implementación. Los usuarios móviles, las sucursales y los comercios minoristas se conectan a redes remotas. También puede ver el estado de los túneles configurados en las redes remotas y los usuarios móviles.
- **View and Monitor Data Centers (Ver y supervisar los centros de datos)**: vaya a **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **Service Connections) (Conexiones de servicio)** para ver los datos añadidos de las conexiones de servicio, así como la información sobre las conexiones de servicio individuales.

  Vaya a **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **ZTNA Connectors** para ver el estado de un grupo de conectores ZTNA Connector y ZTNA Connectors individuales).

 ©2025 Palo Alto Networks, Inc.

- Vaya a **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **ZTNA Access Objects (Objetos de acceso de ZTNA)** para obtener visibilidad de los objetos de acceso de su ZTNA Connector.
- **View and Monitor Network Services (Ver y supervisar los servicios de red)**: vaya a **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **GlobalProtect Authentication (Autenticación de GlobalProtect)** para ver el rendimiento de los servicios de red comunes que afectan su experiencia del usuario para acceder a las aplicaciones. Los servicios de red incluyen informar el número de autenticaciones de GlobalProtect realizados correctamente o que fallaron, como una medida de la capacidad de los usuarios móviles para conectarse a Prisma Access. Vaya a **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **DNS** para ver las solicitudes y respuestas de proxy DNS reenviadas a los servidores durante el rango de tiempo que especifique.
- **View and Monitor Subscription Usage (Ver y supervisar el uso de la suscripción)**: **seleccione Monitor (Supervisar)** > **Subscription Usage (Uso de suscripciones)** para ver detalles sobre sus **Prisma Access Base Subscriptions (Suscripciones básicas a Prisma Access)**, incluido el número de licencias que ha consumido hasta el momento.
- **View and Monitor Prisma Access Locations (Ver y supervisar ubicaciones de Prisma Access)**: vaya a **Monitor (Supervisar)** > **Prisma Access Locations (Ubicaciones de Prisma Access)** para ver una descripción general del estado de todas sus ubicaciones de Prisma Access para sus redes remotas y usuarios móviles. Puede seleccionar un rango de tiempo para ver el estado de la ubicación de Prisma Access y la conectividad de Strata Logging Service durante ese tiempo, vea una tabla que enumera todas las ubicaciones de Prisma Access y seleccione una ubicación de Prisma Access individual por nombre para ver sus detalles.
- **View Prisma Access Upgrades (Ver actualizaciones de Prisma Access)**: Seleccione **Workflows (Flujos de trabajo)** > **Software Upgrades (Actualizaciones de software)** > **Prisma Access** para ver información sobre el proceso de actualización del plano de datos de Prisma Access.
- **View and Monitor Third-Party Device-IDs (Ver y supervisar los Device-ID de terceros)**: vaya a **Monitor (Supervisar)** > **Devices (Dispositivos)** > **IoT** para obtener información sobre sus dispositivos IoT, como la cantidad de dispositivos IoT conectados en los últimos 30 minutos, todos los dispositivos IoT conectados durante el rango de tiempo seleccionado y detalles sobre todos los dispositivos IoT conectados.
- **View and Monitor Remote Browser Isolation (Ver y supervisar el aislamiento remoto del navegador)**: seleccione **Monitor (Supervisar)** > **Users (Usuarios)** para obtener visibilidad de su implementación de RBI al ver métricas como el número de usuarios activos de RBI, tendencias, estado de conectividad, estado de ubicación de RBI, mediciones de tráfico y consumo de licencias.

Comience a utilizar la supervisión de acceso de Prisma en Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Este es una característica de Prisma Access Insights.

 ©2025 Palo Alto Networks, Inc.

Prisma Access Le proporciona una manera de supervisar continuamente su entorno de Prisma Access en el centro de control de Strata Cloud Manager. Los distintos paneles le brindan vistas centradas de sus diferentes implementaciones, sus alertas y la infraestructura de Prisma Access. Cuando un evento o estado requiere su atención, Prisma Access le envía notificaciones de alerta para que pueda identificar rápidamente los problemas que puede solucionar. También le proporciona la visibilidad sobre las correcciones que se ha realizado el equipo de Prisma Access. Puede filtrar los datos que desea ver seleccionando o configurando un rango de tiempo y ver la información de referencia en las páginas de Supervisión con un licencia de Autonomous DEM.

Filtro de selección de intervalo de tiempo

El filtro de selección de **Time Range (Intervalo de tiempo)** aparece en la parte superior de los paneles donde desea filtrar la información por intervalo de tiempo.

La hora está localizada, por lo que puede filtrar según la hora local de su región. Los datos se obtienen cada minuto, pero los puntos de datos que se muestran en la mayoría de los histogramas varían según el **Time Range (Intervalo de tiempo)** seleccionado.

Para su conveniencia, Prisma Access le permite elegir el **Time Range (Intervalo de tiempo)** entre algunos intervalos predefinidos o configure su propio intervalo de fecha y hora:

- **Últimos 15 minutos**

  1 punto de datos por cada 3 minutos para un total de 5 puntos de datos.
- **Última 1 hora**

  1 punto de datos por cada 3 minutos para un total de 20 puntos de datos.
- **Últimas 3 horas**

  1 punto de datos por cada 3 minutos para un total de 60 puntos de datos.
- **Últimas 24 horas**

  1 punto de datos por cada 5 minutos para un total de 288 puntos de datos.
- **Últimos 7 días**

  1 punto de datos por cada 30 minutos para un total de 336 puntos de datos.
- **Últimos 30 días**

  1 punto de datos cada 3 horas para un total de 180 puntos de datos.
- **Personalizado**

  Puede establecer un intervalo de tiempo personalizado (por ejemplo, la fecha y la hora comienzan a las 5:00 p. m. del 1 de junio y finalizan a las 4:00 p. m. del 2 de junio) además de las selecciones de **Time Range (Intervalo de tiempo)** precargadas disponibles en el filtro.

  Para establecer una hora de inicio, primero seleccione la fecha en el calendario, luego seleccione la hora en **Start (Inicio)**. Deberá **Apply (Aplicar)** la hora de inicio, luego configurar la

 ©2025 Palo Alto Networks, Inc.

hora de finalización seleccionando una fecha de finalización en el calendario y una hora en **End (Finalizar)**.

Una vez que establece un rango de tiempo personalizado, este se guarda y se aplica en todos los widgets, dentro de Insights, que usan el filtro de rango de tiempo para mostrar datos en lugar de datos en tiempo real.

Puede elegir entre las selecciones de **Time Range (Rango de tiempo)** precargadas previamente para obtener intervalos de tiempo personalizados:

- **Últimos 15 minutos**

  1 punto de datos cada 3 minutos para un total de 5 puntos de datos.
- **Última 1 hora**

  1 punto de datos cada 3 minutos para un total de 20 puntos de datos.
- **Últimas 3 horas**

  1 punto de datos cada 3 minutos para un total de 60 puntos de datos.
- **Últimas 24 horas**

  1 punto de datos cada 5 minutos para un total de 288 puntos de datos.
- **Últimas 48 horas**

  1 punto de datos cada 30 minutos para un total de 96 puntos de datos.
- **Últimos 7 días**

  1 punto de datos cada 30 minutos para un total de 336 puntos de datos.
- **Últimos 30 días**

  1 punto de datos cada 3 horas para un total de 240 puntos de datos.

Referencias en widgets

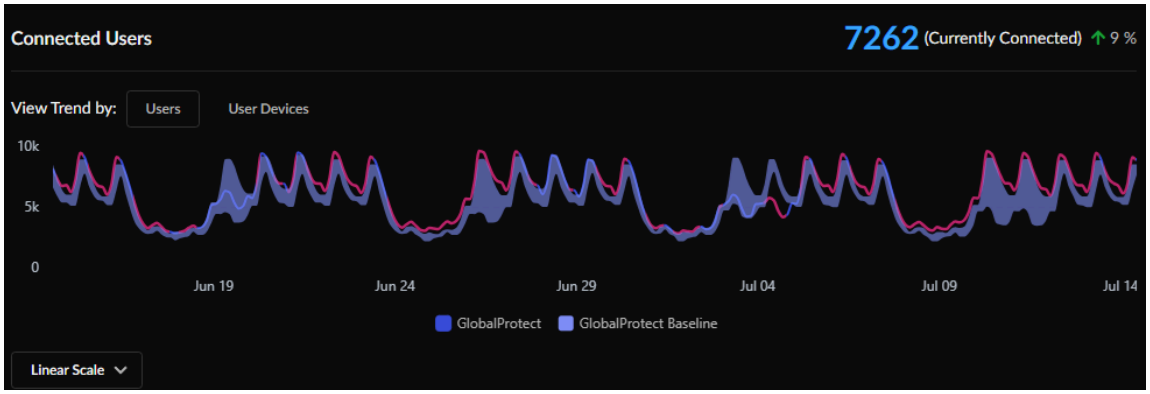
Si usted compró la licencia de AI-Powered ADEM, verá una banda de datos de referencia en los widgets de tendencias en las siguientes páginas de Monitor: Usuarios, sucursales, centros de datos y servicios de red. Los widgets muestran la referencia en el fondo en las líneas de tendencia. Esto le permite ver de un vistazo si sus datos han cruzado los límites superior o inferior de la referencia.

Los datos de referencia se calculan en intervalos de 1 hora y tienen en cuenta los últimos 28 días de datos de esos intervalos de una hora para un túnel o sitio en particular, ubicación de Prisma Access o recuento de usuarios de GlobalProtect. Por ejemplo, la referencia de 1:00 pm a 2:00 pm horas del martes se calcula a partir del intervalo de tiempo de la 1:00 pm a las 2:00 pm de los cuatro martes anteriores. El límite inferior es el percentil 10 de los datos históricos recopilados y el límite superior es su percentil 90. Esto le permite ver tendencias de ancho de banda, recuentos de usuarios, recuentos de autenticación y solicitudes y respuestas de proxy DNS. Debido a que los datos de referencia se toman de los últimos 28 días de datos históricos, los inquilinos recientemente incorporados deberán estar activos y disponer de datos enriquecidos durante 28 días para que la referencia se calcule correctamente. Si sus datos son inferiores a 28 días, es posible que observe algunas discrepancias.

Cuando los valores de la línea de tendencia del widget se desvían de los límites superior o inferior de la referencia, la línea de tendencia para ese período aparece en rojo en la interfaz web.

 ©2025 Palo Alto Networks, Inc.

El siguiente ejemplo muestra el punto de referencia de GlobalProtect desde el widget **Connected User (Usuario conectado)** en la página Usuarios.



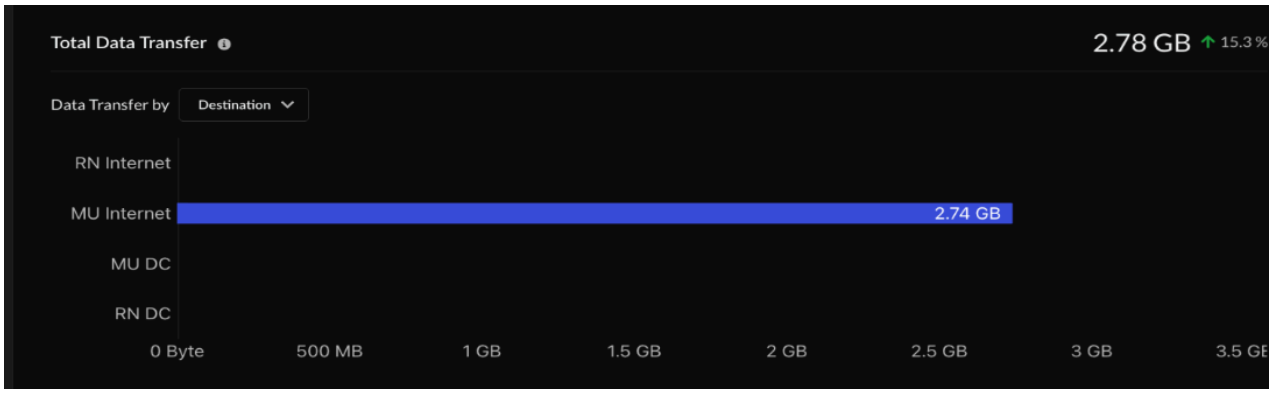
Visualización y supervisión de aplicaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Esta es una característica de Prisma Access Insights.

Utilice el Centro de control de Strata Cloud Manager para supervisar las aplicaciones de Prisma Access en su red, los usuarios que usan la aplicación y su posible impacto en la seguridad. Vaya a **Insights** > **Applications (Aplicaciones)** para obtener visibilidad de las aplicaciones de Prisma Access junto con información sobre amenazas, usuarios, transferencia de datos, puntuaciones de riesgo y experiencia de usuario de las aplicaciones.

Transferencia total de datos

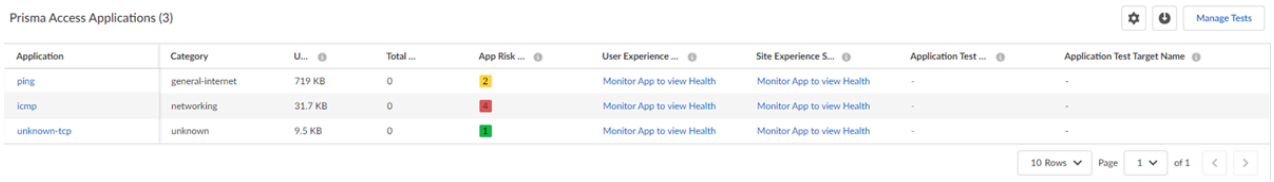
Transferencia total de datos muestra la transferencia total de datos a través de los cortafuegos de Prisma Access durante el intervalo de tiempo seleccionado. Utilice la función **Add Filter (Añadir filtro)** desplegable para otras opciones de filtrado. En el ejemplo, verá la transferencia de datos por **Application Category (Categoría de aplicación)**, que muestra las aplicaciones principales y la transferencia total de datos de esas aplicaciones. También puede ver los datos totales de transferencia por **Destination (Destino)**.



 ©2025 Palo Alto Networks, Inc.

Aplicaciones de Prisma Access

Utilice este widget para ver qué aplicaciones se están supervisando con pruebas sintéticas ejecutándose en ellas. La tabla también muestra sus puntuaciones de experiencia, que le dan el estado de cada aplicación. Haga clic en el botón **Manage Tests (Gestionar pruebas)** para ver todas las pruebas sintéticas que están configuradas para todas las aplicaciones en la tabla Pruebas de aplicaciones.



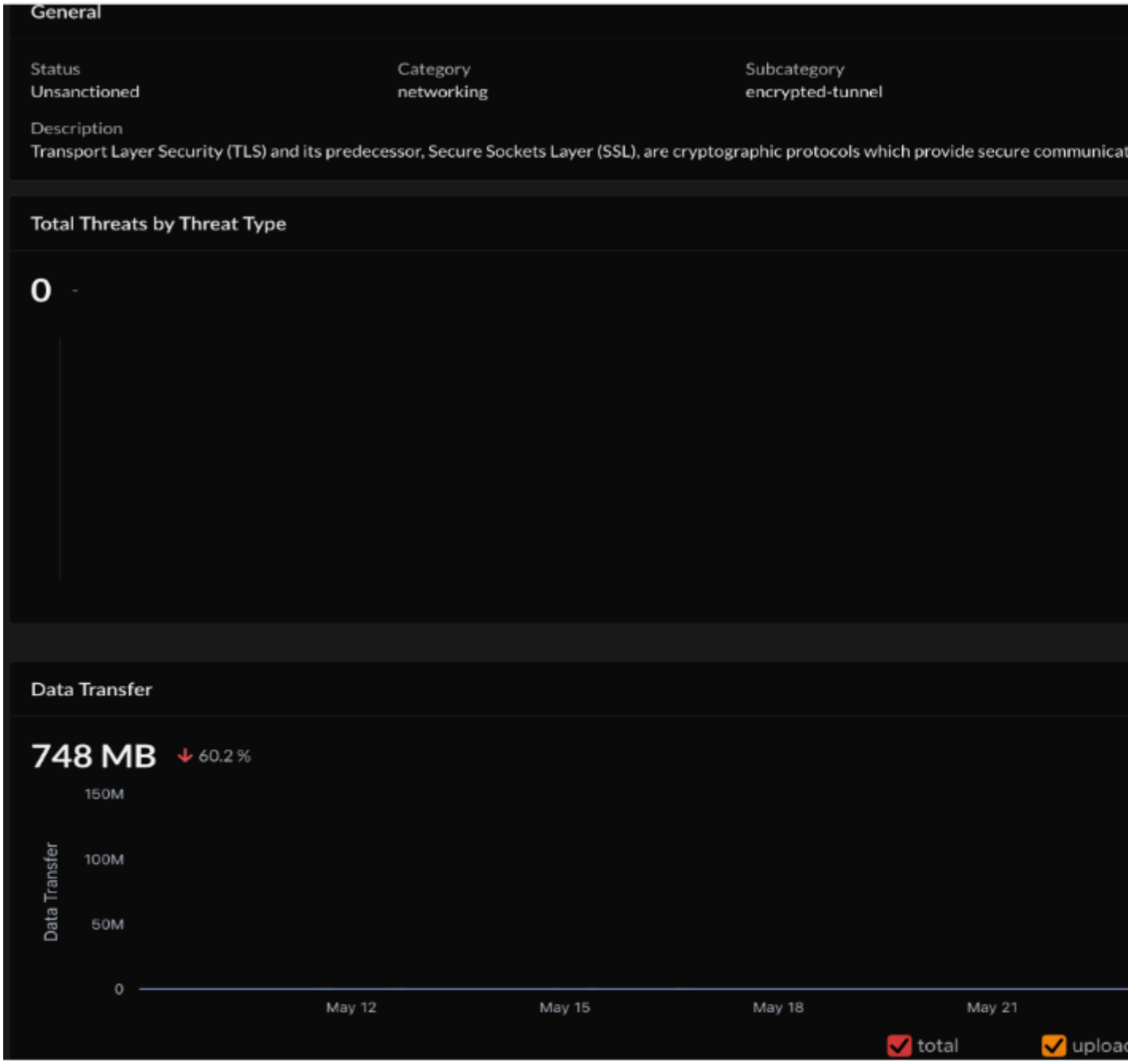
Columna	Descripción
Aplicación	El App-ID de la aplicación que se está supervisando.
Category	El tipo de aplicación.
Uso	Tráfico total en la infraestructura de Prisma Access detectada a la aplicación específica.
Número total de amenazas	Número total de amenazas experimentadas por la aplicación.
Puntuación de riesgo de la aplicación	Datos de amenazas para esta aplicación específica. 1 es el riesgo más bajo y 5 es el riesgo más alto.
Experiencia del usuario	Puntuaciones de experiencia de aplicación recopiladas por Autonomous DEM. Se agrega a todos los usuarios supervisados para esta aplicación.
Puntuación de la experiencia del sitio	Puntuación de la experiencia de la aplicación para este sitio de sucursal específico.
Nombre de la prueba de la aplicación	El nombre de la prueba configurada por el usuario para esta aplicación.
Nombre del objetivo de la prueba de la aplicación	Dirección IP del FQDN al que se dirigen las pruebas sintéticas desde varios endpoints.

Detalles de la aplicación

Seleccione cualquier aplicación para ver los detalles **General (Generales)**, como el estado, la categoría, la subcategoría, los puertos, la tecnología y la puntuación de riesgo.

©2025 Palo Alto Networks, Inc.

- **Total Threats by Threat Type (Total de amenazas por tipo de amenaza)**: amenazas actuales a la aplicación.
- **Total Users (Total de usuarios)**: el número total de usuarios que acceden a esta aplicación durante el intervalo de tiempo especificado.
- **Data Transfer (Transferencia de datos)**: vea los datos que se cargaron o descargaron para esta aplicación.



 ©2025 Palo Alto Networks, Inc.

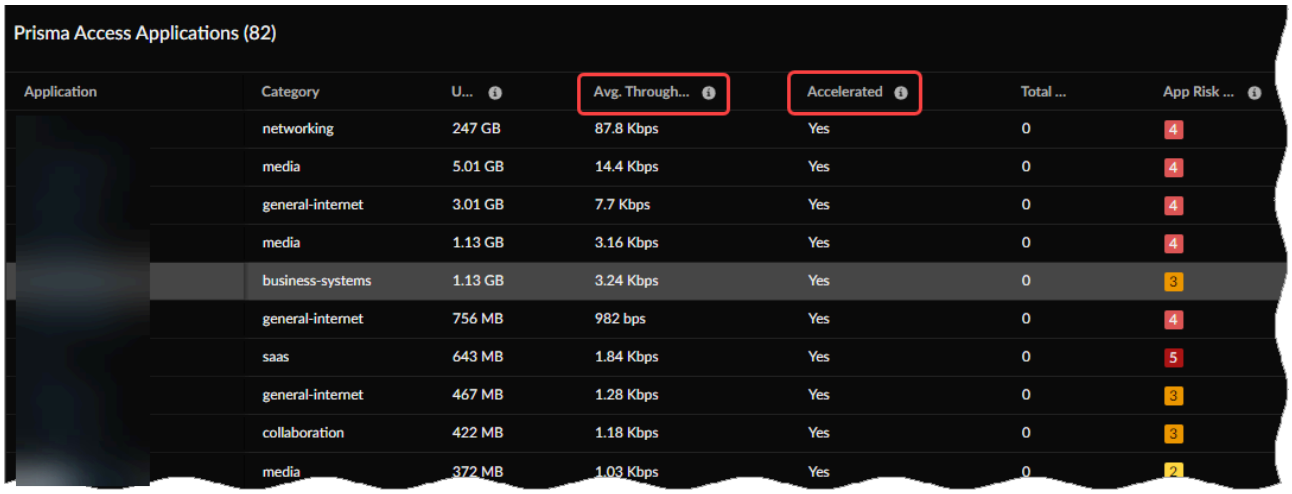
Ver y supervisar la aceleración de aplicaciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

La Aceleración de aplicaciones aborda las causas del mal rendimiento de las aplicaciones y actúa en tiempo real para mitigarlas, mejorando la experiencia del usuario para los usuarios de Prisma Access GlobalProtect y Red remota.

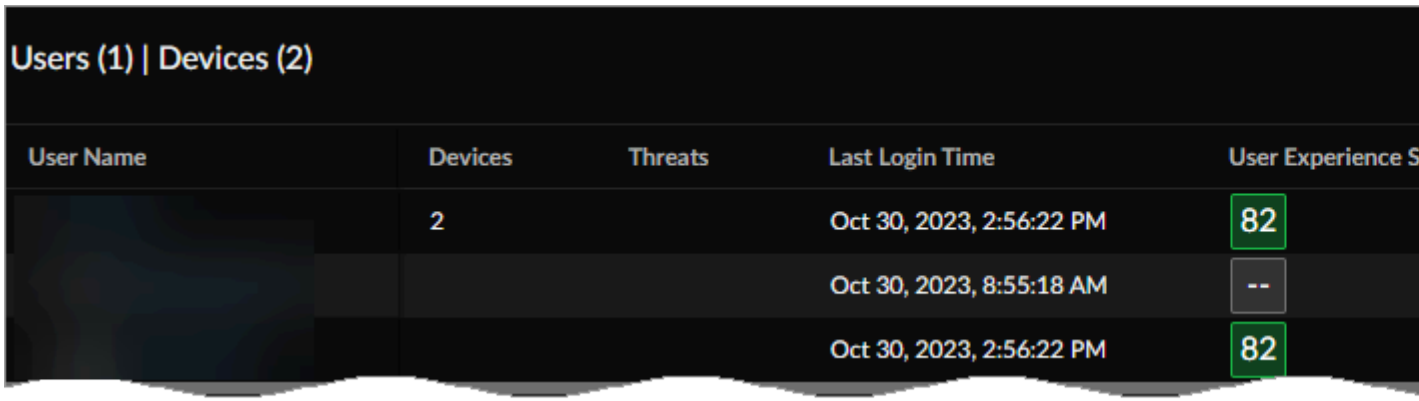
Cuando sus usuarios acceden a las aplicaciones, pueden experimentar un rendimiento deficiente de las mismas debido a una disminución del rendimiento, que puede deberse a una conectividad inalámbrica degradada, congestión de la red y otros factores. Estos problemas de red pueden afectar negativamente la experiencia del empleado y reducir su productividad. La aceleración de aplicaciones crea de forma segura una comprensión de la capacidad del dispositivo, la capacidad de la red y el contexto de la aplicación para maximizar el rendimiento y se ajusta en tiempo real para tener en cuenta las condiciones cambiantes de la red.

En el Centro de control de Strata Cloud Manager, vaya a **Insights** > **Applications (Aplicaciones)** para ver detalles sobre las aplicaciones que se han acelerado en su entorno. La tabla de aplicaciones de Prisma Access incluye la columna rendimiento medio, que solo se ve si el tráfico de su usuario está acelerado, y la columna Acelerado, que muestra que parte o la totalidad del tráfico de su aplicación se ha acelerado.



Vaya a **Insights** > **Users (Usuarios)** para ver información sobre los usuarios de la Aceleración de aplicaciones en su entorno. Los usuarios que tienen Aceleración de aplicaciones habilitada en sus entornos tienen la tabla Usuarios | Dispositivos, que muestra la columna Tráfico acelerado. Esta columna indica que se ha acelerado parte o la totalidad del tráfico de las aplicaciones de los usuarios.

 ©2025 Palo Alto Networks, Inc.



Autonomous DEM impulsado por IA (ADEM) se integra con la Aceleración de aplicaciones y le proporciona métricas como el número de aplicaciones que fueron aceleradas y el aumento de rendimiento obtenido en general. Vaya a **SASE Health (Estado de SASE)** > **Experience (Experiencia)** para ver las métricas de rendimiento de ADEM en las pestañas **Accelerated Applications (Aplicaciones aceleradas)** y **Monitored Applications (Aplicaciones supervisadas)**.

Ver Usuarios móviles

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma® Access (gestionado por Strata Cloud Manager)	• Licencia de Prisma Access • Licencia de ADEM basado en IA

Ver Activity Insights: Usuarios para una visión general de todos los usuarios y hosts conectados a las soluciones de seguridad Prisma Access de Palo Alto Networks. Puede determinar fácilmente el estado de la conexión de un usuario o host a Prisma Access, ya sea en un sitio de sucursal, conexión de servicio o ubicación remota. Ver.

- El número total de usuarios únicos actualmente conectados a las soluciones de seguridad de Palo Alto Networks y usuarios conectados a Prisma Access.
- El número de usuarios conectados durante un determinado intervalo de tiempo, desglosado por usuarios conectados a través de Prisma Access.
- Usuarios basados en agentes conectados a través de Prisma Access.
- Usuarios de proxy explícito basados en agentes o navegadores conectados a Prisma Access.
- Usuarios conectados a través de navegadores Prisma Access Browser.
- Lista de usuarios de dispositivos no gestionados que acceden a Prisma Access.
- Lista de usuarios que se conectan desde sucursales a Prisma Access.
- Lista de usuarios que conectan sus centros de datos mediante conexiones de servicio específicas.

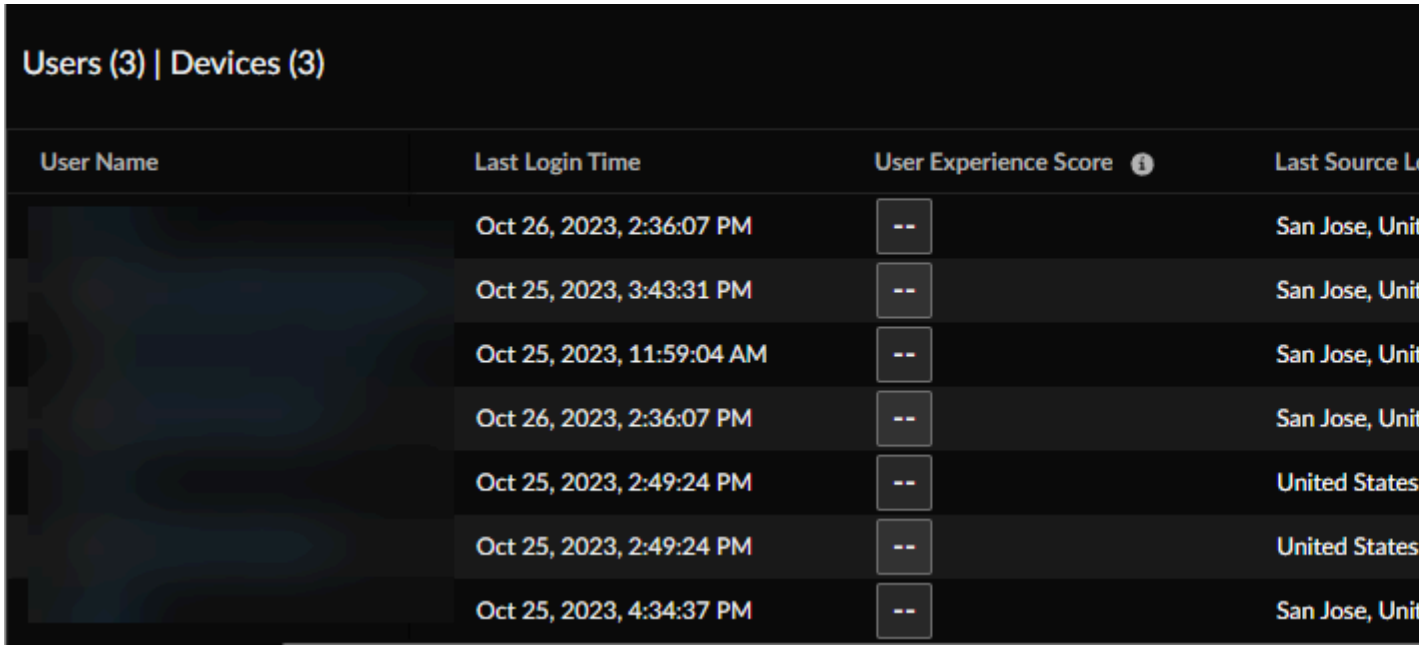
 ©2025 Palo Alto Networks, Inc.

Visualizar y supervisar IPv6 para usuarios móviles

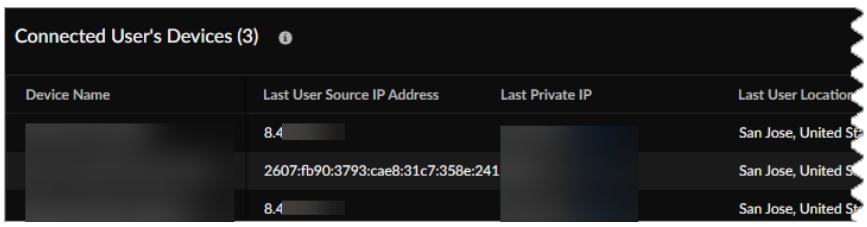
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.0 Innovation ❑ Licencia de Prisma Access

Si utiliza la red IPv6 en su implementación de Usuarios móviles: GlobalProtect, puede configurar Prisma Access para usar direcciones IPv6 en la red de sus usuarios móviles. También debe habilitar la red IPv6 a nivel global en su infraestructura de Prisma Access antes de poder usar el direccionamiento IPv6.

Con IPv6 en su implementación de GlobalProtect, la tabla Usuarios | Dispositivos muestra una dirección IPv4 o IPv6 en la columna Dirección IP de origen.

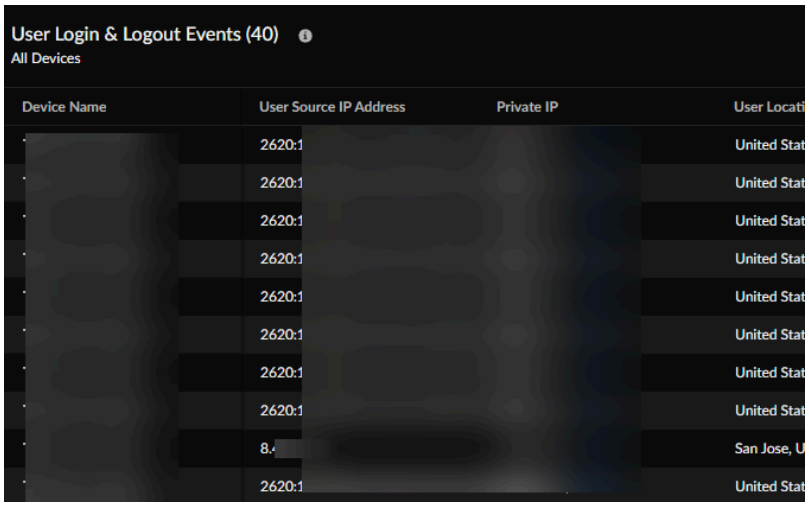


Seleccione cualquier usuario conectado para ver información sobre la tendencia de sus dispositivos. La tabla Dispositivos del usuario conectado muestra datos sobre los dispositivos de un usuario, incluida la última dirección IP de origen del usuario y la última IP privada, las cuales pueden incluir direcciones IPv4 e IPv6 para una sola entrada de dispositivo.



Puede ver la información de la dirección IPv6 en la tabla Eventos de inicio y cierre de sesión de usuario. Las columnas Dirección IP de origen del usuario y Dirección IP privada muestran una dirección IPv4 o IPv6.

 ©2025 Palo Alto Networks, Inc.



Visualizar y supervisar su sucursales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ adem-aiops-value

Seleccione **Monitor (Supervisar)** > **Branch Sites (Sucursales)** > **Prisma Access** para ver el estado y la conectividad de sus Redes remotas y el uso de todas sus Redes remotas implementadas en diferentes ubicaciones de Prisma Access. Muestra el estado de la conectividad en tiempo real y los detalles de consumo de ancho de banda, junto con otros detalles de implementación. También puede ver el estado de los túneles configurados en las redes remotas.

Consulte Redes remotas de Prisma Access para obtener información sobre cómo planificar sus redes remotas, asignar ancho de banda de red remota e integrar redes remotas. Para ver sus sucursales, vaya a **Monitor (Supervisar)** > **Branch Sites (Sucursales)** > **Prisma Access**.

Sitios por estado

Ver sus sitios de redes remotas **Sites by Status (por estado)**. Puede ver cuántos sitios están **Activos**, **Inactivos**, **Inactivos** o **No disponibles** y cuántos sitios tienen una **Advertencia** durante el **Time Range (Intervalo de tiempo)**seleccionado.



 ©2025 Palo Alto Networks, Inc.

Consumo de ancho de banda

Bandwidth Consumption (Consumo de ancho de banda) muestra el pico más alto de ancho de banda consumido en una región de cómputo en todas las regiones de cómputo del inquilino en el modelo de asignación de ancho de banda agregado. El ancho de banda máximo consumido por un sitio en todos los sitios se muestra para el modelo de asignación de ancho de banda por sitio. Los valores máximos se calculan para la duración del filtro de tiempo seleccionado.

Seleccione **View Consumption by Compute Region (Ver consumo por región de cómputo)** para ver los valores de consumo y los gráficos de tendencias de todas las regiones de cómputo y sus nodos de terminación IPSec configurados.

Ver Consumo por Regiones de cómputo

Vaya a **Monitor (Supervisar** > **Branch Sites (Sucursales)** > **Prisma Access**. Al utilizar el modelo de asignación de ancho de banda agregado, seleccione **View Consumption by Compute Regions (Ver consumo por regiones de cómputo)** en el widget **Bandwidth Consumption (Consumo de ancho de banda)** para ver el consumo de ancho de banda y las tendencias de sus regiones.

La página **Compute Regions (Regiones de cómputo)** muestra datos de consumo de ancho de banda durante el **Time Range (Intervalo de tiempo)** que seleccione. Puede ver una tabla con el **Average Bandwidth (Ancho de banda promedio)**, el **Median Bandwidth (Ancho de banda de media)** y el **Peak Bandwidth (Ancho de banda máximo)** de sus regiones de cómputo.

El gráfico **Bandwidth Consumption Trend by Compute Region (Tendencia de consumo de ancho de banda por región de cómputo)** muestra datos sobre su región de cómputo. Filtre los datos para refinar la información que desee ver.

- Seleccione **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]**, **Ingress (Entrada)**, **Egress (Salida)** o **Ingress vs. Egress (Entrada vs. Salida)** desde el menú desplegable.
- Vea la tendencia de consumo de ancho de banda **Peak (Pico)**, **Median (Mediano)** o **Average (Promedio)** durante el rango de tiempo seleccionado. La configuración predeterminada es Consumo de ancho de banda **Peak (Pico)**.
- **Log Scale (Escala de log)** o **Linear Scale (Escala lineal)**.
- **Compute Region (Región de cómputo)**: seleccione una o más regiones para ver.

El gráfico **IPSec Termination Node Utilization (Utilización del nodo de terminación IPSec)** le permite ver el consumo de ancho de banda de los nodos de terminación IPSec configurados en una región de cómputo específica. Filtre los datos para refinar la información que desee ver:

- Seleccione la región de cómputo cuyos datos desea ver.
- Seleccione el sitio específico de la región de cómputo que desea ver.
- Seleccione **Node Aggregate (Agregado de nodos)** o **Breakdown by Sites (Desglosar por sitios)** para ver la tendencia de consumo de ancho de banda de los sitios que terminan en el nodo de terminación IPSec seleccionado.
- Ver **Peak (Máximo)**, **Average (promedio)** o **Median (Media)**.

 ©2025 Palo Alto Networks, Inc.

- Ver **Log Scale (Escala de log)** o **Linear Scale (Escala lineal)**.



Tendencia del consumo de ancho de banda

En la página principal de **Branch Sites (Sucursales)**, puede ver la **Bandwidth Consumption Trend Sites per Compute Region (Tendencia del consumo de ancho de banda por sitio por región de cómputo)** para todas las regiones de cómputo cuando utiliza el modelo de asignación de ancho de banda agregado o la **Bandwidth Consumption Trend per Branch Sites (Tendencia de consumo de ancho de banda por sucursal)** cuando utiliza el **Per-Site Bandwidth Allocation Model (Modelo de asignación de ancho de banda por sitio)**. Para el modelo de asignación de ancho de banda agregado, puede seleccionar una región de cómputo y luego seleccionar los sitios en esa región de cómputo cuya tendencia de consumo de ancho de banda sea de interés. Filtre los datos para refinar la información que desea ver y puede pasar el cursor sobre el gráfico para ver el consumo de ancho de banda de los sitios en ese momento:

- La vista predeterminada muestra el consumo de ancho de banda **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]**. Otras opciones son **Ingress (Entrada)**, **Egress (Salida)**o **Ingreso vs. (Entrada v.) Salida**.

 ©2025 Palo Alto Networks, Inc.

- Vea la tendencia de consumo de ancho de banda **Peak (Pico)**, **Median (Mediano)** o **Average (Promedio)** durante el rango de tiempo seleccionado. La configuración predeterminada es Consumo de ancho de banda **Peak (Pico)**.
- **Log Scale (Escala de log)** o **Linear Scale (Escala lineal)**.
- **Compute Region (Región de cómputo)**: vea las regiones de cómputo con un desglose de los sitios que terminan en la región cuando el inquilino usa el modelo de asignación de ancho de banda agregado. Para cada región de cómputo, seleccione los sitios que terminan en la región de cómputo para ver su tendencia de consumo de ancho de banda.
- **Branch Sites (Sucursales)**: seleccione un mínimo de 1 sitio y un máximo de 10 sitios para ver sus líneas de tendencia en el gráfico durante el intervalo de tiempo seleccionado.



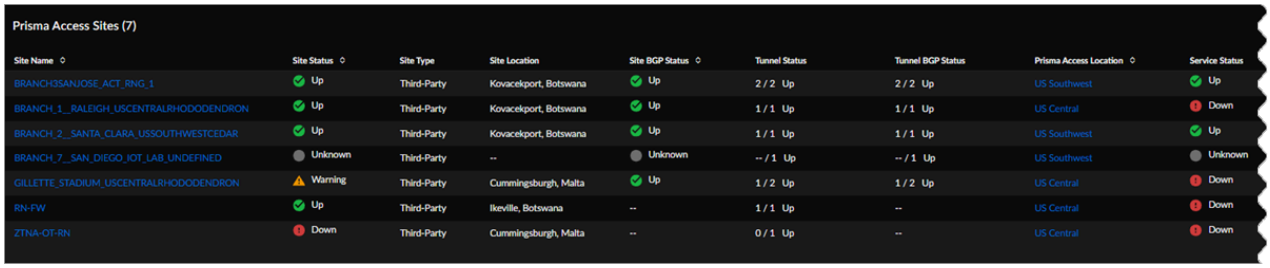
Sitios de Prisma Access

La tabla **Prisma AccessSites (Sitios de Prisma Access)** enumera sus sitios remotos de Prisma Access e información.

- **Site Name (Nombre del sitio)**: el nombre único del sitio de Prisma Access.
- **Site Status (Estado del sitio)**:**Up (Activo)**, **Down (Inactivo)**, **Warning (Advertencia)** o **Unknown (Desconocido)**.

 ©2025 Palo Alto Networks, Inc.

- **Tipo de sitio**:Terceros.
- **Ubicación del sitio**: Ubicación del sitio de Prisma Access.
- **Estado BGP del sitio**: si el estado BGP del sitio es **Up (Activo)**, **Down (Inactivo)** o **Unknown (Desconocido)**.
- **Estado del túnel**: el número de túneles del sitio y cuántos de esos túneles están en funcionamiento.
- **Tunnel BGP Status (Estado del túnel BGP)**: el estado BGP de cada túnel.
- **Prisma Access Location (Ubicación de Prisma Access)**: ubicación de este sitio de Prisma Access. Seleccione una ubicación para ver los detalles de sus ubicaciones de Prisma Access.
- **Estado del servicio**: este campo indica el estado de la instancia o el cortafuegos al que está conectado el sitio. El estado puede ser **Up (Activo)**, **Down (Inactivo)** o **Unknown (Desconocido)**.
- **Compute Location (Ubicación de cómputo)**: todas las ubicaciones de Prisma Access se asignan a una ubicación o región de cómputo de procesamiento de seguridad en función del rendimiento y la latencia optimizados. Las ubicaciones de Prisma Access que están geográficamente cerca unas de otras se agrupan en ubicaciones de proceso.
- **Ancho de banda agregado asignado**: el ancho de banda agregado asignado para el sitio durante el intervalo de tiempo seleccionado. Esta columna solo aparece si utilizó el modelo de ancho de banda agregado.
- **Ancho de banda consumido en ráfaga máxima**: el valor máximo acumulativo obtenido al combinar los valores de entrada y salida de este sitio durante el intervalo de tiempo seleccionado.
- **Ancho de banda promedio consumido**: el valor promedio acumulativo obtenido al combinar los valores de entrada y salido de este sitio durante el intervalo de tiempo seleccionado.
- **Desconexiones**: cuántas desconexiones ocurrieron en este sitio durante el intervalo de tiempo seleccionado.
- **Duración de las desconexiones**: la cantidad total de tiempo, en segundos, que el sitio estuvo desconectado durante el intervalo de tiempo seleccionado.



Visibilidad de sucursales de alto rendimiento

Las sucursales de alto rendimiento (RN-HP) tienen atributos diferentes a las sucursales heredadas, y ambas coexistirán en su inquilino. Las sucursales de alto rendimiento en Prisma Access tienen los siguientes beneficios:

- La arquitectura aborda la eficiencia de la capacidad al separar las funciones de procesamiento de red de las funciones de procesamiento de seguridad. Un dispositivo ION con gran capacidad de procesamiento de paquetes termina múltiples conexiones de sucursales con una capacidad de hasta 5 Gbps y distribuye el procesamiento de seguridad a los SPN.

 ©2025 Palo Alto Networks, Inc.

- Puede utilizar una única IP o FQDN para finalizar varias sucursales de la región en un único nodo de procesamiento de red (NPN).
- Ya no es necesario supervisar ni gestionar la terminación de los sitios de las sucursales en los nodos de terminación IPSec. Los SPN adecuados realizan la inspección del tráfico de la sucursal y el NPN realiza el equilibrio de carga.
- Se puede lograr una verdadera alta disponibilidad al poder especificar diferentes regiones para la redundancia.

Puede ver sucursales heredadas y de alto rendimiento en su entorno. En Strata Cloud Manager, vaya a **Monitor (Supervisar)** > **Branch Sites (Sucursales)** > **Prisma Access** y, en la tabla **Prisma Access Sites (Sitios de Prisma Access)** seleccione una sucursal.

Detalles del sitio de Prisma Access

Seleccione cualquier **Site Name (Nombre de sitio)** de Prisma Access para ver **Site Status (Estado de sitio)**, donde puede ver su **Connectivity (Conectividad)** y **BGP Status (Estado de BGP)** [**Up (Activo)**, **Down (Inactivo)**, **Inactive (Inactivo)** o **Not Available (No disponible)**]. Vea el **Peak Consumption (Consumo máximo)** de ancho de banda para el intervalo de tiempo seleccionado.

Puede ver la información **Cumulative (Ingress + Egress) [acumulada (entrada + salida)]** en el gráfico **de tendencia de consumo de ancho de banda** .

- Utilice el menú desplegable para ver el gráfico de consumo de ancho de banda por **Ingress (Entrada)**, **Egress (Salida)**, **Ingress Vs. (Entrada Vs.) Egress (Salida)**, o **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]**.

- Vea las métricas del gráfico de tendencia de consumo de ancho de banda por **Peak (Pico)** (predeterminado), **Average (Promedio)** o **Median (Mediana)** para la sucursal.

Visibilidad de la tabla de rutas

Para ayudarle a abordar los desafíos de accesibilidad, ofrecemos visibilidad de la tabla de rutas en cada sitio de red remoto. Puede realizar una búsqueda en la tabla de rutas de una dirección IP de destino para determinar si hay una ruta disponible para llegar al destino deseado. Con esta información, puede investigar otras posibles causas de falla. Este conocimiento le permitirá concentrar sus esfuerzos en resolver cualquier problema que pueda estar afectando la accesibilidad.

Seleccione **View Routing Table (Ver tabla de enrutamiento)** para ver la **Routing Table (Tabla de enrutamiento)**de esta sucursal, que tiene rutas IP para los destinos disponibles en la sucursal desde Prisma Access.

- Utilice la barra de búsqueda para seleccionar el destino o buscar la ruta.
- Utilice el menú desplegable para filtrar por **Flag (Marcador)**.

La tabla de enrutamiento muestra:

- **#**—Número de ruta.
- **Destination (Destino)**: dirección IP y subred de la red accesible.

 ©2025 Palo Alto Networks, Inc.

- **Next Hop (Siguiente salto)**: Dirección IP de la puerta de enlace en el siguiente salto hacia la red de destino. Si el siguiente salto es 0.0.0.0, se indica la ruta predeterminada.
- **Metric (Métrica)**: métrica de la ruta determinada por el protocolo de enrutamiento.
- **Flag (Marcador)**: información para esta ruta, como sigue:
- - **A B**: activo y obtenido mediante BGP.
  - **AC**: activo y conectado. Destino: red.
  - **AH**: activo y conectado. Destino: solo host.
  - **A R**: activo y obtenido mediante RIP.
  - **O1**: OSPF externo tipo 1.
  - **O2**: OSPF externo tipo 2.
  - **Oi**: OSPF dentro del área.
  - **Oo**: interárea OSPF.
  - **S**: inactivo y estático.
  - **A S**Activo y estático.

Túneles

Ver túneles y datos de túneles para este sitio.

- **Nombre del túnel**: el nombre exclusivo del túnel.
- **Ubicación de Prisma Access**: la ubicación de Prisma Access para esta red remota.
- **Estado del túnel**:**Up (Activo)**, **Down (Inactivo)**, **Init (Inicializado)**o **Unavailable (No disponible)**.
- **Estado del túnel BGP**:**Up (Activo)**, **Down (Inactivo)** o **Unknown (Desconocido)**.
- **Monitorización de túnel**: si ha habilitado la **Monitorización de túnel**, esta columna muestra si está **Up (Activo)** o **Down (Inactivo)**. Si no lo ha habilitado, esta columna muestra **Not Configured (No configurado)**.
- **Rendimiento promedio**: el ancho de banda promedio para el túnel durante el intervalo de tiempo seleccionado, considerando la **Ingress (Entrada)**, **Egress (Salida)**, **Entrada vs. Salida**, o el valor **Cumulative (Ingress + Egress) [Acumulativo (ingreso + egreso)]** que seleccionó.
- **Rendimiento máximo**: el ancho de banda máximo para el túnel durante el intervalo de tiempo seleccionado, considerando la **Ingress (Entrada)**, la **Egress (Salida)**, **Ingress Vs. (Entrada vs.) Egress (Salida)**, o **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]**.
- **Dirección IP de origen**: la dirección IP de origen.
- **Dirección del endpoint de destino**: dirección IP o FQDN para que Prisma Access determine si el túnel está activo.
- **Desconexiones**: número de desconexiones durante el intervalo de tiempo seleccionado.
- **Duración de las desconexiones**: cuánto tiempo, en segundos, el túnel permanece desconectado durante el intervalo de tiempo seleccionado.

Seleccione un **Nombre de túnel** para ver su **Tunnel Status (Estado de túnel)**, **Bandwidth Consumption Trend (Tendencia de consumo de ancho de banda)** y otros detalles del túnel.

 ©2025 Palo Alto Networks, Inc.

Tendencias de túneles

Con **Tunnel Monitoring (Supervisión de túneles)** habilitado, puede seleccionar una cantidad de túneles y ver su **Round-Trip Time (Tiempo de ida y vuelta)** medio. Si no especifica un conjunto de túneles, de forma predeterminada se calcula el RTT medio para los 10 túneles con el RTT observado más alto.

La **Aggregated Tunnel Connectivity (Conectividad de túneles agregada)** le muestra el número total de túneles conectados para el rango de tiempo seleccionado. Pase el cursor sobre cualquiera de los gráficos para ver la cantidad de conexiones en un momento específico.

Commits Pushed Confirmaciones enviadas) muestra cuántas confirmaciones fueron enviadas durante el **Time Range (Intervalo de tiempo)** seleccionado y cuándo ocurrió la **Last Push Commit (Última confirmación de envío)**.

Estado del sitio

Site Status (Estado del sitio) muestra la disponibilidad del sitio durante el rango de tiempo seleccionado. **Verde** significa que el sitio estuvo activo durante este tiempo, **rojo** significa que el sitio estuvo inactivo y **gris** significa que no hubo datos disponibles durante el tiempo mostrado.

Ver y supervisar centros de datos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Conexiones de servicio

Una conexión de servicio, también conocida como un Nodo de Acceso Corporativo (CAN), permite a los usuarios móviles y a los usuarios de redes remotas acceder a aplicaciones y recursos privados, y permite que sus usuarios móviles y redes remotas se comuniquen entre sí. Palo Alto Networks recomienda siempre crear una conexión de servicio en su implementación de Prisma Access. Todas las conexiones de servicio permiten el acceso a los recursos de su sede central o centro de datos, y permiten que las redes remotas y los usuarios móviles se comuniquen entre sí.

El número de conexiones de servicio que reciba depende de su licencia de Prisma Access. Ver Conexiones del servicio Prisma Access para obtener más información sobre las conexiones de servicio y cómo configurarlas.

En Strata Cloud Manager, seleccione **Monitor (Supervisar)** > **Data Centers (Centros de datos** > **Service Connections (Conexiones de servicio)** para obtener visibilidad de sus conexiones de servicio.

Conectores ZTNA

El Conector Zero Trust Network Access (ZTNA) le permite conectar Prisma Access a las aplicaciones privadas de su organización. ZTNA Connector proporciona a los usuarios móviles

 ©2025 Palo Alto Networks, Inc.

y a los usuarios en sucursales acceso a sus aplicaciones privadas mediante un túnel seguro automatizado. ZTNA Connector configura los túneles automáticamente, por lo que no tiene que configurar manualmente los túneles IPSec y el enrutamiento al centro de datos o a las ubicaciones de la sede, las ubicaciones de la nube pública y las redes de socios donde se encuentran sus aplicaciones privadas.

En Strata Cloud Manager, seleccione **Monitor (Supervisar)** > **Data centers (Centros de datos)** > **ZTNA Connectors (Conectores ZTNA)** para la visibilidad de sus ZTNA Connectors.

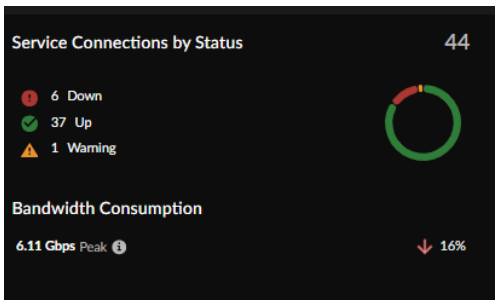
Ver y supervisar conexiones de servicio.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Vea los datos añadidos de conexiones de servicio, así como información sobre conexiones de servicio individuales. Las conexiones de servicio permiten tanto a los usuarios móviles como a las redes remotas. Más allá de proporcionar acceso a los recursos corporativos, las conexiones de servicio permiten a sus usuarios móviles llegar a las sucursales. Puede ver sus conexiones de servicio en Strata Cloud Manager para ver el estado de la conexión de servicio, las tendencias de consumo de ancho de banda, los datos y las tendencias del túnel, e información sobre el estado general de la conexión de servicio. Seleccione **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **Service Connections (Conexiones de servicio)** para comenzar.

Conexiones de servicio por estado

Vea el estado de salud de todas sus conexiones de servicio. El gráfico codificado por colores muestra una distribución de cuántas conexiones de servicio están activas, inactivas o necesitan atención. Puede ver una sinopsis del ancho de banda que consumieron sus conexiones de servicio en los últimos 30 días.



Bandwidth Consumption (Consumo de ancho de banda) muestra el consumo de ancho de banda máximo consumido por un sitio en todos los sitios para el modelo de asignación de ancho de banda por sitio. Los valores máximos se calculan para la duración del filtro de tiempo seleccionado.

Tendencia del consumo de ancho de banda

Visualice **Bandwidth Consumption Trend per Service Connection (Tendencia de consumo de ancho de banda por conexión de servicio)**. La tendencia muestra el consumo de ancho de banda por cada una de sus conexiones de servicio, así como sus utilizaciones medias y máximas.

 ©2025 Palo Alto Networks, Inc.

- La vista predeterminada muestra el consumo de ancho de banda **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]**. Otras opciones son **Ingress (Entrada)**, **Egress (Salida)**o **Ingreso vs. (Entrada v.) Salida**.
- Vea la tendencia de consumo de ancho de banda **Peak (Pico)**, **Median (Mediano)** o **Average (Promedio)** durante el rango de tiempo seleccionado. La configuración predeterminada es **Pico (Máximo)** consumo de ancho de banda.
- **Log Scale (Escala de log)** o **Linear Scale (Escala lineal)**.
- Seleccione del 1 a 10 **Service Connections (Conexiones de servicio)** para ver sus líneas de tendencia en el gráfico durante el intervalo de tiempo seleccionado. Coloque el cursor sobre el gráfico para obtener información sobre cada una de las conexiones de servicio que seleccionó.



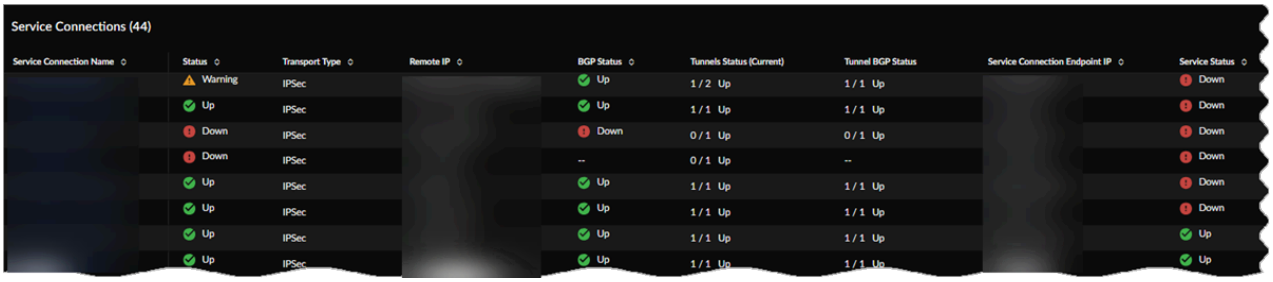
Tabla de Conexiones de servicio/sitios

La tabla **Service Connections (Conexiones de servicio)** muestra datos sobre sus conexiones de servicio, como el estado, la dirección IP remota, el estado BGP, el estado actual del túnel y otros datos. Seleccione un **Service Connection Name (Nombre de la conexión de servicio)** para obtener más información sobre esa conexión de servicio.

- **Service Connection Name (Nombre de la conexión de servicio)**: el nombre único de la conexión de servicio.
- **Status (Estado)**:**Up (Activo)**, **Down (Inactivo)**, **Warning (Advertencia)** o **Unknown (Desconocido)**.
- **Tipo de transporte**: IPSec.
- **IP remota**: la dirección IP remota.
- **Estado de BGP**: si el estado de BGP del sitio es **Up (Activo)**, **Down (Inactivo)**o **Unknow (Desconocido)**.
- **Estado de los túneles (actual)**: el número de túneles del sitio y cuántos de esos túneles están en funcionamiento.
- **Tunnel BGP Status (Estado del túnel BGP)**: el estado BGP de cada túnel.
- **IP de endpoint de conexión de servicio**: la dirección IP del endpoint de la conexión de servicio.
- **Estado del servicio**: este campo indica el estado de la instancia o el cortafuegos al que está conectado el sitio. El estado puede ser **Up (Activo)**, **Down (Inactivo)** o **Unknown (Desconocido)**.
- **Ubicación de Prisma Access**: la ubicación de Prisma Access de la conexión de servicio.

 ©2025 Palo Alto Networks, Inc.

- **Average Bandwidth Consumption (Consumo medio de ancho de banda)**: Consumo medio de ancho de banda en Kbps.
- **Peak Bandwidth Consumption (Consumo máximo de ancho de banda)**: consumo máximo de ancho de banda en Kbps.



Detalles de la conexión del servicio

Seleccione cualquier **Service Connection Name (Nombre de conexión de servicio)** para ver sus detalles. Vea su **Service Connection Status (Estado de la conexión del servicio)**, **Bandwidth Consumed (Ancho de banda consumido)** durante los últimos 30 días. El gráfico **Bandwidth Consumption Trend (Tendencia del consumo de ancho de banda)** muestra el consumo de ancho de banda por cada una de sus conexiones de servicio durante el intervalo de tiempo seleccionado.

Estado del sitio

Seleccione cualquier **Service Connection Name (Nombre de la conexión de servicio)** para ver su **Site Status (Estado del sitio)** donde se puede ver su **Connectivity (Conectividad)** y **Site Status (Estado del sitio)** [**Up (Activo)**, **Down (Inactivo)**, **Inactive (Inactivo)** o **Not Available (No disponible)**]. Vea el **Peak Consumption (Consumo máximo)** de ancho de banda para el intervalo de tiempo seleccionado.

Visibilidad de la tabla de rutas

Para ayudarle a abordar los desafíos de accesibilidad, ofrecemos visibilidad de la tabla de rutas en cada conexión de servicio. Puede realizar una búsqueda en la tabla de rutas de una dirección IP de destino para determinar si hay una ruta disponible para llegar al destino deseado. Con esta información, puede recibir orientación de su infraestructura de Prisma Access para investigar otras posibles causas de fallos. Este conocimiento le permitirá concentrar sus esfuerzos en resolver cualquier problema que afecta la accesibilidad.

Seleccione **View Routing Table (Ver tabla de enrutamiento)** para ver la **Routing Table (Tabla de enrutamiento)**de esta sucursal, que tiene rutas IP para los destinos disponibles en la sucursal desde Prisma Access.

- Utilice la barra de búsqueda para seleccionar el destino o buscar la ruta.
- Utilice el menú desplegable para filtrar por **Flag (Marcador)**.

La tabla de enrutamiento muestra:

- **#**: número de ruta
- **Destination (Destino)**: Dirección IP y subred de la red accesible.
- **Next Hop (Siguiente salto)**: Dirección IP de la puerta de enlace en el siguiente salto hacia la red de destino. Si el siguiente salto es 0.0.0.0, se indica la ruta predeterminada.
- **Metric (Métrica)**: métrica de la ruta determinada por el protocolo de enrutamiento.

 ©2025 Palo Alto Networks, Inc.

- **Flag (Marcador)**: información para esta ruta, como sigue:
- - **A B**: activo y obtenido mediante BGP.
  - **AC**: activo y conectado. Destino: red.
  - **AH**: activo y conectado. Destino: solo host.
  - **A R**: activo y obtenido mediante RIP.
  - **O1**: OSPF externo tipo 1.
  - **O2**: OSPF externo tipo 2.
  - **Oi**: OSPF dentro del área.
  - **Oo**: interárea OSPF.
  - **S**: inactivo y estático.
  - **A S**: Activo y estático.

Tendencia del consumo de ancho de banda

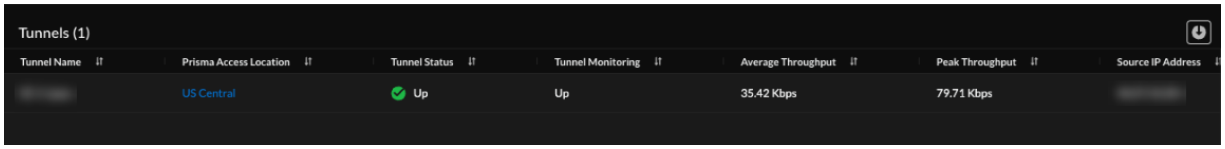
La **Bandwidth Consumption Trend (Tendencia de consumo de ancho de banda)** muestra información **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]** de forma predeterminada.

- Utilice el menú desplegable para ver el gráfico de consumo de ancho de banda por **Ingress (Entrada)**, **Egress (Salida)**, **Ingress Vs. (Entrada Vs.) Egress (Salida)**, o **Cumulative (Ingress + Egress) [Acumulativo (entrada + salida)]**.

- Vea las métricas del gráfico de tendencia de consumo de ancho de banda por **Peak (Pico)** (predeterminado), **Average (Promedio)** o **Median (Mediana)** para la sucursal.

Túneles

Vea cuántos **Tunnels (Túneles)** hay para esta conexión de servicio y ver los detalles de cada túnel. Para descargar datos de **Tunnels (Túneles)**, seleccione el icono Descargar.



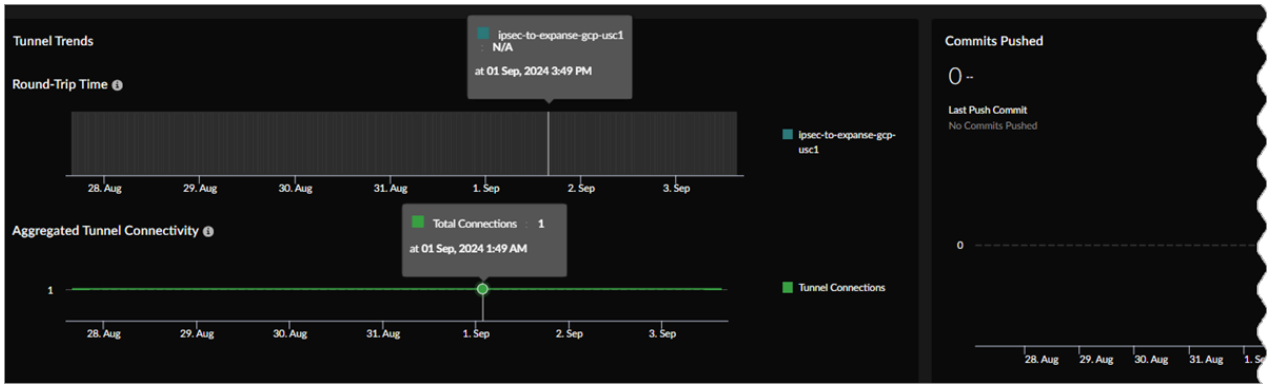
Tendencias de túneles

Puede seleccionar una serie de túneles y ver su **Round-Trip Time (Tiempo de ida y vuelta)** medio. Si no especifica un conjunto de túneles, el RTT mediano se calcula para los 10 túneles con el RTT más alto observado.

La **Aggregated Tunnel Connectivity (Conectividad de túneles agregada)** le muestra el número total de túneles conectados para el rango de tiempo seleccionado. Pase el cursor sobre cualquiera de los gráficos para ver la cantidad de conexiones en un momento específico.

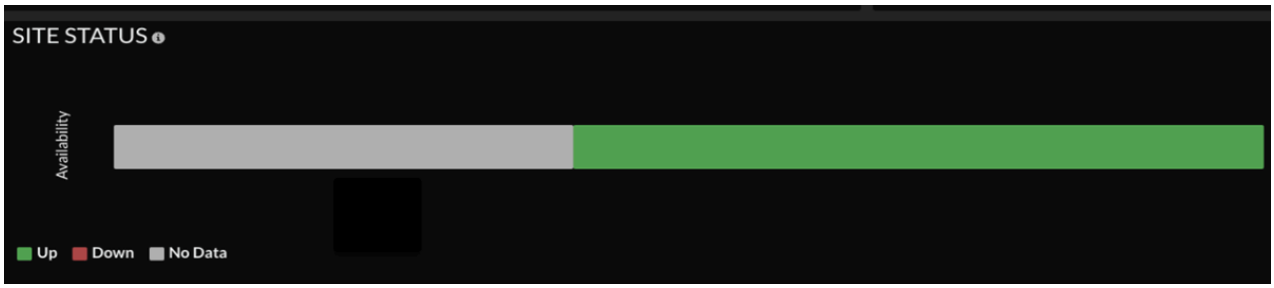
 ©2025 Palo Alto Networks, Inc.

Commits Pushed (Confirmaciones enviadas) muestra cuántas confirmaciones se han enviado durante el **Time Range (Intervalo de tiempo)** seleccionado y cuando se produjo la **Last Push Commit (Última confirmación de envío)**.



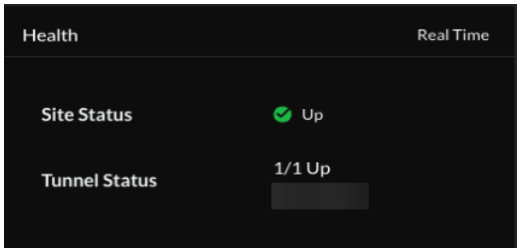
Estado del sitio

Site Status (Estado del sitio) muestra la disponibilidad del sitio durante el rango de tiempo seleccionado. Verde significa que el sitio estuvo activo durante este tiempo, rojo significa que el sitio estuvo inactivo y gris significa que no hubo datos disponibles durante el tiempo mostrado.



Estado

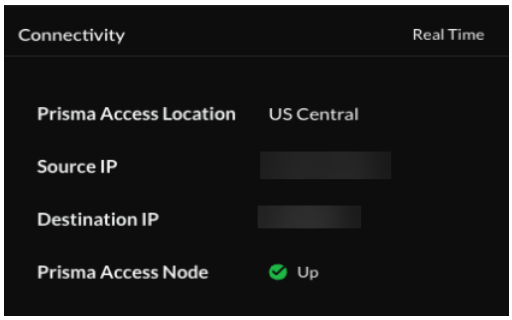
Health (Salud) le muestra el **Site Status (Estado del sitio)** y muestra el nombre y el estado de cada túnel del sitio.



Conectividad

Connectivity (Conectividad) muestra ubicación de Prisma Access a la que está conectado el sitio, sus direcciones IP de origen y destino, y el estado del nodo de Prisma Access.

©2025 Palo Alto Networks, Inc.



Consumo

Consumption (Consumo) muestra los detalles del consumo de ancho de banda.



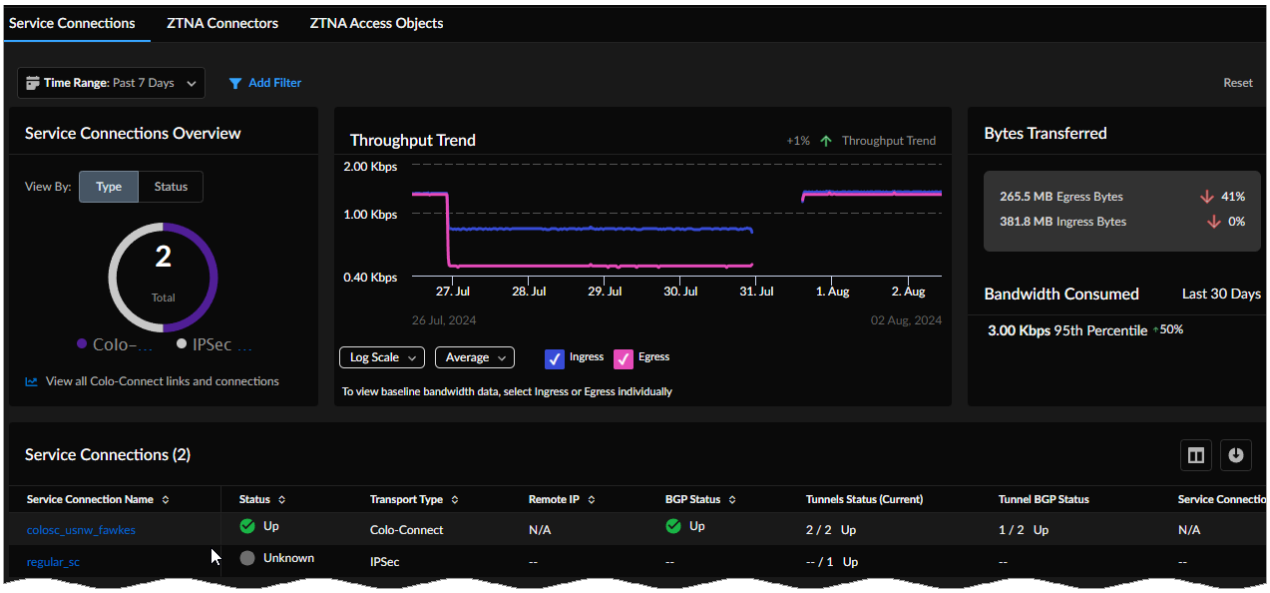
Ver y supervisar Colo-Connect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	Licencia de Prisma Access

Prisma AccessColo-Connect aprovecha la tecnología de interconexión GCP nativa de la nube para proporcionar conexiones de servicio de gran ancho de banda a sus aplicaciones privadas. Colo-Connect coexiste con las conexiones de servicio basadas en túneles IPSec existentes, por lo que si necesita proporcionar acceso a aplicaciones privadas a centros de datos más pequeños que no requieren un alto rendimiento de ancho de banda, también podría utilizar conexiones de servicio a esos centros de datos. Gane visibilidad en su implementación de Colo-Connect al ver métricas como el número de enlaces de Colo-Connect y su estado, tendencias de rendimiento y detalles individuales de túneles, conexiones y enlaces. Al ver datos sobre las conexiones de su servicio Colo-Connect, puede obtener una visión general del estado y la conectividad de su implementación.

Para ver y supervisar su conectividad privada a la nube híbrida y a los centros de datos locales a través de interconexiones en la nube, vaya a **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **Service Connections (Conexiones de servicio)**.

 ©2025 Palo Alto Networks, Inc.



Descripción general de las conexiones de servicio

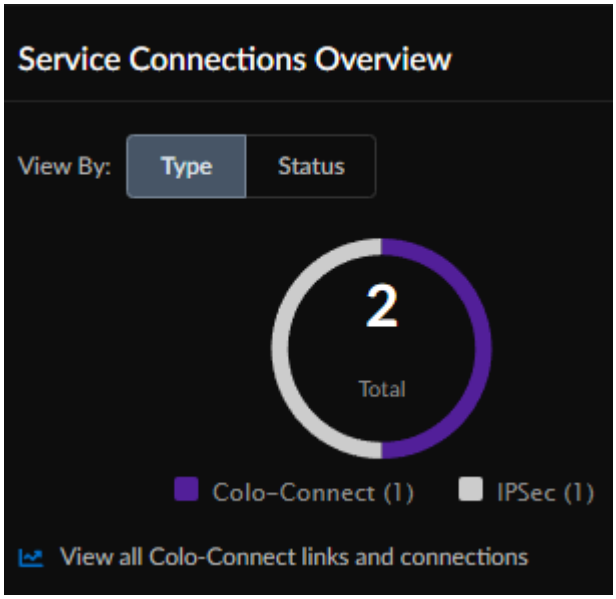
La descripción general de las conexiones de servicio muestra el número de conexiones de servicio por **Type (Tipo)** de transporte.

Puede ver una agregación de transportes conectados por **Type (Tipo)** o su **Status (Estado)** de disponibilidad.

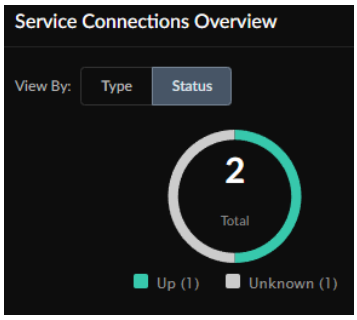
- **IPSec**
- **Colo-Connect**

Puede ver el tipo de transporte de túnel por estado: **Up (Activo)**, **Down (Inactivo)**, **Degraded (Degradado)** o **Unknown (Desconocido)**.

Seleccione **View all Colo-Connect links and connections (Ver todos los enlaces y conexiones de Colo-Connect)** para ver la página de detalles de Colo-Connect.

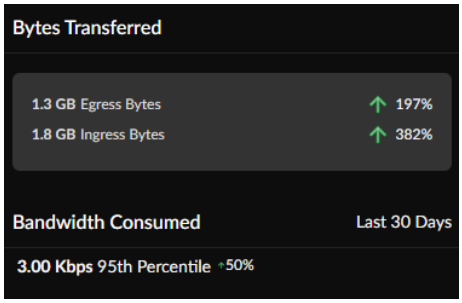


 ©2025 Palo Alto Networks, Inc.



Descripción general de las conexiones de servicio: Bytes transferidos y ancho de banda consumido

Los **Bytes Transferidos** muestran una agregación de los bytes de entrada y salida consumidos, y la diferencia en el consumo desde el intervalo de tiempo que seleccionó anteriormente. El **Bandwidth Consumed (Ancho de banda consumido)** muestra el percentil 95 del ancho de banda consumido en los últimos 30 días.



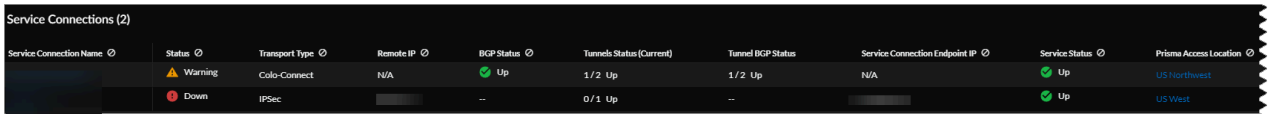
Conexiones de servicio

La tabla de **Service Connections (Conexiones de servicio)** muestra los siguientes detalles para cada Conexión de servicio indicada:

- **Nombre de la conexión de servicio**: nombre de la conexión de servicio Colo-Connect o IPSec. Seleccione un **Service Connection Name (Nombre de conexión de servicio)** para ir a su página de detalles.
- **Estado**: Activo, Inactivo, Degradado o Desconocido.
- **Tipo de transporte**: Colo-Connect o IPSec.
- **IP remota**: IP de destino.
- **Estado BGP**: activo o inactivo o advertencia si algunos túneles BGP están activos y otros están inactivos.
- **Estado del túnel (actual)**: estado actual del túnel.
- **Estado de BGP del túnel**: número de túneles por estado de BGP (Activo, Inactivo o Advertencia).
- **IP de endpoint de conexión de servicio**: La dirección IP del nodo de Prisma Access.
- **Estado del servicio**: El estado del servicio se determina por la conexión de servicio activa o el estado del clúster de centros de datos o clústeres (más de un clúster) (Activo, Inactivo o Advertencia).
- **Ubicación de Prisma Access**: seleccione una **Prisma Access Location (Ubicación de Prisma Access)**.

 ©2025 Palo Alto Networks, Inc.

- **Consumo Promedio de Ancho de Banda**: el consumo promedio de ancho de banda para el sitio durante el intervalo de tiempo seleccionado.
- **Consumo máximo de ancho de banda**: el consumo máximo de ancho de banda para el sitio durante el intervalo de tiempo seleccionado.



Detalles de la conexión del servicio

Desde la tabla de **Service Connections (Conexiones de Servicio)** en la página principal, seleccione una **Service Connection (Conexión de Servicio)** con su **Type (Tipo)** de transporte como Colo-Connect para ir a su página de detalles.



Estado de conexión del servicio, Colo-Connect y sesiones concurrentes

- Vea la **ubicación de acceso** de la conexión de servicio y el estado de los **túneles GRE** (Activo, Inactivo o Advertencia).
- Ver el número total de enlaces y conexiones de **Colo-Connect**.
- Las **sesiones concurrentes** muestran el número de sesiones actuales y el número total de sesiones durante los últimos 30 días.

Tendencia de rendimiento

La **tendencia de rendimiento** muestra el tráfico de entrada y salida consumido por esta conexión de servicio durante el intervalo de tiempo seleccionado.

Bytes transferidos y ancho de banda consumido

Los **Bytes transferidos** muestran una agregación de los bytes de entrada y salida que esta conexión de servicio consumió, así como la diferencia en el consumo con respecto al intervalo de tiempo seleccionado anteriormente. El **Bandwidth Consumed (Ancho de banda consumido)** muestra el percentil 95 del ancho de banda que la conexión del servicio consumió en los últimos 30 días.

Túneles GRE

Ver detalles sobre los túneles en esta conexión de servicio:

- **Nombre del túnel**: el nombre único del túnel.

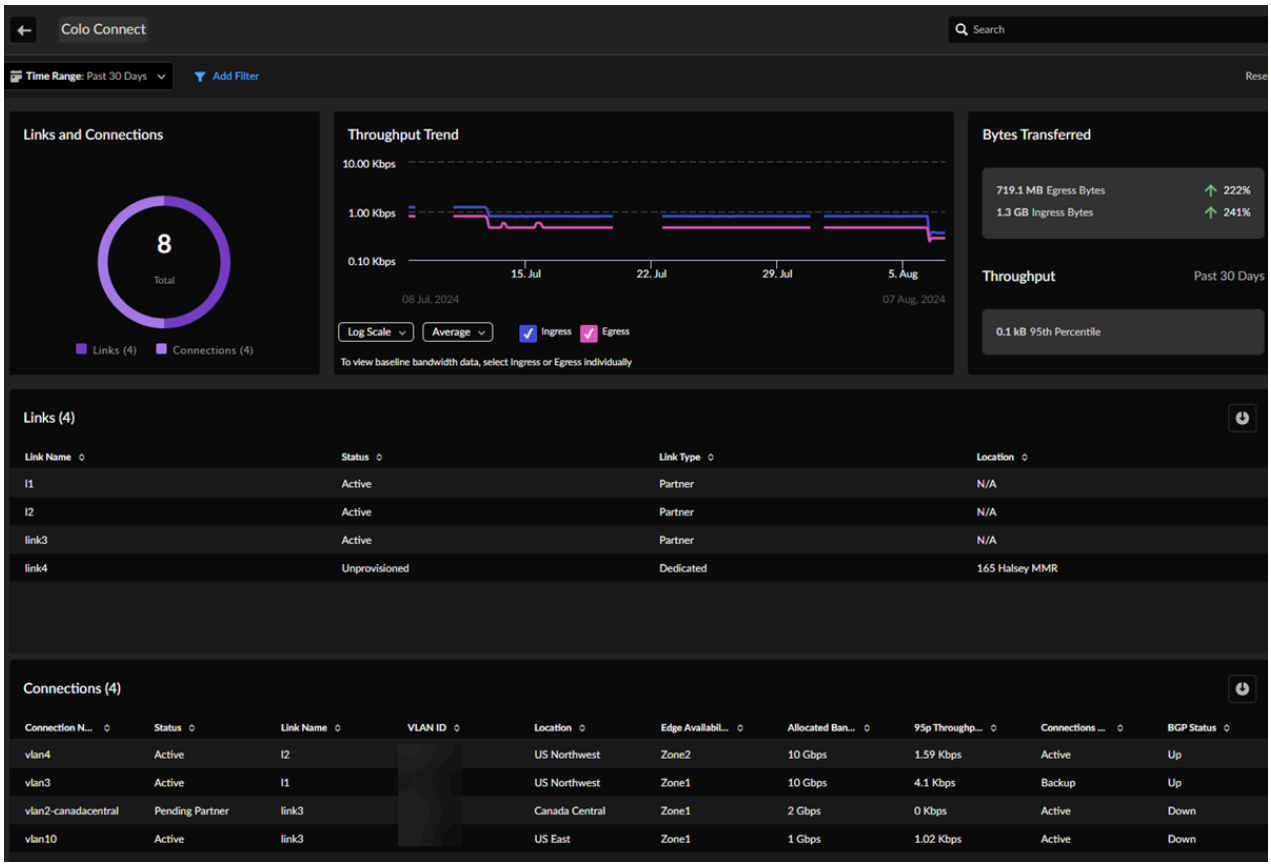
 ©2025 Palo Alto Networks, Inc.

- **Estado del túnel**: Activo, Inactivo o Desconocido.
- **Nombre de la conexión**: el nombre único de la conexión.
- **Estado del túnel**: el estado de la conexión (Activa o de respaldo).
- **IP Remota**: dirección de IP de destino.
- **IP de origen**: dirección IP del dispositivo local.
- **95% de rendimiento**: el percentil 95 del ancho de banda consumido en los últimos 30 días.
- **Rendimiento máximo**: rendimiento máximo durante el intervalo de tiempo seleccionado.
- **Estado BGP**: Activo, Inactivo, Degradado o Desconocido.
- **Dirección IP local de BGP**: La IP local de BGP.
- **Desconexiones**: cuántas desconexiones ha tenido este túnel.
- **Duración de las desconexiones**: cuánto tiempo duraron las desconexiones.
- **Bytes de entrada**: cuántos bytes de entrada se consumieron durante el intervalo de tiempo seleccionado.
- **Bytes de salida**: cuántos bytes de salida se consumieron durante el intervalo de tiempo seleccionado.
- **Recuento de paquetes de entrada**: el recuento de paquetes de entrada.
- **Recuento de paquetes de salida**: el recuento de paquetes de salida.

Detalles de Colo Connect

Desde la página principal de **Service Connections (Conexiones de Servicio)**, seleccione **View all Colo-Connect links and connections (Ver todos los enlaces y conexiones de Colo-Connect)** desde el widget de **Service Connections Overview (Resumen de conexiones de servicio)** para abrir la página de detalles de **Colo-Connect**. Los widgets en esta página muestran sus detalles actuales (actual definido como los últimos 20 minutos).

 ©2025 Palo Alto Networks, Inc.



Enlaces y conexiones

El gráfico circular muestra el número total de enlaces y conexiones de Colo-Connect actuales.

Enlaces

La tabla muestra detalles sobre sus enlaces Colo-Connect actuales.

- **Nombre del enlace**: nombre único del enlace Colo-Connect.
- **Estado**: activo o mantenimiento.
- **Tipo de enlace**: socio o dedicado.
- **Ubicación**: ubicación de Prisma Access.

Conexiones

Ver detalles sobre cada uno de sus enlaces Colo-Connect actuales. Pasa el ratón sobre las conexiones para ver información sobre el estado mostrado.

- **Nombre de conexión**: nombre de conexión Colo-Connect único.
- **Estado**: Activo, Socio pendiente, Inactivo, En desuso.
- **Nombre del enlace**: el nombre del enlace de la conexión.
- **ID de VLAN**: el ID de VLAN de la conexión.
- **Ubicación**: ubicación de Prisma Access.
- **Zona de Disponibilidad de Edge**: Zona1 o Zona2.
- **Ancho de banda asignado**: 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps o 20 Gbps.

 ©2025 Palo Alto Networks, Inc.

- **95 % de rendimiento**: el percentil 95 del ancho de banda consumido.
- **Estado de conexión**: Activo o De respaldo.
- **Estado BGP**: Activo o Inactivo.

Ver y supervisar ZTNA Connectors

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Esta es una característica de Prisma Access Insights.

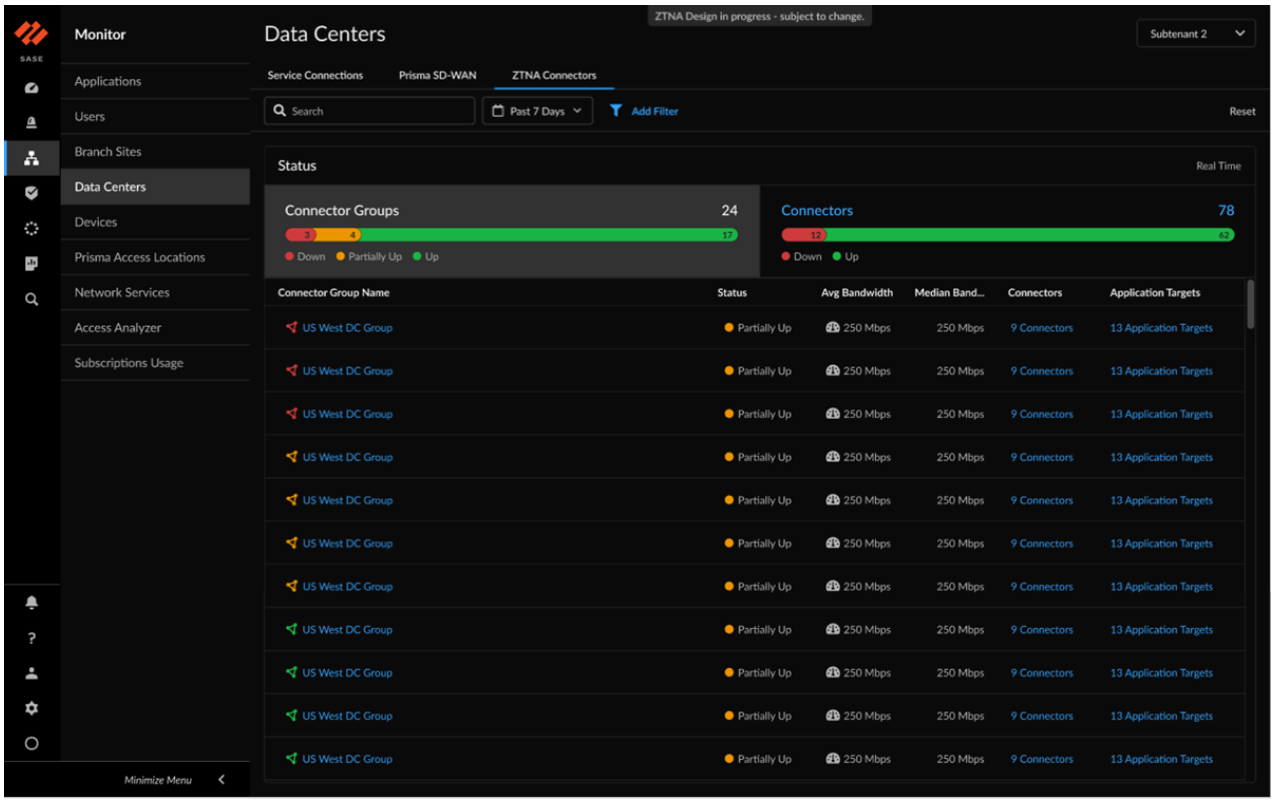
El conector de acceso a la red de confianza cero (ZTNA) simplifica el acceso privado a aplicaciones para todas sus aplicaciones. La máquina virtual de ZTNA Connector en su entorno forma automáticamente túneles entre sus aplicaciones privadas y Prisma Access. Vea un resumen de todos los conectores ZTNA configurados, incluido los **Application Targets (Destinos de la aplicación)** asociados con el conector, su ancho de banda promedio y medio, y el **Status (Estado)** (Activo, Parcialmente activo o Desactivado). Seleccione **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **ZTNA Connectors (Conectores ZTNA)** en Strata Cloud Manager para ver el rendimiento de los conectores ZTNA y los grupos de conectores.

Estado de los grupos de conectores ZTNA

Los conectores de cada grupo determinan el valor del **Status (Estado)** de un grupo de conectores.

- Si todos los **Connectors (Conectores)** en un **Connector Group (Grupo de conectores)** están activos, el **Status (Estado)** es **Up (Activo)** (verde).
- Si todos los **Connectors (Conectores)** están inactivos, el estado es **Down (Inactivo)** (rojo).
- Si algunos conectores están activos y otros inactivos, el **Status (Estado)** es **Partially Up (Parcialmente activo)** (naranja).
- Los conectores deshabilitados aparecen en gris.

 ©2025 Palo Alto Networks, Inc.



Estado de los conectores ZTNA

Vea un resumen de todos los conectores configurados, incluidos los destinos de aplicación asociados con el conector y el **Status (Estado)**.

Seleccione cualquier **Connector Name (Nombre del conector)** para ver detalles sobre los grupos de conectores asociados y los destinos de aplicación asociados a cada conector.

Ver y supervisar objetos de acceso de ZTNA Connector

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Obtenga visibilidad de sus aplicaciones privadas que se añadieron a través de los objetos de acceso de ZTNA Connector al ver datos como el número de aplicaciones agregadas por FQDN, subredes IP y comodines, el estado de conectividad de cada objeto de acceso y los grupos de conectores y conectores asociados con cada objeto de acceso. Al ver esta información, puede obtener una imagen general del estado y la conectividad de su implementación.

Las aplicaciones privadas en los centros de datos se conectan a Prisma Access a través de sus máquinas virtuales (VM) de Connector. Puede añadir aplicaciones basadas en estos objetos de acceso: FQDN, comodines FQDN o subredes IP.

- **FQDNs**: Prisma Access resuelve los FQDNs de las aplicaciones que incorpora a ZTNA Connector a las direcciones IP en el bloque de direcciones IP de la aplicación.

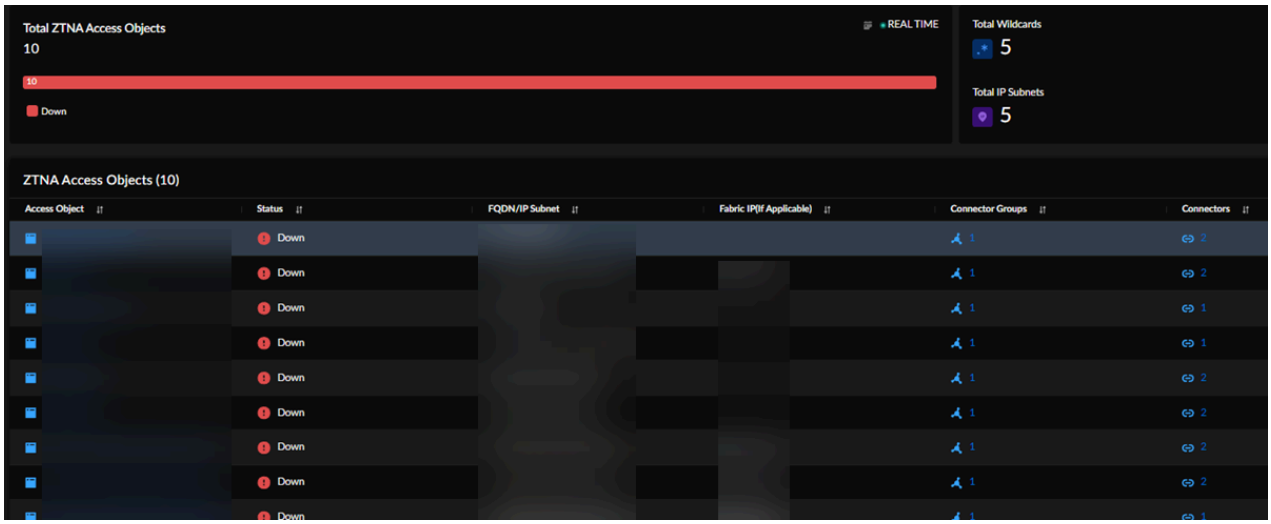
 ©2025 Palo Alto Networks, Inc.

- **Comodines**: para aplicaciones basadas en comodines, cree un grupo de conectores basado en FQDN y, a continuación, especifique el comodín que utilizará (por ejemplo, *.ejemplo.com) para el destino de la aplicación. Cuando los usuarios acceden a sitios que coinciden con el comodín, esas aplicaciones se incorporan automáticamente para acceder desde ZTNA Connector para sus usuarios móviles y usuarios de red remotos.
- **Subredes IP**: cree un grupo de conectores basado en subredes IP y, a continuación, introduzca la subred IP para usarla en el destino de la aplicación.

En Strata Cloud Manager, vaya a **Monitor (Supervisar)** > **Data Centers (Centros de datos)** > **ZTNA Access Objects (Objetos de acceso ZTNA)** para obtener visibilidad de los objetos de acceso a ZTNA Connector.

Todos los objetos de acceso

Vea **Total ZTNA Access Objects (Número total de objetos de acceso ZTNA)** para ver información sobre todos sus objetos de acceso al ZTNA Connector (FQDN, comodines y subredes IP) en tiempo real. El número en **Número total de objetos de acceso ZTNA** y la tabla **Objetos de ZTNA Access** deberá coincidir, lo que representa el número de aplicaciones FQDN, aplicaciones de subred y aplicaciones comodín descubiertas.



- Vea un gráfico de los **objetos de acceso total de ZTNA** en su entorno por Estado, lo que significa que los túneles seguros automatizados para el objeto de acceso están activo, parcialmente activo, inactivo o deshabilitado. Si el estado está inactivo, el conector asociado con este objeto de acceso no puede llegar a su aplicación.
  - **Activo**: todos los túneles están activos.
  - **Parcialmente activo**: algunos túneles están activos y otros inactivos o inhabilitados.
  - **Desactivo**: todos los túneles están inactivos.

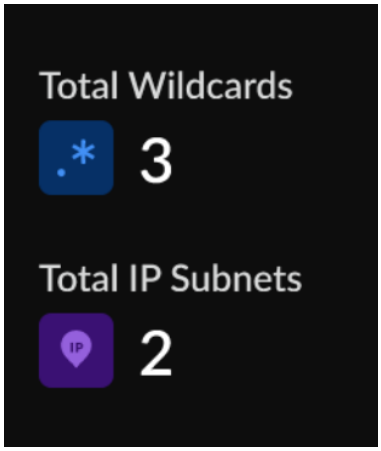
 ©2025 Palo Alto Networks, Inc.

- **Deshabilitado**: todos los túneles están deshabilitados.

Seleccione un cuadrado de color de estado en el widget **Número total de objetos de acceso ZTNA** para ordenar los objetos de acceso por estado en la tabla **Objetos de acceso ZTNA**.

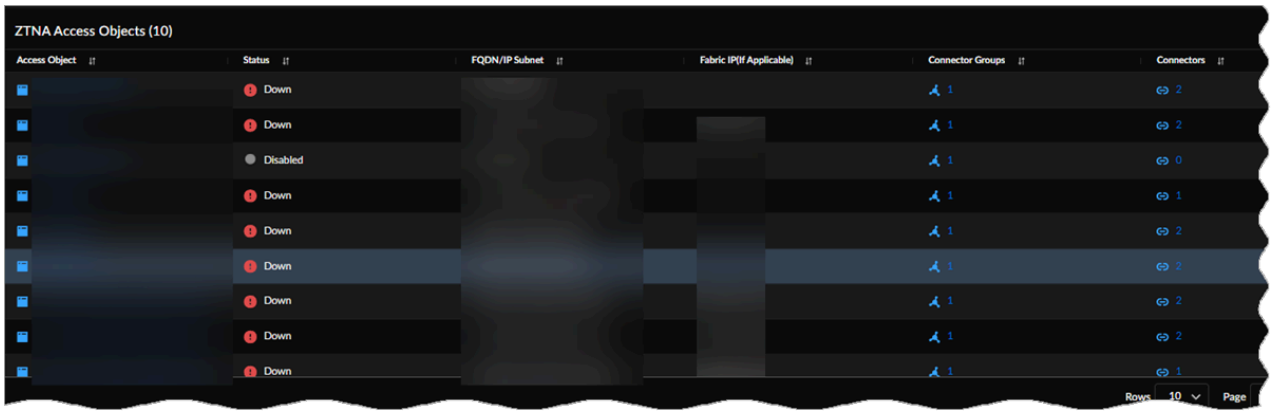


- El **Total Wildcards and Total IP Subnets (Total de comodines y total de subredes IP)** resume cuántas subredes IP y reglas de comodines ha incorporado. Este es el número de reglas comodín que has creado, que es un total diferente al número de aplicaciones descubiertas como resultado de la creación de estas reglas.



 ©2025 Palo Alto Networks, Inc.

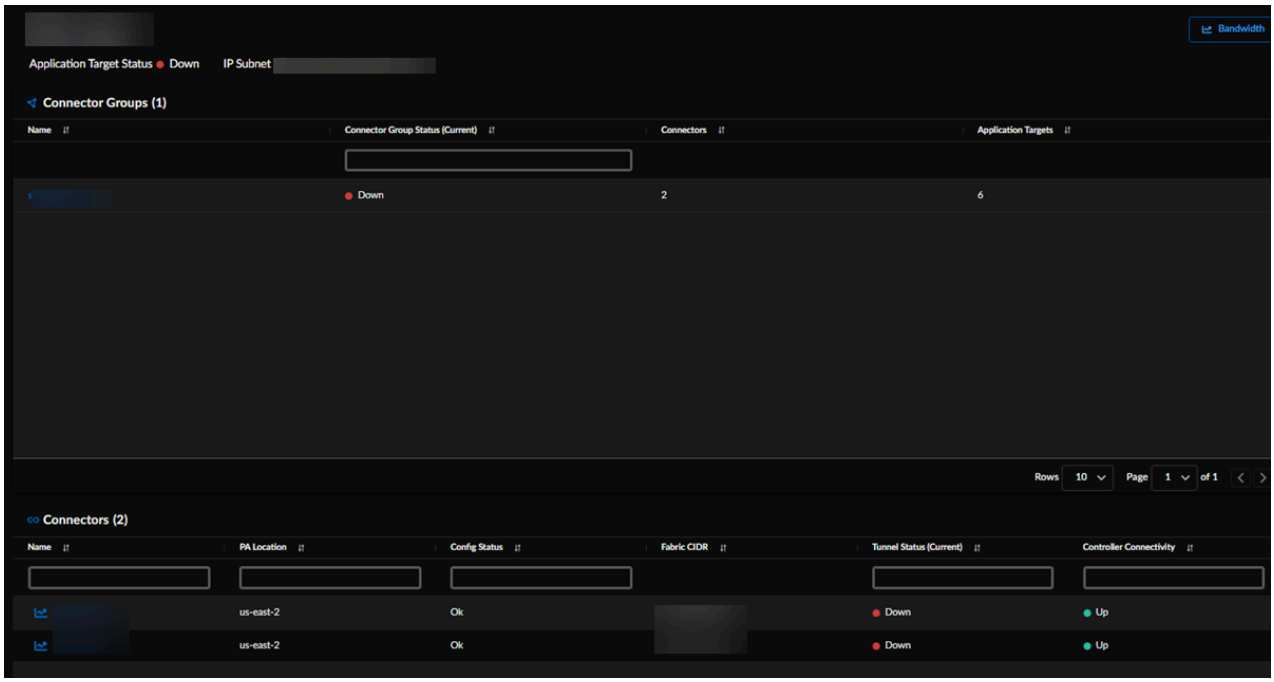
- **ZTNA Access Objects (Objetos de ZTNA Access)** proporciona información sobre todos sus objetos de acceso.
  - **Objeto de acceso**: seleccione un objeto de acceso específico para ver sus detalles.
  - **Estado**: el túnel seguro automatizado para el objeto de acceso es Activo, Parcialmente activo, Inactivo o Desactivado.
  - **Subred FQDN/IP**: la subred FQDN o IP utilizada para añadir este objeto de acceso.
  - **IP de tejido (si aplica)**: la IP del tejido asociado con este objeto de acceso.
  - **Grupos de conectores**: los grupos de conectores son agrupaciones lógicas de conectores y aplicaciones. Vea los grupos de conectores asociados con un objeto de acceso.
  - **Conectores**: los conectores representan las máquinas virtuales que se ejecutan en los centros de datos que se conectan a Prisma Access. Ver los conectores asociados a un objeto de acceso.



Seleccione cualquier **Access Object (Objeto de acceso)** para ver sus detalles.

- **Grupos de conectores**: vea cuántos grupos de conectores están asociados con este objeto de acceso. Seleccione un grupo de conectores para ver información sobre sus Conexiones de servicio.
- **Estado del grupo conector (actual)**: activo, parcialmente activo, desactivado o deshabilitado.
- **Conectores**: número de conectores en este grupo de conectores.
- **Objetivos de aplicación**: número de objetivos de aplicación en este grupo de conectores.
- **Bandwidth (Ancho de banda)**: seleccione el botón **Bandwidth (Ancho de banda)** para ver la información de ancho de banda de este objeto de acceso.

 ©2025 Palo Alto Networks, Inc.



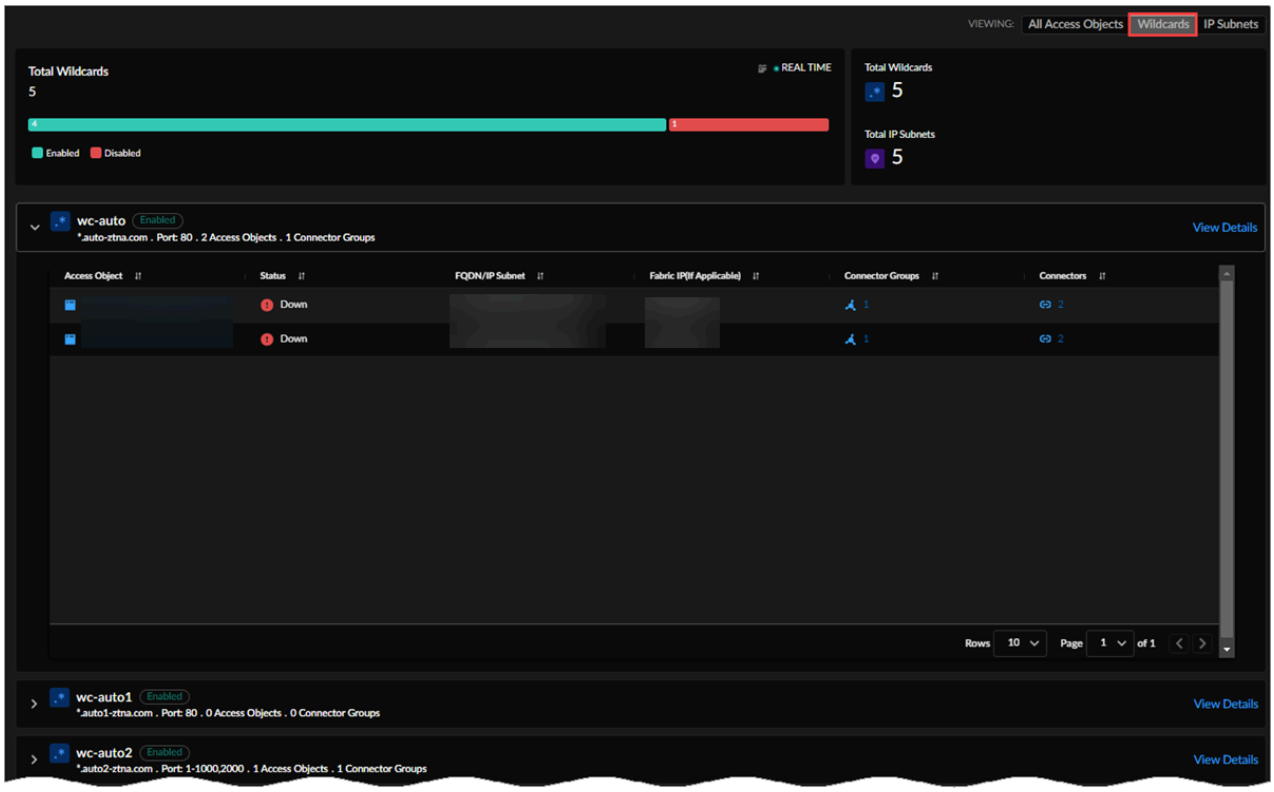
Seleccione cualquiera de los **Connectors (Conectores)** de un objeto de acceso para ver sus detalles.

- **Ubicación de PA (Prisma Access)**: la ubicación de Prisma Access asociada con cada conector.
- **Estado de configuración**: el estado de configuración del conector es OK o Error. Si el estado es Error, ZTNA Connector no ha terminado de incorporarse.
- **CIDR de tejido**: el CIDR de tejido asociado con este conector.
- **Estado del túnel (actual)**: el estado del túnel seguro automatizado para este conector.
- **Conectividad del controlador**: activo, parcialmente activo, inactivo o deshabilitado.

Comodines

Seleccione **Wildcards (Comodines)** para ver sus objetos de acceso comodín. Consulte **Total Wildcards (Total de comodines)** por estado y el número **Total Wildcards (Total de comodines)** y **Total IP Subnets (Total subredes de IP)**.

 ©2025 Palo Alto Networks, Inc.



Seleccione la flecha junto a un comodín o seleccione **View Details (Ver detalles)** para obtener información sobre los objetos de acceso que componen este comodín.

- **Objeto de acceso**: seleccione un objeto de acceso específico para ver sus detalles.
- **Estado**: el túnel seguro automatizado para el objeto de acceso es Activo, Parcialmente activo, Inactivo o Desactivado.
- **Subred FQDN/IP**: la subred FQDN o IP utilizada para añadir este objeto de acceso.
- **IP de tejido (si aplica)**: la IP del tejido asociado con este objeto de acceso.
- **Grupos de conectores**: los grupos de conectores son agrupaciones lógicas de conectores y aplicaciones. Vea los grupos de conectores asociados con un objeto de acceso.
- **Conectores**: los conectores representan las máquinas virtuales que se ejecutan en los centros de datos que se conectan a Prisma Access. Ver los conectores asociados a un objeto de acceso.



Seleccione cualquier **Access Object (Objeto de acceso)** para ver sus detalles.

- **Grupos de conectores**: vea cuántos grupos de conectores están asociados con este objeto de acceso. Seleccione un grupo de conectores para ver información sobre sus Conexiones de servicio.
- **Estado del grupo conector (actual)**: activo, parcialmente activo, desactivado o deshabilitado.
- **Conectores**: número de conectores en este grupo de conectores.

 ©2025 Palo Alto Networks, Inc.

- **Objetivos de aplicación**: número de objetivos de aplicación en este grupo de conectores.
- **Bandwidth (Ancho de banda)**: seleccione el botón **Bandwidth (Ancho de banda)** para ver la información de ancho de banda de este objeto de acceso.

Seleccione **Connector Groups (Grupos de conectores)** o **Connectors (Conectores)** para ver los grupos de conectores o conectores únicos asociados con los objetos de acceso en el comodín.

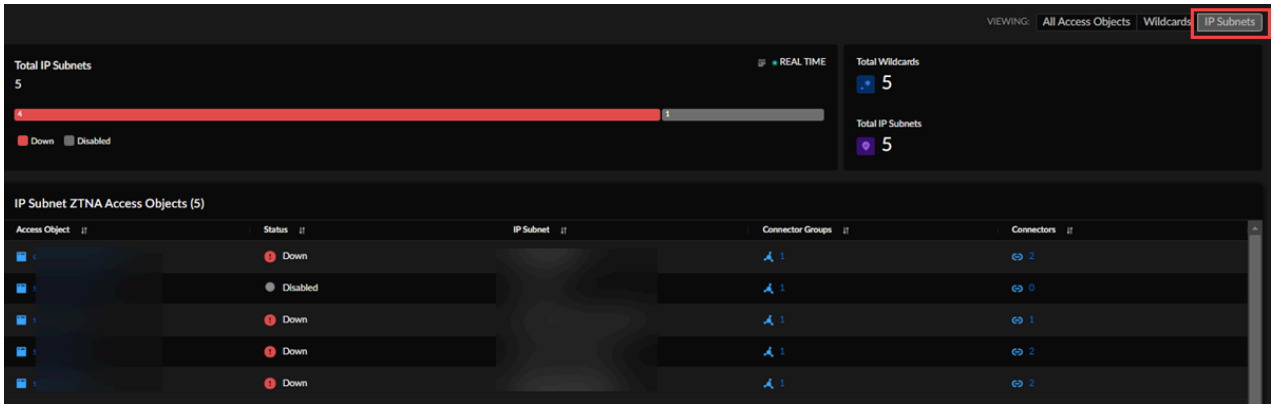
Subredes IP

Seleccione **IP Subnets (Subredes IP)** para ver el total de objetos de acceso a la subred IP. Un objeto de acceso a la subred IP consiste en una agrupación de varias aplicaciones diferentes.

Vea las **subredes IP totales** de su entorno por estado (Activa, parcialmente activa, inactiva o deshabilitada).

IP Subnet ZTNA Access Objects (Objetos de acceso ZTNA de subred IP) proporciona información sobre todos sus objetos de acceso.

- - **Objeto de acceso**: seleccione un objeto de acceso específico para ver sus detalles.
  - **Status (Estado)** : Activo, parcialmente activo, Inactivo o Deshabilitado.
  - **Subred IP**: la subred IP utilizada para añadir este objeto de acceso.
  - **Grupos de conectores**: los grupos de conectores son agrupaciones lógicas de conectores y aplicaciones. Ver los grupos de conectores asociados con un objeto de acceso.
  - **Conectores**: los conectores representan las máquinas virtuales que se ejecutan en los centros de datos y que se conectan a Prisma Access. Ver los conectores asociados a un objeto de acceso.



Seleccione cualquier **Access Object (Objeto de acceso)** para ver sus detalles.

- **Grupos de conectores**: vea cuántos grupos de conectores están asociados con este objeto de acceso. Seleccione un grupo de conectores para ver información sobre sus Conexiones de servicio.
- **Estado del grupo conector (actual)**: activo, parcialmente activo, desactivado o deshabilitado.
- **Conectores**: número de conectores en este grupo de conectores.
- **Objetivos de aplicación**: número de objetivos de aplicación en este grupo de conectores.
- **Bandwidth (Ancho de banda)**: seleccione el botón **Bandwidth (Ancho de banda)** para ver la información de ancho de banda de este objeto de acceso.

 ©2025 Palo Alto Networks, Inc.

Seleccione **Connector Groups (Grupos de conectores)** o **Connectors (Conectores)** para ver los grupos de conectores o conectores únicos asociados con los objetos de acceso en la subred IP.

Ver y supervisar los servicios de red

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Esta es una característica de Prisma Access Insights.

Puede ver el rendimiento de los servicios de red comunes que afectan su experiencia del usuario al acceder a las aplicaciones. Los servicios de red incluyen la notificación del número de autenticaciones correctas o fallidas de GlobalProtect como medida de la capacidad de conexión de los usuarios móviles a Prisma Access, y visualizaciones de las solicitudes y respuestas de proxy DNS reenviadas a los servidores durante un intervalo de tiempo que especifique.

Autenticación de GlobalProtect

Vaya a **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **GlobalProtect Authentication (Autenticación de GlobalProtect)** en Strata Cloud Manager para ver los las autenticaciones correctas y fallidas de GlobalProtect que afectan a su entorno.

- Establezca el filtro de **Time Range (Intervalo de tiempo)** para revisar los datos de los servicios de red para ese intervalo de tiempo.
- Especifique una **Prisma Access Location (Ubicación de Prisma Access)** para ver el éxito de la autenticación, el número total de fallos y los fallos de tiempo de espera en el intervalo de tiempo seleccionado.

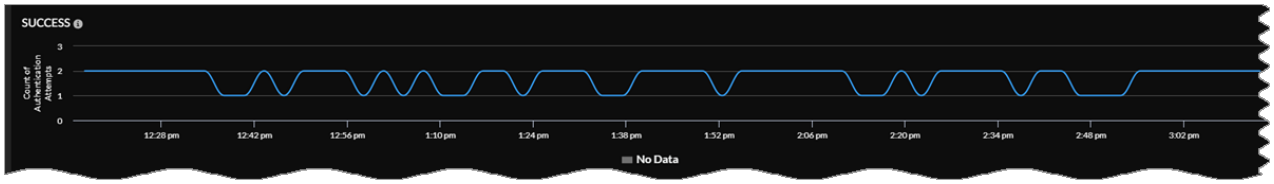
Los datos representan cuántos usuarios móviles en un momento dado intentan autenticarse en un portal de GlobalProtect, que luego envía las credenciales de los usuarios móviles para su verificación a un servidor de directorio activo (AD) local, lo que da como resultado un error de autenticación o una autenticación correcta. Si ve un gran número de errores de autenticación, puede correlacionar los errores con un evento de red que indique un problema con una ubicación determinada o con un servidor de autenticación local que estaba inactivo. Los datos de estos gráficos proporcionan información sobre la solución de problemas para los administradores de red que resuelven problemas de red. Puede ver el recuento de tendencias de autenticaciones realizadas correctamente o de fallos para los usuarios móviles en los portales y puertas de enlace de GlobalProtect, utilizar estos datos para conocer los patrones de autenticaciones correctas o fallidas a lo largo del tiempo y establecer rangos de recuento que pueden ser normales o anómalos en su implementación de Prisma Access. Por ejemplo, los recuentos anómalos podrían indicar la incapacidad de los usuarios existentes para conectarse a Prisma Access debido a problemas de disponibilidad con los portales de GlobalProtect o servidores de autenticación lentos. O bien, los recuentos anómalos pueden representar un gran número de usuarios incorporados a la red del cliente todos a la vez.

Autenticaciones de GlobalProtect realizadas correctamente

Ver detalles sobre los recuentos de autenticaciones realizadas correctamente para GlobalProtect para diferentes ubicaciones. Pase el cursor sobre cualquier punto del gráfico para ver detalles

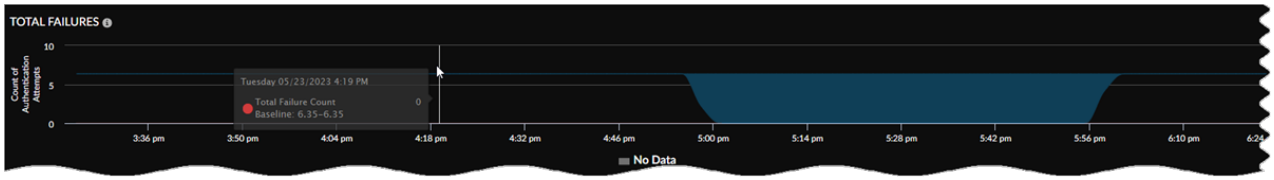
 ©2025 Palo Alto Networks, Inc.

sobre los recuentos de usuarios para autenticaciones llevadas a cabo correctamente en diferentes sitios de ubicaciones de Prisma Access que se muestran en un momento determinado.



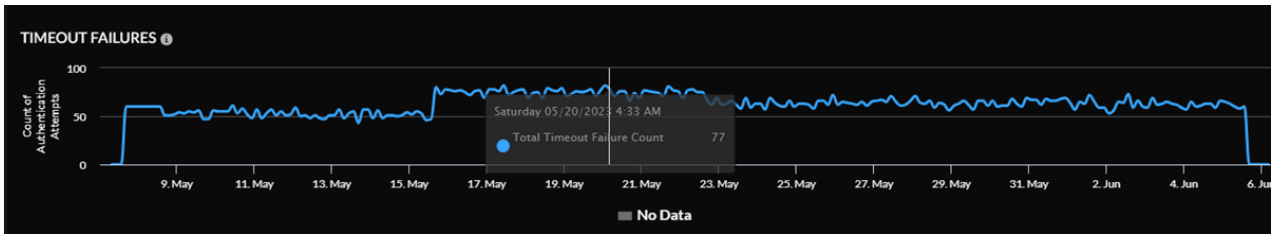
Número total de fallos de autenticación de GlobalProtect

Ver detalles sobre los recuentos de autenticaciones fallidas para GlobalProtect para diferentes ubicaciones. Pase el cursor sobre cualquier punto del gráfico para ver detalles sobre los recuentos de usuarios por autenticaciones fallidas en diferentes sitios de ubicaciones de Prisma Access que se muestran, como EE. UU. Este y Canadá Este, en un momento determinado.



Fallos de tiempo de espera de autenticación de GlobalProtect

Ver detalles sobre el recuento de autenticaciones fallidas para GlobalProtect para diferentes ubicaciones. Pase el cursor sobre cualquier punto del gráfico para ver detalles sobre los recuentos de usuarios por autenticaciones fallidas en diferentes sitios de ubicaciones de Prisma Access que se muestran, como EE. UU. Este y Canadá Este, en un momento determinado.



DNS:

Vaya a **Monitor (Supervisar)** > **Network Services (Servicios de red)** > **GlobalProtect Authentication (Autenticación de GlobalProtect)** en Strata Cloud Manager para ver las solicitudes y respuestas de proxy DNS reenviadas a los servidores durante un intervalo de tiempo que especifique.

Los filtros que puede usar son:

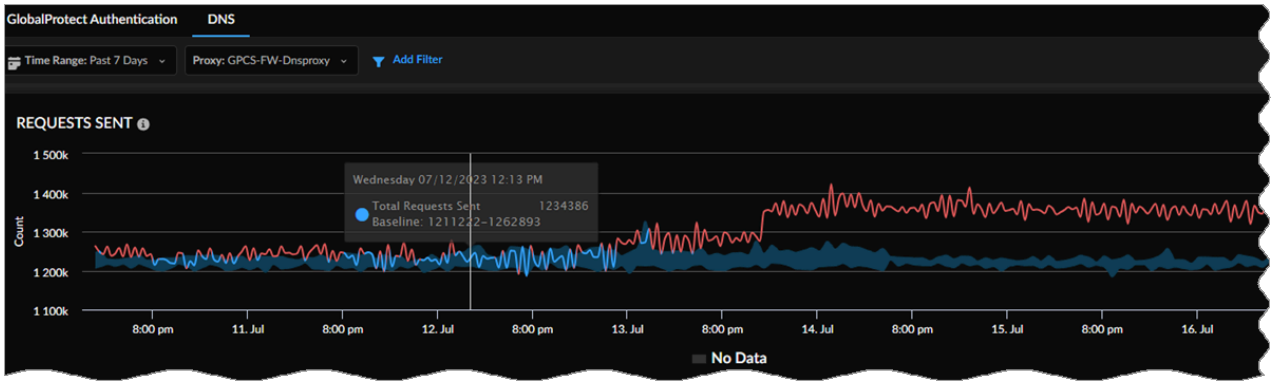
- **Intervalo de tiempo**
- **Nombres de proxy DNS**

Los valores del filtro de proxy DNS están relacionados con los últimos 30 días y se seleccionan automáticamente al cargar (es decir, si no hay datos de proxy explícito, no hay ningún filtro de proxy explícito). Pase el cursor sobre el gráfico para ver detalles sobre todas las **Requests Sent (Solicitudes enviadas)** y **Requests Received (Solicitudes recibidas)** de servidores proxy DNS en un momento específico.

 ©2025 Palo Alto Networks, Inc.

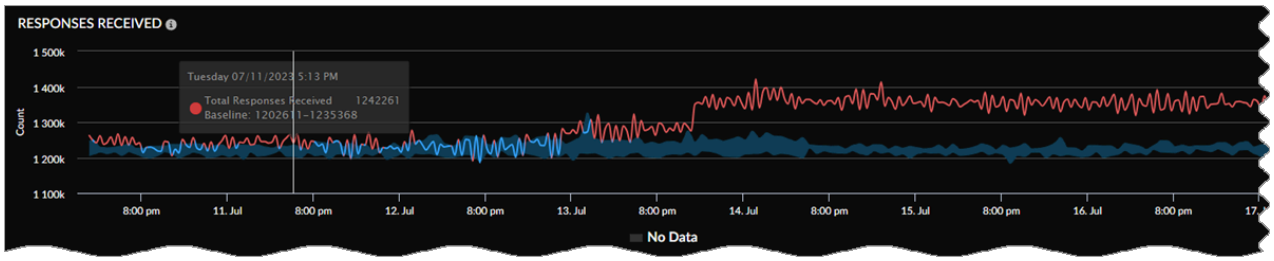
Solicitudes enviadas

Vea las solicitudes de red y las consultas reenviadas a los servidores durante el rango de tiempo que especifique. Pase el cursor sobre cualquier punto del gráfico para ver información sobre las solicitudes enviadas a los servidores proxy DNS en ese momento. Si seleccionó un nombre de proxy para filtrar, verá los datos de ese proxy.



Respuestas recibidas

Vea el número total de respuestas recibidas entre los inquilinos durante el rango de tiempo que especifique. Pase el cursor sobre cualquier punto del gráfico para ver información sobre las respuestas recibidas en ese momento. Si seleccionó un nombre de proxy para filtrar, verá los datos de ese proxy.



Ver y supervisar los servicios de red: Autenticación de GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Esta es una característica de Prisma Access Insights.

Los servicios de red incluyen informar el número de autenticaciones de GlobalProtect realizados correctamente o que fallaron, como una medida de la capacidad de los usuarios móviles para conectarse a Prisma Access. Seleccione**Monitor (Supervisar)** > **Network Services (Servicios de red)** > **GlobalProtect Authentication (Autenticación GlobalProtect)** en Strata Cloud Manager para comenzar.

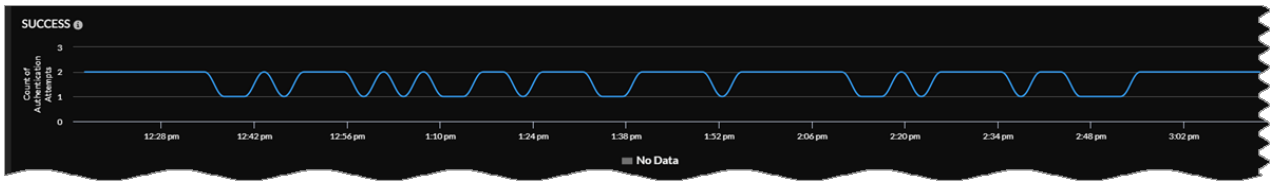
- Establezca el filtro de **Time Range (Intervalo de tiempo)** para revisar los datos de los servicios de red para ese intervalo de tiempo.

 ©2025 Palo Alto Networks, Inc.

- Especifique una **Prisma Access Location (Ubicación de Prisma Access)** para ver el éxito de la autenticación, el número total de fallos y los fallos de tiempo de espera en el intervalo de tiempo seleccionado.

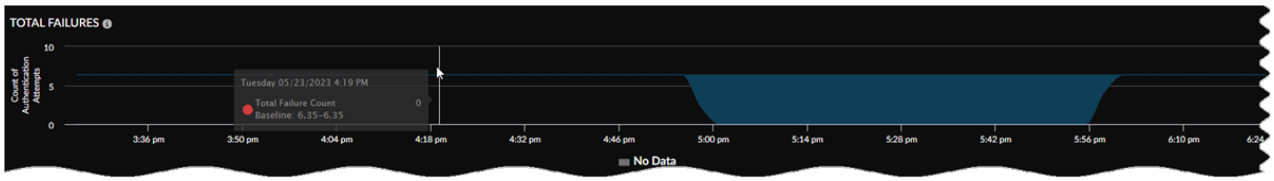
Autenticaciones de GlobalProtect realizadas correctamente

Ver detalles sobre los recuentos de autenticaciones realizadas correctamente para GlobalProtect para diferentes ubicaciones. Pase el cursor sobre cualquier punto del gráfico para ver detalles sobre los recuentos de usuarios para autenticaciones llevadas a cabo correctamente en diferentes sitios de ubicaciones de Prisma Access que se muestran en un momento determinado.



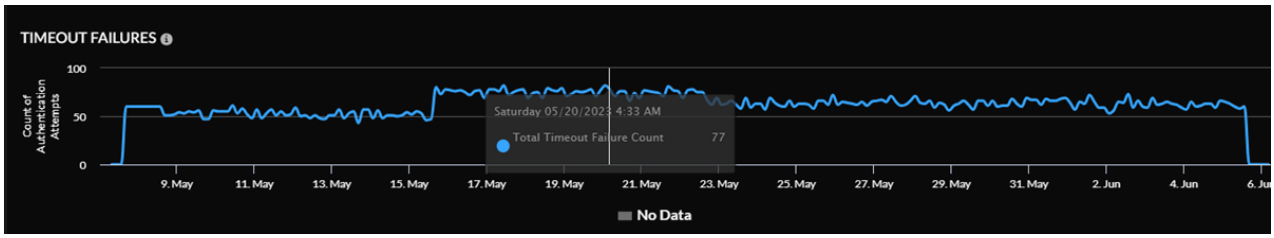
Número total de fallos de autenticación de GlobalProtect

Ver detalles sobre los recuentos de autenticaciones fallidas para GlobalProtect para diferentes ubicaciones. Pase el cursor sobre cualquier punto del gráfico para ver detalles sobre los recuentos de usuarios por autenticaciones fallidas en diferentes sitios de ubicaciones de Prisma Access que se muestran, como EE. UU. Este y Canadá Este, en un momento determinado.



Fallos de tiempo de espera de autenticación de GlobalProtect

Ver detalles sobre los recuentos de autenticaciones fallidas para GlobalProtect para diferentes ubicaciones. Pase el cursor sobre cualquier punto del gráfico para ver detalles sobre los recuentos de usuarios por autenticaciones fallidas en diferentes sitios de ubicaciones de Prisma Access que se muestran, como EE. UU. Este y Canadá Este, en un momento determinado.



Ver y supervisar los servicios de red: DNS:

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Este es una función de Prisma Access Insights.

 ©2025 Palo Alto Networks, Inc.

Servicios de red: DNS muestra las solicitudes y respuestas del proxy DNS reenviadas a los servidores durante un intervalo de tiempo que usted especifique.

Filtros que puede utilizar:

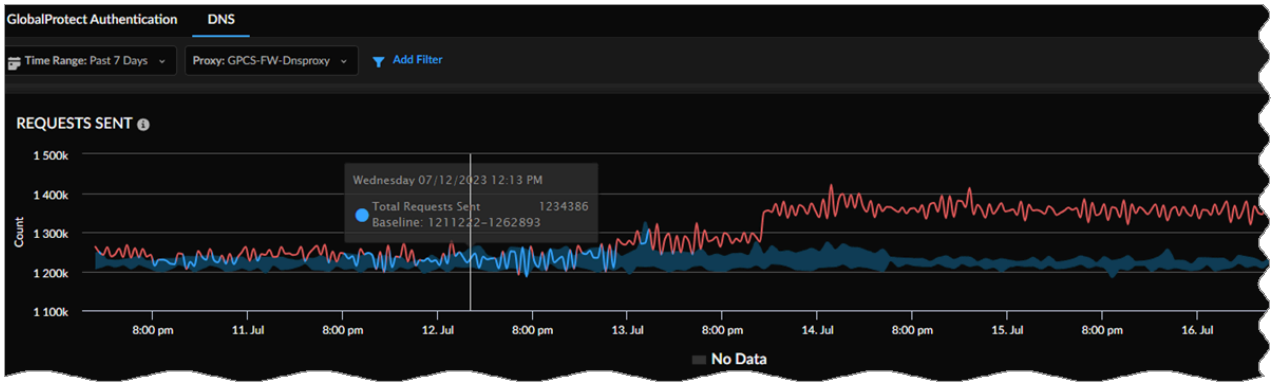
- **Intervalo de tiempo**
- **Nombres de proxy DNS**

Los valores del filtro de proxy DNS están relacionados con los últimos 30 días y se seleccionan automáticamente al cargar (es decir, si no hay datos de proxy explícito, no hay ningún filtro de proxy explícito).

Pase el cursor sobre el gráfico para ver detalles sobre todas las **Requests Sent (Solicitudes enviadas)** y **Requests Received (Solicitudes recibidas)** de servidores proxy DNS en un momento específico.

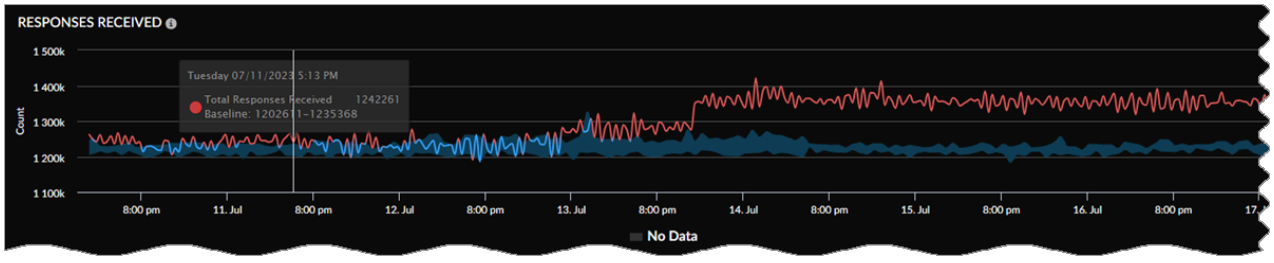
Solicitudes enviadas

Vea las solicitudes de red y las consultas reenviadas a los servidores durante el rango de tiempo que especifique. Pase el cursor sobre cualquier punto del gráfico para ver información sobre las solicitudes enviadas a los servidores proxy DNS en ese momento. Si seleccionó un nombre de proxy para filtrar, verá los datos de ese proxy.



Respuestas recibidas

Vea el número total de respuestas recibidas entre los inquilinos durante el rango de tiempo que especifique. Pase el cursor sobre cualquier punto del gráfico para ver información sobre las respuestas recibidas en ese momento. Si seleccionó un nombre de proxy para filtrar, verá los datos de ese proxy.

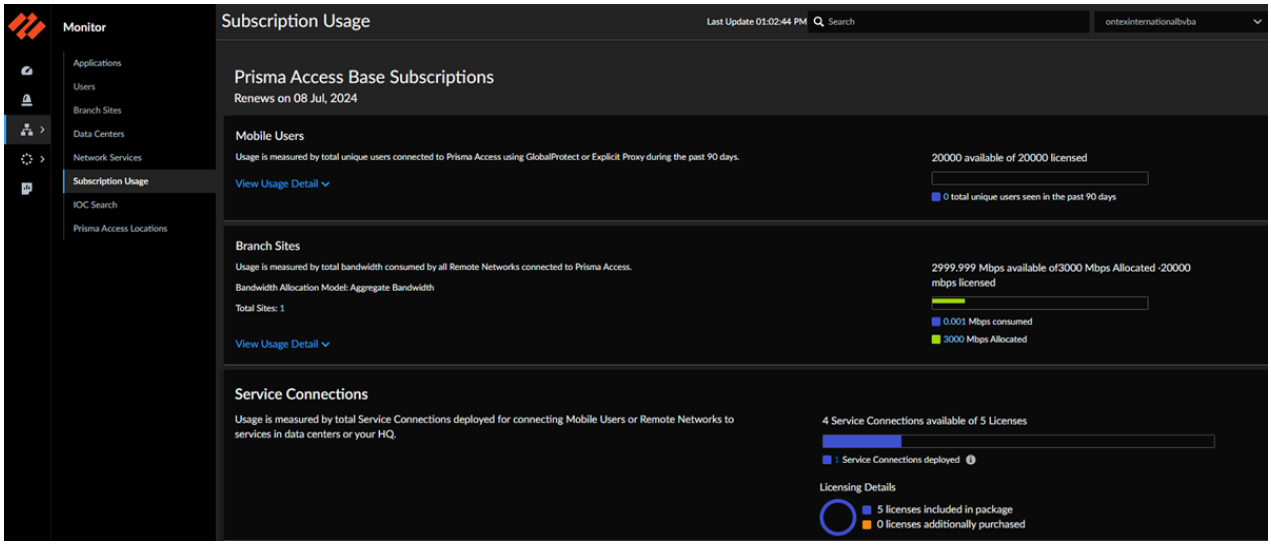


 ©2025 Palo Alto Networks, Inc.

Ver uso de suscripciones

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Seleccione **Monitor (Supervisar)** > **Subscription Usage (Uso de suscripciones)** para ver detalles sobre sus **Prisma Access Base Subscriptions (Suscripciones base de Prisma Access)**, incluyendo cuántas licencias ha consumido hasta ahora.

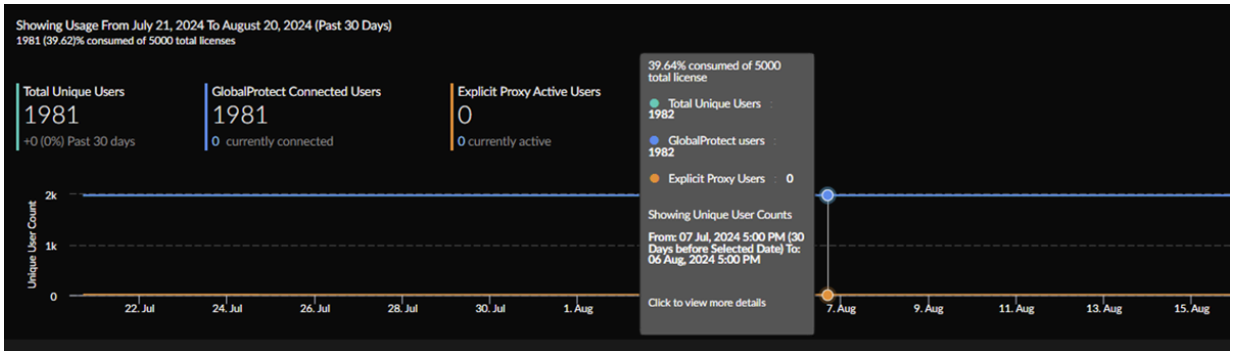


- **Mobile Users (Usuarios móviles)**: vea cuántas licencias de **Mobile Users (Usuarios móviles)** únicas ha consumido hasta ahora. El widget muestra el número total de licencias consumidas por usuarios móviles únicos conectados a Prisma Access en los últimos 30 días, porque las licencias se basan en los últimos 30 días de datos de inicio de sesión de Prisma Access. Un usuario que haya iniciado sesión en Prisma Access al menos una vez en los últimos 30 días contribuye al consumo de una licencia de usuario móvil.

  Seleccione **View Usage Detail (Ver detalles de uso)** para ver detalles sobre el uso de la licencia durante los últimos 30 días. Puede ver el número total de usuarios únicos durante los últimos

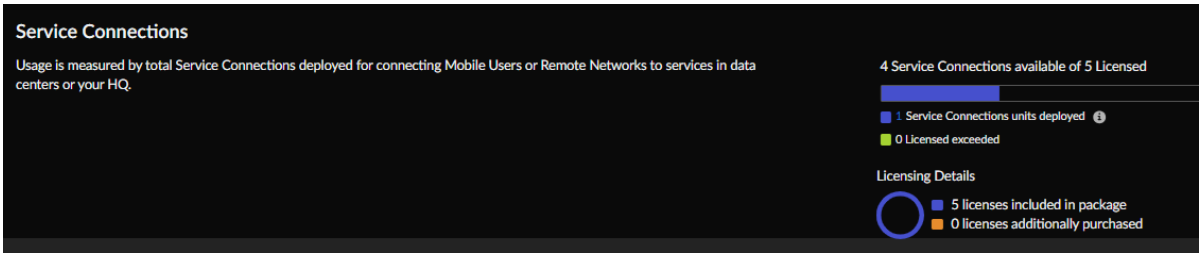
 ©2025 Palo Alto Networks, Inc.

30 días, el total de usuarios conectados a GlobalProtect y el total de usuarios activos del Proxy explícito. Pase el ratón sobre el gráfico para ver las licencias consumidas en ese momento.



- **Branch Sites (Sucursales)**: Consulte el uso total del ancho de banda de todas las redes remotas conectadas a Prisma Access. Consulte cuánto ancho de banda has asignado y cuánto ha consumido, en Mbps. Puede ver el uso del ancho de banda total consumido por todas las redes remotas conectadas a Prisma Access.

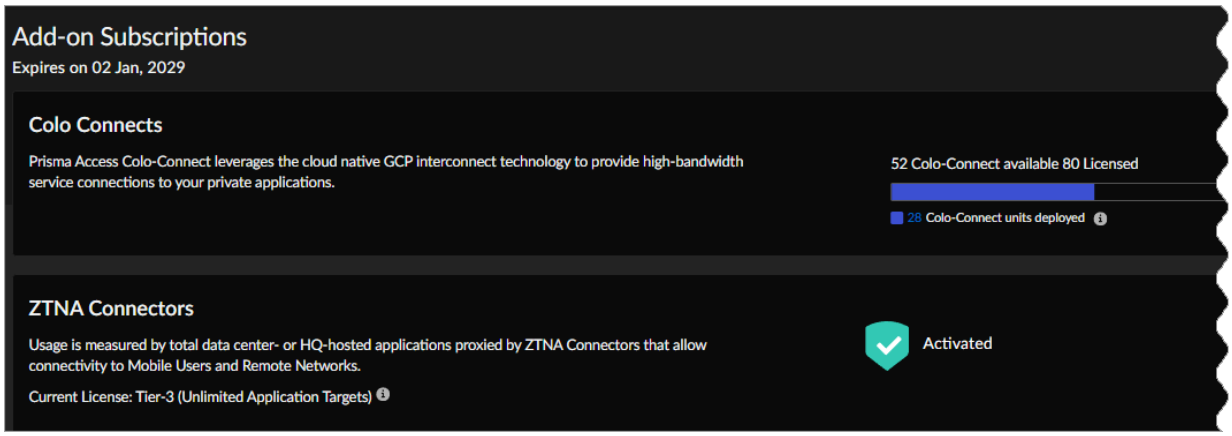
  Seleccione **View Usage Detail (Ver detalle de uso)** para ver su consumo de ancho de banda con licencia por Regiones de cómputo o sucursales según su Modelo de asignación de ancho de banda. En cada caso, se indica un valor de consumo de ancho de banda máximo diario para cada uno de los 30 días considerados para el cálculo de la licencia. Puedes filtrar la vista del gráfico seleccionando Regiones de Cómputo o sitios de sucursales. Se trazan tres líneas por Región de cómputo o por sitio en el gráfico que indican los valores de consumo máximo diario, el ancho de banda asignado a la Región de cómputo o sitio, y el valor del percentil 95 obtenido de los picos diarios.
- **Service Connections (Conexiones de servicio)**: vean cuantas licencias de **Service Connections (Conexiones de servicio)** ha consumido hasta ahora.



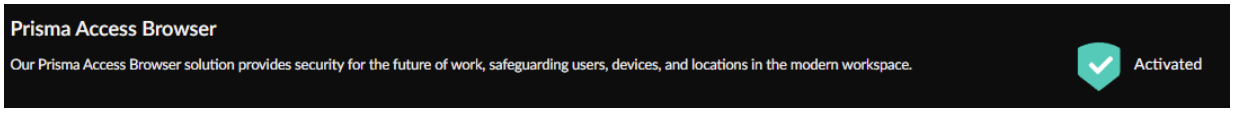
Consulte la sección de **Add-On Subscriptions (Suscripciones de complementos)** en esta página para ver las licencias adicionales que ha comprado. Puede ver el número total de licencias compradas, así como el número de licencias no consumidas hasta ahora. Las siguientes imágenes describen algunas de las licencias adicionales que puedes comprar.

 ©2025 Palo Alto Networks, Inc.

- **Colo-Connects**: Prisma Access Colo-Connect aprovecha la tecnología GCP nativa de la nube para proporcionar conexiones de servicio de gran ancho de banda a sus aplicaciones privadas.



- **Prisma Access Browser**: Prisma Access Secure Enterprise Browser (Prisma Access Browser) es la única solución que protege tanto dispositivos gestionados como no gestionados a través de un navegador empresarial integrado de forma nativa que extiende la protección a dispositivos no gestionados. Prisma Access Browser protege las aplicaciones y datos empresariales al colocar la seguridad en el navegador. Su suscripción de Prisma Access Browser aparece en las **Add-on Subscriptions (Suscripciones de complementos)** o en las **Prisma Access Base Subscriptions (Suscripciones base de Prisma Access)**.
  - **Prisma Access Base Subscriptions (Suscripciones básicas a Prisma Access)**: el inquilino tiene una licencia independiente de Prisma Access Browser.
  - **Add-on Subscriptions (Suscripciones de complementos)**: cuando haya comprado la licencia de Prisma Access Browser para todos los usuarios móviles, la suscripción de Prisma Access Browser estará **Activated (Activada)**.



Ver y supervisar ubicaciones de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Esta es una característica de Prisma Access Insights.

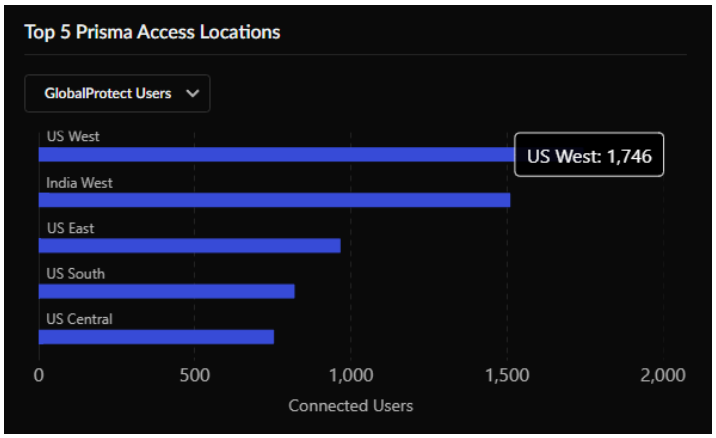
Seleccione **Monitor (Supervisar)** > **Prisma Access Locations (Ubicaciones de Prisma Access)** para ver una visión general del estado de todas las ubicaciones de Prisma Access para sus redes remotas y usuarios móviles.

Top 5 ubicaciones de Prisma Access

Las barras muestran datos sobre las 5 ubicaciones de Prisma Access principales para redes remotas, conexiones de servicio, usuarios móviles de GlobalProtect o usuarios móviles de Proxy

 ©2025 Palo Alto Networks, Inc.

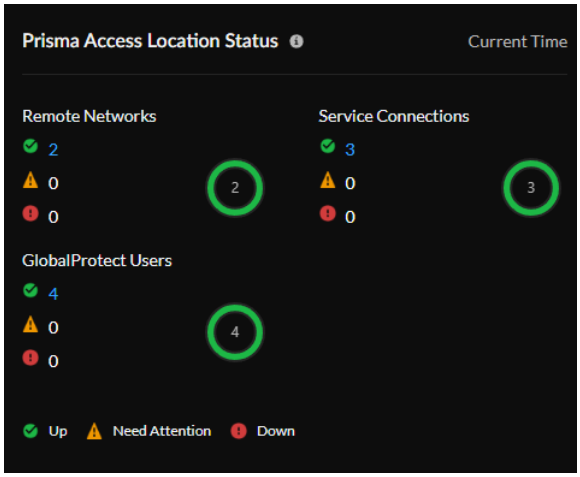
explícito (seleccionados en el menú desplegable), según el ancho de banda total consumido durante el intervalo de tiempo seleccionado. Pase el ratón sobre cualquier barra para ver cuántos usuarios hay en esa ubicación en particular.



Estado de la ubicación de Prisma Access

Dependiendo de su licencia, este widget muestra el número de sitios de red remotos conectados, sitios de conexión de servicio, usuarios únicos de GlobalProtect y usuarios únicos de Proxy explícito conectados a Prisma Access. El código de color del widget se basa en cuántas redes remotas, conexiones de servicio, usuarios de GlobalProtect y usuarios de proxy explícito se encuentran en el siguiente estado:

- **Connected (Conectada)** (verde): todas las ubicaciones de Prisma Access están conectadas.
- **Disconnected (Desconectada)** (rojo): todas las ubicaciones de Prisma Access están desconectadas.
- **Partially Connected (Parcialmente conectado)** (naranja): una o más ubicaciones de Prisma Access están desconectadas.



Conectividad de Strata Logging Service

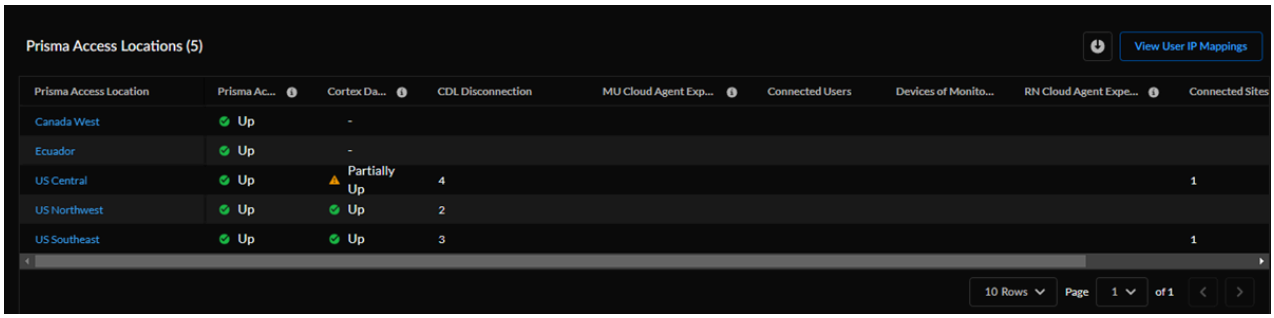
El widget **Strata Logging Service Connectivity (Conectividad)** le da visibilidad del estado de conectividad del Strata Logging Service desde todas las instancias de Prisma Access de la región de Strata Logging Service que seleccionó durante la activación de la licencia de Prisma Access. Le ayuda a determinar si los cortafuegos se han desconectado de Strata Logging Service y

 ©2025 Palo Alto Networks, Inc.

ya no está obteniendo logs de cortafuegos. Cada inquilino puede conectarse a un solo Strata Logging Service en cualquier región de su elección. Prisma Access sondea la base de datos de Strata Logging Service cada 5 minutos para comprobar la conectividad entre los nodos (usuarios móviles, redes remotas y conexiones de servicio) y la base de datos de Strata Logging Service.

Estado de ubicaciones de Prisma Access

Ver el estado de las **Prisma Access Locations (Ubicaciones de Prisma Access)** en tiempo real. Dentro de una ubicación específica, si un usuario inicia sesión desde varios hosts, el usuario se cuenta como un solo usuario, pero si algún usuario inicia sesión desde dos ubicaciones diferentes de Prisma Access al desconectarse de una e iniciar sesión desde otra dentro del período de tiempo, el usuario se cuenta como dos usuarios. Seleccione una ubicación para ver detalles, como el ancho de banda consumido, el estado, la conectividad de Strata Logging Service y las asignaciones de ID de usuario y de grupo.



Ver y supervisar ID de dispositivos de terceros

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ Licencia de Prisma Access

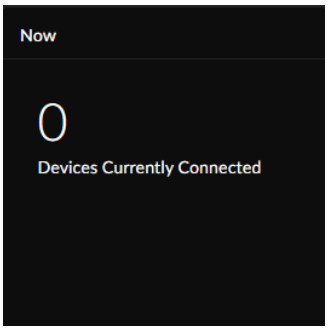
Puede utilizar Cloud Identity Engine con Prisma Access para aplicar información de fuentes de detección de IoT de terceros a fin de simplificar la tarea de identificar y cerrar las brechas de seguridad de los dispositivos de su red. Consulte Configurar ID de dispositivo de terceros en Prisma Access para obtener más detalles sobre la configuración.

Vaya a **Monitor (Supervisar)** > **Devices (Dispositivos)** > **IOT** para obtener información sobre sus dispositivos IoT; como el número de dispositivos IoT conectados en los últimos 30 minutos, todos los dispositivos IoT conectados durante el intervalo de tiempo seleccionado y detalles sobre todos los dispositivos IoT conectados.

Dispositivos actualmente conectados

Vea el número de dispositivos conectados, si los hay, en los últimos 30 minutos. **Ahora** siempre muestra los **Dispositivos actualmente conectados** solo en los últimos 30 minutos.

 ©2025 Palo Alto Networks, Inc.

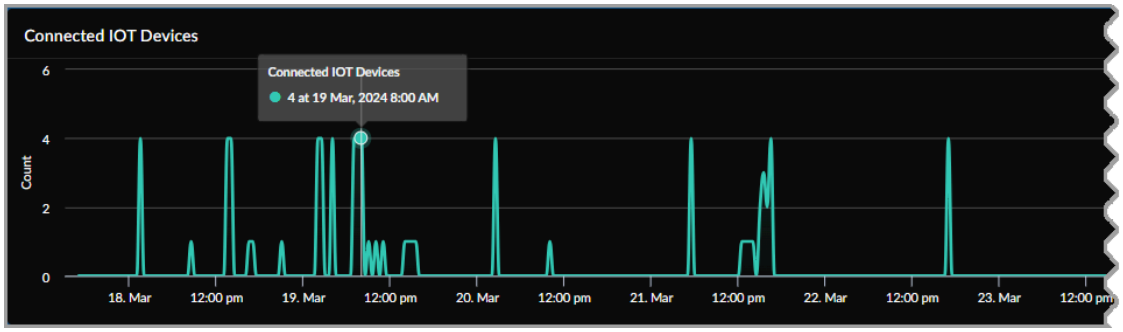


Dispositivos IoT conectados

Dispositivos IoT conectados muestra el número de dispositivos conectados filtrados por **Time Range (Intervalo de tiempo)**. Personalice los datos que se muestran seleccionando otras opciones de filtro en el menú desplegable **Add Filters (Añadir filtros)**.

- **Category (Categoría)**: la categoría a la que pertenece este dispositivo.
- **Mac Address (Dirección Mac)**: la dirección MAC del dispositivo.
- **Profile (Perfil)**: el perfil del dispositivo.
- **Vendor (Proveedor)**: el proveedor del dispositivo.
- **Source IP (IP de origen)**: la dirección IP del dispositivo.
- **Ubicación de Prisma Access**: la ubicación de Prisma Access del dispositivo.
- **Branch Site (Sucursal)**: el sitio de la sucursal donde se encuentra el dispositivo.

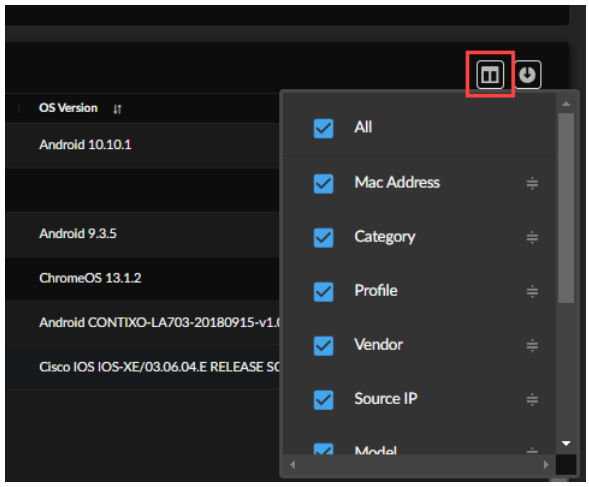
Pase el cursor sobre un punto del gráfico para ver el número de usuarios en un momento específico. Conocer las tendencias de los usuarios durante un período de tiempo específico puede ayudarle a supervisar el uso e investigar cualquier patrón inusual.



Dispositivos de IoT

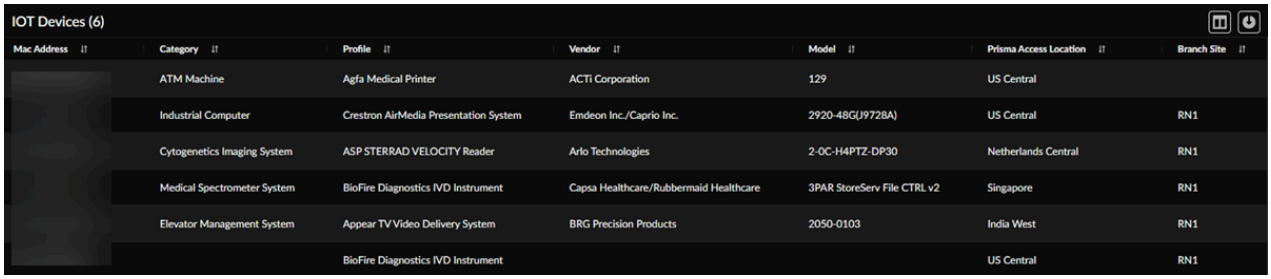
Vea el número de dispositivos IoT conectados durante el **Time Range (Intervalo de tiempo)** seleccionado. Utilice el menú desplegable de columnas para seleccionar o anular la selección de las columnas que aparecen en la tabla.

 ©2025 Palo Alto Networks, Inc.



- **Mac Address (Dirección Mac)**: la dirección MAC del dispositivo.
- **Category (Categoría)**: la categoría a la que pertenece este dispositivo.
- **Profile (Perfil)**: el perfil del dispositivo.
- **Proveedor**: Proveedor del dispositivo.
- **IP de origen**: dirección IP del dispositivo.
- **Modelo**: modelo de dispositivo.
- **Versión del SO**: versión del SO.
- **Familia de SO**: la familia de SO a la que pertenece el dispositivo.
- **Ubicación de Prisma Access**: la ubicación de Prisma Access utilizada.
- **Branch Site (Sucursal)**: el sitio de la sucursal donde se encuentra el dispositivo.

La siguiente tabla de dispositivos IOT muestra una selección de columna personalizada. Para mostrar todas las columnas de la tabla, seleccione todas las opciones en el desplegable.



Ver y supervisar el Aislamiento remoto del navegador

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.0 Innovation

 ©2025 Palo Alto Networks, Inc.

Puede utilizar Strata Cloud Manager para obtener una visibilidad completa de todo el tráfico de su red y para el aislamiento remoto del navegador (RBI) mediante las secciones Monitor (Supervisar) y Workflows (Flujos de trabajo) de Strata Cloud Manager. Obtenga visibilidad de su implementación de RBI al ver métricas como la cantidad de usuarios activos de RBI, tendencias, estado de conectividad, estado de ubicación de RBI, mediciones de tráfico y consumo de licencias. Al ver datos sobre sus usuarios, puede obtener una imagen general del estado y la conectividad de su implementación.

RBI redirige la actividad de navegación de Internet de los usuarios a un entorno aislado alojado por un proveedor de RBI. El sitio web está diseñado para que los usuarios puedan ver los recursos que necesitan, sin acceder directamente a sitios desconocidos o peligrosos desde sus dispositivos y red. Prisma Access se integra fácilmente con los proveedores de RBI para este tipo de redirección del navegador.

 ©2025 Palo Alto Networks, Inc.

Prisma Access y Autonomous DEM

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager Managed Prisma Access • Panorama Managed Prisma Access	❑ Licencia de Prisma Access ❑ Licencia de Autonomous DEM

Comience con Autonomous DEM en Prisma Access para supervisar continuamente la experiencia digital en todos los usuarios, aplicaciones y sitios remotos en su entorno SASE. Siempre y cuando tenga las licencias respectivas, puede habilitar Autonomous DEM para sus usuarios móviles de GlobalProtect que se conectan a Prisma Access.

- Hoja de referencia: ADEM con Prisma Access
- Primeros pasos con Autonomous DEM
- Supervisar el tráfico de usuarios y aplicaciones con Autonomous DEM

 ©2025 Palo Alto Networks, Inc.

Política basada en el usuario de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Licencia de Prisma Access

Prisma Access requiere que configure la asignación de dirección IP a nombre de usuario para hacer cumplir de manera consistente la política basada en el usuario para los usuarios móviles y los usuarios en ubicaciones de red remotas. Además, necesita configurar la asignación de nombre de usuario a grupo de usuarios si desea hacer cumplir la política basada en la pertenencia al grupo.

Para seleccionar los grupos de una lista desplegable al crear y configurar políticas en Panorama, también puede configurar Panorama para obtener la lista de grupos de usuarios recuperados de la asignación de nombre de usuario a grupo de usuarios.

Las siguientes secciones proporcionan una visión general y los pasos que debe seguir para configurar e implementar User-ID y utilizar Cloud Identity Engine para obtener la asignación de dirección IP a nombre de usuario y de nombre de usuario a grupo de usuarios en Prisma Access.

Configurar la política basada en usuario para Prisma Access

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Política basada en el usuario de Prisma Access (Strata Cloud Manager)

Después de integrar Cloud Identity Engine con Prisma Access, debe confirmar que Prisma Access está conectado a Cloud Identity Engine y que Cloud Identity Engine comparte información de directorio con Prisma Access.

- Compruebe que pueda ver sus directorios en Prisma Access.

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Cloud Identity Engine**.

- Verifique que pueda añadir usuarios y grupos a una regla de política.

  Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de Seguridad)** > **Decryption (Descifrado)**.

  En una regla de política de seguridad o descifrado, verifique que el menú desplegable **Usuarios** muestre las entradas de usuarios y grupos de Active Directory. Ahora puede comenzar a añadir estos usuarios y grupos a sus reglas de política de seguridad y descifrado.

Una vez que haya confirmado que Cloud Identity Engine se ha conectado correctamente, puede comenzar a ejecutar informes de actividad de usuario para obtener una mayor visibilidad del comportamiento de su base de usuarios.

 ©2025 Palo Alto Networks, Inc.

Política basada en el usuario de Prisma Access (Panorama)

Esta sección proporciona los pasos que debe realizar para configurar User-ID para Prisma Access.

STEP 1 | Configure la asignación de direcciones IP a nombres de usuario para sus usuarios móviles y usuarios en ubicaciones de red remotas.

- Para usuarios móviles: implementaciones de GlobalProtect, el agente de GlobalProtect en Prisma Access realiza la asignación de User-ID automáticamente.
- Para los usuarios en redes remotas, configure User-ID para implementaciones de redes remotas para asignar direcciones IP a los ID de usuario.

STEP 2 | Configure la asignación de nombre de usuario a grupo de usuarios para sus usuarios móviles y usuarios en ubicaciones de red remotas.

Para Usuarios móviles: GlobalProtect, proxy explícitoe implementaciones de red remota , configure el componente Sincronización de directorios de Cloud Identity Engine para recuperar información de usuarios y grupos de su Active Directory (AD); luego, configure la **Group Mapping Settings (Configuración de asignación de grupos)** en sus usuarios móviles: GlobalProtect o implementación de red remota.

Como alternativa, puede habilitar la asignación de nombre de usuario a grupo de usuarios para usuarios móviles y usuarios en redes remotas que utilicen un perfil de servidor LDAP.



Recomendamos utilizar una lista de inclusión de grupos en el perfil del servidor LDAP, de modo que pueda especificar qué grupos desea recuperar, en lugar de recuperar toda la información del grupo.

STEP 3 | Permita que Panorama utilice la asignación de nombre de usuario a grupo de usuarios en las políticas de seguridad completando una de las siguientes acciones:

- Configure el componente de sincronización de directorios de Cloud Identity Engine para recuperar información de usuarios y grupos de su Active Directory (AD); luego, configure la **Group Mapping Settings (Configuración de asignación de grupos)** en su implementación de Usuarios móviles—GlobalProtect, Usuarios móviles—Proxy explícitoo de red remota.
- Configure la política basada en grupos especificando el nombre distinguido (DN) completo del grupo.

STEP 4 | Redistribuir la información de HIP a Panorama.

 ©2025 Palo Alto Networks, Inc.

Integrar Cloud Identity Engine con Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

- Strata Cloud Manager
- Panorama

Integrar Cloud Identity Engine con Prisma Access (Strata Cloud Manager)

Cloud Identity Engine (Directory Sync) proporciona a Prisma Access acceso de solo lectura a su información de Active Directory, para que pueda configurar y gestionar fácilmente políticas de seguridad y descifrado para usuarios y grupos.

Cloud Identity Engine funciona tanto con Active Directory local como con Azure Active Directory.

Para configurar el Cloud Identity Engine con Prisma Access, comience por ir al hub para activar Cloud Identity Engine y añadirlo a Prisma Access. Luego vaya a Prisma Access para validar que Prisma Access es capaz de acceder a los datos del directorio.

 ©2025 Palo Alto Networks, Inc.



STEP 1 | Activar Cloud Identity Engine

Cloud Identity Engine puede compartir información de Active Directory con cualquier aplicación compatible en el hub. Es gratis y no requiere un código de autorización para comenzar. La configuración de Cloud Identity Engine incluye la activación de la aplicación Cloud Identity Engine en el hub, la configuración del agente de Cloud Identity Engine para recopilar asignaciones de Active Directory y la configuración de la autenticación mutua entre Cloud Identity y el agente.

Asegúrese de implementar la instancia de Cloud Identity Engine en la misma región en la que implementó Prisma Access y Strata Logging Service.

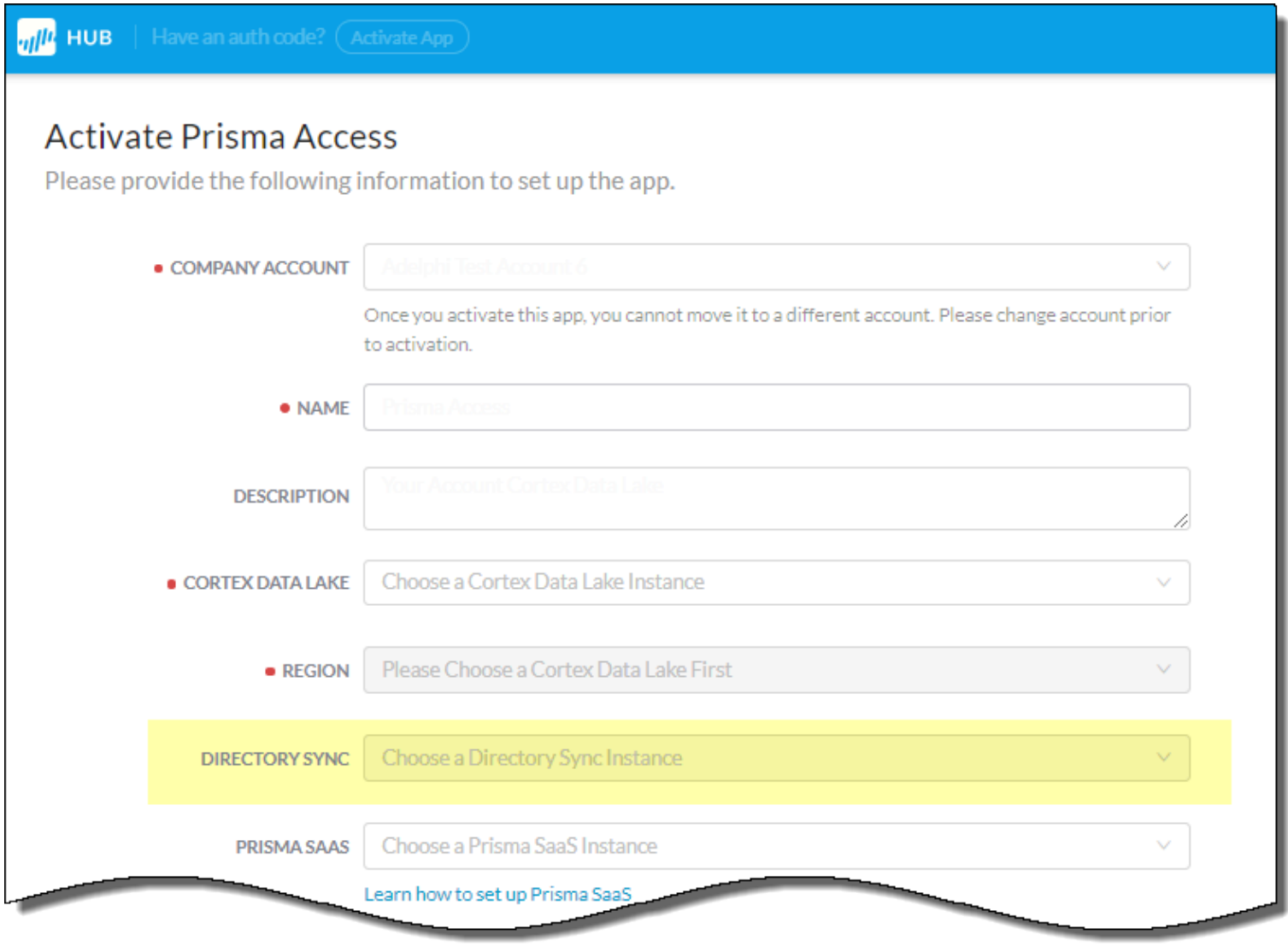
STEP 2 | Habilite Cloud Identity Engine para Prisma Access.

Puede asociar Prisma Access con Cloud Identity Engine cuando active Prisma Access por primera vez o en cualquier momento después:

- **Mientras activa Prisma Access:** Cuando activa por primera vez Cloud Managed Prisma Access, puede elegir una instancia de Cloud Identity Engine para que Prisma Access la

 ©2025 Palo Alto Networks, Inc.

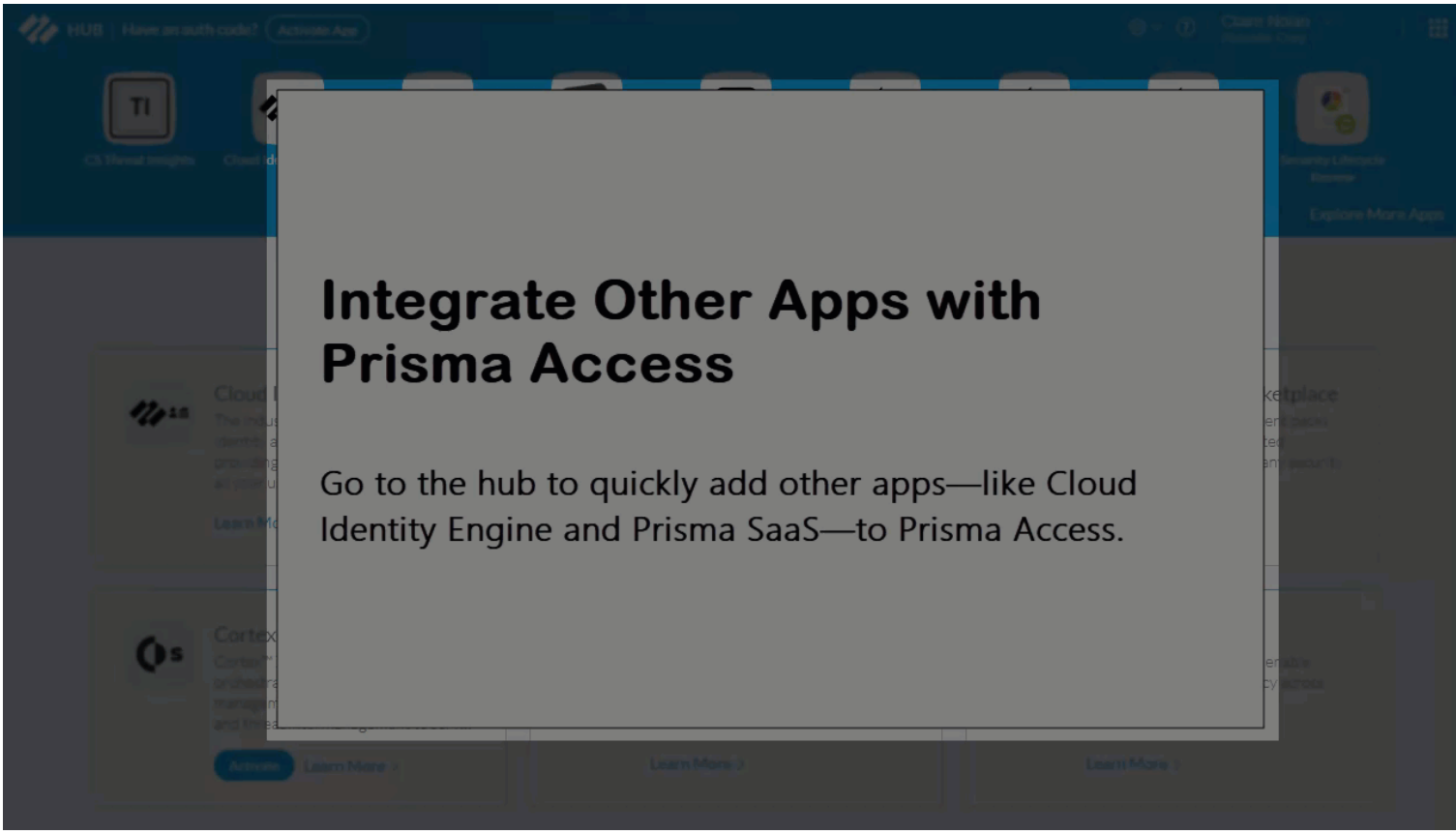
utilice. Asegúrese de seleccionar una instancia que esté implementada en la misma región que Prisma Access.



- **Después de que haya activado Prisma Access:** Para habilitar Cloud Identity Engine para una instancia de Prisma Access existente, inicie sesión en el hub. Desde el menú desplegable de configuración del hub (ver el engranaje en la barra de menú superior), seleccione **Manage**

 ©2025 Palo Alto Networks, Inc.

Apps (Gestionar aplicaciones). Busque la instancia de Prisma Access que desea actualizar y seleccione la instancia de Cloud Identity Engine que desea que Prisma Access utilice.



STEP 3 | Confirme que Prisma Access está conectado a Cloud Identity Engine.

Integrar Cloud Identity Engine con Prisma Access (Panorama)

Prisma Access recupera información de usuarios y grupos del directorio en la nube o Active Directory (AD) de su organización para aplicar políticas basadas en usuarios y grupos. Opcionalmente, Prisma Access recupera señales de riesgo basadas en el comportamiento del usuario de algunos proveedores de directorios en la nube, como Azure Active Directory, para aplicar acciones de seguridad automatizadas. Puede simplificar la recuperación de información de usuario y grupo mediante el uso de Cloud Identity Engine.

Además de simplificar la recuperación de información de usuarios y grupos, la integración de Cloud Identity Engine con Prisma Access puede liberar el ancho de banda y la carga en su directorio en la nube o AD.

Puede usar Cloud Identity Engine para recuperar información de usuarios y grupos para usuarios móviles de Prisma Access, redes remotas o ambas, completando los siguientes pasos.

La integración de Cloud Identity Engine con Prisma Access tiene las siguientes restricciones de implementación:

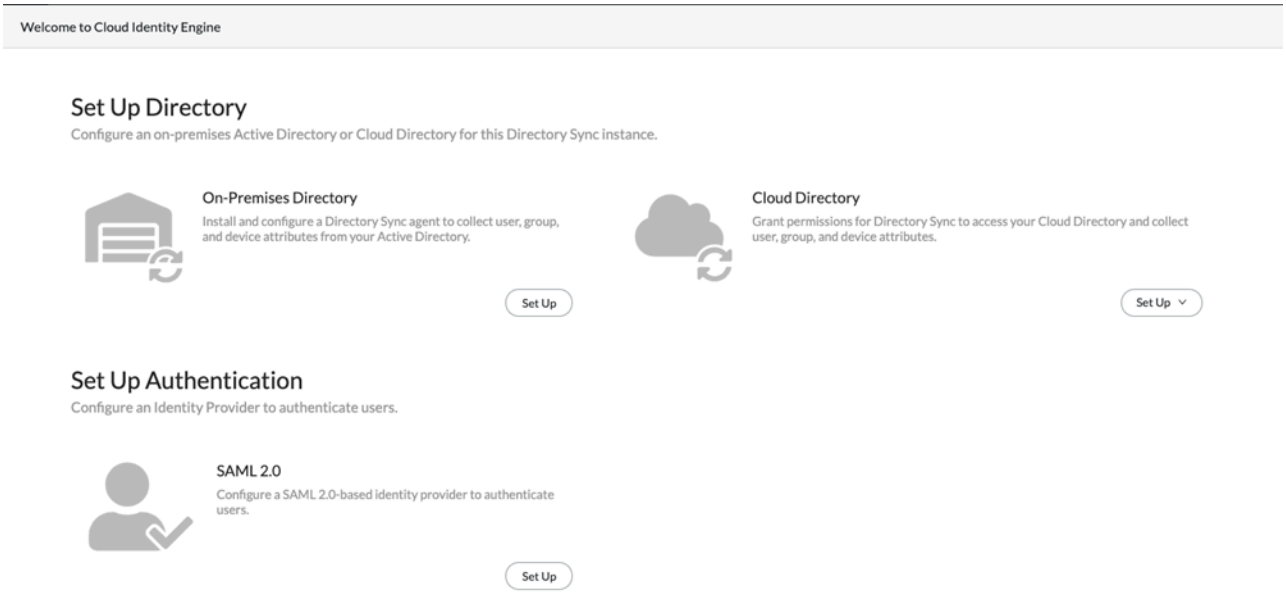
 ©2025 Palo Alto Networks, Inc.

- Asegúrese de que los grupos que usa con Cloud Identity Engine no tengan ninguno de los siguientes caracteres especiales, ya que Prisma Access no admite el uso de los siguientes caracteres especiales en grupos y se producirá un error en las operaciones de confirmación:
  - " (Comilla doble)
  - ' (Apóstrofe)
  - < (signo de menor que)
  - > (signo de mayor que)
  - Y comercial (&)
- Si asocia Cloud Identity Engine con Prisma Access, los nombres de usuario deben utilizar el formato NetBIOS que incluye el dominio. Puede especificar nombres de usuario en formato de correo electrónico (*nombre de usuario*@*dominio*), formato **`NetBIOS\sAMAccountName`** o el formato de nombre principal de usuario (UPN) (*nombre de usuario*@*dominio*.com).
- Introduzca los nombres de los grupos en el formato **distinguishedName** (por ejemplo, **`CN=Usuarios,CN=Incorporado,DC=Ejemplo,DC=com`**).
- Cloud Identity Engine no aplica ninguna configuración que especifique en la lista de inclusión de grupo (**Device (Dispositivo)** > **User Identification (Identificación del usuario)** > **Group Mapping Settings (Configuración de asignación de grupos)** > **Group Mapping Settings (Lista de inclusión de grupo)**); en su lugar, recupera información de usuario y grupo de toda la configuración, incluidos los grupos utilizados en todos los grupos de dispositivos y plantillas.

STEP 1 | Cree una instancia de Cloud Identity Engine para Prisma Access y anote el nombre de la instancia.

Cuando usted activa Cloud Identity Engine, este crea una instancia. Use el nombre de la instancia cuando asocia Cloud Identity Engine con Prisma Access en un paso posterior. Opcionalmente, si necesita crear una instancia separada para Prisma Access, créelo y anote el nombre de la instancia.

STEP 2 | Configure Cloud Identity Engine para recuperar los datos del directorio.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | (Implementaciones solo con Active Directory local) Si utiliza un directorio activo local, Instale y configure el agente de Cloud Identity para comunicarse con su AD local y configurar la autenticación mutua entre el servicio Cloud Identity Engine y el agente.

STEP 4 | Activar Cloud Identity Engine en Prisma Access.

1. En el Panorama que gestiona Prisma Access, seleccione la pestaña de configuración de asignación de nombre de usuario a grupo de usuario.
   - Para una implementación de Usuarios móviles: GlobalProtect, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**, seleccione el icono de engranaje para editar la configuración y, a continuación, seleccione **Group Mapping Settings (Configuración de asignación de grupos)**.
   - Para una implementación de Usuarios móviles: Proxy explícito, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)**, seleccione el icono de engranaje para editar la configuración y, a continuación, seleccione **Group Mapping Settings (Configuración de asignación de grupos)**.
   - Para una implementación de red remota, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, seleccione el icono de engranaje para editar la configuración y, a continuación, seleccione **Group Mapping Settings (Configuración de asignación de grupos)**.
2. Seleccione **Enable Directory Sync Integration (Habilitar la integración de sincronización de directorios)** para habilitar Cloud Identity Engine con Prisma Access.
3. Introduzca la siguiente información:
   - Introduzca el **Primary Username (Nombre de usuario principal)**. Este campo es obligatorio.

     El **Primary Username (Nombre de usuario principal)** controla el formato que se utiliza en los logs y los informes. Si el atributo de nombre de usuario principal es **userPrincipalName** (UPN), todas las entradas de log e informes muestran el usuario de origen en ese formato. Muchas implementaciones usan un formato de UPN, **sAMAccountName**o **mail**. Si su organización utiliza otro atributo, puede especificarlo aquí para garantizar la coherencia del registro de logs y la generación de informes en toda la organización.

     Si configura Azure AD o Directorio de Okta como proveedor de identidad (IdP) en Cloud Identity Engine, especifique el **Nombre de usuario principal** como **userPrincipalName**. Prisma Access admite el atributo userPrincipalName (UPN) que se usa con Azure AD y el directorio de Okta.
   - (Opcional) Introduzca el atributo de **E-Mail (Correo electrónico)** [como **mail (correo)**].
   - (Opcional) Si utiliza atributos de nombre alternativos para el usuario, escríbalos. Puede introducir hasta tres nombres de usuario alternativos [**Alternate User Name 1 (Nombre de usuario alternativo 1)**, **Alternate User Name 2 (Nombre de usuario alternativo 2)** y **Alternate User Name 3 (Nombre de usuario alternativo 3)**].
4. Haga clic en **OK (Aceptar)** cuando se complete.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Confirme y envíe [**Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**] sus cambios.

 ©2025 Palo Alto Networks, Inc.

Recuperar asignaciones de grupos de User-ID para Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Licencia de Prisma Access

Después de configurar la asignación de User-ID en Prisma Access, debe poder recuperar la información actual del nombre de usuario al grupo de usuarios para usuarios móviles y usuarios en redes remotas. Aunque la configuración de la Asignación de grupos en Cloud Identity Engine realiza la asignación de nombre de usuario a grupo de usuarios, esos grupos de usuarios no se pueden seleccionar en las reglas de la política de seguridad. Puede rellenar los grupos para permitir que se seleccionen en las listas desplegables de reglas de política de seguridad mediante la: configuración de un cortafuegos de nueva generación como Dispositivo principal o la configuración de Cloud Identity Engine para hacerlo.

- Motor de identidad en la nube
- Dispositivo principal
- Entradas de nombres distinguidos de formato largo

Motor de identidad en la nube

Además de utilizar Cloud Identity Engine para recuperar información de usuarios y grupos, puede utilizar Cloud Identity Engine para completar los nombres de grupos de usuarios en las reglas de política de seguridad. Esta integración elimina la necesidad de configurar un cortafuegos de nueva generación local o VM-Series como Master Device (Dispositivo principal) para este propósito; sin embargo, los dispositivos principales aún son compatibles.

También puede usar Cloud Identity Engine para completar los nombres de grupos en implementaciones multiinquilinogestionadas por Panorama, lo que no es posible cuando se usa un dispositivo principal.

Para permitir que Cloud Identity Engine complete los nombres de grupos en las reglas de política de seguridad, complete los siguientes pasos.

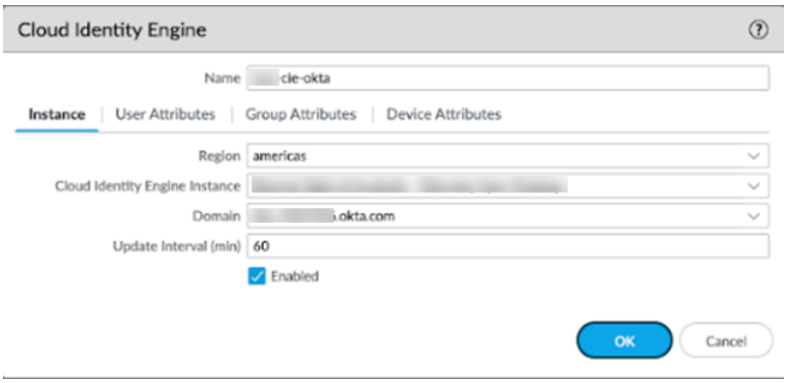
STEP 1 | En Cloud Identity Engine, active Cloud Identity Engine y añada un directorio local o basado en la nube , si aún no lo ha hecho.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurar Cloud Identity Engine como fuente de asignación.

1. Desde el Panorama que gestiona Prisma Access, seleccione **Panorama** > **User Identification (Identificación de usuario)** > **Cloud Identity Engine** y **Add (Añadir)** para añadir un perfil.
2. Para la **Instance (Instancia)**, especifique los siguientes parámetros:
   - **Region (Región)**: seleccione el endpoint regional de la instancia.

     La región que seleccione debe coincidir con la que selecciona cuando activa el inquilino de Cloud Identity Engine.
   - **Cloud Identity Engine Instance (Instancia de Cloud Identity Engine)**: seleccione la instancia de Cloud Identity Engine que desea asociar con el perfil.
   - **Domain (Dominio)**: seleccione el dominio que contiene los directorios que desea utilizar.
   - **Update Interval (min) [Intervalo de actualización (min)]**: introduzca la cantidad de minutos que desea que Panorama espere entre actualizaciones de la aplicación Cloud Identity Engine a Panorama (también conocido como intervalo de actualización). El valor predeterminado es 60 minutos, y el rango de 5 a 1440.
3. Compruebe que el perfil está **Enabled (Habilitado)**.

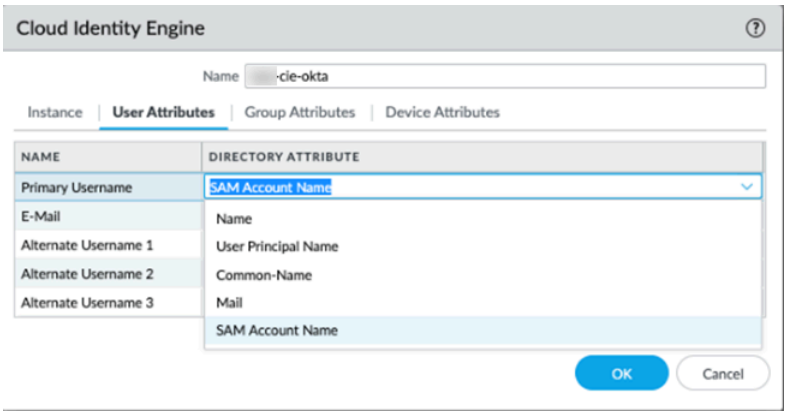


4. En **User Attributes (Atributos de usuario)**, seleccione el formato del **Primary Username (Nombre de usuario principal)**. Opcionalmente, puede seleccionar los formatos para el Correo electrónico y un Nombre de usuario alternativo. Puede configurar hasta tres

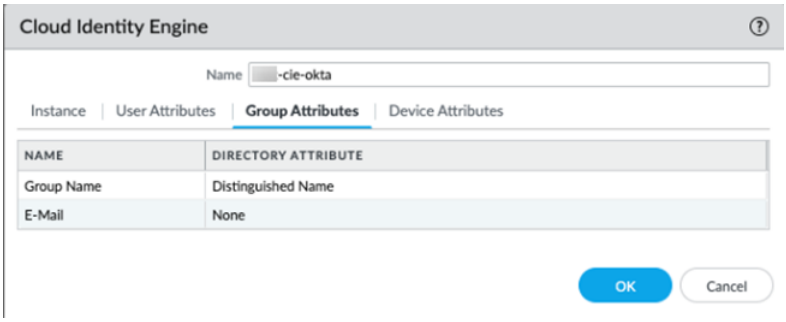
 ©2025 Palo Alto Networks, Inc.

formatos de nombre de usuario alternativos si los usuarios inician sesión con varios formatos de nombre de usuario.

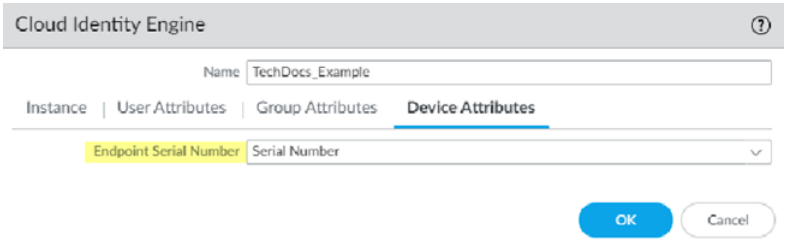
Cuando visualiza usuarios en las reglas de política de seguridad, el nombre de usuario se muestra en el formato de nombre de usuario principal que seleccione aquí.



5. En **Group Attributes (Atributos de grupo)**, seleccione el formato del **Group Name (Nombre del grupo)**.



6. Deje los **Device Attributes (Atributos del dispositivo)** como **None (Ninguno)**.



7. Haga clic en **OK (Aceptar)** y luego en **Commit and Push (Confirmar y enviar)** para confirmar y enviar los cambios.

STEP 3 | Adjunte su perfil a su configuración de Prisma Access.

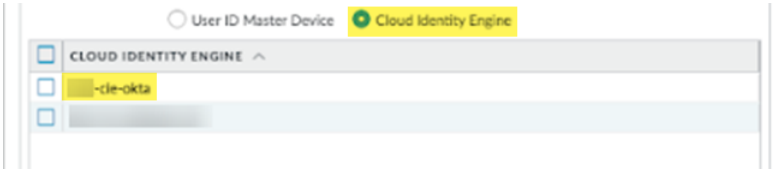
1. Vaya a la Configuración de la implementación que está añadiendo.
   - Para una implementación de Usuarios móviles: GlobalProtect, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)** y haga clic en el engranaje para editar la **Settings (Configuración)**.
   - Para una implementación de Usuarios móviles: Proxy explícito, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile**

 ©2025 Palo Alto Networks, Inc.

Users—Explicit Proxy (Usuarios móviles: Proxy explícito y haga clic en el engranaje para editar la **Settings (Configuración)**.

- Para una implementación de Usuarios móviles: Redes remotas, seleccione **de Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—Remote Networks (Usuarios móviles: Redes remotas)** y haga clic en el engranaje para editar la **Settings (Configuración)**.

2. Seleccione **Cloud Identity Engine**.
3. Seleccione el perfil de Cloud Identity Engine que creó.



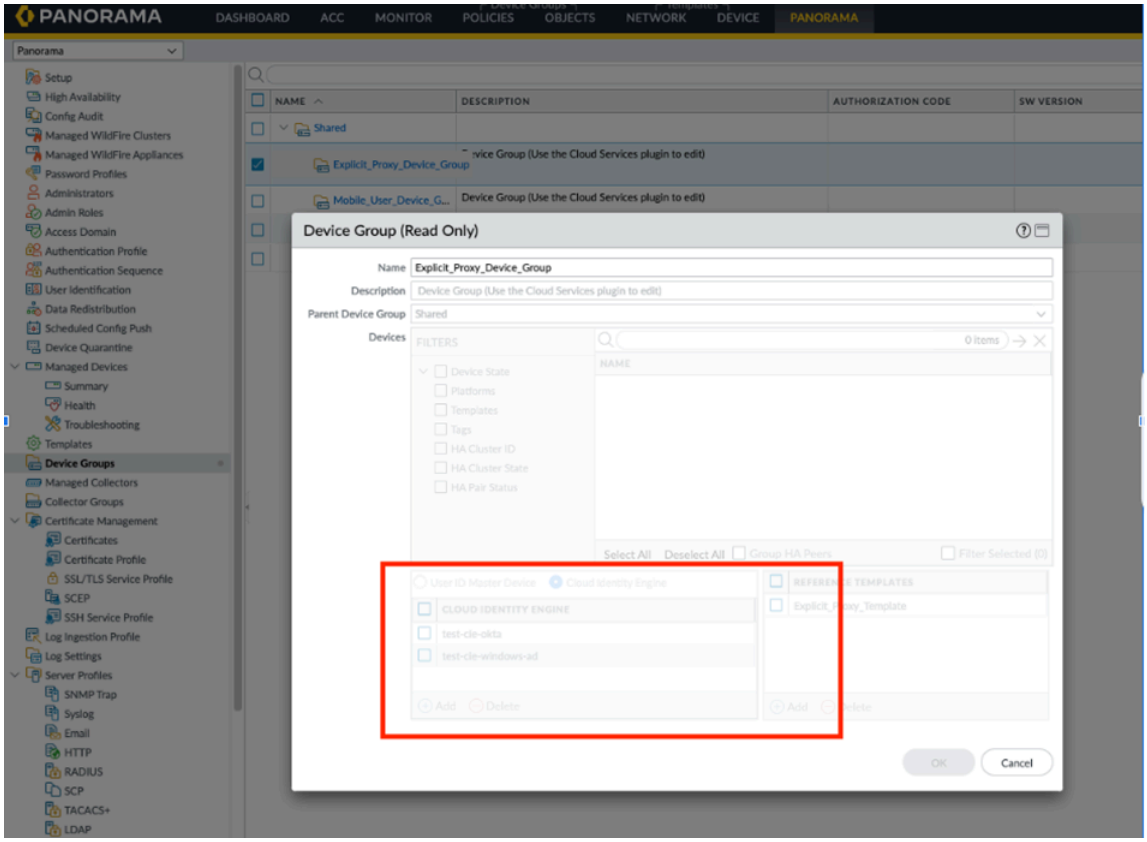
STEP 4 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Compruebe que Prisma Access tiene la información de asignación de Cloud Identity Engine.

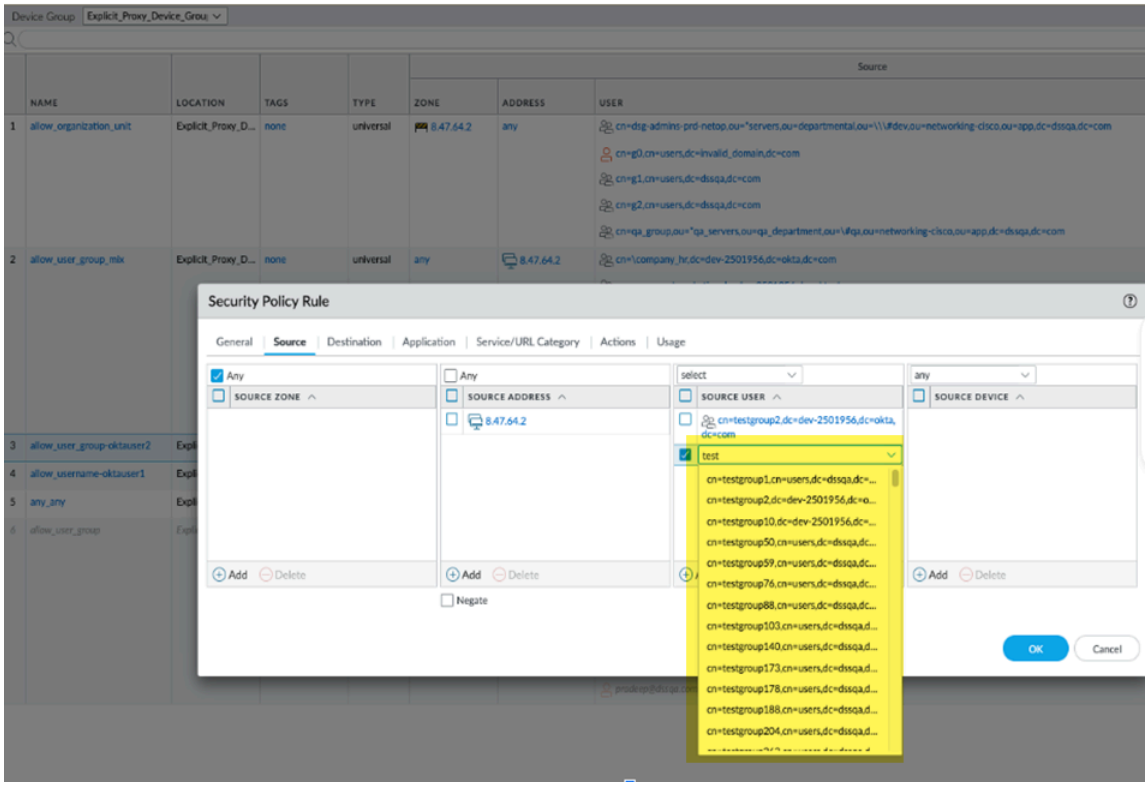
1. Seleccione **Panorama** > **Device Groups (Grupo de dispositivos)** > ***<template-name>***, donde *<template-name>* es la plantilla para la implementación que está configurando y verifique que el perfil de Cloud Identity Engine esté asociado al grupo de dispositivos.

   El siguiente ejemplo muestra que el grupo de dispositivos se adjuntó correctamente a Explicit_Proxy_Device_Group.



2. Seleccione **Objects (Objetos)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)** y elija **Add (Añadir)** para añadir una regla de política de seguridad. Verifique que los grupos estén completos en el área de usuario.

 ©2025 Palo Alto Networks, Inc.



Dispositivo principal

Mientras se configura la Asignación de grupos en Cloud Identity Engine, se realiza la asignación de nombre de usuario a grupo de usuario, esos nombres de usuario y grupos de usuario no se reflejan en las políticas de seguridad. Para simplificar la creación o modificación de políticas basadas en usuarios y grupos, puede usar un Dispositivo principal para añadir los nombres de los grupos a las listas desplegables en las reglas de políticas de seguridad. Necesita designar un cortafuegos como el Dispositivo principal para cada grupo de dispositivos. Después de añadir un Dispositivo principal, el grupo de dispositivos hereda todas las políticas definidas en el dispositivo principal; por esta razón, debe ser un dispositivo independiente y dedicado para ser utilizado para ese grupo de dispositivos.

Para permitir la selección de nombres de grupo en listas desplegables en políticas de seguridad, Palo Alto Networks recomienda que designe un **Master Device (Dispositivo principal)** para cada grupo de dispositivos. Puede configurar un cortafuegos local o un cortafuegos VM-Series como un dispositivo principal.

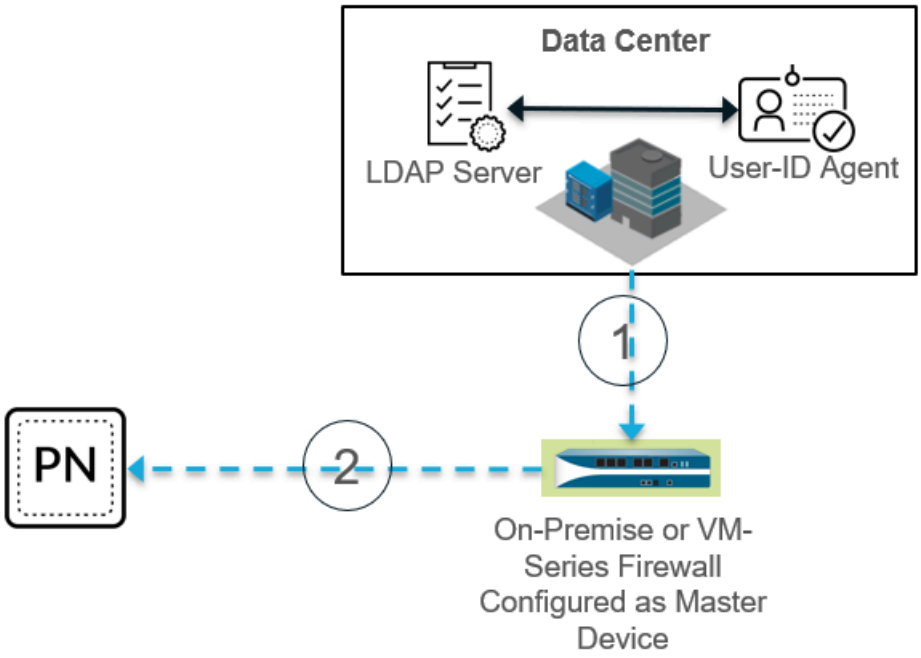
La siguiente imagen muestra una implementación de User-ID donde el administrador ha configurado un dispositivo local como **Master Device (Dispositivo principal)**. Las llamadas en la imagen muestran el proceso.

1. Un cortafuegos de nueva generación en las instalaciones o VM-Series que el administrador ha configurado como un Dispositivo principal recupera la última asignación de nombre de usuario a grupo de usuarios del servidor LDAP y del agente User-ID en el centro de datos.

 ©2025 Palo Alto Networks, Inc.

2. Panorama obtiene la asignación de nombre de usuario a grupo de usuarios del dispositivo principal.

   Panorama utiliza esta asignación solo con el propósito de rellenar los nombres de grupo en listas desplegables en políticas de seguridad, simplificando así la creación de políticas basadas en grupos.



Configurar un cortafuegos en las instalaciones o VM-Series como un dispositivo principal

Utilice el siguiente procedimiento para configurar un cortafuegos local o VM-Series como un dispositivo principal.

Solo puede usar un Dispositivo principal por grupo de dispositivos; si necesita configurar un Dispositivo principal para diferentes grupos de dispositivos, debe crear un Dispositivo principal separado para cada grupo de dispositivos.

STEP 1 | Asegúrese de que el dispositivo que desea usar como dispositivo principal esté gestionado por el mismo Panorama que gestiona Prisma Access.

Puede comprobar sus dispositivos gestionados en **Panorama** > **Managed Devices (Dispositivos gestionados)**.

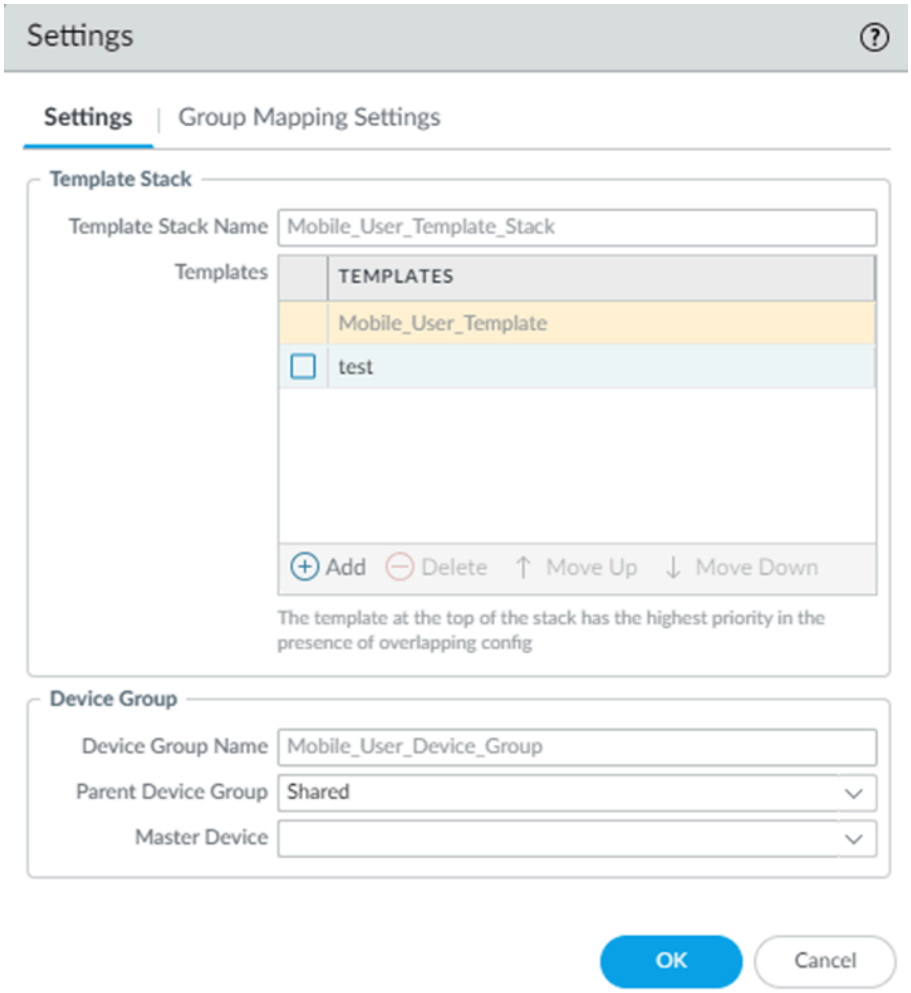
STEP 2 | Añada el dispositivo principal a su implementación de usuario móvil o de red remota de Prisma Access.

- Para una implementación de Usuarios móviles: GlobalProtect, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**, haga clic en el icono de engranaje en

 ©2025 Palo Alto Networks, Inc.

Settings (Configuración) y seleccione el cortafuegos local que desea especificar como **Master Device (Dispositivo principal)**.

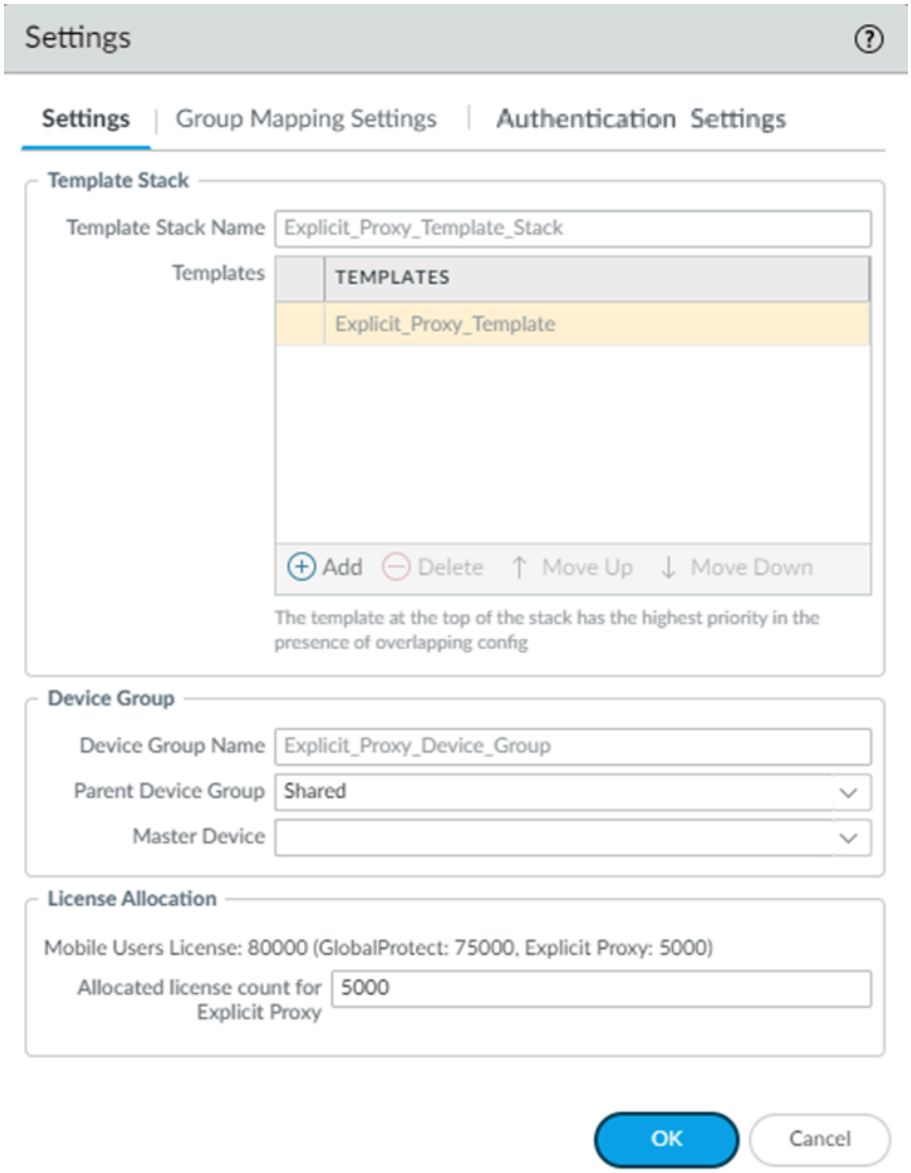
*Si utiliza el **Device Group Name (Nombre de grupo de dispositivos)** predeterminado (**Mobile_User_Device_Group** en este caso) y el **Parent Device Group (grupo de dispositivos primario)** (**Shared (Compartido)** en este caso), cualquier dispositivo que no esté asociado con otro grupo de dispositivos se mostrará en las opciones del menú desplegable. Si ha asociado el dispositivo maestro con otro grupo de dispositivos, seleccione el **Parent Device Group (Grupo de dispositivos primario)** asociado con ese grupo de dispositivos para que se muestre en el menú desplegable.*



- Para una implementación de Usuarios móviles: Proxy explícito, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—**

 ©2025 Palo Alto Networks, Inc.

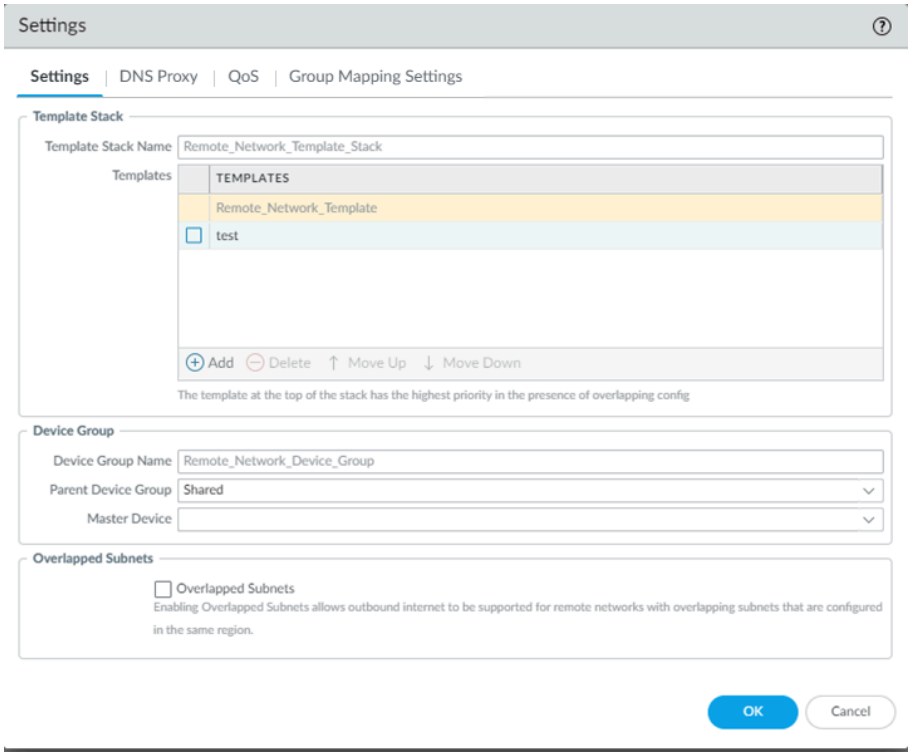
Explicit Proxy (Usuarios móviles; Proxy explícito), haga clic en el icono de engranaje en **Settings (Configuración)** y seleccione el **Master Device (Dispositivo principal)** que creó.



- Para implementaciones de red remota, el grupo de dispositivos con una conexión de red remota, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, haga clic en el icono de engranaje

©2025 Palo Alto Networks, Inc.

en **Settings (Configuración)** y seleccione el **Master Device (Dispositivo principal)** que creó.



Prisma Access puebla automáticamente la asignación de nombre de usuario a grupo de usuario para el grupo de dispositivos que está asociado solo con el dispositivo maestro. Para este ejemplo, el completado automático ocurriría solo en el grupo de dispositivos ***Remote_Network_Device_Group*** *y no se poblaría en ningún otro grupo de dispositivos.*

STEP 3 | Haga clic en **OK (Aceptar)**.

Entradas de nombres distinguidos de formato largo

Si no ha configurado un cortafuegos de nueva generación como dispositivo maestro o no ha configurado un Cloud Identity Engine para completar usuarios y grupos en las reglas de política de seguridad, puede usar entradas de nombre distintivo (DN) de formato largo en Panorama. Prisma Access utiliza las entradas DN para evaluar las políticas basadas en User-ID que ha configurado en Panorama.

Por ejemplo, dado un usuario llamado **Bob Alice** que trabaja en TI y está ubicado en la primera planta, una política de seguridad coincidente puede tener `cn=first_floor, ou=it_staff, dc=dev, dc=example, dc=com` si la política se va a aplicar a todo el personal de TI en la primera planta, o `cn=Bob Alice, ou=it_staff, dc=dev, dc=example, dc=com` si la política solo se aplicará a Bob Alice.

©2025 Palo Alto Networks, Inc.

Redistribución de identidades

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Para que pueda hacer cumplir su política de seguridad de manera coherente, Prisma Access comparte los datos de identidad que GlobalProtect descubre localmente en todo su entorno de Prisma Access. Prisma Access también puede compartir datos de identidad con dispositivos locales en sitios de red remotos o sitios de conexión de servicio (sede y centros de datos).

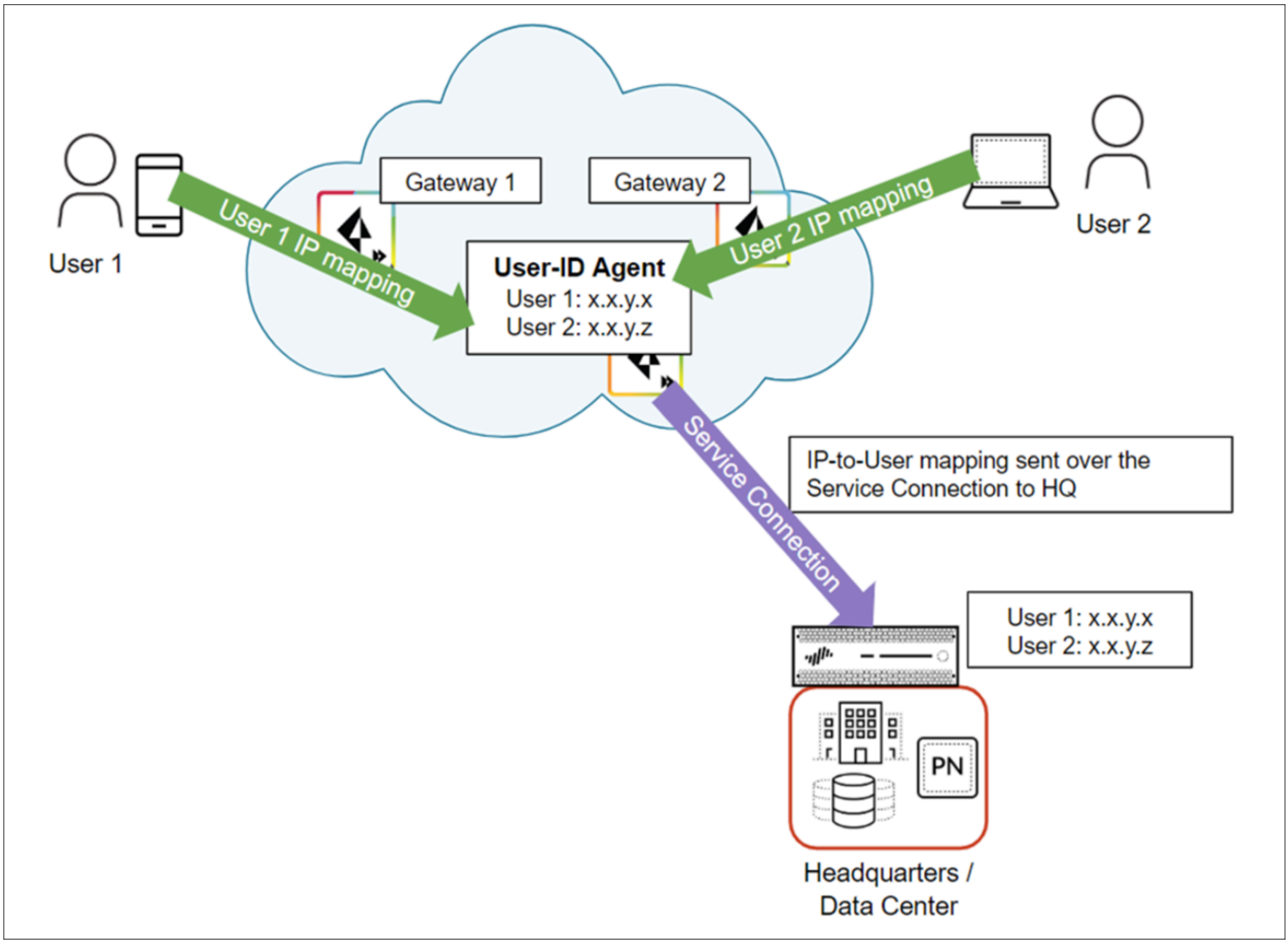
Para que los usuarios móviles accedan a un recurso en una ubicación de red remota o en una sede o centro de datos protegido por un dispositivo con políticas basadas en el usuario, debe redistribuir los datos de identidad de los usuarios móviles de Prisma Access y los usuarios de redes remotas a ese dispositivo local.

Cuando los usuarios se conectan a Prisma Access, Prisma Accessrecopila los datos de identidad del usuario y los almacena.

El siguiente ejemplo muestra a dos usuarios móviles que tienen una asignación existente de dirección IP a nombre de usuario en Prisma Access. Prisma Access luego redistribuye esta asignación a través de una conexión de servicio a los dispositivos locales que están protegiendo la sede / centro de datos.

Prisma Access (Managed by Strata Cloud Manager) habilita automáticamente las conexiones de servicio para que funcionen como agentes de redistribución de identidad (también llamados agentes de User-ID).

 ©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

Redistribución de identidades (Strata Cloud Manager)

Para que pueda hacer cumplir su política de seguridad de manera coherente, Prisma Access comparte los datos de identidad que GlobalProtect descubre localmente en todo su entorno de Prisma Access. Prisma Access también puede compartir datos de identidad con dispositivos locales en sitios de red remotos o sitios de conexión de servicio (sede y centros de datos).

Para Prisma Access (Managed by Strata Cloud Manager), hemos habilitado parte de la redistribución de datos de identidad de forma predeterminada y, para lo que queda, hemos simplificado mucho la configuración para habilitar la redistribución (simplemente seleccione una casilla de verificación para seleccionar qué datos desea compartir).

Desde el panel de control de Distribución de identidades, puede ver cómo se comparten los datos de identidad y gestionar la redistribución de datos (**Manage (Gestionar)** > **Configuration**

 ©2025 Palo Alto Networks, Inc.

(Configuración) > NGFW and Prisma Access (NGFW y Prisma Access) > Identity Services (Servicios de identidad).

Entre los datos de identidad que se pueden redistribuir se incluyen:

- Datos de HIP
- Asignaciones de direcciones IP a etiquetas
- Asignaciones de dirección IP a usuario
- Asignaciones de usuario a etiqueta
- Dispositivos en cuarentena

Introducción a la redistribución de identidades:

- Configurar la redistribución de identidades
- Identificar y poner en cuarentena los dispositivos comprometidos

Configurar la redistribución de identidades

Configurar la redistribución de identidades

1. Confirme la configuración de la conexión de servicio.

   Si aún no ha configurado una conexión de servicio para su sede central o centros de datos, comience por Configurar una conexión de servicio. Se requiere una conexión de servicio para que Prisma Access comparta datos de identidad en todo su entorno; Prisma Access permite automáticamente que las conexiones de servicio funcionen como agentes de redistribución. Un sitio de conexión de servicio recién creado estará listo para usarse como agente de redistribución cuando vea que se le ha asignado una Dirección de agente de User-ID (Prisma Access lo hace automáticamente y sólo tomará unos minutos).

   > ***Gestión de redistribución de User-ID**: a veces, se necesitan controles granulares para la redistribución de User-ID en implementaciones de Prisma Access a gran escala. Gestión de la redistribución de User-ID le permite desactivar manualmente el comportamiento de redistribución de identidad predeterminado para determinadas conexiones de servicio eliminando la marca de verificación en la columna **User ID (ID de usuario)** y, a continuación, seleccionar conexiones de servicio específicas que se utilizarán para la redistribución de identidad. No es necesario hacer esto para la mayoría de las configuraciones. Póngase en contacto con la asistencia de Palo Alto Networks para activar esta funcionalidad.*

   Vaya a **Manage (Gestionar) > Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access) > Identity Services (Servicios de identidad) > Identity Redistribution (Redistribución de identidad)** establezca el ámbito de configuración en **Service Connections (Conexiones de servicio)** para verificar los detalles del agente de User-ID de la conexión de servicio.

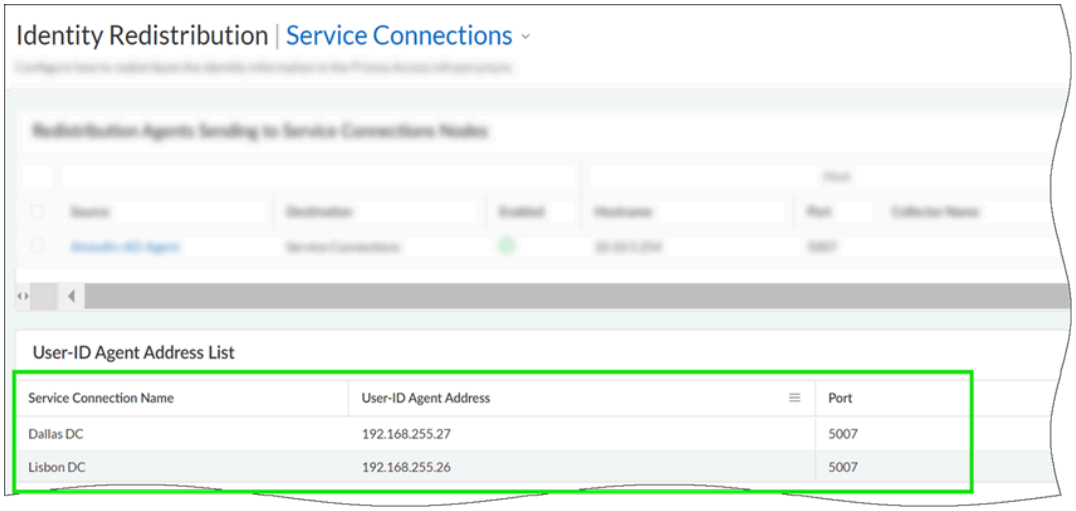
 ©2025 Palo Alto Networks, Inc.

- Envíe datos de identidad desde Prisma Access a dispositivos locales

  La información del agente de User-ID de la conexión de servicio es todo lo que necesita para configurar Prisma Access para distribuir datos de identidad a dispositivos locales.

  Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identity Services (Servicios de identidad)** > **Identity Redistribution (Redistribución de identidades)** y establezca el parámetro ámbito de la configuración en **Service Connections (Conexiones de servicio)** para obtener los detalles del agente de User-ID de la conexión de servicio.

  Utilice estos detalles para configurar Prisma Access como agente de redistribución de datos en Panorama o un NGFW de Palo Alto Networks.



- Envíe datos de identidad desde dispositivos locales a Prisma Access

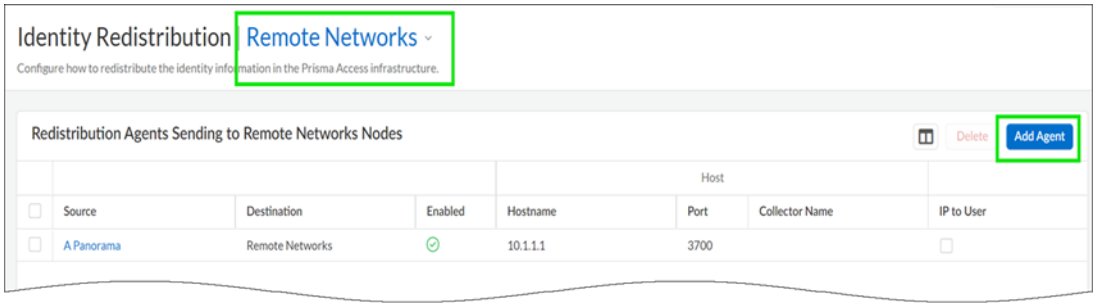
  Añada dispositivos locales a Prisma Access como agentes de redistribución; los dispositivos que añada podrán distribuir datos de identidad a Prisma Access.

  - **Desde dispositivos en sitios de red remotos:**

    Vaya al panel **Identity Redistribution (Redistribución de identidades)**, establezca el Configuration Scope (Alcance de la configuración) para **Remote Networks (Redes remotas)**y **Add Agent (Añadir agente)**. Además de especificar los detalles del host, seleccione el tipo de

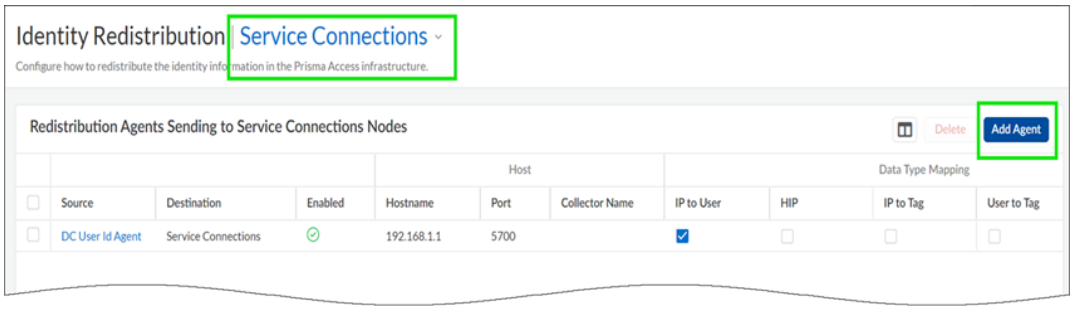
 ©2025 Palo Alto Networks, Inc.

datos que el dispositivo comparte con Prisma Access. La configuración opcional incluye el nombre y una clave previamente compartida para el dispositivo.



- **Desde dispositivos en sitios de conexión de servicio:**

  Vaya al panel **Identity Redistribution (Redistribución de identidades)**, establezca el Configuration Scope (Alcance de la configuración) para **Service Connections (Conexiones de servicio)**y **Add Agent (Añadir agente)**. Además de especificar los detalles del host, seleccione el tipo de datos que el dispositivo comparte con Prisma Access. La configuración opcional incluye el nombre y una clave previamente compartida para el dispositivo.



- Configure el agente de Terminal Server para la asignación de usuarios

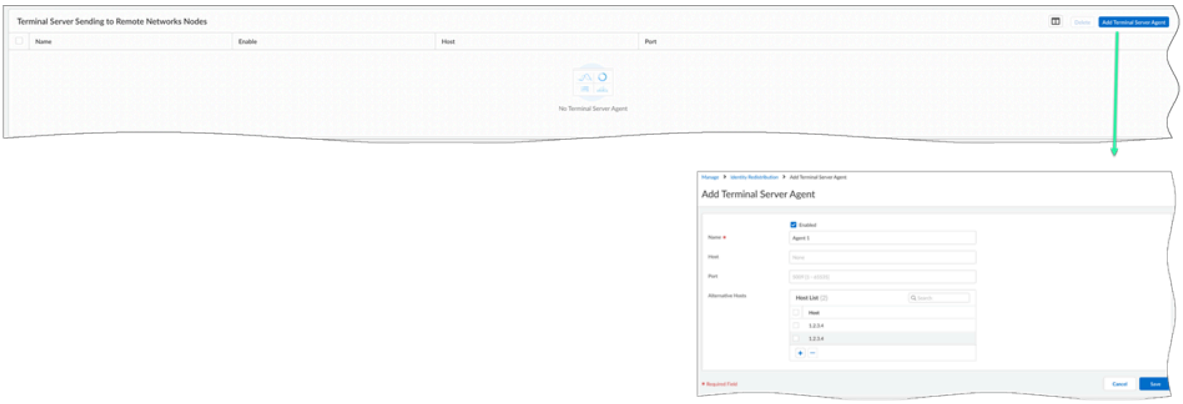
  El agente de Terminal Server (TS) asigna un intervalo de puertos a cada usuario para identificar a usuarios específicos en servidores de terminal basados en Windows. El agente TS notifica a Prisma Access los rangos de puertos asignados, de modo que Prisma Access pueda aplicar la política basada en usuarios y grupos de usuarios.

  En el panel **Identity Redistribution (Redistribución de identidades)**, establezca el Configuration Scope (Alcance de la configuración) para **Remote Networks (Redes remotas)** y **Add Terminal**

 ©2025 Palo Alto Networks, Inc.

Server Agent (Añadir agente de Terminal Server) en **Terminal Server Sending to Remote Networks Nodes (Envío de Terminal Server a nodos de redes remotas)**.

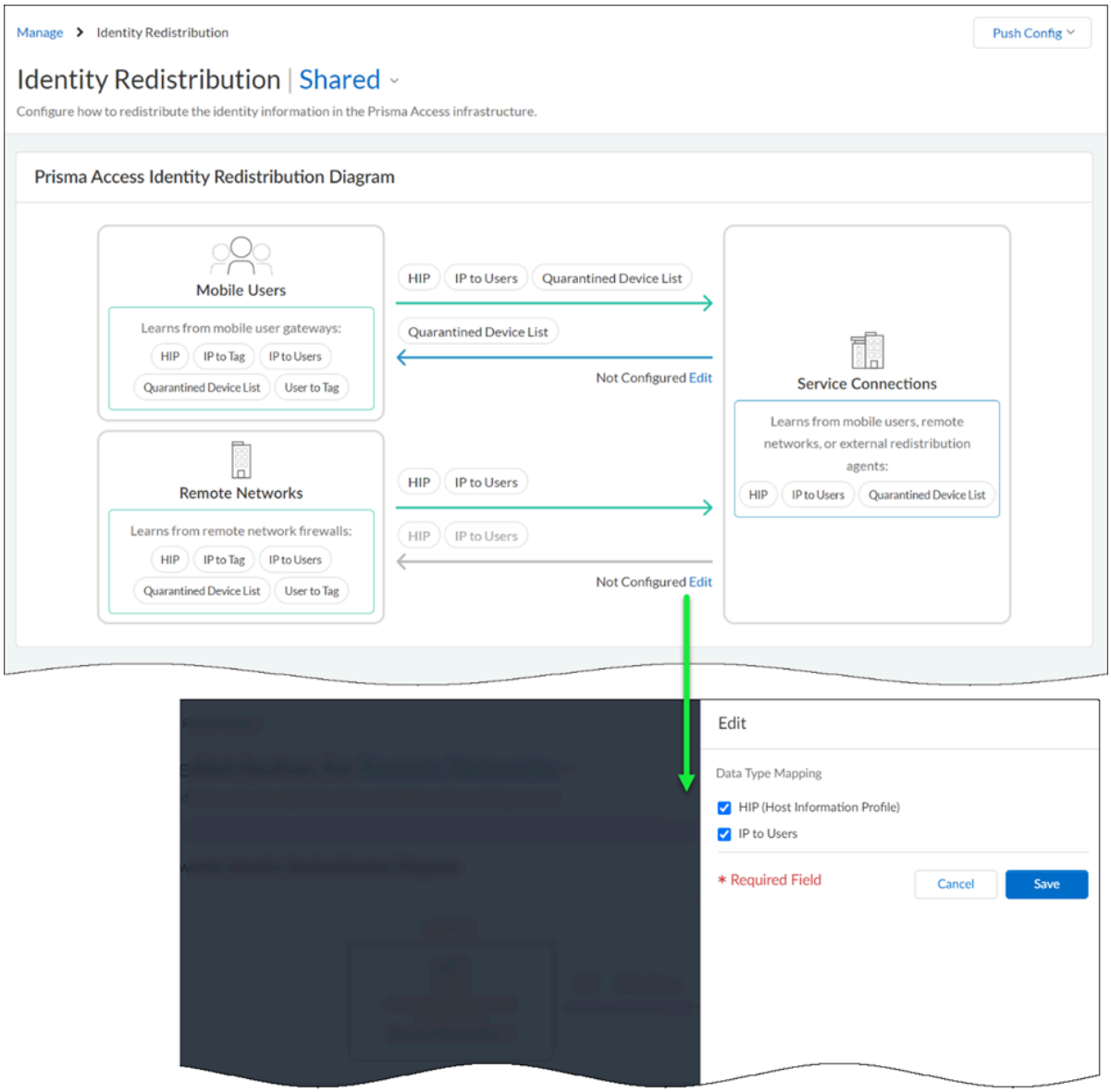
- De forma predeterminada, la configuración está **Enabled (Habilitada)**.
- Introduzca un **Name (Nombre)** para el agente TS.
- Introduzca la dirección IP del **Host** de Windows en el que está instalado el agente TS.
- Introduzca el número de **Port (Puerto)** en el que el agente escucha solicitudes de asignación de usuarios. El puerto está establecido en 5009 de forma predeterminada.
- Haga clic en **Save (Guardar)** para guardar sus cambios.



 ©2025 Palo Alto Networks, Inc.

- Distribuya los datos de identidad en su entorno de Prisma Access

  En el panel **Identity Redistribution (Redistribución de identidades)**, debe **Edit (Editar)** el diagrama para especificar los datos de identidad que desea recopilar de cada origen y compartir a través de Prisma Access.



- Para activar los cambios, envíe la configuración a Prisma Access.

Redistribución de identidades (Panorama)

Después de configurar User-ID, aplica de manera coherente la política basada en usuarios para todos los usuarios móviles y usuarios en ubicaciones de red remotas redistribuyendo la asignación de dirección IP a nombre de usuario de Prisma Access a todos los cortafuegos de nueva generación que aseguran el acceso a los recursos de la red. Utilice uno de los siguientes métodos para redistribuir la asignación de direcciones IP a nombres de usuario a usuarios móviles

 ©2025 Palo Alto Networks, Inc.

y usuarios en redes remotas desde un cortafuegos de nueva generación en las instalaciones y viceversa:

- Redistribuir la información de User-ID de Prisma Access a un cortafuegos local
- Redistribuir la información del User-ID desde un cortafuegos local a Prisma Access

Redistribuir la información del User-ID de Prisma Access a un cortafuegos local

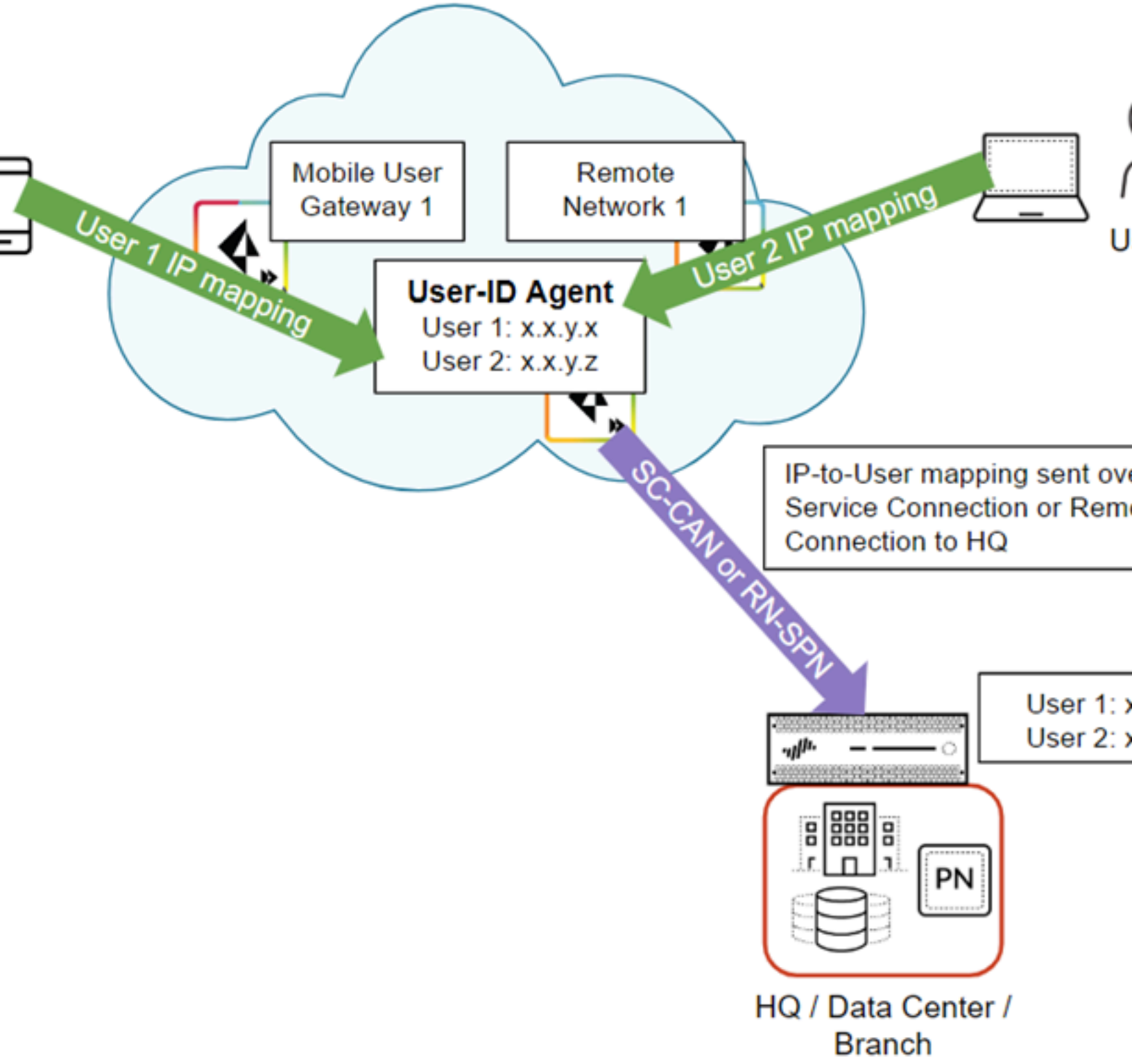
Redistribuir la información del User-ID de Prisma Access a un cortafuegos local.

En los casos en que los usuarios móviles necesiten acceder a un recurso en una ubicación de red remota o en la sede/centro de datos y el recurso esté protegido por un cortafuegos de nueva generación en las instalaciones con políticas basadas en usuarios, debe redistribuir la asignación de direcciones IP a nombres de usuario de los usuarios móviles de Prisma Access y de los usuarios en redes remotas al cortafuegos en las instalaciones. Cuando el usuario se conecta a Prisma Access, recopila esta asignación de usuario a dirección IP y lo almacena.

La siguiente imagen muestra a dos usuarios móviles que tienen una asignación existente de dirección IP a nombre de usuario en Prisma Access. Prisma Access luego redistribuye esta asignación a través de una conexión de servicio (SC-CAN) o conexión de red remota (RN-SPN) al cortafuegos local que asegura la sede/centro de datos.

Prisma Access utiliza la conexión de servicio o la conexión de red remota como un túnel IPSec que sirve como la ruta subyacente a la red de Capa 3. Puede usar cualquier ruta a través de un túnel IPSec de confianza para destinos con direcciones privadas para redistribuir esta asignación.

 ©2025 Palo Alto Networks, Inc.



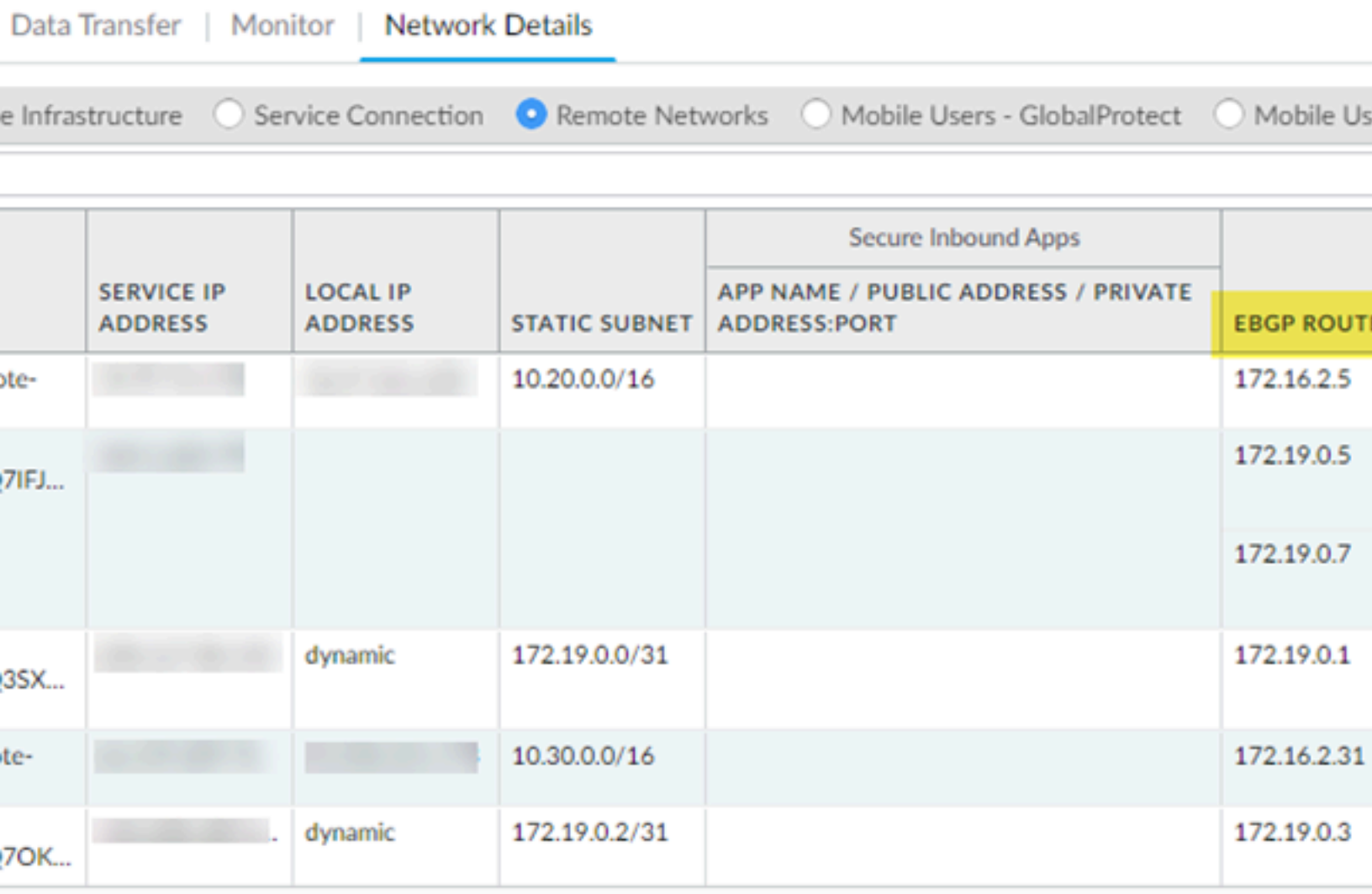
Para redistribuir las asignaciones de User-ID de Prisma Access a un cortafuegos local, complete los siguientes pasos.

 ©2025 Palo Alto Networks, Inc.

Asegúrese de no aplicar ninguna descifrado SSL en ninguna conexión que redistribuya la identidad del usuario al cortafuegos local (SC-CAN o RN-SPN), incluidos los cortafuegos que están en la ruta de redistribución. Alternativamente, puede aplicar una exclusión de descifrado al tráfico de redistribución.

STEP 1 | Tome nota de la dirección IP que debe usar cuando configure el agente de redistribución de datos.

- Para conexiones de red remotas, encuentre la dirección del **EBGP Router (Enrutador EBGP)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** > **EBGP Router (Enrutador EBGP)**].



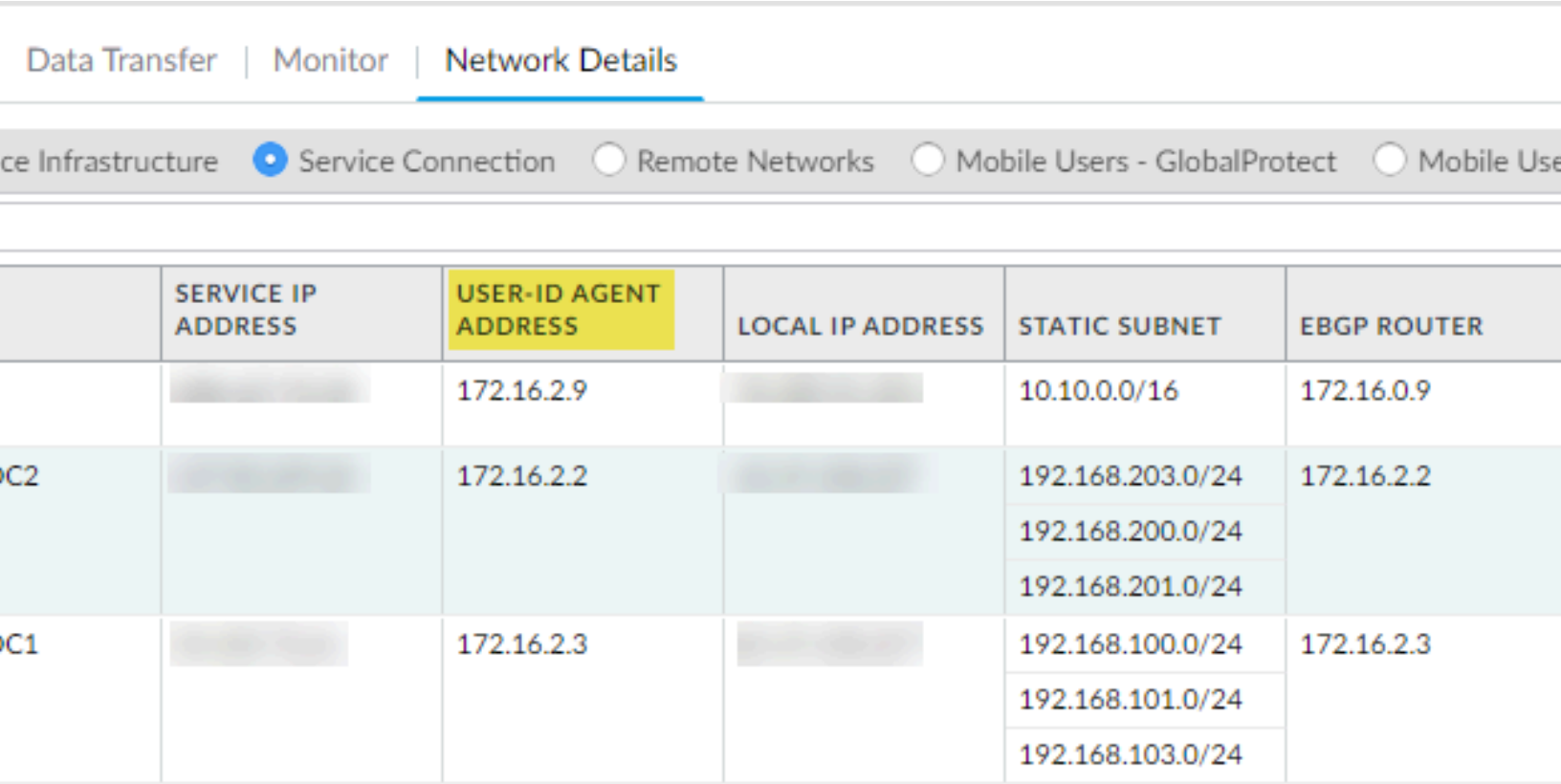
- Para las conexiones de servicio, encuentre **User-ID Agent Address (Dirección del agente de User-ID)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **User-ID Agent Address (Dirección del agente de User-ID)**].

  Si aún no ha configurado una conexión de servicio para su sede o centros de datos, comience configurando una conexión de servicio. Prisma Access utiliza conexiones

 ©2025 Palo Alto Networks, Inc.

de servicio para compartir datos de identidad en su entorno; Prisma Access habilita automáticamente las conexiones de servicio para que funcionen como agentes de redistribución. Una conexión de servicio recién creado estará listo para usarse como agente de redistribución cuando vea que se le ha asignado una dirección de agente de User-ID (Prisma Access hace esto automáticamente, y esto puede tardar unos pocos minutos).

***Gestión de redistribución de User-ID**: a veces, se necesitan controles granulares para la redistribución de User-ID en implementaciones de Prisma Access de tamaño particularmente grande. Gestión de la redistribución de User-ID le permite desactivar manualmente el comportamiento de redistribución de identidad predeterminado para determinadas conexiones de servicio eliminando la marca de verificación en la columna **User ID (ID de usuario)** y, a continuación, seleccionar conexiones de servicio específicas que se utilizarán para la redistribución de identidad. No es necesario hacer esto para la mayoría de las configuraciones. Póngase en contacto con la asistencia de Palo Alto Networks para activar esta funcionalidad.*

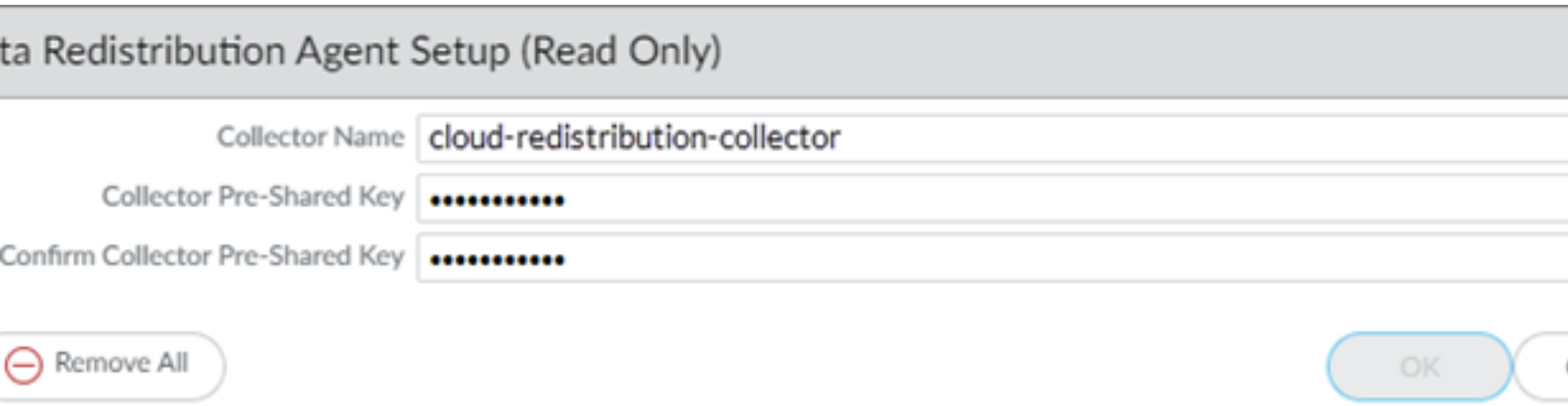


 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configure Prisma Access como un agente de User-ID que redistribuye la información de asignación de usuarios.

1. En el Panorama que gestiona Prisma Access, seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Collector Settings (Configuración del recopilador)**.

   Para configurar el recolector en una conexión de servicio, seleccione la plantilla **Service_Conn_Template**; para configurar el recolector en una conexión de red remota, seleccione la plantilla **Remote_Network_Template.**
2. Para editar la configuración, haga clic en el engranaje.
3. Proporcione un **Collector Name (Nombre del recopilador)** y una **Collector Pre-Shared Key (Clave precompartida de recopilador)** para identificar Prisma Access como un agente de User-ID.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

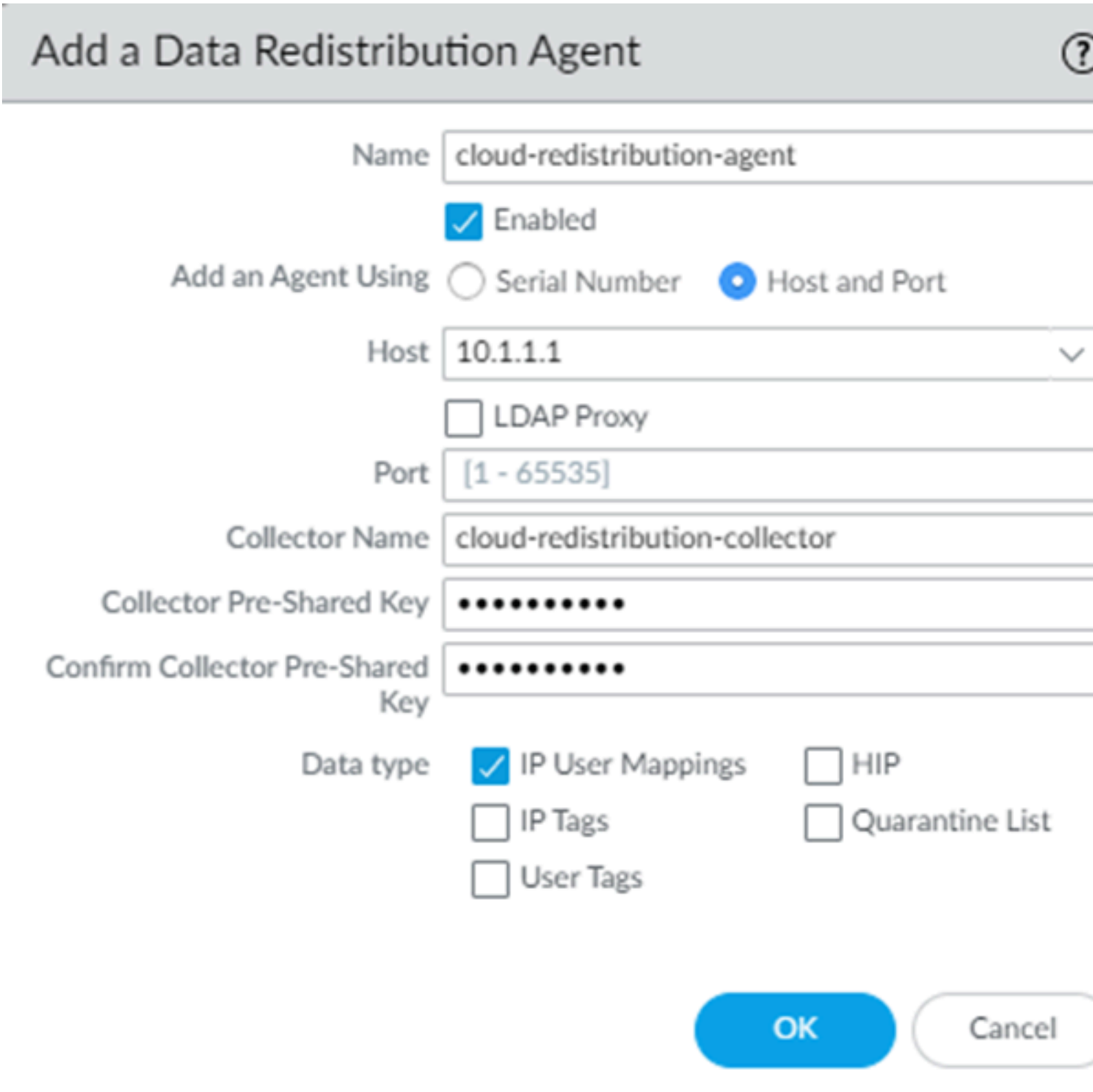


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure el cortafuegos local para recopilar la asignación de User-ID de Prisma Access.

1. Desde el cortafuegos local, seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**.
2. **Add (Añadir)** para añadir un agente de User-ID y asignarle un **Name (Nombre)**.
3. Seleccionar **Host and Port (Host y puerto)**.
4. Introduzca la **User-ID Agent Address (Dirección del agente de User-ID)** (para una conexión de servicio) o la **EBGP Router Address (Dirección del enrutador EBGP)** (para una conexión de red remota) de Prisma Access en el campo **Host**.
5. Introduzca el **Collector Name (Nombre del recopilador)** y la **Collector Pre-Shared Key (Clave precompartida de recopilador)** para el recopilador de Prisma Access que creó anteriormente en el procedimiento.
6. Seleccionar **IP User Mappings (asignaciones de usuario de IP)**.
7. Haga clic en **OK (Aceptar)**.
8. Repita estos pasos para cada conexión de servicio o conexión de red remota para la que desee redistribuir asignaciones.

 ©2025 Palo Alto Networks, Inc.



Redistribuir la información del User-ID desde un cortafuegos local a Prisma Access

Redistribuir la información de User-ID desde un cortafuegos local a Prisma Access.

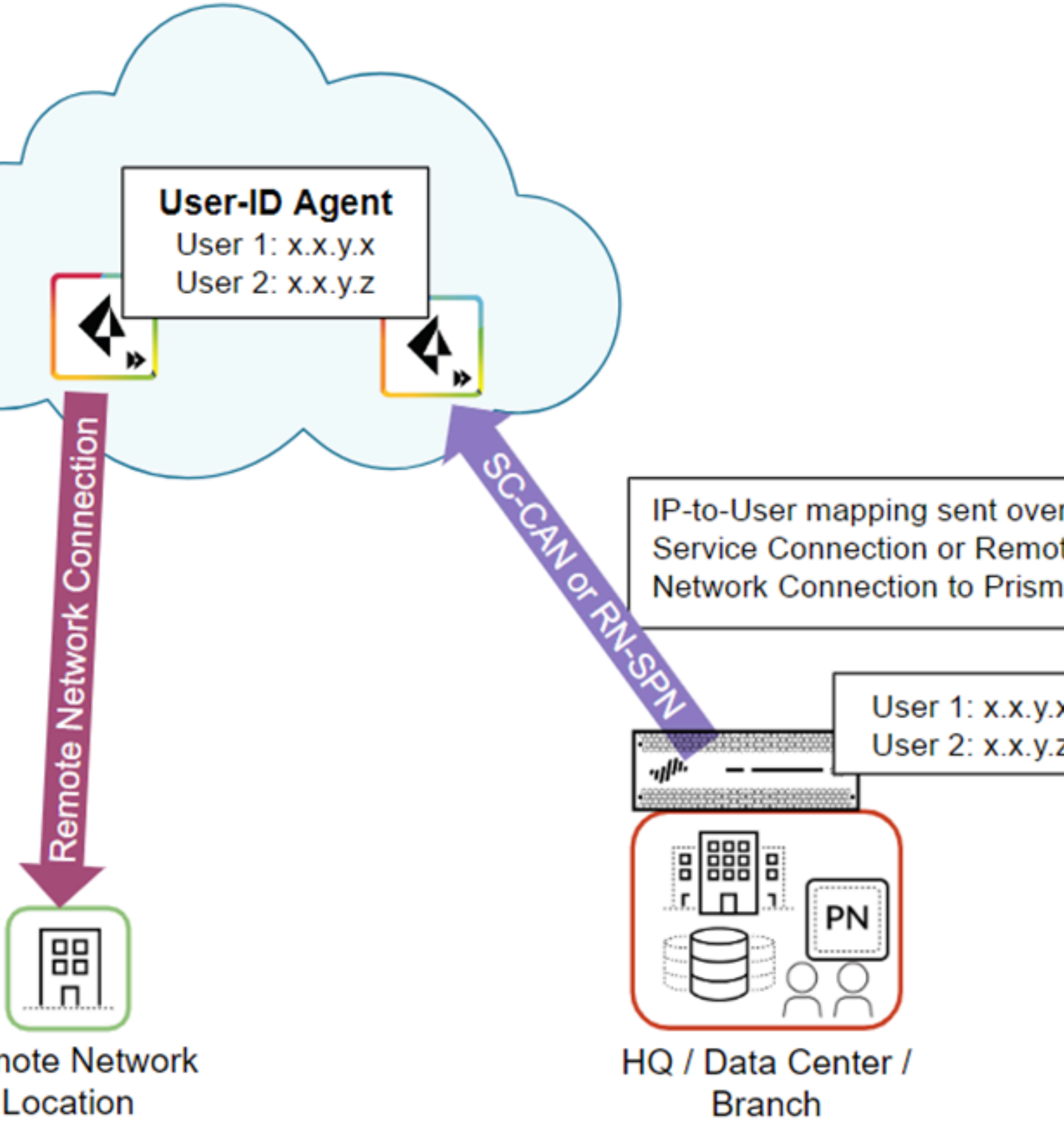
 ©2025 Palo Alto Networks, Inc.

En los casos en que los usuarios se encuentren en una ubicación de sucursal o en la sede central que esté protegida por un cortafuegos de nueva generación en las instalaciones con políticas basadas en usuarios, y necesiten acceder a recursos en otra ubicación de sucursal que haya protegido con Prisma Access, debe redistribuir las asignaciones de direcciones IP a nombres de usuario desde el cortafuegos en las instalaciones a Prisma Access.

La siguiente imagen muestra un centro de datos/sede central con un cortafuegos de nueva generación en las instalaciones con una asignación existente de direcciones IP a nombres de usuario. Prisma Access se conecta al cortafuegos ya sea con una conexión de servicio (SC-CAN) o una conexión de red remota (RN-SPN), y el cortafuegos en las instalaciones redistribuye la asignación a Prisma Access.

La siguiente imagen muestra una conexión de servicio de Prisma Access o una conexión de red remota que se utiliza para redistribuir la asignación. Puede usar cualquier ruta a través de un túnel IPSec de confianza para destinos con direcciones privadas para redistribuir esta asignación.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Para redistribuir las asignaciones de User-ID desde un cortafuegos local a Prisma Access, complete los siguientes pasos.

STEP 1 | Configure el cortafuegos local para redistribuir la información de User-ID a Prisma Access.

1. Desde el cortafuegos local, seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Collector Settings (Configuración del recopilador)**.
2. Para editar la configuración, haga clic en el engranaje.
3. Proporcione un **Collector Name (Nombre del recopilador)** y una **Collector Pre-Shared Key (Clave precompartida de recopilador)** para identificar el cortafuegos local como un agente de User-ID.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 2 | Configurar Prisma Access para recopilar la asignación de User-ID del cortafuegos local.

1. En el Panorama que gestiona Prisma Access, seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**.

   Asegúrese de haber seleccionado la plantilla **Service_Conn_Template** (para conexiones de servicio) o la plantilla **Remote_Network_Template** (para conexiones de red remota) en el menú desplegable de **Templates (Plantillas)** en la parte superior de la página.
2. **Add (Añadir)** para añadir un agente de User-ID y asignarle un **Name (Nombre)**.
3. Seleccionar **Host and Port (Host y puerto)**.
4. Introduzca la dirección IP de la interfaz MGT o la ruta de servicio que el cortafuegos utiliza para enviar asignaciones de usuario en el campo **Host**.

   Para la interfaz MGT, puede introducir un nombre de host en lugar de la dirección IP.
5. Introduzca el **Collector Name (Nombre del recopilador)** y la **Collector Pre-Shared Key (Clave precompartida de recopilador)** utilizando los valores del colector que usó para el cortafuegos local en el Paso 1.
6. Seleccionar **IP User Mappings (asignaciones de usuario de IP)**.
7. Haga clic en **OK (Aceptar)**.

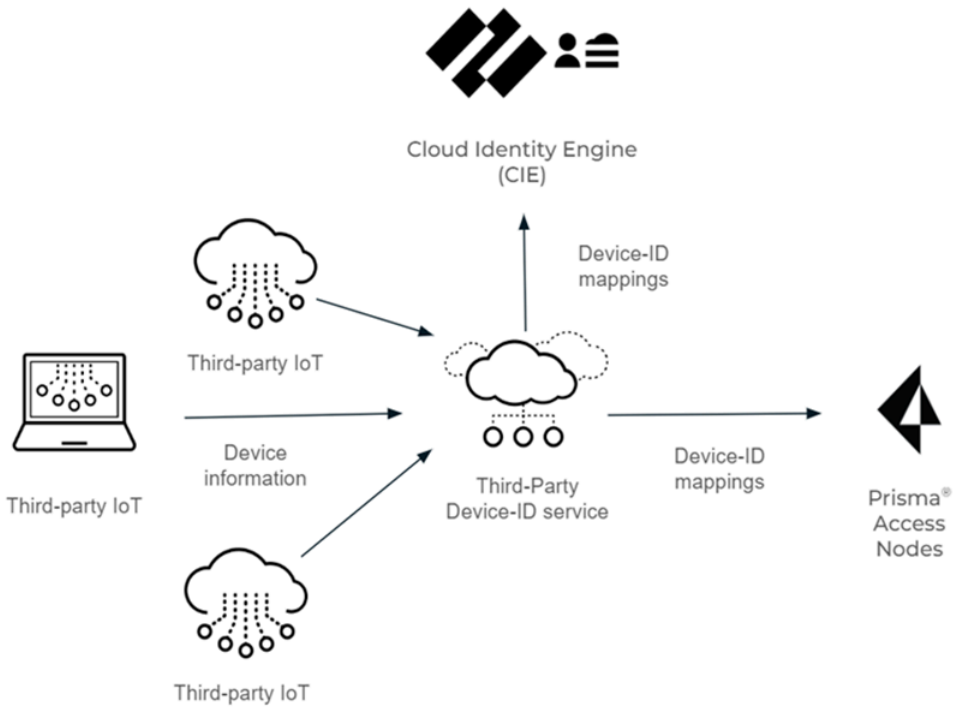
 ©2025 Palo Alto Networks, Inc.

Configurar el Device-ID de terceros en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si desea utilizar esta función en su entorno de Prisma Access, póngase en contacto con su equipo de cuenta para obtener más información.	❑ Licencia de Prisma Access con funcionalidad Cloud Identity Engine habilitada

Puede usar Cloud Identity Engine junto con Prisma Access para aplicar información de fuentes de detección de IoT de terceros para simplificar la tarea de identificar y cerrar las brechas de seguridad de los dispositivos de su red. Después de configurar un Device-ID de terceros en Cloud Identity Engine mediante una API, puede configurar un objeto de dispositivo y una regla de política de seguridad en Prisma Access para obtener y usar información de soluciones de visibilidad de IoT de terceros a través de Cloud Identity Engine para la visibilidad y el control de los dispositivos.

En la siguiente figura, el servicio de Device-ID de terceros recibe la información del dispositivo de las soluciones de IoT de terceros, que luego transmite como asignaciones de dirección IP a dispositivo a Cloud Identity Engine y a los Nodos de procesamiento de seguridad (SPN) de Prisma Access.



 ©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

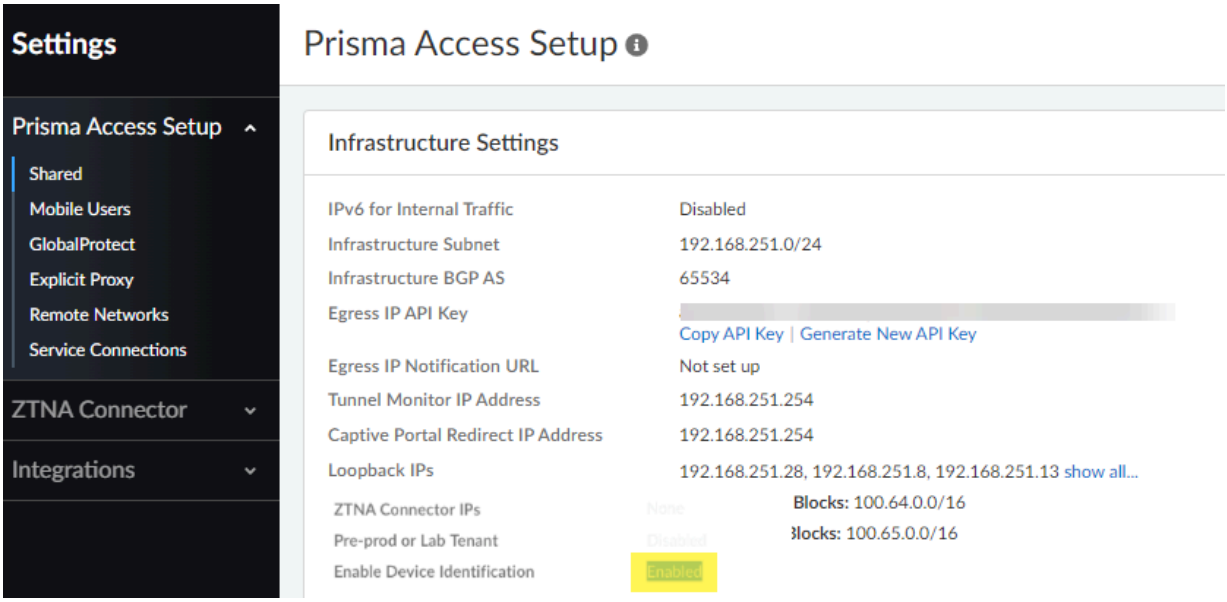
Configurar el Device-ID de terceros en Prisma Access (Strata Cloud Manager)

Para configurar el Device-ID de terceros, complete la siguiente tarea.

STEP 1 | Activar Device-ID de terceros en Cloud Identity Engine.

Este procedimiento incluye la carga de un certificado firmado y su uso con una API para comunicarse con el proveedor de IoT de terceros y descargarlo de él.

STEP 2 | Activar Device-ID de terceros en Prisma Access al ir a **Settings (Configuración)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Shared (Compartido)** o **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Accessy** establecer **Enable Device Identification (Habilitar la identificación de dispositivos)** como **Enabled (Habilitado)**.



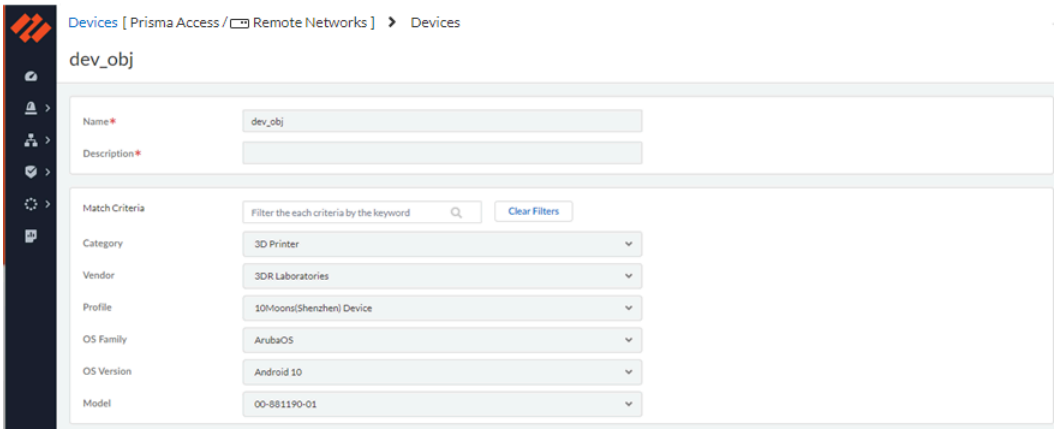
STEP 3 | Configure un objeto de dispositivo e introduzca los atributos del dispositivo. **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)**, establezca el ámbito de la configuración para **Remote Networks (Redes remotas)** y

 ©2025 Palo Alto Networks, Inc.

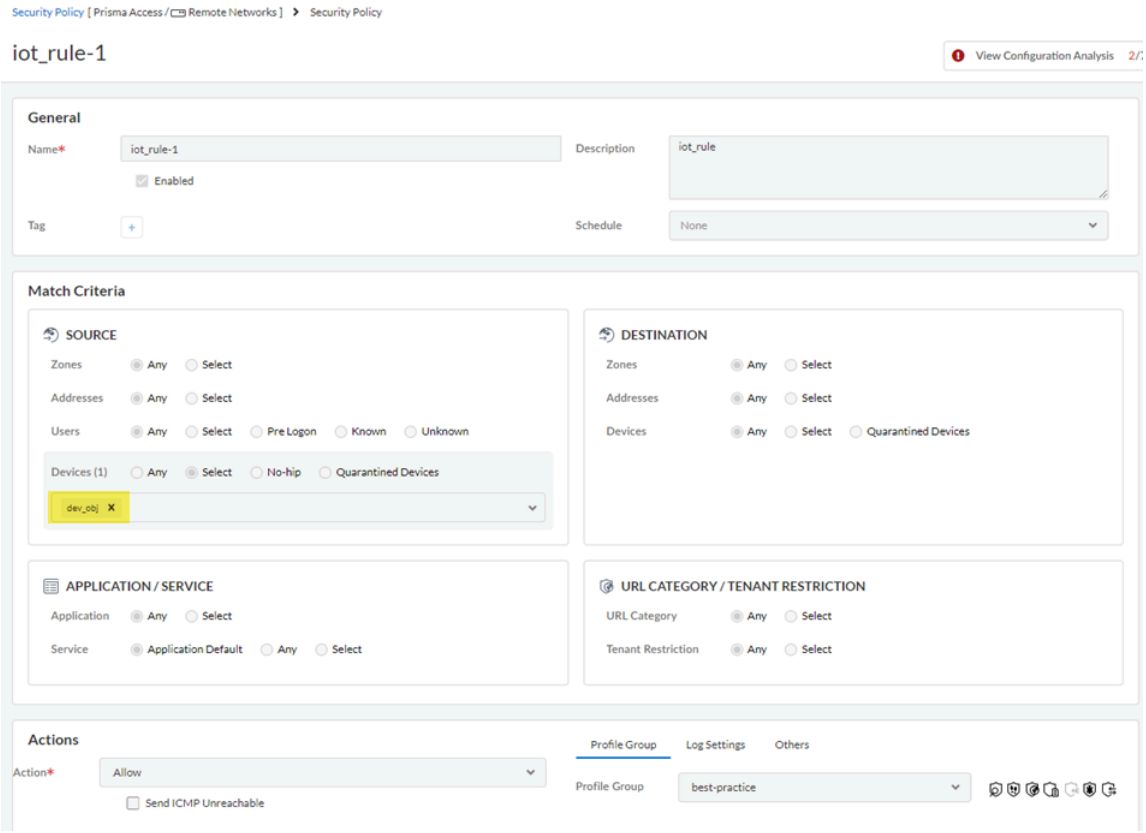
seleccione **Objects (Objetos)** > **Devices (Dispositivos)** y **Add Devices (Añadir dispositivos)**. Asegúrese de que se encuentra en el grupo de dispositivos de Redes remotas.

1. Añada un objeto de dispositivo que coincida con los atributos de los objetos de terceros.

   El área de **Mappings (Asignaciones)** de Cloud Identity Engine muestra los atributos de los dispositivos de terceros; puede utilizar cualquier atributo recuperado de allí.



STEP 4 | Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access (NGFW y Prisma Access)**, establezca el ámbito de la configuración para **Remote Networks (Redes remotas)** y seleccione **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)** y **Add (Añadir)** una política de seguridad, añadiendo los objetos de dispositivo que creó en el área **Devices (Dispositivos)**.

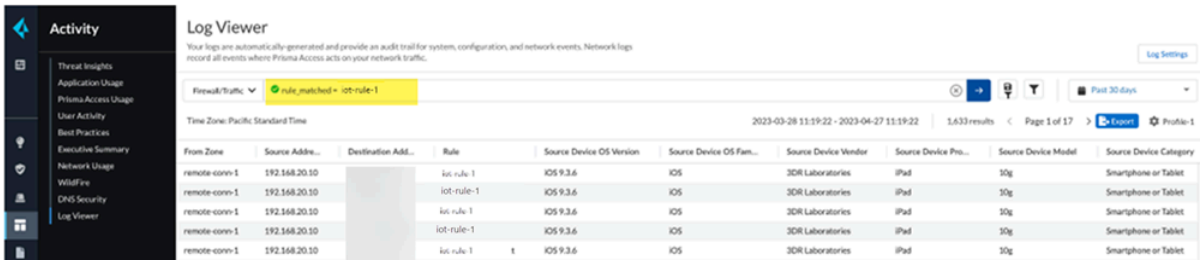


 ©2025 Palo Alto Networks, Inc.

STEP 5 | Debe **Push Config (Enviar configuración)** para guardar los cambios en el archivo de configuración de Prisma Access, asegurándose de seleccionar **Remote Networks (Redes remotas)** en el ámbito de envío.

STEP 6 | Verifique que Prisma Access está recibiendo los logs de Device-ID yendo a **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**, seleccionando **Firewall/ Traffic (Cortafuegos/tráfico)** y buscando tráfico según la regla que creó introduciendo `rule_matched = nombre de la regla` dónde *nombre de la regla* es la regla de política de seguridad que ha creado para los dispositivos IoT de terceros.

Las asignaciones de Device-ID a direcciones IP se muestran en los logs.



Configurar el Device-ID de terceros en Prisma Access (Panorama)

Para configurar el Device-ID de terceros, complete la siguiente tarea.

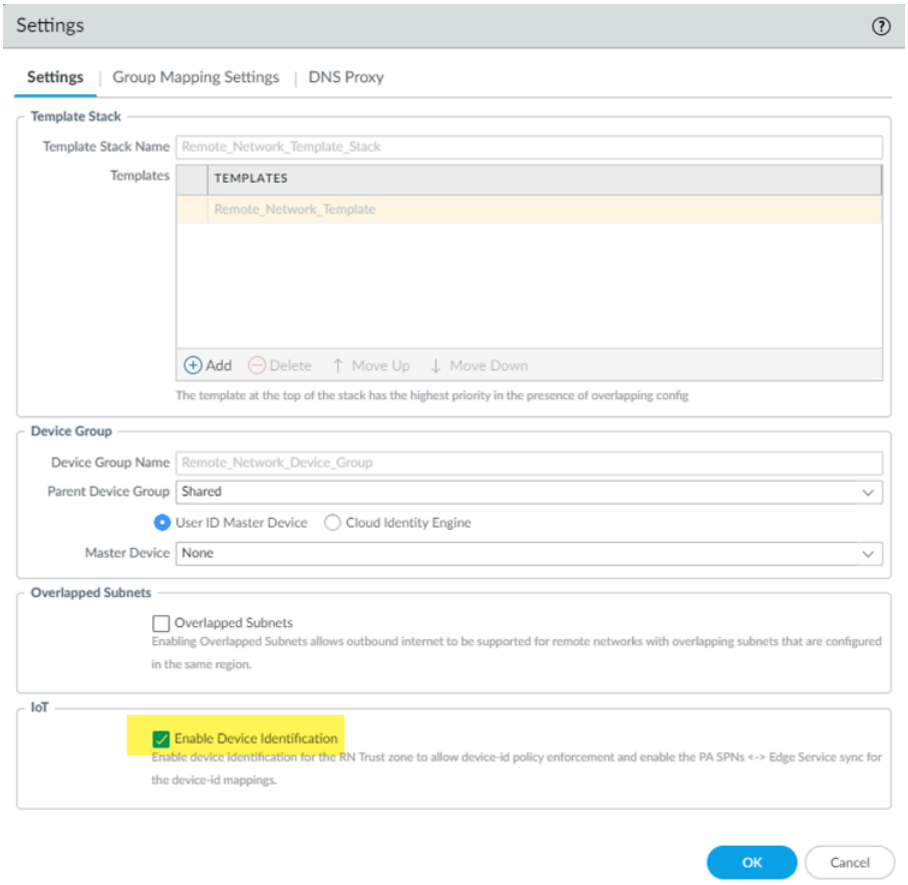
STEP 1 | Activar Device-ID de terceros en Cloud Identity Engine.

Este procedimiento incluye la carga de un certificado firmado y su uso con una API para comunicarse con el proveedor de IoT de terceros y descargarlo de él.

STEP 2 | Para activar Device-ID de terceros en Prisma Access vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**

 ©2025 Palo Alto Networks, Inc.

> **Settings (Configuración)**, haga clic en el engranaje para editar la **Settings (Configuración)** y seleccionar **Enable Device Identification (Habilitar la identificación de dispositivos)**.



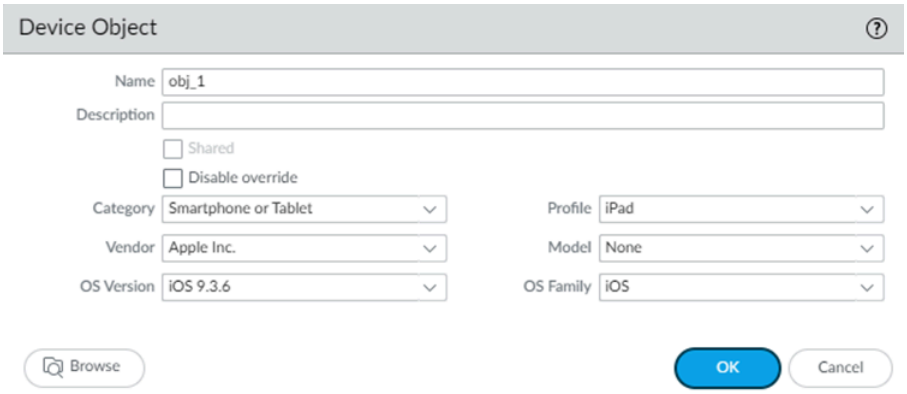
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure un objeto de dispositivo e introduzca los atributos del dispositivo.

1. Vaya a **Objects (Objetos)** > **Devices (Dispositivos)** y use **Add (Añadir)** para añadir un objeto de dispositivo que coincida con todos los atributos de ID de dispositivo.

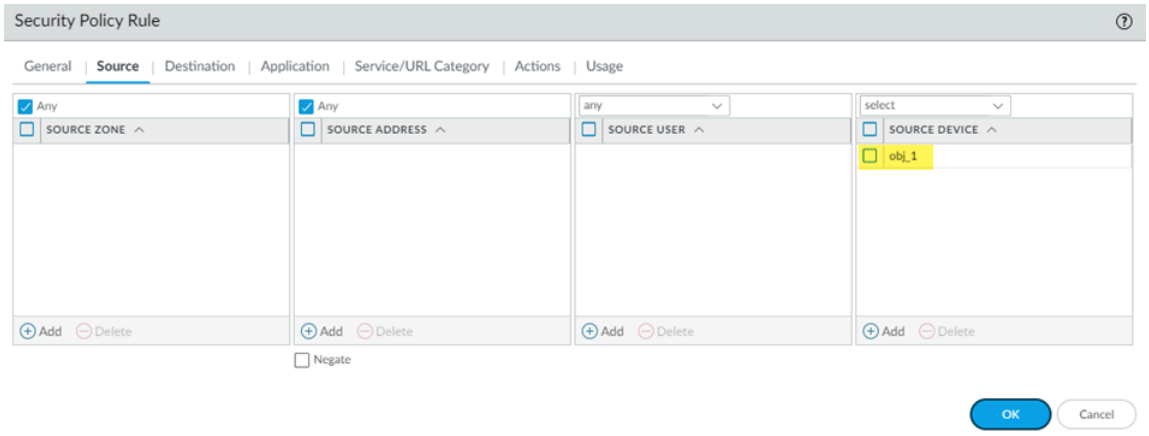
   Asegúrese de que está en **Remote_Network_Device_Group** o en el grupo de dispositivos **Shared (Compartido)**.
2. Elija **Add (Añadir)** un objeto de dispositivo que coincida con los atributos de los objetos de terceros.

   *El área de **Mappings (Asignaciones)** de Cloud Identity Engine muestra los atributos de los dispositivos de terceros; puede utilizar cualquier atributo recuperado de allí.*



STEP 4 | Vaya a **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Reglas previas)** y seleccione **Add (Añadir)** para añadir una política de seguridad, añadiendo los objetos de dispositivo que creó en el área de **Devices (Dispositivos)** como el **Source Device (Dispositivo de origen)**.

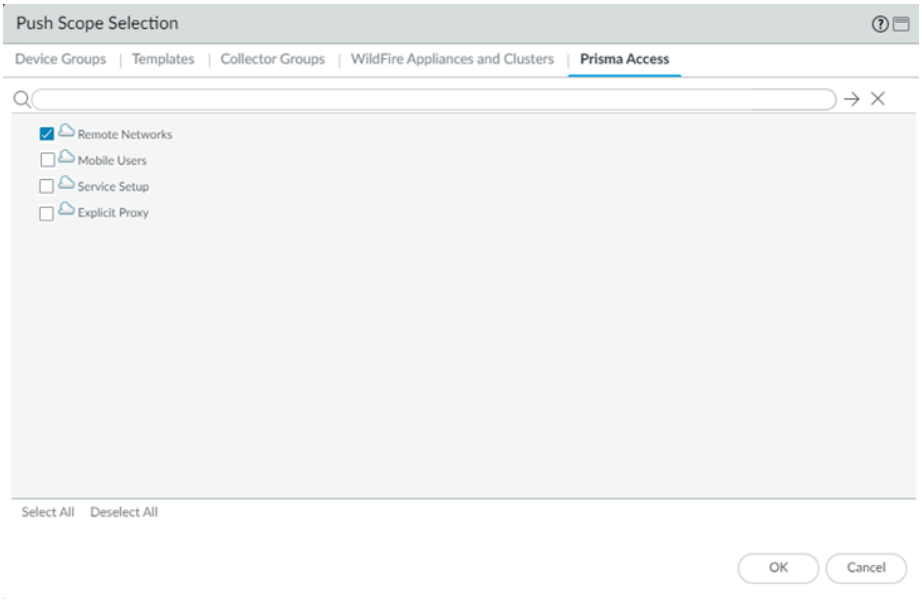
Asegúrese de que está en **Remote_Network_Device_Group** o en el grupo de dispositivos **Shared (Compartido)**.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Confirme y envíe sus cambios, asegurándose de que **Remote Networks (Redes remotas)** esté seleccionado en el **Push Scope (Ámbito de envío)**.

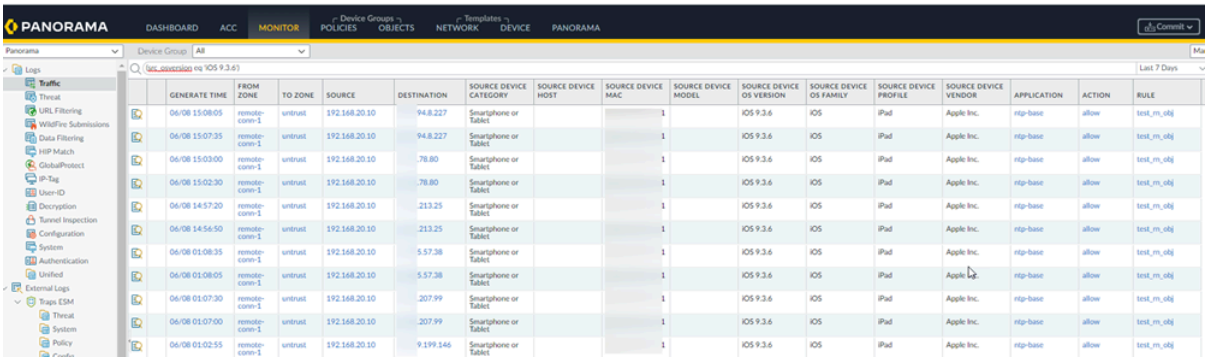
1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Debe **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access**, asegurarse de que **Remote Networks (Redes remotas)** esté seleccionada en **Push Scope (Alcance de envío)**, luego haga clic en **OK (Aceptar)**.



3. Haga clic en **Commit and Push (Confirmar y enviar)**.

STEP 6 | Verifica que Prisma Access está recibiendo los logs de Device-ID yendo a **Monitor (Supervisar)** > **Logs** y buscando los logs de **Traffic (Tráfico)** para el tráfico bajo la regla que creó introduciendo `rule_matched` = *rulename*, donde *rulename* es la regla de política de seguridad que creó para los dispositivos IoT de terceros.

Las asignaciones de Device-ID a direcciones IP se muestran en los logs.



 ©2025 Palo Alto Networks, Inc.

API de Device-ID de terceros

Una vez que se haya incorporado al servicio de Device-ID de terceros mediante la interfaz de usuario de Cloud Identity Engine, puede usar estas API para gestionar los *veredictos* o las asignaciones de dirección IP a dispositivo detectados en su red y almacenados en el servicio de Device-ID de terceros. Estas asignaciones indican a Prisma Access qué atributos pertenecen a un dispositivo con una dirección IP determinada para que pueda definir la política de seguridad que se dirige a dispositivos con atributos específicos.

Estas API no acceden directamente a los datos almacenados en su inquilino de Cloud Identity Engine. Más bien, las API interactúan con las asignaciones de dirección IP a dispositivo en el servicio de Device-ID de terceros, que comparte esas asignaciones con Cloud Identity Engine.

Las API de Device-ID de terceros utilizan un certificado, una clave de API y una URL base para las solicitudes de API. Para autenticar las solicitudes de API de Device-ID de terceros, debe utilizar el certificado firmado y el token API que obtuvo durante la incorporación en la interfaz de usuario de Cloud Identity Engine.

Cuando tenga un certificado y una clave API, puede realizar solicitudes al servicio de Device-ID de terceros. Proporcione al certificado su clave pública, la clave API y la URL base en cada solicitud. Ejemplo:

```
curl --cert onida1.crt --key onida.key "https://device-identity-
broker-beta.service-edge.panservicetest.com/:443/api/v1/token/
{apiKey}/verdicts"
```

- Veredictos de actualización
- Borrar todos los veredictos
- Veredictos de consulta
- Veredictos de consulta por dirección IP
- Estadísticas de veredictos de consulta

Veredictos de actualización

Añade, modifica o elimina asignaciones de direcciones IP a dispositivos.

Sinopsis

URI	`/api/v1/token/{apiKey}/verdicts:update`
Método HTTP	POST

Descripción

El Device-ID de terceros ingiere datos de fuentes de detección de IoT de terceros en su red y crea asignaciones de direcciones IP a dispositivos que Prisma Access puede usar para aplicar reglas de políticas de seguridad específicas del dispositivo. Utilice esta API para añadir una nueva asignación, modificar una asignación existente o eliminar una asignación.

 ©2025 Palo Alto Networks, Inc.

Puede agregar o modificar una asignación mediante el comando `actualizar` y se elimina una asignación mediante el campo `borrar`.

Si la asignación ya existe, `actualizar` sobrescribe los atributos de dispositivo existentes con los atributos especificados en el cuerpo de la solicitud. Si la asignación no existe, la actualización crea la nueva asignación.

Esta API no admite actualizaciones parciales. Si desea actualizar atributos específicos de una asignación, también debe volver a introducir los valores anteriores para los atributos que no desea actualizar. Si se dejan los atributos en blanco, se borrarán los valores existentes.

Puede actualizar o eliminar hasta 10.000 asignaciones a la vez. La solicitud es atómica: una respuesta correcta significa que el sistema procesó todo, y una respuesta de error significa que el sistema no procesó nada.

Campos

Campo	Descripción
actualizar	Un objeto JSON que proporciona los atributos de una asignación de dirección IP a dispositivo que desea actualizar o crear. Debe tener ip y al menos otro atributo rellenado.
eliminar	Un objeto JSON que especifica la dirección IP de la asignación que desea eliminar.

Por ejemplo:

```
{ "update": [ { "ip": "string", "serialNo": "string", "mac":
 "string", "category": "string", "vendor": "string", "model":
 "string", "os": "string", "osFamily": "string", "hostname":
 "string", "profile": "string", } ], "delete": [ { ip: "string" } ] }
```

Respuesta realizada correctamente

Tras realizarse correctamente, el código de respuesta HTTP es 200. Además, la respuesta contiene un objeto JSON con el siguiente campo:

Campo	Descripción
`updateTime`	Una marca de tiempo de Unix que representa cuándo se realizó correctamente la solicitud.

Por ejemplo:

```
{ "updateTime": unix-timestamp }
```

 ©2025 Palo Alto Networks, Inc.

Respuesta de error

Al producirse un error, el código de respuesta HTTP es uno de los siguientes:

Código de respuesta	Descripción
400	Solicitud no válida La solicitud estaba incompleta o mal formada de alguna manera. Arregle la solicitud antes de reintentarlo.
401	Token no autorizado. Pruebe a volver a generar su token API. Si eso no funciona, póngase en contacto con la asistencia.
409	Conflicto. La solicitud no se pudo procesar porque hay otro trabajo de actualización o eliminación en curso. Inténtalo de nuevo cuando termine el otro trabajo.
429	Demasiadas solicitudes La solicitud no se pudo procesar porque el sistema ha emitido demasiadas solicitudes en un período de tiempo específico. No supere más de una solicitud por segundo. Espere e inténtalo de nuevo.

Además, el órgano de respuesta contiene los siguientes campos:

Campo	Descripción
código	El código de error.
mensaje	El mensaje de error.

actualizar Objeto

Contiene la información necesaria para actualizar las asignaciones de direcciones IP a dispositivos. Este objeto JSON tiene los siguientes campos:

Campo	Descripción
ip	Dirección IP del dispositivo.
actualizar Hora	Marca de tiempo de Unix que representa cuándo se produjo la última actualizaci asignación.
categoría	Tipo de dispositivo. Ejemplo: Impresora
proveedor	Proveedor del dispositivo. Ejemplo: Corporación SHARP
modelo	Modelo de dispositivo. Ejemplo: MX-6070N

 ©2025 Palo Alto Networks, Inc.

os	Sistema operativo del dispositivo. Ejemplo: ThreadX 5
OsFamily	Familia a la que pertenece el sistema operativo del dispositivo. Ejemplo: ThreadX
perfil	Perfil del dispositivo. Ejemplo: Impresora Sharp

Borrar todos los veredictos

Elimina todas las asignaciones de direcciones IP a dispositivos del servicio Device-ID de terceros.

Sinopsis

URI	/api/v1/token/{apiKey}/verdicts:all
Método HTTP	ELIMINAR

Descripción

Pide al servicio de Device-ID de terceros que elimine todas las asignaciones de direcciones IP a dispositivos del servicio de Device-ID de terceros. Una respuesta exitosa significa que el servicio ha eliminado todas las asignaciones. Una respuesta de error significa que no puede eliminar ninguna asignación.

Respuesta exitosa

Tras realizarse correctamente, el código de respuesta HTTP es 200. El cuerpo de respuesta está vacío.

Respuesta de error

Al producirse un error, el código de respuesta HTTP es uno de los siguientes:

Código de respuesta	Descripción
401	Token no autorizado. Pruebe a volver a generar su token API. Si eso no funciona, póngase en contacto con la asistencia.
409	Conflicto. El sistema no pudo procesar la solicitud porque hay otra actualización o eliminación de trabajo en curso. Inténtalo de nuevo cuando termine el otro trabajo.
429	Demasiados errores. El sistema no pudo tramitar la solicitud porque ha emitido demasiadas solicitudes en un período de tiempo específico. No supere más de una solicitud por segundo. Espera e inténtalo de nuevo.

Además, el órgano de respuesta contiene los siguientes campos:

 ©2025 Palo Alto Networks, Inc.

Campo	Descripción
código	El código de error.
mensaje	El mensaje de error.

Veredictos de consulta

Recupera las asignaciones de dirección IP a dispositivo en el servicio Device-ID de terceros.

Sinopsis

URI	/api/v1/token/{apiKey}/verdicts? bookmark={STRING}&pageLen={INTEGER}
Método HTTP	OBTENER

Descripción

Devuelve todas las asignaciones o un subconjunto.

Para devolver todas las asignaciones, envíe la solicitud una vez sin ningún parámetro. Tome nota del valor de `nextBookmark` en la respuesta. Enviar otra solicitud utilizando ese valor para el `marcador` adjunto a la URI. La persona que llama repetirá la consulta hasta que el `recuento` esté vacío en la respuesta, indicando que ha devuelto todas las asignaciones.

Para devolver un subconjunto de asignaciones, especifique el número de asignaciones que desea recuperar con `pageLen`, hasta 10000.

Parámetros

Esta API acepta estos parámetros:

Parámetro	Descripción
marcador	(Opcional) Se utiliza después de la primera solicitud para devolver todas las asignaciones.
pageLen	(Opcional) El número de asignaciones a recuperar. El intervalo es de 1-10000. Si no se especifica, el valor predeterminado es 10000.

Respuesta realizada correctamente

Tras realizarse correctamente, el código de respuesta HTTP es 200. Además, la respuesta contiene un objeto JSON con los siguientes campos:

Campo	Descripción

 ©2025 Palo Alto Networks, Inc.

nextBookmark	El valor que utiliza en el parámetro marcador para realizar consultas repetidas ha devuelvan todas las asignaciones.
recuento	Entero que representa el número de asignaciones devueltos en la respuesta.
veredictos	Objeto que contiene las asignaciones especificadas en la solicitud.

Por ejemplo:

```
{ "nextBookmark": CkcKVxdWVuY2USAggEEjFqCHN, "count": 1, "verdicts" :
 [ { "ip": "10.10.10.10", "updateTime": 1623974506, "mac":
 "0a:d4:5f:e9:96:10", "category": "Smartphone or Tablet", "vendor":
 "Apple Inc.", "model": "iPad2", "os": "iOS 9.3.6", "osFamily":
 "iOS", "profile": "iPad" } ] } }
```

Respuesta de error

Al producirse un error, el código de respuesta HTTP es uno de los siguientes:

Código de respuesta	Descripción
400	Invalid request. La solicitud estaba incompleta o mal formada de alguna manera. Debería arreglar la solicitud antes de reintentarlo.
401	Token no autorizado.
429	Demasiadas solicitudes La solicitud no pudo tramitarse porque se habían present solicitudes en un período de tiempo determinado. No se permite más de una soli segundo. Espere e inténtelo de nuevo.

Además, el órgano de respuesta contiene los siguientes campos:

Campo	Descripción
código	El código de error.
mensaje	El mensaje de error.

Objeto veredictos

El objeto devuelto cuando se consulta correctamente una asignación de dirección IP a dispositivo. Este objeto contiene la siguiente información:

Campo	Descripción

 ©2025 Palo Alto Networks, Inc.

ip	Dirección IP del dispositivo.
updateTime	Marca de tiempo de Unix que representa cuándo se produjo la última actualizaci asignación.
categoría	Tipo de dispositivo Ejemplo: Impresora
proveedor	Proveedor del dispositivo. Ejemplo: Corporación SHARP
modelo	Modelo de dispositivo Ejemplo: MX-6070N
os	Sistema operativo del dispositivo. Ejemplo: ThreadX 5
osFamily	Familia a la que pertenece el sistema operativo del dispositivo. Ejemplo: ThreadX
perfil	Perfil del dispositivo. Ejemplo: Impresora Sharp

Veredictos de consulta por dirección IP

Recupera asignaciones de dirección IP a dispositivo basadas en la dirección IP.

Sinopsis

URI	/api/v1/token/{apiKey}/verdicts?ip={STRING}
Método HTTP	OBTENER

Descripción

Utiliza direcciones IP para devolver las asignaciones de dispositivos correspondientes. Puede recuperar varias asignaciones proporcionando una lista de hasta 10 direcciones IP, separadas por comas, adjuntas a la URI.

Si el servicio no puede encontrar una asignación asociada con una dirección IP, no devolverá una asignación para esa dirección IP.

Respuesta realizada correctamente

Tras realizarse correctamente, el código de respuesta HTTP es 200. Además, la respuesta contiene un objeto JSON con los siguientes campos:

Campo	Descripción
recuento	Entero que representa el número de asignaciones devueltos en la respuesta.
veredictos	Objeto que contiene las asignaciones de especificadas en la solicitud.

Por ejemplo:

 ©2025 Palo Alto Networks, Inc.

```
{ "count": 1, "verdicts" : [ { "ip": "10.10.10.10", "updateTime":
 1623974506, "mac": "0a:d4:5f:e9:96:10", "category": "Smartphone
 or Tablet", "vendor": "Apple Inc.", "model": "iPad2", "os": "iOS
 9.3.6", "osFamily": "iOS", "profile": "iPad" } ] } }
```


Respuesta de error

Al producirse un error, el código de respuesta HTTP es uno de los siguientes:

Código de respuesta	Descripción
400	Invalid request. La solicitud estaba incompleta o mal formada de alguna manera. Arregle la solicitud antes de reintentarlo.
401	Token no autorizado.
429	Demasiadas solicitudes El sistema no pudo tramitar la solicitud porque ha emitid solicitudes en un período de tiempo específico. No supere más de una solicitud p Espera e inténtalo de nuevo.

Además, el órgano de respuesta contiene los siguientes campos:

Campo	Descripción
código	El código de error.
mensaje	El mensaje de error.

Estadísticas de veredictos de consulta

Recupera estadísticas sobre el servicio Device-ID de terceros.

Sinopsis

URI	/api/v1/token/{apiKey}/verdicts:statistics
Método HTTP	OBTENER

Respuesta realizada correctamente

Tras realizarse correctamente, el código de respuesta HTTP es 200. Además, la respuesta contiene un objeto JSON con los siguientes campos:

Campo	Descripción

 ©2025 Palo Alto Networks, Inc.

veredictos	Objeto que contiene estadísticas sobre las asignaciones de direcciones IP a dispo inquilino. Contiene los siguientes campos: • totalCount: el número total de asignaciones de direcciones IP a dispositivos e • totalUpdate: el número de asignaciones de dirección IP a dispositivo que se ha desde que se crearon. • totalDelete: el número de asignaciones de dirección IP a dispositivo que se ha desde que se creó su inquilino.
requestRcvd	Objeto que contiene el número de veces que el inquilino recibió cada tipo de soli • update: el número de solicitudes de Veredictos de actualización recibidas. • deleteAll: el número de solicitudes de Borrar todos los veredictos recibidas. • consulta: el número de solicitudes de Veredictos de consulta y Veredictos de dirección IP recibidas. • Estadísticas: el número de solicitudes de Estadísticas de veredictos de consult

Por ejemplo:

```
{ "verdicts: { "totalCount": 1, "totalUpdate": 0, "totalDelete":
 0, }, "requestRcvd": { "update": 1, "deleteAll": 0, "query": 0,
 "statistics": 1 } }
```

Respuesta de error

Al producirse un error, el código de respuesta HTTP es uno de los siguientes:

Código de respuesta	Descripción
401	Token no autorizado.
429	Demasiadas solicitudes La solicitud no pudo tramitarse porque se habían present solicitudes en un período de tiempo determinado. No se permite más de una soli segundo. Espere e inténtelo de nuevo.

Además, el órgano de respuesta contiene los siguientes campos:

Campo	Descripción
código	El código de error.
mensaje	El mensaje de error.

 ©2025 Palo Alto Networks, Inc.

Multitenencia de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Esta sección solo proporciona información para gestionar varios inquilinos en Prisma Access (Panorama). Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.

Para permitirle crear y gestionar múltiples instancias de Prisma Access, Prisma Access ofrece multitenencia, lo que le permite crear hasta 200 instancias (inquilinos) en un solo dispositivo Panorama (o 2 dispositivos en modo de alta disponibilidad (HA)), y cada inquilino tiene sus propias plantillas y pilas de plantillas, grupos de dispositivos y dominios de acceso.

Las implementaciones existentes o futuras que no sean multiinquilino no se verán afectadas por la multitenencia y continuarán funcionando normalmente. Le recomendamos que habilite la multitenencia solo si su organización necesita gestionar varios inquilinos en Prisma Access.

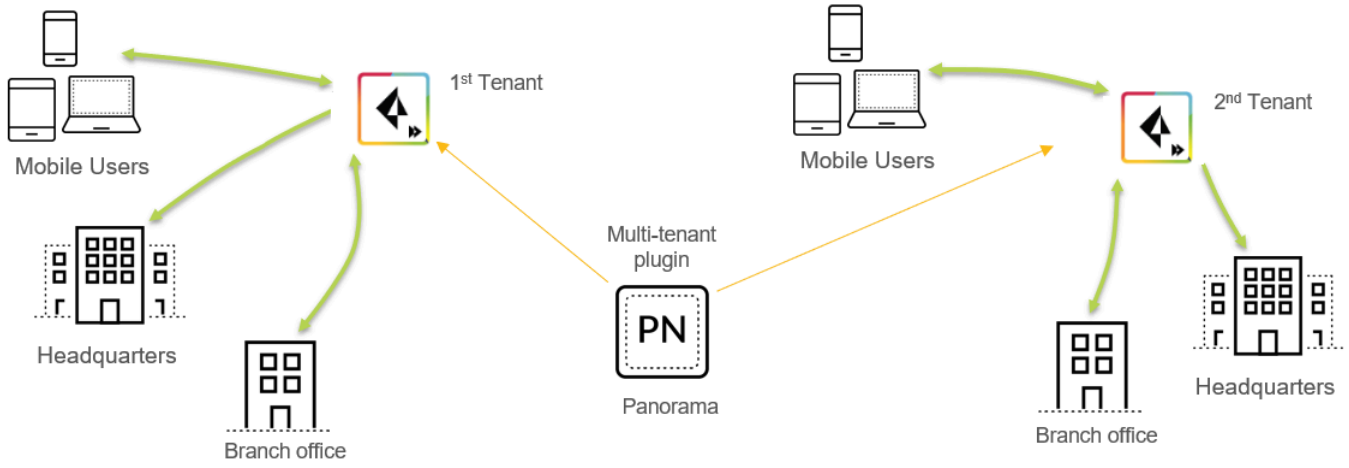
Esta sección solo proporciona las tareas que realiza para configurar inquilinos para redes remotas, usuarios móviles o una combinación de implementaciones de redes remotas y usuarios móviles. Para configurar el servicio Clean Pipe, consulte Prisma Access para Clean Pipe.

Descripción general de la configuración de multitenencia

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Habilitar la multitenencia le permite alojar varias instancias de Prisma Access en un solo dispositivo Panorama. Cada instancia se conoce como un *Inquilino*.

Los inquilinos de Prisma Access obtienen sus propias instancias dedicadas de Prisma Access y no se comparten entre inquilinos.



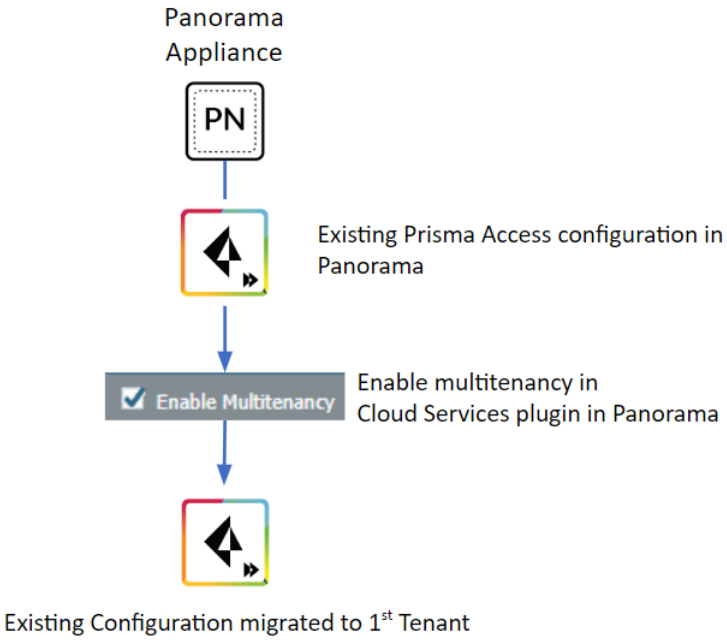
Utilice el siguiente flujo de trabajo para configurar la capacidad de gestionar varios inquilinos en un solo dispositivo Panorama:

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Habilitar la multitenencia. Si tiene una instancia de Prisma Access existente, habilitar la multitenencia migra automáticamente su configuración de Prisma Access existente al primer inquilino.

Le da un nombre al primer inquilino (migrado) y especifica un dominio de acceso. Prisma Access migra las plantillas, las pilas de plantillas y los grupos de dispositivos asociados con la configuración existente y los asocia con el dominio de acceso que crea.

Después de migrar su configuración inicial, el usuario administrativo en Panorama se convierte en un superusuario con la capacidad de crear y gestionar todos los inquilinos de Prisma Access.



STEP 2 | Luego, añada inquilinos a Prisma Access.

Para implementar múltiples inquilinos, asegúrese de tener los siguientes licencias como mínimo:

*Para determinar el tipo de licencia de Prisma Access que tiene de Panorama, seleccione **Panorama** > **Licenses (Licencias)**.*

- Si tiene una licencia de **Business**, **Business Premium**, **Zero Trust Network Access (ZTNA)** **Secure Internet Gateway (SIG)** o **Enterprise**, utilice los siguientes mínimos como una pauta:

  Prisma Access para redes y **Prisma Access para Usuarios**:

  Si tiene una Edición **Local**, se requiere una cantidad mínima de 200 unidades para cada inquilino, y todos los inquilinos serán Locales.

  Si tiene una Edición **Worldwide (Mundial)**, se requiere una cantidad mínima de 1.000 unidades para crear un inquilino **Worldwide (Mundial)**. Si asigna entre 200 y 999 unidades

 ©2025 Palo Alto Networks, Inc.

a un inquilino, Prisma Access crea un inquilino **Local**; si asigna 1.000 o más unidades a un inquilino, entonces Prisma Access crea un inquilino **Worldwide (Mundial)**.

Las *unidades* corresponden al ancho de banda en Mbps para Prisma Access para Redes remotas y al número de usuarios móviles para Prisma Access para Usuarios.

- Si su tipo de licencia comienza con **GlobalProtect Cloud Service**, utilice los siguientes mínimos como guía:

  Prisma Access para redes: debe tener un mínimo de 200 Mbps disponibles en su licencia para cada inquilino.

  Prisma Access para Usuarios: Debe tener un mínimo de 200 usuarios móviles disponibles en su licencia para cada inquilino.

  En ambos tipos de configuraciones de Prisma Access, puede añadir licencias adicionales (por encima de estos mínimos) de cualquiera de los tipos. Puede aumentar o disminuir el ancho de banda o la asignación de usuarios móviles para cualquier inquilino después de la incorporación, siempre que mantenga la asignación mínima requerida por inquilino y no se supere la capacidad total de licencias.

Puede configurar una configuración de varios inquilinos solo para redes remotas, solo para usuarios móviles o para ambos. Asigna licencias de acuerdo a cada inquilino cuando habilita la multitenencia.

Si tiene una licencia para redes remotas y usuarios móviles, puede configurar un inquilino individual solo con usuarios móviles o solo con redes remotas. Por ejemplo, si su implementación de Prisma Access tiene una licencia de edición **Mundial** para usuarios móviles y redes remotas, podría configurar un inquilino solo para usuarios móviles, siempre que especifique un mínimo de 1.000 usuarios móviles para el inquilino.

Para cada inquilino que cree después del primero, Prisma Access crea automáticamente plantillas, pilas de plantillas y grupos de dispositivos para cada inquilino y se asocian al dominio de acceso que crea. Prisma Access crea este entorno para permitirle crear un usuario administrativo a nivel de inquilino utilizando una función administrativa basada en los grupos de dispositivos y plantillas del inquilino, y luego crear un usuario administrativo basado en esa función. De esta manera, crea un usuario administrativo que tiene acceso a un solo inquilino

 ©2025 Palo Alto Networks, Inc.

sin permitir que ese usuario acceda a los otros inquilinos que son gestionados por el dispositivo Panorama.

Prisma Access crea pilas de plantillas, plantillas y grupos de dispositivos utilizando la siguiente convención de nombres:

- Una pila de plantillas de conexión de servicio con el nombre de **sc-stk***tenant*, donde *tenant* es el nombre del inquilino.
- Una plantilla de conexión de servicio con el nombre de **sc-tpl-***tenant*.
- Un grupo de dispositivos de conexión de servicio con el nombre de **sc-dg-***tenant*.
- Una pila de plantillas de usuarios móviles con el nombre de **mu-stk-***tenant*.
- Una plantilla de usuario móvil con el nombre de **mu-tpl-***tenant*.
- Un grupo de dispositivos de usuario móvil con el nombre de **mu-dg-***tenant*.
- Una pila de plantillas de red remota con el nombre de **rn-stk-***tenant*.
- Una plantilla de red remota con el nombre de **rn-tpl-***tenant*.
- Un grupo de dispositivos de red remota con el nombre de **rn-dg-***tenant*.
- Una pila de plantillas de proxy explícito con el nombre de **ep-stk-***tenant*.
- Una plantilla de proxy explícito con el nombre de **ep-tpl-***tenant*.
- Un grupo de dispositivos de proxy explícito con el nombre de **ep-dg-***tenant*.
- Una pila de plantillas de Clean Pipe con el nombre de **cp-stk-***tenant*.
- Una plantilla de Clean Pipe con el nombre de **cp-tpl-***tenant*.
- Un grupo de dispositivos Clean Pipe con el nombre de **cp-dg-***tenant*.

Las pilas de plantillas, las plantillas y los grupos de dispositivos se crean para todos los tipos de Prisma Access, incluso para aquellos para los que es posible que no tenga licencia. Por ejemplo, si compra una licencia para redes remotas, Prisma Access automáticamente se crean pilas de plantillas, plantillas y grupos de dispositivos para redes remotas, usuarios móviles y Clean Pipe.

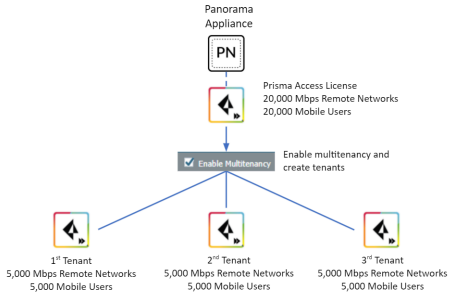
Si añade plantillas personalizadas, estas no pueden tener prioridad sobre las plantillas creadas de Prisma Access.

Asigna recursos de licencia de usuario móvil y de red remota para cada inquilino en función de la licencia que está asociada con el complemento de Servicios en la nube en Panorama.

La siguiente figura muestra una implementación de Prisma Access muestra que utiliza una licencia con un grupo de ancho de banda de red remoto de 20.000 Mbps y 20.000 usuarios móviles. El administrador asignó 5.000 Mbps en ancho de banda de red remota y 5.000 usuarios móviles para la configuración existente. Después de que el administrador habilitó la multitenencia, la asignación de licencias se migró junto con todas las otras configuraciones al primer inquilino. El administrador luego creó inquilinos adicionales, cada uno con un grupo de ancho de banda de 5.000 Mbps para redes remotas y 5.000 usuarios móviles para cada inquilino. Prisma Access asigna los recursos de licencia de la asignación general de licencias.

 ©2025 Palo Alto Networks, Inc.

Después de completar esta configuración, hay 5.000 Mbps de ancho de banda de red remoto y 5.000 usuarios móviles disponibles en la licencia.



 ©2025 Palo Alto Networks, Inc.

Planificar su implementación multiinquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	• Licencia de Prisma Access

Antes de habilitar la multitenencia, migrar al primer inquilino y crear inquilinos adicionales, asegúrese de tener toda la información y los recursos necesarios para hacerlo completando las siguientes tareas:

- ☐ Si va a migrar una implementación de un solo inquilino existente a una implementación de varios inquilinos, tenga en cuenta las siguientes características de Prisma Access que no son compatibles. Consulte la matriz de compatibilidad de Palo Alto Networks para obtener la lista de características no compatibles.
- ☐ Si no tiene una configuración de Prisma Access existente, deberá **Enable Multitenancy (Habilitar la multitenencia)** y añadir sus inquilinos; luego, configurar los inquilinos después de crearlos. Consulte Crear una implementación multiinquilino totalmente nueva para obtener más información.
- ☐ Tome nota de su asignación de licencia para redes remotas y usuarios móviles.

  Abra su licencia [**Panorama** > **Licenses (Licencias)**] y busque el **Total Mbps** de Prisma Access (grupo de ancho de banda de redes remotas) para redes remotas y el **User Limit (Límite de usuarios)** (número total de usuarios con licencia) para usuarios móviles.

  Cuando crea inquilinos, asigna recursos para redes remotas y usuarios móviles desde esta asignación de licencias. Si se queda sin los Mbps con licencia mínimos requeridos para redes remotas o usuarios móviles, no puede crear inquilinos adicionales.

  También debe tomar nota del ancho de banda y la asignación de usuarios móviles para su configuración existente. Después de migrar su configuración al primer inquilino, compruebe estos valores para verificar que el primer inquilino migró correctamente.
- ☐ Haga una lista de los nombres que usará para identificar a cada inquilino.

  Cuando cree nombres de inquilino, evite usar nombres como Inquilino-1, Inquilino-2, Inquilino-3, etc. Los logs del sistema reservan un pequeño número de caracteres para el nombre del inquilino en la salida del log y, si los inquilinos tienen nombres similares, puede ser difícil asociar al inquilino con los logs. Recomendamos usar un nombre corto y único para los inquilinos (por ejemplo, Acme o Hooli).

 ©2025 Palo Alto Networks, Inc.

- Haga una lista de los usuarios administrativos que creará y asignará para cada inquilino, y anote el número máximo de usuarios administrativos que pueden iniciar sesión simultáneamente.

  Cuando los usuarios administrativos están realizando operaciones multiinquilino normales, como cambios de configuración y operaciones de confirmación, recomendamos tener un máximo de 12 usuarios administrativos conectados a Panorama al mismo tiempo.

  Un usuario administrativo que puede gestionar varios inquilinos puede aprovisionar hasta 200 inquilinos al mismo tiempo con una sola operación de confirmación.
- Asegúrese de tener suficientes recursos de licencia para habilitar a varios inquilinos.

  La asignación mínima de licencias para cada inquilino es de 200 Mbps para cada red remota o 200 usuarios móviles. También puede crear un inquilino solo con redes remotas o usuarios móviles, y puede configurar inquilinos en diferentes configuraciones en el mismo Panorama. Por ejemplo, puede crear un inquilino solo con redes remotas, un inquilino solo con usuarios móviles o un inquilino tanto con usuarios móviles como con redes remotas, siempre que cada inquilino cumpla con la asignación mínima de licencias y las licencias pertinentes estén activadas y asociadas al Panorama donde configura los inquilinos.
- Al configurar un inquilino en modo multitenencia, cree un nombre único para cada túnel IPSec y puerta de enlace IKE para conexiones de servicio y conexiones de red remotas, e intente usar un nombre que no sea duplicado por otro inquilino. Si bien no hay ningún efecto en la funcionalidad, no puede eliminar un túnel IPSec o puerta de enlace IKE si otro inquilino está usando un túnel o puerta de enlace con el mismo nombre.

  Esta advertencia se aplica a todos los objetos, incluidos los perfiles de QoS (no se pueden eliminar objetos con nombres duplicados en una implementación de múltiples inquilinos si otro inquilino hace referencia a uno de los objetos).
- Los usuarios de un solo inquilino no pueden ver los logs del sistema; solo los superusuarios pueden. Sin embargo, puede ordenar logs por inquilino.
- Cuando un usuario móvil inicia sesión en un solo inquilino de Prisma Access, el usuario consume una unidad de licencia. Si un usuario inicia sesión en inquilinos adicionales bajo una única implementación de varios inquilinos, el usuario consume una unidad de licencia por cada inquilino que haya iniciado sesión. Por ejemplo, si un solo usuario inicia sesión en cinco inquilinos, el usuario consume cinco unidades de licencia de usuario móvil en total.
- Al utilizar la función multiinquilino e iniciar sesión como usuario administrativo de nivel de inquilino, al abrir el Administrador de tareas de Panorama (haciendo clic en **Tasks (Tareas)** en la parte inferior de la interfaz web de Panorama) se muestran todas las tareas para todos los inquilinos, incluidas las tareas realizadas a nivel de superusuario (Administrador).
- Algunas características de Prisma Access no son compatibles para su uso con multitenencia. Consulte Características no compatibles de multitenencia en la matriz de compatibilidad de Palo Alto Networks para obtener más detalles.

 ©2025 Palo Alto Networks, Inc.

- Si hace una copia de seguridad de una configuración de Panorama y la revierte a una configuración guardada anteriormente, Panorama no podrá volver a la configuración que guardó si realiza las siguientes acciones en el orden siguiente:

  1. Respaldar una configuración de Panorama
  2. Eliminar un inquilino.
  3. Restaurar la configuración.

  Si elimina un inquilino, no puede usar ninguna de las copias de seguridad anteriores que guardó antes de eliminarlo. Sin embargo, puede usar cualquier copia de seguridad que realice después de eliminar al inquilino.

 ©2025 Palo Alto Networks, Inc.

Crear una implementación multiinquilino totalmente nueva

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Si desea crear una implementación de varios inquilinos y no tiene una configuración de Prisma Access existente, puede **Enable Multitenancy (Habilitar multitenencia)** y añadir sus inquilinos; luego configurar los inquilinos después de crearlos.

Si tiene una implementación de un solo inquilino existente y desea migrar a una implementación de varios inquilinos, utilice el flujo de trabajo para habilitar la multitenencia y migrar el primer inquilino.

Cuando cree el primer inquilino sin configuración existente, asegúrese de las siguientes diferencias y pautas a seguir:

- Dado que no hay configuración para hacerse a un lado, Prisma Access crea plantillas, pilas de plantillas y grupos de dispositivos para cada inquilino y los asocia al dominio de acceso que usted cree durante la creación del inquilino. Consulte Descripción general de la configuración de multitenencia para la convención de nomenclatura que usa Prisma Access.
- Opcionalmente, después de crear el dominio de acceso de nivel de inquilino, puede crear un usuario administrativo que permita la administración de un solo inquilino mediante la asociación de un administrador al dominio de acceso.
- Si tiene plantillas o grupos de dispositivos existentes (por ejemplo, plantillas de un dispositivo local gestionado por Panorama que también debe utilizar Prisma Access), asegúrese de añadir esos grupos de dispositivos y dominios de plantillas al **Access Domain (Dominio de acceso)** cuando lo cree y lo configure. Si no añade grupos de dispositivos y plantillas al dominio de acceso, no podrá verlos ni seleccionarlos cuando configure los componentes de Prisma Access en el complemento Cloud Services.

 ©2025 Palo Alto Networks, Inc.

Habilitar la multitenencia y migrar el primer inquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Utilice el siguiente flujo de trabajo para habilitar la multitenencia y migrar su configuración existente al primer inquilino que cree. Si no tiene ninguna configuración existente, puede habilitar la multitenencia y añadir sus inquilinos; luego configúrelos.

Cuando habilita la multitenencia, Prisma Access migra los siguientes componentes de su configuración:

- Toda la información de conexión de servicio e incorporación de túnel de red remota, incluida la configuración del túnel.
- Información de incorporación para usuarios móviles existentes.
- Información de Strata Logging Service
- Configuración del Autonomous DEM (ADEM) existente
- Las plantillas, pilas de plantillas y grupos de dispositivos para conexiones de servicio, redes remotas y usuarios móviles.

Debe especificar la cantidad de usuarios (para una implementación de usuarios móviles), el ancho de banda (para una implementación de redes remotas) y el Autonomous DEM (ADEM) que se asignará para cada implementación (si ha comprado una licencia ADEM).

Debido a estos cambios en el grupo de dispositivos, se crea un dominio de acceso y se añaden grupos de dispositivos, plantillas y pilas de plantillas migrados, como se muestra en el flujo de trabajo a continuación.

Si no tiene una configuración de Prisma Access existente y está creando una implementación multiinquilino completamente nueva, no utilice este flujo de trabajo; en su lugar, complete los pasos en Añadir inquilinos a Prisma Access para crear el primer inquilino.

STEP 1 | Determine la cantidad de unidades con licencia que desea asignar a esta implementación.

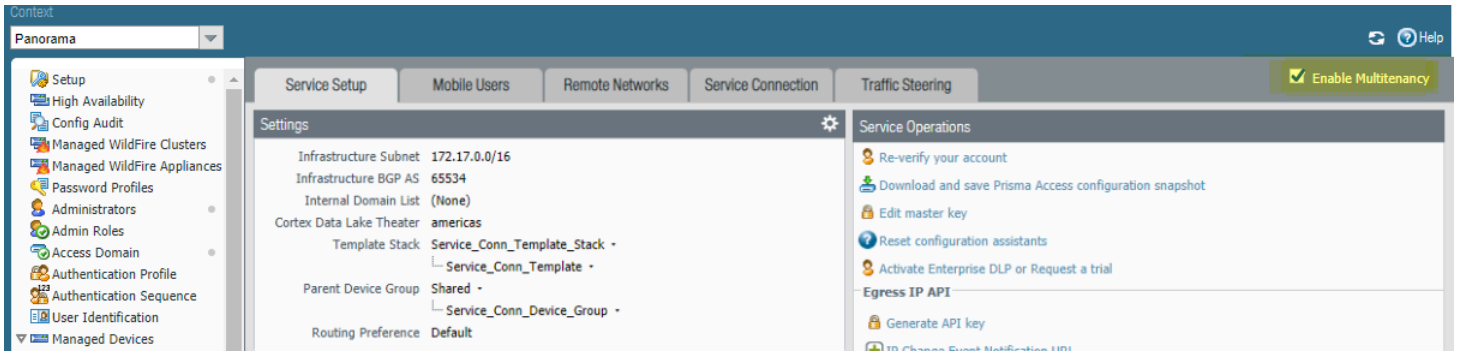
Mientras que Prisma Access migra su configuración al primer inquilino, debe especificar:

- El **Bandwidth (Ancho de banda)** que se asignará para la implementación de usuarios remotos del inquilino (si corresponde).
- Los **Users (Usuarios)** que asignarán para la implementación de usuarios móviles del inquilino (si corresponde).
- El número de unidades ADEM que se asignarán para usos móviles y redes remotas (si corresponde).

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)**.

STEP 3 | Seleccione **Enable Multitenancy (Habilitar Multitenencia)** (ubicado en la parte superior derecha de la página).



Después de habilitar la multitenencia, Panorama muestra una notificación que le informa que la configuración existente de Prisma Access pasa al primer inquilino.

Después de habilitar la multitenencia, su implementación cambia permanentemente a una implementación de varios inquilinos y no puede volver al modo de inquilino único.

STEP 4 | Haga clic en **OK (Aceptar)** para migrar la configuración existente al primer inquilino.

La página **Tenants (Inquilinos)** se muestra y se muestran gráficos circulares en el centro de la ventana.

- Si tiene una licencia de redes remotas o usuarios móviles, se mostrará la cantidad disponible de ancho de banda de red remota y usuarios móviles con licencia.
- (Solo redes remotas e implementaciones de usuarios móviles) Si ha adquirido una licencia de Autonomous DEM, se muestra el número de unidades disponibles para el uso de ADEM.
- Si tiene una implementación de Clean Pipe, se muestra la cantidad de ancho de banda para el inquilino.

STEP 5 | Seleccione el tipo de implementación que desea utilizar para el inquilino.

- Para una red remota, una implementación de usuario móvil o para configurar ambos tipos de implementación para un inquilino, seleccione **Remote Networks/Mobile Users (Redes remotas/Usuarios móviles**.
- Para una implementación de clean pipe, seleccione **Clean Pipe**.

  Esta sección solo describe cómo configurar inquilinos para tipos de implementación de red remota, usuario móvil o ambos. Para configurar el servicio de clean pipe, consulte Prisma Access para Clean Pipe.

 ©2025 Palo Alto Networks, Inc.

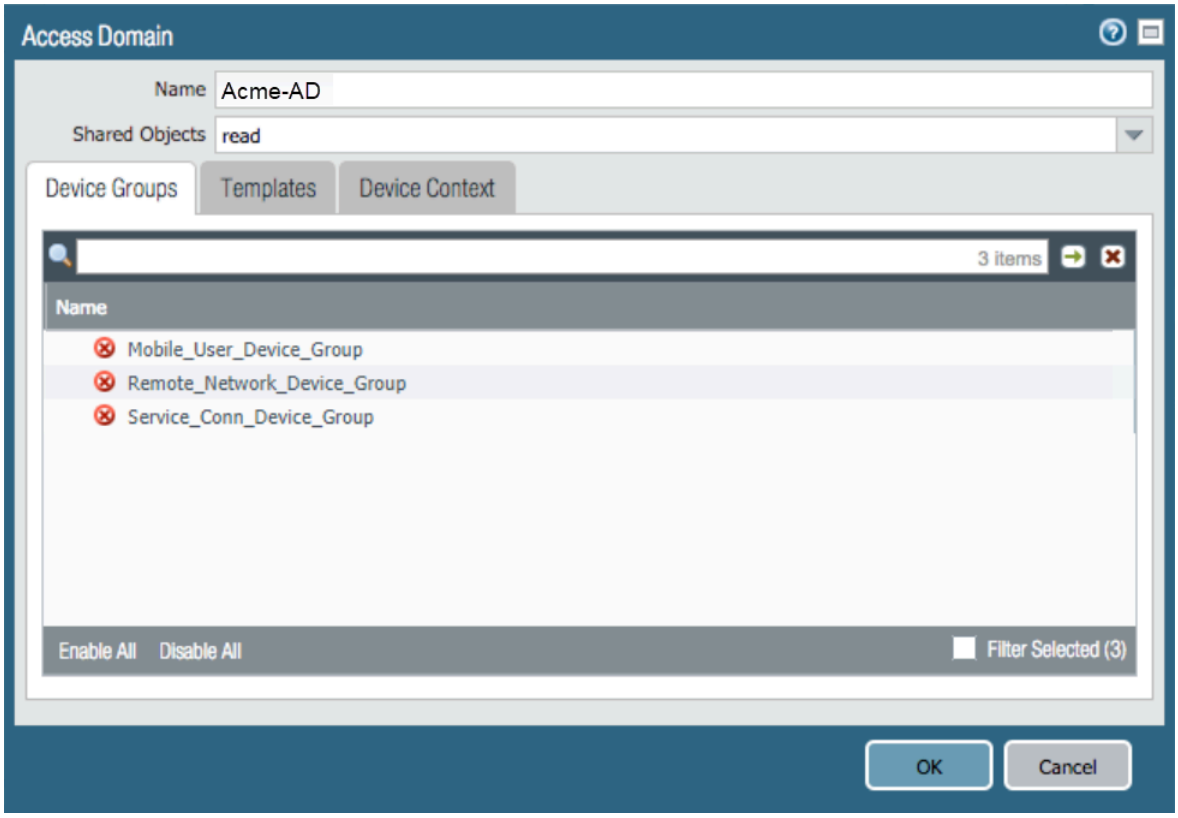
STEP 6 | Migre la configuración existente al primer inquilino.

El nombre del primer subinquilino migrado se completa automáticamente a partir del inquilino que está migrando y no se puede editar.

1. Cree un nuevo **Access Domain (Dominio de acceso)** haciendo clic en la flecha hacia abajo y seleccionando **New Access Domain (Nuevo dominio de acceso)**.
2. Introduzca un **Name (Nombre)** para el dominio de acceso y haga clic en **OK (Aceptar)**.

   Prisma Access añade los **Device Groups (Grupos de dispositivos)** **Mobile_User_Device_Group**, **Remote_Network_Device_Group** y **Service_Conn_Device_Group** al nuevo dominio de acceso.

   No asocie los Grupos de dispositivos y Plantillas predeterminados a otros subinquilinos que no sean el primer subinquilino migrado.

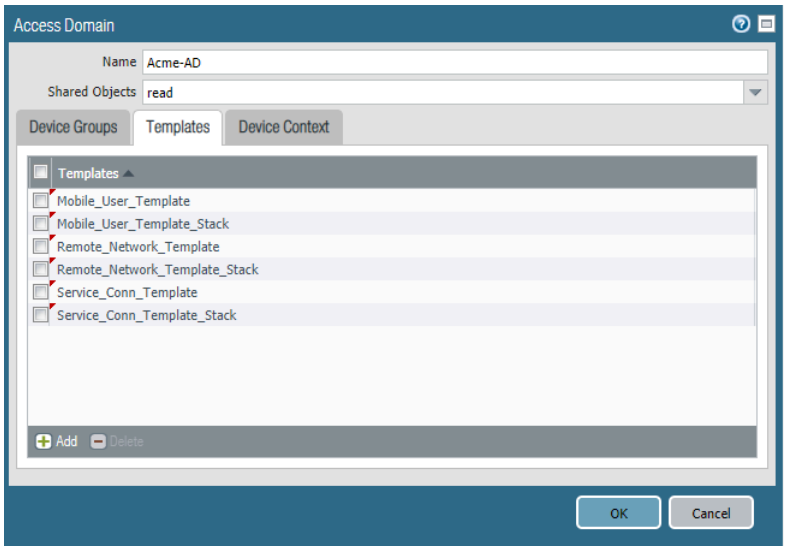


3. (Opcional) Haga clic en **Templates (Plantillas)** para verificar que Prisma Access añadió las siguientes plantillas y pilas de plantillas:
   - **Explicit_Proxy_Template**
   - **Explicit_Proxy_Template_Stack**
   - **Mobile_User_Template**
   - **Mobile_User_Template_Stack**
   - **Remote_Network_Template**
   - **Remote_Network_Template_Stack**
   - **Service_Conn_Template**

 ©2025 Palo Alto Networks, Inc.

- **Service_Conn_Template_Stack**

  Estas son las plantillas y pilas de plantillas predeterminadas para una implementación estándar de Prisma Access; si agregó otras plantillas, asegúrese de que Prisma Access las añadió.



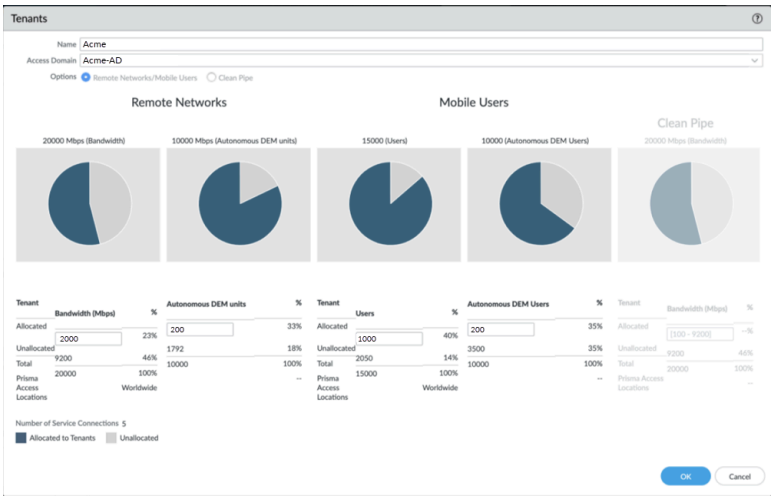
4. (Opcional) Si tiene otras plantillas asociadas con esta configuración, selecciónelas.
5. Haga clic en **OK (Aceptar)** para cerrar la página **Access Domain (Dominio de acceso)** y regresar a la página **Tenants (Inquilinos)**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Introduzca los valores en **Bandwidth (Ancho de banda) (Mbps)** para redes remotas, **Users (Usuarios)** para usuarios móviles y el número de **Autonomous DEM Users (Usuarios de Autonomous DEM)** que desea asignar para cada tipo de implementación.

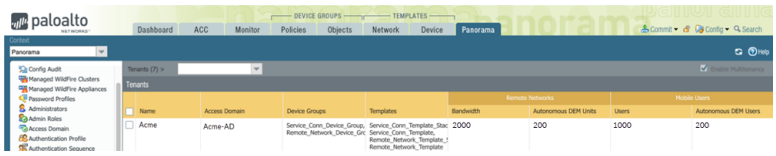
Utilice las siguientes pautas al asignar unidades ADEM a un inquilino:

- El número de unidades ADEM que puede asignar para usuarios móviles y redes remotas solo puede ser igual o menor que la licencia base.
- El número mínimo de unidades que puede asignar es 200.
- Después de asignar las unidades ADEM para un inquilino, puede editar o eliminar esas unidades.
- Si no compró una licencia de ADEM para su tipo de implementación (Usuarios móviles o Redes remotas), esa opción estará atenuada.



STEP 8 | Haga clic en **OK (Aceptar)**.

La página **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** muestra el primer inquilino migrado correctamente y se añade un menú desplegable **Tenants (Inquilinos)** por encima del área **Tenants (Inquilinos)**.



 ©2025 Palo Alto Networks, Inc.

STEP 9 | Asegúrese de que todas las plantillas y los grupos de dispositivos se hayan completado en el inquilino.

1. Seleccione el inquilino de la lista desplegable.
2. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)**.
3. Seleccione **Service Setup (Configuración del servicio)**.
4. Haga clic en el engranaje para editar la **Settings (Configuración)**.
5. Asegúrese de que la pila de plantillas, la plantilla y el grupo de dispositivos correctos (Service_Conn_Template_Stack, Service_Conn_Template y Service_Conn_Device_Group, respectivamente) se hayan completado en la configuración.
6. Vaya a otras pestañas para las que tenga una configuración existente [por ejemplo, **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**, **Mobile Users—Explicit Proxy (Usuarios móviles: Proxy explícito)**, **Remote Networks (Redes remotas)** o **Service Connection (Conexión de servicio)**], haga clic en el engranaje para editar la **Settings (Configuración)** y asegúrese de que la pila de plantillas, la plantilla y el grupo de dispositivos correctos se hayan completado en la configuración.

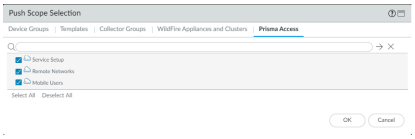
STEP 10 | Confirme sus cambios localmente en Panorama (**Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 11 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar con Panorama)**para guardar sus cambios localmente en el Panorama que gestiona Prisma Access.

Si no realiza una confirmación local, los componentes de Prisma Access no se muestran en el ámbito de envío cuando usted confirma y envía sus cambios.

STEP 12 | Confirme y envíe sus cambios para hacerlos activos en Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Prisma Access**, luego seleccione el inquilino que creó, **Service Setup (Configuración de servicio)**, **Remote Networks (Redes remotas)** y **Mobile Users (Usuarios móviles)**.

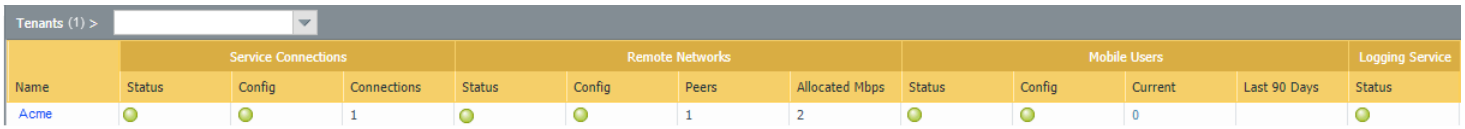


3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Haga clic en **Commit (Confirmar)** y **Push (Enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 13 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)**.

La página de estado muestra el estado de todos los inquilinos. Debido a que ha creado un solo inquilino, ese inquilino es el único que se muestra. Si selecciona ese inquilino en el menú desplegable, se mostrará un estado detallado de ese inquilino.



Al seleccionar un inquilino del menú desplegable, regresará a la página de Estado de ese inquilino.

STEP 14 | Continúe añadiendo más inquilinos a Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Añadir inquilinos a Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Después de migrar la información existente como primer inquilino, puede crear y configurar inquilinos adicionales. Para cada inquilino que cree después del primero, Prisma Access crea un dominio de acceso separado con su propio conjunto de pilas de plantillas y plantillas y sus propios grupos de dominio.

Utilice este flujo de trabajo para añadir más inquilinos a Prisma Access.

Si está creando una implementación de varios inquilinos completamente nueva, utilice este flujo de trabajo para añadir el primer inquilino, así como también inquilinos adicionales. Consulte Crear una implementación multiinquilino totalmente nueva *para obtener más información.*

STEP 1 | Inicie sesión en Panorama como superusuario.

STEP 2 | Añada y configure el inquilino.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** y luego **Add (Añadir)** un nuevo inquilino.

   Asegúrese de seleccionar **Remote Networks/Mobile User (Redes remotas/Usuarios móviles)**; para crear y configurar una implementación de Clean Pipe, consulte Prisma Access para Clean Pipe.
2. Introduzca un **Name (Nombre)** descriptivo para la plantilla.
3. Seleccione **Add (Añadir)** un nuevo **Access Domain (Dominio de acceso)**, asígnele un **Name (Nombre)**descriptivo y haga clic en **OK (Aceptar)** para volver a la ventana **Tenants (Inquilinos)**.

   Después de hacer clic en **OK (Aceptar)**, Prisma Access crea automáticamente plantillas, pilas de plantillas y grupos de dispositivos y los asocia al dominio de acceso que usted crea.

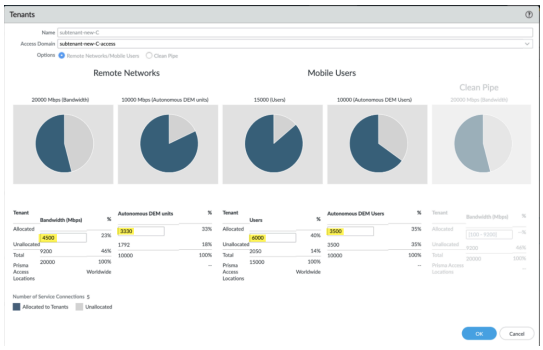
STEP 3 | Especifique la cantidad de **Bandwidth (Mbps) [Ancho de banda (Mbps)]** a asignar para las **Remote Networks (Redes remotas)** y el número de **Users (Usuarios)** a asignar para los **Mobile Users (Usuarios móviles)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Solo implementaciones con Autonomous DEM) Si ha adquirido una licencia de Autonomous DEM (ADEM), seleccione el número de unidades que desea asignar para ADEM.

Utilice las siguientes pautas al asignar unidades ADEM a un inquilino:

- El número de unidades ADEM que puede asignar para usuarios móviles y redes remotas solo puede ser igual o menor que la licencia base.
- El número mínimo de unidades que puede asignar es 200.
- Después de asignar las unidades ADEM para un inquilino, puede editar o eliminar esas unidades.
- Si no compró una licencia de ADEM para su tipo de implementación (Usuarios móviles o Redes remotas), esa opción estará atenuada.

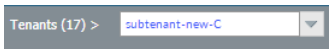


STEP 5 | Haga clic en **OK (Aceptar)** para crear el primer inquilino.

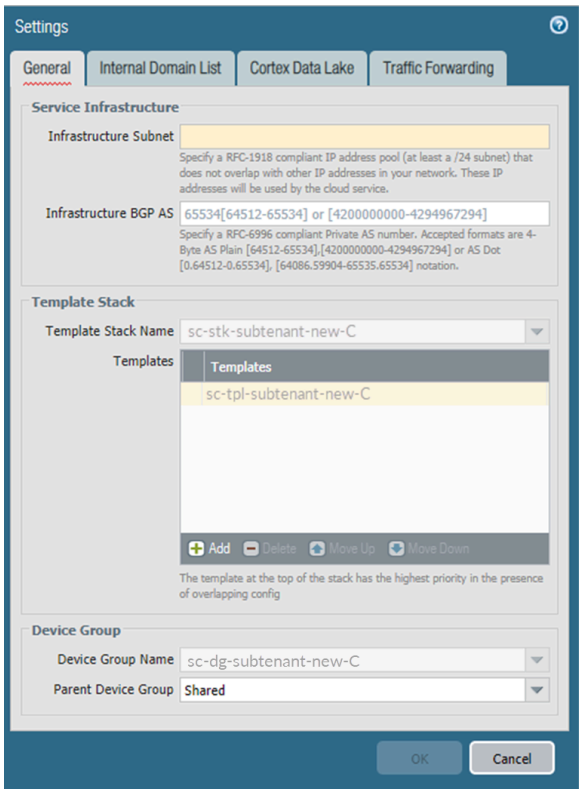
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Asegúrese de que Prisma Access aplicó la pila de plantillas, la plantilla y la configuración del servicio del grupo de dispositivos a la configuración de conexión de servicio del inquilino que acaba de crear.

1. Seleccione el inquilino que creó en el menú desplegable **Tenant (Inquilino)**.



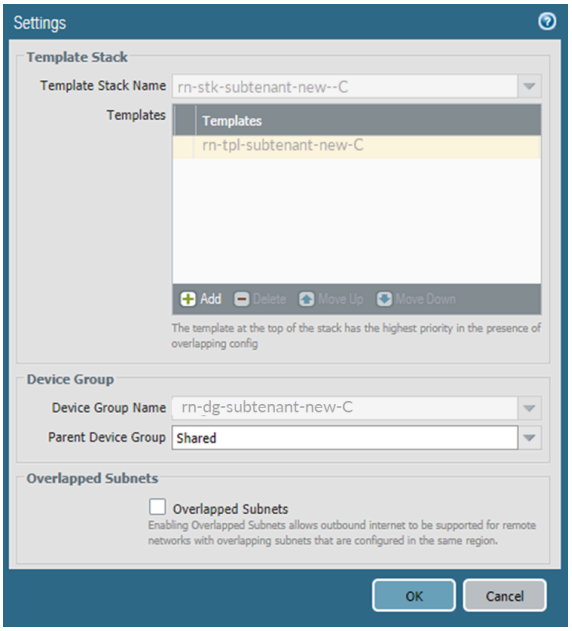
2. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.
3. Haga clic en el icono de engranaje a la derecha del área de **Settings (Configuración)** para editar la configuración.
4. Asegúrese de que Prisma Access ha asociado la pila de plantillas (**sc-stk-***tenant*), la plantilla (**sc-tpl-***tenant*) y el grupo de dispositivos (**sc-dg-***tenant*) a la configuración de conexión de su servicio.
5. Asegúrese de que el **Parent Device Group (Grupo de dispositivos primario)** esté configurado como **Shared (Compartido)** y haga clic en **OK (Aceptar)**.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Asegúrese de que Prisma Access ha aplicado la pila de plantillas, la plantilla y el grupo de dispositivos a la configuración de red remota.

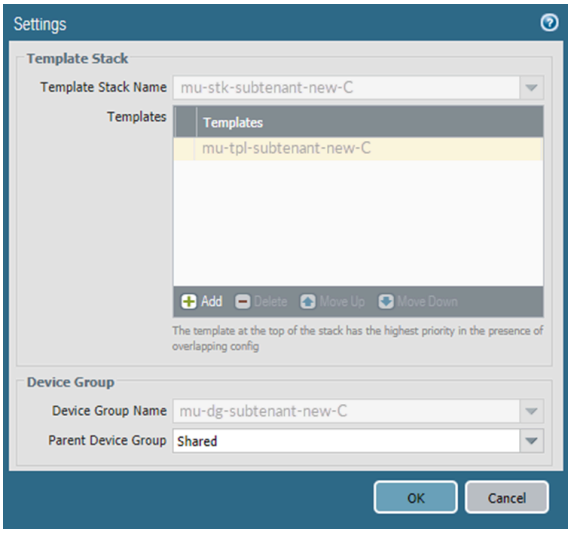
1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks Redes remotas)** y haga clic en el icono de engranaje a la derecha del área de **Settings (Configuración)** para editar la configuración.
2. Asegúrese de que Prisma Access ha asociado la pila de plantillas (**rn-stk-***tenant*), la plantilla (**rn-tpl-***tenant*) y el grupo de dispositivos (**rn-dg-***tenant*) a su configuración de red remota.
3. Asegúrese de que el **Parent Device Group (Grupo de dispositivos primario)** esté configurado como **Shared (Compartido)** y haga clic en **OK (Aceptar)**.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Asegúrese de que Prisma Access aplicó la pila de plantillas, la plantilla y el grupo de dispositivos a la configuración del usuario móvil.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)** y haga clic en el icono de engranaje a la derecha del área **Settings (Configuración)** para editar la configuración.
2. Asegúrese de que Prisma Access ha asociado la pila de plantillas (**mu-stk-***tenant*), la plantilla (**mu-tpl-***tenant*) y el grupo de dispositivos (**mu-dg-***tenant*) a su configuración de red remota.
3. Asegúrese de que el **Parent Device Group (Grupo de dispositivos primario)** esté configurado como **Shared (Compartido)** y haga clic en **OK (Aceptar)**.



STEP 9 | Confirme sus cambios localmente en Panorama (**Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.

STEP 10 | (Solo implementaciones de usuarios móviles): añada una subred de infraestructura, luego confirme y envíe sus cambios para que estén activos en Prisma Access.

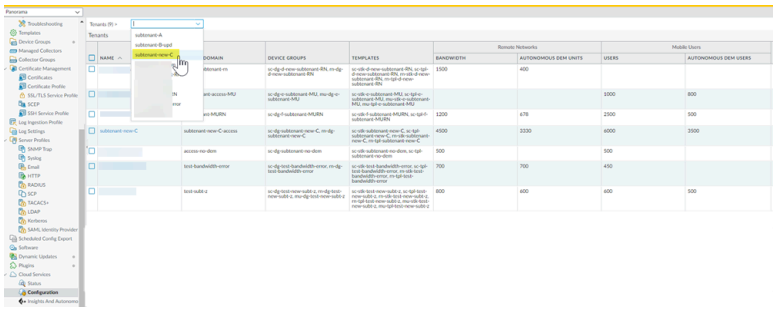
Estos pasos son necesarios para que los cambios realizados al usuario móvil surtan efecto.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicio)**, haga clic en el icono de engranaje para editar la Configuración y configure una subred de infraestructura.
2. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**, **Edit Selections (Editar selecciones)** en el Ámbito de envío y asegúrese de que **Mobile Users (Usuarios móviles)** esté seleccionado.
3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Seleccione **Commit (Confirmar)** y **Push (Enviar)**sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | Seleccione el nuevo inquilino que creó seleccionando **Panorama** > **Cloud Services Servicios en la nube)** > **Configuration (Configuración)** > ***tenant-name*** y continúe con la configuración de su inquilino.

1. Configurar la infraestructura del servicio.
2. Crear una conexión de servicio para permitir el acceso a aplicaciones privadas.
3. Incorpore y configure redes remotas si tiene licencia para redes remotas.
4. Configurar Global Protect para Prisma Access (Managed by Panorama) si tiene licencia para usuarios remotos.



 ©2025 Palo Alto Networks, Inc.

Eliminar un inquilino

Elimine un inquilino en una implementación de Prisma Access (Managed by Panorama) completando los siguientes pasos.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ LicenciaPrisma Access

- *Si bien puede eliminar todos los inquilinos en una implementación de varios inquilinos, no puede eliminar la configuración de Prisma Accessa nivel de administrador donde se añaden o eliminan inquilinos.*
- *Cuando elimina un inquilino, Prisma Access elimina el conjunto de plantillas y grupos de dispositivos para los cuales tiene licencia, pero no elimina el conjunto sin licencia. Por ejemplo, si tiene una licencia de Prisma Access para usuarios y elimina un inquilino, Prisma Access elimina las pilas de plantillas, plantillas y grupos de dispositivos relacionados con el usuario móvil, pero no elimina el conjunto que creó para Prisma Access sin licencia para redes. Puede eliminar manualmente estos conjuntos de plantillas y grupos de dispositivos no utilizados después de eliminar el inquilino.*

STEP 1 | Desde el Panorama que gestiona Prisma Access, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)**.

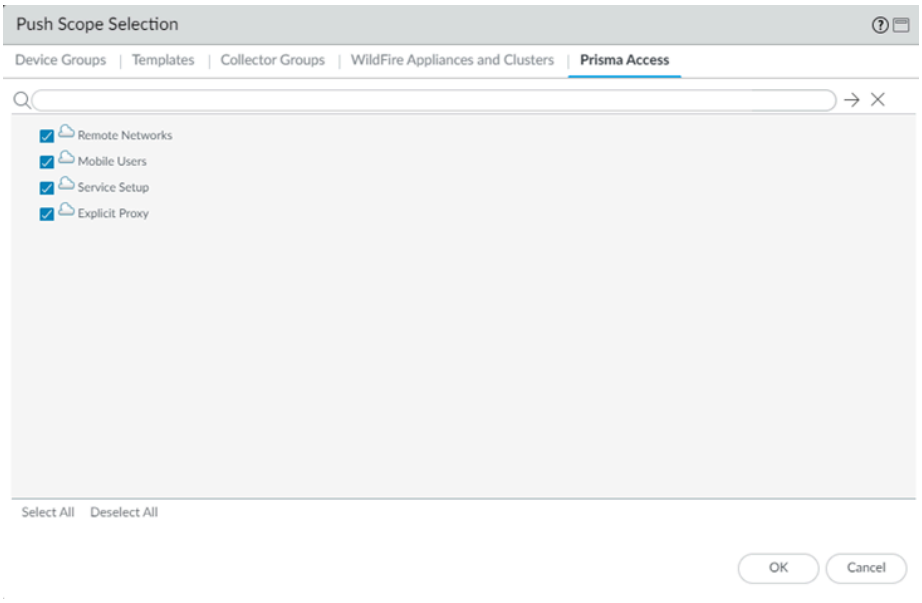
STEP 2 | Seleccione el inquilino y elimine toda la configuración asociada a él.

Realice este paso como práctica recomendada para asegurarse de que se elimine toda la configuración del inquilino, incluida cualquier conexión de servicio, usuario móvil, red remota o configuración de Clean Pipe.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirme y envíe sus cambios a Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**.
2. Debe **Edit Selections (Editar selecciones)** y asegúrese de que todos los componentes que eliminó (incluidos Redes remotas, Usuarios móviles, Configuración de servicio, Proxy explícito y Clean Pipe, según su implementación) estén seleccionados.



3. Haga clic en **Push (Enviar)**.

STEP 4 | Seleccione uno o más inquilinos y luego seleccione **Delete (Eliminar)** para eliminarlos.

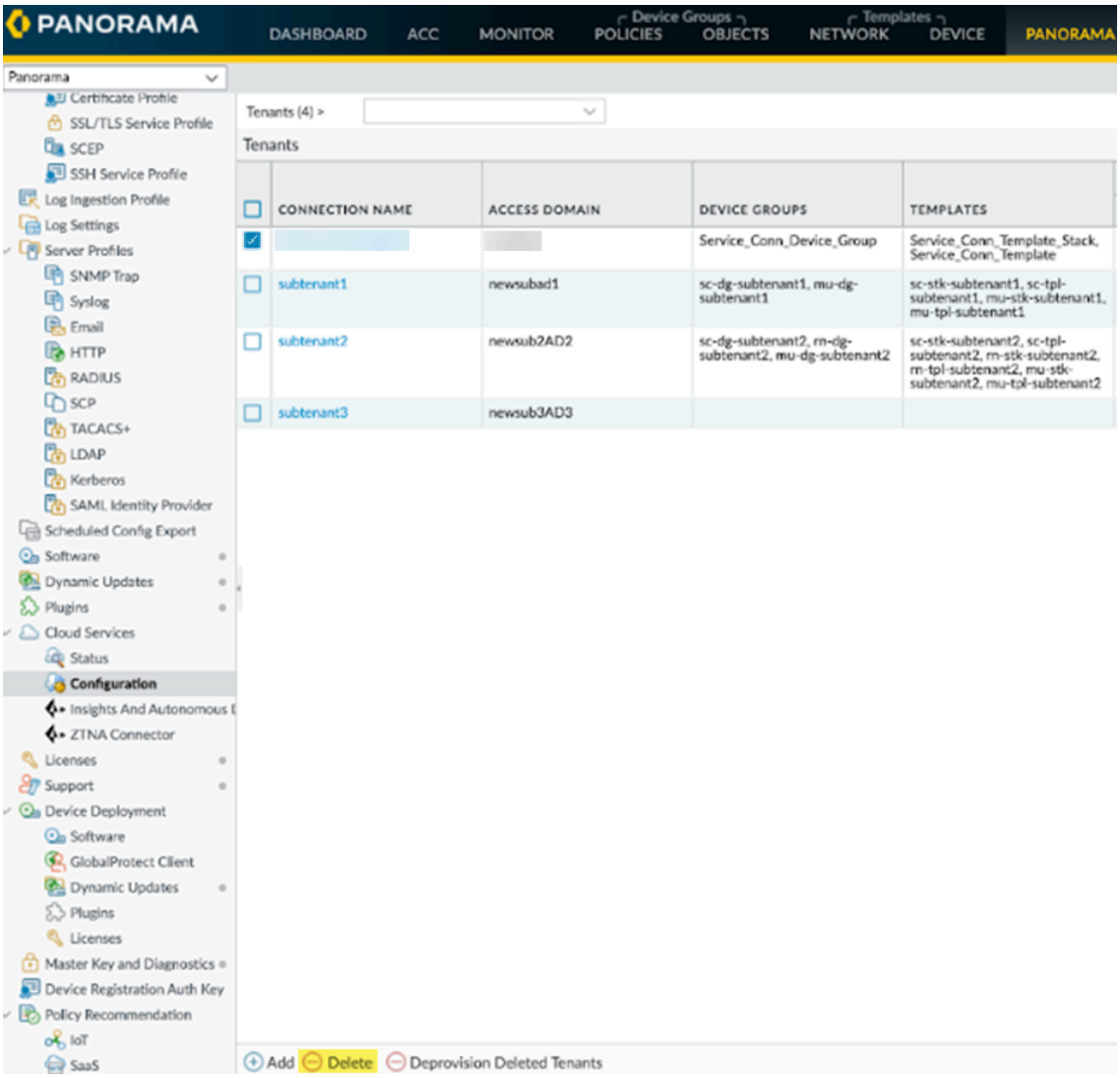
Eliminar un inquilino elimina el inquilino de Panorama, pero no elimina el inquilino de la infraestructura de Prisma Access. Para eliminar un inquilino y quitarlo de la infraestructura,

 ©2025 Palo Alto Networks, Inc.

elimínelo, realice una confirmación local y luego elimine el aprovisionamiento como se muestra en los siguientes pasos.

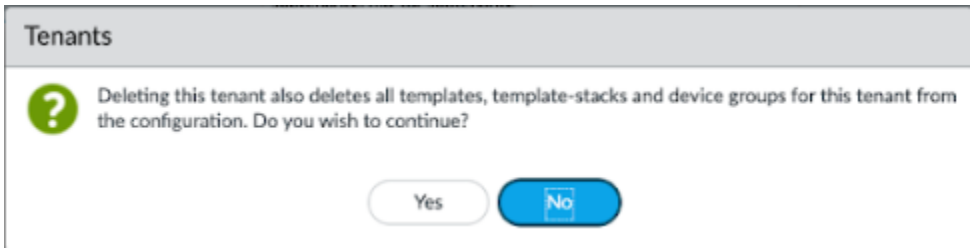
Si elimina el inquilino pero no retira el aprovisionamiento, aún puede recuperarlo poniéndose en contacto con la asistencia de Palo Alto Networks.

Si tiene sus Panorama instalados en una configuración de alta disponibilidad, solo realice las operaciones de eliminación y eliminación de aprovisionamiento desde el Panorama activo en un par de alta disponibilidad.



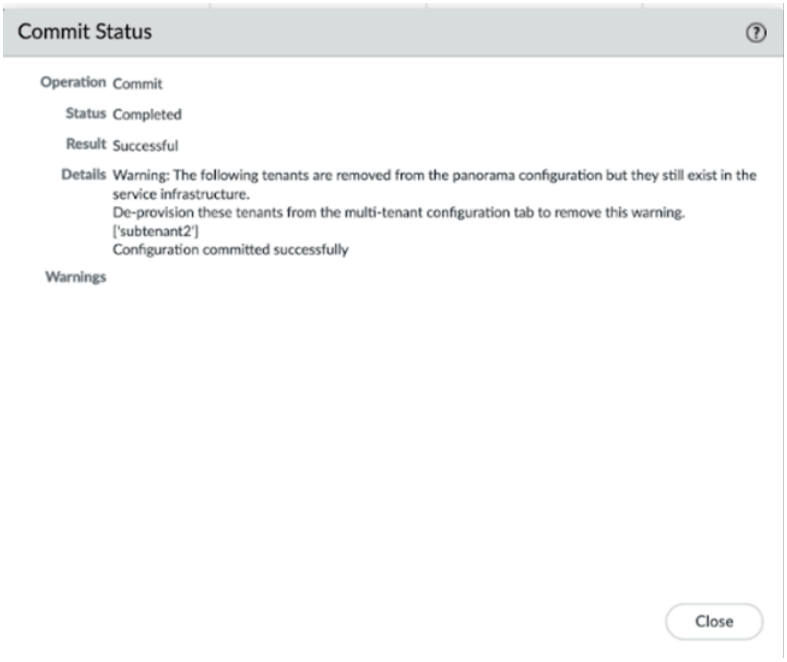
Aparece una ventana emergente que confirma el proceso de eliminación del inquilino. Haga clic en **Yes (Sí)** para continuar o haga clic en **No** para cancelar la eliminación.

 ©2025 Palo Alto Networks, Inc.



STEP 5 | Confirme sus cambios localmente en Panorama seleccionando **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **Commit (Confirmar)** sus cambios.

Después de la confirmación local, los inquilinos se marcan para su eliminación y se eliminan de la lista de inquilinos, pero no se eliminan de la infraestructura de Prisma Access. Aparece una ventana emergente que muestra los inquilinos que se eliminaron.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Para eliminar completamente a los inquilinos de la infraestructura de Prisma Access, deberá **Deprovision Deleted Tenants (Eliminar el aprovisionamiento de inquilinos eliminados)**.

Eliminación del aprovisionamiento de un inquilino:

- Lo elimina de su configuración y la infraestructura de Prisma Access y no se puede recuperarlo.
- Recupera la licencia que le fue asignada al inquilino.



Aparecerá un mensaje de confirmación con los nombres de los inquilinos cuyos aprovisionamientos se han eliminado; haga clic en **OK (Aceptar)** para continuar con el desaprovisionamiento del inquilino o en **Cancel (Cancelar)** para cancelar la operación.

Cuando deja de aprovisionar a un inquilino, elimina por completo al inquilino y todos los recursos que están asignados a él, y recuperas las licencias que estaban asignadas a dichos inquilinos. No es posible recuperar al inquilino.

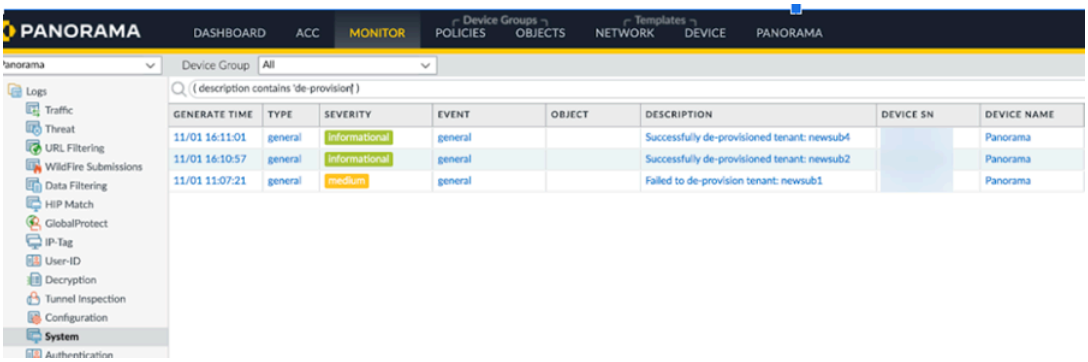


Si no es necesario retirar el aprovisionamiento a ningún inquilino, se mostrará el siguiente mensaje.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | (Opcional) Verifique el estado de la operación de desaprovisionamiento yendo a **Monitor (Supervisar) (Supervisar)** > **Logs** > **System (Sistema)**. La operación de anulación del aprovisionamiento y el nombre del inquilino se muestran en los logs.



 ©2025 Palo Alto Networks, Inc.

Crear un usuario administrativo a nivel de inquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Deberá crear un usuario administrativo para cada inquilino. De esa manera, un administrador de nivel de inquilino puede ver y realizar cambios en la configuración de su inquilino pero no tiene acceso a otros inquilinos. Para crear un usuario administrativo para un inquilino específico, complete la siguiente tarea. Para obtener más información acerca del control de acceso basado en roles (RBAC) para usuarios administrativos de nivel de inquilino, consulte Control de acceso basado en funciones para usuarios administrativos de nivel de inquilino.

*Los usuarios que gestionan inquilinos individuales no pueden ver los logs del sistema porque la opción **Monitor (Supervisar)** > **Logs** > **System (Sistema)** no está disponible. Esta limitación se aplica a todos los administradores que tienen una función administrativa de **Device Group and Template (Grupo de dispositivos y plantilla)**. Solo los superusuarios pueden ver los logs del sistema en modo multitenencia.*

 ©2025 Palo Alto Networks, Inc.

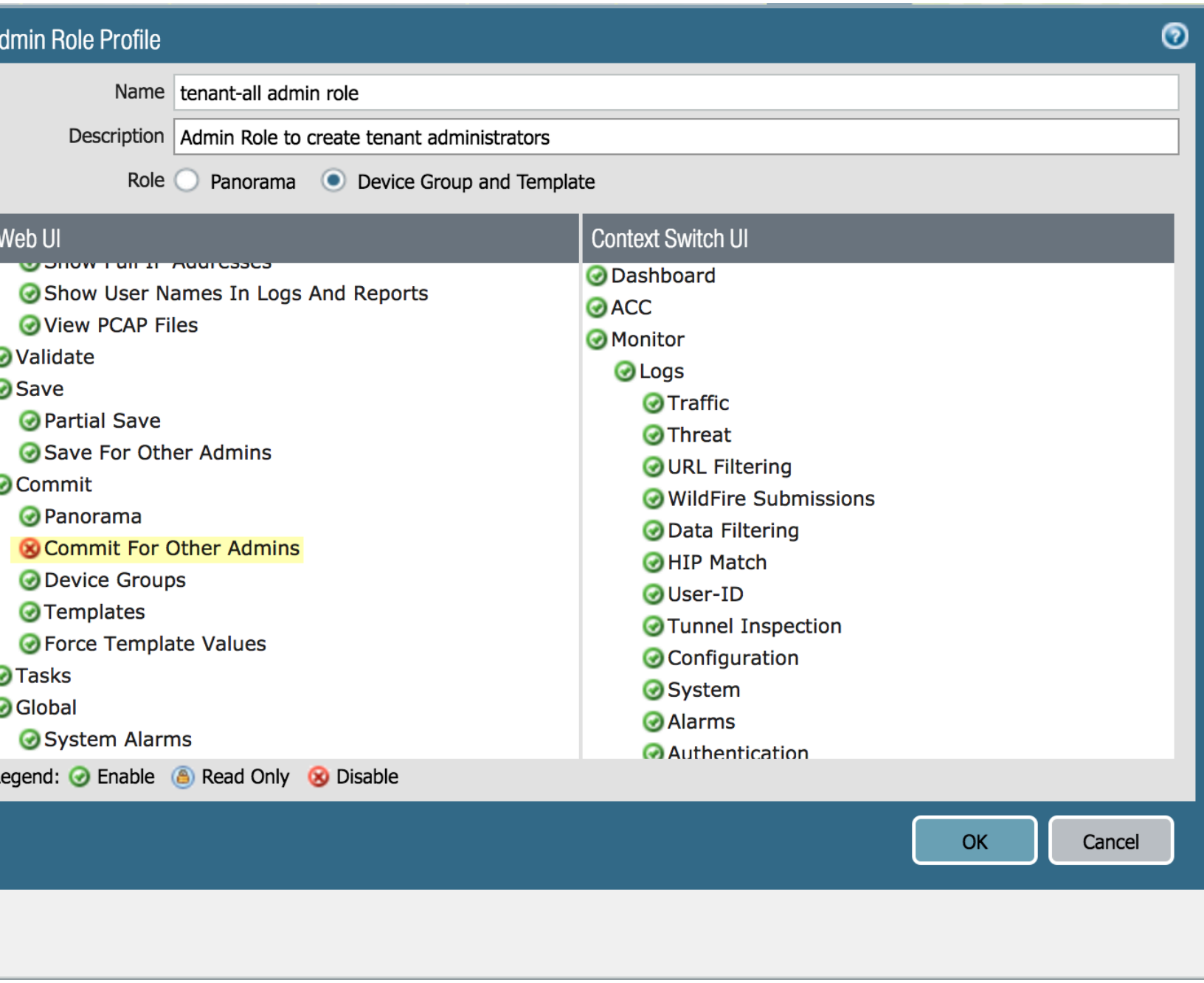
STEP 1 | Crear una función administrativa con un tipo de **Device Group and Template (Grupo de dispositivos y plantilla)**.

1. Seleccione **Panorama** > **Admin Roles (Funciones de gestor)**.
2. Debe **Add (Añadir)** un perfil de función de administrador con una **Role (Función)** de **Device Group and Template (Grupo de dispositivos y plantilla)**.
3. Haga clic en **OK (Aceptar)**.

Puede crear un único perfil de función de administrador y compartirlo entre varios inquilinos; sin embargo, debe crear un administrador independiente para cada inquilino.

*Aunque adapte la función administrativa a las necesidades de su organización, le recomendamos que deseleccione **Commit for Other Admins (Confirmación para otros administradores)**. Anular la selección de esta opción permite a un usuario de nivel de inquilino confirmar solo los cambios que ha realizado, y le impide confirmar involuntariamente otros cambios que otros usuarios administrativos de nivel de inquilino han realizado que aún no se han confirmado.*

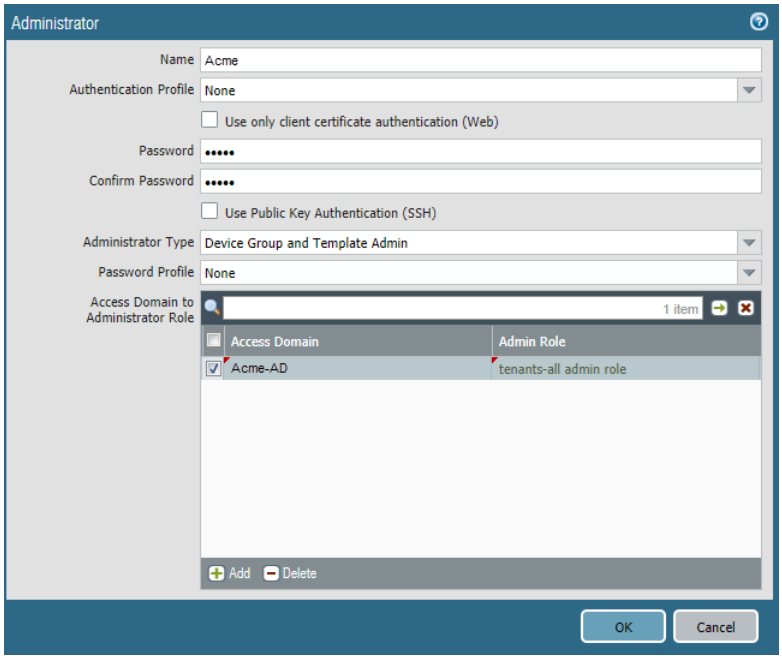
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Crear y configurar un Administrator (Administrador) para el inquilino.

1. Seleccione **Panorama** > **Administrators (Administradores)**.
2. **Add (Añadir)** un administrador.
3. Introduzca y confirme una **Password (Contraseña)** para el nuevo Administrador.
4. Especifique un **Administrator Type (Tipo de administrador)** de **Device Group and Template Admin (Administrador de grupo de dispositivos y plantilla)**.
5. Especifique el **Access Domain (Dominio de acceso)** que está asociado con los grupos de dispositivos para ese inquilino.
6. Especifique la **Admin Role (Función de administrador)** que creó en el Paso 1 para el inquilino.



STEP 3 | Haga clic en **OK (Aceptar)**.

STEP 4 | Repita los pasos 2 y 3 para añadir usuarios adicionales para gestionar sus inquilinos según sea necesario.

STEP 5 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar sus cambios

 ©2025 Palo Alto Networks, Inc.

Control de acceso basado en funciones para usuarios administrativos de nivel de inquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

Si gestiona una implementación de varios inquilinos, puede usar el control de acceso basado en funciones (RBAC) para crear usuarios administrativos de nivel de inquilino.

Para modificar el acceso de nivel RBAC para los usuarios administrativos de nivel de inquilino en Panorama, cree un usuario administrativo de nivel de inquilino, utilice un Perfil de función de administrador con una **Role (Función)** de **Device Group and Template (Grupo de dispositivos y plantilla)** y elija **Enable (Habilitar)**, **Disable (Deshabilitar)** o dé acceso de **Read Only (Solo lectura)** a áreas de la **Web UI (Interfaz de usuario web)** de Panorama. Utilice este método para gestionar el acceso a todos los componentes de Panorama, para los usuarios de nivel de inquilino, con la excepción del acceso al complemento Cloud Services donde gestiona Prisma Access.

Si desea restringir la configuración de los componentes de Prisma Access en Panorama para un usuario de nivel de inquilino, no puede usar Funciones de administrador. Para no permitir que los usuarios configuren tareas de configuración específicas de Prisma Access, debe impedir que el usuario acceda al complemento Cloud Services, que también le impide verlo. Con este método, puede crear un usuario administrativo para un profesional de la seguridad que tenga permisos para realizar cambios en las políticas de seguridad y enviar esos cambios a Panorama, pero no puede ver ni realizar ningún cambio en la configuración de Prisma Access.

Puede habilitar o deshabilitar el acceso al complemento Cloud Services para un usuario, pero no puede darle acceso de solo lectura; si un usuario tiene acceso a ver el complemento Cloud Services, el usuario también puede realizar cambios de configuración en sus componentes, incluido Prisma Access.

La siguiente tabla muestra ejemplos de funciones administrativas a nivel de inquilino y los pasos que realiza para crear esas funciones.

Configuración de muestra de nivel de inquilino	Tarea de configuración
Cree un usuario centrado en las redes que: • Pueda editar configuraciones de complementos • Pueda confirmar a Panorama	Cree un usuario administrativo de nivel de inquilino, habilitando las opciones de **Save (Guardar)** y **Commint (Confirmar)**los permisos en el **Admin Role Profile(Perfil de función de administrador)**, y deshabilitando o haciendo de **Read Only (Solo lectura)**

 ©2025 Palo Alto Networks, Inc.

Configuración de muestra de nivel de inquilino	Tarea de configuración
• Pueda enviar la configuración a Prisma Access	cualquier permiso que no desee que tenga el usuario administrativo de nivel de inquilino.
Crear un usuario centrado en la seguridad que: • Puede ver y realizar cambios en las políticas de seguridad • Puede confirmar con Panorama • No puede ver ni realizar cambios en el complemento Cloud Services • No puede enviar la configuración a Prisma Access (requiere que el superusuario envíe la configuración)	Para evitar que un usuario administrativo de nivel de inquilino vea o acceda al complemento, elimine el acceso al complemento para un administrador de nivel de inquilino. Para todos los demás permisos relacionados con Panorama, cambie los permisos de función de administrador para el usuario.
Crear un usuario híbrido que: • Tiene acceso de solo lectura al complemento Cloud Services • Tiene acceso de lectura-escritura a la política de seguridad • No puede enviar la configuración a Prisma Access (requiere que el superusuario envíe la configuración)	Esta configuración no es posible. No puede hacer que el complemento Cloud Services sea de solo lectura. Solo puede proporcionar acceso a los usuarios de gestión para verlo y usarlo para realizar cambios de configuración o impedir que se vean.

Eliminar el acceso al complemento para un usuario administrativo de nivel de inquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre cómo administrar varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia de Prisma Access

En configuraciones multiinquilino normales, se utilizan dominios de acceso Añadir inquilinos a Prisma Access y asocian cada dominio de acceso con un inquilino. Para evitar que un usuario administrativo de nivel de inquilino vea o realice cambios de configuración en Prisma Access, cree un dominio de acceso, pero no lo asocie a un inquilino.

Debido a que asoció el dominio de acceso a los grupos de dispositivos y las pilas de plantillas para el inquilino, el usuario administrativo de nivel de inquilino tiene acceso RBAC a nivel de

 ©2025 Palo Alto Networks, Inc.

inquilino y puede realizar la configuración solo para ese inquilino. Dado que no asoció el dominio de acceso con un inquilino en Prisma Access, el dominio de acceso no puede ver el complemento de Servicios en la nube, que proporciona acceso a Prisma Access. De esta manera, crea un usuario que puede realizar tareas de configuración a nivel de inquilino sin poder acceder, ver o realizar cambios de configuración en Prisma Access.

Para eliminar Prisma Access para un usuario de nivel administrativo, complete la siguiente tarea.



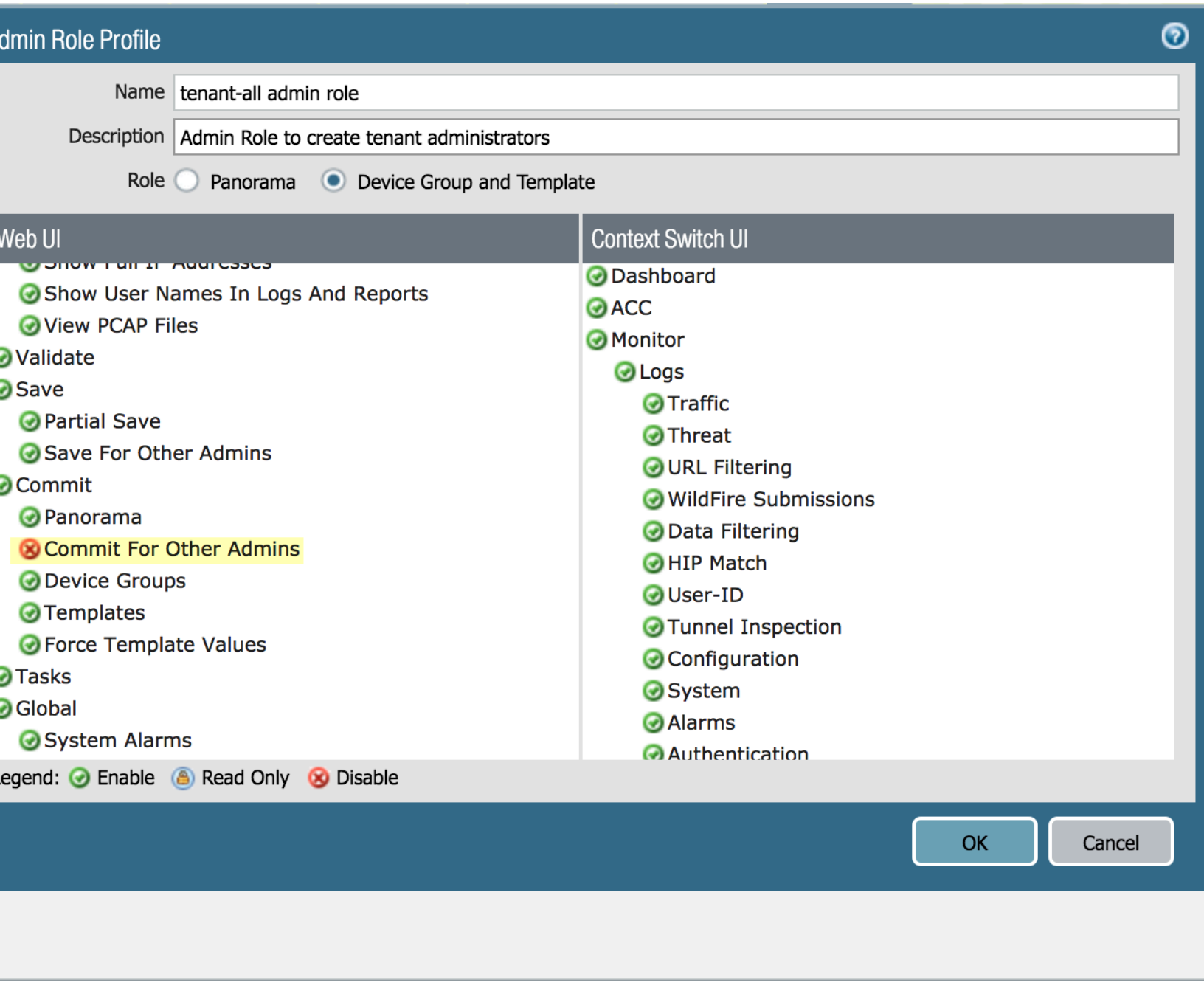
Esta tarea supone que tiene Añadir inquilinos a Prisma Access *plantillas, pilas de plantillas y grupos de dispositivos para el inquilino que usted asociará al usuario administrativo de nivel de inquilino.*

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Crear una función administrativa con un tipo de **Device Group and Template (Grupo de dispositivos y plantilla)**.

1. Seleccione **Panorama** > **Admin Roles (Funciones de gestor)**.
2. Debe **Add (Añadir)** un perfil de función de administrador con una **Role (Función)** de **Device Group and Template (Grupo de dispositivos y plantilla)**.
3. Haga clic en **OK (Aceptar)**.

   Puede crear un único Perfil de función de administrador y compartirlo entre varios inquilinos.

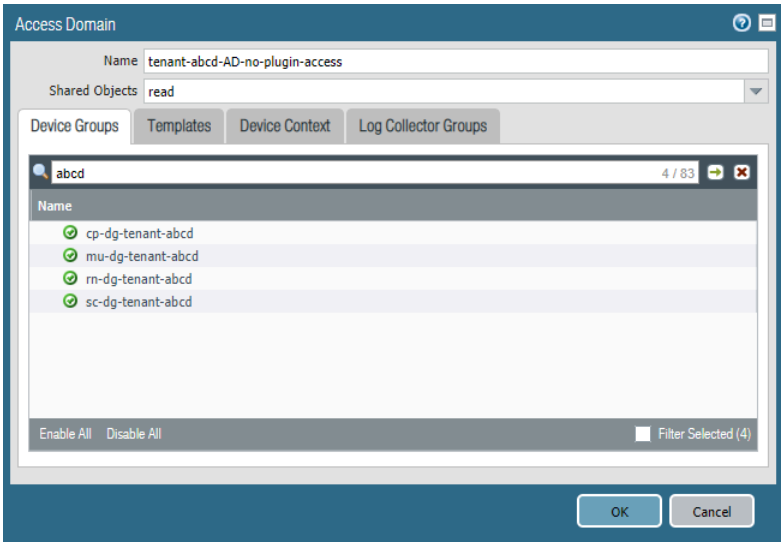


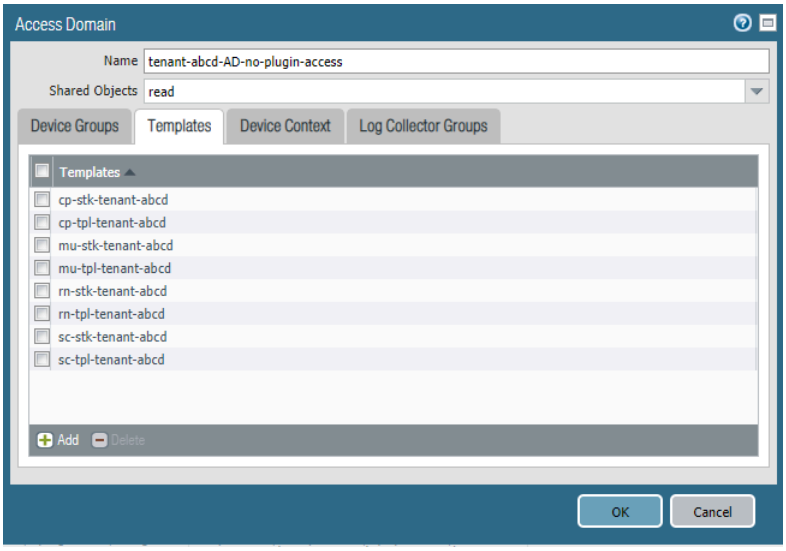
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Panorama** > **Access Domain (Dominio de acceso)** y luego **Add (Añadir)** para añadir un Access Domain (Dominio de acceso).

STEP 3 | Especifique los **Device Groups (Grupos de dispositivos)** y las **Templates (Plantillas)** asociadas con el inquilino.

*Si creó grupos de dispositivos que son secundarios o terciarios de otros grupos de dispositivos bajo el grupo de dispositivos principal **Shared (Compartido)**, seleccione solo el grupo de dispositivos en el nivel jerárquico más bajo (secundario o terciario); no seleccione el principal o tendrá errores al confirmar.*



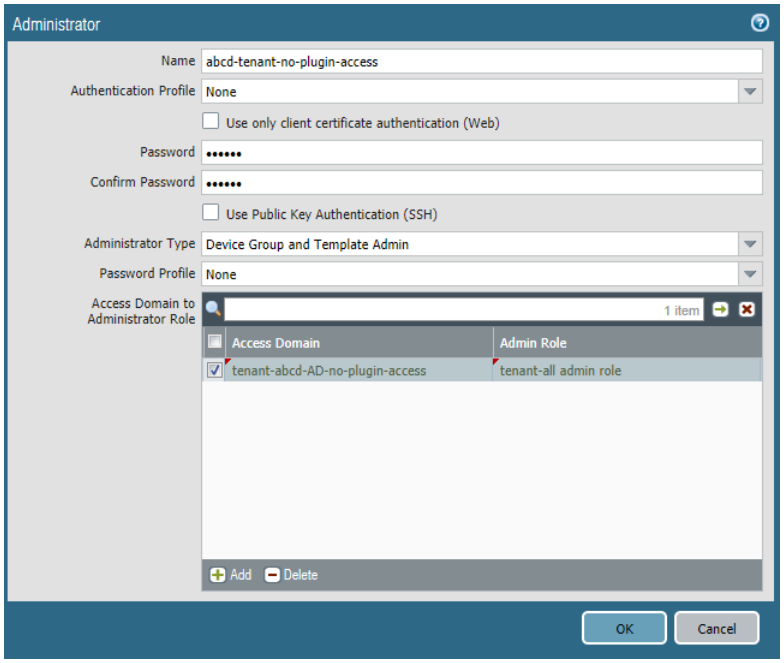


 ©2025 Palo Alto Networks, Inc.

STEP 4 | Cree y configure un Administrador para el usuario administrativo de nivel de inquilino, especificando el dominio de acceso que acaba de crear.

1. Seleccione **Panorama** > **Administrators (Administradores)**.
2. **Add (Añadir)** un administrador.
3. Introduzca y confirme una **Password (Contraseña)** para el nuevo Administrador.
4. Especifique un **Administrator Type (Tipo de administrador)** de **Device Group and Template Admin (Administrador de grupo de dispositivos y plantilla)**.
5. Especifique el **Access Domain (Dominio de acceso)** que está asociado con los grupos de dispositivos para ese inquilino.
6. Especifique la **Admin Role (Función de administrador)** que creó en el Paso 1 para el inquilino.

   Cuando complete este ejemplo, el usuario administrativo **abcd-tenant-no-plugin-access** tendrá permisos según lo que haya definido en el perfil de función de administrador, pero no podrá ver ni configurar el complemento de Cloud Services (incluido Prisma Access). Sin embargo, tenga en cuenta que no podrán enviar a la nube ningún cambio que realicen.



STEP 5 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar sus cambios

 ©2025 Palo Alto Networks, Inc.

Ordenar logs por identificador de grupo de dispositivos en una implementación multiinquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Para obtener información sobre la gestión de varios inquilinos en Prisma Access (Managed by Strata Cloud Manager), consulte Prisma SASE.	❑ Licencia Prisma Access

Para ordenar los logs manualmente por inquilino en Panorama, seleccione **Monitor (Supervisar)** > **Logs** y elija el **Device Group (Grupo de dispositivos)** asociado a ese inquilino para mostrar los logs de ese grupo de dispositivos. Sin embargo, si va a reenviar los logs a un dispositivo externo, es posible que tenga que ordenar esos logs en el nivel de inquilino. Para ello, busque el identificador de grupo de dispositivos en los logs asociados al grupo de dispositivos y use esa asignación de identificador de grupo a grupo de dispositivos para asociar los logs a un inquilino.

Hay cuatro campos asociados con el grupo de dispositivos en los logs: **DG Hierarchy Level 1 (Jerarquía de DG de nivel 1)**, **DG Hierarchy Level 2 (Jerarquía de DG de nivel 2)**, **DG Hierarchy Level 3 (Jerarquía de DG de nivel 3)** y **DG Hierarchy Level 4 (Jerarquía de DG de nivel 4)**. Estos campos muestran los ID de grupo de dispositivos en su jerarquía. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura.

DG Hierarchy Level 1 (Jerarquía DG de nivel 1) hace referencia al primer nivel de grupo de dispositivos de la jerarquía. Si ha agregado grupos de dispositivos secundarios o terciarios, los campos **DG Hierarchy Level 2 (Jerarquía de DG de nivel 2)** a **DG Hierarchy Level 4 (Jerarquía de DG de nivel 4)** muestran la jerarquía desde el grupo secundario hasta el grupo cuaternario, respectivamente.

Para buscar logs por inquilino, complete la siguiente tarea.

STEP 1 | Busque los ID de grupo de dispositivos asociados con el grupo de dispositivos.

- Para encontrar esta información mediante un comando de la CLI, inicie sesión en Panorama como superusuario (usuario de nivel de administrador), introduzca el comando `show readonly` en el modo de configuración y vea los valores en el encabezado **device-group (grupo-dispositivo)**. Los ID de los grupos de dispositivos se muestran debajo del nombre del grupo de dispositivos. En el ejemplo siguiente se muestra que el ID del dispositivo para el grupo de dispositivos **Acme-SC** es **20**.

  Tenga en cuenta que estos grupos de dispositivos se encuentran en el primer nivel de la jerarquía [**DG Hierarchy Level 1 (Jerarquía de DG de nivel 1)**]; esa información se usa en la consulta en el paso siguiente.

```
admin# show readonly ... device-group { acme-sc { id 20; } acme-
rn { id 39; } acme-mu { id 40; } hooli-rn { id 56; } hooli-sc
 { id 57; } hooli-mu {
```

 ©2025 Palo Alto Networks, Inc.

- Para utilizar una consulta de API, introduzca el siguiente comando de API:

```
/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
```

Para obtener más información sobre el uso de las API con logs, consulte Recuperar logs (API).

STEP 2 | Use la asignación de nombre de ID de grupo de dispositivos a grupo de dispositivos para asociar los logs a un inquilino.

STEP 3 | **Add (Añadir)** los parámetros de **Forwarding (Reenvío)** que seleccionan los logs que desea reenviar.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Prisma Access en un entorno de FedRAMP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Complemento Cloud Services, versión 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+

El Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP (en inglés)) es un programa del gobierno de los Estados Unidos que proporciona un enfoque estandarizado para la evaluación de seguridad, la autorización y la supervisión continua de productos y servicios en la nube para usuarios gubernamentales. Palo Alto Networks ha demostrado el cumplimiento de FedRAMP Moderado para Prisma Access (Managed by Panorama). Lea los siguientes temas para obtener más información sobre cómo configurar Prisma Access para garantizar el cumplimiento de FedRAMP Moderado.

Para servicios basados en la nube, como Prisma Access, el gobierno de los Estados Unidos requiere un nivel específico de seguridad, llamado *Moderado*, donde la pérdida de confidencialidad, integridad y disponibilidad resultaría en efectos adversos graves en las operaciones, activos o personas de una agencia. Los efectos adversos graves podrían incluir daños operativos significativos a los activos de la agencia, pérdidas financieras o daños individuales que no son la pérdida de vida o los daños físicos.

Prisma Access cumple con los requisitos FedRAMP Moderado y ha obtenido una Autorización para operar (ATO) del gobierno federal. Para garantizar el cumplimiento de FedRAMP moderado, debe instalar y configurar Prisma Access usando los requisitos y las directrices que se enumeran en los temas siguientes.

Requisitos de Prisma Access FedRAMP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Complemento Cloud Services, versión 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+

FedRAMP es el programa utilizado por el gobierno de los Estados Unidos que proporciona un enfoque estándar para el cumplimiento de las ofertas de servicios en la nube (CSO). Para asegurarse de que su Prisma Access (Managed by Panorama) Access cumple con FedRAMP Moderado, utilice estas directrices y requisitos al instalar, activar, configurar por primera vez y configurar Prisma Access.

Requisitos previos a la instalación y activación del producto

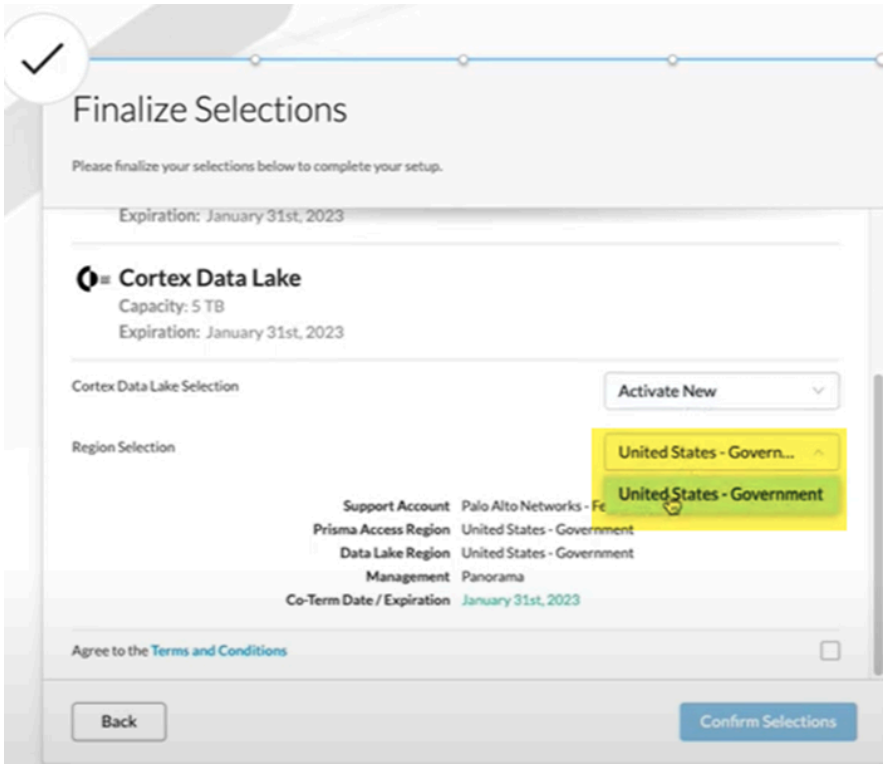
Para asegurarse de que su implementación de Prisma Access sigue cumpliendo con la normativa, asegúrese de seguir estos requisitos de instalación y activación del producto.

- **Requisitos previos a la instalación:**
  - **Tipo de implementación (nueva o existente)**: nuevas implementaciones de Prisma Access se admiten en un entorno FedRAMP moderado. Las actualizaciones de una implementación de Prisma Access en una implementación de Prisma Access FedRAMP Moderado no son compatibles.
  - **SKU requeridos**: cuando compra Prisma Access para una implementación moderada de FedRAMP, Prisma Access requiere SKU que sean específicas del entorno de FedRAMP. Trabaje con su representante o socio autorizado de Palo Alto Networks para asegurarse de que compra las SKU correctas para su implementación de FedRAMP Moderado.
  - Utilice únicamente las versiones de Panorama, las versiones de GlobalProtect y las versiones del complemento Cloud Services enumeradas en Versiones necesarias de Panorama, complemento y plano de datos de PAN-OS.
  - **Lista de permitidos para las direcciones IP públicas de Strata Logging Service**: el bloque de direcciones IP que utiliza la Strata Logging Service región federal es 34.67.50.64/28. Si su empresa utiliza listas de permitidos, asegúrese de añadir estas direcciones IP a las listas de permitidos para asegurarse de que Strata Logging Service puede recibir los registros de Prisma Access.
  - **Cambios en las URL de la API**: cuando usted ejecuta el script de la API para recuperar las direcciones IP públicas que Prisma Access utiliza, cambie la URL de la API de **`https://api.gpcloudservice.com/GetPrismaAccessIP/v2`** a **`https://api.fed.prismaaccess.com/GetPrismaAccessIP/v2`**.

    Si el dispositivo Panorama utiliza un servidor proxy [**Panorama** > **Setup (Configuración)** > **Servicio (Servicio)** > **Proxy Server (Servidor proxy)**] o si utiliza el descifrado de proxy de reenvío SSL con Prisma Access, asegúrese de añadir la URL api.fed.prismaaccess.com a su lista de permitidos en el proxy o servidor proxy.

 ©2025 Palo Alto Networks, Inc.

  - **Cambio de nombre del portal de GlobalProtect**: el nombre de host del portal predeterminado para una implementación de Prisma Access Usuarios móviles de FedRAMP: GlobalProtect es diferente de una implementación que no es de FedRAMP. El nombre del portal es *<portal-name>*.fed.prismaaccess.com. en lugar de *<portal-name>*.gpcloudservice.com.
  - **Requisitos de soporte**: Prisma Access FedRAMP Moderado requiere los Servicios de asistencia al Gobierno de EE. UU. de Palo Alto Networks, que incluyen soporte ininterrumpido para el personal de los Estados Unidos en los Estados Unidos.
- **Requisitos de activación**: cuando active e instale su implementación de Prisma Access, las tareas de activación e instalación son similares a una implementación que no es de FedRAMP. Sin embargo, debe seleccionar una región de **Strata Logging Service** de **United States—Government (Estados Unidos: Gobierno)** durante la activación del producto.



Versiones necesarias de Panorama, complemento y plano de datos de PAN-OS

Para garantizar que Prisma Access cumple con los requisitos moderados de FedRAMP, asegúrese de que la implementación de su Prisma Access (Managed by Panorama) utiliza las siguientes versiones de Panorama, complemento Cloud Services y GlobalProtect.

Componente	Versión requerida
Versión PAN-OS para Panorama	Versión PAN-OS 10.2.8-h3 o una revisión posterior de 10.2.8.

 ©2025 Palo Alto Networks, Inc.

Componente	Versión requerida
	Versión PAN-OS 10.2.9-h1 o una revisión posterior de 10.2.9. La habilitación de la norma de procesamiento y los criterios comunes (FIPS-CC) en el Panorama que gestiona Prisma Access es la práctica recomendada alineada con los controles de FedRAMP. La habilitación de la compatibilidad con FIPS-CC en Panorama requiere acceder a la carpeta Herramienta de recuperación de mantenimiento (MRT). *Para simplificar el proceso de instalación y activación, puede seleccionar un Panorama existente que ya haya configurado en modo FIPS, si ha registrado Panorama, instalado las licencias y activado la licencia de soporte en el Portal de atención al cliente (CSP). Si ha añadido el número de serie de Panorama a la misma cuenta de CSP en la que desea realizar la implementación de Prisma Access, puede seleccionar el número de serie de este dispositivo Panorama durante la instalación.* No puede utilizar un Panorama que se haya utilizado para gestionar otro Prisma Access o implementación de Strata Logging Service.
Versión del complemento Cloud Services	• 3.2.1-h94+ • 4.0.0-h88+ • 4.1.0-h58+ • 5.0.0-h31+
Versión de GlobalProtect	5.1.4+ y 6.0.7+ 5.1.4 está certificada por FIPS y es la versión predeterminada que se debe usar para las implementaciones basadas en el gobierno federal. Si usted cambia la versión predeterminada de GlobalProtect de 5.1.4, no puede seleccionar la versión 5.1.4 en la interfaz de usuario de Panorama y debe abrir un Caso de asistencia con el Soporte Técnico de Palo Alto Networks para volver a añadirlo.

 ©2025 Palo Alto Networks, Inc.

Ubicaciones de Prisma Access FedRAMP compatibles

Las siguientes ubicaciones están autorizadas para su uso con Prisma Access en un entorno FedRAMP de nivel moderado, que incluye compatibilidad con ubicaciones en Estados Unidos continental (CONUS) y fuera de Estados Unidos continental (OCONUS):

- Sureste de Australia
- Bélgica
- Brasil Sur
- Canadá Este
- Finlandia
- Alemania Central
- India Oeste
- Japón Central
- Japón Sur
- Países Bajos Central
- Singapur
- Suiza
- Taiwán
- Reino Unido
- EE. UU. Central
- EE. UU. Este
- EE. UU. Noroeste
- EE. UU. Sureste
- EE. UU. Suroeste

Características compatibles y no compatibles en un Implementación de Prisma Access FedRAMP

La compatibilidad con IPv6 para el acceso a aplicaciones privadas es compatible con un entorno Prisma Access FedRAMP Moderado.

Las siguientes aplicaciones y funciones no son compatibles para su uso en un entorno Prisma Access FedRAMP Moderado:

- Prisma Access Insights
- Autonomous DEM
- Proxy explícito
- Prisma Access para Clean Pipe
- DLP empresarial
- IoT Security (Seguridad de IoT)
- Soporte de SaaS Security Inline: Visibilidad

 ©2025 Palo Alto Networks, Inc.

Configurar Prisma Access en un entorno FedRAMP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Complemento Cloud Services, versión 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+

Una vez que haya completado los requisitos, complete la configuración de la implementación de Prisma Access para un entorno moderado de FedRAMP completando los siguientes pasos.

Antes de comenzar, tome nota de los requisitos y las pautas específicas de una implementación de Prisma Access FedRAMP, incluida la configuración del dispositivo Panorama en modo FIPS-CC y las versiones específicas que se requieren para Panorama, el complemento Cloud Services y GlobalProtect.

STEP 1 | Asegúrese de tener una cuenta de Portal de atención al cliente (CSP) que pueda dedicar exclusivamente a sus implementaciones de FedRAMP.

No es posible tener implementaciones de FedRAMP y no FedRAMP en una única cuenta CSP. Por este motivo, Palo Alto Networks recomienda crear una nueva cuenta CSP que se utilizará únicamente para cuentas FedRAMP.

STEP 2 | Prepare su dispositivo Panorama para usarlo en el entorno FedRAMP de Prisma Access.

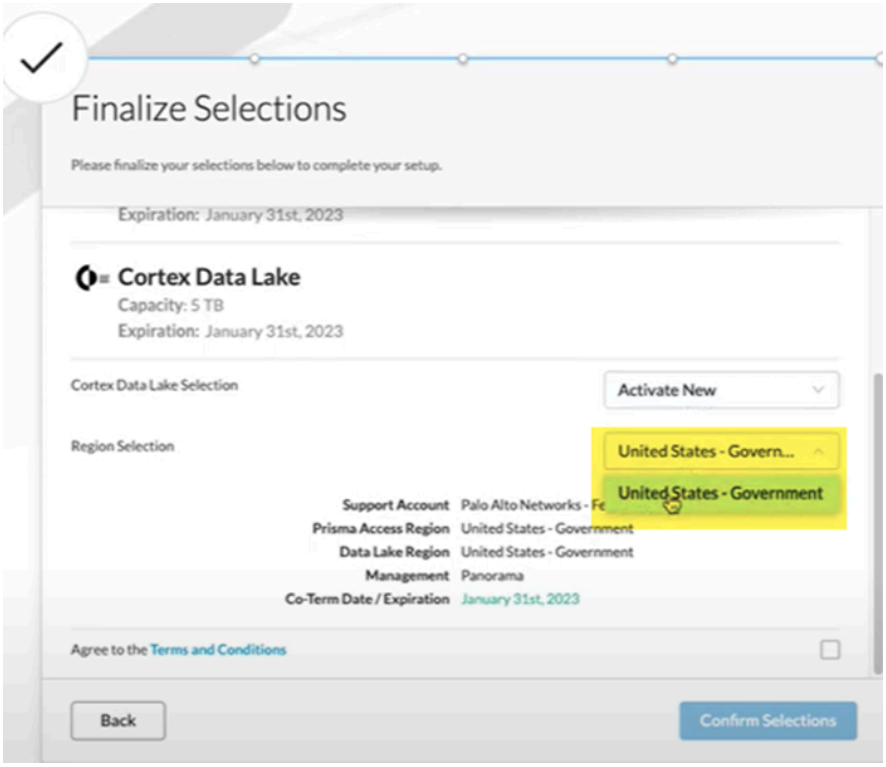
1. Instale el dispositivo Panorama (ya sea un dispositivo M-Series o un dispositivo virtual).
2. (Opcional, recomendado) Habilite la compatibilidad con el Estándar federal de procesamiento de la información y Criterios Comunes (FIPS-CC) en el dispositivo Panorama.

   Para habilitar la compatibilidad con FIPS es necesario acceder a la Herramienta de recuperación de mantenimiento (MRT).
3. Actualice su versión de Panorama a la versión que aparece en Versiones necesarias de Panorama, complemento y plano de datos de PAN-OS.

©2025 Palo Alto Networks, Inc.

STEP 3 | Identifique sus requisitos de su licencia; luego actívela e instale los componentes de la licencia de Prisma Access.

Seleccione una región de **Strata Logging Service** de **United States—Government (Estados Unidos—Gobierno)** durante la activación del producto.



STEP 4 | Añada las siguientes URL, direcciones IP y puertos a una lista de permitidos en cualquier dispositivo de seguridad que use con el dispositivo Panorama que gestiona Prisma Access.

Además, si su dispositivo Panorama utiliza un servidor proxy [**Panorama** > **Setup (Configuración)** > **Service (Servicio)** > **Proxy Server (Servidor proxy)**] o si utiliza un proxy de reenvío SSL con Prisma Access, asegúrese de añadir las siguientes URL, direcciones IP y puertos a una lista de permitidos en el proxy o servidor proxy.

- api.gpcloudservice.com (para Prisma Access)
- api.paloaltonetworks.com (para Prisma Access)
- api.fed.prismaaccess.com (para Prisma Access)
- apitrusted.paloaltonetworks.com (para Prisma Access)
- Los FQDN y puertos necesarios para Strata Logging Service
- 34.67.50.64/28

  El bloque de dirección IP que utiliza la región federal de Strata Logging Service es 34.67.50.64/28. Añada estas direcciones IP a su lista de permitidos para que el Strata Logging Service pueda recibir los logs de Prisma Access.
- Los puertos utilizados por Panorama.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Abra un caso en el Portal de atención al cliente (CSP) para que Palo Alto Networks permita incluir en la lista los puertos de origen y destino de Strata Logging Service.

Para utilizar Strata Logging Service en un entorno de Prisma Access, debe crear un caso para que Palo Alto Networks pueda permitir enumerar los puertos de origen y destino internamente.

STEP 6 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** e introduzca **`wildfire.gov.paloaltonetworks.com`**.

Las implementaciones de FedRAMP requieren que utilice el WildFire EE. UU. Nube gubernamental.

STEP 7 | Incorpore usuarios móviles y protéjalos con GlobalProtect, si es necesario para su implementación.

Recomendamos utilizar la autenticación local como primer paso para verificar que el servicio esté configurado y que sus usuarios tengan acceso a internet. Posteriormente podrá cambiar y utilizar sus métodos de autenticación corporativos.

1. Configurar usuarios móviles de GlobalProtect.
2. Configure zonas para usuarios móviles.
   1. Cree dos zonas en la plantilla de usuario móvil. Por ejemplo, usuarios móviles e Internet.
   2. Asignar las zonas. Asigne cualquier zona que no sea usuarios o sedes o sucursales conectados de Prisma Access a No fiable.

      En **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)**, asigne Internet a No fiable y Usuarios móviles a Fiable.
3. Configure las políticas de seguridad para el grupo de dispositivos.

   Para crear una política de seguridad que permita el tráfico a Internet, seleccione Mobile_User_Device_Group **Policies (Políticas)** > **Security (Seguridad)** > **Prerules (Reglas previas)** > **Add (Añadir)** una regla. Por ejemplo: Usuarios móviles a Internet.
4. Confirme y envíe sus cambios para comenzar a utilizar el servicio.
   1. **Commit (Confirmar)** localmente en Panorama.
   2. **Commit and Push (Confirmar y enviar)** a Prisma Access.
   3. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Mobile Users (Usuarios móviles)** para ver el **Status (Estado)** y verificar que puede hacer ping en el Portal FQDN.
5. Validar que Prisma Access asegure el tráfico de Internet para los usuarios móviles.
   1. Descargar e instalar la aplicación GlobalProtect
   2. Utilice la aplicación para conectarse al portal como usuario móvil (usuario local).
   3. Navegue por algunos sitios web en Internet y verifique los logs de tráfico en Panorama.

STEP 8 | (Solo usuarios móviles: implementaciones de GlobalProtect) Cree un certificado de anulación de autenticación en su implementación de usuarios móviles: Implementación de

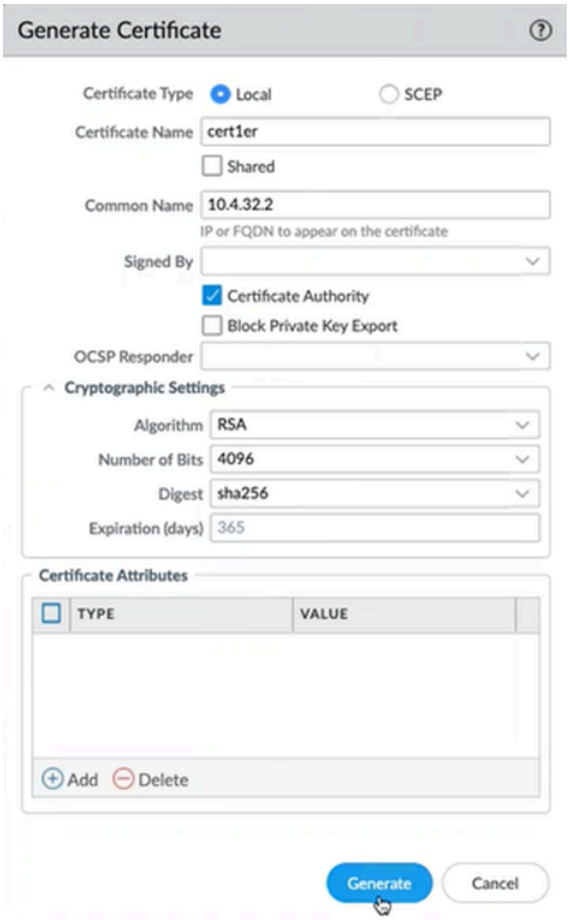
 ©2025 Palo Alto Networks, Inc.

GlobalProtect que cumple con los requisitos para un Panorama que se ejecuta en modo FIPS y aplique ese certificado a su implementación.

Genere un nuevo certificado porque el certificado predeterminado para usuarios móviles—GlobalProtect, **Authentication Cookie CA (CA de cookie de autenticación)**, no cumple con los requisitos mínimos del conjunto de cifrado para un Panorama que se ejecuta en modo FIPS-CC.

1. Desde el Panorama que gestiona Prisma Access, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**.

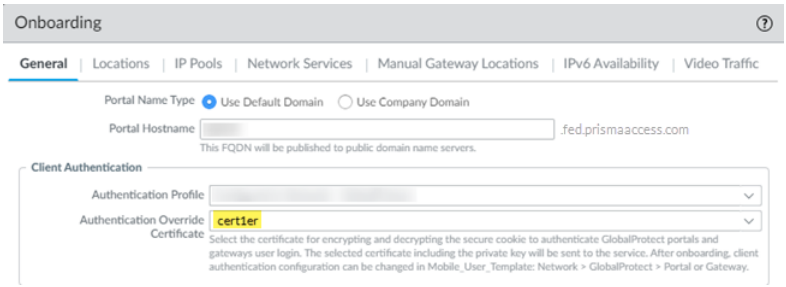
   Asegúrese de que está en **Mobile_User_Template**.
2. Genere un certificado que cumpla con los requisitos mínimos del conjunto de cifrado para un Panorama en modo FIPS-CC.



3. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles—GlobalProtect)**, seleccione el **Hostname (Nombre de host)** y, en el área **Client Authentication**

 ©2025 Palo Alto Networks, Inc.

(Autenticación de cliente) , seleccione el **Authentication Override Certificate (Certificado de anulación de autenticación)** que creó.



Si ya ha creado su configuración de Usuarios móviles—GlobalProtect, esta área aparecerá en gris. Para cambiar el certificado de anulación de autenticación, seleccione ***Network (Red)*** *>* ***GlobalProtect*** *>* ***Portals (Portales)*** *>* ***<portal-config>*** *>* ***Agent (Agente)*** *>* ***DEFAULT (PREDETERMINADO)*** *>* ***Authentication (Autenticación)*** *y seleccione este certificado en* ***Certificate to Encrypt/Decrypt Cookie (Certificado a cifrar/descifrar cookie)****.*

STEP 9 | Habilite la infraestructura de servicio y las conexiones de servicio que permiten la comunicación entre elementos de Prisma Access.

1. Planifique habilitar la infraestructura de servicios y conexiones de servicios.
2. Habilite la infraestructura del servicio.
3. Cree una conexión de servicio para permitir el acceso a sus recursos corporativos.

   Si no necesita acceso a sus recursos corporativos, aún deberá crear una conexión de servicio para permitir el acceso entre usuarios móviles y redes remotas.

STEP 10 | Planificar, crear y configurar conexiones de red remotas.

1. Añada una o más redes remotas a Prisma Access.

   Puede incorporar una ubicación y luego añadir ubicaciones adicionales utilizando la capacidad de importación masiva.
2. Cree una regla de política de seguridad para permitir el tráfico desde las redes remotas a la sede central (por ejemplo: De confianza a confianza).
3. Valide la conectividad entre la conexión de servicio, la conexión de red remota y los usuarios móviles.

STEP 11 | Recuperar las direcciones IP públicas y privadas de Prisma Access.

Agregue estas direcciones a una lista de permitidos en la red de su organización para limitar el acceso entrante a su red empresarial y a sus aplicaciones.

Si tiene una implementación de GlobalProtect para usuarios móviles, puede usar el UI de Prisma Access en lugar de esta API para gestionar la asignación de direcciones IP públicas y confirmar que las direcciones IP se han añadido a sus listas de permitidos antes de que Prisma Access libere las direcciones IP. De este modo, Prisma Access solo aprovisiona las direcciones IP que usted haya permitido en la lista.

 ©2025 Palo Alto Networks, Inc.

STEP 12 | (Opcional) Cambie el método de autenticación de autenticación local al método de autenticación de su organización.

Utilice uno de los siguientes métodos para configurar la autenticación SAML para usuarios móviles:

- Configurar la autenticación SAML de Azure AD para implementaciones de usuarios móviles

  Configure solo las partes GlobalProtect de esta configuración y omita la configuración de Proxy explícito.
- Configurar la autenticación SAML usando Okta como IdP para usuarios móviles
- Configurar ADFS como proveedor SAML para usuarios móviles

Si bien puede usar Cloud Identity Engine para recuperar información de usuarios y grupos mediante Cloud Identity Engine después de configurar la autenticación, no puede autenticar usuarios usando solo Cloud Identity Engine.

STEP 13 | (Opcional) Reenvíe logs desde Strata Logging Service a un receptor Syslog externo configurando la aplicación Log Forwarding.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Implementaciones avanzadas de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Algunas implementaciones de enrutamiento y redes de Prisma Access requieren un conocimiento profundo de la topología y los dispositivos de enrutamiento de su organización, junto con un conocimiento de cómo funciona el enrutamiento de Prisma Access. Lea sobre estas implementaciones avanzadas y cómo configurarlas en esta sección.

Implementaciones avanzadas que se aplican a conexiones de servicio, usuarios móviles y redes remotas:

- Añadir una nueva ubicación de cómputo para una ubicación de Prisma Access implementada
- Compatibilidad con IPv6
- Resolución de DNS para Usuarios móviles: GlobalProtect e implementaciones de redes remotas
- Cómo BGP anuncia los grupos de direcciones IP de usuarios móviles para conexiones de servicio y conexiones de red remotas
- Soporte de proxy para Prisma Access y Strata Logging Service
- Bloquear conexiones entrantes de países específicos
- Tráfico de Internet seguro de AWS WorkSpace
- Prisma Access para redes sin ruta predeterminada

Implementaciones avanzadas de conexión de servicio:

- Redundancia multicloud de conexión de servicio
- Uso de la dirección de tráfico para reenviar el tráfico enlazado a Internet a las conexiones de servicio
- Enrutamiento para el tráfico de conexión de servicio
- Conservar la asignación de User-ID y Device-ID para conexiones de servicio con NAT de origen

Usuarios móviles : Implementaciones avanzadas de GlobalProtect

- Configurar múltiples portales en Prisma Access
- Compatibilidad con el registro de DNS dinámico para la resolución de problemas y actualizaciones remotas
- Compatibilidad con el registro de DNS dinámico para usuarios móviles: GlobalProtect
- Identificación y cuarentena de dispositivos en riesgo en una implementación de Prisma Access GlobalProtect

- Tráfico IPV6 de sinkhole en implementaciones de Usuarios móviles: GlobalProtect
- Redistribuir la información de HIP con Prisma Access
- Ver informes de HIP
- Soporte para codificación Gzip en VPN sin cliente
- Replicación de tráfico en Prisma Access

Implementaciones avanzadas de red remota:

- Proporcionar acceso seguro entrante a ubicaciones de red remotas
- Crear una red de gran ancho de banda para un sitio remoto

 ©2025 Palo Alto Networks, Inc.

Añadir una nueva ubicación de cómputo para una ubicación de Prisma Access implementada

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para optimizar el rendimiento y mejorar la latencia, Prisma Access puede introducir nuevas ubicaciones de cómputo para las ubicaciones que ya has desplegado como parte de una actualización de complemento. Cuando actualiza el complemento, la asignación existente de ubicación a ubicación no cambia, pero puede optar por aprovechar la nueva ubicación de cómputo. Si cambia la ubicación de cómputo, Prisma Access cambia las direcciones IP de la puerta de enlace y del portal (para usuarios móviles) y las direcciones IP de servicio las (para redes remotas) para la ubicación o ubicaciones a las que se asocia la nueva ubicación de cómputo. Si utiliza listas de permitidos en su red para proporcionar a los usuarios acceso a recursos de internet, como aplicaciones SaaS o aplicaciones de socios accesibles públicamente, necesita añadir estas nuevas direcciones IP a sus listas de permitidos.

Para actualizar a una nueva ubicación de cómputo después de que esté disponible, complete la siguiente tarea.

Dado que necesita permitir tiempo para eliminar y añadir la ubicación existente y cambiar sus listas de permitidos (para usuarios móviles) o la dirección IP del túnel IPSec de pares (para implementaciones de red remota), Palo Alto Networks recomienda que programe un cambio de ubicación de cómputo durante una ventana de mantenimiento o durante horas de menor actividad.



Para reducir el tiempo de inactividad en las implementaciones de usuarios móviles, utilice la API para preasignar las nuevas direcciones IP de las puertas de enlace y del portal de usuarios móviles antes de realizar estos pasos.

STEP 1 | Añada ancho de banda para las nuevas ubicaciones de cómputo de red remota.

1. (Implementaciones de red remota que asignan ancho de banda de red remota solo por ubicaciones de cómputo) Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.
2. Haga clic en el icono de engranaje en el área de **Bandwidth Allocation (Asignación de ancho de banda)** y añada **Bandwidth Allocation (Mbps) [Asignación de ancho de banda (Mbps)]** para la nueva ubicación de cómputo.
3. Espere a que el ancho de banda se refleje en el campo Total asignado en la parte superior de la página; luego, haga clic en **OK (Aceptar)**.

STEP 2 | (Implementaciones de usuarios móviles únicamente) Recupere las nuevas direcciones IP de la puerta de enlace y del portal utilizando el script de API y añádalas a sus listas de permitidos.

STEP 3 | Elimina la conexión de servicio, la conexión de red remota o la ubicación del usuario móvil asociada con la nueva ubicación de cómputo.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Confirmar y enviar sus cambios.

STEP 5 | Vuelva a añadir las ubicaciones que acaba de eliminar.

STEP 6 | Confirmar y enviar sus cambios.

STEP 7 | (Implementaciones de red remota y conexión de servicios únicamente) Cambie su CPE para que apunte a las nuevas direcciones IP para el túnel IPSec para la conexión de red remota o la conexión de servicio.

Para conexiones de red remotas, seleccione **Panorama** > **Cloud Services (Servicios en la nube** > **Status (Estado)** > **Network Details (Detalles en la red)** > **Remote Networks (Redes remotas)**, tome una nota de la **Service IP Address (Dirección IP de servicio)**, and configure the new **Service IP Address** como el peer dirección para el túnel IPSec de la red remota en su CPE.

Para las conexiones de servicio, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)**, tome nota de la **Service IP Address (Dirección IP del servicio)**, and configure the new **Service IP Address** como el peer la dirección IP para el túnel IPSec de la conexión de servicio en su CPE.

STEP 8 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube** > **Status (Estado)** > **Network Details (Detalles en la red)** > **Remote Networks (Redes remotas)**, tome una nota de la **Service IP Address (Dirección IP de servicio)**, and configure the new **Service IP Address** como el peer dirección para el túnel IPSec de la red remota en su CPE.

Cuando elimina y vuelve a añadir una conexión de red remota, la dirección IP del túnel IPSec en el lado de Prisma Access cambia.

STEP 9 | (Implementaciones de usuarios móviles únicamente) Después de que se vuelva a asignar una ubicación, recupere el nuevo FQDN de puerta de enlace y añádalo a la configuración de autenticación de su proveedor SAML.

Si la ubicación de un usuario móvil se reasigna, el FQDN de la puerta de enlace podría cambiar después de la actualización de la infraestructura que causa la reasignación, lo que podría causar problemas con la autenticación SAML. Para encontrar el nombre de la puerta de enlace:

- En Prisma Access (Managed by Strata Cloud Manager), seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect Setup (Configuración de GlobalProtect)** > **Infrastructure (Infraestructura)** > **Infrastructure Settings (Configuración de infraestructura)**, haga clic en el engranaje para ver la Configuración de Infraestructura y copie la puerta de enlace renombrada en el área de los FQDN de la puerta de enlace.
- En Prisma Access (Managed by Panorama), seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)** y copie la puerta de enlace renombrada en el área de puertas de enlace

 ©2025 Palo Alto Networks, Inc.

Compatibilidad con IPv6

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access versión de licencia 2.2 Preferred y posteriores ❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 solo para nuevas implementaciones. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

Si su organización utiliza el direccionamiento IPv6, Prisma Access le permite acceder a aplicaciones internas (privadas) que están detrás de direcciones IPv6. Dependiendo de su versión de Prisma Access, puede acceder a aplicaciones privadas (internas) mediante IPv6 o a aplicaciones internas y públicas (externas) tanto para GlobalProtect como para redes remotas.

Para acceder a aplicaciones externas, algunos componentes de Prisma Access no tienen habilitada la funcionalidad IPv6 de forma predeterminada. Antes de habilitar IPv6 nativo para el acceso a aplicaciones públicas, póngase en contacto con su equipo de cuentas de Palo Alto Networks y abra un ticket de incidencia del TAC para comenzar el proceso de habilitación

Una de las ventajas de la compatibilidad nativa con IPv6 es la capacidad de los usuarios móviles solo en IPv6 y en los endpoints de doble pila para conectarse a Prisma Access a través de conexiones IPv6 utilizando GlobalProtect. Otra ventaja es la capacidad de GlobalProtect y Remote Networks de acceder a Internet y a las aplicaciones SaaS públicas a través de Internet cuando esos destinos de Internet requieren conexiones IPv6.

IPv6 ofrece un espacio para direcciones significativamente mayor que IPv4, lo que permite un número casi ilimitado de direcciones IP únicas. Al mismo tiempo, la pila dual es un enfoque de transición que permite que las redes y los dispositivos funcionen utilizando IPv4 e IPv6 simultáneamente. La compatibilidad nativa con IPv6 hace que Prisma Access sea compatible con conexiones IPv6 y de doble pila para facilitar el proceso de migración de IPv4 a IPv6, garantizar la compatibilidad con versiones anteriores y potenciar su viaje hacia la nube y a las redes habilitadas para IPv6.

Configura IPv6 en la siguiente red de componentes de Prisma Access:

 ©2025 Palo Alto Networks, Inc.

- Habilite IPv6 y especifique una subred IPv6 en su Subred de infraestructura para establecer una infraestructura de red IPv6 que permita la comunicación entre las redes remotas (sucursales), los usuarios móviles y las conexiones de servicio (centros de datos o ubicaciones de oficinas centrales).

  Para obtener los mejores resultados, proporcione su propio grupo de direcciones IPv6 (público o privado) con una longitud de prefijo de /64, como 3005:10:209:55::/64.

- Para una implementación de Usuarios móviles: GlobalProtect, especifique si se deben utilizar o no redes IPv6 para las Ubicaciones de cómputo que están asociados con las ubicaciones de usuario móvil.

  Puede especificar los grupos de direcciones IP de usuarios móviles IPv6 y direcciones de servidor DNS IPv6 según sea necesario.

  Para obtener los mejores resultados, proporcione su propio grupo de direcciones IPv6 (públicas o privadas) con una longitud de prefijo de /64, como 3001:192:168:32::/64, aplicado a nivel mundial.

  Prisma Access Asigna a cada región de cómputo un grupo de una subred /80 y a cada ubicación (puerta de enlace) un grupo de una subred /112. Debido a que cada conexión GlobalProtect utiliza una dirección IP del grupo, esta asignación permite asignar más de 65.000 direcciones IPv6 disponibles (/128) a los endpoints de los usuarios por ubicación.

- Para las conexiones de servicio y las conexiones de red remotas, puede especificar el direccionamiento IPv6 para el tipo de enrutamiento que utiliza la conexión (rutas estáticas o BGP).
  - En el caso de las rutas estáticas, especifique una dirección IPv6 para las subredes utilizadas para las rutas estáticas.
  - Para las rutas BGP, especifique una **Peer Address (Dirección de peer)** y **Local Address (Dirección local)** IPv6.

    También puede especificar el método de transporte utilizado para intercambiar información de emparejamiento BGP. Puede especificar el uso de IPv4 para intercambiar toda la información de emparejamiento de BGP (incluidos IPv4 e IPv6), usar IPv6 para intercambiar toda la información de emparejamiento de BGP o usar IPv4 para intercambiar información de emparejamiento de BGP IPv4 e IPv6 para intercambiar información de emparejamiento de BGP IPv6.

    Para obtener los mejores resultados, proporcione su propio grupo de direcciones IPv6 (público o privado) con una longitud máxima de prefijo de /64, como 2005:10:209:79::/64.

 ©2025 Palo Alto Networks, Inc.

- En el caso de las redes remotas, puede añadir direcciones IPv6 para los servidores DNS.

  Para obtener los mejores resultados, proporcione su propio grupo de direcciones IPv6 (público o privado) con una longitud de prefijo máxima de /64, como 2001:10:209:65::/64.

  Cada sucursal debe usar una subred /112 única (longitud máxima), lo que permite más de 65.000 hosts únicos.

- *Las direcciones IPv6 que proporcione no deben superponerse con el espacio de direcciones IPv6 públicas BYOIP de Prisma Access.*
- *El grupo de direcciones IP, las subredes de sucursales (red remota), las subredes corporativas (conexión de servicio) y la subred de infraestructura no deben superponerse entre sí (deben ser mutuamente excluyentes).*

Las siguientes ubicaciones de cómputo no son compatibles con IPv6:

- Corea del Sur
- Asia Noreste
- Sudamérica Este
- Baréin
- Sudáfrica Oeste
- Europa Norte (Estocolmo)
- Oriente Medio Central (EAU)

Las siguiente ubicaciones no son compatibles con IPv6:

- Todas las ubicaciones de Zona local
- Canadá Oeste
- Sudáfrica Central

Las siguientes implementaciones no admiten el direccionamiento IPv6:

- Redes remotas—Alto rendimiento
- Optimización de IP

  Las implementaciones de optimización de IP no admiten IPv6 para el acceso a aplicaciones públicas (externas); el acceso a aplicaciones privadas es compatible. Para habilitar IPv6 para su nueva implementación de Prisma Access, póngase en contacto con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de TAC para encargarse de la solicitud.
- Implementaciones de Clean Pipe
- Dirección de tráfico (uso de reglas de dirección de tráfico para redirigir el tráfico vinculado a Internet mediante una conexión de servicio)
- Rutas de salida para el servicio para conexiones de servicio y conexiones de red remotas

  Prisma Access no anuncia rutas predeterminadas IPv6.

 ©2025 Palo Alto Networks, Inc.

Descripción general de la compatibilidad nativa con IPv6

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access versión de licencia 2.2 Preferred y posteriores ❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 solo para nuevas implementaciones. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

Prisma Access amplía el soporte para IPv6 más allá del acceso a aplicaciones privadas para soportar IPv6 para GlobalProtect así como también redes remotas de forma nativa.

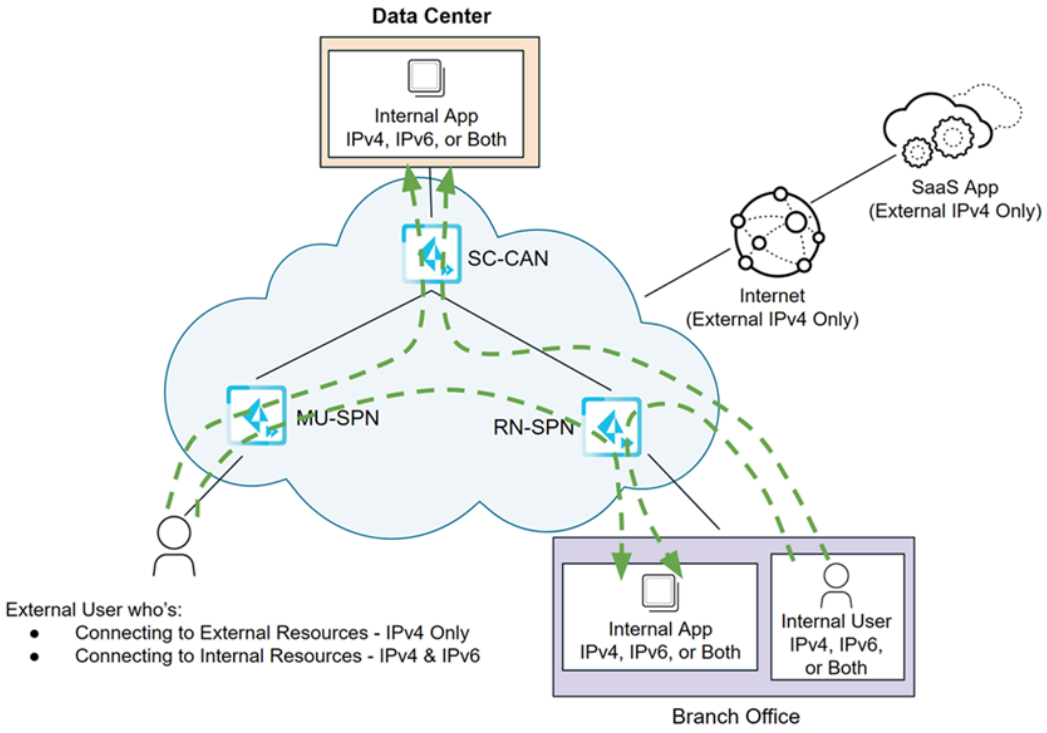
Una de las ventajas de la compatibilidad nativa con IPv6 es la capacidad de los usuarios móviles solo en IPv6 y en los endpoints de doble pila para conectarse a Prisma Access a través de conexiones IPv6 utilizando GlobalProtect. Otra ventaja es la capacidad de GlobalProtect y Remote Networks de acceder a Internet y a las aplicaciones SaaS públicas a través de Internet cuando esos destinos de Internet requieren conexiones IPv6.

IPv6 ofrece un espacio para direcciones significativamente mayor que IPv4, lo que permite un número casi ilimitado de direcciones IP únicas. Al mismo tiempo, la pila dual es un enfoque de transición que permite que las redes y los dispositivos funcionen utilizando IPv4 e IPv6 simultáneamente. La compatibilidad nativa con IPv6 hace que Prisma Access sea compatible con conexiones IPv6 y de doble pila para facilitar el proceso de migración de IPv4 a IPv6, garantizar la compatibilidad con versiones anteriores y potenciar su viaje hacia la nube y a las redes habilitadas para IPv6.

Soporte de aplicaciones privadas

Algunas implementaciones de Prisma Access admiten conexiones IPv6 a aplicaciones "privadas" internas. Prisma Access se conecta a centros de datos (conexiones de servicio) y sucursales (redes remotas) mediante una subyacente en el que el tráfico IPv6 pasa a través de un túnel IPv4.

 ©2025 Palo Alto Networks, Inc.



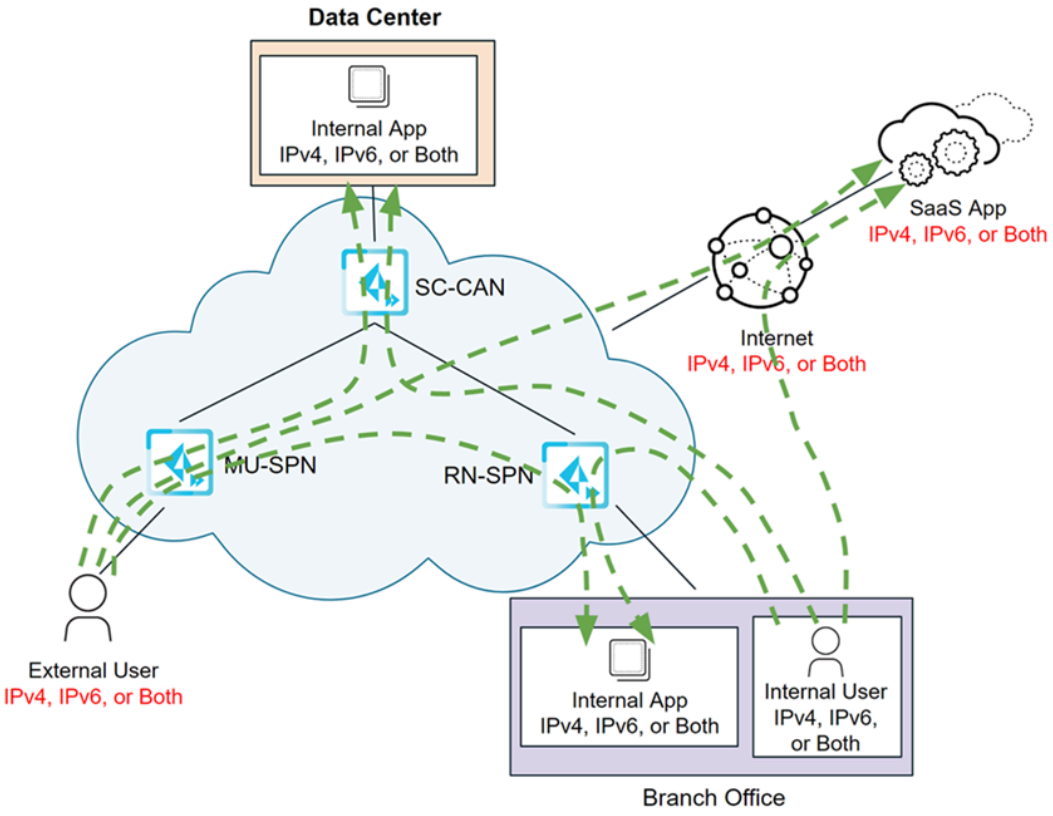
IPv6 nativa en Prisma Access

Prisma Access

- Conexiones entrantes IPv4/IPv6 de doble pila a Prisma Access
- Conexiones de salida de doble pila IPv4/IPv6 a Internet y aplicaciones SaaS a través de Internet

Ahora, los usuarios pueden conectarse a Internet y a aplicaciones SaaS “públicas” a través de Internet utilizando IPv6.

 ©2025 Palo Alto Networks, Inc.



Los usuarios externos (usuarios móviles) deben tener una de las siguientes versiones compatibles de GlobalProtect para que funcione el IPv6 nativo:

- *5.2.13-c418 (Windows/Mac)*
- *6.0.7-c378 (Windows/Mac)*
- *6.0.7-c20 (Linux)*
- *6.1.2 (Windows/Mac/Linux)*
- *6.2.0-c89 (Windows/Mac)*

La siguiente tabla muestra la conectividad compatible con implementaciones IPv4 e IPv6 de Prisma Access. Una marca de verificación indica que esta conectividad es compatible y un guion indica que no lo es.

 ©2025 Palo Alto Networks, Inc.

IPv6 Not Enabled

Mobile User IP Version	GlobalProtect IP Version	Internet Destination Gateway ➞ Internet		Private App Access Service Connection ➞ Internet		GlobalProtect Tunnel	NAT Gateway ➞ Internet
		IPv4	IPv6	IPv4	IPv6	ESP	IPv4 ➞ IPv4
IPv4	IPv4	✓	—	✓	—	IPv4	NAT44
Dual Stack	Dual Stack	✓	✓ Sinkhole	✓	✓	IPv4	NAT44
IPv6	—	—	—	—	—	—	—

IPv6 Enabled

Mobile User IP Version	GlobalProtect IP Version	Internet Destination Gateway ➞ Internet		Private App Access Service Connection ➞ Internet		GlobalProtect Tunnel	NAT Gateway ➞ Internet	
		IPv4	IPv6	IPv4	IPv6	ESP	IPv6 ➞ IPv4	IPv6 ➞ IPv6
IPv4	IPv4	✓	—	✓	—	IPv4	NAT64	NPTv6
Dual Stack	Dual Stack	✓	✓	✓	✓	IPv6	NAT64	NPTv6
IPv6	Dual Stack	✓ (DNS64 & NAT64 Req'd)	✓	✓ (Custom DNS64 + NAT64)	✓	IPv6	NAT64	NPTv6

Siga estos flujos de trabajo para habilitar IPv6 en su configuración.

- ❑ Habilite y configure redes IPv6 y grupos de IP en su infraestructura de Prisma Access
- ❑ Habilite la red IPv6 para la implementación de Usuarios móviles: GlobalProtect
- ❑ Habilitar redes IPv6 para conexiones de servicio
- ❑ Habilitar redes IPv6 para Redes remotas

Habilitar y configurar la red IPv6 y los grupos de direcciones IP en su infraestructura de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access versión 2.2 Preferred y posteriores

 ©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
	❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 para nuevas implementaciones únicamente. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

Para cualquier implementación de Prisma Access, necesita habilitar IPv6 globalmente y especificar una subred IPv6 en su Subred de infraestructura para que Prisma Access pueda establecer una infraestructura de red IPv6 entre sus ubicaciones de red remotas, usuarios móviles y conexiones de servicio. Para hacerlo, complete los siguientes pasos.

- Strata Cloud Manager
- Panorama

Habilitar y configure redes IPv6 y grupos de direcciones IP en su infraestructura de Prisma Access (Strata Cloud Manager)

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** y seleccione el icono de engranaje para editar la configuración.

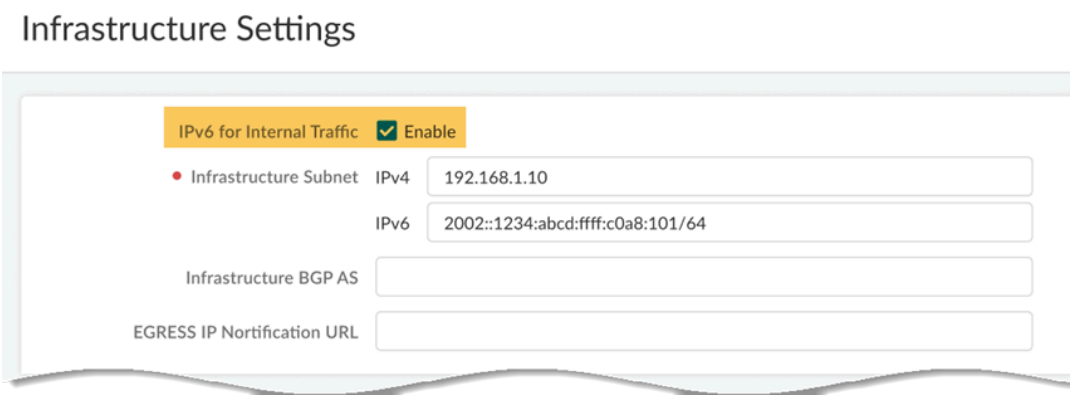
STEP 2 | Active la casilla de verificación para **Enable (Habilitar)** IPv6 para tráfico interno.

Activar o desactivar IPv6 resulta en una breve interrupción del tráfico (hasta 120 segundos) mientras el plano de datos se prepara para aceptar o rechazar rutas IPv6 en la red troncal de

 ©2025 Palo Alto Networks, Inc.

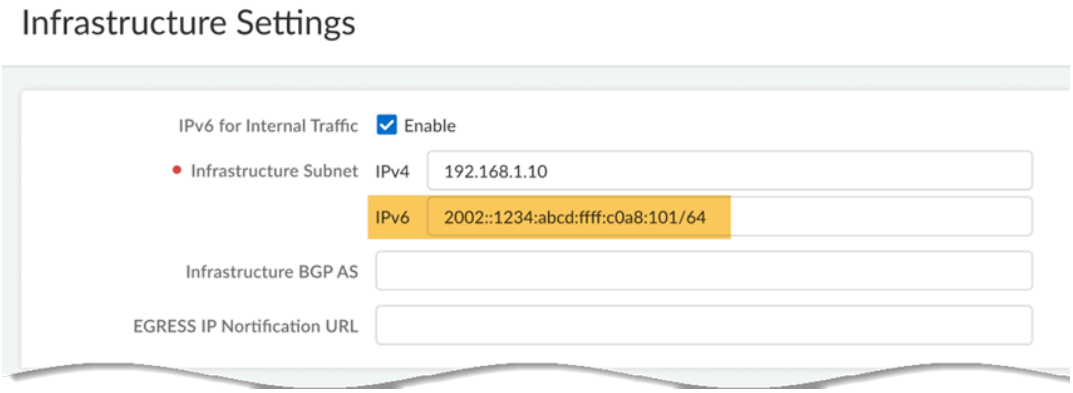
Prisma Access. Recomendamos que envíe este cambio de configuración durante una ventana de mantenimiento o durante las horas de menor actividad.

Si necesita eliminar IPv6, elimine toda la configuración (incluso para usuarios móviles, redes remotas y conexiones de servicio, según corresponda) antes de quitar la marca de la casilla de verificación de la opción ***Enable (Habilitar)*** *IPv6 para tráfico interno.*



STEP 3 | Especifique una subred de infraestructura **IPv6** y una **Infrastructure BGP AS (Infraestructura BGP AS)**.

- Especifique una subred mínima de /96.
- También debe introducir una subred IPv4; Prisma Access requiere subredes IPv4 e IPv6 en su infraestructura de red para usar IPv6. Consulte Prisma Access Gestión de infraestructuras para obtener más detalles.
- Palo Alto Networks recomienda que utilice direcciones IPv4 e IPv6 privadas (no públicas).
- No utilice direcciones locales de enlace IPv6 (fe80::/10).



STEP 4 | Introduzca la **Infrastructure BGP AS (Infraestructura BGP AS)** que desea utilizar dentro de la infraestructura Prisma Access.

Si desea utilizar el enrutamiento dinámico para permitir que Prisma Access descubra dinámicamente rutas a recursos en sus redes remotas y ubicaciones de centros de datos/sede, especifique el número de sistema autónomo (AS). Si no proporciona un número AS, se utilizará el número AS predeterminado 65534.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Si aún no lo ha hecho, considere añadir Servidores DNS Internos para permitir que Prisma Access resuelva sus dominios internos para acceder a servicios, como LDAP y servidores DNS, en su red corporativa.

Consulte Prisma Access Gestión de infraestructuras para obtener más detalles.

STEP 6 | (Solo implementaciones de usuarios móviles) Añada grupos de direcciones IP IPv6 para sus implementaciones de Usuarios móviles: GlobalProtect.

Una implementación de Usuarios móviles: GlobalProtect requiere grupos de direcciones IP. Se requieren grupos de direcciones IP tanto IPv4 como IPv6 para habilitar la funcionalidad IPv6. Aplica direcciones IPv4 a nivel regional o mundial; aplica direcciones IPv6 a nivel mundial. Especifique una subred mínima de /80.

Prisma Access subdivide las direcciones IPv6 mundiales utilizando el siguiente método:

- Prisma Access asigna a cada ubicación (puerta de enlace) un grupo de una subred /112. Debido a que cada conexión GlobalProtect utiliza una dirección IP del grupo, esta asignación permite asignar más de 65.000 direcciones IPv6 disponibles a los endpoints de los usuarios por ubicación.

  Si experimenta un evento de escalado automático (si un gran número de usuarios inicia sesión en una sola ubicación de Prisma Access), Prisma Access puede añadir otra ubicación con otra subred /112.
- Cuando habilita una ubicación para usar IPv6, Prisma Access asigna un grupo de direcciones IPv6 a la región a la que pertenece la ubicación y divide el grupo entre el número total de regiones que tienen habilitada IPv6.

No utilice direcciones de enlace local (fe80::/10) en un grupo de direcciones IP.

1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** y seleccione el icono de engranaje para editar la configuración de infraestructura.
2. En la sección Grupos de IP de clientes, seleccione una **Region (Región)** o **Add IP Portal (Añadir portal IP)**.
3. Entre en un **IPv6 Address Pool (Grupo de direcciones IPv6)**.
   - Debe introducir direcciones IP IPv4 e IPv6 para usuarios móviles. Prisma Access requiere que las direcciones IPv4 e IPv6 sean compatibles con su infraestructura interna cuando se utiliza IPv6.
   - Introduzca una subred IPv6 mínima de /80.
   - Prisma Access subdivide cada subred por región.



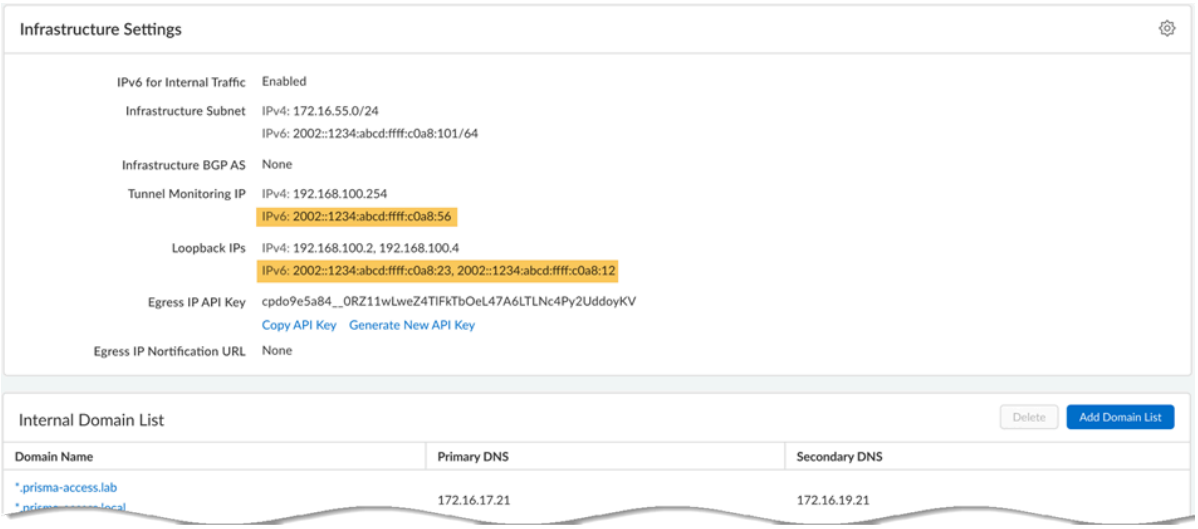
 ©2025 Palo Alto Networks, Inc.

STEP 7 | **Save (Guardar)** y **Push Config (Enviar configuración)**.

STEP 8 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** y tome nota de las siguientes direcciones IPv6 en la configuración de infraestructura:

- **Captive Portal Redirect IP Addresses (Direcciones IP de redireccionamiento del portal cautivo)**: se utiliza con la asignación de direcciones de User-ID basada en el Portal de autenticación
- **Dirección IP del** monitor de túnel: se utiliza para la supervisión de túneles

Debido a que los usuarios móviles de GlobalProtect requieren una dirección IPv4 para los túneles VPN, direcciones de bucle invertido, cuyas direcciones IP se toman de la subred de infraestructura, siguen utilizando direcciones IPv4.



Habilitar y configure redes IPv6 y grupos de direcciones IP en su infraestructura de Prisma Access (Panorama)

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y haga clic en el icono de engranaje para editar la Configuración.

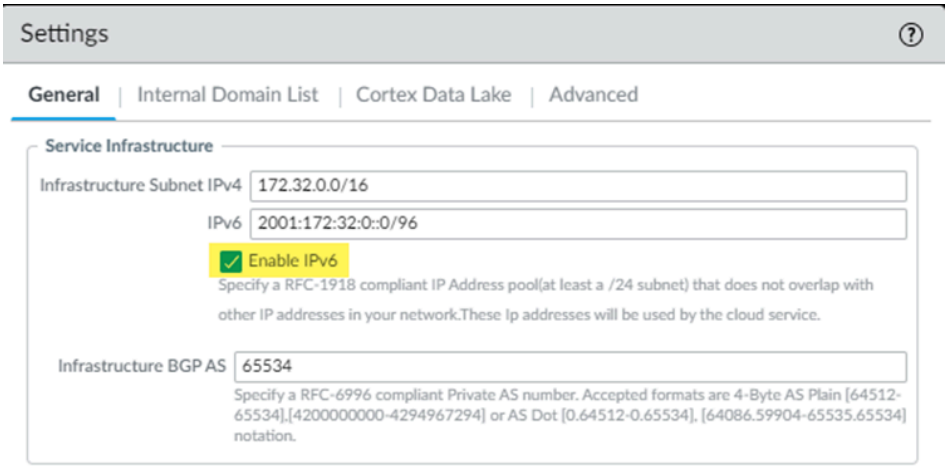
STEP 2 | En la pestaña **General**, seleccione **Enable IPv6 (Habilitar IPv6)**.

Activar o desactivar IPv6 resulta en una breve interrupción del tráfico (hasta 120 segundos) mientras el plano de datos se prepara para aceptar o rechazar rutas IPv6 en la red troncal de

 ©2025 Palo Alto Networks, Inc.

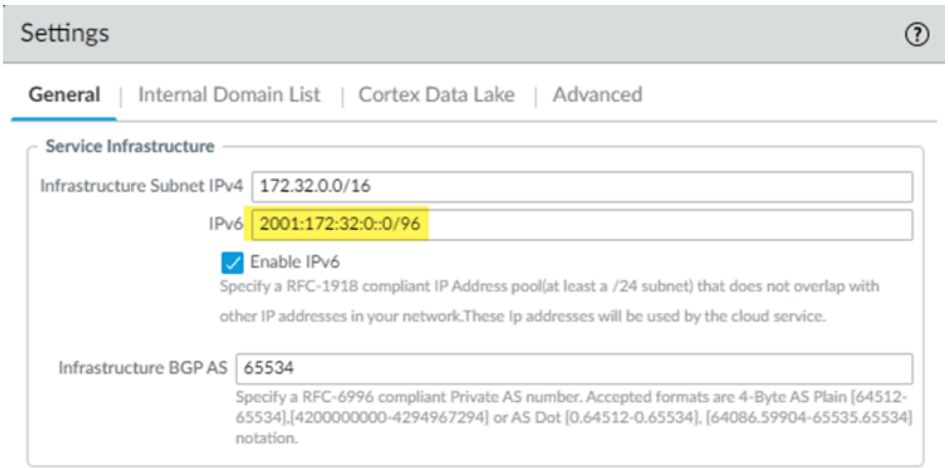
Prisma Access. Palo Alto Networks recomienda que confirme este cambio de configuración durante una ventana de mantenimiento o durante las horas de menor actividad.

Si necesita eliminar IPv6, elimine toda la configuración (incluidas las de usuarios móviles, redes remotas y conexiones de servicio, según corresponda) antes de anular la selección de la casilla de verificación ***Enable IPv6 (Habilitar IPv6)****.*



STEP 3 | Especifique una subred de infraestructura **IPv6** y una **Infrastructure BGP AS (Infraestructura BGP AS)**.

- Especifique una subred mínima de /96.
- También debe introducir una subred IPv4; Prisma Access requiere subredes IPv4 e IPv6 en su infraestructura de red para usar IPv6. Consulte Configure la Infraestructura de servicios de Prisma Access (Panorama) para obtener más detalles.
- Palo Alto Networks recomienda que utilice direcciones IPv4 e IPv6 privadas (no públicas).
- No utilice direcciones locales de enlace IPv6 (fe80::/10).



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Introduzca la **Infrastructure BGP AS (Infraestructura BGP AS)** que desea utilizar dentro de la infraestructura Prisma Access.

Si desea utilizar el enrutamiento dinámico para permitir que Prisma Access descubra dinámicamente rutas a recursos en sus redes remotas y ubicaciones de centros de datos/sede, especifique el número de sistema autónomo (AS). Si no proporciona un número AS, se utilizará el número AS predeterminado 65534.

STEP 5 | Si aún no ha completado la configuración de instalación del servicio, introduzca las configuraciones de **Internal Domain List (Lista de dominios internos)**, **Strata Logging Service (Servicio de creación de logs de Strata)** y **Advanced (Avanzado)**.

Consulte Configure la Infraestructura de servicios de Prisma Access (Panorama) para obtener más detalles.

STEP 6 | (Solo implementaciones de usuarios móviles) Añada grupos de direcciones IP IPv6 para sus implementaciones de Usuarios móviles: GlobalProtect.

Una implementación de Usuarios móviles: GlobalProtect requiere grupos de direcciones IP. Se requieren grupos de direcciones IP tanto IPv4 como IPv6 para habilitar la funcionalidad IPv6. Aplica direcciones IPv4 a nivel regional o mundial; aplica direcciones IPv6 a nivel mundial. Especifique una subred mínima de /80.

Prisma Access subdivide las direcciones IPv6 mundiales utilizando el siguiente método:

- Prisma Access asigna a cada ubicación (puerta de enlace) un grupo de una subred /112. Debido a que cada conexión GlobalProtect utiliza una dirección IP del grupo, esta

 ©2025 Palo Alto Networks, Inc.

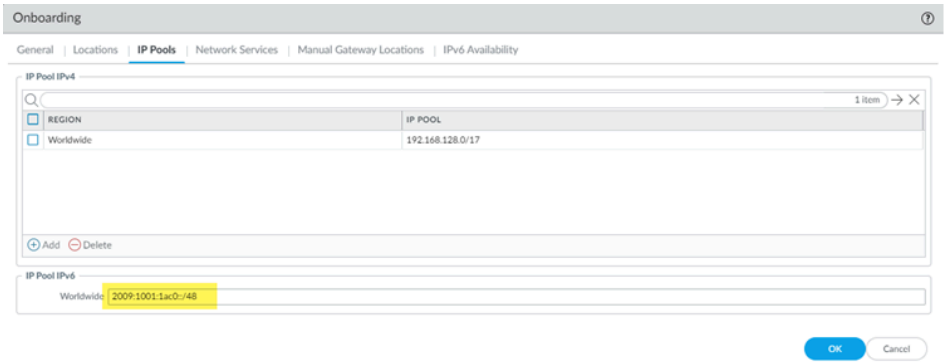
asignación permite asignar más de 65.000 direcciones IPv6 disponibles a los endpoints de los usuarios por ubicación.

Si experimenta un evento de escalado automático (si un gran número de usuarios inicia sesión en una sola ubicación de Prisma Access), Prisma Access puede añadir otra ubicación con otra subred /112.

- Cuando habilita una ubicación para usar IPv6, Prisma Access asigna un grupo de direcciones IPv6 a la región a la que pertenece la ubicación y divide el grupo entre el número total de regiones que tienen habilitada IPv6.

No utilice direcciones de vínculo local (fe80::/10) en un grupo de direcciones IP.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect**.
2. En la sección Incorporación, seleccione el **Hostname (Nombre de host)** del portal o seleccione **Configure (Configurar)**.
3. Seleccione la pestaña **IP Pools (Grupos de IP)**.
4. Introduzca un **IP Pool IPv6 (Grupo de direcciones IP IPv6)**.
   - Debe introducir direcciones IP IPv4 e IPv6 para usuarios móviles. Prisma Access requiere que las direcciones IPv4 e IPv6 sean compatibles con su infraestructura interna cuando se utiliza IPv6.
   - Introduzca una subred IPv6 mínima de /80.
   - Prisma Access subdivide cada subred por región.



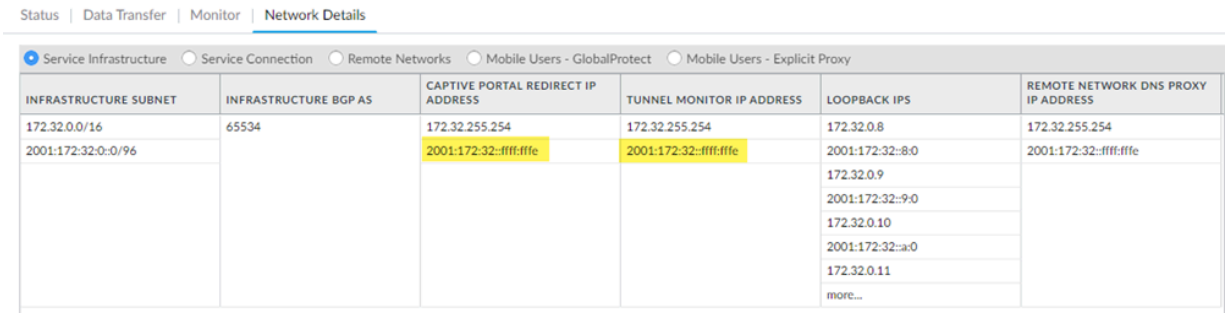
STEP 7 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Infrastructure (Infraestructura de servicios)** y tome nota de las siguientes direcciones IPv6:

- **Captive Portal Redirect IP Addresses (Direcciones IP de redireccionamiento del portal cautivo)**: se utiliza con la asignación de direcciones de User-ID basada en el Portal de autenticación
- **Dirección IP del** monitor de túnel: se utiliza para la supervisión de túneles

Debido a que los usuarios móviles de GlobalProtect requieren una dirección IPv4 para los túneles VPN, direcciones de bucle invertido, cuyas direcciones IP se toman de la subred de infraestructura, siguen utilizando direcciones IPv4.



Habilite la red IPv6 para la implementación de Usuarios móviles: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access versión 2.2 Preferred y posteriores ❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 para nuevas implementaciones únicamente. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

Además de especificar grupos de direcciones IP de usuarios móviles, debe configurar la **IPv6 Availability (Disponibilidad IPv6)** para sus implementaciones de Usuarios móviles: GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

Si su red utiliza servidores DNS IPv6 para resolver dominios internos, también puede especificar direcciones IPv6 para servidores DNS primarios y secundarios, como se muestra en la sección a continuación.

- Strata Cloud Manager
- Panorama

Habilitar las redes IPv6 para una implementación de Usuarios móviles: GlobalProtect (Strata Cloud Manager)

Además de especificar grupos de direcciones IP de usuarios móviles, debe configurar la **IPv6 Availability (Disponibilidad IPv6)** para sus implementaciones de Usuarios móviles: GlobalProtect. Si su red utiliza servidores DNS IPv6 para resolver dominios internos, también puede especificar direcciones IPv6 para servidores DNS primarios y secundarios, como se muestra en la sección a continuación.

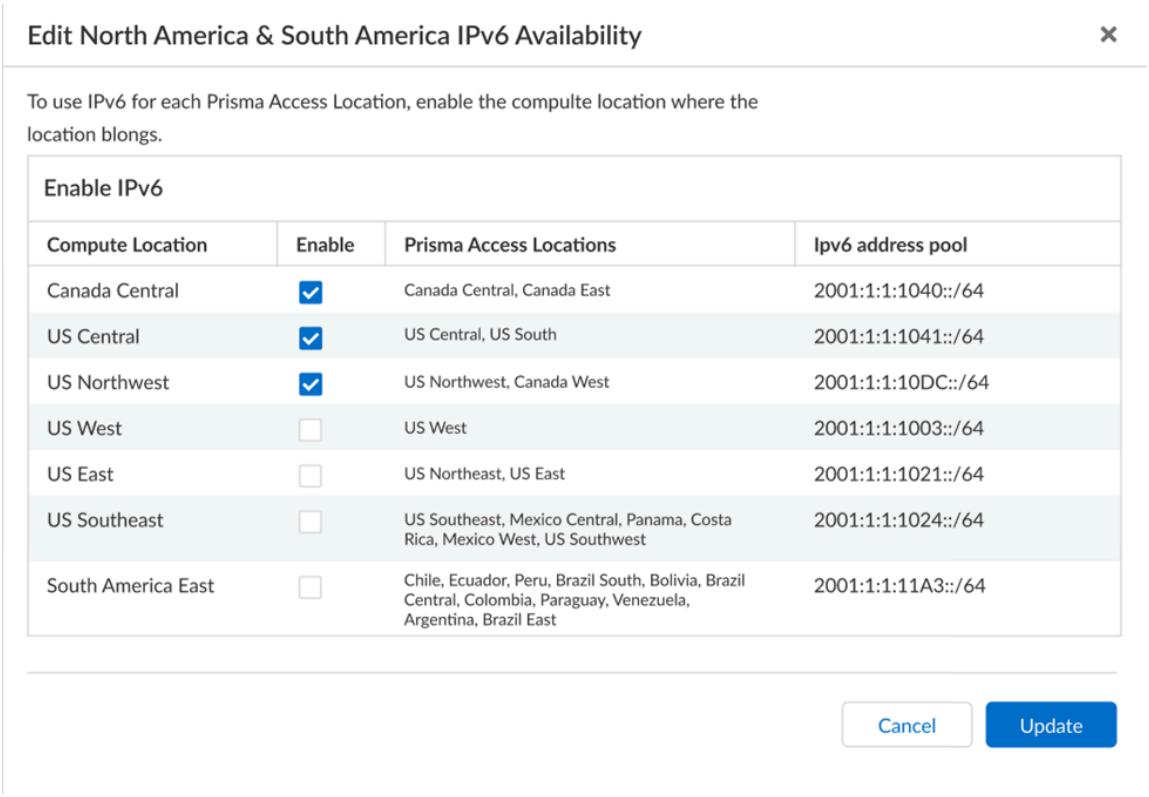
STEP 1 | Planifique si desea implementar IPv6 en toda la implementación de su Prisma Access, o solo para un cierto número de ubicaciones de cómputo.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configure la disponibilidad de IPv6 para las regiones donde desea implementar IPv6.

1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** y seleccione el icono de engranaje para editar la **Infrastructure Settings (Configuración de infraestructura)**.
2. En la sección **IPv6 Settings (Configuración IPv6)**, elija las ubicaciones para las que desea **Enable (Habilitar)** IPv6.

   Todas las ubicaciones están asociadas a una ubicación de cómputo. Si las ubicaciones en una ubicación de cómputo no tienen habilitada IPv6, deje esa ubicación de cómputo sin seleccionar.



STEP 3 | (Opcional) Si las direcciones IPv6 son accesibles para sus servidores DNS internos, seleccione **Add Region (Añadir región)** en la sección **Client DNS (DNS cliente)**, active la casilla de verificación para **Resolve Internal Domains (Resolver dominios internos)**, y **Add (Añadir)** una regla o especificar la regla predeterminada, y especificar direcciones IPv6 **Custom (Personalizadas)** del servidor DNS para el servidor **Primary DNS (DNS primario)** y el **Secondary DNS (DNS secundario)**.

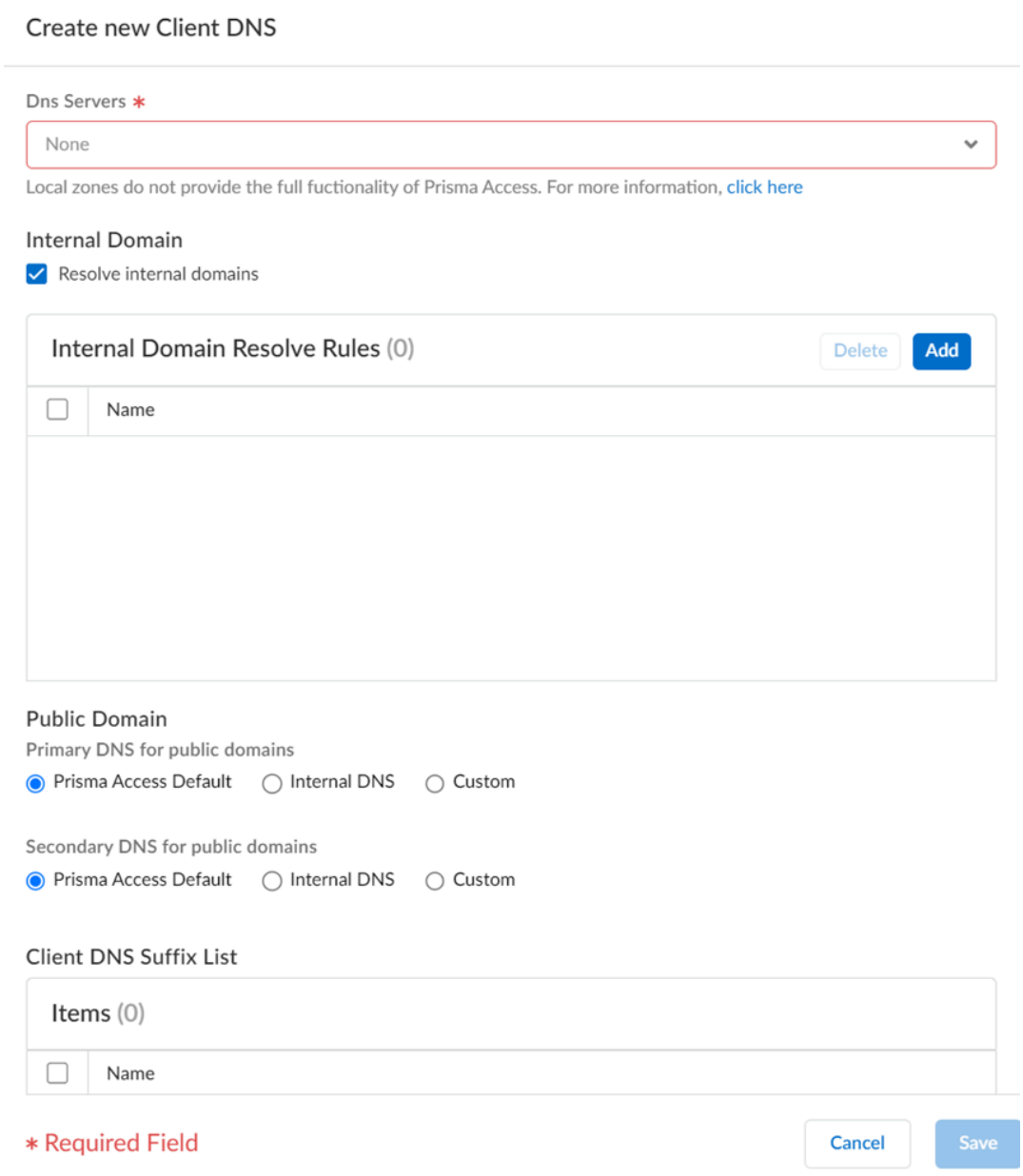
Si introduce direcciones IPv6 para servidores DNS, también debe tener direcciones IPv6 en su grupo de direcciones IP de usuario móvil.

Puede introducir cualquier combinación de direcciones IPv4 o IPv6 para servidores DNS primarios y secundarios. Si introduce una dirección IPv6 para el servidor DNS primario y una dirección IPv4 para el servidor DNS secundario, y se recibe una consulta DNS desde una

 ©2025 Palo Alto Networks, Inc.

ubicación de cómputo que no tiene habilitada la **IPv6 Availability (Disponibilidad IPv6)**, Prisma Access usa el servidor DNS secundario porque usa una dirección IPv4.

Las direcciones IPv4 usan registros A, mientras que las direcciones IPv6 usan registros AAAA. Algunos servidores DNS pueden realizar consultas DNS AAAA a través del transporte IPv4; por lo tanto, es posible que no necesite un servidor con una dirección IP IPv6.



STEP 4 | (Opcional) Si aún no has completado la configuración de usuarios móviles, complétala ahora. Consulte Configurar usuarios móviles de GlobalProtect para obtener más detalles.

STEP 5 | **Push Config (Enviar configuración)** para implementar los cambios en su red.

 ©2025 Palo Alto Networks, Inc.

Habilitar las redes IPv6 para una implementación de Usuarios móviles: GlobalProtect (Panorama)

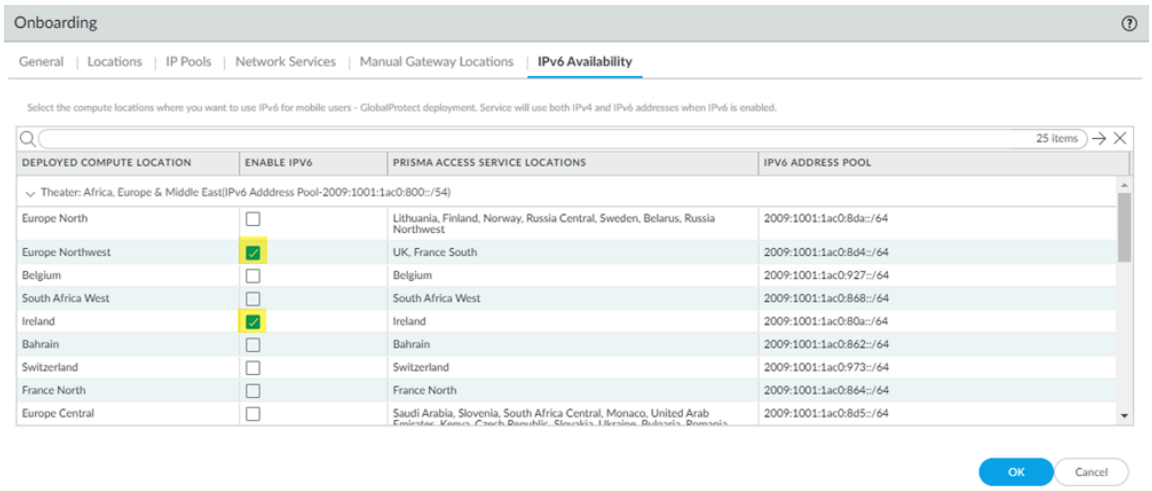
Además de especificar grupos de direcciones IP de usuarios móviles, debe configurar la **IPv6 Availability (Disponibilidad IPv6)** para sus implementaciones de Usuarios móviles: GlobalProtect. Si su red utiliza servidores DNS IPv6 para resolver dominios internos, también puede especificar direcciones IPv6 para servidores DNS primarios y secundarios, como se muestra en la sección a continuación.

STEP 1 | Planifique si desea implementar IPv6 en toda la implementación de su <ph keyref="pa"/>, o solo para un cierto número de ubicaciones de cómputo.

STEP 2 | Configure la disponibilidad de IPv6 para las regiones donde desea implementar IPv6.

1. En la pestaña de **IPv6 Availability (Disponibilidad de IPv6)**, **Enable IPv6 (Habilitar IPv6)** para las ubicaciones para las que desea habilitar IPv6.

   Todas las ubicaciones están asociadas a una ubicación de cómputo. Si las ubicaciones en una ubicación de cómputo no tienen habilitada IPv6, deje esa ubicación de cómputo sin seleccionar.



STEP 3 | (Opcional) Si sus servidores DNS internos son accesibles mediante direcciones IPv6, haga clic en la pestaña **Network Services (Servicios de red)**, **Add (Añadir)** una regla o especificar la regla predeterminada, y especificar las direcciones IPv6 del **Custom DNS Server (Servidor DNS personalizado)** para el servidor **Primary DNS (DNS primario)** y el servidor **Secondary DNS (DNS secundario)**.

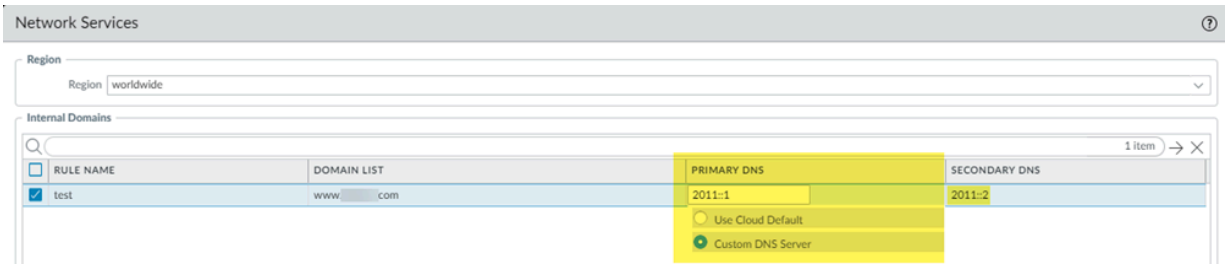
Si introduce direcciones IPv6 para servidores DNS, también debe tener direcciones IPv6 en su grupo de direcciones IP de usuario móvil.

Puede introducir cualquier combinación de direcciones IPv4 o IPv6 para servidores DNS primarios y secundarios. Si introduce una dirección IPv6 para el servidor DNS primario y una dirección IPv4 para el servidor DNS secundario, y se recibe una consulta DNS desde una

 ©2025 Palo Alto Networks, Inc.

ubicación de cómputo que no tiene habilitada la **IPv6 Availability (Disponibilidad IPv6)**, <ph keyref="pa"/> usa el servidor DNS secundario porque usa una dirección IPv4.

Las direcciones IPv4 usan registros A, mientras que las direcciones IPv6 usan registros AAAA. Algunos servidores DNS pueden realizar consultas DNS AAAA a través del transporte IPv4; por lo tanto, es posible que no necesite un servidor con una dirección IP IPv6.



STEP 4 | (Opcional) Si aún no ha completado la configuración de usuarios móviles, complétela ahora. Consulte Configurar usuarios móviles de GlobalProtect para obtener más detalles.

STEP 5 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

Habilitar redes IPv6 para conexiones de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access versión 2.2 Preferred y posteriores ❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 para nuevas implementaciones únicamente. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

Para conexiones de servicio, puede utilizar subredes IPv6 para el enrutamiento estático o BGP. Para el enrutamiento BGP, puede introducir direcciones de peers IPv6 y especificar las opciones de enrutamiento IPv4 e IPv6.

Para configurar redes IPv6 para conexiones de servicio, complete la siguiente tarea.

 ©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

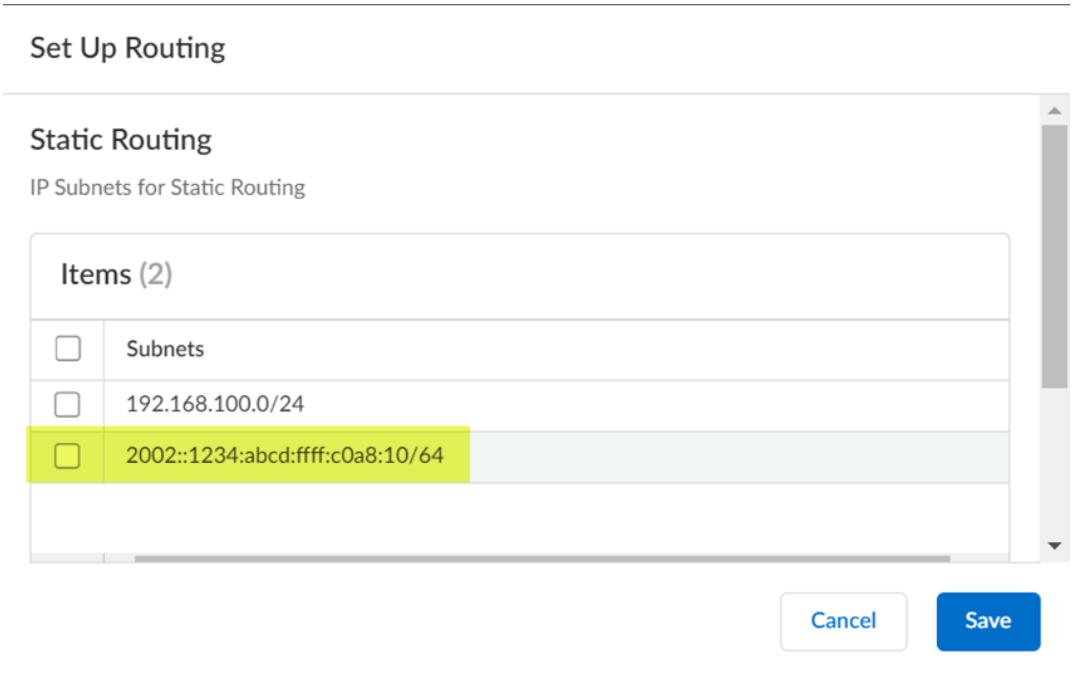
Habilitar redes IPv6 para conexiones de servicio (Strata Cloud Manager)

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)** y **Add Service Connection (Añadir conexión de servicio)**.

STEP 2 | Deberá añadir una nueva conexión de servicio o seleccionar una conexión de servicio existente para modificarla.

STEP 3 | Configurar el enrutamiento IPv6 para la conexión del servicio.

1. (Solo implementaciones de enrutamiento estático) Introduzca una o más **Corporate Subnets (Subredes corporativas)** en la pestaña **Static Routes (Rutas estáticas)**.



2. (Solo implementaciones de enrutamiento BGP) Especifique el método para intercambiar rutas IPv4 e IPv6 con BGP; luego, introduzca una **Peer Address (Dirección de peer)** y **Local Address (Dirección local)** de IPv6.
   - Para utilizar una única sesión IPv4 con BGP para intercambiar información de emparejamiento IPv4 y IPv6 con BGP, seleccione **Exchange both IPv4 and IPv6 routes over IPv4 peering (Intercambiar rutas IPv4 e IPv6 a través de emparejamiento IPv4)**.
   - Para que una sesión BGP IPv4 intercambie información de emparejamiento BGP IPv4 y una sesión IPv6 para intercambiar información de emparejamiento BGP IPv6, seleccione **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Intercambiar rutas IPv4 a través del emparejamiento IPv4 y rutas IPv6 a través del emparejamiento IPv6**.

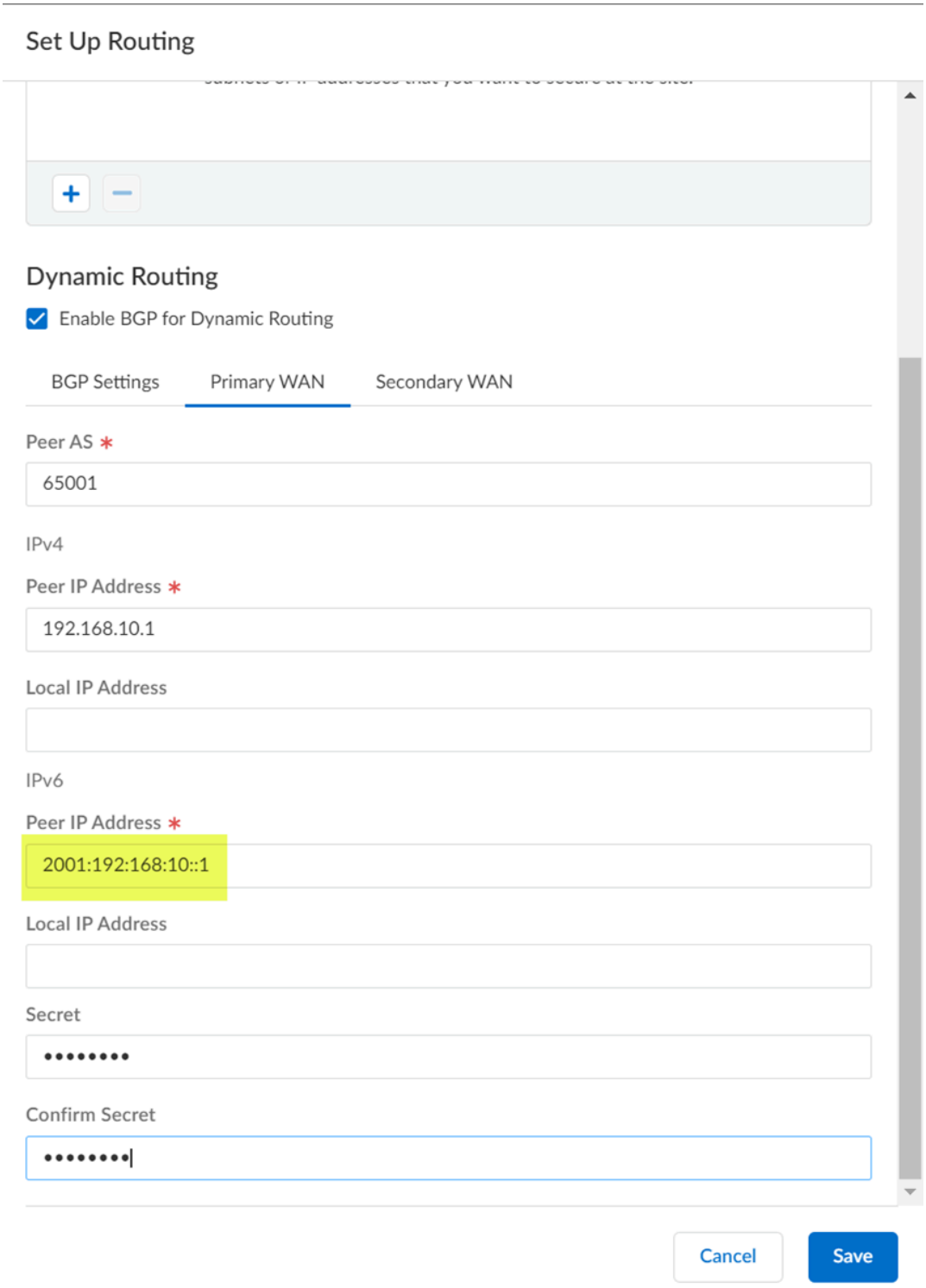
 ©2025 Palo Alto Networks, Inc.

- Para utilizar una única sesión IPv6 con BGP para intercambiar información de emparejamiento IPv6 con BGP, seleccione **Exchange IPv6 routes over IPv6 peering (Intercambiar rutas IPv6 a través de emparejamiento IPv6)**.

3. Si su WAN secundaria utiliza una dirección local o un peer diferente, quite la marca de verificación de la opción **Same as Primary WAN (Igual que la WAN principal)** e

 ©2025 Palo Alto Networks, Inc.

introduzca la **Peer Address (Dirección peer)** y **Local Address (Dirección local)** de IPv6 para la WAN secundaria.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Si aún no ha completado la configuración de la conexión de su servicio, complétela ahora. Consulte Configurar una conexión de servicio en Prisma Access para obtener más detalles.

> *El acceso a Internet mediante IPv6 para conexiones de servicio se habilita mediante una conexión subyacente, en la que el tráfico IPv6 pasa a través de un túnel IPv4.*

STEP 5 | **Push Config (Enviar configuración)** para implementar los cambios en su red.

STEP 6 | Si aún no ha completado la configuración de usuarios móviles, complétela ahora.

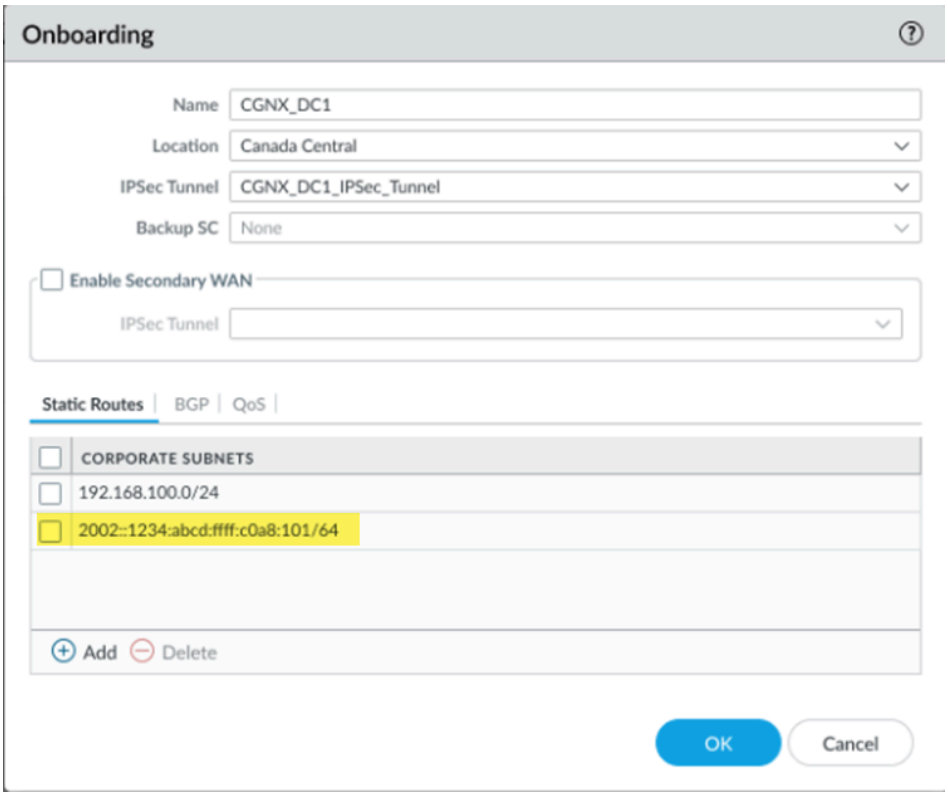
Habilitar redes IPv6 para conexiones de servicio (Panorama)

STEP 1 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicios)**.

STEP 2 | Deberá **Add (Añadir)** una nueva conexión de servicio o seleccionar una conexión de servicio existente para modificarla.

STEP 3 | Configurar el enrutamiento IPv6 para la conexión del servicio.

1. (Solo implementaciones de enrutamiento estático) Introduzca una o más **Corporate Subnets (Subredes corporativas)** en la pestaña **Static Routes (Rutas estáticas)**.



2. (Solo implementaciones de enrutamiento BGP) Especifique el método para intercambiar rutas IPv4 e IPv6 con BGP; luego, introduzca una **Peer Address (Dirección de peer)** y **Local Address (Dirección local)** de IPv6.
   - Para utilizar una única sesión IPv4 con BGP para intercambiar información de emparejamiento IPv4 y IPv6 con BGP, seleccione **Exchange both IPv4 and IPv6**

 ©2025 Palo Alto Networks, Inc.

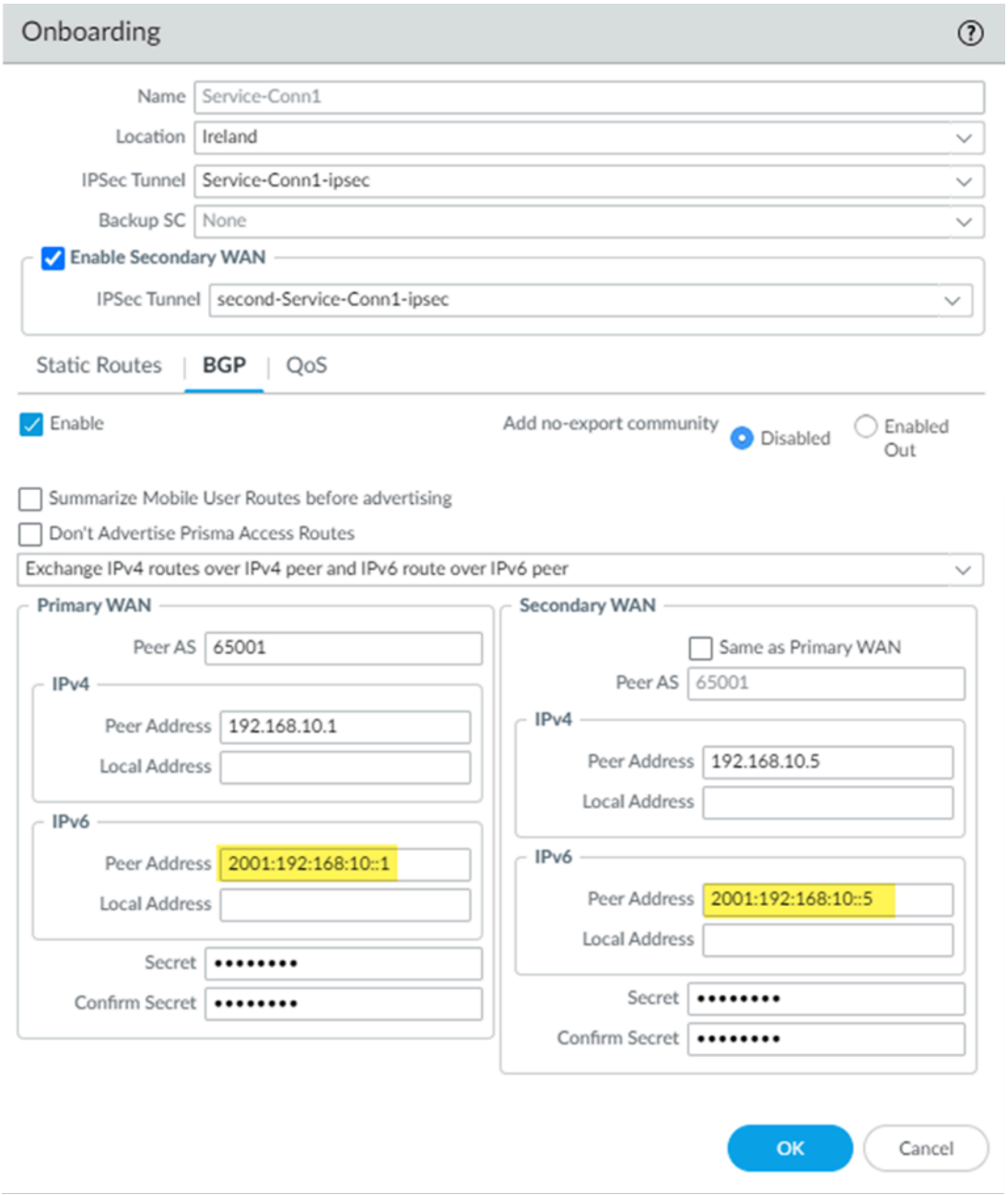
routes over IPv4 peering (Intercambiar rutas IPv4 e IPv6 a través de emparejamiento IPv4).

- Para que una sesión BGP IPv4 intercambie información de emparejamiento BGP IPv4 y una sesión IPv6 para intercambiar información de emparejamiento BGP IPv6, seleccione **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Intercambiar rutas IPv4 a través del emparejamiento IPv4 y rutas IPv6 a través del emparejamiento IPv6**.
- Para utilizar una única sesión IPv6 con BGP para intercambiar información de emparejamiento IPv6 con BGP, seleccione **Exchange IPv6 routes over IPv6 peering (Intercambiar rutas IPv6 a través de emparejamiento IPv6)**.

3. Si su WAN secundaria utiliza una dirección local o un peer diferente, quite la marca de verificación de la opción **Same as Primary WAN (Igual que la WAN principal)** e

 ©2025 Palo Alto Networks, Inc.

introduzca la **Peer Address (Dirección peer)** y **Local Address (Dirección local)** de IPv6 para la WAN secundaria.



STEP 4 | Si aún no ha completado la configuración de la conexión de su servicio, complétela ahora. Consulte Configurar una conexión de servicios en Prisma Access para obtener detalles.

STEP 5 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 6 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** y tome nota de

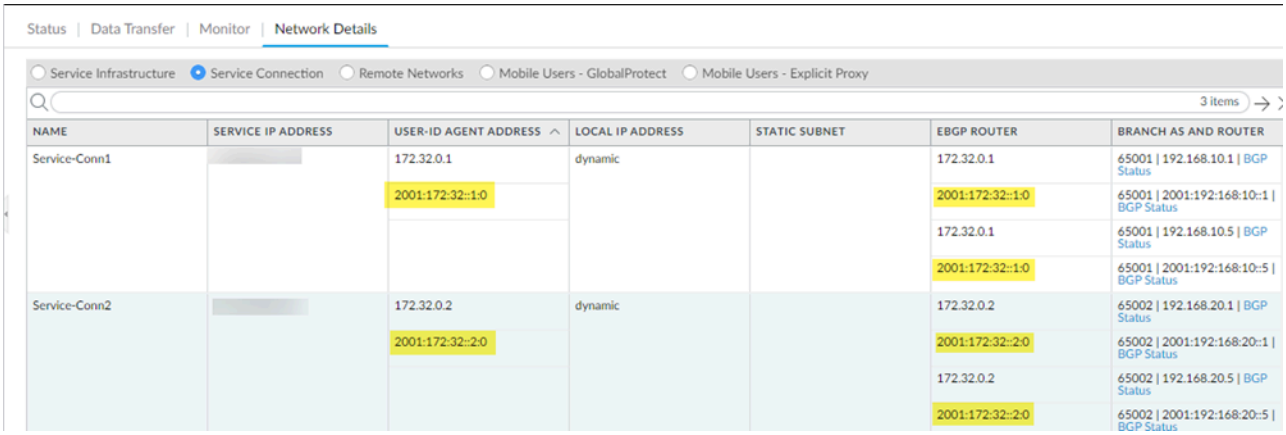
 ©2025 Palo Alto Networks, Inc.

las direcciones IPv6 de **User-ID Agent Address (Dirección del agente de User-ID)** y **EBGP Router (Enrutador EBGP)**.

Después de Commit (Confirmar) sus cambios, tendrá una **dirección de agente de ID de usuario** IPv6 (utilizada para la recuperación y distribución de ID de usuario) y direcciones **de enrutador EBGP** para conexiones de servicio.

Debido a que el túnel IPSec utilizado para la conexión de servicio utiliza direccionamiento IPv4, la **Service IP Address (Dirección IP del servicio)** es una dirección IPv4.

El acceso a Internet mediante IPv6 para conexiones de servicio se habilita mediante una conexión subyacente, en la que el tráfico IPv6 pasa a través de un túnel IPv4.



STEP 7 | Si aún no ha completado la configuración de usuarios móviles, complétela ahora.

Habilitar redes IPv6 para Redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access versión 2.2 Preferred y posteriores ❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 para nuevas implementaciones únicamente. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

 ©2025 Palo Alto Networks, Inc.

Para las conexiones de redes remotas, puede utilizar subredes IPv6 para rutas estáticas. Para el enrutamiento BGP, puede introducir direcciones de pares IPv6 y especificar que BGP use solo enrutamiento IPv6 o enrutamiento IPv4 e IPv6.

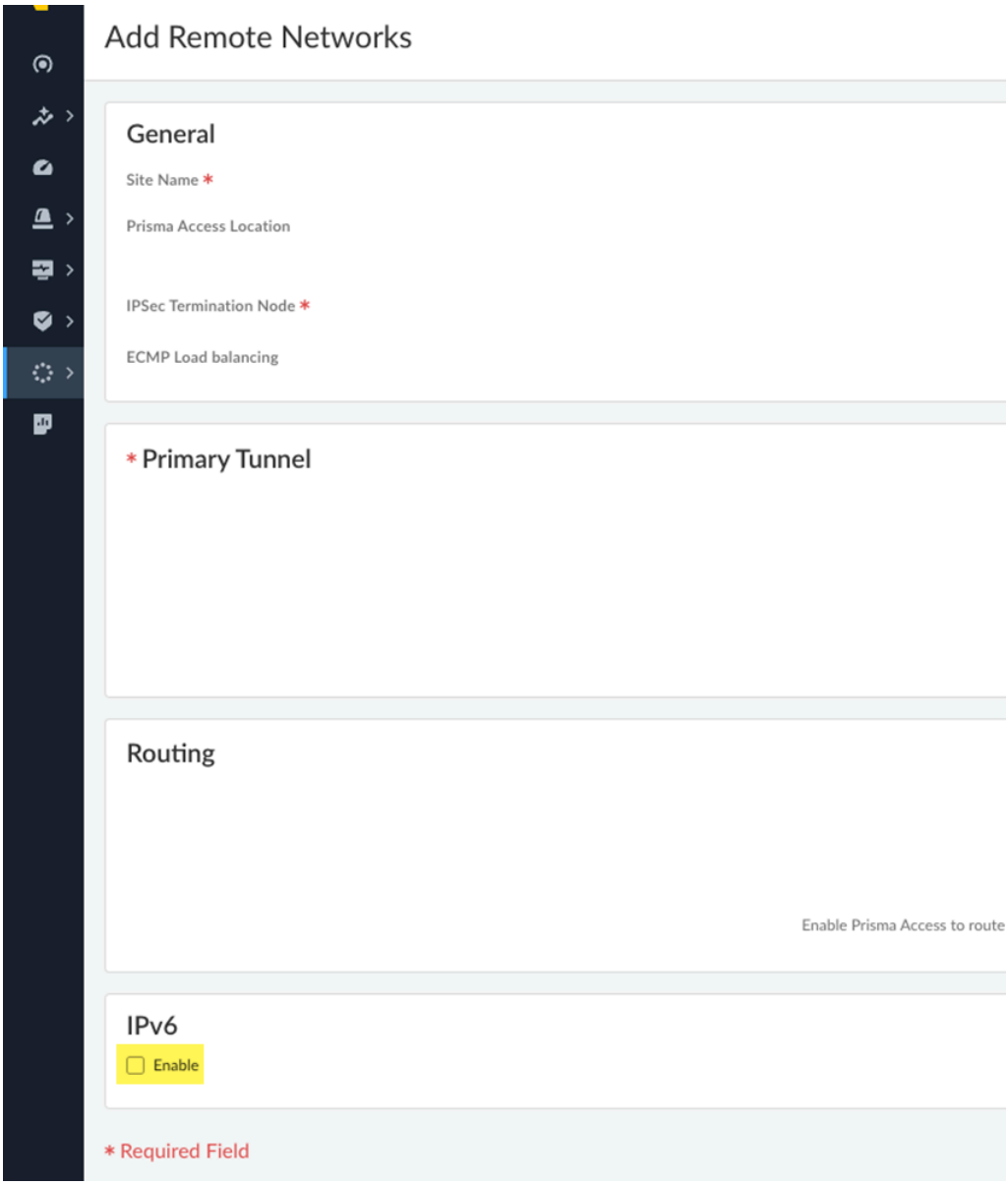
Para configurar la red IPv6 para conexiones de red remotas, complete la siguiente tarea.

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

Habilitar redes IPv6 para redes remotas (Strata Cloud Manager)

STEP 1 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)**y **Add Remote Networks (Añadir redes remotas)**.

STEP 2 | **Enable (Habilitar)** IPv6.

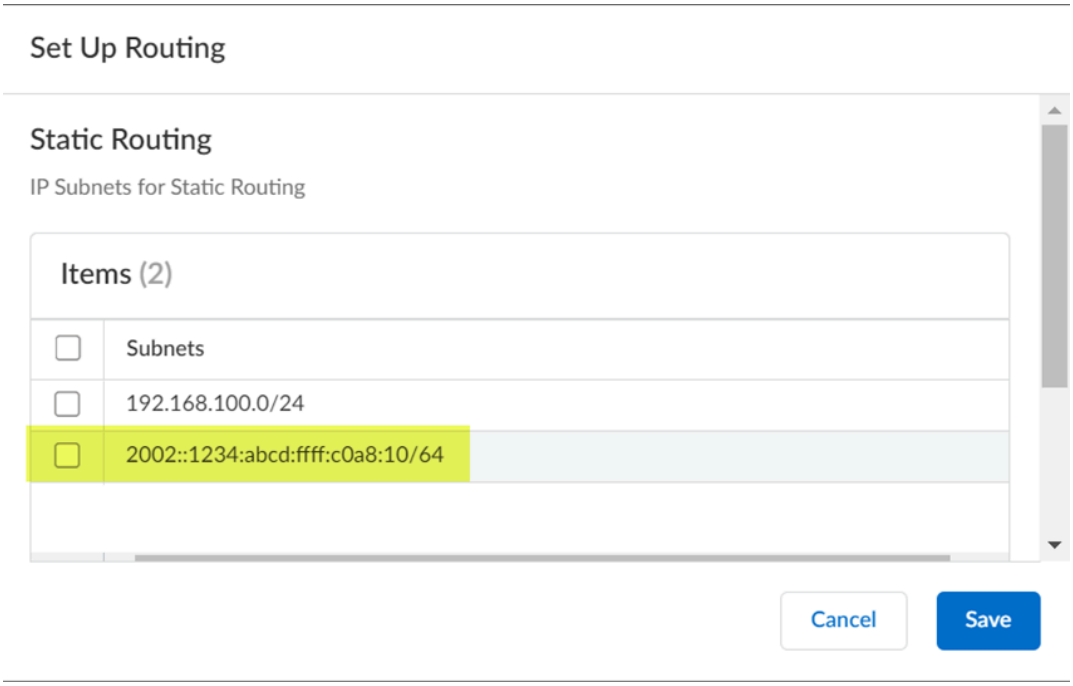


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Añada una nueva conexión de red remota o seleccione una conexión de red remota existente para modificarla.

STEP 4 | Configure el enrutamiento IPv6 para su red remota.

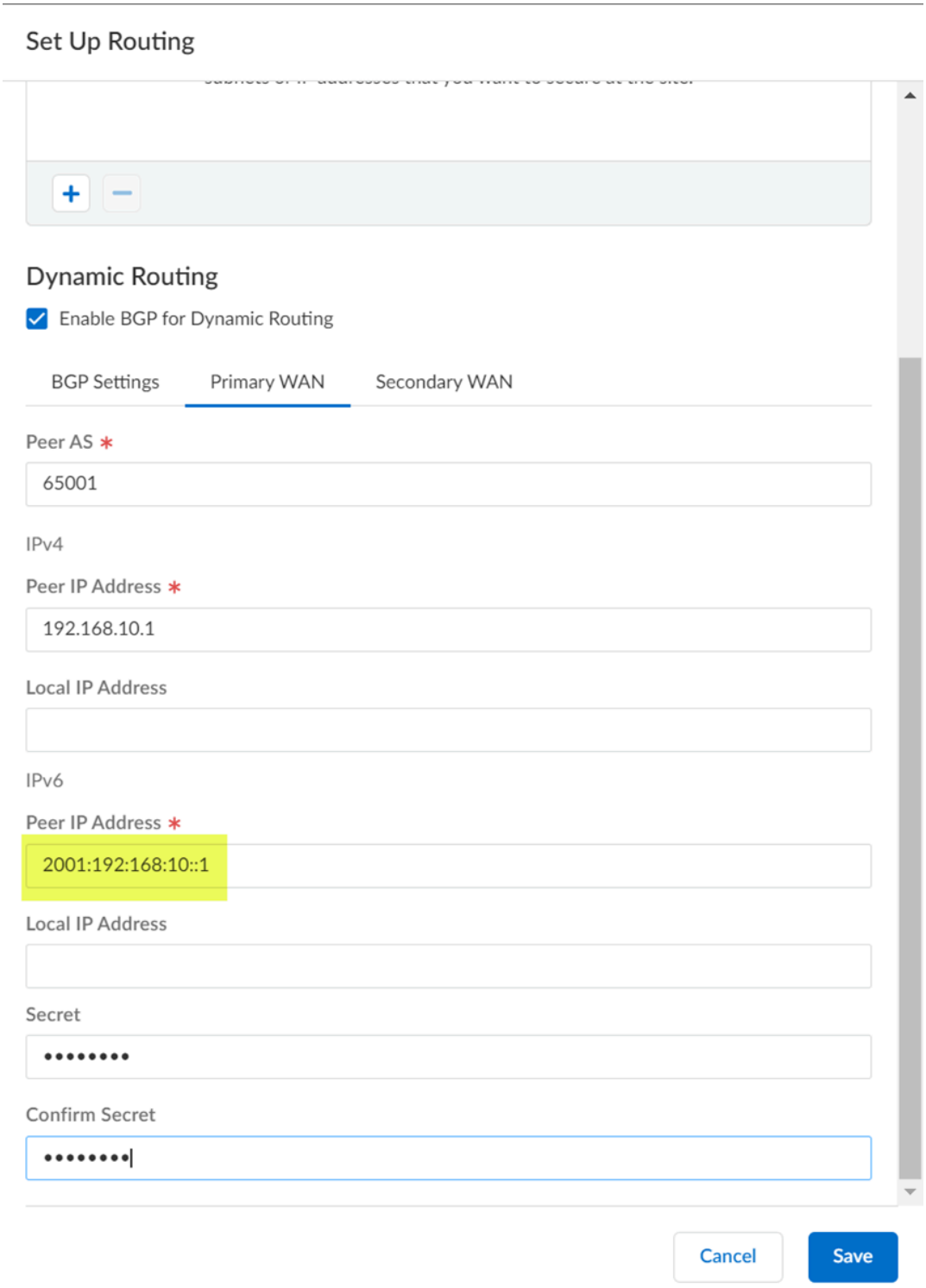
1. (Solo implementaciones de enrutamiento estático) Introduzca una o más **Corporate Subnets (Subredes corporativas)** en la pestaña **Static Routes (Rutas estáticas)**.



2. (Solo implementaciones de enrutamiento BGP) Especifique el método para intercambiar rutas IPv4 e IPv6 con BGP; luego, introduzca una **Peer Address (Dirección de peer)** y **Local Address (Dirección local)** de IPv6.
   - Para utilizar una única sesión IPv4 con BGP para intercambiar información de emparejamiento IPv4 y IPv6 con BGP, seleccione **Exchange both IPv4 and IPv6 routes over IPv4 peering (Intercambiar rutas IPv4 e IPv6 a través de emparejamiento IPv4)**.
   - Para que una sesión BGP IPv4 intercambie información de emparejamiento BGP IPv4 y una sesión IPv6 para intercambiar información de emparejamiento BGP IPv6, seleccione **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Intercambiar rutas IPv4 a través del emparejamiento IPv4 y rutas IPv6 a través del emparejamiento IPv6**.
   - Para utilizar una única sesión IPv6 con BGP para intercambiar información de emparejamiento IPv6 con BGP, seleccione **Exchange IPv6 routes over IPv6 peering (Intercambiar rutas IPv6 a través de emparejamiento IPv6)**.
3. Si su WAN secundaria utiliza una dirección local o un peer diferente, quite la marca de verificación de la opción **Same as Primary WAN (Igual que la WAN principal)** e

 ©2025 Palo Alto Networks, Inc.

introduzca la **Peer Address (Dirección peer)** y **Local Address (Dirección local)** de IPv6 para la WAN secundaria.



STEP 5 | (Opcional) Si sus servidores DNS internos son accesibles mediante direcciones IPv6, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración Prisma Access)** > **Remote Networks (Redes remotas)** > **Advanced Settings (Configuración**

 ©2025 Palo Alto Networks, Inc.

avanzada) busque **DNS Proxy (Proxy DNS)**, **Add (Añadir)** una regla o especifique la regla predeterminada, y especifique las direcciones IPv6 del **Custom DNS Server (Servidor DNS personalizado)** para el servidor **Primary DNS (DNS primario)** y el servidor **Secondary DNS (DNS secundario)**.

Prisma Access le permite especificar los servidores DNS para resolver tanto los dominios internos de su organización como los dominios externos. Si no especifica ninguna configuración, Prisma Access no envía solicitudes DNS para redes remotas. También debe seleccionar una **Region (Región)**.

Puede introducir cualquier combinación de direcciones IPv4 o IPv6 para servidores DNS primarios y secundarios.

- *Las direcciones IPv4 usan registros A, mientras que las direcciones IPv6 usan registros AAAA. Algunos servidores DNS pueden realizar consultas DNS AAAA a través del transporte IPv4; por lo tanto, es posible que no necesite un servidor con una dirección IP IPv6.*

STEP 6 | Si aún no ha completado la configuración de la conexión de red remota, complétela ahora.

El acceso a Internet mediante IPv6 para conexiones de red remotas se habilita mediante una conexión subyacente, en la que el tráfico IPv6 pasa a través de un túnel IPv4.

STEP 7 | **Push Config (Enviar configuración)** para implementar los cambios en su red.

Habilitar redes IPv6 para redes remotas (Panorama)

STEP 1 | (Opcional) Introduzca direcciones IPv6 en su configuración de proxy de servidor DNS personalizado.

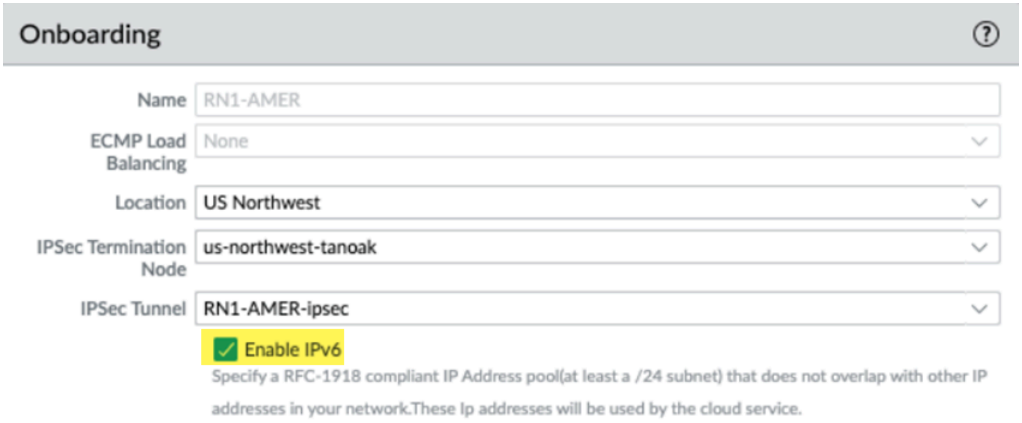
1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y edite la configuración haciendo clic en el icono de engranaje en el área **Settings (Configuración)**.
2. En el área **DNS Proxy (Proxy DNS)**, introduzca direcciones de **Custom DNS Server (Servidor DNS personalizado)** IPv6 para su configuración de proxy DNS.

STEP 2 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.

STEP 3 | Seleccione **Add (Añadir)** una nueva conexión de red remota o seleccione una conexión de red remota existente para modificarla.

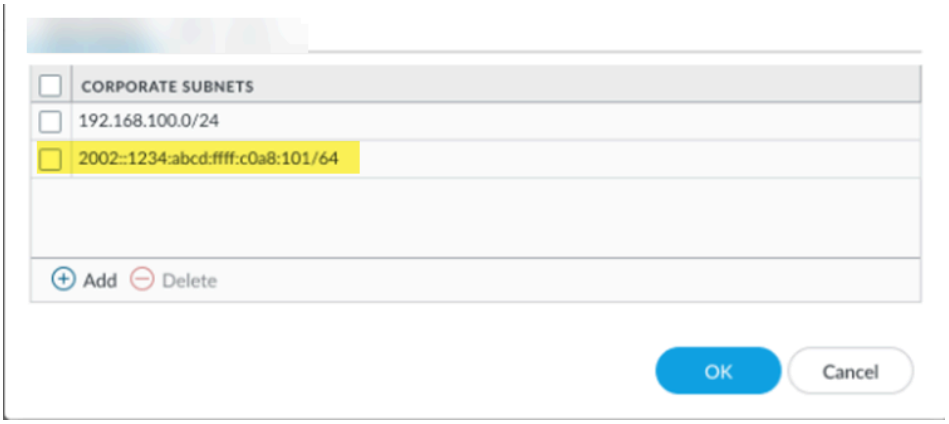
 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Enable IPv6 (Habilitar IPv6).**



STEP 5 | Configure el enrutamiento IPv6 para su red remota.

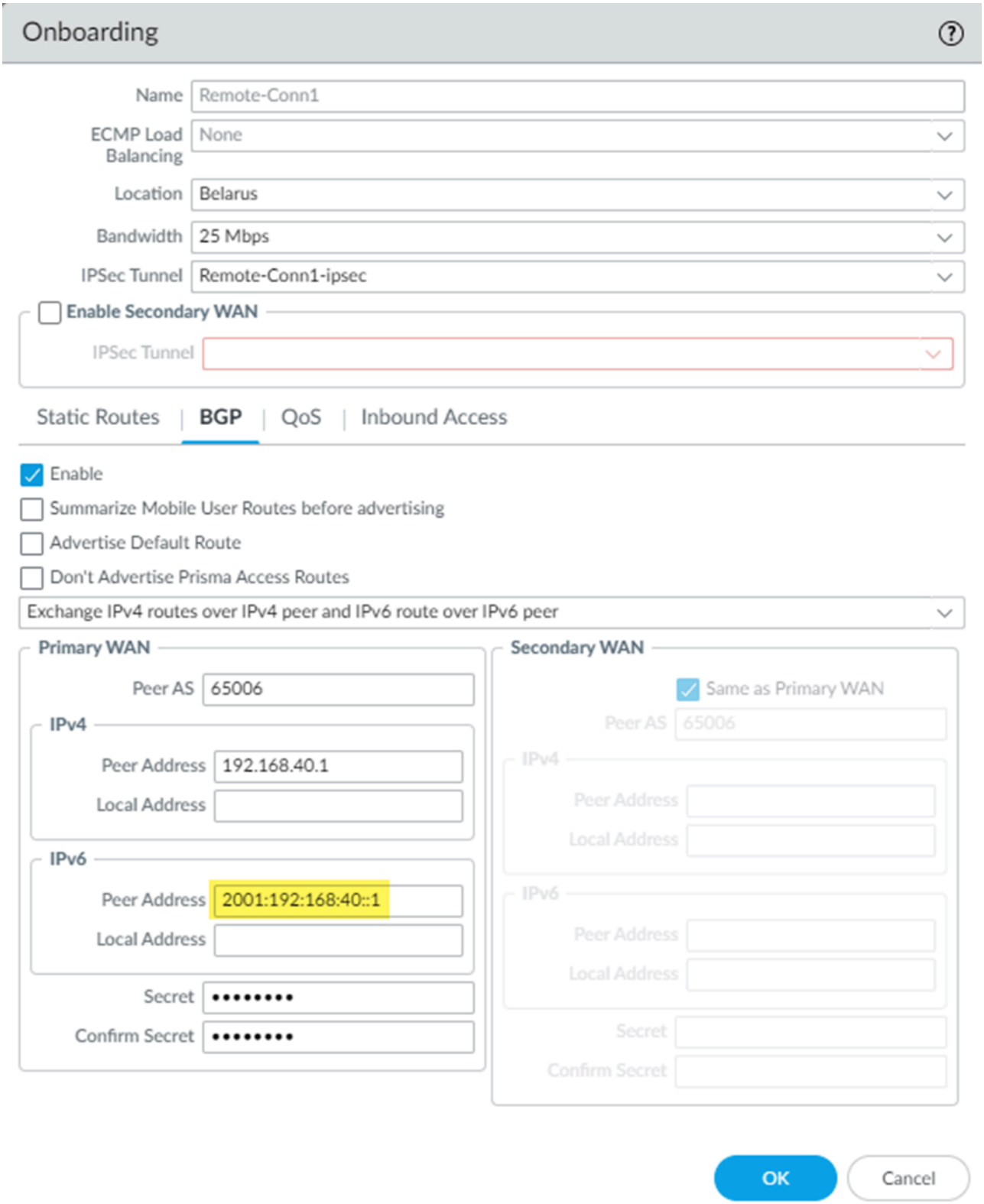
1. (Solo implementaciones de enrutamiento estático) Introduzca una o más **Corporate Subnets (Subredes corporativas)** en la pestaña **Static Routes (Rutas estáticas)**.



2. (Solo implementaciones de enrutamiento BGP) Especifique el método para intercambiar rutas IPv4 e IPv6 con BGP; luego, introduzca una **Peer Address (Dirección de peer)** y **Local Address (Dirección local)** de IPv6.
   - Para utilizar una única sesión IPv4 con BGP para intercambiar información de emparejamiento IPv4 y IPv6 con BGP, seleccione **Exchange both IPv4 and IPv6 routes over IPv4 peering (Intercambiar rutas IPv4 e IPv6 a través de emparejamiento IPv4)**.
   - Para que una sesión BGP IPv4 intercambie información de emparejamiento BGP IPv4 y una sesión IPv6 para intercambiar información de emparejamiento BGP IPv6, seleccione **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Intercambiar rutas IPv4 a través del emparejamiento IPv4 y rutas IPv6 a través del emparejamiento IPv6**.
   - Para utilizar una única sesión IPv6 con BGP para intercambiar información de emparejamiento IPv6 con BGP, seleccione **Exchange IPv6 routes over IPv6 peering (Intercambiar rutas IPv6 a través de emparejamiento IPv6)**.
3. Si su WAN secundaria utiliza una dirección local o un peer diferente, quite la marca de verificación de la opción **Same as Primary WAN (Igual que la WAN principal)** e

 ©2025 Palo Alto Networks, Inc.

introduzca la **Peer Address (Dirección peer)** y **Local Address (Dirección local)** de IPv6 para la WAN secundaria.



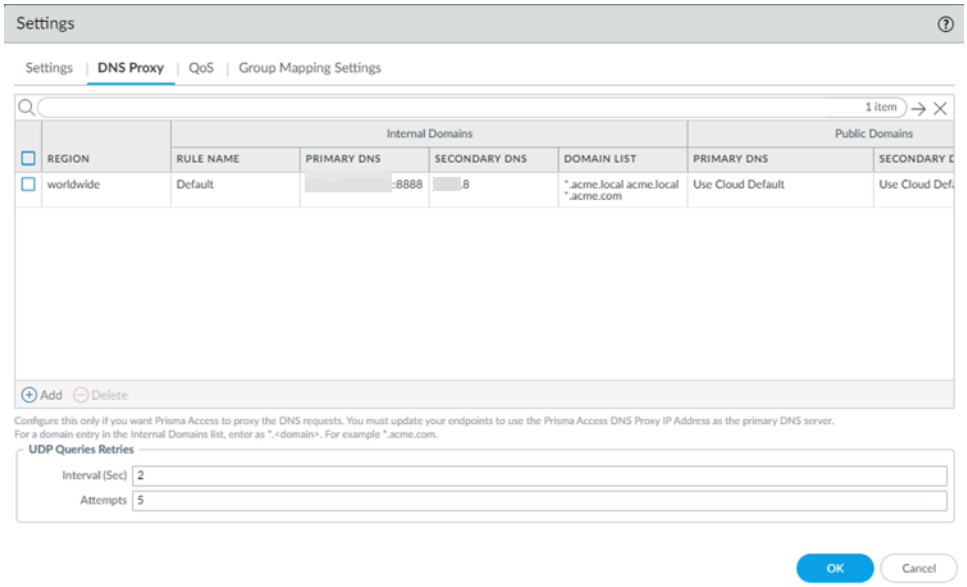
 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Si sus servidores DNS internos son accesibles mediante direcciones IPv6, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Network (Red remota)** > **Settings (Configuración)**, haga clic en el icono de engranaje para editar la configuración, seleccione la pestaña **DNS Proxy (Proxy DNS)**, elija **Add (Añadir)** una regla o especifique la regla predeterminada y especifique las direcciones IPv6 del **Custom DNS Server (Servidor DNS personalizado)** para el servidor de **Primary DNS (DNS primario)** y el servidor de **Secondary DNS (DNS secundario)** .

Prisma Access le permite especificar servidores DNS para resolver tanto los dominios internos de su organización como los dominios externos. Si no especifica ninguna configuración, Prisma Access no procesa solicitudes DNS para redes remotas. También debe seleccionar una **Region (Región)**.

Puede introducir cualquier combinación de direcciones IPv4 o IPv6 para servidores DNS primarios y secundarios.

Las direcciones IPv4 usan registros A, mientras que las direcciones IPv6 usan registros AAAA. Algunos servidores DNS pueden realizar consultas DNS AAAA a través del transporte IPv4; por lo tanto, es posible que no necesite un servidor con una dirección IP IPv6.



STEP 7 | Si aún no ha completado la configuración de la conexión de red remota, complétela ahora.

STEP 8 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** y tome nota de las direcciones del **EBGP Router (Enrutador EBGP)**.

Después de confirmar sus cambios, tendrá una dirección de **EBGP Router (Enrutador EBGP)** IPv6 para conexiones de servicio.

Debido a que el túnel IPSec utilizado para la conexión de red remota utiliza direcciones IPv4, la **Service IP Address (Dirección IP del servicio)** permanece como una dirección IPv4.

El acceso a Internet mediante IPv6 para conexiones de red remotas se habilita mediante una conexión subyacente, en la que el tráfico IPv6 pasa a través de un túnel IPv4.

 ©2025 Palo Alto Networks, Inc.

Resolución de DNS para Usuarios móviles: GlobalProtect e implementaciones de redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access versión 2.2 Preferred y posteriores ❑ El acceso IPv6 nativo a aplicaciones públicas y privadas requiere las siguientes versiones mínimas: • Prisma Access (Managed by Strata Cloud Manager): Versión de junio de 2024 • Prisma Access (Managed by Panorama): Prisma Access 5.1.1 para nuevas implementaciones únicamente. Cualquier otra implementación (incluidas las implementaciones Prisma Access (Managed by Panorama) existentes) es compatible con el acceso a aplicaciones privadas únicamente.

Prisma Access le permite especificar servidores DNS para resolver tanto los dominios internos de su organización como los dominios externos. Prisma Access realiza un proxy de la solicitud DNS en función de la configuración de sus servidores DNS. La siguiente tabla muestra los métodos de resolución de DNS admitidos para dominios internos y externos e indica cuándo Prisma Access envía por proxy las solicitudes de DNS.

Método de resolución de DNS interno	Método de resolución de DNS externo	Prisma Access realiza la proxy de la solicitud DNS (Sí/No)
Regla única, servidor DNS configurado para dominios internos	Nube predeterminada (DNS64 público de Google para IPv6)	Sí
Regla única, servidor DNS configurado para dominios internos	Igual que los dominios internos	No
Regla única, servidor DNS configurado para dominios internos	Servidor DNS personalizado (Google Public DNS64 para IPv6)	Sí

©2025 Palo Alto Networks, Inc.

Método de resolución de DNS interno	Método de resolución de DNS externo	Prisma Access realiza la proxy de la solicitud DNS (Sí/No)
Regla única, configuración predeterminada de la nube para un dominio	Nube predeterminada (DNS64 público de Google para IPv6)	Sí
Regla única, configuración predeterminada de la nube para un dominio	Igual que los dominios internos (Google Public DNS64 para IPv6)	Sí
Regla única, configuración predeterminada de la nube establecido para el dominio	Servidor DNS personalizado (Google Public DNS64 para IPv6)	Sí
Varias reglas, servidor DNS configurado para dominios internos	Nube predeterminada (DNS64 público de Google para IPv6)	Sí
Varias reglas, servidor DNS configurado para dominios internos	Igual que los dominios internos	Sí
Varias reglas, servidor DNS configurado para dominios internos	Servidor DNS personalizado (Google Public DNS64 para IPv6)	Sí
Sin configuración	Servidor DNS personalizado (Google Public DNS64 para IPv6)	Sí
Sin configuración	Cloud Default (para IPv6, principal = Google Public DNS64, secundaria = Cloud Default)	No
Sin configuración	Sin configuración	No
No se especificó ninguna resolución de DNS (la configuración predeterminada está presente, que utiliza Cloud Default)	No se especificó ninguna resolución DNS	No
ZTNA Connector (*independientemente del método de resolución DNS*)	n/c	Sí

 ©2025 Palo Alto Networks, Inc.

Método de resolución de DNS interno	Método de resolución de DNS externo	Prisma Access realiza la proxy de la solicitud DNS (Sí/No)
Después de habilitar ZTNA Connector, Prisma Access redirecciona todas las solicitudes DNS utilizando las Reglas DNS configuradas para redes remotas y Usuarios móviles: GlobalProtect.		

La dirección IP de origen de la solicitud de DNS depende de si Prisma Access utiliza o no el proxy para la solicitud de DNS.

- Cuando Prisma Access no procesa las solicitudes de DNS, la dirección IP de origen de la solicitud de DNS cambia a la dirección IP del dispositivo que solicitó la búsqueda de DNS. Esta dirección IP de origen le permite aplicar políticas de DNS basadas en direcciones IP de origen o identificar endpoints que se comunican con dominios maliciosos. Este comportamiento se aplica tanto a usuarios móviles como a implementaciones de red remotas.
- Cuando Prisma Access realiza el proxy de las solicitudes DNS, la dirección IP de origen de la solicitud DNS cambia a las siguientes direcciones:
  - **Implementaciones de usuarios móviles**: la dirección IP de origen de la solicitud de DNS es una dirección IP tomada del grupo de direcciones IP del usuario móvil para solicitudes internas y la dirección IP de puerta de enlace de la ubicación del usuario móvil para solicitudes externas.
  - **Implementaciones de red remota**: la dirección IP de origen de la solicitud de DNS es la **EBGP Router Address (Dirección del enrutador EBGP)** para solicitudes internas y la Service IP Address (Dirección IP de servicio) de la conexión de red remota para solicitudes externas.

Las siguientes directrices y restricciones se aplican al uso de la resolución DNS con Prisma Access:

- El número máximo de solicitudes DNS TCP pendientes simultáneas [**Max Pending Requests (Número máximo de solicitudes pendientes)**] que Prisma Access admite es 64.
- Para las consultas UDP, el proxy DNS envía otra solicitud si no ha recibido una respuesta en 2 segundos y vuelve a intentarlo un máximo de 5 veces antes de probar con el siguiente servidor DNS.
- Prisma Access almacena en caché las entradas DNS con un valor de tiempo de vida (TTL) de 300 segundos. Las respuestas EDNS también se almacenan en caché.

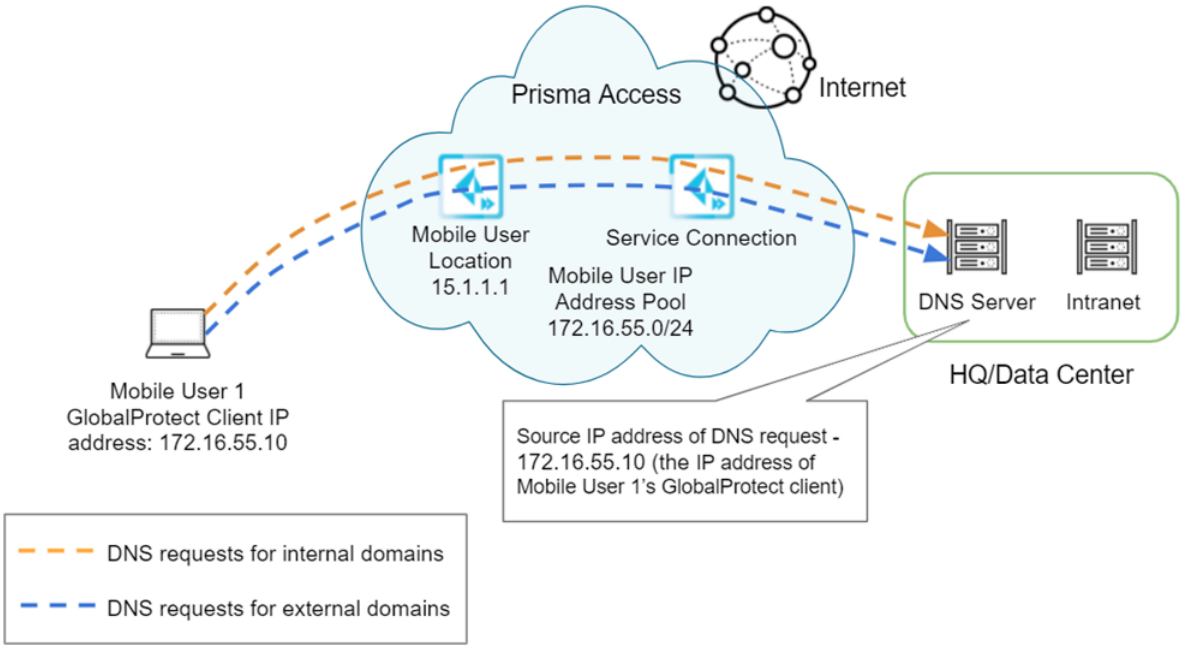
Resolución de DNS para implementaciones de Usuarios móviles: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

En la siguiente sección se proporcionan ejemplos de cómo Prisma Access procesa la dirección IP de origen de las solicitudes DNS después de configurar la resolución DNS para usuarios móviles y para redes remotas.

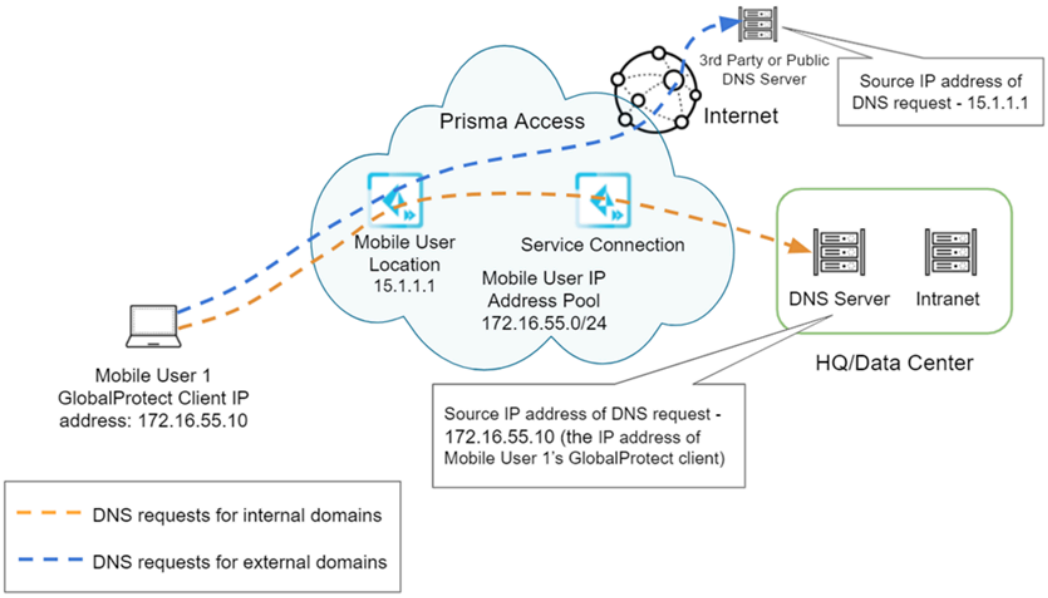
 ©2025 Palo Alto Networks, Inc.

En la siguiente figura se muestra una implementación en la que ha asignado un servidor DNS interno para resolver dominios internos y externos. En este caso, Prisma Access no utiliza el proxy para las solicitudes DNS, y la solicitud DNS proviene de la dirección IP del cliente GlobalProtect del usuario móvil 1. El cliente de GlobalProtect asigna esta dirección IP al usuario móvil y se toma de la dirección IP de la puerta de enlace de la ubicación del usuario móvil.

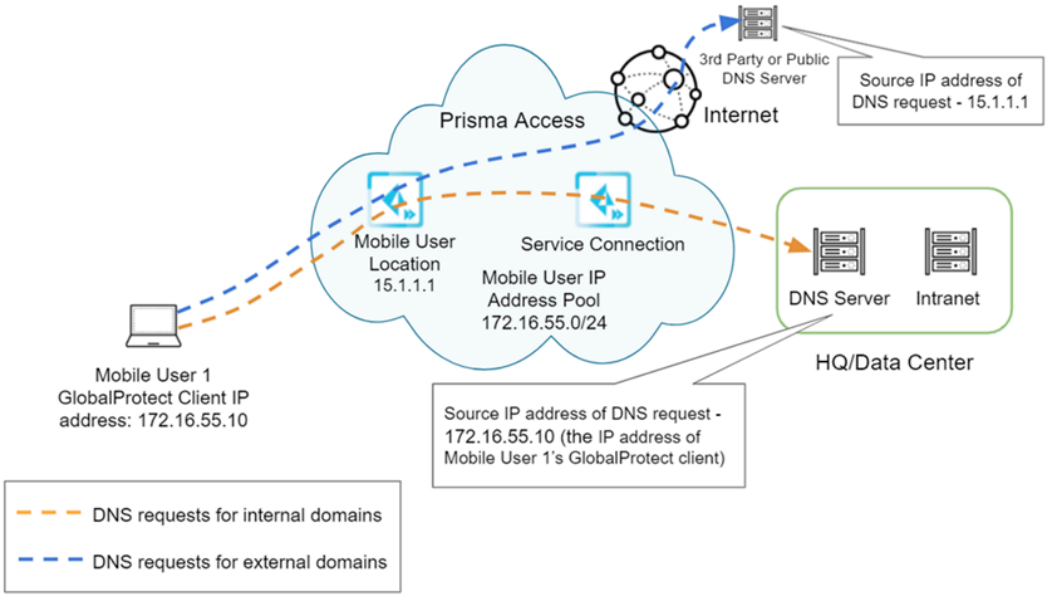


La siguiente figura muestra las solicitudes de DNS para dominios internos que resuelve el servidor DNS en la sede central o en la ubicación del centro de datos, mientras que las solicitudes de dominios externos las resuelve el servidor DNS predeterminado en la nube de Prisma Access. En este caso, Prisma Access utiliza un proxy para las solicitudes para la solicitud externa, y la dirección IP de origen es la dirección IP de la puerta de enlace de Prisma Access (15.1.1.1 en este ejemplo), mientras que la IP de origen interna permanece como la dirección IP del cliente GlobalProtect del usuario móvil 1.

 ©2025 Palo Alto Networks, Inc.



En la siguiente figura se muestra la organización que utiliza un servidor DNS público o de terceros al que se puede acceder a través de Internet para solicitudes a dominios externos. Prisma Access utiliza un proxy para estas solicitudes también.



Resolución DNS para redes remotas

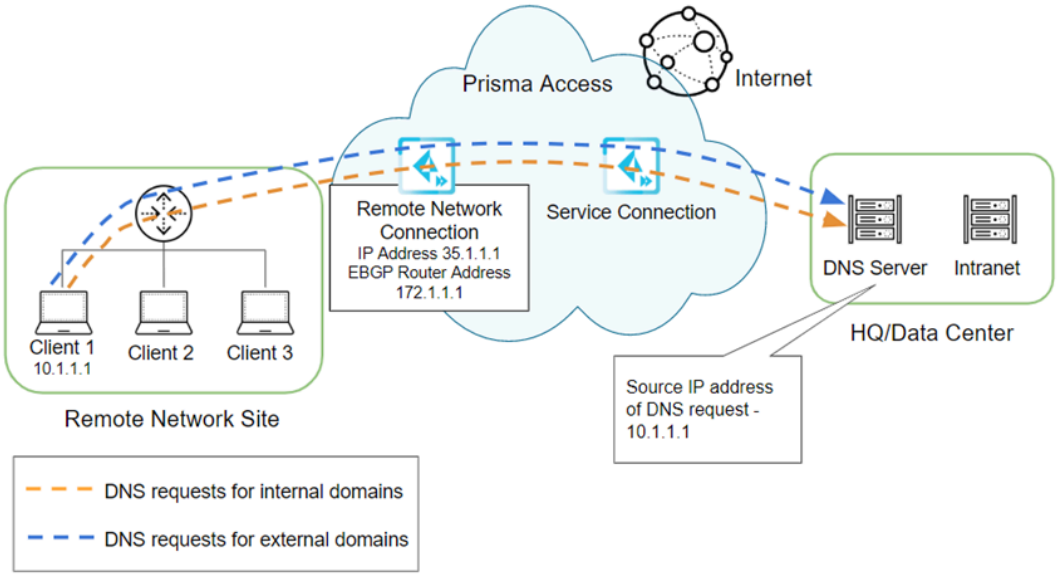
¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

Si tiene una implementación de red remota existente, puede seguir usando los métodos de resolución de DNS que ya tiene implementados o puede usar Prisma Access para realizar un proxy de la solicitud DNS. La solicitud de proxy de las solicitudes DNS le permite enviar solicitudes

 ©2025 Palo Alto Networks, Inc.

DNS para dominios públicos a un servidor y enviar solicitudes DNS para dominios internos a otro servidor.

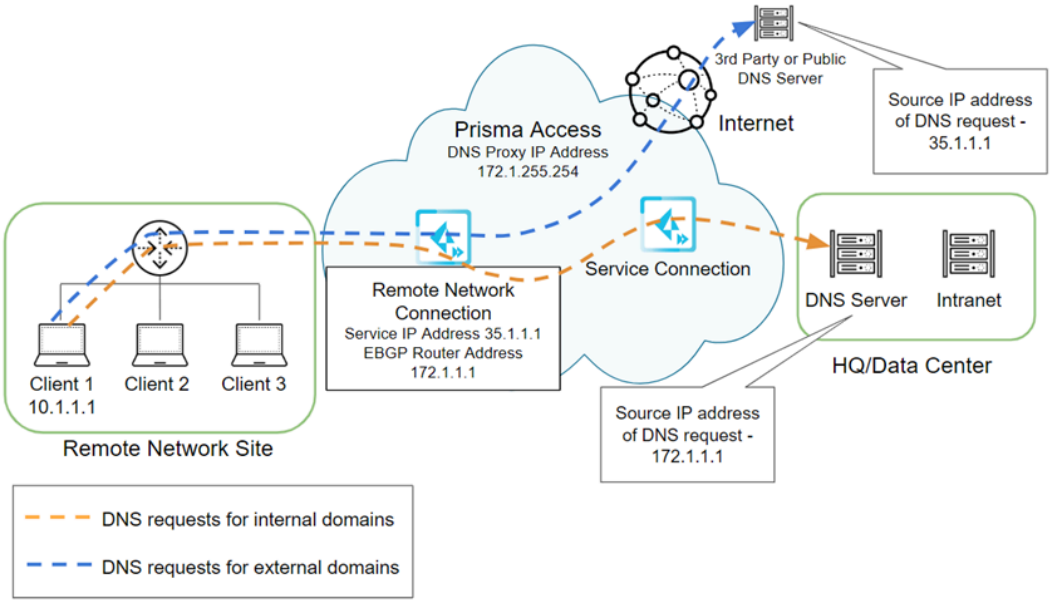
En la siguiente figura se muestra una solicitud DNS a una implementación en la que se usa un servidor DNS interno para procesar solicitudes de dominios internos y externos. La dirección IP de la red remota es 35.1.1.1 y la dirección IP del **EBGP Router (Enrutador EBGP)** es 172.1.1.1. En este caso, Prisma Access no utiliza el proxy para las solicitudes y, si el servidor DNS interno no usa NAT, la IP de origen de la solicitud DNS es 10.1.1.1 (la dirección IP del dispositivo del cliente 1 en el sitio de red remoto).



Si Prisma Access negocia la solicitud DNS, las direcciones IP de origen de las solicitudes DNS negociadas cambian a la **EBGP Router Address (Dirección del enrutador EBGP)** en el caso de las solicitudes internas y la Service IP Address (Dirección IP del servicio)de la conexión de red remota para solicitudes externas, como se muestra en la siguiente figura.

*Al configurar la dirección DNS de la red que se va a utilizar para las solicitudes externas negociadas de Prisma Access, especifique la **Remote Network DNS Proxy IP Address (Dirección IP de proxy DNS de red remota)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Service Infrastructure (Infraestructura de servicios)** > **Remote Network DNS Proxy IP Address (Dirección IP de proxy DNS de red remota)**]. En el siguiente ejemplo, especificaría 172.1.255.254 en la red para el servidor DNS.*

 ©2025 Palo Alto Networks, Inc.



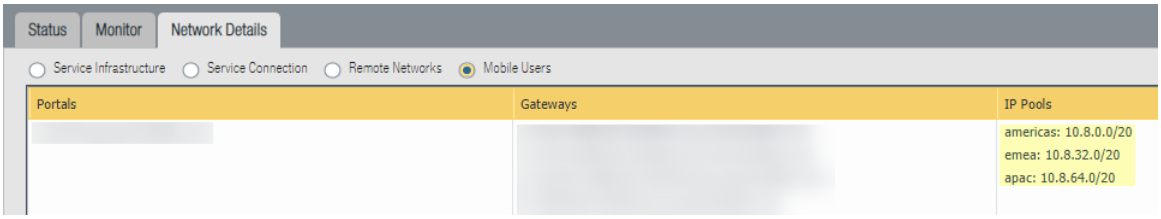
 ©2025 Palo Alto Networks, Inc.

Cómo BGP anuncia los grupos de direcciones IP de usuarios móviles para conexiones de servicio y conexiones de red remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

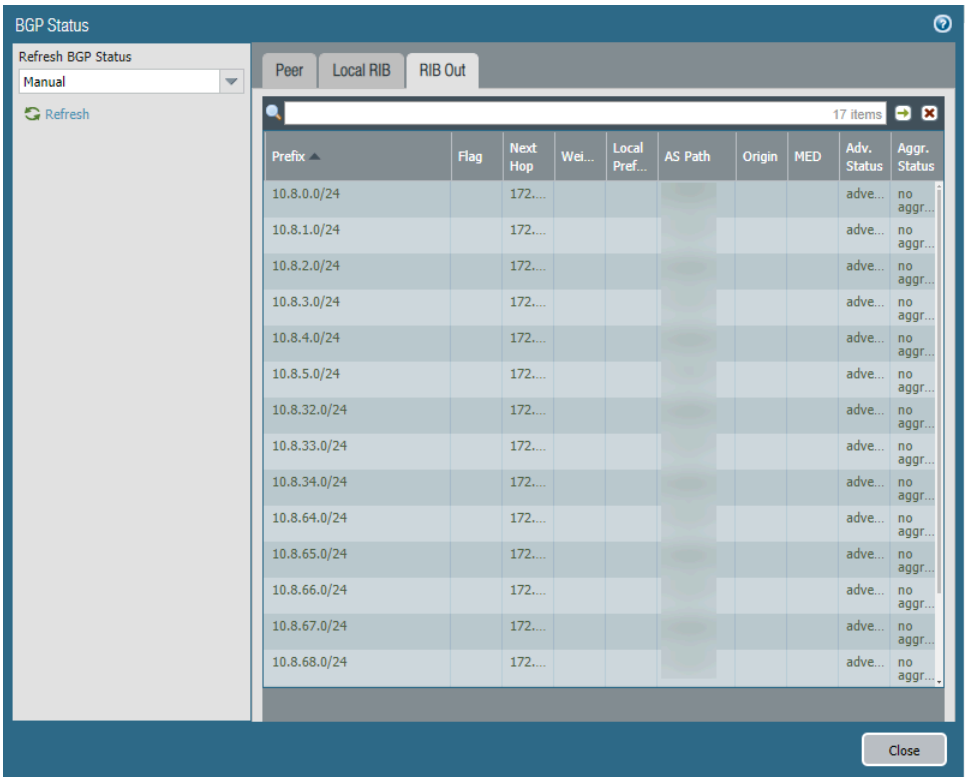
Si habilita BGP para conexiones de servicio o conexiones de red remotas, después de Configurar usuarios móviles de GlobalProtect (Panorama), Prisma Access asigna los grupos de direcciones IP de usuario móvil que especificó mediante bloques de direcciones de clase C (/24). Por lo tanto, BGP anuncia las subredes de usuarios móviles asignadas en bloques de /24, en lugar de en todo el grupo o grupos asociados con esa región. Cuando Prisma Access añade una subred /24 para una puerta de enlace de Prisma Access, este envía automáticamente un anuncio BGP. A medida que se añaden y quitan subredes, Prisma Access actualiza automáticamente sus anuncios BGP. Este método de asignación proporciona más flexibilidad a la hora de anunciar rutas BGP, especialmente si ha configurado un grupo **Worldwide (Mundial)** en lugar de asignar grupos por región. Dividir el grupo de direcciones IP en subredes más pequeñas permite añadir, eliminar o eliminar la misma subred y luego reutilizarla en diferentes regiones cuando se agote el espacio de direcciones asignado.

La siguiente captura de pantalla, de **Panorama** > **Cloud Services (Servicios en la nube)** > , **Status (Estado)** > **Network Details (Detalles de la red)** > **Mobile Users—GlobalProtect (Usuarios móviles: GlobalProtect)**, muestra tres grupos de IP /20 para usuarios móviles divididos por región.



La tabla **RIB Out (Salida de RIB)**, de **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicios)** > **Show BGP Status (Mostrar estado de BGP)** [en el área **Branch AS and Router (AS de sucursal y enrutador)**], muestra el grupo de direcciones de usuarios móviles dividido en bloques de /24 subredes para anuncios de rutas BGP. Tenga en cuenta que las subredes /20 completas no se anuncian.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Soporte de proxy para Prisma Access y Strata Logging Service

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

Si implementa un servidor proxy entre Panorama, la infraestructura de Prisma Access y Strata Logging Service, consulte la siguiente tabla para obtener detalles sobre el comportamiento esperado:

Funcionalidad	Soporte a través de un servidor proxy que no realiza el descifrado SSL	Soporte a través de un servidor proxy que realiza el descifrado SSL
Incorporación inicial a Strata Logging Service con comprobaciones del estado de revocación de certificados utilizando OCSP	Compatible	Solo se admiten proxies de paso; no se admite ningún proxy que utilice el descifrado SSL.
Panorama consulta a Strata Logging Service para obtener informes y logs	Si el servidor proxy es la ruta predeterminada en Panorama, no puede ver los datos en el ACC y las páginas **Monitor (Supervisar)** > **Logs**. Puede ver datos en las páginas de ACC y **Monitor (Supervisar)** > **Logs** si Panorama tiene una ruta alternativa a Strata Logging Service y puedes eludir el servidor proxy.	

 ©2025 Palo Alto Networks, Inc.

Bloquear conexiones entrantes de países específicos

Prisma Access permite crear reglas de políticas de seguridad para bloquear intentos de inicio de sesión para la Red Remota, Usuarios Móviles, GlobalProtect y Usuarios Móviles, implementaciones de Proxy Explícito de los países que especifique. Prisma Access bloquea las conexiones entrantes de los países que especifique en función de la información de geolocalización de la dirección IP de origen del cliente.

Para bloquear las conexiones entrantes de estos países, complete la siguiente tarea.

STEP 1 | Cree una regla previa de política de seguridad utilizando uno de los nombres de regla específicos:

Asegúrese de que configura esta regla como una regla previa.

- Para bloquear un país para usuarios móviles en implementaciones de GlobalProtect, cree una regla llamada **Mobile_User_EMBG_Source_Countries**.
- Para bloquear un país para usuarios móviles: implementaciones de proxy explícito, cree una regla llamada **Explicit_Proxy_EMBG_Source_Countries.**
- Para bloquear un país para implementaciones de red remota, cree una regla llamada **Remote_Network_EMBG_Source_Countries**.

STEP 2 | Añada una **Tag (Etiqueta)** para la regla llamada **PA_predefined_embargo_rule**.

STEP 3 | Añada uno o más países a bloquear en la **Source (Fuente)**.

STEP 4 | Especifique una **Action (Acción)** de **Drop (Descartar)**.

 ©2025 Palo Alto Networks, Inc.

Tráfico de Internet seguro de AWS WorkSpace

Las organizaciones deben replantearse su enfoque para proteger a sus trabajadores remotos, contratistas, personal de hospitales y usuarios de centros de llamadas que acceden a Internet a través de máquinas virtuales basadas en la nube de Amazon WorkSpace. Estos usuarios deben poder acceder a Internet de forma segura y permanecer protegidos de las amenazas basadas en Internet, mientras que la organización mantiene una visibilidad completa del tráfico de Internet generado a través de estas máquinas virtuales alojadas en la nube.

Los modelos de red tradicionales diseñados para trabajadores y recursos remotos ya no son suficientes en la compleja e innovadora economía actual, donde la fuerza laboral, los datos y las aplicaciones en la nube están cada vez más distribuidos. Las organizaciones necesitan la flexibilidad y la escalabilidad de los servicios en la nube, pero estos servicios requieren soluciones de seguridad en la nube que estén diseñadas para satisfacer sus necesidades únicas.

Obtenga más información sobre Prisma SASE y AWS WorkSpace.

Con el uso de Palo Alto Networks Strata Cloud Manager puede proporcionar acceso seguro a Internet para AWS WorkSpace usando los siguientes métodos:

- Configurar un archivo PAC en los clientes de AWS WorkSpace
- Configurar un túnel de sitio a sitio entre AWS y Prisma Access

Configurar un archivo PAC en los clientes de AWS WorkSpace

Un método para proteger el tráfico de Internet de Amazon WorkSpaces es mediante el uso de un archivo de configuración automática de proxy (PAC). Un archivo PAC es un código JavaScript que le dice a un navegador web cómo conectarse a un servidor proxy. Los entornos empresariales emplean archivos PAC para controlar el tráfico web y aplicar reglas de políticas de seguridad. Un servidor web normalmente almacena el archivo PAC y el navegador web descarga el archivo PAC cuando se inicia.

STEP 1 | Si aún no lo ha hecho, configure el Proxy explícito de Prisma SASE.

Puede alojar un archivo PAC en Prisma SASE o en el servidor web. Verifique que el servidor PAC sea accesible desde los clientes de WorkSpace accediendo a la URL del PAC mediante un navegador web.

STEP 2 | Personalice el archivo PAC del proxy explícito de Prisma SASE para actualizar el FQDN del proxy y definir exclusiones.

1. Desde Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Explicit Proxy (Proxy explícito)** > **Forwarding Rules (Reglas de reenvío)**.
2. Edite el archivo PAC de acuerdo con las directrices del archivo PAC.

STEP 3 | Descargue los certificados raíz de proxy explícito de Prisma SASE para instalarlos en AWS WorkSpace.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Instale el certificado en el cliente de AWS WorkSpace para aplicar reglas de políticas basadas en el usuario, inspección de tráfico y generación de informes.

Esto permitirá que el cliente de WorkSpace se comunique con el proxy explícito de Prisma SASE.

STEP 5 | Configure el archivo PAC en AWS WorkSpace.

La forma de hacer esto depende del navegador que utilice.

- Google Chrome:
  1. Abra Chrome.
  2. Seleccione los tres puntos en la esquina superior derecha de la ventana.
  3. Seleccione **Settings (Configuración)**.
  4. Seleccione **Advanced (Avanzado)**.
  5. En **System (Sistema)**, seleccione **Open proxy settings (Abrir configuración de proxy)**.
  6. En la ventana Configuración de red de área local (LAN), seleccione **Use automatic configuration script (Usar script de configuración automática)**.
  7. En el campo **Address (Dirección)**, introduzca la URL de su archivo PAC.
  8. Seleccione **OK (Aceptar)** para guardar los cambios.
- Firefox
  1. Abra Firefox.
  2. Seleccione las tres líneas en la esquina superior derecha de la ventana.
  3. Seleccione **Options (Opciones)**.
  4. Seleccione **Advanced (Avanzado)**.
  5. En **Network (Red)**, seleccione **Settings (Configuración)**.
  6. En la ventana **Connection Settings (Configuración de conexión)**, seleccione **Automatic proxy configuration URL (URL de configuración de proxy automática)**.
  7. En el campo **URL**, introduzca la URL de su archivo PAC.
  8. Seleccione **OK (Aceptar)** para guardar los cambios.

Cuando haya aplicado el archivo PAC, Chrome y Firefox lo utilizarán para determinar qué servidor proxy utilizar para cada sitio web.

STEP 6 | Reiniciar el navegador de AWS WorkSpace.

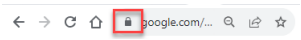
Después de reiniciar el navegador WorkSpace, este recogerá el nuevo archivo PAC y comenzará a enrutar el tráfico a través del proxy de Prisma SASE.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Probar y verificar el flujo de tráfico.

Una vez que haya configurado los clientes de WorkSpace para usar el proxy explícito SASE de Prisma, puede probar el flujo de tráfico validando el certificado en el navegador y viendo los logs en Prisma Access.

1. Si utiliza Google Chrome, seleccione el candado en la barra de direcciones.



   1. Seleccione la **Connection is secure (Conexión es segura)**.
   2. Seleccione **Certificate is valid (Certificado es válido)**.
   3. Verifique los detalles correctos del certificado que aparecen en la ventana emergente.
2. Si usa Safari, seleccione el icono del candado en la barra de direcciones.
   1. Seleccione **Connection secure (Conexión segura)**.
   2. Seleccione **More information (Más información)**.
   3. Seleccione **View Certificate (Ver certificado)**.
   4. Verifique los detalles correctos del certificado que aparecen en la ventana emergente.

Configurar un túnel de sitio a sitio entre AWS y Prisma Access

A medida que su negocio crece y tiene varios clientes de AWS WorkSpace en ejecución, Las redes remotas de Prisma Access le permiten incorporar rápidamente su WorkSpace y ofrecer la mejor seguridad para sus usuarios. Ofrece una opción conveniente que simplifica la configuración y gestión de WorkSpace.

Las organizaciones pueden incorporar usuarios de AWS WorkSpace a Prisma Access mediante el establecimiento de un túnel IPSec entre AWS y Prisma Access.

La ventaja de utilizar una red remota es que protege el tráfico saliente de internet para los usuarios que se conectan a través de Prisma Access para acceder a internet.

STEP 1 | Configure una nube privada virtual (VPC) para su Amazon WorkSpace o utilice la VPC existente para su Amazon WorkSpace.

STEP 2 | Adjunte AWS Transit Gateway a la VPC para configurar el túnel IPSec de sitio a sitio entre AWS y Prisma Access.

STEP 3 | Configure la VPN de IPSec entre AWS Transit Gateway y la Red remota de Prisma Access.

STEP 4 | En la red remota de Prisma Access, puede definir reglas de seguridad para restringir el tráfico de Internet y proteger a los usuarios de AWS WorkSpace.

 ©2025 Palo Alto Networks, Inc.

Prisma Access para redes sin ruta predeterminada

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access	❑ Licencia de Prisma Access

¿Qué es una red sin ruta predeterminada?

Una red sin ruta predeterminada es una red que no tiene una ruta predeterminada configurada. Cuando una red no tiene una ruta predeterminada configurada, descarta paquetes destinados a destinos desconocidos. Las empresas a menudo no utilizan redes de rutas predeterminadas para restringir el acceso a sus usuarios. Si un dispositivo en una red sin ruta predeterminada necesita acceder a un destino determinado (dirección IP o subred), el administrador deberá configurar manualmente una ruta para ese destino. Las empresas también requieren acceso a Internet restringido y seguro para los usuarios, servidores y dispositivos en una red sin ruta predeterminada.

Hay algunas razones por las que alguien podría querer configurar una red sin ruta predeterminada:

- Mejorar la seguridad bloqueando el tráfico malicioso saliente y el tráfico DDoS a destinos aleatorios desde endpoints comprometidos en la red, lo que protege contra ataques de denegación de servicio y otro tráfico malicioso.
- Mejorar el rendimiento de los dispositivos de enrutamiento al reducir la cantidad de rutas a procesar.
- Implementar políticas de enrutamiento que satisfagan las necesidades específicas de los usuarios configurando rutas específicas para destinos específicos.

Consideraciones sobre la red sin ruta predeterminada

Al proteger el tráfico de Internet desde una red sin una red predeterminada, las empresas deben evaluar claramente los usuarios, los endpoints, los servidores y los dispositivos de la red de la sucursal que podrían estar comunicándose con Internet.

En las sucursales sin ruta predeterminada, podría haber dispositivos con una variedad de sistemas operativos diferentes, endpoints multiusuario o compartidos como VDI y dispositivos sin cabeza como servidores y dispositivos IoT. El tráfico de Internet de todos estos dispositivos requiere seguridad. Es fundamental contar con una solución que cubra todos estos casos de uso, proporcione flexibilidad con diferentes métodos de conectividad y ofrezca una plataforma unificada para proteger constantemente el acceso a Internet independientemente del tipo de dispositivo.

Recomendaciones de implementación para proteger el acceso a Internet en redes sin ruta predeterminada

Si no tiene una red con ruta predeterminada, aquí le ofrecemos nuestra recomendación para proteger el tráfico de Internet:

 ©2025 Palo Alto Networks, Inc.

Dispositivos	Recomendación
Windows, macOS	Agente GlobalProtect en modo Proxy
ChromeOS, VDI	Archivos PAC sin agente
iOS, Android	Archivos PAC sin agente
Linux	Archivos PAC sin agente
los servidores	Archivos PAC sin agente
Dispositivos IoT (compatibles con proxy)	Archivos PAC sin agente
Dispositivos IoT (sin proxy)	Redes remotas (IPSec)

Consideraciones clave

Al implementar GlobalProtect en una red sin ruta predeterminada, tenga en cuenta estos puntos:

- Añada una ruta en el dispositivo perimetral para enrutar el tráfico de Internet del usuario a Prisma Access Dirección IP de Proxy explícito.
- Aloje el archivo PAC internamente para reenviar la URL del IdP y la URL del portal de Prisma Access al proxy explícito para permitir que GlobalProtect se conecte al Portal y al IdP.
- Añada registros DNS internos para resolver el proxy explícito, el archivo PAC y el FQDN del portal de Prisma Access si el servidor DNS en la red sin ruta predeterminada no puede resolver FQDN externos.
- Configurar DNAT para la dirección IP interna de Prisma Access Proxy explícito y la dirección IP del portal de Prisma Access a la dirección IP de Proxy explícito real y dirección IP del portal.

Para las implementaciones basadas en PAC, no es necesario reenviar la URL del portal de Prisma Access a un proxy explícito y excluirlo de la configuración de autenticación en la configuración de proxy explícita de Prisma Access.

©2025 Palo Alto Networks, Inc.

Prisma Access implementaciones avanzadas de conexión de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

Las siguientes secciones le muestran las implementaciones avanzadas disponibles para las conexiones de servicio de Prisma Access:

- Redundancia multicloud de conexión de servicio
- Uso de la dirección de tráfico para reenviar el tráfico enlazado a Internet a las conexiones de servicio
- Enrutamiento para el tráfico de conexión de servicio
- Cree una red de gran ancho de banda utilizando múltiples conexiones de servicio

Redundancia multicloud de conexión de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

La redundancia multinube de conexiones de servicio es compatible a partir de Prisma Access 3.1. Innovation

Si utiliza Conexiones de servicio de Prisma Access para proporcionar a los usuarios móviles y a los usuarios en sitios remotos acceso a recursos internos y aplicaciones en una sede o centro de datos, puede garantizar un acceso más resistente a esos recursos creando conexiones de servicio activas y de respaldo en diferentes proveedores de nube. Puede especificar estas conexiones de servicio activas y de respaldo en la misma ubicación o en ubicaciones diferentes en regiones geográficas diferentes, lo que le permite acceder a los recursos a través de conexiones de servicio incluso cuando un proveedor o región de la nube no está disponible.

Especifica conexiones de servicio activas y de respaldo en un *sitio*. Un sitio es un centro de datos de clientes o una sede central (local o en la nube pública) donde terminan una o más conexiones de servicio. Después de crear conexiones de servicio, cree un sitio, añada conexiones de servicio a ese sitio y, a continuación, especifique las conexiones de servicio que añadió como activas o de copia de seguridad.

Si un proveedor de nube o un corte de luz regional provoca que se caiga una conexión de servicio activa en un sitio, Prisma Access redirige el tráfico mediante estas reglas, que permiten a los usuarios móviles continuar accediendo a los recursos de esa sede o centro de datos:

- Si hay una sola conexión de servicio activa en un sitio, Prisma Access selecciona la conexión de servicio de respaldo en ese sitio para enrutar el tráfico.

 ©2025 Palo Alto Networks, Inc.

- Si hay varias conexiones de servicio activas en un sitio, Prisma Access selecciona otra de las conexiones de servicio activas para enrutar el tráfico, y la conexión de servicio de respaldo solo se utiliza para enrutar el tráfico cuando se interrumpen todas las conexiones de servicio activas.

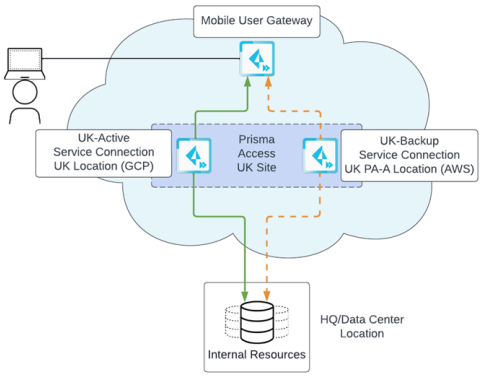
Para utilizar un sitio que utiliza ubicaciones activas y de copia de seguridad en el mismo país, incorpore conexiones de servicio utilizando ubicaciones preferidas y alternativas en el país, luego cree un sitio y añada esas ubicaciones en el país al sitio.

Prisma Access también le proporciona mensajes de estado sobre las conexiones de servicio que ha incorporado en un sitio (por ejemplo, si todas las conexiones de servicio en un sitio se implementan en una sola región).

Los siguientes ejemplos muestran cómo puede aprovechar la creación de sitios y añadir conexiones de servicio a los mismos:

- **Diferentes proveedores de nube en la misma región geográfica**: si es una organización (como un banco) que requiere que se acceda a sus datos en un país específico, puede seleccionar una ubicación preferida de ese país y una ubicación alternativa de ese mismo país. El siguiente ejemplo muestra una organización en el Reino Unido que incorpora sus conexiones de servicio en el Reino Unido para seguir las regulaciones de ubicación de datos. En este caso, el administrador de la organización incorpora dos conexiones de servicio en el Reino Unido, ubicación UK-Active en el Reino Unido y ubicación PA-a UK-Backup en el Reino Unido. La ubicación del Reino Unido está alojada en el proveedor de nube preferido (GCP) en el Reino Unido, y la ubicación PA-A del Reino Unido está alojada en el proveedor de nube alternativo (AWS) en ese país. La lista de ubicaciones en el país muestra el proveedor de nube preferido y alternativo para un país. A continuación, el administrador crea un sitio y designa UK-Active como la ubicación activa y UK-Backup como la ubicación de respaldo en ese sitio.

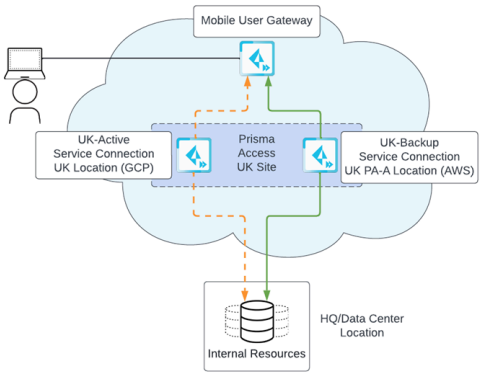
  Durante la operación normal, los usuarios móviles acceden a los recursos internos en la sede o centro de datos utilizando la conexión de servicio UK-Active.



  Si una interrupción de GCP afecta a la conexión de servicio UK-Active, Prisma Access falla a la conexión de servicio UK-Backup, que está alojada en AWS. De esta manera, Prisma Access permite a los usuarios móviles acceder a los recursos en el centro de datos o la sede, incluso en

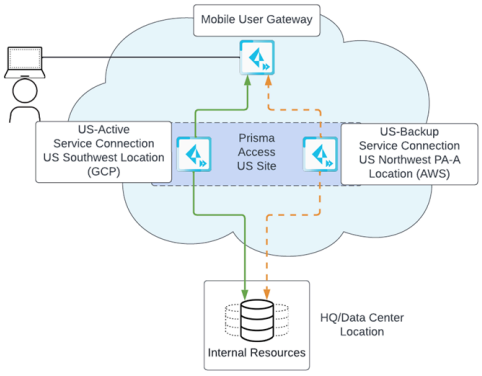
 ©2025 Palo Alto Networks, Inc.

caso de una interrupción del proveedor de servicios en la nube. El siguiente diagrama muestra el flujo de tráfico.



- **Diferentes regiones geográficas**: si desea garantizar la redundancia en caso de una interrupción regional, puede especificar dos o más conexiones de servicio en diferentes ubicaciones de cómputo, así como diferentes proveedores de nube, que le proporcionan acceso de copia de seguridad en caso de una interrupción en una región geográfica. En el siguiente diagrama, el administrador ha incorporado conexiones de servicio desde ubicaciones en los Estados Unidos (US-Active en la ubicación EE. UU. Suroeste y US-Backup en la ubicación EE. UU. Noroeste PA-A) y ha creado un sitio que convierte a US-Active en la conexión de servicio activa en el sitio y US-Backup en el respaldo.

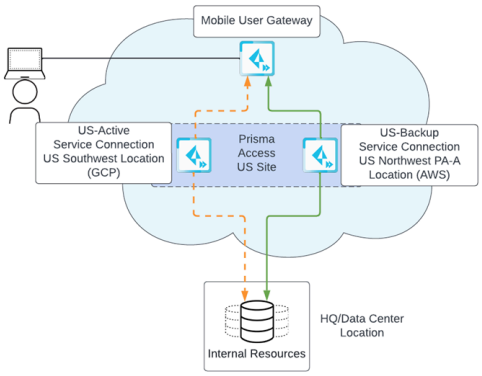
  Dado que tiene conexiones de servicio incorporadas que se encuentran en diferentes ubicaciones de cómputo, así como en diferentes proveedores de nube, ha configurado un sitio que le proporciona redundancia geográfica y de proveedores de nube.



  Si la ubicación de US-Active se cae (ya sea debido a un proveedor de nube o a un corte regional), la conexión de servicio falla a la ubicación de US-Backup, que utiliza un proveedor de

 ©2025 Palo Alto Networks, Inc.

nube y una ubicación de cómputo diferentes de la conexión de servicio de US-Active, como se muestra en el siguiente diagrama.

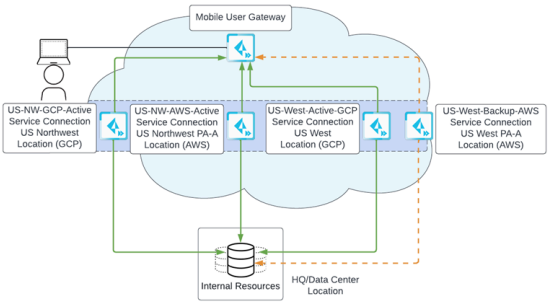


- **Conexión de alto ancho de banda con varias conexiones de servicio**: si necesita una conexión de mayor ancho de banda con sus recursos internos, puede crear un sitio con varias conexiones activas. El siguiente diagrama muestra cuatro sitios incorporados, con una mezcla de proveedores de nube GCP y AWS:
  - US-NW-GCP-Active, utilizando la ubicación EE. UU. Noroeste (GCP)
  - US-NW-AWS-Active, utilizando la ubicación EE. UU. Noroeste PA-A (AWS)
  - US-West-Active-GCP, utilizando la ubicación EE. UU. Oeste (GCP)
  - US-West-Backup-AWS, utilizando la ubicación EE. UU. Oeste PA-A (AWS)

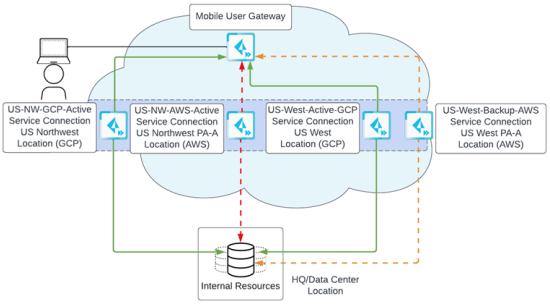
  En el sitio, tres de las conexiones de servicio se designan como conexiones de servicio activas, y una cuarta conexión de servicio se designa como respaldo. Designar tres conexiones de

 ©2025 Palo Alto Networks, Inc.

servicio como activas de manera efectiva le da el triple de ancho de banda a sus recursos internos en comparación con una sola conexión de servicio.

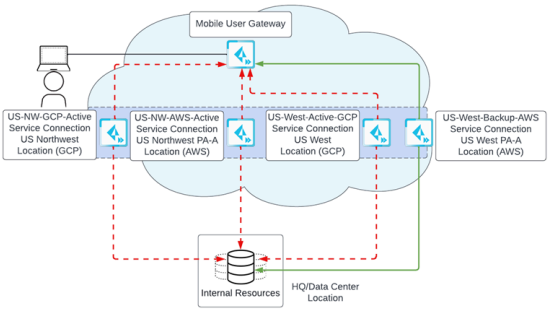


Si una de las conexiones de servicio activas se cae, la conexión de respaldo no se pone en uso; en su lugar, Prisma Access desvía el tráfico a las conexiones de servicio activas restantes que están en funcionamiento, como se muestra en el siguiente diagrama.



Si todas las conexiones de servicio activas se caen, entonces la conexión de servicio de respaldo se pone en uso y se hace la conexión activa.

Si configura varias conexiones de servicio como conexiones de servicio de respaldo, Prisma Access pone en uso todas las conexiones de servicio de respaldo y comparte la carga del tráfico de conexión de servicio.



Utilice las siguientes directrices al configurar conexiones de servicio de proveedor de nube redundantes:

 ©2025 Palo Alto Networks, Inc.

- Puede añadir conexiones de servicio utilizando ubicaciones preferidas o alternativas en un sitio.

  Palo Alto Networks recomienda encarecidamente que utilice el proveedor de nube preferido como conexión de servicio activa en un sitio.
- Todas las conexiones de servicio en un sitio deben apuntar al mismo recurso en la misma sede o ubicación del centro de datos. No puede tener conexiones de servicio en un sitio que apunten a diferentes recursos en diferentes ubicaciones.
- Debe seleccionar al menos una conexión de servicio activa en un sitio; sin embargo, también puede tener varias conexiones de servicio activas en un único sitio. La siguiente configuración del sitio es válida:
  - EE. UU. Central (activo)
  - EE. UU. Central PA-A (de respaldo)
  - EE. UU. Este (activo)
  - EE. UU. ESTE PA-A (de respaldo)
- Si tiene varias conexiones de servicio activas en un sitio y una conexión de servicio activa se cae, el tráfico se desviará a la otra conexión de servicio activa (es decir, la conexión de servicio de respaldo no se utiliza mientras una de las conexiones de servicio activa esté en funcionamiento).
- Utilice las siguientes directrices para el enrutamiento de conexiones de servicio estático y dinámico:
  - Si utiliza enrutamiento estático para conexiones de servicio, asegúrese de que las subredes que especifique para las conexiones de servicio apunten a las mismas subredes.

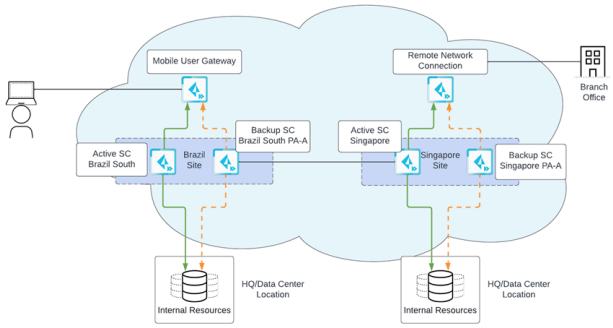
    Por ejemplo, si tiene un sitio que utiliza 192.168.41.0/24, 192.168.44.0/24 y 192.168.47.0/24 como subredes para las conexiones de servicio activas, asegúrese de especificar las mismas subredes para las conexiones de servicio de respaldo.
  - Si utiliza el enrutamiento dinámico (BGP) para las conexiones de servicio, asegúrese de que todas las conexiones de servicio anuncian los mismos prefijos al mismo centro de datos o sede.
- Prisma Access utiliza los valores de BGP Multi Exit Discriminator (MED) para distinguir entre conexiones de servicio activas y de respaldo en un sitio como se muestra en la siguiente tabla. Tenga en cuenta que los valores MED para las conexiones de servicio activas cambian dependiendo de si ha habilitado o no un túnel IPSec secundario para la conexión de servicio activa. Prisma Access anuncia estos valores MED al CPE (par BGP).

Tipo de conexión	Valor MED
Conexiones de servicio IPSec activas en un sitio	
Conexión de servicio activa, sin túnel IPSec secundario configurado	0
Conexión de servicio activa, túnel IPSec secundario configurado, túnel primario	100

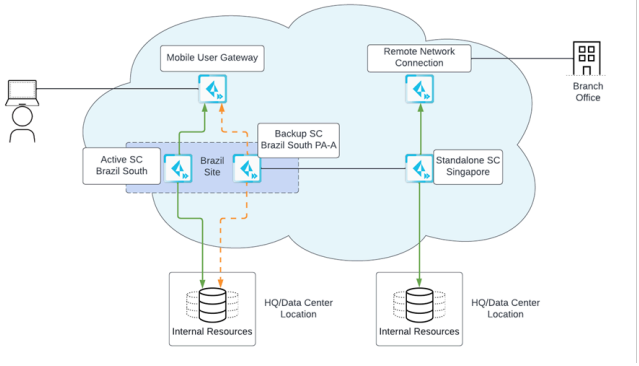
 ©2025 Palo Alto Networks, Inc.

Tipo de conexión	Valor MED
Conexión de servicio activa, túnel IPSec secundario configurado, túnel secundario	200
Conexiones de servicio IPSec de respaldo en un sitio	
Conexión de servicio de respaldo, túnel primario (independientemente de si está configurado o no un túnel IPSec secundario)	500
Conexión de servicio de respaldo, túnel IPSec secundario configurado, túnel secundario	600

- Puede añadir varios sitios en una sola implementación de Prisma Access, como se muestra en el siguiente diagrama.



- Todavía puede utilizar una única conexión de servicio independiente para acceder a los recursos internos. También puede mezclar conexiones de servicio independientes con conexiones de servicio activas y de respaldo, como se muestra en el siguiente diagrama.



- No se admite la redundancia multinube de conexiones de servicio cuando se utiliza el enrutamiento Hot Potato para conexiones de servicio.
- No utilice la CLI para incorporar y configurar conexiones de servicio. Si necesita el uso de la CLI para integrar conexiones de servicio, póngase en contacto con su equipo de Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

Configurar y activar la redundancia del proveedor de la nube de conexión de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para configurar múltiples conexiones de servicio para proveedores de nube, complete los siguientes pasos.

STEP 1 | (Solo implementaciones de Prisma Access existentes) Si ha actualizado su complemento a una versión que admite la redundancia del proveedor de nube, realice una operación de **Commit and Push (Confirmar y enviar)** después de actualizar al complemento compatible.

La redundancia de varias nubes para la conexión de servicio es compatible a partir de Prisma Access 3.1 Preferred and Innovation. Después de actualizar el complemento Cloud Services, debe realizar una acción de **Commit and Push (Confirmar y enviar)** para que los cambios de redundancia en la nube aparezcan en la interfaz de usuario.

Si tiene una nueva implementación (no una actualización), omita este paso.

 ©2025 Palo Alto Networks, Inc.

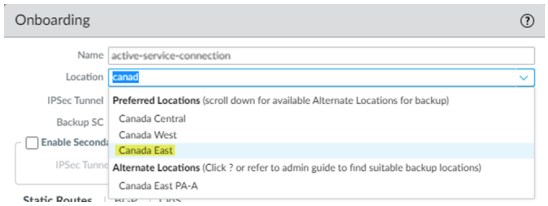
STEP 2 | Cree las conexiones de servicio que se utilizarán como conexiones de servicio activas y de respaldo en un sitio.

Después de crear ubicaciones preferidas y alternativas, y confirmar y enviar sus cambios, no podrá cambiar estas ubicaciones. Por ejemplo, no puede cambiar la ubicación preferida de Canadá Este a Canadá Este PA-A y no puede cambiar la ubicación alternativa de Canadá Este PA-A a Canadá Este.

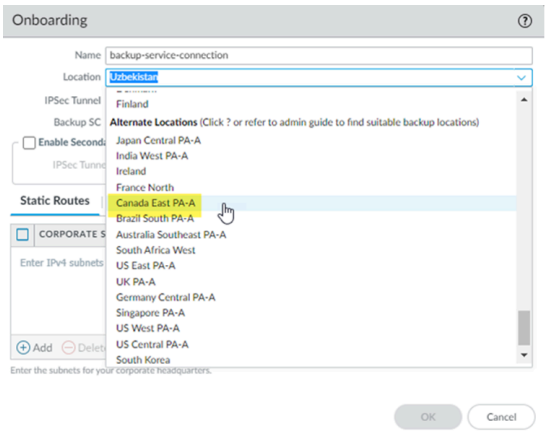
1. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)**.
2. **Add (Añadir)** una conexión de servicio que designará como conexión de servicio activa en un sitio.

   Seleccione de la lista de ubicaciones preferidas o alternativas.

   *Para buscar una ubicación, comience a escribir el nombre de la **Location (Ubicación)**.*



3. **Add (Añadir)** una conexión de servicio que designará como conexión de servicio de respaldo en un sitio.



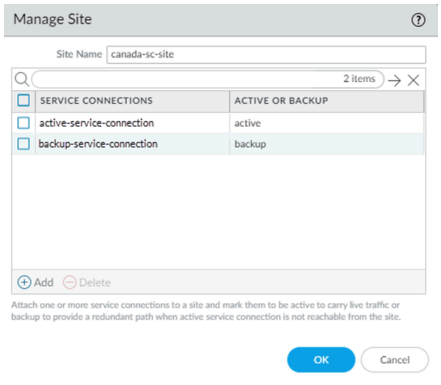
4. (Opcional) Continúe incorporando conexiones de servicio que se designarán como sitios activos y de respaldo, según sea necesario.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cree un sitio; luego, designe las conexiones de servicio que añadió como conexiones de servicio activas o de respaldo en el sitio.

1. En **Manage Sites (Gestionar sitios)**, seleccione **Add (Añadir)** un nuevo sitio.
2. **Add (Añadir)** las conexiones de servicio que incorporó.
3. Designe las ubicaciones de servicio que añadió como **active (activas)** y **backup (de respaldo)** en el sitio.

   Puede crear varios sitios activos y de copia de seguridad. Especifique al menos un sitio para que sea un sitio activo.
4. Haga clic en **OK (Aceptar)**.
5. (Opcional) Continúe añadiendo sitios para sus conexiones de servicio activas y de respaldo, según sea necesario.



STEP 4 | Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

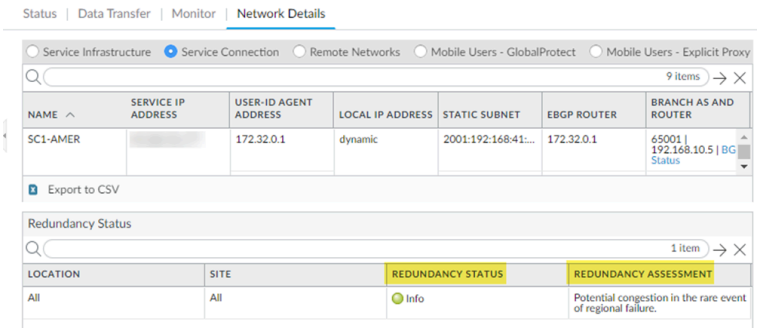
STEP 5 | Compruebe el estado de sus sitios.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **Redundancy Status (Estado de redundancia)**.
2. Verifique la información en los campos **Redundancy Status (Estado de redundancia)** y **Redundancy Assessment (Evaluación de redundancia)**. El estado de redundancia le proporciona el estado de los sitios que implementa y la evaluación de redundancia le proporciona más detalles sobre las conexiones de servicio implementadas en el sitio.

Estado de redundancia	Evaluación de redundancia
info	Es posible que sus conexiones de servicio experimenten congestión en caso de un fallo regional.
Warning (Advertencia)	Todas las conexiones de servicio se implementan en una sola región. Considere implementarlo en ubicaciones cercanas. Este mensaje le informa que todas sus conexiones de servicio están implementadas en una única región.

 ©2025 Palo Alto Networks, Inc.

Estado de redundancia	Evaluación de redundancia
Precaución	Todas las conexiones de servicio que se conectan al sitio se implementan en una sola región. Considere implementarlo en ubicaciones cercanas. Este mensaje le informa que todas las conexiones de servicio que se conectan a un sitio están implementadas en una sola región.



Ubicaciones compatibles de redundancia de proveedores de nube activas y de respaldo en el país

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

Si desea configurar una implementación donde las ubicaciones activa y de respaldo estén en el mismo país, seleccione de esta lista de ubicaciones Preferred y Alternate dentro del país.

Ubicaciones preferidas	Ubicaciones alternativas
Sureste de Australia	Australia Sureste PA-A
Bahréin PA-A	Baréin
Brasil Sur	Brasil Sur PA-A
Canadá Este	Canadá Este PA-A
Francia Norte PA-A	Francia Norte
Alemania Central	Alemania Central PA-A
India Oeste	India Oeste PA-A
Irlanda PA-A	Irlanda

©2025 Palo Alto Networks, Inc.

Ubicaciones preferidas	Ubicaciones alternativas
Japón Central	Japón Central PA-A
Singapur	Singapur PA-A
Sudáfrica Oeste PA-A	Sudáfrica Oeste
Corea del Sur PA-A	Corea del Sur
RU	Reino Unido PA-A
Emiratos Árabes Unidos PA-A	Emiratos Árabes Unidos
EE. UU. Central	EE. UU. Central PA-A
EE. UU. Este	EE. UU. Este PA-A
EE. UU. Noroeste	EE. UU. Noroeste PA-A
EE. UU. Oeste	EE. UU. Oeste PA-A

Uso de la dirección de tráfico para reenviar el tráfico enlazado a Internet a las conexiones de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ La capacidad de enviar la lista de revocación de certificados (CRL) y el Protocolo de Estado de Certificados en Línea (OCSP) directamente a Internet requiere una versión de Prisma Access 5.1.1 como mínimo.

Prisma Access permite crear reglas de direccionamiento de tráfico para especificar objetivos para el tráfico vinculado a Internet de usuarios móviles y conexiones de red remotas. Puede especificar el tráfico que se redirigirá a una conexión de servicio antes de enviarlo a Internet, o puede especificar el tráfico que saldrá directamente a Internet. Esta funcionalidad se conoce como *Dirección de tráfico*.

Como alternativa, puede configurar Prisma Access para aceptar un ruta predeterminada desde su CPE hasta Prisma Access para que Prisma Access reenvíe el tráfico de usuarios móviles enlazado a Internet a la mejor conexión de servicio de la implementación.

 ©2025 Palo Alto Networks, Inc.

Rutas predeterminadas con dirección del tráfico de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Utilice la capacidad de ruta predeterminada en Prisma Access para aceptar las rutas predeterminadas que se anuncian desde su CPE a las conexiones de servicio. Puede utilizar BGP o rutas estáticas para anunciar la ruta predeterminada. Prisma Access utiliza BGP para anunciar estas rutas a través de múltiples conexiones de servicio, lo que permite a Prisma Access enrutar el tráfico de usuarios móviles a través de la mejor conexión de servicio para una ubicación determinada del usuario móvil. Para permitir que las conexiones de servicio acepten rutas predeterminadas, especifique **Accept Default Route over Service Connections (Aceptar ruta predeterminada a través de conexiones de servicio)** cuando Configurar la dirección del tráfico en Prisma Access.

Después de habilitar las rutas predeterminadas, el tráfico con destino a Internet se dirigirá a las conexiones de servicio en lugar de salir de las ubicaciones de los usuarios móviles. Esta funcionalidad puede ser útil si desea redirigir el tráfico de Internet al centro de datos; por ejemplo, si tiene una pila de seguridad de terceros en su centro de datos y desea que la pila realice una inspección o detección adicional.

Utilice las siguientes pautas al implementar rutas predeterminadas:

- Las rutas predeterminadas se aplican únicamente a las implementaciones de usuarios móviles; las conexiones de red remotas funcionan normalmente sin cambios cuando habilita las rutas predeterminadas.
- No es necesario especificar conexiones de servicio de destino ni reglas de dirección de tráfico cuando se permiten rutas predeterminadas, aunque se admiten para su uso con rutas predeterminadas.
- Cuando especifica la configuración **Accept Default Route over Service Connections (Aceptar ruta predeterminada sobre conexiones de servicio)**, todas las conexiones de servicio de Prisma Access, con excepción de las conexiones de servicio dedicadas, aceptan rutas predeterminadas y utilizarán las rutas en las decisiones de dirección del tráfico.
- Antes de habilitar esta configuración, asegúrese de que sus centros de datos estén enviando rutas predeterminadas; de lo contrario, el enrutamiento a través de conexiones de servicio fallará.
- Palo Alto Networks recomienda que todos los centros de datos anuncien una ruta predeterminada; cuando Prisma Access recibe las rutas, este puede seleccionar la mejor conexión de servicio para usar para la ubicación de red remota.
- Al configurar conexiones de servicio, utilice solo rutas estáticas o solo BGP para las conexiones. Palo Alto Networks no recomienda mezclar conexiones de servicio que utilizan BGP y rutas estáticas cuando se utilizan rutas predeterminadas.
- (Para implementaciones de Prisma Access (Managed by Panorama) únicamente) El uso de rutas predeterminadas es compatible con implementaciones de varios inquilinos.

 ©2025 Palo Alto Networks, Inc.

- Prisma Access no reenvía el tráfico de autenticación SAML de VPN sin cliente, portal o puerta de enlace a un proveedor de identidad pública (IdP) mediante la ruta predeterminada.

Para obtener más información y ejemplos de implementación de rutas predeterminadas con direccionamiento de tráfico, consulte Ejemplo de Rutas predeterminadas con dirección de tráfico, Ejemplo de rutas predeterminadas con dirección de tráfico directo a Internet y Ejemplo de rutas predeterminadas con dirección de tráfico y conexión de servicio dedicado.

Dirección de tráfico en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En las implementaciones de Prisma Access estándar, una conexión de servicio proporciona acceso a recursos de red internos, como servicios de autenticación y aplicaciones privadas en su sede o centro de datos. Las conexiones de servicio procesan el tráfico interno, donde no se requiere acceso a Internet. En algunos casos, es posible que desee redirigir el tráfico orientado a Internet al centro de datos. La gestión del tráfico le permite redirigir el tráfico de usuarios móviles o de redes remotas a una conexión de servicio antes de enviarlo a Internet.

Puede utilizar la dirección del tráfico con implementaciones de usuarios móviles, implementaciones de red remotas o una combinación de ambas. Utilice la dirección de tráfico para dirigir el tráfico de red vinculado a Internet en función de muchos criterios, incluidas direcciones IP, usuarios, URL, categorías de URL personalizadas, tipo de servicio (HTTP o HTTPS), User-ID, grupos de direcciones dinámicas (DAG), grupos de usuarios dinámicos (DUG) y listas dinámicas externas (EDL).

Hay dos tipos de acción compatibles con la dirección de tráfico:

- **Forward to the target (Reenviar al objetivo)**: utilice los criterios de las reglas de direccionamiento de tráfico para reenviar el tráfico enlazado a Internet a través de un destino que cree y que utilice una o varias conexiones de servicio.
- **Forward to the internet (Reenviar a Internet)**: utilice los criterios de las reglas de dirección de tráfico para reenviar directamente el tráfico desde su origen (ubicación de usuario móvil o conexión de red remota) a Internet, sin que se reenvíe a una conexión de servicio.

Si reenvía a un objetivo, puede optar por crear dos tipos de grupos de objetivo: dedicados y no dedicados.

- Una conexión de servicio que se utiliza solo para el tráfico relacionado con la dirección del tráfico es una *Conexión de servicio dedicado*. Para configurar una conexión de servicio que se utilizará como una conexión de servicio dedicada, seleccione **Dedicated for Traffic Steering Only (Dedicado solo para la dirección de tráfico)** cuando usted Configurar la dirección del tráfico en Prisma Access en Panorama. Seleccione **Dedicated for PBF Only (Dedicado para PBF únicamente)** Al configurar una regla de dirección de tráfico en Strata Cloud Manager.

  Es posible que desee configurar una conexión de servicio dedicado si utiliza una pila de seguridad de terceros que esté fuera de la red interna de su organización para procesar el tráfico antes de que se envíe a una aplicación SaaS pública o a Internet. Dado que la pila de

 ©2025 Palo Alto Networks, Inc.

seguridad no forma parte de la red de su organización, no desea que esta conexión de servicio procese ningún tráfico de red interno.

- Una conexión de servicio que se utiliza para el direccionamiento del tráfico y para el tráfico relacionado con la conexión de servicio estándar (como el tráfico que va a un servidor de autenticación en el centro de datos) es una *Conexión de servicio no dedicado*.

La configuración de una conexión de servicio como una conexión de servicio dedicada provoca los siguientes cambios en la implementación:

- (Para implementaciones de Prisma Access (Managed by Strata Cloud Manager) únicamente) Las conexiones de servicio aplican NAT de origen al tráfico reenviado. La dirección IP de origen es la dirección de la conexión de servicio del **EBGP Router (Enrutador EBGP)**, que se toma de la subred de infraestructura.
- La zona para todas las conexiones de servicio asociadas a este destino cambia de Confianza a No confianza, o Fiable a No fiable. Revise su asignación de zonas y Configurar la asignación de zonas y las políticas de seguridad para la dirección de tráfico de conexiones dedicadas para asegurarse de que su red refleje este cambio.
- Las conexiones de servicio que se configuran como conexiones de servicio dedicadas no participan en el enrutamiento BGP, ya sea interna o externamente.
- (Para implementaciones de Prisma Access (Managed by Panorama) únicamente) Si la conexión de servicio dedicado utiliza BGP, el estado del BGP se muestra como **Not Enabled (No habilitado)** al abrir la página de estado[**Panorama** > **Cloud Service (Servicio en la nube)** > **Status (Estado)** > **Monitor (Supervisar)** > **Service Connection (Conexión de servicio)**], seleccione una región y, a continuación, seleccione la pestaña Status (Estado). Para comprobar el estado de BGP de una conexión de servicio, consulte la página de configuración de conexiones de servicio (**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)**).
- (Para implementaciones de Prisma Access (Managed by Panorama) únicamente) De forma predeterminada, las conexiones de servicio aplican NAT de origen al tráfico reenviado. La dirección IP de origen es la **User-ID Agent Address (Dirección del agente de User-ID)** de la conexión de servicio [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles en la red)** > **Service Connection (Conexión de servicio)** > **User-ID Agent Address (Dirección del agente de User-ID)**], que se toma de la subred de infraestructura [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Infrastructure (Infraestructura de servicios)**].

  (Para implementaciones de Prisma Access (Managed by Panorama) únicamente) Puede deshabilitar la TDR de origen y utilizar las direcciones IP de origen de su organización para la conexión de servicio dedicado; Para ello, seleccione **Disable Source NAT for Dedicated SC (Deshabilitar NAT de origen para SC dedicado)** cuando usted vaya a **Add (Añadir)** un objetivo en el área **arget Service Connections for Traffic Steering (Conexiones de servicio de destino para la dirección del tráfico)**.

Requisitos de dirección del tráfico

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

 ©2025 Palo Alto Networks, Inc.

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	

Antes de implementar la dirección de tráfico en su Implementación de Prisma Access, asegúrese de que su entorno de red tenga los siguientes requisitos de infraestructura:

- Prisma Access debe poder conectarse al CPE compatible con IPSec (como un enrutador o dispositivo SD-WAN) que su organización utiliza para finalizar la conexión del servicio, y la dirección IP del dispositivo debe ser accesible desde Prisma Access.

  Crea una conexión de servicio utilizando perfiles criptográficos IPSec e IKE estándar entre la ubicación de la pila y Prisma Access. Puede utilizar rutas estáticas, BGP o una combinación de ambas cuando configura una conexión de servicio y utiliza la dirección de tráfico. Si utiliza rutas predeterminadas con dirección de tráfico, Palo Alto Networks recomienda que utilice solo BGP o solo rutas estáticas. Si utiliza enrutamiento estático, especifique la dirección IP pública utilizada por el CPE de la organización como **Peer Address (Dirección del peer** cuando cree una puerta de enlace IKE.
- Prisma Access podría no coincidir con los primeros paquetes de una URL de una categoría de URL en una regla de dirección de tráfico, lo que significa que los primeros paquetes de una sesión de red (por ejemplo, un protocolo de enlace TCP) podrían no coincidir con la regla. Palo Alto Networks recomienda que, para las URL que utiliza en las reglas de direccionamiento de tráfico, cree una regla de política de seguridad para permitirles pasar a través de la zona de no confianza (Untrust) para que el protocolo de enlace pueda completarse cuando comience una nueva sesión.
- Si utiliza esta configuración con una pila de seguridad, la ubicación de la pila debe ser accesible desde la conexión de servicio mediante una configuración de túnel IPSec estándar.

Utilice las siguientes directrices cuando configure un túnel IPSec:

- Puede especificar hasta 1000 URL (agregadas) en una configuración de dirección de tráfico, incluidas URL normales y comodín (*.example.com) en categorías de URL personalizadas.

  Este número incluye las URL introducidas manualmente, las URL comodín y las URL que se introducen en una categoría de URL personalizada.
- Prisma Access antepone un asterisco a las URL en categorías de URL personalizadas, si utiliza esta categoría en una regla de dirección de tráfico. Si utiliza las mismas políticas de categoría de URL para la dirección de tráfico y otras reglas de políticas de seguridad, estos cambios se aplicarán tanto a las reglas de dirección de tráfico como a otras reglas de políticas de seguridad.

  Si tiene categorías de URL personalizadas que no se utilizan en las reglas de dirección de tráfico, Prisma Access no cambia las URL en esas categorías.
- Utilice URL en minúsculas cuando introduzca las URL en una regla de reenvío de tráfico y cuando añada las URL en una categoría de URL personalizada.
- Puede configurar un máximo de 100 reglas de reenvío de tráfico.
- Si tiene túneles primarios y de respaldo configurados, la dirección de tráfico mediante reglas de dirección de tráfico no funcionará después de una conmutación por error del túnel primario (activo) al de respaldo. Rutas predeterminadas con dirección del tráfico de Prisma Access funciona en un escenario de conmutación por error con túneles primarios y de respaldo.

 ©2025 Palo Alto Networks, Inc.

Ejemplo de Rutas predeterminadas con dirección de tráfico

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

El siguiente ejemplo muestra una implementación de Prisma Access de muestra con los siguientes componentes:

- Dos ubicaciones de usuarios móviles de Prisma Access; una en los Estados Unidos (EE. UU.) y otra en Europa (UE).
- Dos conexiones de servicio de Prisma Access; una en los EE. UU. y otra en la UE, con ambos centros de datos enviando rutas predeterminadas a las conexiones de servicio [**Accept Default Route over Service Connections (Aceptar ruta predeterminada a través de conexiones de servicio)** está habilitado].
- Dos centros de datos; uno en los EE. UU. y otro en la UE.

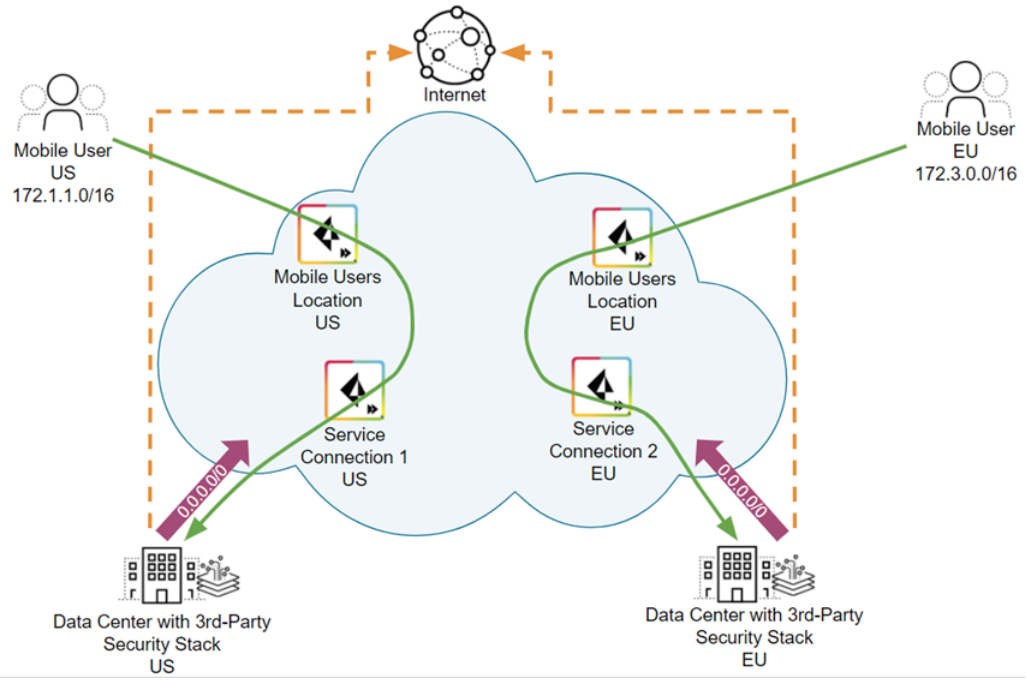
  Cada centro de datos tiene una pila de seguridad de terceros; por esta razón, desea que todo el tráfico destinado a Internet pase por el centro de datos antes de salir a Internet.

Cuando un usuario móvil envía tráfico de centro de datos, Prisma Access verifica sus tablas de enrutamiento, determina la conexión de servicio más cercana y reenvía el tráfico a esa conexión de servicio. En el siguiente ejemplo, Prisma Access envía el tráfico del centro de datos de los usuarios móviles en los EE. UU a la Conexión de servicio y el tráfico de los usuarios móviles en la UE a Conexión de servicio 2.

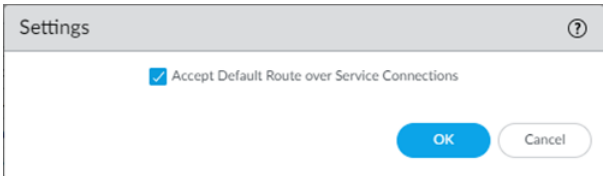


*No utilice conexiones de servicio que sean **Dedicated for Traffic Steering Only (Dedicadas únicamente para la dirección del tráfico)** con rutas predeterminadas; las conexiones de servicio dedicadas no participan en el enrutamiento BGP, por lo que no pueden recibir anuncios BGP de la sede o del centro de datos.*

 ©2025 Palo Alto Networks, Inc.



Para habilitar rutas predeterminadas, seleccione **Accept Default Route over Service Connections (Aceptar ruta predeterminada sobre conexiones de servicio)** cuando configure la configuración de dirección de tráfico. Después de que configure esta opción y confirme y envíe sus cambios, Prisma Access envía el tráfico destinado a Internet a través de las conexiones de servicio.

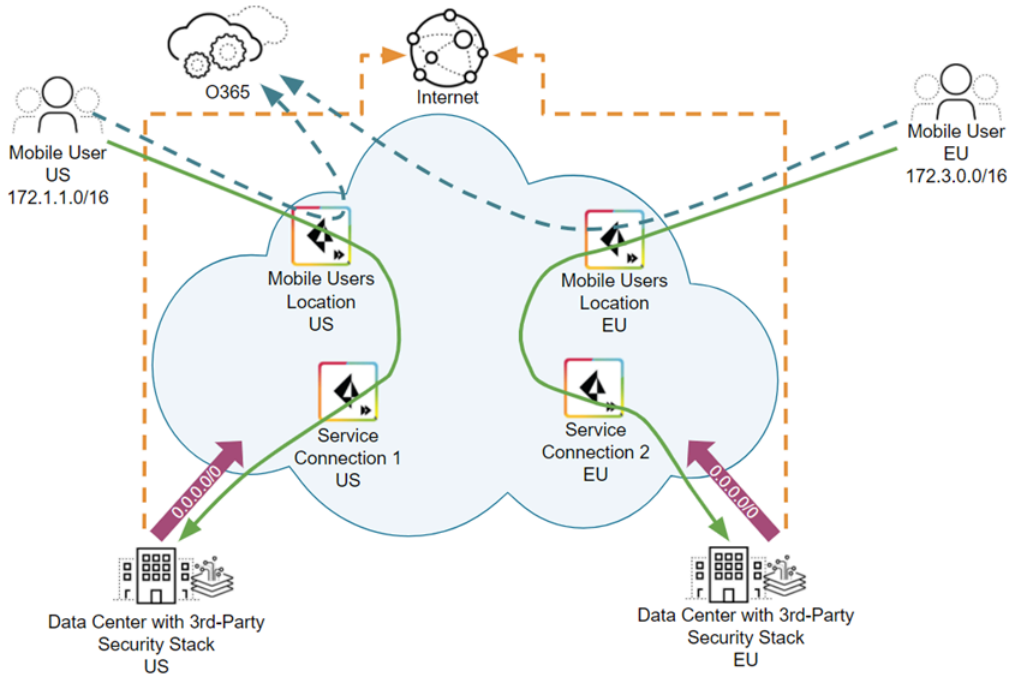


Ejemplo de rutas predeterminadas con dirección de tráfico directo a Internet

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En el ejemplo siguiente se muestra el uso de un control más granular para el tráfico dirigido a aplicaciones SaaS externas En este caso, desea enviar el tráfico de Office 365 para que salga a Internet directamente desde la ubicación del usuario móvil, en lugar de enviarlo al centro de datos para su posterior procesamiento. Utilice la dirección de tráfico junto con las rutas predeterminadas para esta configuración.

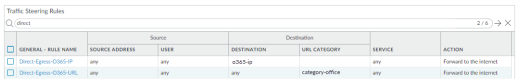
 ©2025 Palo Alto Networks, Inc.



Para permitir que Prisma Access enrute el tráfico de Office 365 directamente a Internet, realice las siguientes acciones:

- Cree un EDL [**Object (Objeto)** > **External Dynamic Lists (Listas dinámicas externas)**] con direcciones IP que coincidan con las direcciones de Office 365.
- Cree una Custom URL category (Categoría de URL personalizada) [**Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)**] con direcciones URL que coincidan con la dirección URL de Office 365.
- Cree Configurar la dirección del tráfico en Prisma Access y especifique la EDL y la categoría de URL que creó como criterios de coincidencia de destino con una **Action (Acción)** de **Forward to the internet (Reenviar a Internet)**.

Esta configuración envía el tráfico de Office 365 directamente a Internet, mientras que el resto del tráfico enlazado a Internet se envía al centro de datos para su posterior procesamiento antes de salir a Internet.



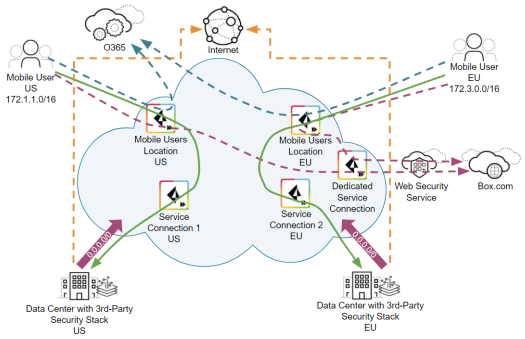
Ejemplo de rutas predeterminadas con dirección de tráfico y conexión de servicio dedicado

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	☐ Licencia de Prisma Access

En este ejemplo, además de la configuración anterior, tiene un servicio de seguridad de Internet de terceros y desea enviar tráfico desde box.com para que el servicio de seguridad lo procese antes de salir a Internet. No desea enviar ningún otro tráfico vinculado a Internet al servicio de

 ©2025 Palo Alto Networks, Inc.

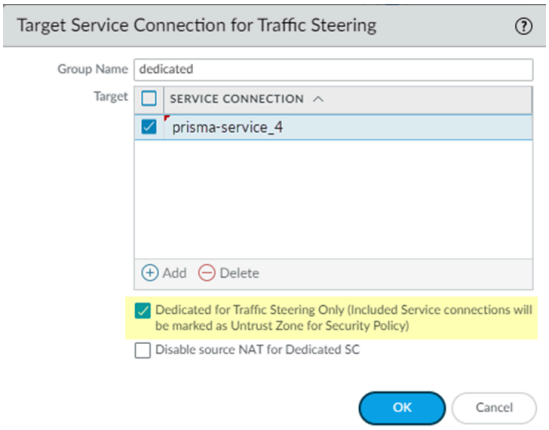
seguridad; por este motivo, se crea una conexión de servicio dedicada para el tráfico box.com. Una vez completada la configuración, Prisma Access envía tráfico de destino *.box.com a la pila.



Para habilitar esta implementación, realice las siguientes acciones en la pestaña Traffic Steering (Dirección de tráfico):

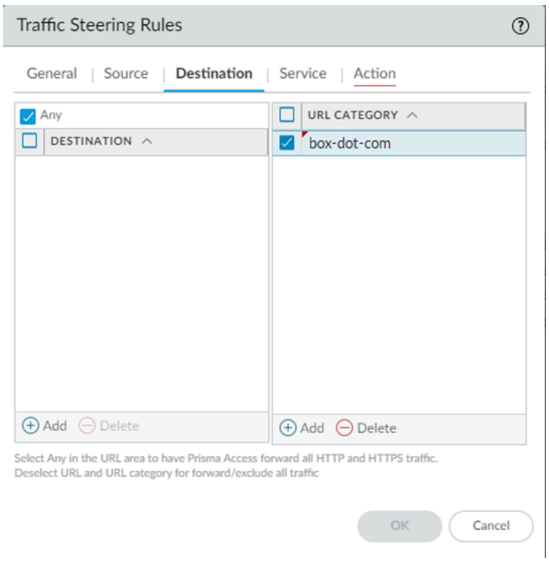
- Cree un grupo de conexiones de servicio de destino que asigne una o más conexiones de servicio al destino y seleccione **Dedicated for Traffic Steering Only (Dedicado solo para la dirección de tráfico)**, lo que hace que la conexión o conexiones de servicio de destino sean dedicadas.

  Si crea un destino con más de una conexión de servicio, Prisma Access selecciona la mejor conexión de servicio para reenviar el tráfico vinculado a Internet.

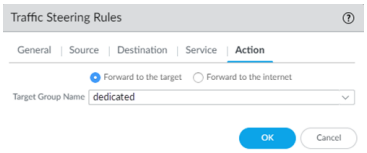


 ©2025 Palo Alto Networks, Inc.

- Cree una regla de dirección de tráfico que reenvíe el tráfico a la dirección URL. En la siguiente captura de pantalla se muestra el destino del tráfico al que se le asigna una categoría de URL personalizada que contiene la URL *.box.com.



- Cree una **Action (Acción)** en la regla de dirección de tráfico de **Forward to the target (Reenviar al objetivo)** y especifique el nombre del grupo de destino que ha creado [**dedicated (dedicado)** en este caso].



Directrices de la Regla de dirección de tráfico de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

La dirección de tráfico puede procesar una amplia variedad de configuraciones posibles; sin embargo, es importante entender cómo Prisma Access procesa las reglas, para que pueda crear reglas que sean fáciles de mantener y administrar. Para ayudarle a crear las reglas que mejor funcionan para su implementación, siga estas directrices:

- Prisma Access evalúa las reglas en el orden en que las crea (de arriba hacia abajo). Especifique reglas más específicas en la parte superior y reglas más generales en la parte inferior.
- Cree varias reglas con menos criterios coincidentes, en lugar de crear menos reglas con varios tipos de criterios. Crear reglas más simples acelera la creación de reglas y facilita la modificación de una regla.
- Como no puede mover una regla hacia arriba o hacia abajo en una lista después de crearla, planifique cuidadosamente su orden de reglas antes de crear las reglas.

 ©2025 Palo Alto Networks, Inc.

- No se admiten reglas que especifiquen **Any (Cualquier)** dirección de origen y usuario, **Any (Cualquier)** destino de origen y categoría de URL, ni **Any (Cualquier)** servicio. Utilice reglas más específicas; por ejemplo, especifique una regla con **Any (Cualquier)** tráfico de origen o destino y un servicio de **servicio-http** y **servicio-https**.
- Si va a especificar reglas para usuarios en el campo **Source User (Usuario de origen)**, asegúrese de que Prisma Access pueda distinguir entre usuarios si se comparte el mismo nombre de usuario entre usuarios que se autentican localmente y usuarios que se autentican mediante LDAP autenticando usuarios de LDAP en el formato de `dominio/nombre de usuario` y autenticando usuarios locales en el formato de `nombre de usuario` (sin el nombre de dominio).
- Si ha configurado un cortafuegos local de nueva generación como dispositivo principal, puede rellenar automáticamente la información de usuario y grupo para grupos de dispositivos de usuarios móviles en las reglas de políticas de dirección de tráfico y seguridad seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)**, haciendo clic en el icono de engranaje para editar la configuración y seleccionando el **Master Device (Dispositivo principal)** en el área Grupo de dispositivos. Si bien esto rellena el dispositivo maestro en cada grupo de dispositivos, solo rellena la información de usuario y grupo para usuarios móviles en las reglas de política de seguridad.
- Si se utiliza una EDL (lista de IP de tipo) en una regla de dirección de tráfico y la URL de origen de EDL de la EDL se actualiza a una URL que no es accesible, Prisma Access puede seguir utilizando la lista de IP almacenada en caché de la URL anterior.
- Prisma Access evita la dirección del tráfico para las reglas con un tipo de servicio HTTP o HTTPS si utiliza una política de anulación de aplicaciones para los puertos TCP 80 y 443.

  Además, la dirección de tráfico no funciona para las URL de las categorías de URL a las que se hace referencia en la regla de dirección de tráfico si ha configurado una política de cancelación de aplicación para los puertos TCP 80 o 443.
- Puede especificar direcciones IP de destino y categorías de URL en la misma regla. Si lo hace, Prisma Access utiliza un OR lógico para procesar los criterios de destino en la regla, pero procesa las URL y el tráfico de categoría de URL basándose en los puertos TCP 80 y 8080 para HTTP y el puerto TCP 443 para HTTPS.

  Para una regla con direcciones IP y categorías de URL, el tráfico coincide con la regla si coincide la dirección IP o la categoría de URL, pero procesa el tráfico de categoría de URL basándose solo en los puertos 80, 443 y 8080. Palo Alto Networks no recomienda crear una regla de este tipo, sino reglas más simples.

Por ejemplo, desea hacer cumplir las siguientes reglas para el tráfico de red:

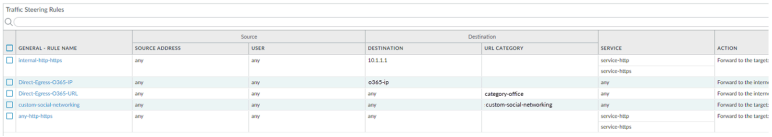
- Tiene un servidor HTTP interno con una dirección IP de 10.1.1.1 en el centro de datos, y desea dirigir el tráfico HTTP y HTTPS interno a este servidor. La dirección IP del servidor es 10.1.1.1.

  El tráfico a este servidor no debe ir a Internet y debe procesarse internamente; por lo tanto, elija un destino no dedicado para este tráfico, porque este tipo de destino procesa el tráfico interno y el dirigido a Internet.
- Desea que el tráfico de office365.com se enrute directamente a Internet.
- Desea que el tráfico de *.ejemplo.com o cualquier tráfico definido en una categoría de URL personalizada de **custom-social-networking** se enrute a una conexión dedicada.

 ©2025 Palo Alto Networks, Inc.

- Desea que cualquier otro tráfico HTTP y HTTPS utilice el mismo destino de conexión de servicio no dedicado que el utilizado para el servidor HTTP interno.

Para este ejemplo, cree las reglas desde las más específicas hasta las menos específicas, como se muestra en la siguiente captura de pantalla. No añada la regla que permite todo el tráfico HTTP y HTTPS primero, o Prisma Access dirigiría todo el tráfico HTTP y HTTPS a la conexión no dedicada sin evaluar ninguna de las otras reglas.



Configurar la asignación de zonas y las políticas de seguridad para la dirección de tráfico de conexiones dedicadas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si crea un destino que utiliza una conexión de servicio dedicada, la zona de la conexión de servicio dedicada cambia de **Trust (Fiable)** a **Untrust (No fiable)** (los destinos de conexión de servicio no dedicados no cambian sus zonas). Dado que no puede crear zonas ni configurar la asignación de zonas para conexiones de servicio, en su lugar, en su lugar realiza cambios en la asignación de zonas y la política de seguridad para conexiones de servicio dedicadas a los usuarios móviles y grupos de dispositivos. Complete los siguientes pasos para configurar la asignación de zonas para conexiones dedicadas.

Estos pasos muestran una configuración de muestra; puede adaptar este ejemplo para adaptarlo a su implementación.

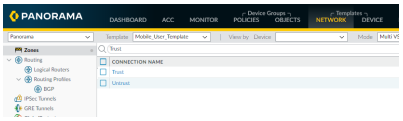
STEP 1 | Seleccione **Network (Red)** > **Zones (Zonas)**.

STEP 2 | Seleccione la **Template (Plantilla)** correcta de la lista desplegable (**Mobile_User_Template** para usuarios móviles o **Remote_Network_Template** para redes remotas).

Si tiene un usuario móvil y una implementación de red remota, debe realizar estos pasos dos veces: una en **Mobile_User_Template** y otra en **Remote_Network_Template**.

STEP 3 | **Add (Añadir)** dos zonas para sus zonas fiables y no fiables.

Este ejemplo crea dos zonas llamadas **Trust (Fiable)** y **Untrust (No fiable)**.



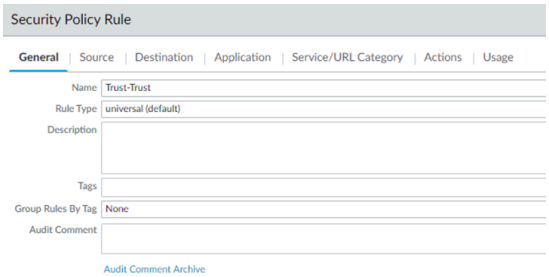
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Cree políticas predeterminadas para las zonas que creó.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Post Rules (Reglas posteriores)**.
2. Seleccione el **Device Group (Grupo de dispositivos)** correcto de la lista desplegable (**Mobile_User_Device_Group** para redes remotas o **Remote_Network_Device_Group** para usuarios móviles).

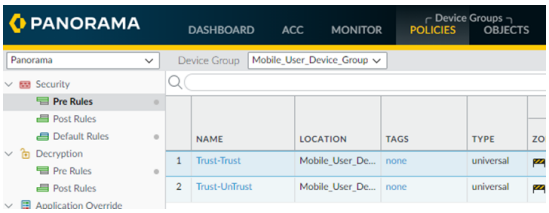
   Si tiene un usuario móvil y una implementación de red remota, debe realizar estos pasos dos veces: una en **Mobile_User_Device_Group** y otra en **Remote_Network_Device_Group**.
3. Deberá **Add (Añadir)** una política predeterminada para usar en el tráfico de zona de confianza a zona de confianza.

   Esta política permite que **Any (Cualquier)** tráfico pase para todo el tráfico de **Source (Origen)**, **User (Usuario)**, **Destination (Destino)**, **Application (Aplicación)** y **Service/URL Category (Categoría de servicio/URL**.



4. Elija **Add (Añadir)** una política predeterminada para usar en el tráfico de la zona de confianza a la zona de no confianza, utilizando los mismos parámetros que utilizó para la política de confianza a confianza.

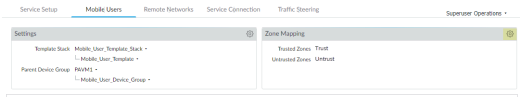
   Una vez completado, tendrá dos políticas de seguridad: una para el tráfico de confianza a confianza y otra para el tráfico de confianza a no confianza.



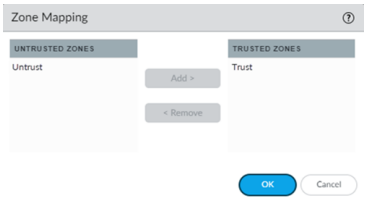
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Defina la asignación de zonas para las redes remotas, los usuarios móviles o ambos, según sea necesario para su implementación.

1. Establezca la asignación de zonas para las redes remotas, los usuarios móviles o ambos.
   - Para usuarios móviles, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users (Usuarios móviles)**.
   - Para redes remotas, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**.
2. Haga clic en el icono de engranaje junto a **Zone Mapping (Asignación de zonas)** para editar la configuración.



3. Establezca la **Zone Mapping (Asignación de zonas)** para su implementación, moviendo la zona para el tráfico fiable a las **Trusted Zones (Zonas de confianza)** y la zona para el tráfico no fiable a las **Untrusted Zones (Zonas no fiables)**; luego, haga clic en **OK (Aceptar)**.



Configurar la dirección del tráfico en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ La capacidad de enviar la lista de revocación de certificados (CRL) y el Protocolo de Estado de Certificados en Línea (OCSP) directamente a Internet requiere una versión de Prisma Access mínima de 5.1.1.

La gestión del tráfico le permite configurar el acceso de Prisma Access para crear reglas de gestión del tráfico que especifiquen objetivos para el tráfico destinado a Internet desde usuarios móviles y conexiones de red remotas. Puede especificar el tráfico que se redirigirá a una conexión de servicio antes de enviarlo a Internet, o puede especificar el tráfico que saldrá directamente a Internet. Configure la dirección del tráfico para su implementación de Prisma Access completando los siguientes pasos.

- Strata Cloud Manager
- Panorama

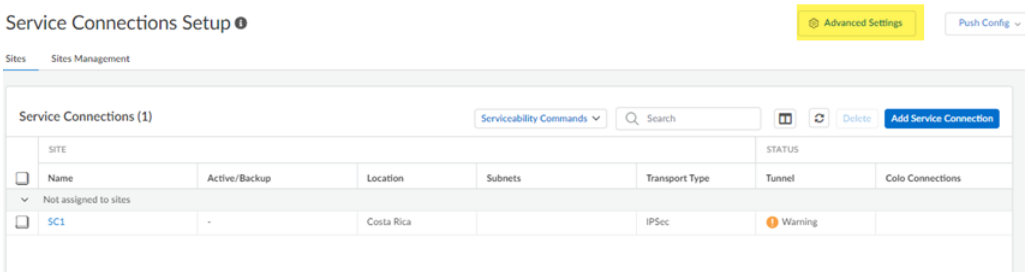
 ©2025 Palo Alto Networks, Inc.

Configurar la dirección de tráfico en Prisma Access (Strata Cloud Manager)

En las implementaciones de Prisma Access, una conexión de servicio proporciona acceso a recursos de red internos, como servicios de autenticación y aplicaciones privadas en su sede o centro de datos. El proceso de conexiones de servicio gestiona el tráfico interno, donde no se requiere acceso a internet. En algunos casos, es posible que desee redirigir el tráfico destinado a Internet al centro de datos. La gestión del tráfico le permite redirigir el tráfico de usuarios móviles o de redes remotas a una conexión de servicio antes de enviarlo a Internet. Configure la dirección del tráfico para su implementación de Prisma Access completando los siguientes pasos.

STEP 1 | Integre sus conexiones de servicio, usuarios móviles y redes remotas, según corresponda a su implementación.

STEP 2 | Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Service Connections (Conexiones de servicio)** > **Advanced Settings (Configuración avanzada)**.



STEP 3 | Configure las reglas de **Traffic Steering (Dirección de tráfico)**.

1. (Opcional, solo implementaciones de usuarios móviles) Permitir a Prisma Access aceptar e instalar la ruta predeterminada anunciada en una o más conexiones de servicio desde el CPE haciendo clic en el icono de engranaje para abrir la Configuración y seleccionando **Accept Default Route over Service Connections (Aceptar ruta predeterminada en conexiones de servicio)**.

   Las rutas predeterminadas tienen pautas que debe seguir al usarlas; por ejemplo, las rutas predeterminadas solo son compatibles con implementaciones de usuarios móviles y no tienen efecto en las implementaciones de redes remotas. Asegúrese de revisar estas pautas antes de implementar rutas predeterminadas con direccionamiento de tráfico.

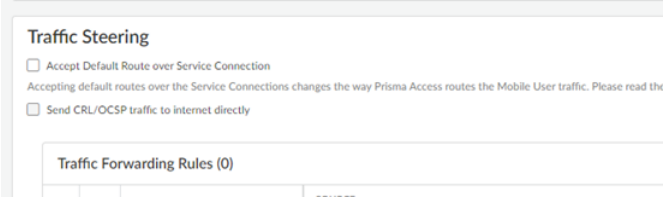
STEP 4 | (Opcional) Permita a Prisma Access enviar tráfico de lista de revocación de certificados (CRL) y Protocolo de estado de certificado en línea (OCSP) directamente a Internet

 ©2025 Palo Alto Networks, Inc.

seleccionando **Send CRL/OCSP traffic to internet directly (Enviar tráfico CRL/OCSP a Internet directamente)**.

Seleccione esta opción si tiene un servidor OCSP o CRP en Internet público y desea enviar ese tráfico directamente a Internet utilizando la zona que no es de confianza. Si no selecciona esta opción, Prisma Access envía este tráfico a la conexión de servicio.

*Asegúrese de haber actualizado su implementación de Prisma Access a una versión mínima de 5.1.1 antes de seleccionar **Send CRL/OCSP traffic to internet directly (Enviar tráfico CRL/OCSP a Internet directamente)**.*



STEP 5 | Cree reglas para el objetivo que ha creado y aplíquelas al objetivo.

1. **Add Rule (Añadir regla)**.
2. Introduzca un **Name (Nombre)** único para la regla.
3. En el área **Source (Origen)**:
   - Especifique la lista de usuarios a coincidir.

     Puede **Match Any User (Hacer coincidir con cualquier usuario)**, **Match Pre-logon (Hacer coincidir con pre inicio de sesión)**, **Match known-user (Hacer coincidir con usuario conocido)**, **Match unknown (Hacer coincidir con desconocido)** o **Add Users (Añadir usuarios)**, y seleccionar el usuario o los usuarios con los que coincida.
   - Seleccione **Source Address Entities (Entidades de dirección de origen)** Puede seleccionar uno o más de los siguientes objetos:
     - Una dirección IP
     - Un grupo de direcciones
     - Una lista dinámica externa (EDL) que utiliza direcciones IP o direcciones URL
4. En el área **Destination (Destino)**, especifique una de las siguientes **Destination Address Entities (Entidades de dirección de destino)** o seleccione **Any (Cualquiera)** para que el tráfico sea procesado por las reglas en el campo Categoría de URL:
   - Una dirección IP
   - Un grupo de direcciones
   - Una Lista dinámica externa (EDL) que utiliza direcciones IP o URL
5. Especifique una **categoría de URL**.

   Si crea una categoría de URL personalizada, introduzca las URL en minúsculas. La dirección del tráfico admite categorías de URL personalizadas y categorías de URL

 ©2025 Palo Alto Networks, Inc.

predefinidas. Puede usar comodines con las URL en las categorías de URL. Los siguientes formatos de comodín son compatibles:

- *.example.com
- *.fqdn.example.com

Los siguientes formatos no son compatibles:

- *
- *.*
- *example.com
- example.com/ (las barras diagonales finales en las URL no son compatibles en las categorías de URL que se utilizan con la dirección de tráfico)
- example.com/path (solo se admiten nombres de dominio)
- *fqdn.example.com
- fqdn.example.*

Utilice las siguientes pautas al configurar las opciones de destino:

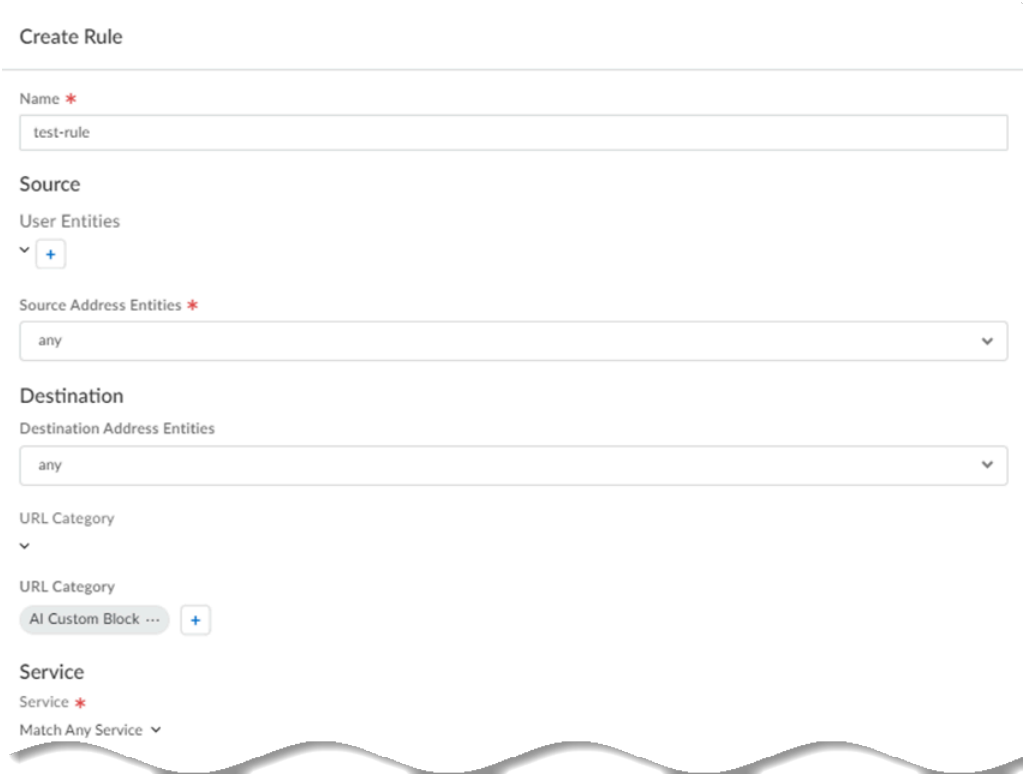
- Si especifica una categoría de URL, Prisma Access solo hace coincidir el tráfico HTTP y HTTPS, incluso cuando el servicio está configurado como **Any (Cualquiera)**.
- No cree una categoría de URL personalizada con un tipo de **Category Match (Coincidencia de categoría)**.

No cree una categoría de URL personalizada con el nombre **Custom_URL_Category_TFR**.

6. Especifique un tipo de **Service (Servicio)** y luego seleccione **Add Service (Añadir servicio)**.

   Especifique **service-http** para reenviar tráfico HTTP y especifique **service-https** para especificar tráfico HTTPS. Seleccione **Match Any Service (Hacer coincidir cualquier servicio)** para reenviar el tráfico de cualquier tipo de servicio.

 ©2025 Palo Alto Networks, Inc.



7. Cree un grupo de conexión de servicio y especifique una **Action (Acción)**.
   1. Elija **Create New (Crear nuevo)** o **Manage (Gestionar)** un grupo y dele un **Name (Nombre)** único.
   2. Especifique la conexión de **servicio o las conexiones** de servicio que se utilizarán con el destino.

      Palo Alto Networks no recomienda utilizar múltiples conexiones de servicio (ya sean dedicadas o no dedicadas) en un grupo de conexiones de servicio de destino que se menciona en una regla de direccionamiento de tráfico. Además, una conexión de servicio determinada solo puede existir en un destino y no se puede añadir una única conexión de servicio a dos destinos diferentes.
   3. (Opcional) Utilice una conexión de servicio dedicada para dirigir el tráfico a una pila de seguridad de terceros o a la nube que no esté en sus instalaciones y que no necesite participar en el enrutamiento. Para configurar una conexión de servicio que se utilizará como una conexión de servicio dedicada, seleccione **Dedicated for Traffic Steering Only (Dedicado solo para la dirección de tráfico)**.

      Las conexiones de servicio dedicadas cambian sus zonas y se marcan como una Zona no fiable para las reglas de política de seguridad.

      Anule la selección de **Dedicated for Traffic Steering Only (Dedicado solo para dirección de tráfico)** si enviará tanto tráfico relacionado con la conexión de servicio

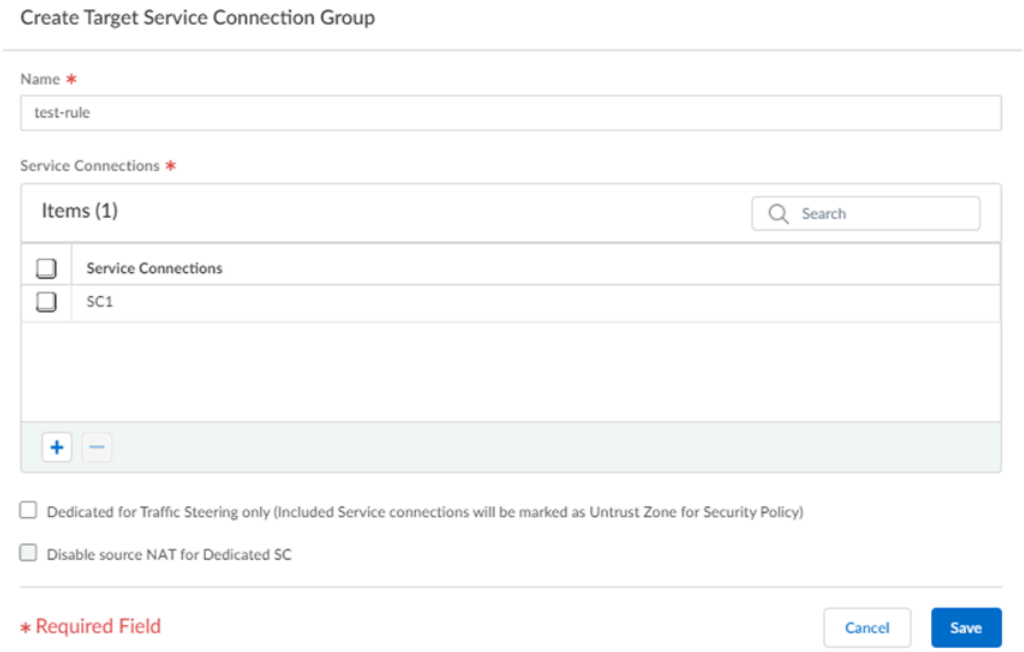
 ©2025 Palo Alto Networks, Inc.

normal como tráfico de direccionamiento de tráfico a través de la conexión de servicio; con esta opción, la zona para la conexión de servicio permanece como Fiable.

4. Deshabilite NAT de origen para conexiones de servicio dedicadas seleccionando, seleccione **Disable Source NAT for Dedicated SC (Deshabilitar NAT de origen para SC dedicado)**. NAT de origen está habilitado por defecto (la casilla está desmarcada).

   Si deshabilita el NAT de origen, Prisma Access utiliza las direcciones IP de origen de su organización para la conexión de servicio dedicada. Si habilita NAT de origen, Prisma Access utiliza la dirección del **EBGP Router (Enrutador EBGP)** de la conexión de servicio [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **EBGP Router (Enrutador EBGP)**] como dirección IP de origen, incluso después de que el tráfico salga de la conexión de servicio dedicada.

5. Haga clic en **Save (Guardar)** para guardar sus cambios.



8. Reenvíe el tráfico al destino de conexión de servicio especificado o envíe el tráfico directamente a Internet sin pasar por la conexión de servicio.

   - Para que Prisma Access reenvíe el tráfico hacia un destino de conexión de servicio, seleccione **Forward to the target (Reenviar al objetivo)**; luego seleccione el **Target Service Connection Group (Grupo de conexión de servicio de destino)**.

     Especifique esta opción si tiene tráfico que necesita enviar a su entorno existente o heredado debido a las limitaciones de la lista permitida de aplicaciones SaaS, o si

 ©2025 Palo Alto Networks, Inc.

desea crear un flujo de tráfico para dirigir el tráfico de internet especificado de vuelta a su red local.

- Para que Prisma Access reenvíe tráfico directamente a Internet sin enviarlo primero a una conexión de servicio, seleccione **Forward to the internet (Reenviar a internet)**.

  Especifique esta opción si está enviando una ruta predeterminada a Prisma Access y desea dirigir parte del tráfico directamente a Internet.



STEP 6 | Elija **Push Config (Enviar configuración)** para guardar sus cambios.

Configurar la dirección del tráfico en Prisma Access (Panorama)

STEP 1 | Integre sus conexiones de servicio, usuarios móviles y redes remotas, según corresponda a su implementación.

STEP 2 | Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Traffic Steering (Dirección del tráfico)**.

STEP 3 | (Opcional, solo implementaciones de usuarios móviles) Permitir a Prisma Access aceptar e instalar la ruta predeterminada anunciada en una o más conexiones de servicio desde el CPE haciendo clic en el icono de engranaje para abrir la Configuración y seleccionando **Accept Default Route over Service Connections (Aceptar ruta predeterminada en conexiones de servicio)**.

Las rutas predeterminadas tienen pautas que debe seguir al usarlas; por ejemplo, las rutas predeterminadas solo son compatibles con implementaciones de usuarios móviles y no tienen efecto en las implementaciones de redes remotas. Asegúrese de revisar estas pautas antes de implementar rutas predeterminadas con direccionamiento de tráfico.

STEP 4 | (Opcional) Permita a Prisma Access enviar tráfico de lista de revocación de certificados (CRL) y Protocolo de estado de certificado en línea (OCSP) directamente a Internet

 ©2025 Palo Alto Networks, Inc.

seleccionando **Send CRL/OCSP traffic to internet directly (Enviar tráfico CRL/OCSP a Internet directamente)**.

Seleccione esta opción si tiene un servidor OCSP o CRP en Internet público y desea enviar ese tráfico directamente a Internet utilizando la zona que no es de confianza. Si no selecciona esta opción, Prisma Access envía este tráfico a la conexión de servicio.

*Asegúrese de haber actualizado su implementación de Prisma Access a una versión mínima de 5.1.1 antes de seleccionar **Send CRL/OCSP traffic to internet directly (Enviar tráfico CRL/OCSP a Internet directamente)**.*



STEP 5 | (Opcional) Cree un grupo de destino y asígnele una conexión de servicio.

1. En el área **Target Service Connections for Traffic Steering (Conexiones de servicio de destino para la dirección de tráfico)**, elija **Add (Añadir)** un grupo y asígnele un **Group Name (Nombre de grupo)**.
2. Deberá**Add (Añadir)** un **Target (Destino)** para el tráfico, especificando la **Service Connection (Conexión de servicio)** que se utilizará con el destino; luego, haga clic en **OK (Aceptar)**.

   Palo Alto Networks no recomienda utilizar múltiples conexiones de servicio (ya sean dedicadas o no dedicadas) en un grupo de conexiones de servicio de destino al que se hace referencia en una regla de dirección de tráfico. Además, una conexión de servicio determinada solo puede existir en un destino y no se puede añadir una única conexión de servicio a dos destinos diferentes.
3. Elija si desea que las conexiones de servicio asociadas con este objetivo sean una conexión de servicio dedicada.
   - Puede utilizar una conexión de servicio dedicada para dirigir el tráfico a una pila de seguridad de terceros o a la nube que no esté en sus instalaciones y que no necesite participar en el enrutamiento. Para configurar una conexión de servicio que se utilizará como una conexión de servicio dedicada, seleccione **Dedicated for Traffic Steering Only (Dedicado solo para la dirección de tráfico)**.

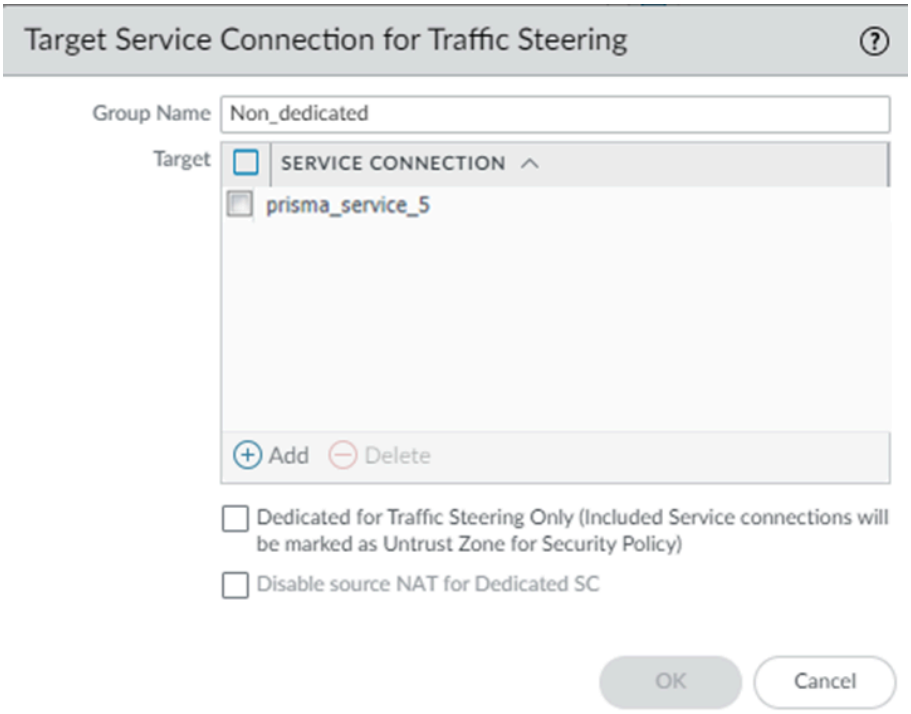
     Las conexiones de servicio dedicadas cambian sus zonas.
   - Anule la selección de **Dedicated for Traffic Steering Only (Dedicado solo para dirección de tráfico)** si enviará tanto tráfico relacionado con la conexión de servicio normal como tráfico de direccionamiento de tráfico a través de la conexión de servicio; con esta opción, la zona para la conexión de servicio permanece como Fiable.

 ©2025 Palo Alto Networks, Inc.

4. Elija si desea habilitar o deshabilitar el NAT de origen.

   Para deshabilitar NAT de origen para conexiones de servicio dedicadas, seleccione **Disable Source NAT for Dedicated SC (Deshabilitar NAT de origen para SC dedicado)**. La NAT de origen está habilitada de forma predeterminada (la casilla de verificación no está seleccionada).

   Si deshabilita el NAT de origen, Prisma Access utiliza las direcciones IP de origen de su organización para la conexión de servicio dedicada. Si habilita NAT de origen, Prisma Access utiliza la dirección del **EBGP Router (Enrutador EBGP)** de la conexión de servicio [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **EBGP Router (Enrutador EBGP)**] como dirección IP de origen, incluso después de que el tráfico salga de la conexión de servicio dedicada.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | Cree reglas para el objetivo que ha creado y aplíquelas al objetivo.

1. En el área **Traffic Steering Rules (Reglas de dirección del tráfico)**, debe **Add (Añadir)** una regla de dirección de tráfico.
2. En la pestaña **General**, asigne un **Name (Nombre)** a la regla de dirección de tráfico.
3. En la pestaña **Source (Origen)**, especifique las reglas para el tráfico de origen.
   - En el campo **Source Address (Dirección de origen)**, especifique uno o más de los siguientes objetos o seleccione **Any (Cualquiera)** para que el tráfico de cualquier origen se dirija a este destino:
     - Una dirección IP
     - Un objeto de dirección que usted creó en Panorama [**Objects (Objetos)** > **Addresses (Direcciones)**]
     - Un Grupo de direcciones dinámicas (DAG)
     - Una Lista dinámica externa (EDL) que utiliza direcciones IP o URL
   - En el campo **Source User (Usuario de origen)**, especifique reglas para el tráfico del usuario de origen. Puede especificar la siguiente información de usuario:
     - Usuarios

       Introduzca los usuarios en el formato *dominio/usuario* o *usuario@dominio*.
     - Grupos de usuarios

       Utilice nombres distinguidos (DN) completos al introducir grupos de usuarios.
     - Usuarios configurados en Panorama [**Device (Dispositivo)** > **Local User Database (Base de datos de usuario local)** > **Users (usuarios)**]
     - Grupos de usuarios configurados en Panorama [**Device (Dispositivo)** > **Local User Database (Base de datos de usuario local)** > **User Groups (Grupos de usuarios)**]

   Si utiliza objetos de dirección, DAG, EDL, usuarios o grupos de usuarios, especifíquelos como **Shared (Compartidos)** para compartirlos con todos los grupos de dispositivos en

 ©2025 Palo Alto Networks, Inc.

Prisma Access. Además, no introduzca 0.0.0.0/0 en objetos de dirección, DAG o EDL; en su lugar, introduzca 0.0.0.0/0 directamente en la regla.

Prisma Access completa automáticamente los datos de los usuarios del grupo de dispositivos de usuarios móviles únicamente.

4. En la pestaña **Destination (Destino)**, especifique los siguientes valores:

   - En el área **Destination (Destino)**, especifique uno de los siguientes criterios o seleccione **Any (Cualquiera)** para que el tráfico sea procesado por las reglas en el campo **URL Category (Categoría de URL)**:
     - Una dirección IP o prefijo
     - Un objeto de dirección que usted creó en Panorama [**Objects (Objetos)** > **Addresses (Direcciones)**]
     - Un Grupo de direcciones dinámicas (DAG)
     - Una lista dinámica externa (EDL) basada en direcciones IP

     No introduzca 0.0.0.0/0 en objetos de dirección, DAG o EDL; en su lugar, introduzca 0.0.0.0/0 directamente en la regla.

     Deje **Any (Cualquier)** seleccionado para que todo el tráfico sea procesado por las reglas en el área **URL Category (Categoría de URL)**. Si especifica reglas en las áreas **Destination (Destino)** y **URL Category (Categoría de URL)**, Prisma Access procesa primero las reglas en la categoría **Destination (Destino)**.
   - En el campo **URL Category (Categoría de URL)**, introduzca una URL category (Categoría de URL) personalizada [**Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)**]. Cuando cree una categoría de URL personalizada, introduzca las URL en minúsculas. La dirección de tráfico admite URL personalizadas y categorías de URL predefinidas.

     Puede utilizar comodines con las URL en las categorías de URL. Se admiten los siguientes formatos de comodín:
     - *.example.com

 ©2025 Palo Alto Networks, Inc.

- *.fqdn.example.com

Los siguientes formatos no son compatibles:

- *
- *.*
- *example.com
- example.com/ (las barras diagonales finales en las URL no son compatibles con las categorías de URL que se utilizan con la Dirección de tráfico)
- example.com/*ruta* (solo compatible con nombres de dominio)
- *fqdn.example.com
- fqdn.example.*

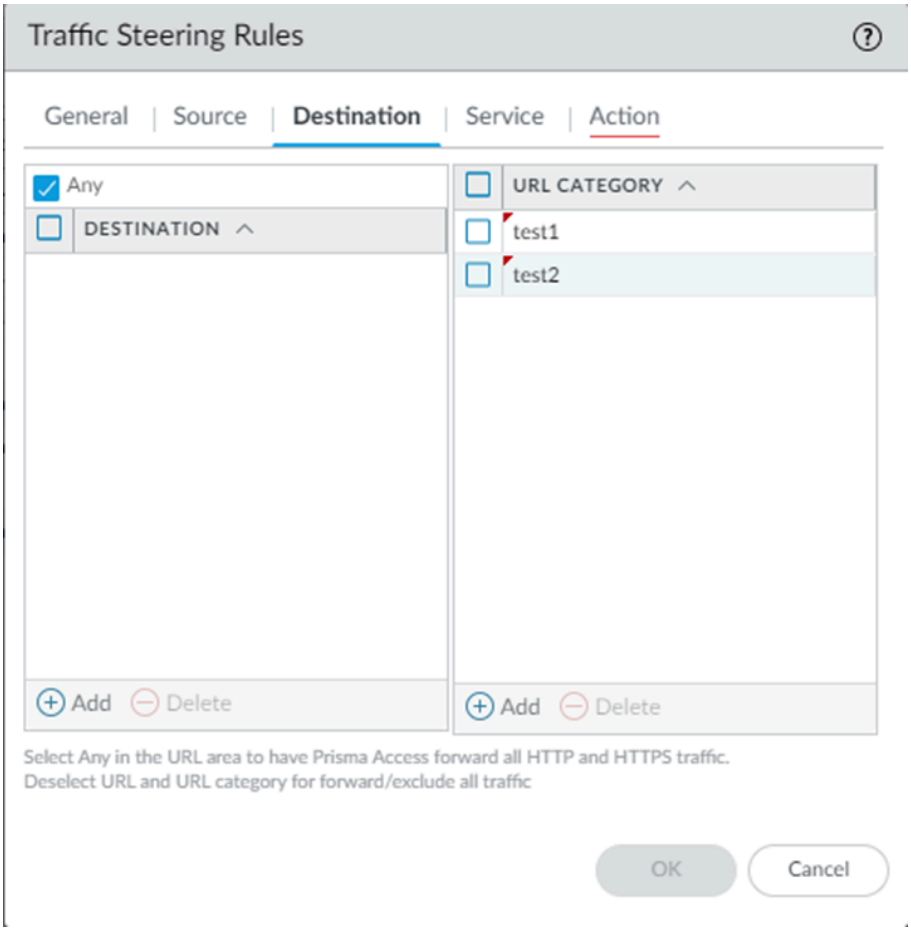
Las URL en categorías de URL personalizadas utilizan el mismo patrón de coincidencia de URL que utilizan los cortafuegos de nueva generación.

Utilice las siguientes pautas cuando configure opciones de destino:

- Si especifica una categoría de URL, Prisma Access solo coincide con el tráfico HTTP y HTTPS, incluso cuando el servicio está configurado en Any (Cualquiera).
- No cree una categoría de URL personalizada con un tipo de **Category Match (Coincidencia de categoría)**.
- No cree una categoría de URL personalizada con el nombre **Custom_URL_Category_TFR** porque, para las implementaciones que se migran desde Prisma Access 1.7 a 2.0, las URL introducidas en el área de URL desde 1.7 se mueven a una categoría de URL personalizada denominada

 ©2025 Palo Alto Networks, Inc.

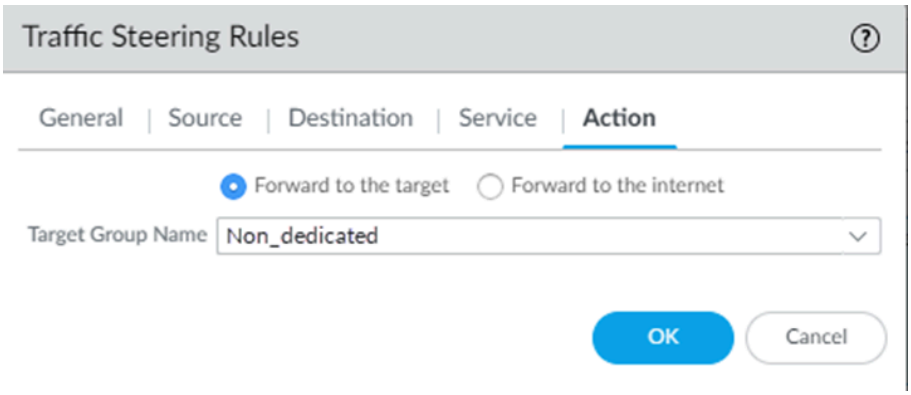
Custom_URL_Category_TFR*número*, donde *número* es un número añadido a la categoría de URL personalizada.



5. En la pestaña **Service (Servicio)**, especifique un tipo de servicio.

   Especifique **service-http** para reenviar tráfico HTTP y especifique **service-https** para especificar tráfico HTTPS. Seleccione **Any (Cualquiera)** para reenviar tráfico de cualquier tipo de servicio.
6. En la pestaña **Action (Acción)**, seleccione el **Target Group Name (Nombre del grupo de destino)** que desea aplicar a la regla de dirección de tráfico.
7. Reenvíe el tráfico al destino de conexión de servicio especificado o envíe el tráfico directamente a Internet sin pasar por la conexión de servicio.
   - Para que Prisma Access reenvíe el tráfico hacia un destino de conexión de servicio, seleccione **Forward to the target (Reenviar al objetivo)**; luego seleccione el **Target Group Name (Nombre del grupo de destino)**.
   - Para que Prisma Access reenvíe tráfico directamente a Internet sin enviarlo primero a una conexión de servicio, seleccione **Forward to the internet (Reenviar a internet)**.

 ©2025 Palo Alto Networks, Inc.



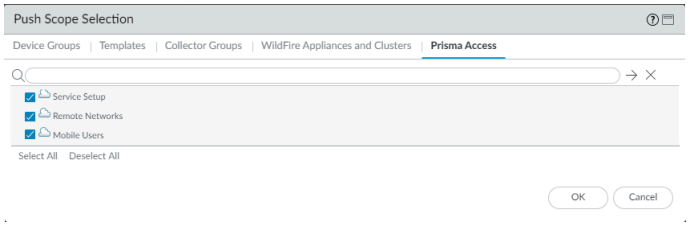
8. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 7 | Opcional Especifique reglas de dirección de tráfico adicionales.

Prisma Access procesa múltiples reglas en el orden en que las crea (de arriba a abajo).

STEP 8 | Confirme y envíe sus cambios para que estén activos en Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Prisma Access**, luego seleccione **Service Setup (Configuración de servicio)**, **Remote Networks (Redes remotas)** y **Mobile Users (Usuarios móviles)**.



3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Seleccione **Commit (Confirmar)** y **Push (Enviar)** sus cambios.

Enrutamiento para el tráfico de conexión de servicio

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Prisma Access utiliza BGP para el enrutamiento dinámico y utiliza la selección de rutas de BGP para instalar rutas en la tabla de rutas. Cuando Prisma Access enruta el tráfico a su sede o centro de datos mediante conexiones de servicio, utiliza métodos de enrutamiento que dirigen ese tráfico de manera efectiva. Prisma Access utiliza un modelo de enrutamiento predeterminado que se diseñó para adaptarse a la mayoría de las implementaciones de red; sin embargo, no todas las redes de la organización son iguales. Para adaptarse a una gama más amplia de implementaciones, Prisma Access le permite elegir otro modo para el enrutamiento de la conexión de servicio.

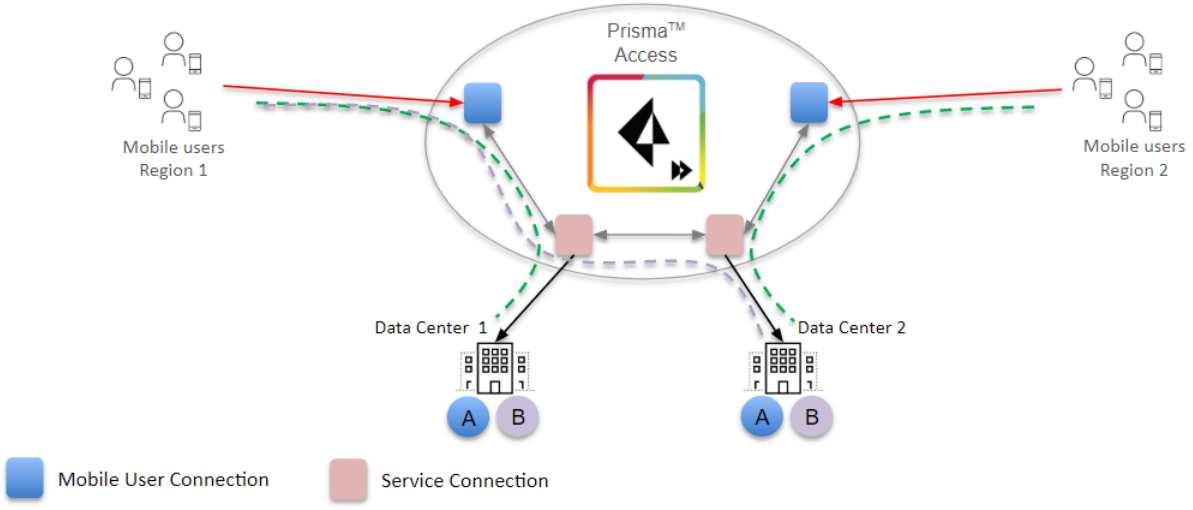
 ©2025 Palo Alto Networks, Inc.

Cambiar el método de enrutamiento de la conexión de servicio de Prisma Access requiere una comprensión profunda de la topología y los dispositivos de enrutamiento de su organización, junto con una comprensión de cómo Prisma Access funciona, como se describe en esta sección. Lea atentamente esta sección antes de cambiar el método de enrutamiento de la configuración predeterminada.

Prisma Access admite el enrutamiento estático y el enrutamiento dinámico mediante BGP para conexiones de servicio y conexiones de red remotas. Cuando utiliza el enrutamiento BGP para sus conexiones, la red de su organización aprende la información de BGP de Prisma Access.

Antes de decidir qué enrutamiento de conexión de servicio usar, debe comprender cómo Prisma Access enruta el tráfico entre usuarios móviles, redes remotas y conexiones de servicio, ya que el enrutamiento utilizado por el tráfico de usuarios móviles y el tráfico de red remota entre conexiones de servicio es diferente.

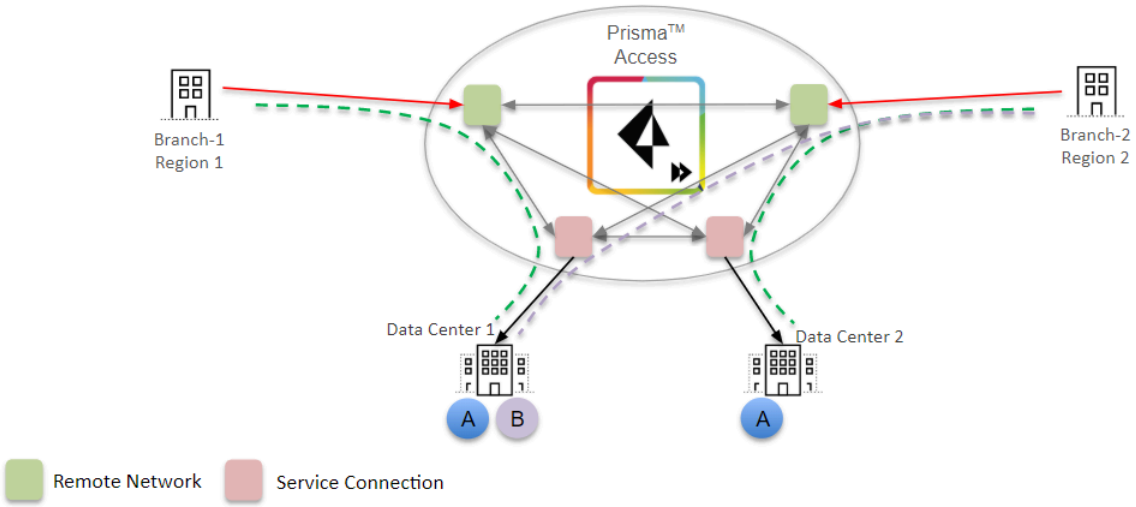
Enrutamiento de conexión de servicio de usuario móvil: la conexión de usuario móvil forma un túnel IPSec con la conexión de servicio más cercana. Prisma Access utiliza iBGP para el enrutamiento interno y eBGP para emparejarse con el equipo de las instalaciones del cliente en el centro de datos. En el diagrama siguiente se muestra cómo se enruta a los usuarios móviles de las regiones 1 y 2 a las respectivas conexiones de servicio de esa región. Los usuarios móviles de la Región 1 acceden a las aplicaciones **A** y **B** ubicadas en el Centro de Datos 1. Si la red de su organización utiliza el enrutamiento BGP para sus conexiones de servicio y una conexión de servicio experimenta un error de ISP en el centro de datos 1, Prisma Access detecta el error y enruta el tráfico de las aplicaciones **A** y **B** al centro de datos 2 después de la convergencia de BGP, lo que proporciona redundancia a los centros de datos de su red.



 ©2025 Palo Alto Networks, Inc.

Prisma Access utiliza la siguiente temporización con BGP cuando detecta un error: Si configura el enrutamiento de BGP y ha habilitado la supervisión del túnel, el tiempo de espera predeterminado más corto para determinar que un índice de parámetro de seguridad (SPI) está fallando es el monitor del túnel, que elimina todas las rutas a un par cuando detecta un fallo del túnel durante 15 segundos consecutivos. De esta forma, el monitor de túnel determina el comportamiento de las rutas BGP. Si no configura la supervisión del túnel, el temporizador de mantenimiento determina el tiempo que el túnel estará inactivo antes de eliminar la ruta. Prisma Access utiliza el valor BGP HoldTime predeterminado de 90 segundos según lo definido por RFC 4271, que es el tiempo máximo de espera antes de que Prisma Access elimine una ruta para un SPI inactivo. Si el dispositivo peer BGP tiene un tiempo de espera configurado más corto, el temporizador de espera BGP utilizará el valor más bajo. Cuando el túnel secundario se instala correctamente, la ruta secundaria tiene prioridad hasta que el túnel principal vuelva a subir. Si tanto la ruta primaria como la secundaria están activas, la ruta principal tiene prioridad.

Enrutamiento de conexión de servicio de red remota: Prisma Access crea una red de malla completa con otras redes remotas y conexiones de servicio. Al igual que con los usuarios móviles, Prisma Access utiliza iBGP para su enrutamiento interno y eBGP para emparejarse con el equipo de las instalaciones del cliente para intercambiar rutas. Si un usuario de la Sucursal 1 está accediendo a la aplicación **A** desde el Centro de datos 1 en el centro de datos de su organización y el enlace entre la Sucursal 1 y el Centro de datos 1 se desactiva, Prisma Access enruta el tráfico para la aplicación **A** al centro de datos 2 después de la convergencia de BGP.



Después de que se familiarice con el enrutamiento de la conexión de servicio de Prisma Access y cómo se relaciona con su red, puede elegir uno de los siguientes modos de enrutamiento para las conexiones de servicio:

- Enrutamiento Predeterminado: este es el modelo de enrutamiento predeterminado que Prisma Access usa.

  Utilice este modo de enrutamiento si desea que Prisma Access utilice los mecanismos de selección de la mejor ruta de BGP sin ajustar ninguno de los atributos de BGP. En este modo, Prisma Access respetará cualquier atributo anunciado por el equipo de las instalaciones del cliente (CPE).

 ©2025 Palo Alto Networks, Inc.

- Enrutamiento Hot Potato: Prisma Access entrega el tráfico lo más rápido posible a la red de su organización.

  Utilice este método de enrutamiento si desea que la red de su organización realice la mayoría de las decisiones de enrutamiento.

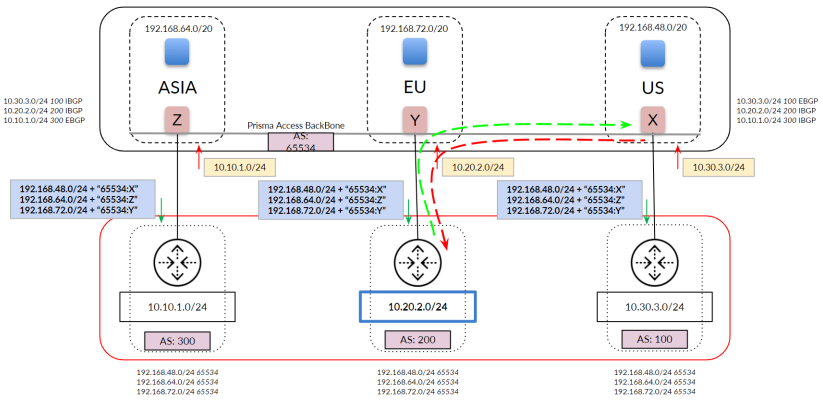
Enrutamiento predeterminado de Prisma Access

En la siguiente imagen se muestra un ejemplo del enrutamiento del tráfico de conexión del servicio de Prisma Access en el modo de enrutamiento predeterminado. La red de la organización tiene tres redes separadas en tres centros de datos y no tiene una red troncal que conecte las redes. En el modo de enrutamiento predeterminado, los grupos de usuarios móviles se anuncian por igual en las tres redes, como se muestra en la parte inferior de la imagen.

Tenga en cuenta que, cuando Prisma Access anuncia las rutas de los usuarios móviles, este divide las subredes en bloques de direcciones de clase C /24 antes de publicitarlos; por lo tanto, anuncia las subredes de usuario móvil /20 en fragmentos de /24 a medida que las puertas de enlace consumen los prefijos.

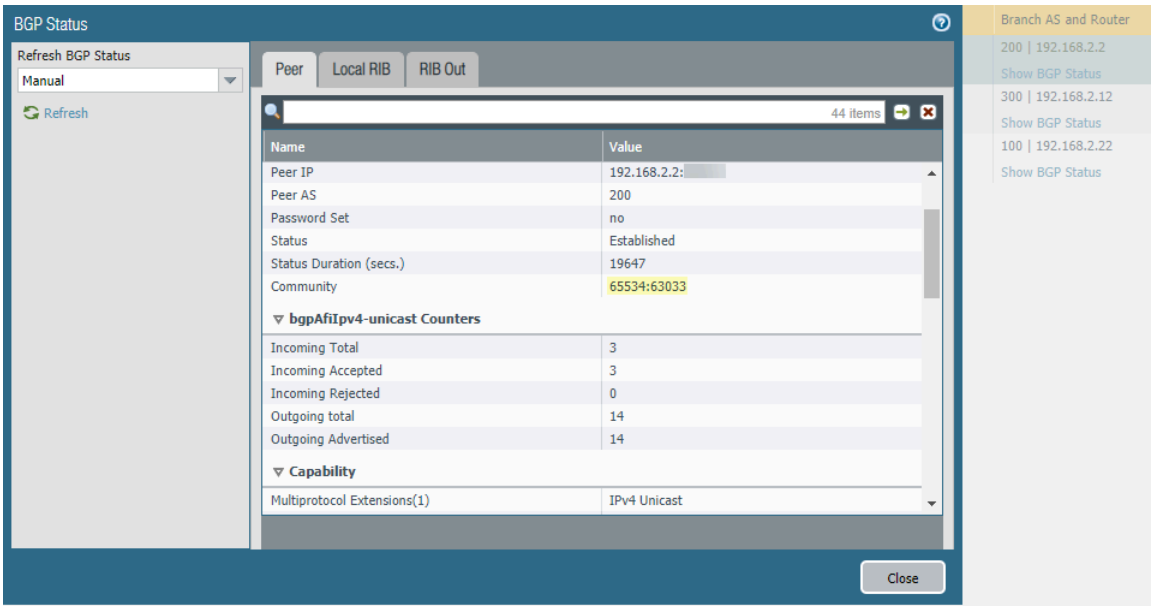
Tome nota de cómo Prisma Access utiliza anuncios de ruta BGP:

- Prisma Access no ajusta los atributos BGP predeterminados para las rutas anunciadas por el usuario móvil (Prisma Access añade su número de AS a los anuncios de ruta).
- Prisma Access anuncia rutas de usuarios móviles en bloques de subredes /24 y añade valores de comunidad BGP en las rutas que anuncia a través de la conexión de servicio. En la siguiente imagen se muestra una implementación de usuario móvil con tres conexiones de servicio y tres bloques de direcciones IP diferentes especificados para el Grupo de direcciones IP de usuarios móviles: `192.168.64.0/20` para la región de **Asia, Australia y Japón**, `192.168.72.0/20` para la región de **África, Europa y Oriente Medio** y `192.168.48.0/20` para la región de **América del Norte y América del Sur**. Prisma Access divide estas rutas en un bloque de /24 y las anuncia con un Número de AS de **65534**, sino que también añade los valores de la comunidad BGP a los anuncios (**Z** para Asia, **Y** para la UE, y **X** para EE. UU.). Esas rutas se muestran en el centro de la imagen. De esta manera, puede diferenciar las conexiones de servicio en su red, aunque Prisma Access les asigna el mismo número de AS.



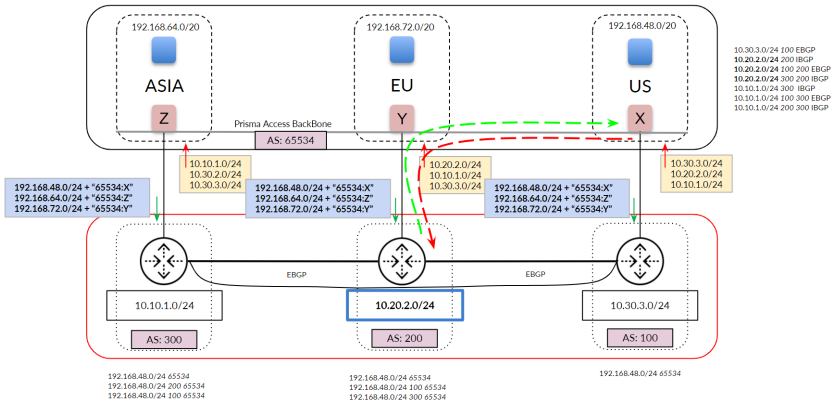
Para ver la cadena de comunidad, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **Show BGP Status (Mostrar estado de BGP)** y encuentre el campo **Community (Comunidad)** en la pestaña **Peer (Par)**.

 ©2025 Palo Alto Networks, Inc.



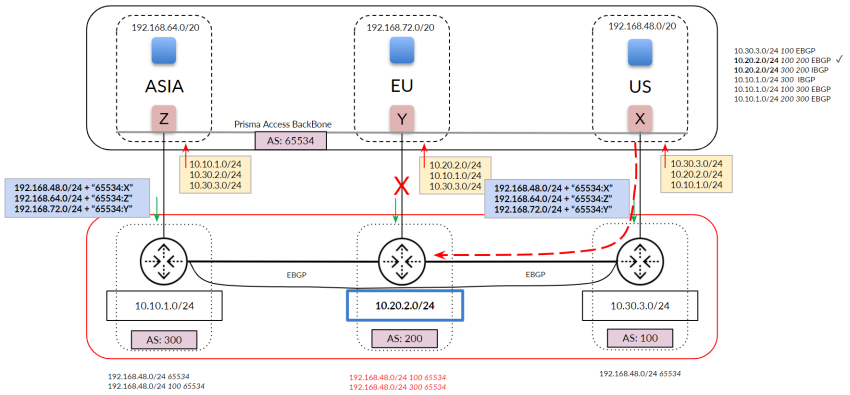
En la siguiente imagen se muestra una red más común con una red troncal eBGP de malla completa. En la imagen se muestran las rutas que Prisma Access ha aprendido de la red de su organización en la parte superior derecha. Tenga en cuenta las rutas adicionales que Prisma Access ha aprendido a través de la red troncal de Prisma Access (iBGP) y la red troncal de su organización (eBGP).

Para el tráfico entre usuarios móviles en la región de **North America & South America (América del Norte y América del Sur)** (EE. UU. en el diagrama) y el centro de datos de la región **Africa, Europe & Middle East (África, Europa y Oriente Medio)** (UE en el diagrama), Prisma Access selecciona la ruta a través de la conexión de servicio de la UE porque prefiere rutas con un AS-PATH más corto.



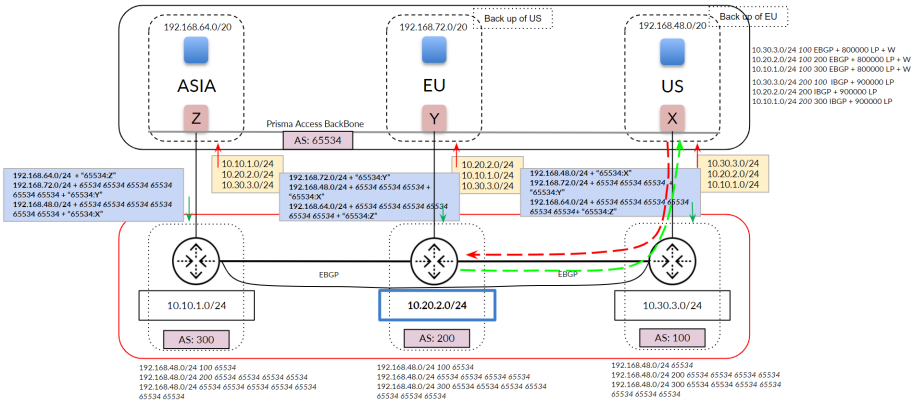
En implementaciones con una red troncal eBGP de malla completa, puede surgir asimetría cuando Prisma Access no puede llegar a un centro de datos en particular debido a un fallo de ISP/CPE en el centro de datos del cliente. La siguiente imagen muestra lo que podría suceder cuando el enlace a la conexión de servicio de la UE se cae. La red detecta el error de enlace y crea una nueva tabla de rutas para AS 200. El tráfico desde la conexión de servicio en EE. UU. hacia AS 200 utiliza la ruta a través de AS 100 porque la ruta eBGP para su red troncal entre AS 200 y AS 100 tiene prioridad sobre la ruta iBGP entre las conexiones de servicio en la UE y EE. UU. Sin embargo, el tráfico de retorno no está garantizado a través de la misma ruta porque el CPE local puede elegir cualquiera de las rutas (que se muestra en rojo) para devolver el tráfico.

 ©2025 Palo Alto Networks, Inc.



Los ejemplos anteriores muestran una red cuyas rutas no se han añadido (es decir, no ha realizado el resumen de rutas antes de enviar los anuncios de ruta BGP a Prisma Access). En el ejemplo siguiente se muestra una red que resume sus rutas a 10.0.0.0/8 antes de enviarlas a Prisma Access. Si selecciona el enrutamiento predeterminado, esta configuración puede provocar problemas de enrutamiento asimétrico, ya que Prisma Access no se puede determinar la ruta de retorno correcta a partir de las rutas resumidas.

Si su implementación de Prisma Access tiene redes remotas, Palo Alto Networks no recomienda el uso de resumen de rutas en conexiones de servicio. El resumen de rutas en las conexiones de servicio es solo para implementaciones de usuarios móviles.



Si usa la agregación de rutas para usuarios móviles, le recomendamos encarecidamente que habilite el enrutamiento hot potato en lugar del enrutamiento predeterminado, donde Prisma Access entrega el tráfico lo más rápido posible a la red de su organización; además, le recomendamos que seleccione una **Backup SC (SC de copia de seguridad)** como se describe en la siguiente sección para que cada conexión de servicio tenga un comportamiento de enrutamiento determinista.

Enrutamiento hot potato de Prisma Access

Cuando selecciona **Hot Potato Routing (Enrutamiento hot potato)**, Prisma Access egresa el tráfico destinado a conexiones de servicio/centros de datos de su red interna lo más rápido posible.

Con el enrutamiento hot potato, Prisma Access antepone la ruta AS (AS-PATH) a los anuncios de prefijo BGP enviados desde las puertas de enlace. Esta anteposición se realiza cuando los prefijos se anuncian fuera de la conexión de servicio al CPE local de su organización. Prisma Access antepone los AS-PATH para que su CPE dé la preferencia correcta a los túneles primario

 ©2025 Palo Alto Networks, Inc.

y secundario, de modo que si el túnel primario deja de funcionar, su CPE elige el túnel secundario como respaldo.

Si especificó una dirección IP diferente para el par BGP secundario (de respaldo), Prisma Access añade más prefijos según el tipo de túnel, como se muestra en la siguiente tabla.

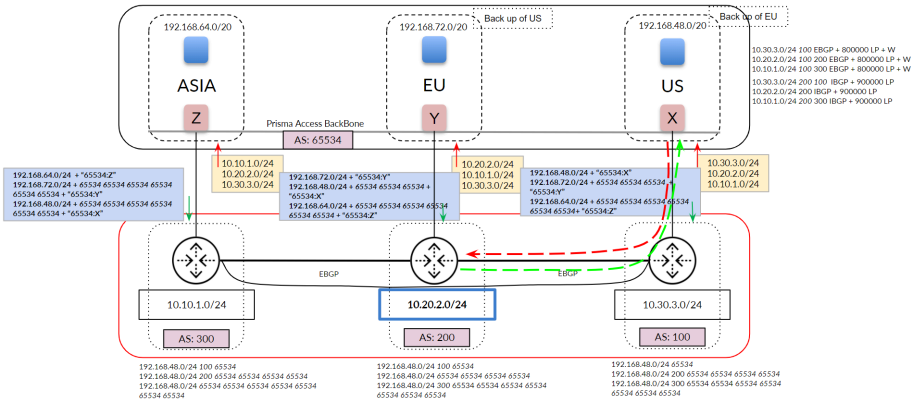
Tipo de prefijo	Tipo de túnel de conexión de servicio	Número de anteposiciones de As-Path	Número total de AS-PATH observados en el CPE
Prefijos de puerta de enlace de la conexión del servicio principal	Túnel primario o secundario con la misma dirección IP del peer de BGP	0	1
Prefijos de puerta de enlace de la conexión del servicio de copia de seguridad	Túnel primario o secundario con la misma dirección IP del peer de BGP	3	4
Prefijos de puerta de enlace de todas las demás conexiones de servicio	Túnel primario o secundario con la misma dirección IP del peer de BGP	6	7
Prefijos de puerta de enlace de la conexión del servicio principal	Túnel secundario con una dirección IP de peer BGP diferente	1	2
Prefijos de puerta de enlace de la conexión del servicio de copia de seguridad	Túnel secundario con una dirección IP de peer BGP diferente	4	5
Prefijos de puerta de enlace de todas las demás conexiones de servicio	Túnel secundario con una dirección IP de peer BGP diferente	7	8

En el modo de enrutamiento hot potato, Prisma Access le permite especificar una conexión de servicio de respaldo durante la incorporación. Al especificar un **Backup SC (SC de respaldo)**, se informa a Prisma Access para que utilice esa conexión de servicio como respaldo cuando falla un enlace de conexión de servicio.

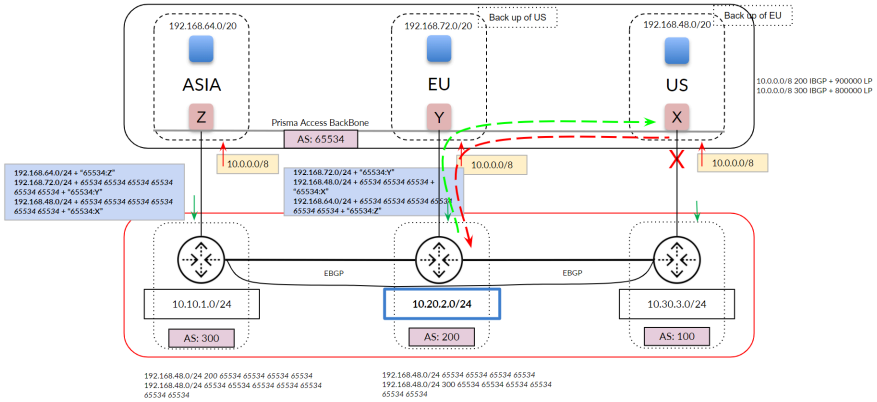
La siguiente imagen muestra una configuración de enrutamiento hot potato para el tráfico entre la conexión de servicio de EE. UU. y AS 200, con la conexión de servicio de la UE configurada como **Backup SC (Copia de seguridad de SC)** de la conexión de EE. UU. Usando el enrutamiento hot potato, Prisma Access envía el tráfico desde su ruta de salida más cercana a través de la conexión de servicio de EE. UU. El tráfico de retorno toma la misma ruta a través de AS100 porque esta ruta tiene un AS-PATH más corto hacia el grupo de usuarios móviles en la ubicación de EE. UU.

 ©2025 Palo Alto Networks, Inc.

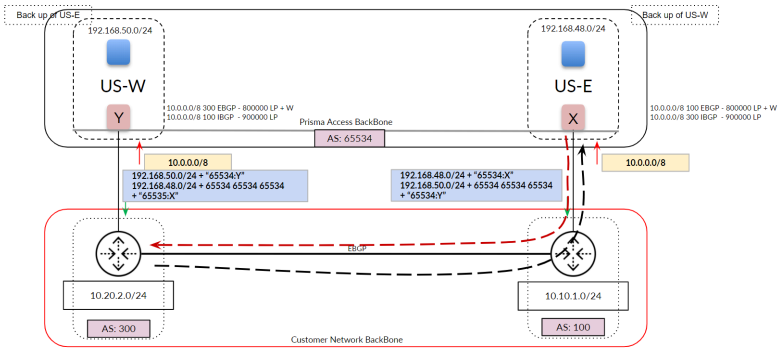
Prisma Access antepone AS-PATH a sus anuncios de prefijo dependiendo de si el túnel es un túnel principal, un túnel de respaldo o no se utiliza ni como túnel principal ni como túnel de respaldo.



Debido a que ha configurado una conexión de servicio de respaldo, si el enlace a la conexión de servicio de EE. UU. deja de funcionar, el enrutamiento hot potato envía el tráfico utilizando su ruta más corta a través de la conexión de servicio de la UE. Este escenario de enrutamiento también se aplica a las redes que utilizan agregación de rutas.



También puede utilizar conexiones de servicio de respaldo para múltiples conexiones de servicio en una sola región. La siguiente imagen muestra una implementación de Prisma Access con dos conexiones de servicio en la región de América del Norte. En este caso, se especifica un **Backup SC (SC de respaldo)** de US-E para la conexión de servicio US-W, y viceversa, para garantizar un enrutamiento simétrico.



 ©2025 Palo Alto Networks, Inc.

Configurar preferencias de enrutamiento

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

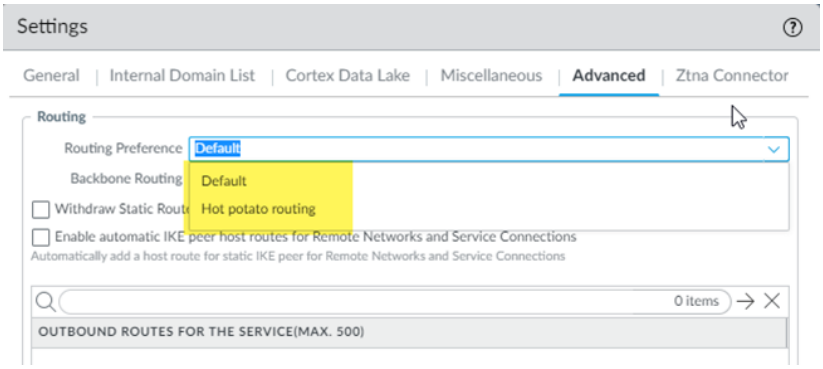
Para habilitar las preferencias de enrutamiento, complete los siguientes pasos.

Para configurar estas preferencias de enrutamiento, debe utilizar el enrutamiento BGP y no el enrutamiento estático para sus conexiones de servicio.

STEP 1 | Configurar su conexión de servicio.

STEP 2 | (Opcional) Seleccione la ruta a utilizar para sus conexiones de servicio.

1. Desde el Panorama que gestiona Prisma Access, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicio)** y haga clic en el icono de engranaje para editar la **Settings (Configuración)**.
2. En la configuración **Advanced (Avanzada)**, seleccione su **Routing Preference (Preferencia de enrutamiento)** [ya sea **Default (Predeterminada)** o **Hot Potato**].



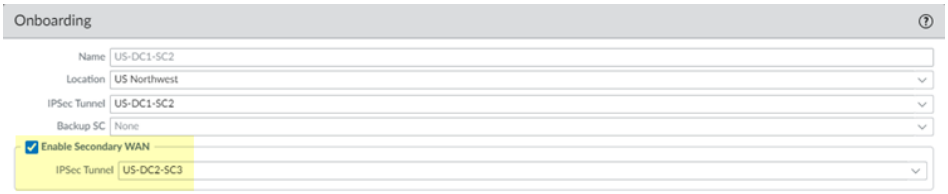
STEP 3 | (Opcional, solo implementaciones de enrutamiento Hot Potato) Para especificar una conexión de servicio preferida que se utilice si un enlace falla, configure un **Backup SC (SC de respaldo)** cuando configure una conexión de servicio.

Puede seleccionar cualquier conexión de servicio que ya haya agregado. Prisma Access utiliza el **Backup SC (SC de copia de seguridad)** que seleccione como la conexión de servicio preferida en caso de un fallo en el enlace. La selección de una conexión de servicio de respaldo puede evitar problemas de enrutamiento asimétrico si ha incorporado más de dos conexiones de servicio. Esta opción está disponible en el modo de ruta de hot potato únicamente.

1. Vaya a **Panorama** > **Cloud Service (Servicio en la nube)** > **Configuration (Configuración)** > **Service Connection (Conexión de servicio)**
2. Seleccione la conexión de servicio que desea configurar o seleccione **Add (Añadir)** para añadir una nueva.

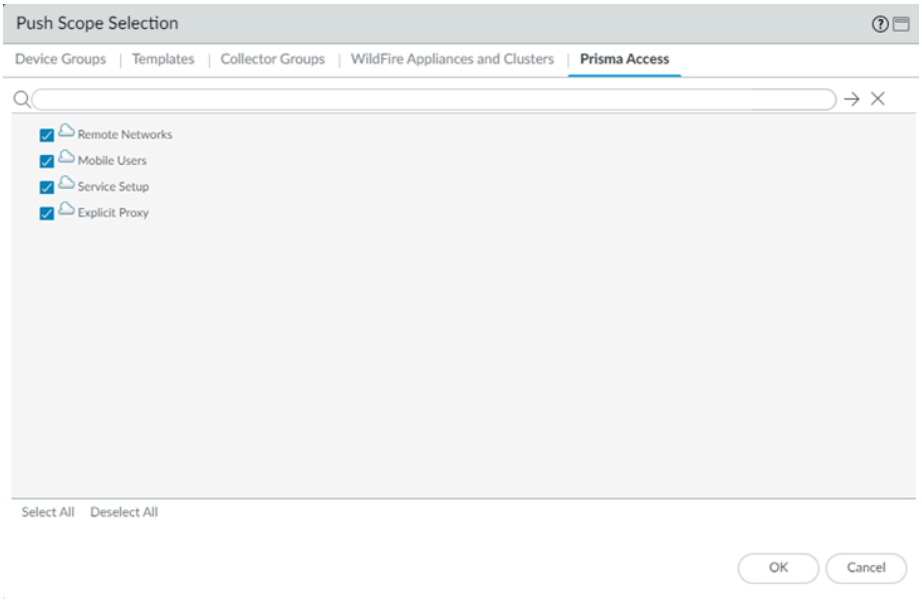
 ©2025 Palo Alto Networks, Inc.

3. Seleccione una conexión de servicio para usar como la copia de seguridad preferida [**Backup SC (Copia de seguridad SC)**)].



STEP 4 | Compruebe sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. **Edit Selections (Editar selecciones)** y, en la pestaña Prisma Access, asegúrese de que **Service Setup (Configuración del servicio)** esté seleccionada en el **Push Scope (Ámbito de envío)**, luego haga clic en **OK (Aceptar)**.

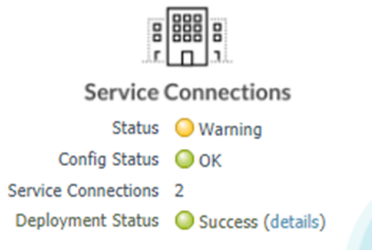


3. Haga clic en **Commit and Push (Confirmar y enviar)**.

 ©2025 Palo Alto Networks, Inc.

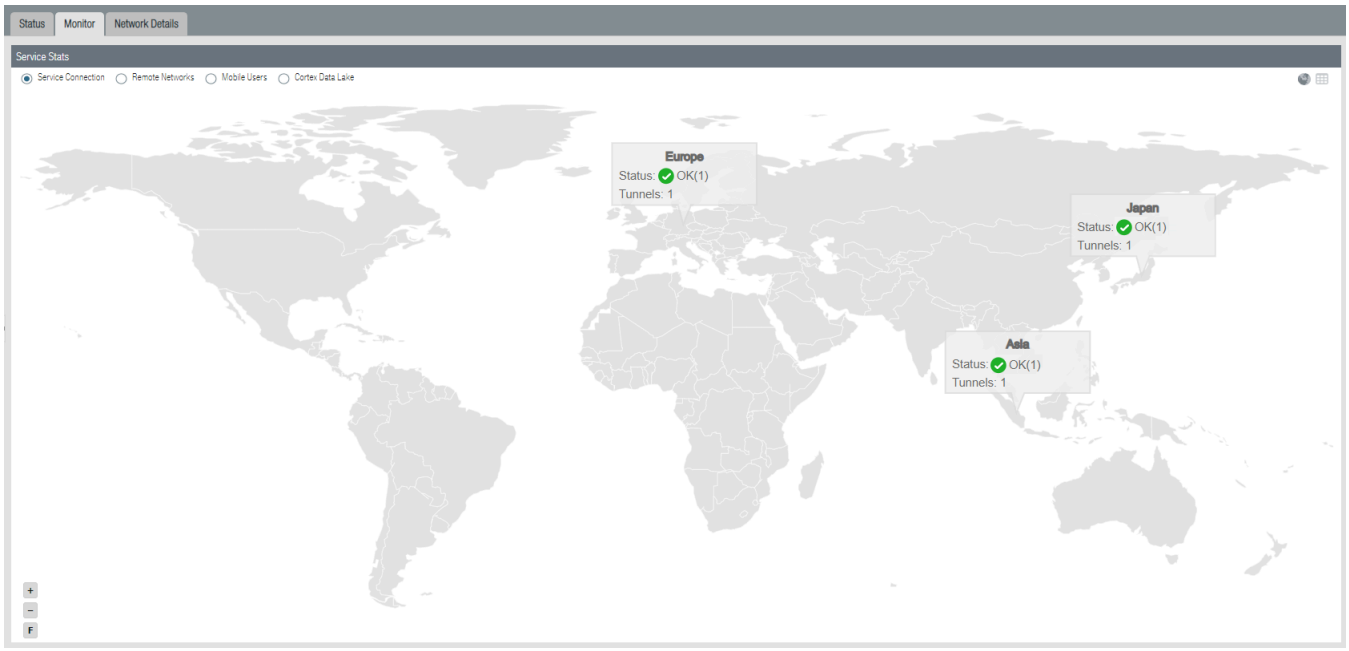
STEP 5 | Verifica que tu conexión de servicio esté activa seleccionando **Panorama > Cloud Services > Status > Status (Panorama > Servicios en la nube > Estado > Estado)** y comprobando que su estado sea **OK (Aceptar)**.

El área de **Deployment Status (Estado de implementación)** le permite ver el progreso de los trabajos de incorporación y implementación antes de que se completen, así como ver más información sobre el estado de los trabajos completados.



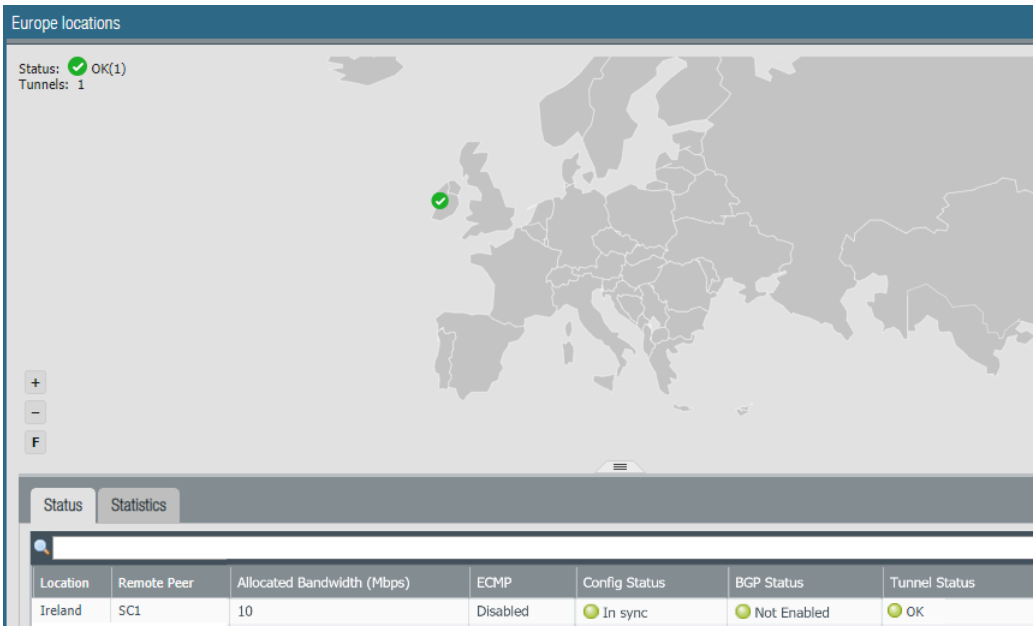
Si el estado no está **OK**, sitúe el cursor sobre el icono Estado para ver cualquier error.

Para ver una representación gráfica de la conexión de servicio junto con los detalles de estado, seleccione **Service Connection (Conexión de servicio)** en la pestaña **Monitor (Supervisar)**.



Seleccione una región para obtener más detalles sobre esa región.

 ©2025 Palo Alto Networks, Inc.



Haga clic en las pestañas debajo del mapa para ver información adicional sobre las conexiones de servicio.

Pestaña **Status (Estado)**:

- **Location (Ubicación)**: la ubicación donde se implementa su conexión de servicio.
- **Remote Peer (Peer remoto)**: la ubicación corporativa a la que esta infraestructura de servicio está configurando un túnel IPSec.
- **Allocated Bandwidth (Ancho de banda asignado)**: el número de conexiones de servicio que ha asignado se multiplica por 300 Mbps.

  Este número no refleja el ancho de banda de conexión de servicio disponible.

  Si bien cada conexión de servicio proporciona aproximadamente 1 Gbps de rendimiento, el rendimiento real depende de varios factores, incluidos:

  - *Mezcla de tráfico (por ejemplo, tamaño de trama)*
  - *Latencia y pérdida de paquetes entre la conexión de servicio y la ubicación de la sede o el centro de datos*
  - *Límites de rendimiento del proveedor de servicios*
  - *Límites de rendimiento del dispositivo de terminación de cliente*
  - *Otro tráfico del centro de datos del cliente*
- **ECMP**: si tiene configurada la ruta múltiple de igual coste (ECMP) para esta conexión de servicio. Dado que ECMP no se utiliza para conexiones de servicio, este estado está **Disabled (Deshabilitado)**.

 ©2025 Palo Alto Networks, Inc.

- **Config Status (Estado de configuración)**: el estado de su último envío de configuración al servicio. Si la configuración local y la configuración en la nube coinciden, el Estado de configuración es **In sync (Sincronizado)**. Si ha realizado un cambio localmente y aún no ha enviado la configuración a la nube, es posible que se muestre el estado **Out of sync (Fuera de sincronización)**. Pase el cursor sobre el indicador de estado para obtener información más detallada. Después de confirmar y enviar la configuración a Prisma Access, el estado de configuración cambia a **In sync (Sincronizado)**.
- **BGP Status (Estado de BGP)**: muestra información sobre el estado de BGP entre el cortafuegos o enrutador en su ubicación corporativa/sede y Prisma Access donde se establece la conexión de servicio. Aunque es posible que vea pasar temporalmente el estado a través de los diversos estados de BGP [**idle (inactivo)**, **active (activo)**, **open send (abrir envío)**, **open pend (abrir pendiente)**, **open confirm (abrir confirmación)**], lo más común es que el estado de BGP muestre:
  - **Connect (Conectar)**: el enrutador de su centro de datos/sede está tratando de establecer la relación de peers BGP con Prisma Access.
  - **Established (Establecido)**: se ha establecido la relación entre pares BGP.

  Este campo también mostrará si la conexión BGP está en un estado de error:
  - **Advertencia**: no se ha actualizado el estado del BGP en más de ocho minutos. Esto puede indicar un corte en el cortafuegos.
  - **Error**: se desconoce el estado de BGP.
- **Tunnel Status (Estado del túnel)**: estado operativo de la conexión entre Prisma Access y su conexión de servicio.

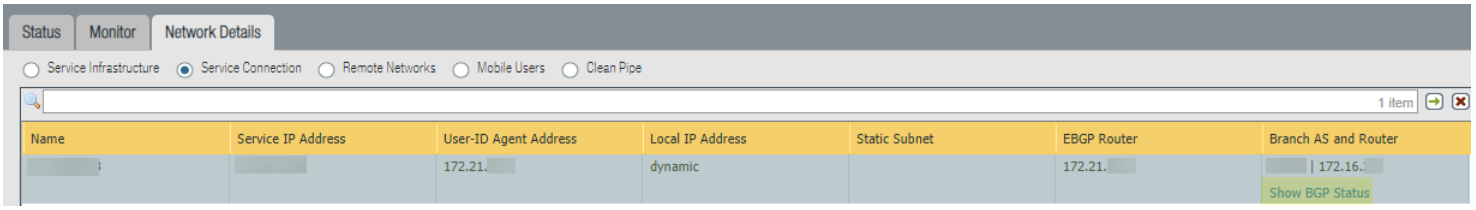
Pestaña **Statistics (Estadísticas)**

- **Location (Ubicación)**: la ubicación donde se implementa su conexión de servicio.
- **Remote Peer (Peer remoto)**: la ubicación corporativa a la que la conexión de servicio está configurando un túnel IPSec.
- **Ingress Bandwidth (Mbps) [Ancho de banda de entrada (Mbps)]**: el ancho de banda desde la ubicación del centro de datos hasta Prisma Access.
- **Ingress Peak Bandwidth (Mbps) [Ancho de banda máximo de entrada (Mbps)]**: la carga máxima desde la ubicación de la sede/centro de datos hacia el servicio en la nube.
- **Egress Bandwidth (Mbps) [Ancho de banda de salida (Mbps)]**: el ancho de banda de Prisma Access a la ubicación de la sede / centro de datos.
- **Egress Peak Bandwidth (Mbps) (Ancho de banda de salida (Mbps) pico**: la carga máxima desde Prisma Access hasta la ubicación de la sede o centro de datos.
- **QoS**: seleccione este botón para mostrar un gráfico que muestra estadísticas de QoS en tiempo real e históricas, incluyendo el número de paquetes perdidos por clase. Este gráfico

 ©2025 Palo Alto Networks, Inc.

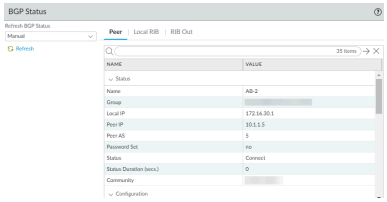
se muestra solo para conexiones de servicio o conexiones de red remotas que tengan habilitada la QoS.

Si has configurado BGP, puede comprobar su estado seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **Show BGP Status (Mostrar estado de BGP)**.



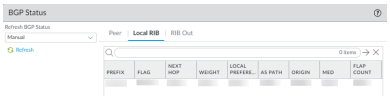
Se muestra el cuadro de diálogo Estado de BGP. Esta tabla le proporciona la siguiente información:

- **Peer**: información de enrutamiento para el peer de BGP, incluido el estado, el número total de rutas, la configuración y las estadísticas y contadores de tiempo de ejecución. El número total de rutas que se muestran en el área **bgpAfiIpv4-unicast Counters (Contadores de bgpAfiIpv4-unicast**, en los campos **Incoming Total (Total entrante)** y **Outgoing Total (Total saliente)**.



- **RIB local**: rutas BGP que Prisma Access utiliza localmente. Prisma Access selecciona esta información de la tabla BGP RIB-In, que almacena la información enviada por los dispositivos de red vecinos, aplica políticas de importación y decisiones de enrutamiento locales de BGP y almacena la información de RIB local en la base de información de enrutamiento (RIB).

  Tenga en cuenta que solo se muestran las primeras 256 entradas. Para ver entradas adicionales, introduzca una subred o dirección IP en el campo de Filtro y haga clic en Aplicar filtro para ver un subconjunto de las entradas de enrutamiento hasta un máximo de 256.



- **Salida de RIB**: información de enrutamiento que Prisma Access anuncia a sus peers a través de mensajes de actualización BGP.

Cree una red de gran ancho de banda utilizando múltiples conexiones de servicio

Si tiene una sede central o un centro de datos que requiere ancho de banda de conexión de servicio adicional, puede configurar múltiples conexiones de servicio a esa ubicación.

Cada conexión de servicio de Prisma Access no tiene límite de ancho de banda, pero Palo Alto Networks espera que cada conexión de servicio pueda proporcionar aproximadamente 1 Gbps

 ©2025 Palo Alto Networks, Inc.

de rendimiento. Si bien este ancho de banda suele ser suficiente para acceder a recursos internos en una sede central o un centro de datos, es posible que tenga una implementación que requiera ancho de banda adicional; por ejemplo, si está alojando una aplicación SaaS interna o privada en un centro de datos.

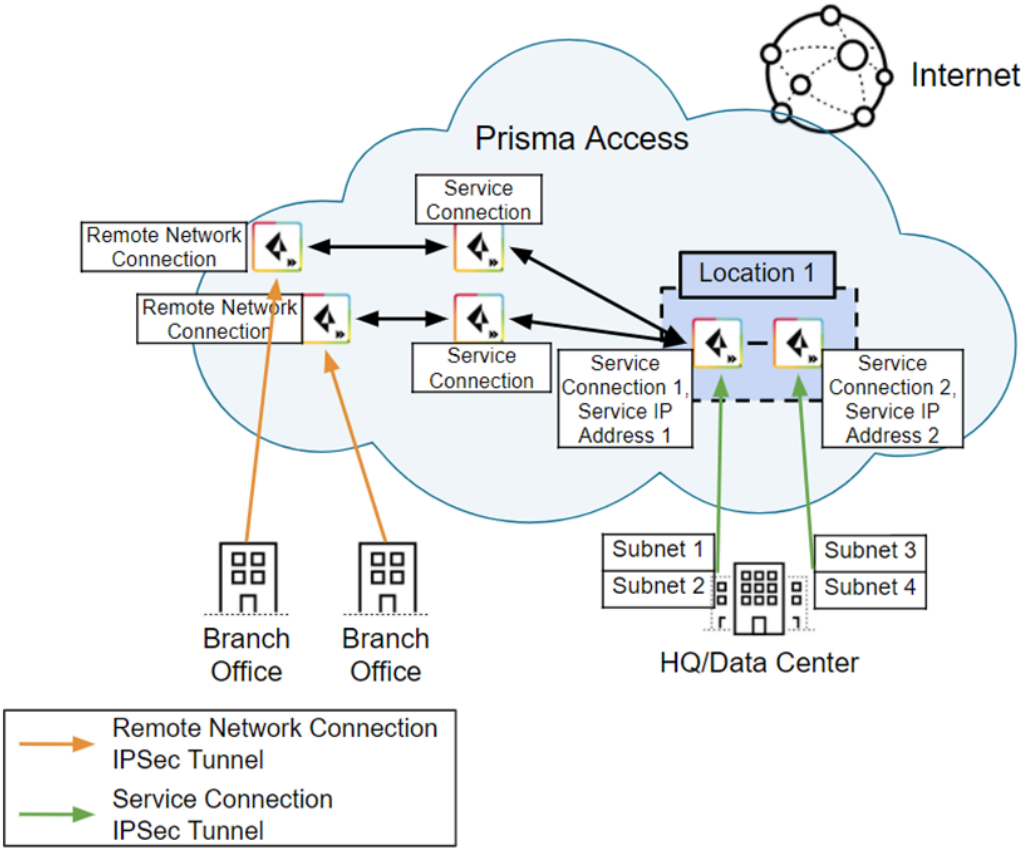
Para crear una conexión de servicio de alto ancho de banda a una sede central o un sitio de centro de datos, debe incorporar el sitio utilizando múltiples conexiones de servicio a la misma ubicación de Prisma Access.

Mientras Prisma Access no limita el número máximo de conexiones de servicio que puede incorporar a una sola ubicación de red remota de la sede o del centro de datos, Palo Alto Networks recomienda no utilizar más de cuatro conexiones de servicio en una implementación de gran ancho de banda. Si necesita más ancho de banda para acceder a aplicaciones internas, utilice ZTNA Connector *o* Colo-Connect *en lugar de múltiples conexiones de servicio.*

El siguiente diagrama muestra una implementación de red remota de Prisma Access con una sede central o un sitio de centro de datos que tiene dos conexiones de servicio desde la misma ubicación de Prisma Access, proporcionando de forma efectiva 2 Gbps de ancho de banda entre el sitio y la ubicación de Prisma Access.

Además de las conexiones de servicio que se implementan para el acceso de gran ancho de banda, el diagrama muestra otro conjunto de conexiones de servicio. Estas conexiones de servicio proporcionan funciones de enrutamiento normales para Prisma Access (en este diagrama, proporcionan acceso de enrutamiento interno entre las conexiones de red remotas y las conexiones de servicio de alto ancho de banda). Palo Alto Networks recomienda que, al implementar una conexión de alto ancho de banda, reserve conexiones de servicio para brindar acceso al recurso en la sede central o en el centro de datos únicamente, e implemente conexiones de servicio adicionales para usar en el enrutamiento interno entre redes remotas, usuarios móviles y los recursos en el centro de datos.

 ©2025 Palo Alto Networks, Inc.



Cada conexión de servicio está activa y tiene su propia **Service IP Address (Dirección IP de servicio)** ; usted utiliza esa dirección para finalizar el túnel IPSec para cada conexión de servicio.

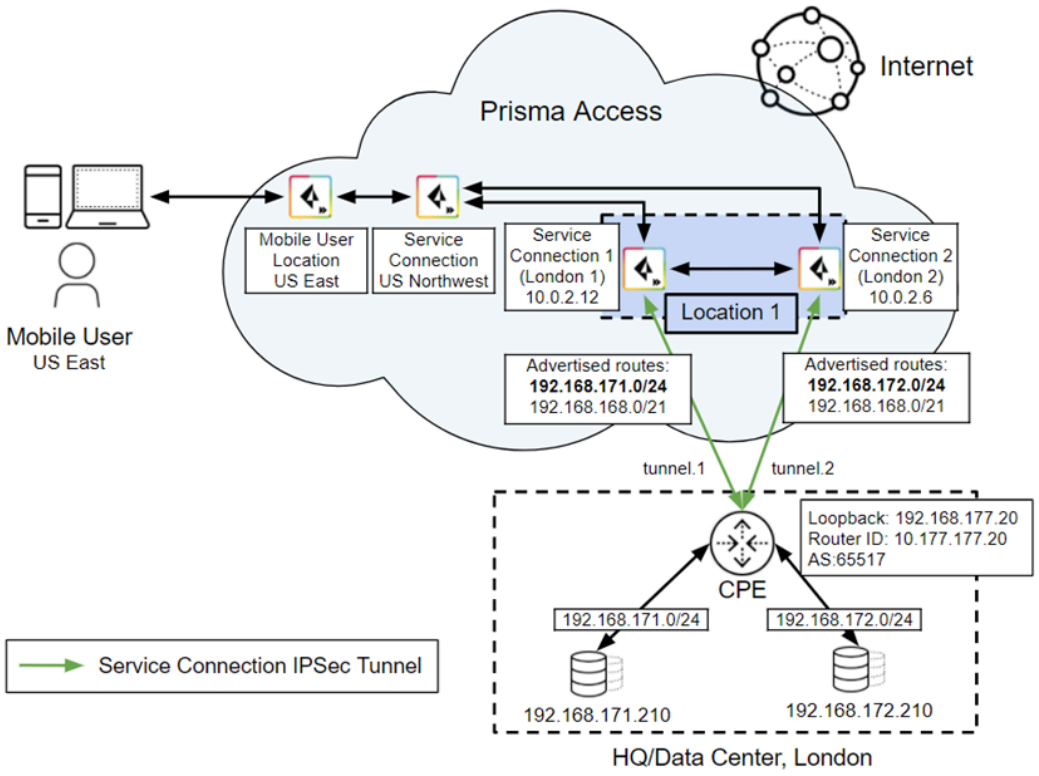
Crear una conexión de gran ancho de banda a una sede o ubicación de centro de datos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para configurar varias conexiones de servicio a una sola sede o ubicación de centro de datos, complete los siguientes pasos.

Los pasos de esta sección utilizan un ejemplo de implementación como se muestra en el siguiente diagrama. En este ejemplo, la sede central de Londres se conecta a dos conexiones de servicio diferentes (Londres 1 y Londres 2) mediante dos túneles IPSec diferentes que terminan en dos interfaces de equipos de las instalaciones del cliente (CPE) diferentes (túnel. 1 y túnel. 2).

 ©2025 Palo Alto Networks, Inc.



En este ejemplo y en los pasos de esta sección, utilice un cortafuegos de nueva generación para terminar las conexiones de servicio en el CPE; sin embargo, puede utilizar cualquier CPE que admita enrutamiento simétrico y PBF o enrutamiento basado en políticas como CPE.

Utilice estos pasos como orientación; cada caso de uso podría requerir un diseño y planificación adicionales que están fuera del alcance de este documento.

STEP 1 | Antes de implementar varias conexiones de servicio desde una sola ubicación de Prisma Access a un solo sitio, asegúrese de que su red tenga los siguientes requisitos previos:

- Debe dividir las subredes en la sede o en la ubicación del centro de datos, y anunciar una subred única en cada conexión de servicio.
- El equipo de las instalaciones de su cliente (CPE) debe dar soporte y usted debe poder configurar las siguientes características de red:
  - Reenvío basado en políticas (PBF) o enrutamiento basado en políticas: su CPE debe poder elegir selectivamente una ruta específica para una dirección IP y una subred de origen local específicas.
  - Retorno simétrico: debe poder configurar su CPE para garantizar flujos de tráfico simétricos hacia y desde una dirección IP y subred específicas, y configurar el retorno simétrico para túneles de conmutación por error si uno de los túneles se cae.

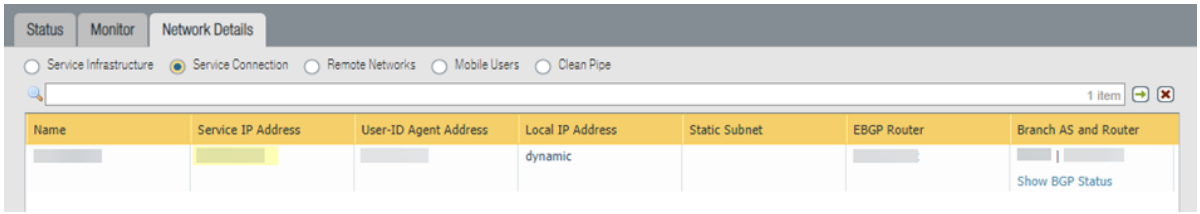
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Cree las conexiones de servicio y establezca conectividad para los túneles IPSec utilizados para las conexiones de servicio.

1. En el Panorama que administra Prisma Access, configure una conexión de servicio, incluida la creación de una nueva configuración de túnel IPSec, puerta de enlace IKE, perfil criptográfico IPSec y ajustes de supervisión de túnel.

   Prisma Access ofrece plantillas IPSec predefinidas que puede utilizar para simplificar el proceso de creación de túneles IPSec.

2. Busque la dirección IP para usar como el sitio remoto del túnel IPSec desde su CPE a Prisma Access seleccionando **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)**, haciendo clic en el botón de radio **Service Connection (Conexión de servicio)** y anotando la **Service IP Address (Dirección IP de servicio)** para el sitio.



3. En su CPE, cree un túnel IPSec a las conexiones de servicio

   1. Compruebe que los túneles IKE e IPSec utilizan los mismos perfiles criptográficos para la autenticación y el cifrado entre peers.
   2. Utilice la **Service IP Address (Dirección IP de servicio)** como el peer dirección IP para el túnel.

   Si utiliza un cortafuegos de nueva generación como CPE, seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** y cree dos túneles para las conexiones de servicio [**tunnel.1 (túnel.1)** y **tunnel.2 (túnel.2)** en la siguiente captura de pantalla).



STEP 3 | Cree la configuración del enrutador virtual para el CPE.

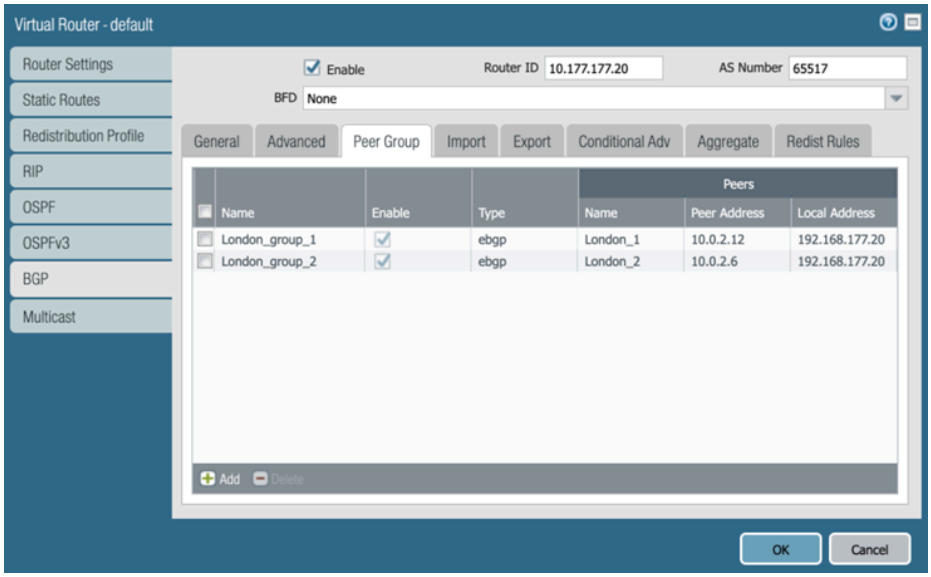
Crea instancias de enrutamiento BGP que anuncian una subred en un túnel y la otra subred en otro túnel, lo que garantiza el equilibrio de carga en los dos túneles activos.

Si está utilizando un cortafuegos de nueva generación como CPE, seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, **Add (Añadir)** ajustes de enrutador virtual y, a

 ©2025 Palo Alto Networks, Inc.

continuación, **Add (Añadir) BGP Peer Group (Grupo de peers)** para cada túnel, especificando los siguientes ajustes:

- Especifique un **Router ID (ID de enrutador)** y un **AS Number (número AS)** del enrutador CPE (10.177.177.20 y 65517, respectivamente, en este ejemplo).
- Especifique la dirección del **Router EBGP (Enrutador EBGP)** de las conexiones de servicio [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **EBGP Router (Enrutador EBGP)**] como **Peer Address (Dirección de pares)** para las conexiones de servicio (10.0.2.12 para Conexión de servicio 1 y 10.0.2.6 para Conexión de servicio 2 en este ejemplo).
- Para la **Local Address (Dirección local)**, puede especificar la dirección de bucle de retorno del CPE (192.168.177.20 en este ejemplo).



STEP 4 | Cree una subred resumida para las direcciones IP utilizadas para ambos túneles.

Proporcionar una subred resumida garantiza la redundancia. Cuando ambos túneles están activos, el tráfico utiliza las rutas más específicas para llegar a su destino; por ejemplo, 192.168.171.0/24 utiliza el túnel.1 para llegar a su destino. Añadir una subred resumida que cubra todas las subredes anunciadas (192.168.168.0/21 en este ejemplo) garantiza que el tráfico de 192.168.171.0/24 sea accesible desde el túnel.2 si el túnel.1 cae y el tráfico de 192.168.172.0/24 sea accesible desde el túnel.1 si el túnel.2 cae.

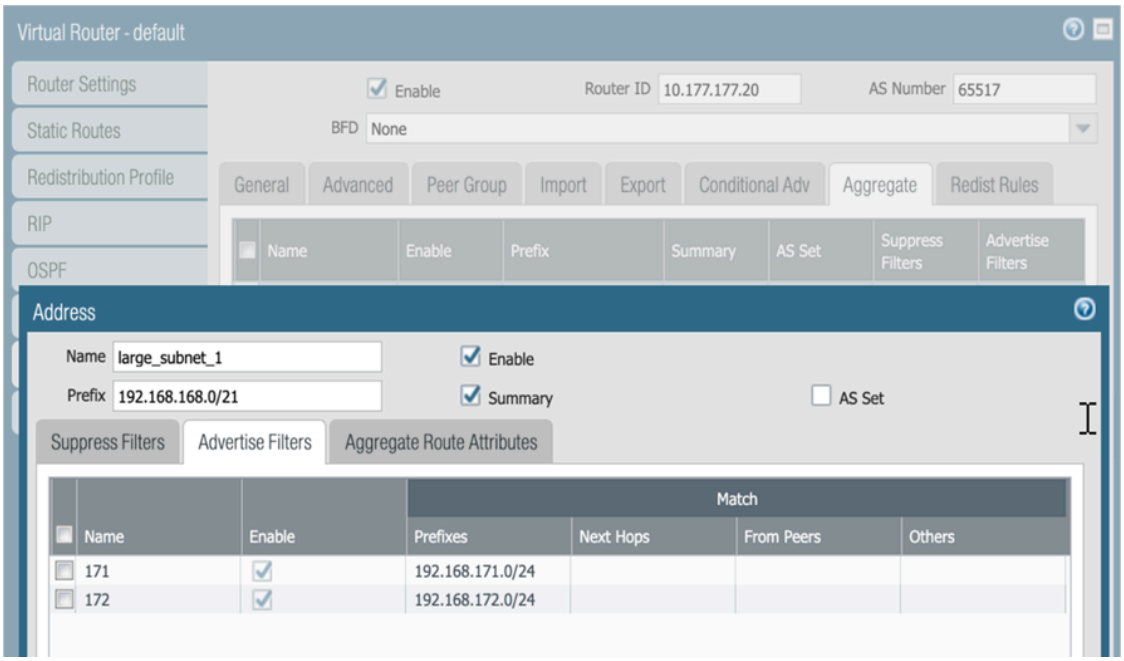
Si está utilizando un cortafuegos de nueva generación como CPE, complete los siguientes pasos.

1. Continúe modificando el perfil del enrutador virtual y seleccione **Add (Añadir)** para añadir parámetros de agregación de rutas [**Network (Red)** > **Virtual Routers(Enrutadores virtuales)** > **BGP** > **Aggregate (Agregado)**].

 ©2025 Palo Alto Networks, Inc.

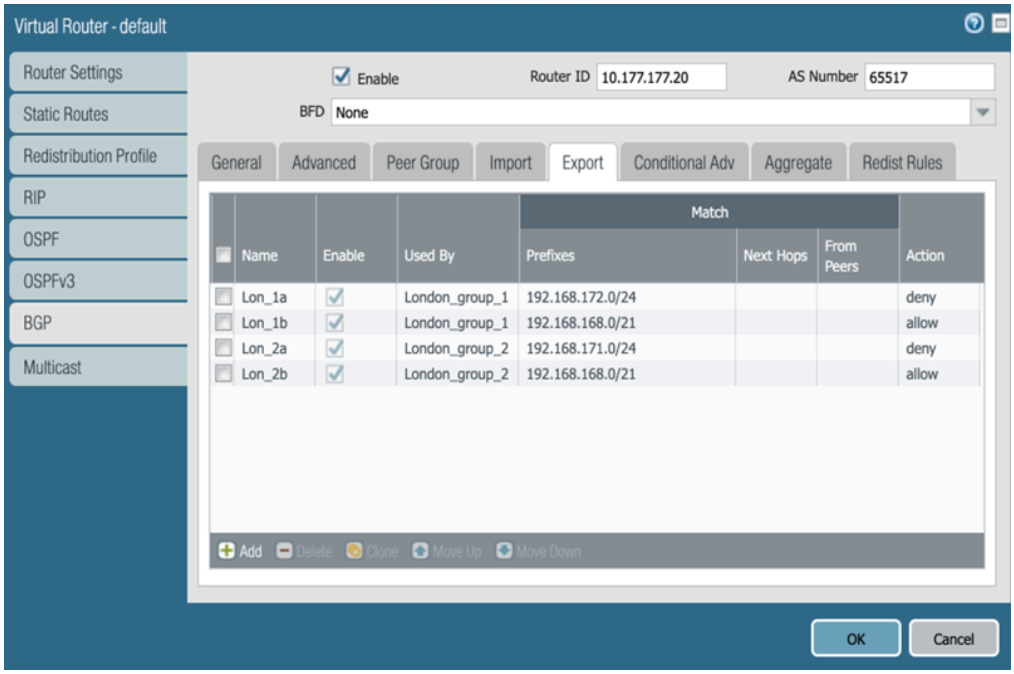
2. Introduzca subredes de resumen para las subredes que está anunciando para las conexiones de servicio.

   En este ejemplo, introduzca un **Prefix (Prefijo)** de **192.168.168.0/21**, que resume las dos subredes del centro de datos.



3. Introduzca la configuración de **Export (Exportar)** para asegurarse de que los túneles anuncian las subredes correctas.

   En este ejemplo, especifica una **Action (Acción)** de **deny (denegación)** y **allow (permitir)** para las subredes, de forma que la primera subred (192.168.171.0/24) sea accesible desde el túnel.1 y la segunda subred (192.168.172.0/24) accesible desde el túnel.2.



 ©2025 Palo Alto Networks, Inc.

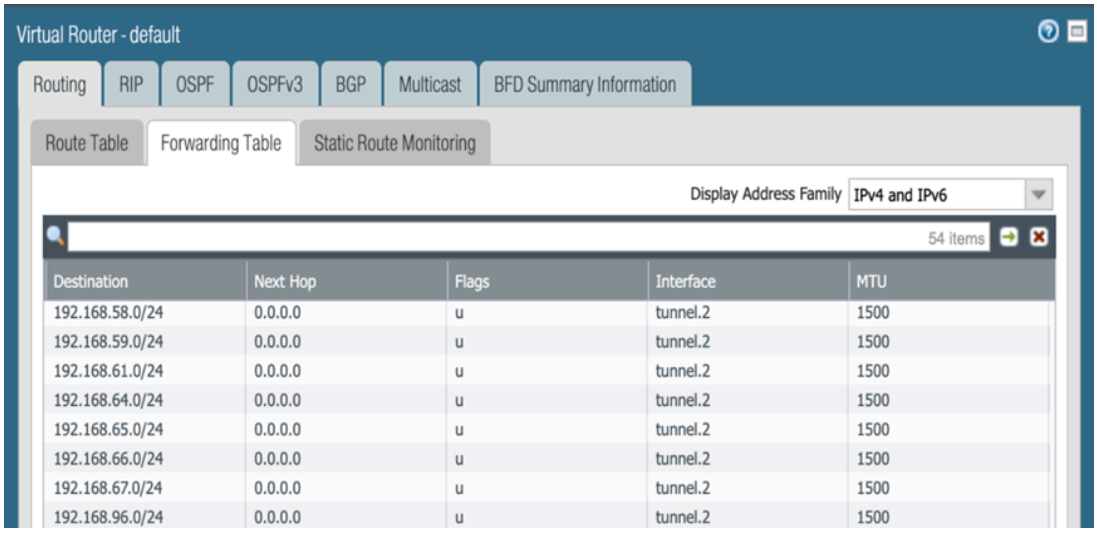
STEP 5 | (Implementaciones con más de dos conexiones de servicio únicamente) Si necesita más de dos conexiones de servicio para conectar a los usuarios a recursos privados con un ancho de banda de más de 2 Gbps, añada prefijos AS-PATH para las rutas exportadas de modo que las conexiones de servicio utilicen un enrutamiento simétrico hacia y desde el centro de datos en caso de una conmutación por error. Consulte Configure más de dos conexiones de servicio a una sede o centro de datos para obtener más detalles.

STEP 6 | Para garantizar un retorno simétrico (para asegurarse de que el tráfico de 192.168.171.0/24 siempre usa túnel.1 y el tráfico de 192.168.172.0 siempre usa túnel.2), introduzca PBF o reglas de enrutamiento basadas en políticas.

De forma predeterminada, BGP instala rutas en la tabla de enrutamiento para todos los destinos diferentes, independientemente del túnel preferido. La siguiente captura de pantalla

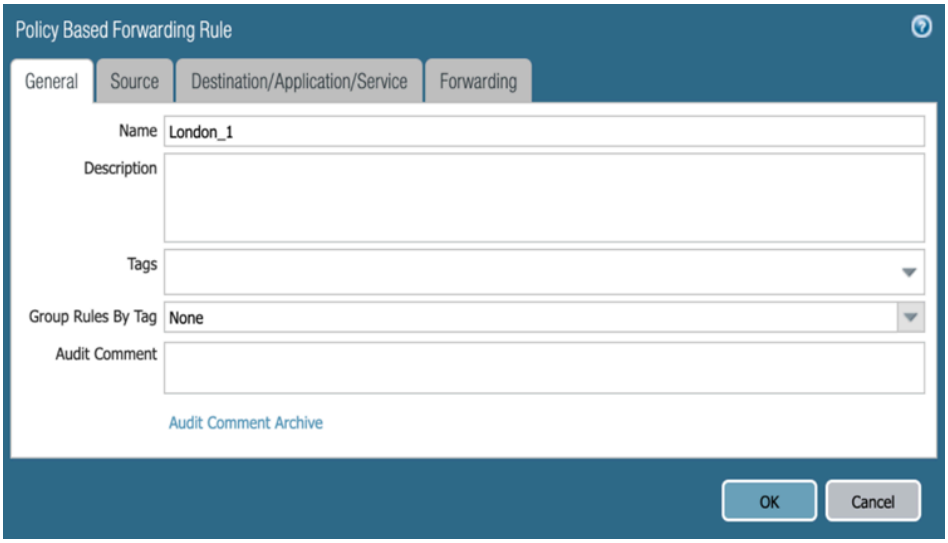
 ©2025 Palo Alto Networks, Inc.

muestra que BGP anuncia todos los destinos de la subred 192.168.168.0/21 para tunnel.2, lo que podría causar enrutamiento asimétrico para el tráfico desde 192.168.171.0/24.



Para garantizar un enrutamiento simétrico, configure un conjunto de reglas de reenvío basadas en rutas o PBF. Si está utilizando un cortafuegos de nueva generación como CPE, complete los siguientes pasos.

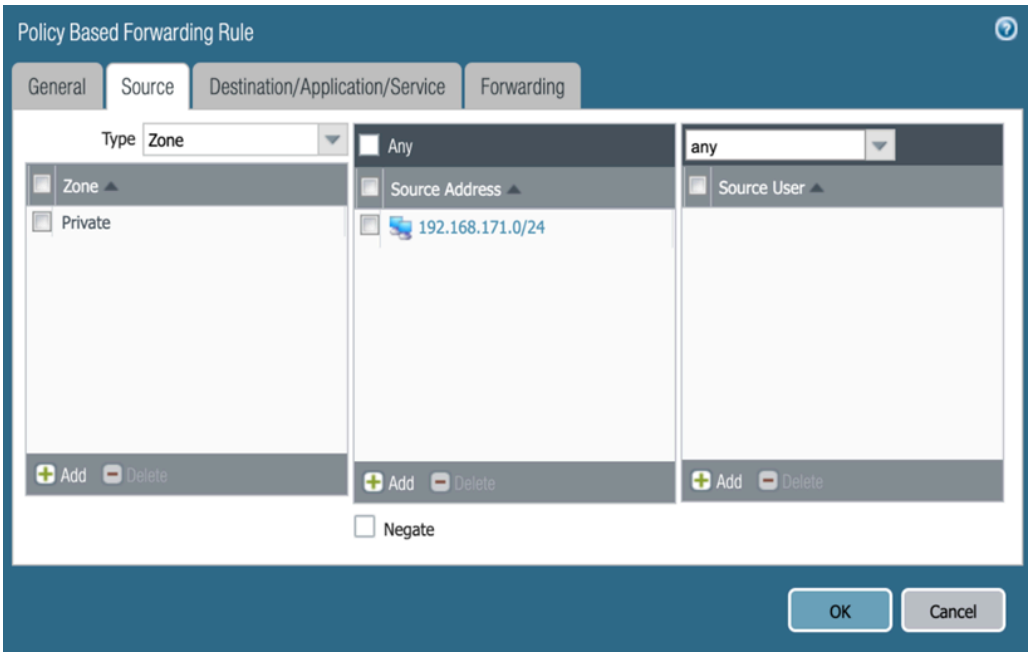
1. Seleccione **Policies (Políticas)** > **Policy Based Forwarding (Reenvío basado en políticas)** y **Add (Añadir)** una regla de políticas PBF.



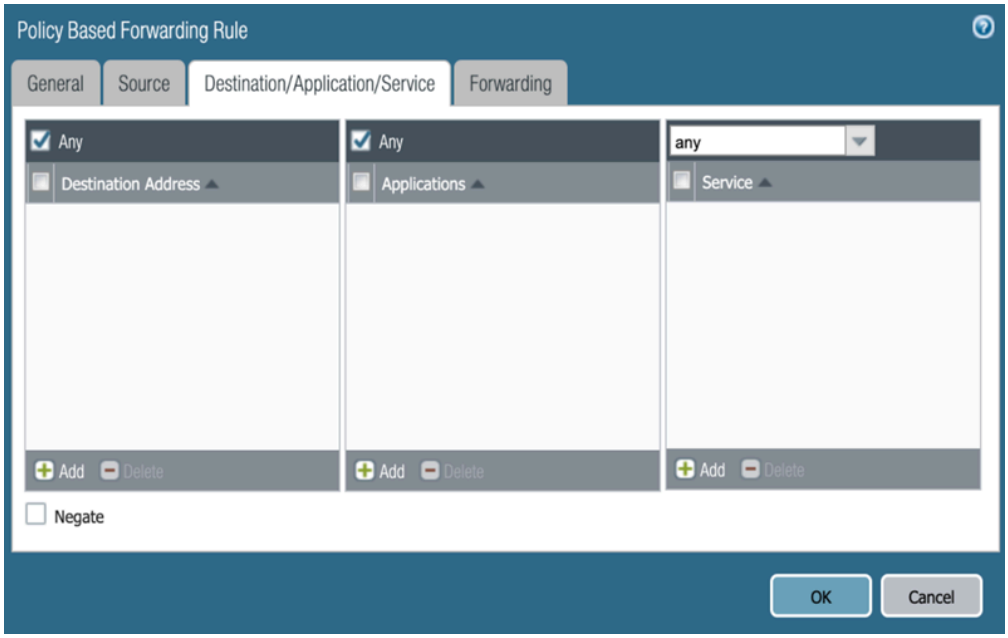
2. Seleccione **Source (Origen)** y **Add (Añadir)** para añadir una **Source Address (Dirección de origen)** para usar en el PBF.

   En este caso, desea crear un PBF para el túnel.1, por lo que introduce la subred 192.168.171.0/24.

 ©2025 Palo Alto Networks, Inc.



3. Seleccione **Destination/Application/Service (Destino/Aplicación/Servicio)** y seleccione **Any (Cualquier)** dirección de destino y **Any (Cualquier)** aplicación.

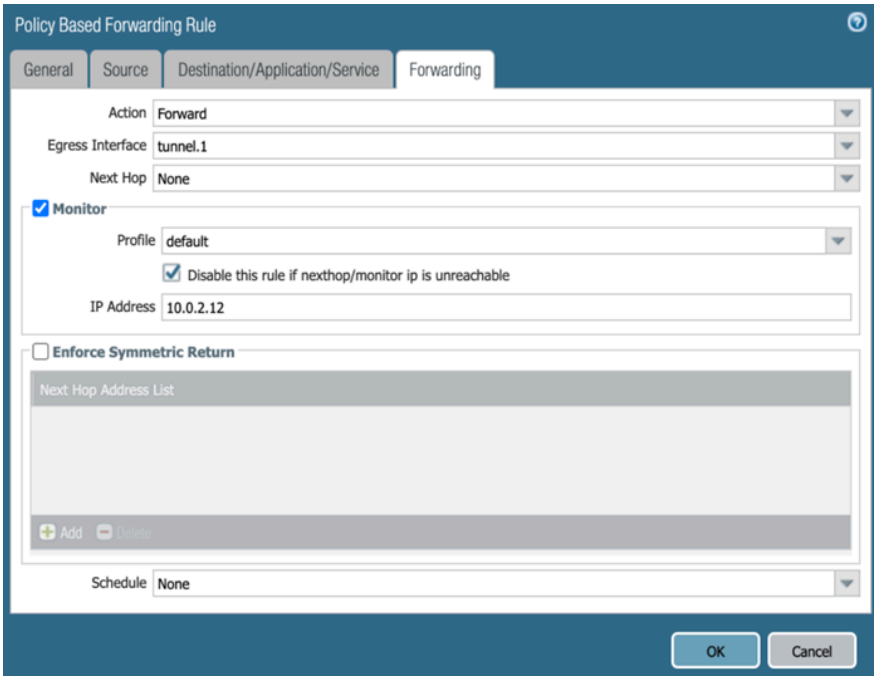


4. Seleccione **Forwarding (Reenvío)** y especifique los siguientes parámetros, luego, haga clic en **OK (Aceptar)**:
   - Seleccione una **Action (Acción)** de **Forward (Reenviar)**.
   - Seleccione una **Egress Interface (Interfaz de salida)** del túnel al que desea reenviar la subred IP [**tunnel.1 (túnel.1)** en este caso].
   - Seleccione **Monitor (Supervisar)** y seleccione los siguientes perfiles de supervisión:
     - Seleccione un **Profile (Perfil)** de **default (predeterminado)**.

 ©2025 Palo Alto Networks, Inc.

- Seleccione **Disable this rule if nexthop/monitor ip is unreachable (Deshabilitar esta regla si no se puede acceder al siguiente salto o la IP de supervisión)**.
- Especifique una **IP Address (Dirección IP)** de la dirección del **Router EBGP (Enrutador EBGP)** de la conexión de servicio [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **Router EBGP (Enrutador EBGP)**].

Activar la supervisión y seleccionar la dirección del enrutador EBGP de la conexión de servicio garantiza que, si el túnel.1 se cae, el cortafuegos deshabilite la política PBF y enrute el tráfico en el túnel que aún está subiendo (túnel.2).



5. Repita el Paso 6, sustituyendo la dirección del **Router EBGP (Enrutador EBGP)** de la Conexión de Servicio 1 por la dirección del **Router EBGP (Enrutador EBGP)** de la Conexión de Servicio 2 y la subred del túnel.1 por la subred del túnel.2.

   Cuando se complete, tiene dos políticas de PBF, una para el túnel.1 y otra para el túnel.2.

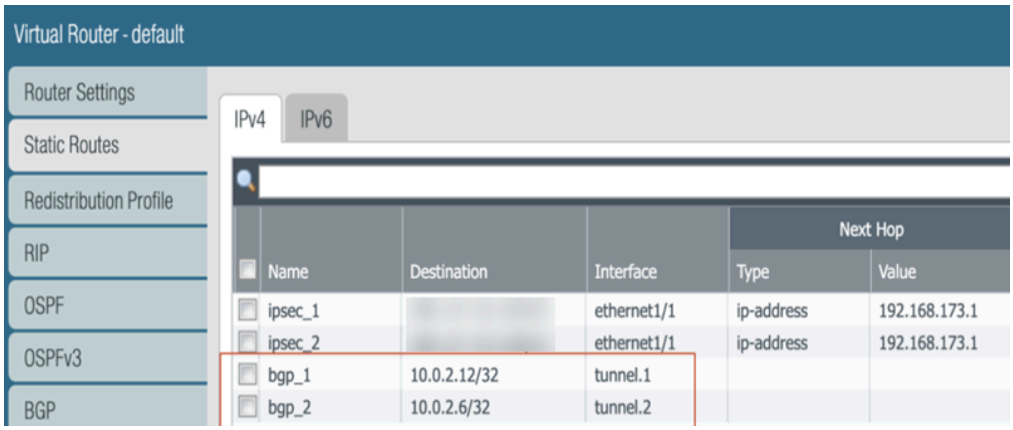


STEP 7 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** > **Static Routes (Rutas estáticas)** y asigne la dirección del **Router EBGP (Enrutador EBGP)** de la Conexión de Servicio 1 a la **Interface (Interfaz)** del **tunnel.1 (túnel.1)**; a continuación, asigne la dirección del **Router EBGP (Enrutador EBGP)** de la Conexión de Servicio 2 a la **Interface (Interfaz)** del **tunnel.2 (túnel.2)**

La introducción de rutas estáticas específicas para cada una de las direcciones BGP del enrutador garantiza que la supervisión del túnel funcione correctamente, ya que la dirección

 ©2025 Palo Alto Networks, Inc.

IP del enrutador EBGP de la conexión de servicio 1 solo se puede acceder por túnel.1 y la dirección IP del enrutador EBGP de la conexión de servicio 2 solo se puede acceder por túnel.2.



Configure más de dos conexiones de servicio a una sede o centro de datos

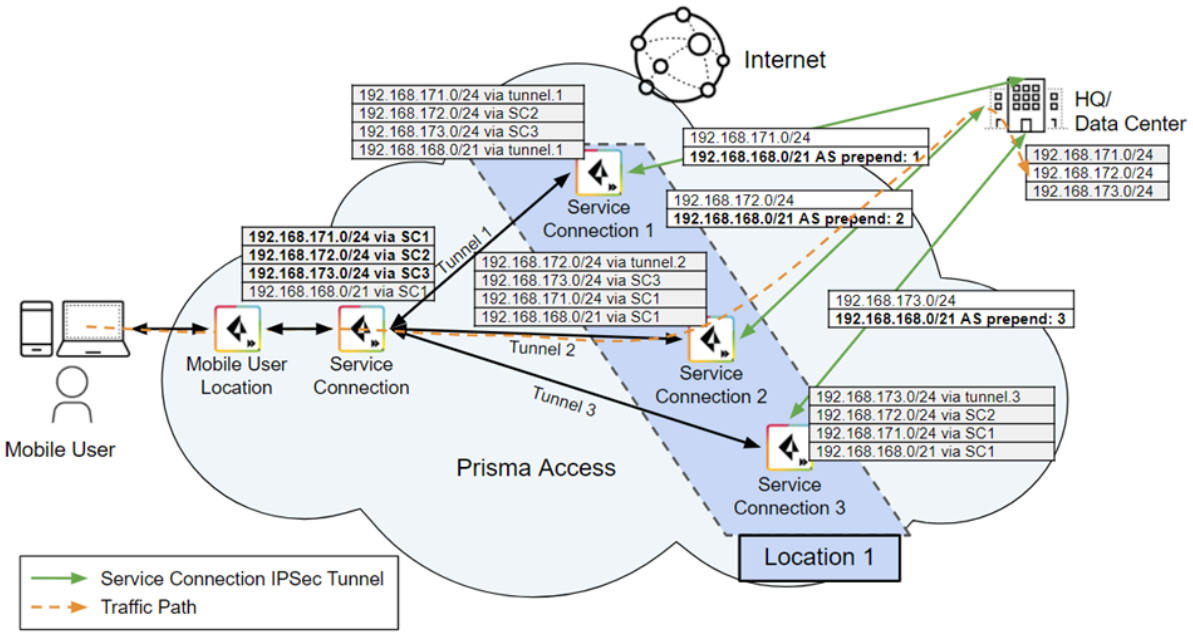
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Cuando utiliza dos túneles para una conexión de servicio de gran ancho de banda, solo queda una ruta de tráfico disponible en caso de fallo del túnel, lo que simplifica la configuración de una ruta de conmutación por error. Si utiliza más de dos conexiones para una conexión de gran ancho de banda, debe realizar una configuración adicional para garantizar un comportamiento coherente para las conmutaciones por error de túnel.

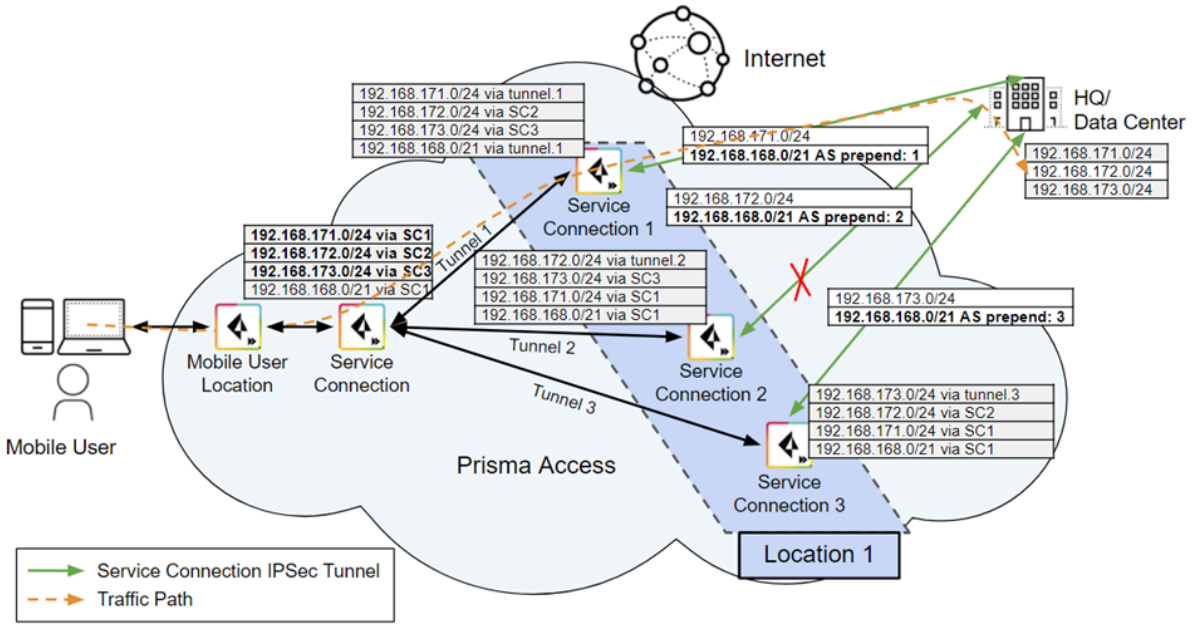
Debido a que utiliza una subred resumida para la conmutación por error de túnel, debe indicar explícitamente el túnel de conexión de servicio que debe utilizar si se produce una conmutación por error. Dado que el enrutamiento BGP elige el número más corto de AS-PATH para una ruta, puede adjuntar AS-PATH a las rutas para que BGP prefiera un túnel en caso de una conmutación por error.

El siguiente ejemplo muestra tablas de enrutamiento para una conexión de servicio de gran ancho de banda utilizando tres conexiones de servicio. Si los tres túneles están activados, Prisma Access utiliza las rutas más específicas para llegar a las subredes en la sede o la ubicación del centro de datos. Dado que el usuario está accediendo a un recurso en la subred 192.168.172.0/24, la conexión de servicio más cercana al usuario móvil comprueba su tabla de enrutamiento y selecciona Túnel 2 como la ruta al recurso del centro de datos.

 ©2025 Palo Alto Networks, Inc.



Si el túnel 2 se cae, la ruta más específica al recurso en la subred 192.168.172.0/24 no está disponible, por lo que la conexión de servicio más cercana al usuario utiliza la subred 192.168.168.0/21 resumida. Ha configurado solo un prefijo AS-PATH para la conexión de servicio 1; por lo tanto, Prisma Access elige Túnel 1 como ruta de conmutación por error porque tiene menos prefijos AS-PATH.

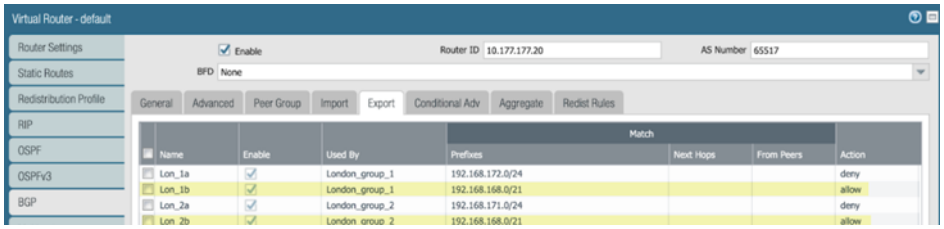


Para añadir prefijos a las rutas si está utilizando un cortafuegos de nueva generación como CPE, complete la siguiente tarea.

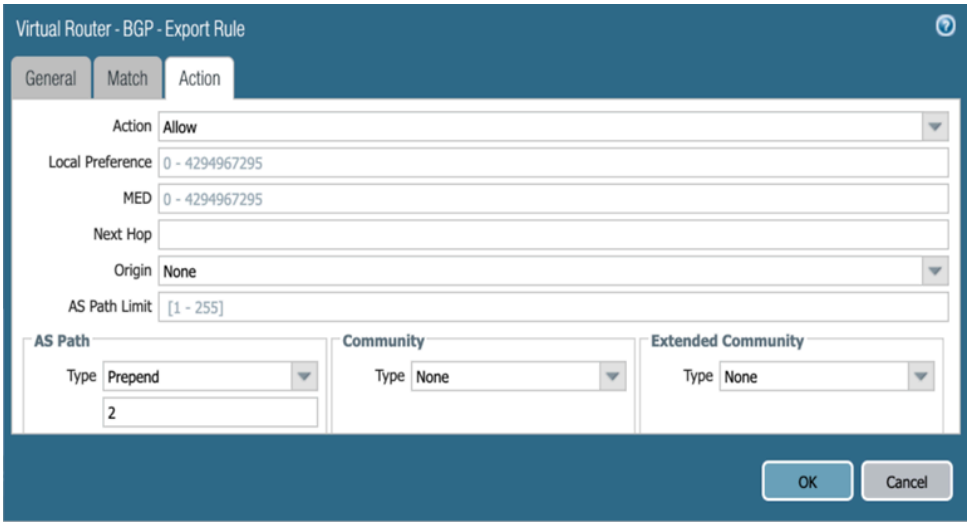
STEP 1 | Seleccione los perfiles de exportación BGP del enrutador virtual [**Network (Red)** > **Virtual Routers (Enrutadores virtuales)** > **BGP** > **Export (Exportar)**].

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Modifique la regla de exportación que creó cuando configuró las conexiones de servicio que tienen una **Action (Acción)** de **Allow (Permitir)**.



STEP 3 | En el área Ruta de AS, añada un **Prepend (Prefijo)** y, a continuación, introduzca el número de prefijos AS-PATH que desea añadir (**2** en este ejemplo).



STEP 4 | Repita los pasos 2 y 3 para cada regla de exportación que tenga una **Action (Acción)** de **Allow (Permitir)**, añadiendo prefijos AS-PATH para que coincidan con los escenarios de conmutación por error que ha planeado para su implementación.

En los ejemplos utilizados en esta sección, añada un prefijo AS-PATH de 1 para el túnel a la ubicación del centro de datos para la conexión de servicio 1 (túnel.1), un prefijo AS-PATH de 2 para el túnel utilizado para la conexión de servicio 2 (túnel.2) y un prefijo AS-PATH de 3 para el túnel utilizado para la conexión de servicio 3 (túnel.3).

Cuando se completa, este ejemplo utiliza los siguientes túneles en caso de conmutación por error:

- Si el túnel 2 o el túnel 3 se cae, el tráfico de la subred correspondiente conmuta al túnel 1, que tiene el AS-PATH anunciado más corto.
- Si el túnel.1 cae, el tráfico de su subred (192.168.171.0/24) conmuta al túnel.2, que tiene el AS-PATH más corto anunciado.

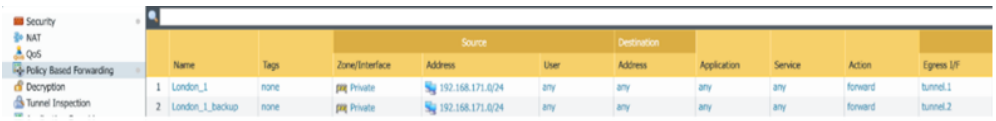
STEP 5 | Añada PBF de respaldo o políticas de enrutamiento basadas en políticas para garantizar un tráfico de retorno simétrico en caso de un fallo del túnel.

Mientras que el AS-PATH se encarga de garantizar que el tráfico de Prisma Access al centro de datos utilice un túnel específico en caso de una conmutación por error, también debe garantizar una ruta de retorno simétrica para el tráfico del centro de datos a Prisma Access. Para garantizar un retorno simétrico, utilice PBF o políticas de enrutamiento basadas en

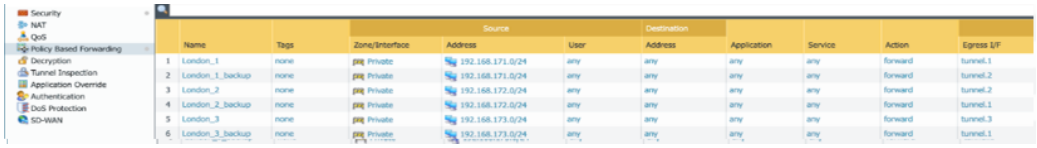
 ©2025 Palo Alto Networks, Inc.

políticas que reflejen los escenarios de conmutación por error que creó para el tráfico de Prisma Access al centro de datos.

En este ejemplo, para el tráfico de túnel.1 que tiene una IP de origen de 192.168.171.0/24, cree una política de PBF de copia de seguridad que obligue al tráfico de retorno a usar túnel.2 en caso de una conmutación por error. La primera regla PBF se deshabilita si no se puede acceder a la dirección IP del monitor de túnel; cuando se produce esta conmutación por error, el CPE (un cortafuegos de nueva generación en este ejemplo) evalúa la siguiente regla de la lista.



A continuación, añada más reglas PBF para que coincidan con los escenarios de conmutación por error que creó para el tráfico de Prisma Access al centro de datos.



Conservar la asignación de User-ID y Device-ID para conexiones de servicio con NAT de origen

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Cortafuegos de nueva generación (NGFW) que ejecuta una versión mínima de PAN-OS 11.2 ❑ Esta funcionalidad utiliza la encapsulación Geneve. Asegúrese de que los cortafuegos descendentes, además de los NGFW que ejecutan PAN-OS 11.2 o posterior, puedan desencapsular la encapsulación de Geneve. Esta funcionalidad no es compatible con el Acceso dinámico a privilegios.

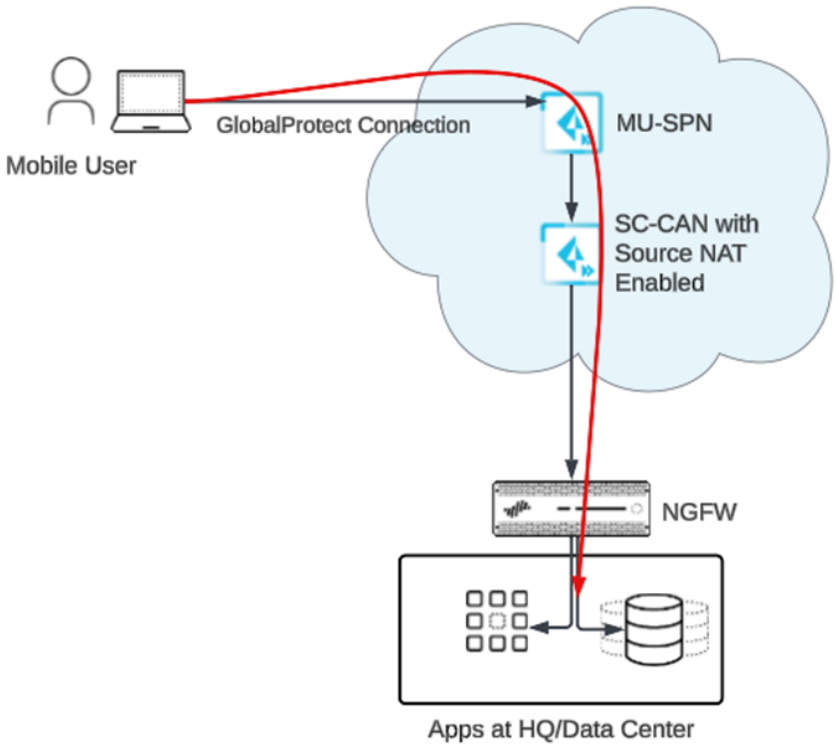
Utiliza conexiones de servicio, también conocidas como conexión de servicio: nodos de acceso corporativo (SC-CAN), en Prisma Access para proteger aplicaciones privadas. Para limitar el acceso a las aplicaciones en función de User-ID o Device-ID, puede implementar un cortafuegos de nueva generación (NGFW) en el centro de datos o en la ubicación de la sede central donde se encuentran las aplicaciones privadas; a continuación, configure las reglas de la política en el NGFW en función de la asignación de User-ID, la asignación de Device-ID o ambas.

Para utilizar estas reglas, el NGFW debe recibir la asignación de User-ID o Device-ID del SC-CAN; sin embargo, si los usuarios se conectan a Prisma Access mediante GlobalProtect y el SC-CAN

 ©2025 Palo Alto Networks, Inc.

tiene **Data Traffic source NAT (NAT de origen de tráfico de datos)** habilitado, el NGFW no puede obtener esta asignación. Si **Data Traffic source NAT (NAT de origen de tráfico de datos)** está habilitado en el SC-CAN, este realiza NAT en el grupo de direcciones IP del usuario móvil y no anuncia esas direcciones IP en el centro de datos o en la ubicación de la sede.

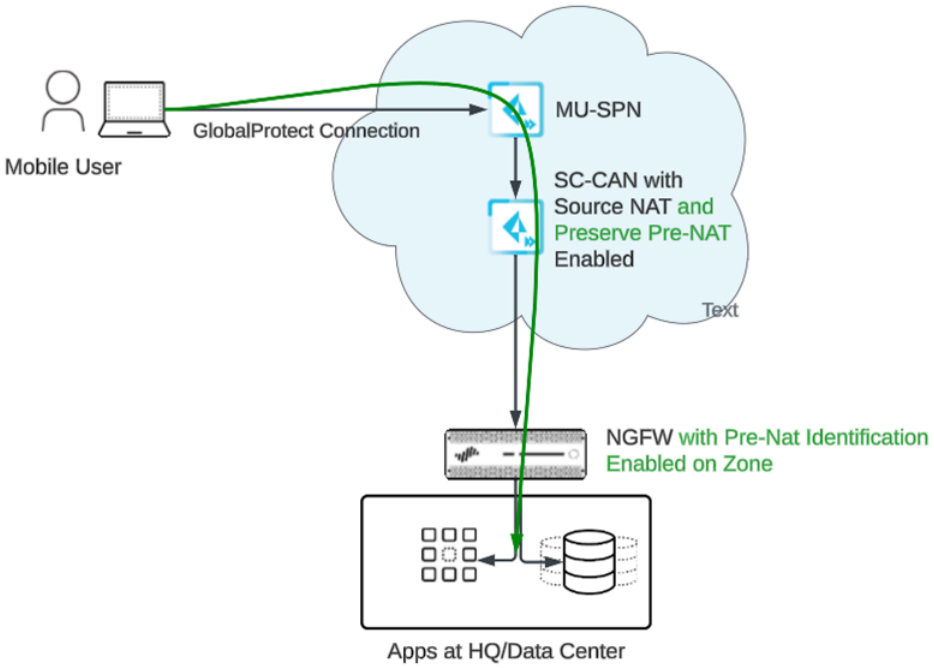
En este caso, el NGFW no puede recuperar el User-ID o el Device-ID del usuario de GlobalProtect, lo que significa que no se puede aplicar la política basada en User-ID o Device-ID.



Para asegurarse de que su red distribuye la asignación de User-ID o Device-ID a la sede central o al centro de datos, complete el procedimiento enumerado en una de las siguientes secciones, que permite al NGFW aplicar reglas de política de seguridad basadas en la asignación de User-ID que aprende de GlobalProtect.

Se requiere un NGFW con una versión mínima de PAN-OS 11.2. La conexión de servicio no tiene que terminar en el NGFW y puede terminar en otro dispositivo compatible con IPSec, siempre que el NGFW esté en sentido descendente desde donde se termina la conexión de servicio.

©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

Conservar la asignación de User-ID y Device-ID para conexiones de servicio con NAT de origen (Strata Cloud Manager)

Para que Prisma Access distribuya asignaciones de ID de usuario de los usuarios de GlobalProtect a un NGFW en la sede central o el centro de datos en Prisma Access (Managed by Strata Cloud Manager), complete los siguientes pasos.

Este procedimiento supone que tiene la siguiente configuración de red:

- Ha habilitado la **Data Traffic source NAT (NAT de origen de tráfico de datos)** en la conexión de servicio.
- Ha implementado un NGFW en la sede o el centro de datos donde se encuentran las aplicaciones privadas.
- Ha aplicado reglas de política de seguridad para Prisma Access en el NGFW según las zonas que ha creado en el NGFW.

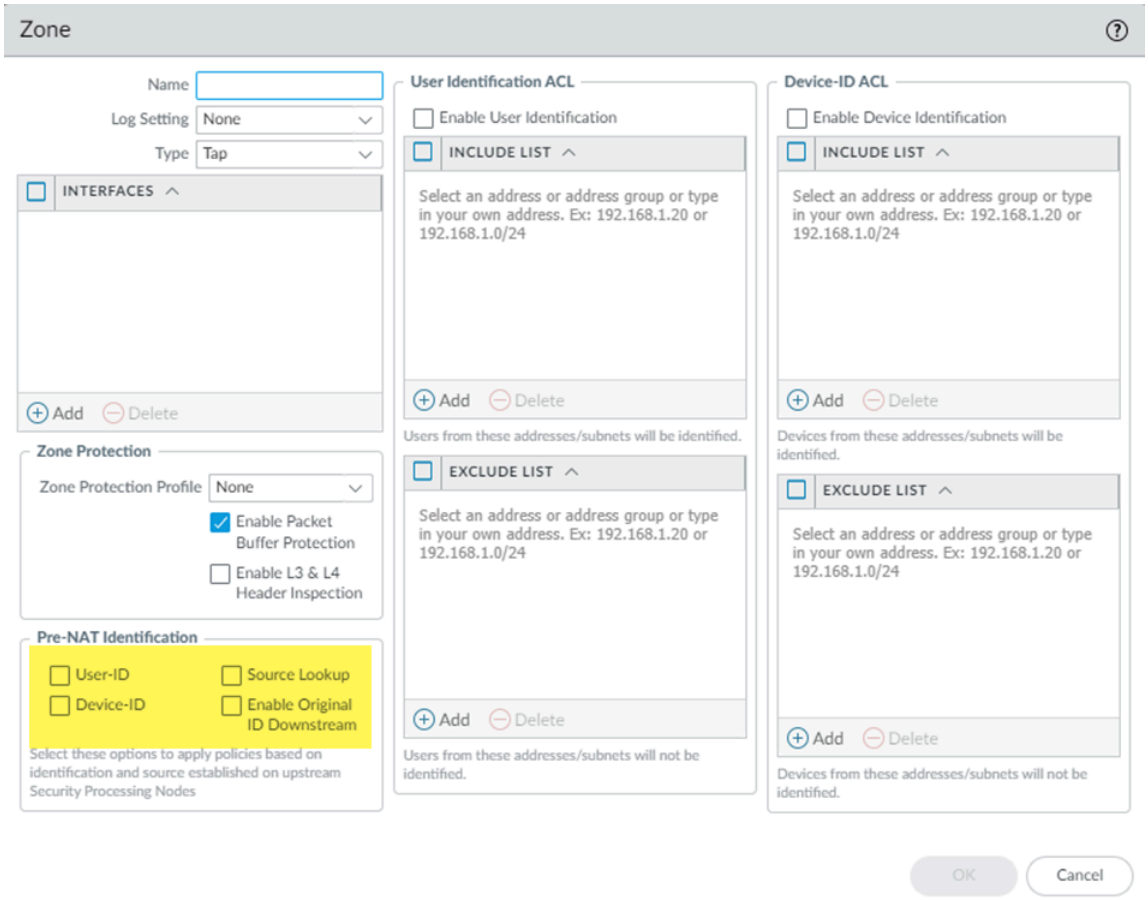
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Introduce parámetros de identificación pre-NAT en el NGFW.

1. Inicie sesión en el NGFW o inicie sesión en el SCM o Panorama que gestione el NGFW, y vaya a **Network (red)** > **Zones (Zonas)**.
2. **Add (Añadir)** una zona o seleccione una zona existente.
3. Seleccione uno o más parámetros de **Pre-NAT Identification (Identificación previa a NAT)**:
   - **User-ID**: conserva la asignación de User-ID de usuario móvil utilizada antes de que se aplique NAT a las direcciones IP. Habilite esta opción si usa User-ID en las reglas de la política de seguridad.
   - **Device-ID**: conserva la asignación de Device-ID de usuario móvil utilizada antes de que se aplique NAT a las direcciones IP. Habilite esta opción si usa Device-ID en las reglas de la política de seguridad.
   - **Source Lookup (Búsqueda de fuente)**: le permite hacer coincidir la dirección IP de origen original recibida de GlobalProtect. Si usa la búsqueda de fuente en QoS o políticas de reenvío basado en políticas (PBF), la comparación de IP de origen se basa en la dirección IP de origen anterior a NAT. Por ejemplo, si tenía una política de seguridad que permitía una dirección IP de origen de 1.1.1.1 y una dirección IP de destino de Any (Cualquiera), 1.1.1.1 se compara con la dirección IP de origen anterior a NAT en el encabezado del paquete.
   - **Enable Original ID Downstream (Habilitar ID original anterior)**: si tiene dos NGFW seguidos, especifique esta opción para que el primer NGFW envíe la información previa a la NAT al segundo NGFW después de que el primer NGFW

 ©2025 Palo Alto Networks, Inc.

haya inspeccionado el tráfico y le haya aplicado las políticas. Esta es la configuración predeterminada en SC-CAN.



4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 2 | Cree una sesión de interfaz de línea de comandos (CLI) con el NGFW e introduzca el siguiente comando en el modo de configuración:

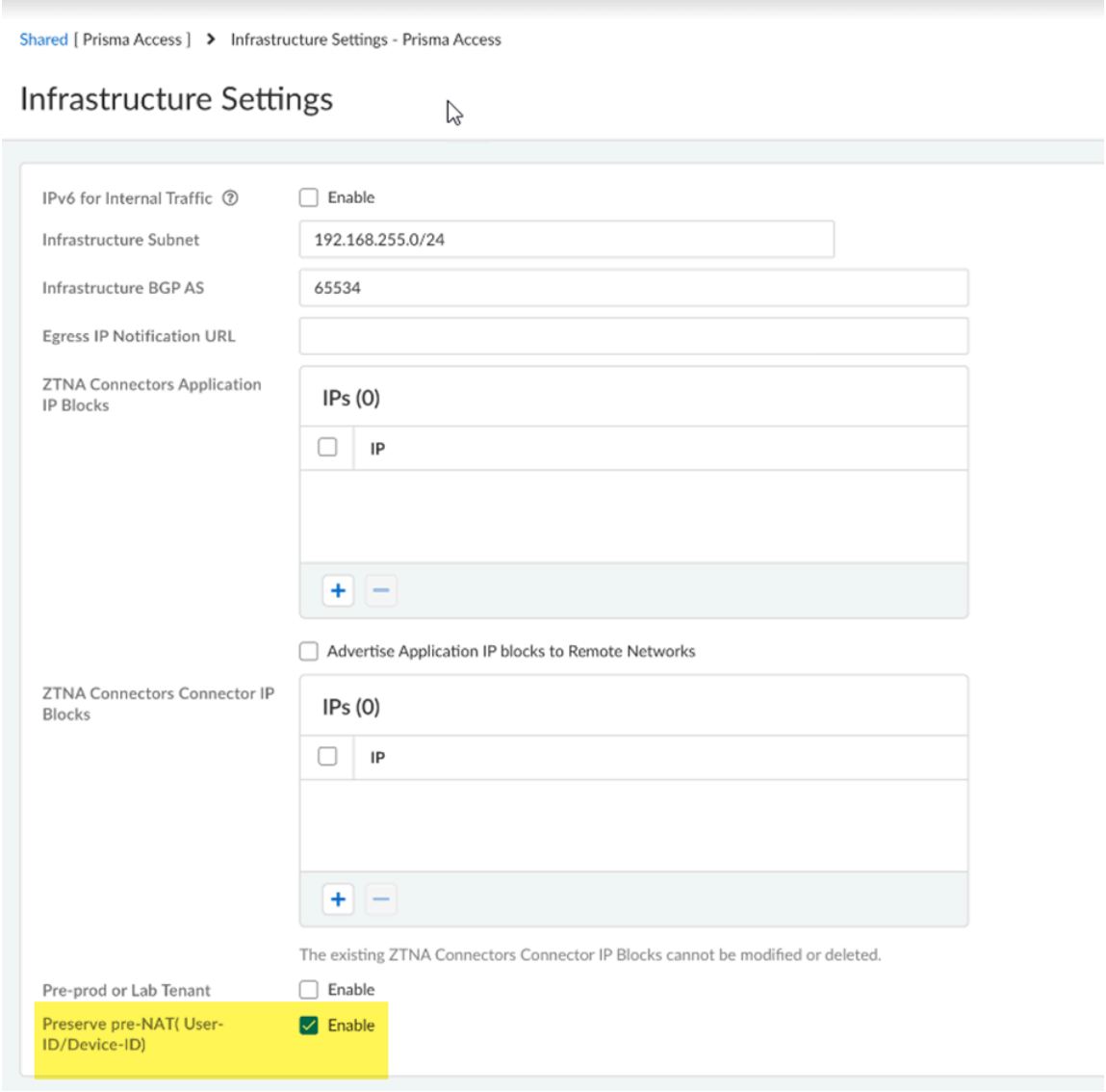
```
set deviceconfig setting preserve-prenat-feature yes
```

Si necesita deshabilitar esta función en el futuro, introduzca `set deviceconfig setting preserve-prenat-feature no`.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Habilite la configuración previa a NAT en Strata Cloud Manager.

1. Vaya a **Flujos de trabajo (Workflows)** > **Prisma Access Setup (Configuración de Prisma Access)** > **de Prisma Access** > **Infrastructure Settings (Configuración de infraestructura)**.
2. **Enable (Habilitar) Preserve pre-NAT (User-ID/Device-ID) [Conservar pre-NAT (User-ID/Device-ID)]**.



3. Elija **Push Config (Enviar configuración)** para guardar sus cambios.

Conservar la asignación de User-ID y Device-ID para conexiones de servicio con NAT de origen (Panorama)

Para que Prisma Access distribuya asignaciones de ID de usuario de los usuarios de GlobalProtect a un NGFW en la sede central o el centro de datos en Prisma Access (Managed by Panorama), complete los siguientes pasos.

Este procedimiento supone que tiene la siguiente configuración de red:

- Ha habilitado la **Data Traffic source NAT (NAT de origen de tráfico de datos)** en la conexión de servicio.

 ©2025 Palo Alto Networks, Inc.

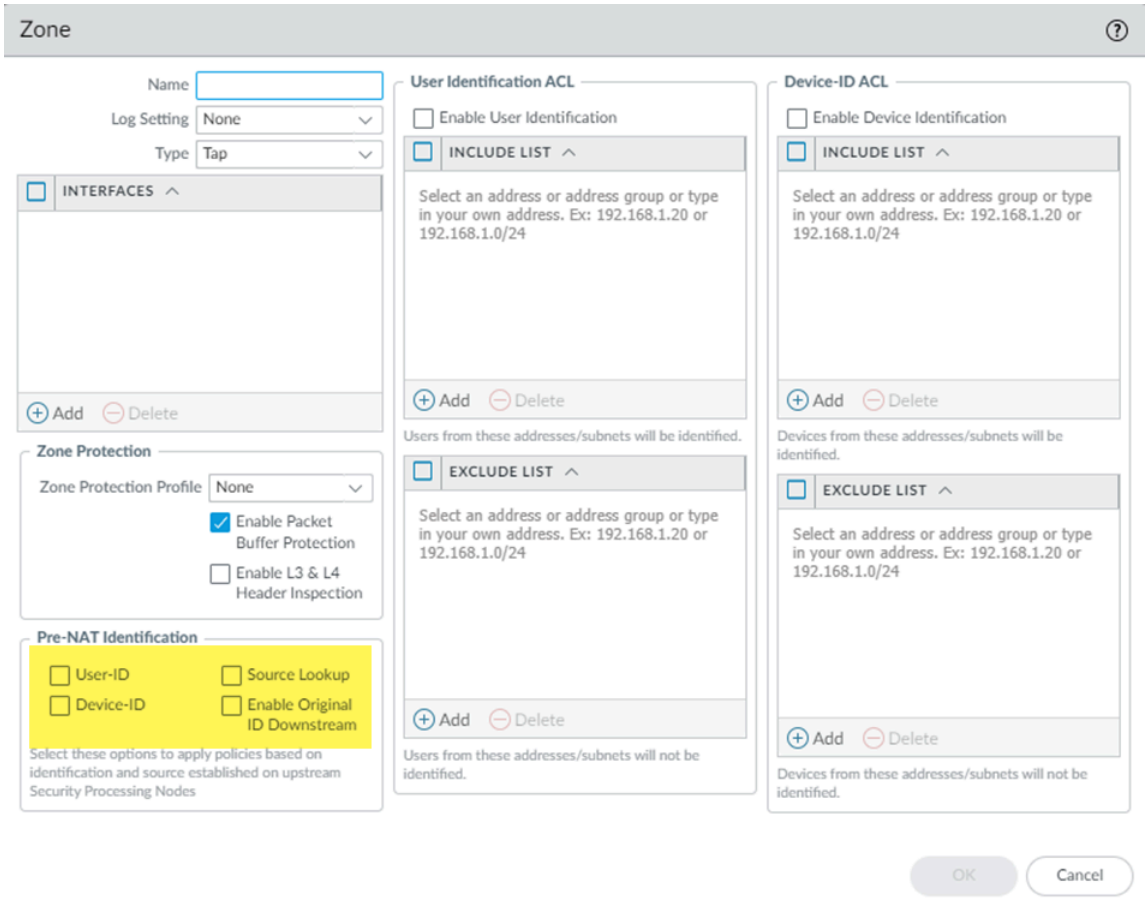
- Ha implementado un NGFW en la sede o el centro de datos donde se encuentran las aplicaciones privadas.
- Ha aplicado reglas de política de seguridad para Prisma Access en el NGFW según las zonas que ha creado en el NGFW.

STEP 1 | Introduce parámetros de identificación pre-NAT en el NGFW.

1. Inicie sesión en el NGFW o inicie sesión en el SCM o Panorama que gestione el NGFW, y vaya a **Network (red)** > **Zones (Zonas)**.
2. **Add (Añadir)** una zona o seleccione una zona existente.
3. Seleccione uno o más parámetros de **Pre-NAT Identification (Identificación previa a NAT)**:
   - **User-ID**: conserva la asignación de User-ID de usuario móvil utilizada antes de que se aplique NAT a las direcciones IP. Habilite esta opción si usa User-ID en las reglas de la política de seguridad.
   - **Device-ID**: conserva la asignación de Device-ID de usuario móvil utilizada antes de que se aplique NAT a las direcciones IP. Habilite esta opción si usa Device-ID en las reglas de la política de seguridad.
   - **Source Lookup (Búsqueda de fuente)**: le permite hacer coincidir la dirección IP de origen original recibida de GlobalProtect. Si usa la búsqueda de fuente en QoS o políticas de reenvío basado en políticas (PBF), la comparación de IP de origen se basa en la dirección IP de origen anterior a NAT. Por ejemplo, si tenía una política de seguridad que permitía una dirección IP de origen de 1.1.1.1 y una dirección IP de destino de Any (Cualquiera), 1.1.1.1 se compara con la dirección IP de origen anterior a NAT en el encabezado del paquete.
   - **Enable Original ID Downstream (Habilitar ID original anterior)**: si tiene dos NGFW seguidos, especifique esta opción para que el primer NGFW envíe la información previa a la NAT al segundo NGFW después de que el primer NGFW

 ©2025 Palo Alto Networks, Inc.

haya inspeccionado el tráfico y le haya aplicado las políticas. Esta es la configuración predeterminada en SC-CAN.



4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 2 | Cree una sesión de interfaz de línea de comandos (CLI) con el NGFW e introduzca el siguiente comando en el modo de configuración:

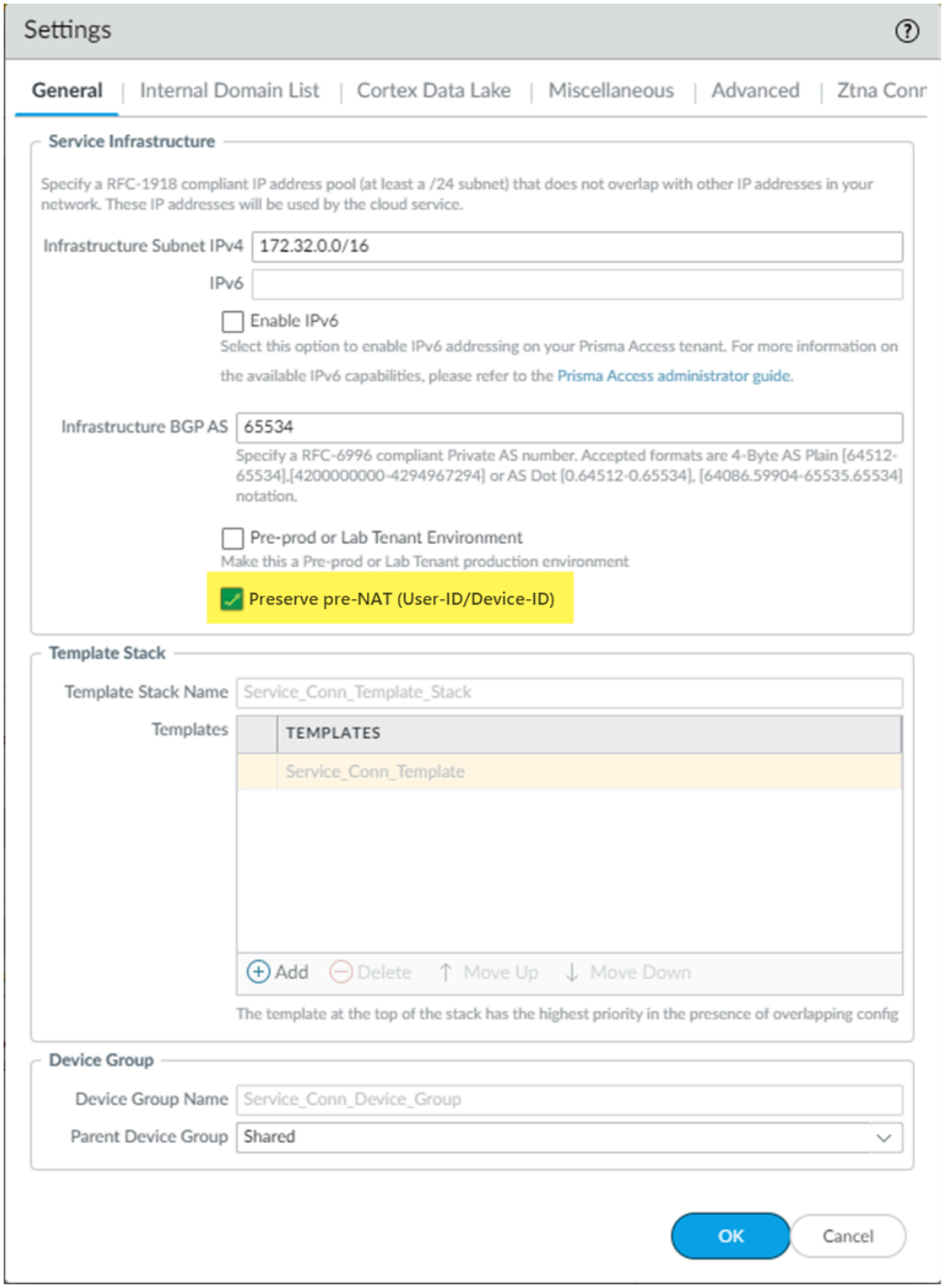
```
set deviceconfig setting preserve-prenat-feature yes
```

Si necesita deshabilitar esta función en el futuro, introduzca `set deviceconfig setting preserve-prenat-feature no`.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | En el Panorama que gestiona a Prisma Access, habilite la configuración previa a NAT.

1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y haga clic en el engranaje para editar la **Settings (Configuración)**.
2. Seleccione **Preserve pre-NAT (User-ID/Device-ID) [Conservar pre-NAT (User-ID/Device-ID)]**.



3. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

Implementaciones avanzadas de Usuarios móviles de Prisma Access: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En las siguientes secciones se muestran las implementaciones avanzadas que están disponibles en una implementación de Usuarios móviles: GlobalProtect:

- Compatibilidad con el registro de DNS dinámico para usuarios móviles: GlobalProtect
- Identificación y cuarentena de dispositivos en riesgo en una implementación de Prisma Access GlobalProtect
- Tráfico IPV6 de sinkhole en implementaciones de Usuarios móviles: GlobalProtect
- Redistribuir la información de HIP con Prisma Access
- Ver informes de HIP
- Soporte para codificación Gzip en VPN sin cliente
- Replicación de tráfico en Prisma Access

Configurar múltiples portales en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Versión mínima requerida del cliente de GlobalProtect: 6.1 (Solo Windows y macOS)

Puede configurar dos portales basados en números de puerto en el mismo inquilino de Prisma Access, con cada portal soportando un método de autenticación diferente. Habilite esta función para migrar usuarios móviles de un método de autenticación a otro sin crear un nuevo inquilino de Prisma Access. Esta configuración permite una mayor flexibilidad de autenticación al permitirle mover gradualmente a los usuarios a la autenticación basada en la nube, sin necesidad de una instancia de Prisma Access separada.

Prisma Access con varios portales de GlobalProtect utilizan un número de puerto diferente para cada portal dentro del mismo inquilino. Configura el primer portal de GlobalProtect utilizando el puerto estándar 443. Cuando habilita la función de varios portales, Prisma Access configura un segundo portal de GlobalProtect utilizando un puerto alternativo 8443, y permite conexiones al segundo portal utilizando el mismo FQDN que el primero. La función de múltiples portales solo admite dos portales por FQDN.

Cuando un usuario se conecta al portal utilizando el puerto 443, el tráfico se envía al primer portal de autenticación sin cambios en la dirección IP. Este flujo no ha cambiado con respecto

 ©2025 Palo Alto Networks, Inc.

a las configuraciones sin la función de varios portales de GlobalProtect. Cuando un usuario se conecta utilizando el puerto 8443, el tráfico en su lugar toca una regla NAT de destino. Esto lleva al usuario al segundo portal de autenticación en una dirección IP diferente. Después de autenticarse en cualquiera de los portales, el usuario es redirigido a la puerta de enlace con la cookie de anulación de autenticación. Esta función depende de la configuración de cookies de anulación de autenticación y está habilitada para ambos portales y en las puertas de enlace.

La siguiente tabla describe la compatibilidad de múltiples portales de GlobalProtect con combinaciones de métodos de autenticación y certificados utilizando autenticación heredada (como RADIUS o LDAP) en el portal principal y autenticación en la nube (como SAML o SAML con CAS) en el portal secundario.

Autenticación de usuario del portal principal	Autenticación de usuario del portal secundario	Opciones de método de conexión
Heredado, sin certificado	Nube, Sin certificado	Inicio de sesión de usuario (siempre activo, bajo demanda)
Heredado, <auth profile selection> Y Certificado de cliente Nota: El perfil del certificado debe ser el mismo.	Nube, <auth profile selection> Y Certificado de cliente Nota: El perfil del certificado debe ser el mismo.	Inicio de sesión de usuario (siempre activo, bajo demanda) Pre inicio de sesión (siempre activo, a petición)
Heredado, sin certificado	Nube, <auth profile selection> O Certificado de cliente	Inicio de sesión de usuario (siempre activo, bajo demanda)
Heredado, <auth profile selection> O Certificado de cliente Varias configuraciones de portal no admiten clientes que utilizan solo certificado de cliente para la autenticación.	Nube, Sin certificado	Inicio de sesión de usuario (siempre activo, bajo demanda) Pre inicio de sesión (siempre activo, a petición), si es certificado
Heredado, <auth profile selection> O Certificado de cliente Varias configuraciones de portal no admiten clientes que utilizan solo certificado de cliente para la autenticación.	Nube, <auth profile selection> O Certificado de cliente Varias configuraciones de portal no admiten clientes que utilizan solo certificado de cliente para la autenticación.	Inicio de sesión de usuario (siempre activo, bajo demanda) Pre inicio de sesión (siempre activo, a petición), si es certificado

Asegúrese de lo siguiente antes de configurar múltiples portales:

 ©2025 Palo Alto Networks, Inc.

- Ambos portales tienen los mismos perfiles de certificado o no tienen perfiles de certificado.
- La lista de permitidos asociada con los perfiles de autenticación debe ser la misma.
- Cuando acepte una cookie para la anulación de autenticación en el portal, asegúrese de que la duración de la cookie sea la misma en el portal que en la puerta de enlace.
- Varias configuraciones de portal no admiten el uso únicamente de la autenticación basada en certificados de cliente.

> La VPN sin cliente *no es compatible para su uso en el portal secundario en una implementación de múltiples portales; sin embargo, la VPN sin cliente funciona en el portal principal con su método de autenticación existente.*

- Strata Cloud Manager
- Panorama

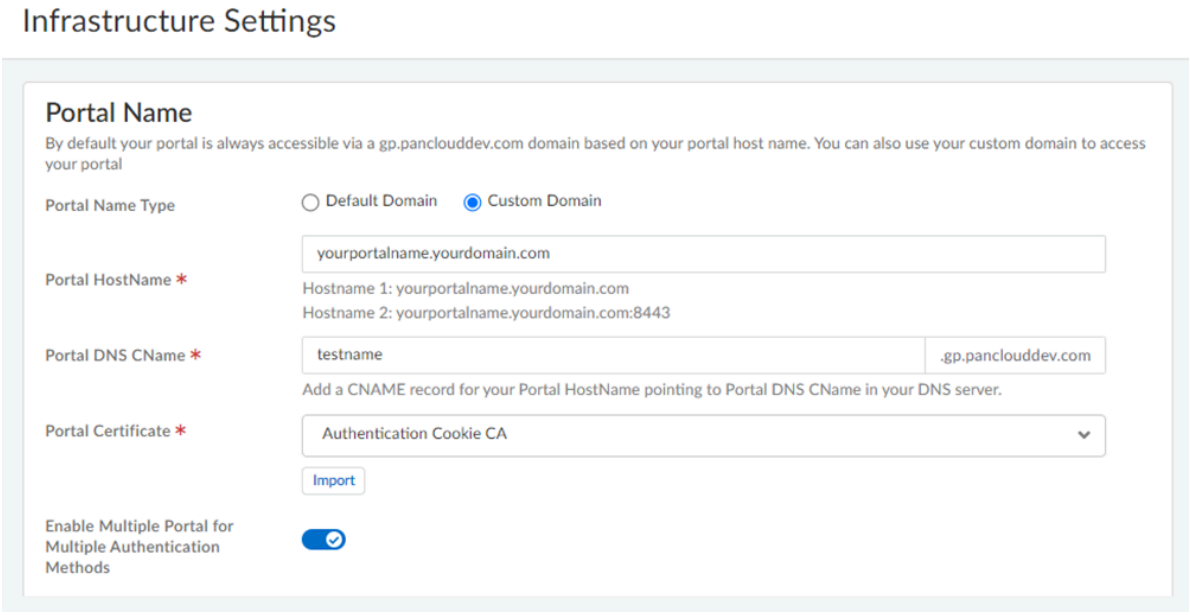
Configurar varios portales en Prisma Access (Strata Cloud Manager)

STEP 1 | Póngase en contacto con la asistencia de Palo Alto Networks para activar esta funcionalidad.

STEP 2 | Configure un usuario móvil y el método de autenticación para él.

STEP 3 | Habilite varios portales para la misma puerta de enlace.

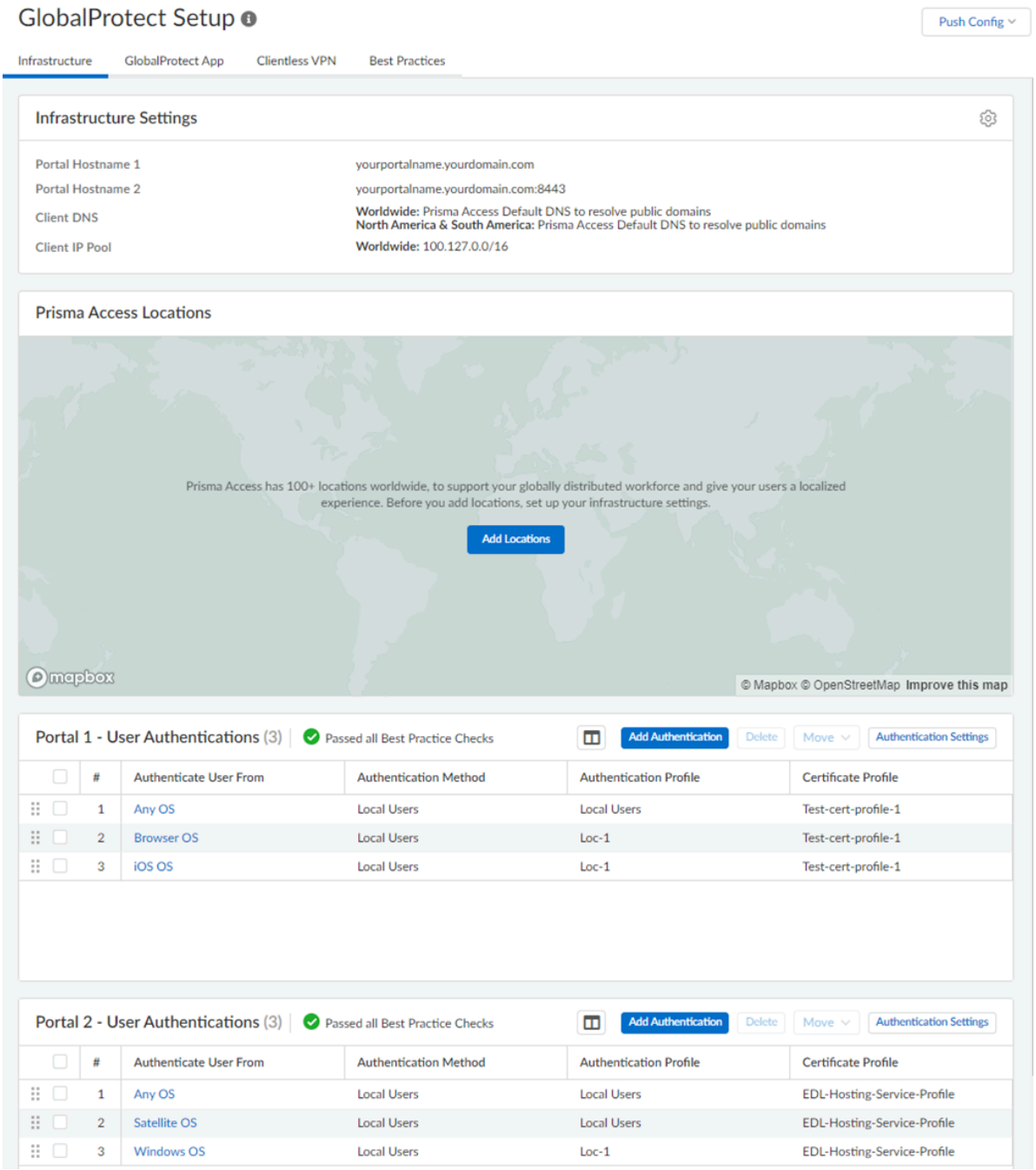
1. Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect Setup (Configuración de GlobalProtect)** > **Infrastructure (Infraestructura)**.
2. Edite la **Infrastructure Settings (Configuración de la infraestructura)**.
3. **Habilite varios portales para varios métodos de autenticación**



Aparece el nuevo portal para el puerto 8443 para el mismo inquilino. Este portal hereda las opciones de configuración del puerto original, que es el puerto 443.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Edite las configuraciones del portal para actualizar la configuración de autenticación.

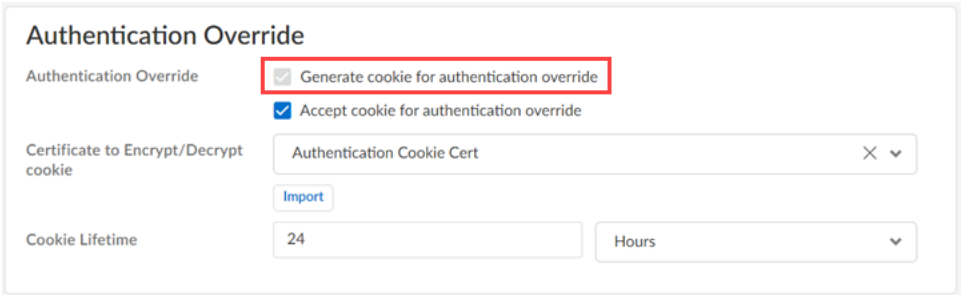


Solo puede editar la configuración de autenticación **Authentication Settings (Configuración de autenticación)** y **Certificate Profile (Perfil de certificado)** del portal.

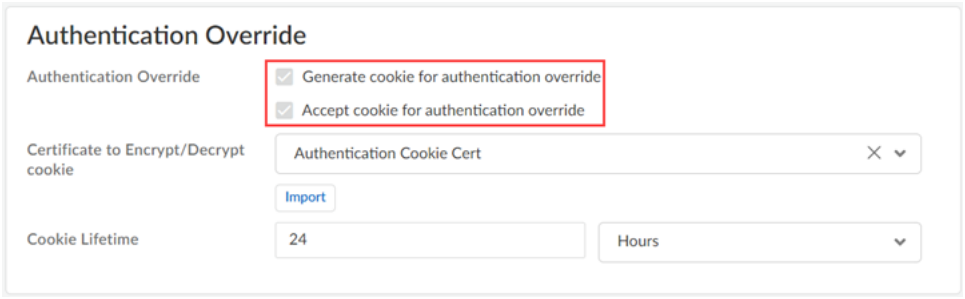
Si utiliza la autenticación basada en certificados en ambos portales, asegúrese de que ambos portales utilicen el mismo perfil de certificado de cliente para la autenticación.

Esta función permite que la configuración de anulación de autenticación genere cookies para ambos portales en la configuración de la aplicación GlobalProtect.

 ©2025 Palo Alto Networks, Inc.



Esta función permite que la configuración de anulación de autenticación genere y acepte cookies para ambos portales en la configuración del túnel.



STEP 5 | Guarde todos los cambios y seleccione **Push (Enviar)** los cambios de configuración a Prisma Access.

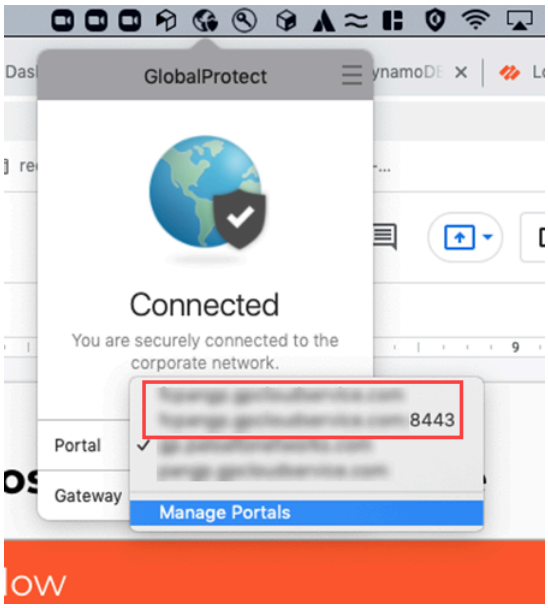
STEP 6 | Añada los portales manualmente o mediante el software de gestión de endpoints en la aplicación GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Compruebe si puede conectarse a ambos portales con diferentes perfiles de autenticación para la puerta de enlace.

1. Inicie sesión en su máquina con Windows.
2. Conéctese a los portales de su aplicación de GlobalProtect.

   Al cambiar la conexión entre portales de diferentes métodos de autenticación, autentique el inicio de sesión del usuario.



*Si la cookie de autenticación caduca cuando se conecta al portal 8443 y cambia a la puerta de enlace manual, GlobalProtect se conecta a la **Best Available Gateway (Mejor puerta de enlace disponible)**.*

Si la aplicación GlobalProtect utiliza configuraciones de portal almacenadas en caché, la alternativa al portal no funciona.

Si está usando autenticación basada en SAML para el portal secundario, introduzca los valores de la siguiente manera durante la integración:

- ***Single sign on URL (Inicio de sesión único en URL)**: Introduzca **`https://Portal-FQDN:443/SAML20/SP/ACS`***

  Portal-FQDN es el FQDN para el portal de Prisma Access

  *Utilice portal **`443`** incluso si ha configurado el portal secundario (8443).*
- ***Audience URI (SP Entity ID) [URI de audiencia (ID de entidad SP)]**: Introduzca **`https://Portal-FQDN:443/SAML20/SP`***

Configurar varios portales en Prisma Access (Panorama)

STEP 1 | Póngase en contacto con su representante de cuentas de Palo Alto Networks para activar esta funcionalidad.

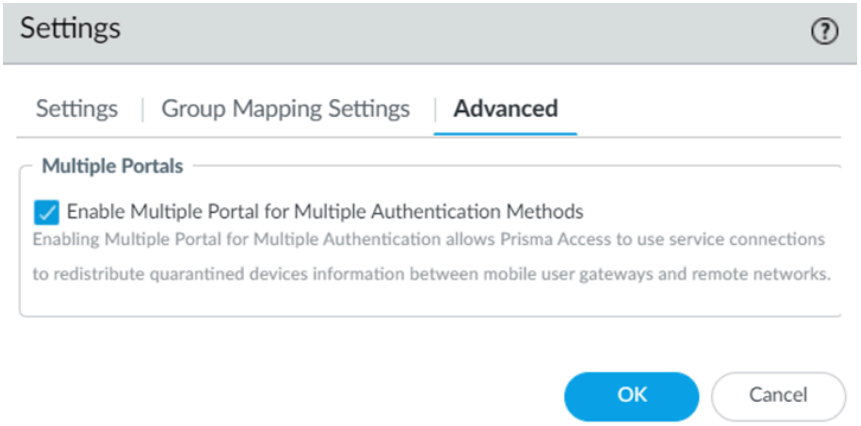
 ©2025 Palo Alto Networks, Inc.

Al configurar varios portales de GlobalProtect con Dirección de tráfico, no configure ***Accept Default Routes over Service Connections (Aceptar rutas predeterminadas a través de conexiones de servicio) [Panorama > Cloud Services (Servicios en la nube) > Configuration (Configuración) > Traffic Steering (Dirección de tráfico) > Settings (Configuración) > Accept Default Route over Service Connection (Aceptar ruta predeterminada a través de la conexión de servicio)]****; si lo hace, los usuarios móviles no podrán conectarse al portal secundario.*

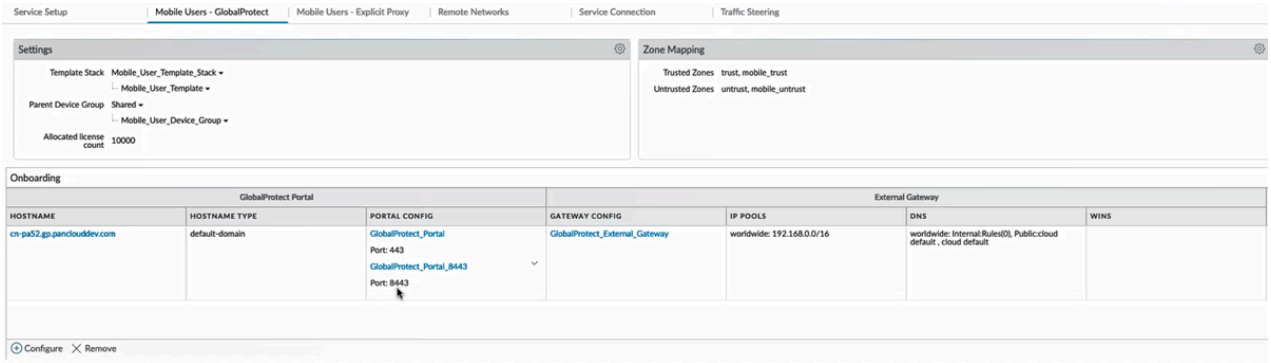
STEP 2 | Configurar un usuario móvil y el método de autenticación para ello.

STEP 3 | Seleccione **Cloud Services (Servicios en la nube) > Configuration (Configuración) > Mobile Users—GlobalProtect (Usuarios móviles—GlobalProtect) > Settings (Configuración) > Advanced (Avanzado)**.

STEP 4 | **Habilite varios portales para varios métodos de autenticación**



Aparece el nuevo portal para el puerto 8443 para el mismo inquilino. Este portal hereda las opciones de configuración del puerto original, que es el puerto 443.



 ©2025 Palo Alto Networks, Inc.

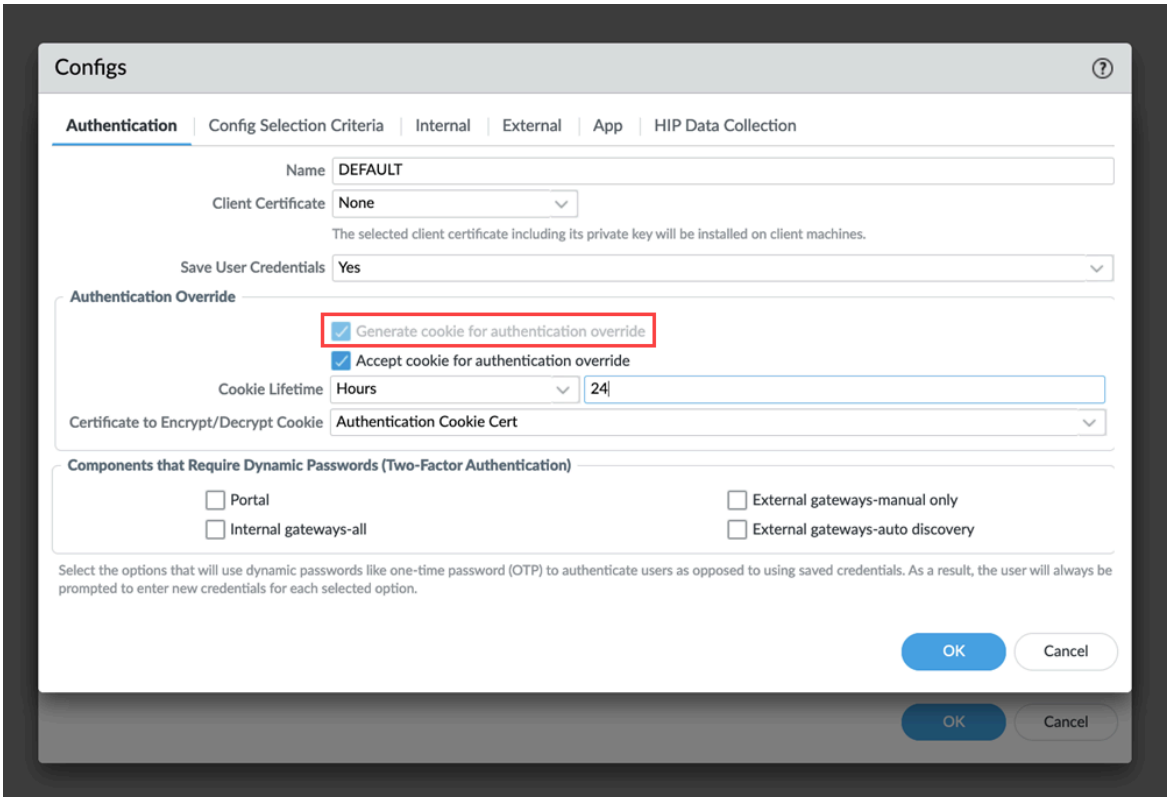
STEP 5 | Edite las configuraciones del portal para actualizar la configuración de autenticación.

1. Haga clic en el hipervínculo del portal o seleccione **Panorama** > **Templates (Plantillas)** > **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y haga clic en el hipervínculo del portal.
2. En la sección **Authentication (Autenticación)**, seleccione **Add (Añadir)** una **Client Authentication (Autenticación de cliente)** con un **Authentication Profile (Perfil de autenticación)** diferente.

Solo puede editar las configuraciones de autenticación de **Client Authentication (Autenticación de cliente)** y **Certificate Profile (Perfil de certificado)**.

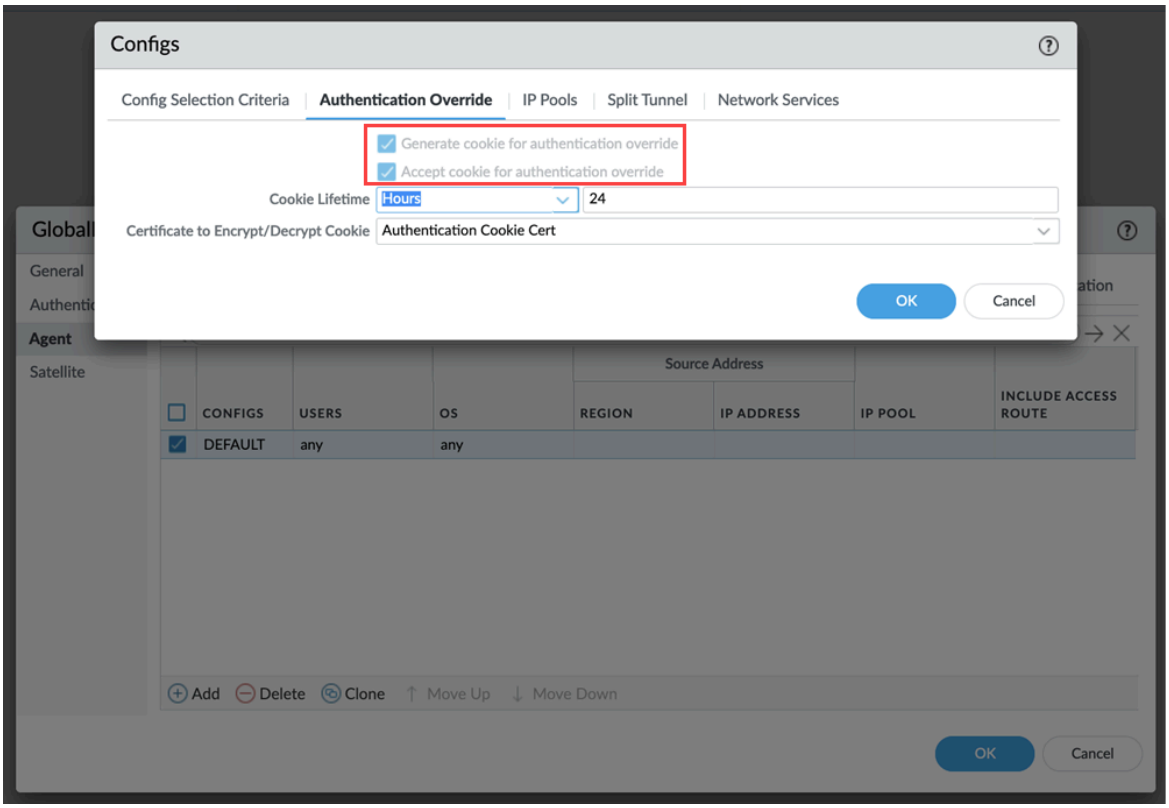
Si usa la autenticación basada en certificados en ambos portales, asegúrese de que la puerta de enlace no tenga autenticación basada en certificados.

Esta función permite que la configuración de anulación de autenticación genere cookies para ambos portales en la configuración de la aplicación GlobalProtect.



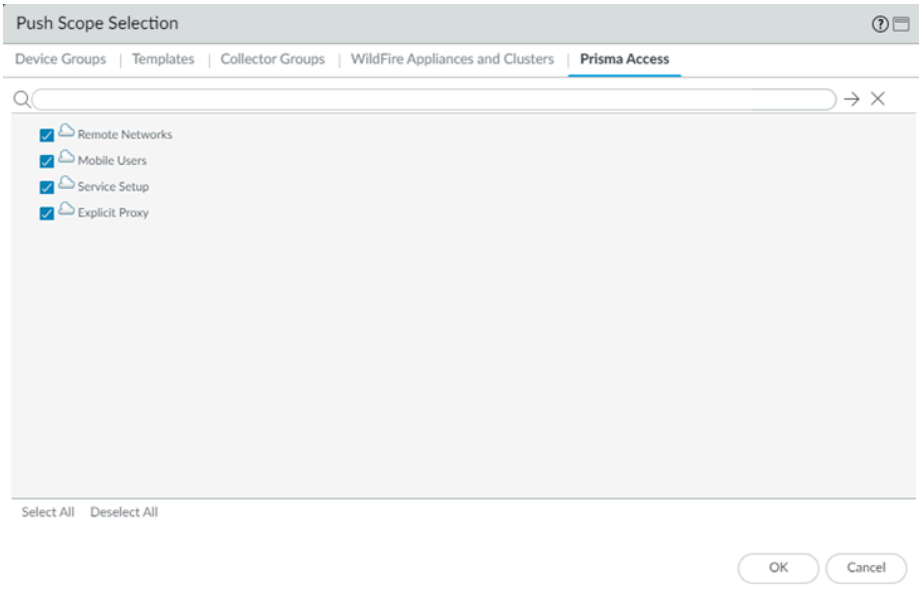
Esta función permite que la configuración de anulación de autenticación genere y acepte cookies para ambos portales en la configuración del túnel.

 ©2025 Palo Alto Networks, Inc.



STEP 6 | Confirme todos sus cambios en Panorama y envíe los cambios de configuración a Prisma Access.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access**, asegúrese de que **Mobile Users (Usuarios móviles)** se selecciona en **Push Scope (Ámbito de envío)** y, a continuación, haga clic en **OK (Aceptar)**.



3. Haga clic en **Commit and Push (Confirmar y enviar)**.

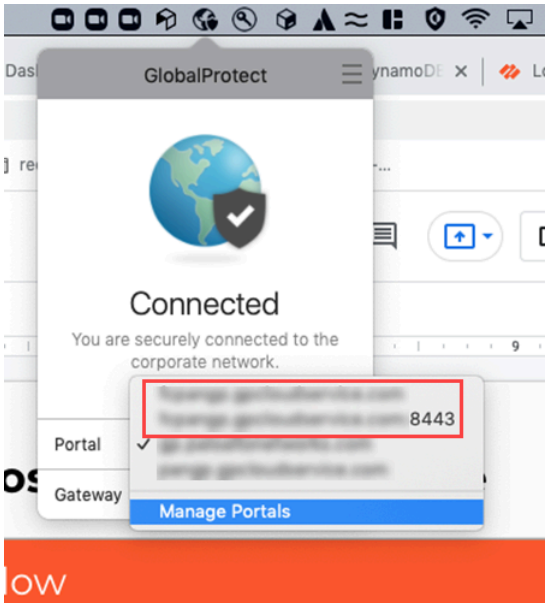
 ©2025 Palo Alto Networks, Inc.

STEP 7 | Añada los portales manualmente o mediante el software de gestión de endpoints en la aplicación GlobalProtect.

STEP 8 | Compruebe si puede conectarse a ambos portales con diferentes perfiles de autenticación para la puerta de enlace.

1. Inicie sesión en su máquina con Windows.
2. Conéctese a los portales de su aplicación de GlobalProtect.

   Al cambiar la conexión entre portales de diferentes métodos de autenticación, autentique el inicio de sesión del usuario.



   Si la cookie de autenticación caduca cuando se conecta al portal 8443 y cambia a la puerta de enlace manual, GlobalProtect se conecta a la ***Best Available Gateway (Mejor puerta de enlace disponible)****.*

   Si la aplicación GlobalProtect utiliza configuraciones de portal almacenadas en caché, la alternativa al portal no funciona.

3. Ver los logs de ambos portales en **Monitor (Supervisar)** > **Logs** > **GlobalProtect** para ver el portal y la información de autenticación.

Si está usando autenticación basada en SAML para el portal secundario, introduzca los valores de la siguiente manera durante la integración:

- ***Single sign on URL (Inicio de sesión único en URL)****: Introduzca* ***`https://Portal-FQDN:443/SAML20/SP/ACS`***

  Portal-FQDN es el FQDN para el portal de Prisma Access

  Utilice portal ***`443`*** *incluso si ha configurado el portal secundario (8443).*

- ***Audience URI (SP Entity ID) [URI de audiencia (ID de entidad SP)]****: Introduzca* ***`https://Portal-FQDN:443/SAML20/SP`***

 ©2025 Palo Alto Networks, Inc.

Compatibilidad con el registro de DNS dinámico para la resolución de problemas y actualizaciones remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access, incluido Usuarios móviles: GlobalProtect ❑ Versión mínima de Prisma Access requerida: 5.1 Innovation (se requiere una versión mínima del plano de datos de PAN-OS de 11.2)

Cuando un usuario móvil se conecta de forma remota a Prisma Access utilizando el agente GlobalProtect, la puerta de enlace de GlobalProtect asigna una dirección IP y un FQDN de endpoint al usuario. Sin embargo, Prisma Access no actualiza los servidores DNS en su empresa con esta información. Dado que los servidores DNS no tienen la dirección IP asignada al usuario móvil ni la información FQDN, su administrador de TI y las aplicaciones en su red no pueden identificar y actualizar los endpoints remotos utilizando FQDN.

Usar el registro DNS dinámico le permite integrar Prisma Access con proveedores de Gestión de direcciones IP (IPAM) para crear dinámicamente registros A y PTR en los servidores DNS utilizando nsupdate y ofrece estos beneficios:

- Integración directa con los principales proveedores de IPAM como InfoBlox, BlueCat y Windows.
- Las actualizaciones de DDNS se realizan utilizando ya sea la firma de transacción (TSIG) o Kerberos como protocolo de autenticación, asegurando actualizaciones seguras a la base de datos DNS.
- Las actualizaciones DDNS en tiempo real se realizan desde Prisma Access al servidor DNS utilizando llamadas nsupdate agrupadas basadas en eventos de conexión y desconexión de GlobalProtect. Estas actualizaciones utilizan un servicio DDNS en el Nodo de procesamiento de seguridad de usuarios móviles (MU-SPN).

Después de configurar esta solución, puede realizar las siguientes acciones:

- Puede utilizar herramientas de software como Microsoft Endpoint Configuration Manager (MECM) para enviar actualizaciones de software a los endpoints de GlobalProtect.
- El personal de TI y de asistencia técnica puede conectarse y gestionar el endpoint de GlobalProtect utilizando el FQDN del dispositivo.
- Puede implementar aplicaciones para clientes (como aplicaciones bancarias) que dependan de búsquedas inversas de DNS para permitir el acceso desde endpoints de GlobalProtect aprobados.

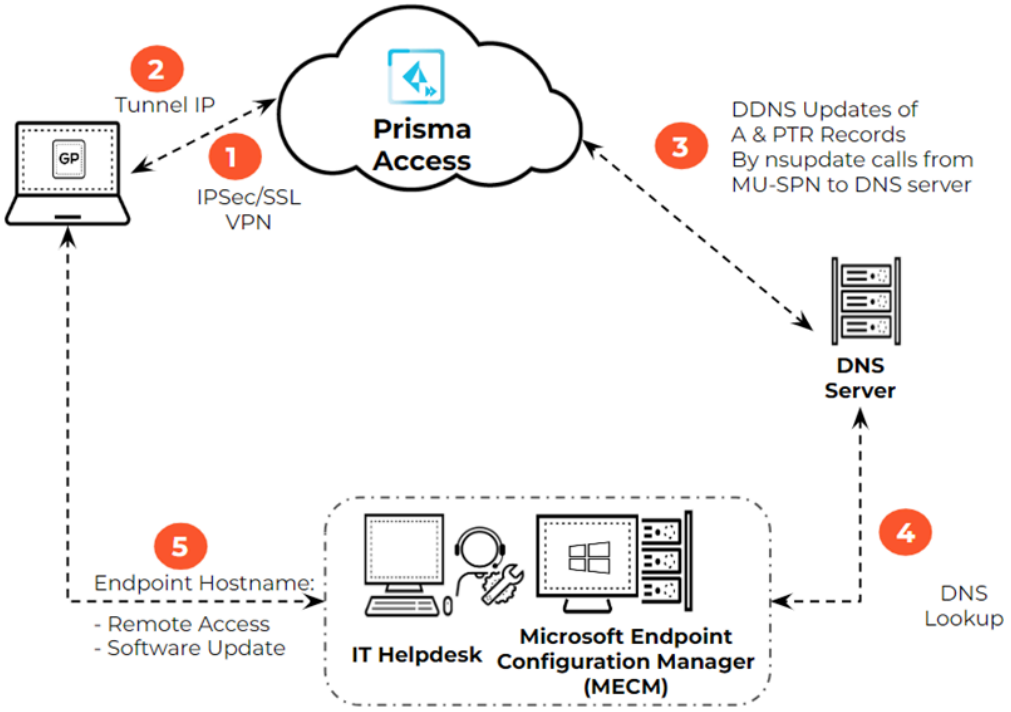
Esta solución DDNS no es compatible con la Compatibilidad con el registro de DNS dinámico para usuarios móviles: GlobalProtect que Strata Logging Service utiliza para enviar las actualizaciones DDNS al servidor. Si tiene la solución existente utilizando el Strata Logging Service implementado y luego implementa esta solución, Prisma Access utiliza esta solución y desactiva la solución existente utilizando Strata Logging Service.

 ©2025 Palo Alto Networks, Inc.

Caso de uso de soporte de registro de DNS dinámico

El siguiente diagrama ilustra un caso de uso típico para la solución DDNS de Prisma Access. En este ejemplo, desea actualizar los endpoints de GlobalProtect utilizando MECM o le gustaría que el servicio de asistencia de TI pudiera iniciar sesión en el endpoint de GlobalProtect de forma remota para solucionar problemas.

1. GlobalProtect establece un túnel SSL entre el endpoint de GlobalProtect y la puerta de enlace de Prisma Access.
2. GlobalProtect envía el nombre de host, el nombre de dominio y la información de la dirección IP del túnel del dispositivo del usuario móvil a través del túnel al servidor local o puerta de enlace de Prisma Access.
3. Prisma Access proporciona actualizaciones DDNS de registros A y PTR utilizando nsupdate al servidor DNS. Prisma Access proporciona estas actualizaciones seguras en tiempo real cuando procesa eventos de inicio y cierre de sesión.
4. El administrador de TI o un software empresarial utiliza estos registros a través de una búsqueda DNS o RDNS, y resuelve el nombre del endpoint o la dirección IP.
5. El administrador de TI o el software de gestión de endpoints utiliza esta información para gestionar el endpoint o enviar actualizaciones de software.



Requisitos de conectividad de red

Antes de implementar esta solución, asegúrese de que su red tenga los siguientes requisitos en su lugar:

©2025 Palo Alto Networks, Inc.

- Ha añadido rutas para asegurar la conectividad al servidor DNS desde el MU-SPN y desde las conexiones de servicio de Prisma Access.

  Para hacer esto, añada rutas desde la Subred de Infraestructura de Prisma Access, que puede encontrar en **Workflows (Flujos de trabajo)** > > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Infrastructure Subnet (Subred de infraestructura)** y el grupo de direcciones IP de Usuarios móviles—GlobalProtect, que puede encontrar en **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Client IP Pool (Grupo de IPs del cliente)**.
- Ha establecido conectividad al crear una conexión de servicio entre Prisma Access y el dispositivo de terminación IPSec (por ejemplo, un cortafuegos o enrutador de nueva generación) que tiene conectividad con el servidor DNS.
- Se ha asegurado de que su servidor DNS sea accesible a través del túnel de conexión de servicio IPSec.
- Ha verificado que los comandos nsupdate enviados desde Prisma Access Usuarios Móviles —nodos de procesamiento de seguridad GlobalProtect (SPNs) están permitidos y pueden alcanzar el servidor DNS.

  Los pasos que realiza para lograr esta conectividad difieren según la ubicación y el tipo de servidor DNS que se utilice. Por ejemplo:

  - Si el servidor DNS está en el centro de datos, puede configurar la conectividad utilizando túneles IPSec desde el SPN de Usuarios móviles—GlobalProtect a las conexiones de servicio, y luego desde la conexión de servicio al enrutador de puerta de enlace (por ejemplo, un cortafuegos de nueva generación configurado como una VM) detrás del cual existe el servidor DNS.
  - Si el servidor DNS está en la nube, puede lograr conectividad con el servidor DNS desde el SPN de Usuarios móviles—GlobalProtect utilizando las reglas de política de seguridad apropiadas.
- Ha configurado zonas de búsqueda directa e inversa en los servidores DNS.
- Ha implementado un servidor DNS de Infoblox, Bluecat o Windows que soporta nsupdate.
- Si mantiene permisos para zonas de forma individual, asegúrese de haber creado reglas de políticas de seguridad para permitir nsupdates desde dispositivos que tengan la clave TSIG o Kerberos correcta.

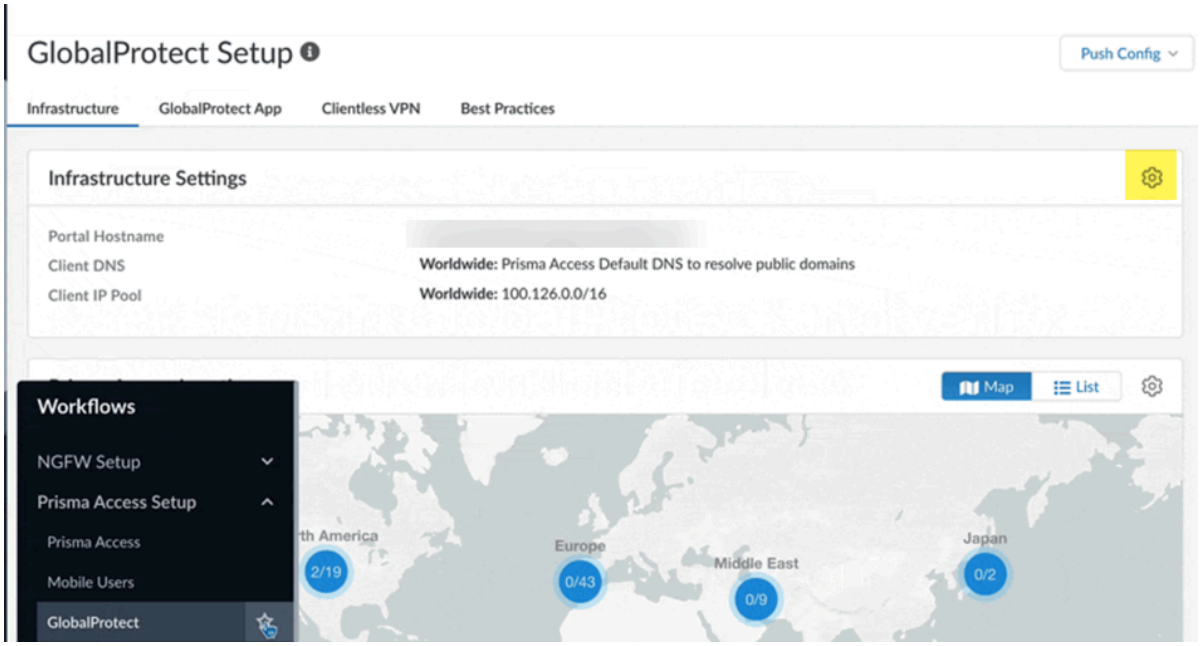
Para configurar esta solución, utilice uno de los siguientes procedimientos, según su tipo de implementación.

- Gestión de la nube
- Panorama

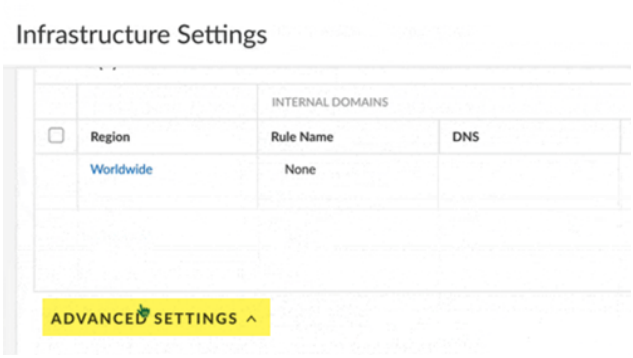
Configurar actualizaciones de DNS dinámico para Prisma Access (Managed by Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Desde Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **GlobalProtect** y haga clic en el engranaje para editar la **Infrastructure Settings (Configuración de infraestructura)**.



STEP 2 | Seleccione **Advanced Settings (Configuración avanzada)**.



STEP 3 | Configure los ajustes de la **Dynamic DNS Support (Compatibilidad con DNS dinámico)**.

1. Seleccione **Dynamic DNS Support for GlobalProtect (Compatibilidad con DNS dinámico para GlobalProtect)**.
2. Seleccione el **Domain Type (Tipo de dominio)**.

   - **Fallback Domain (Dominio alternativo)**: el dominio utilizado para los eventos de nsupdate vuelve al dominio que especifique en el área **Fallback Domain (Dominio alternativo)**. Utilice esta opción si los clientes de GlobalProtect no están unidos a ningún dominio o si están unidos a un dominio que es el mismo que el que utiliza el servicio DDNS para actualizar los registros en el servidor DNS.

     Si selecciona **Fallback Domain (Dominio alternativo)** y los usuarios que no están conectados a un dominio inician sesión en GlobalProtect, su información se añade bajo la zona de dominio alternativo que se crea en el servidor DNS.

     Si los clientes de GlobalProtect que están iniciando sesión en GlobalProtect pertenecen a un dominio inesperado que no está configurado en el servidor DNS,

 ©2025 Palo Alto Networks, Inc.

nsupdate podría fallar; en este caso, seleccione **Override Domain (Sobrescribir dominio)** para sobrescribir el dominio desconocido con el dominio que es conocido por el servidor DNS.

- **Override Domain (Dominio de anulación)**: Prisma Access utiliza solo el dominio especificado para actualizar el servidor DNS y anula todos los demás dominios. Si los clientes de GlobalProtect inician sesión en otro dominio, el servicio DDNS utiliza el dominio que especifique aquí para actualizar los registros DNS A y PTR.

3. Seleccione el dominio que se utiliza para actualizar los registros PTR para dominios de respaldo o de anulación en el campo **Fallback Domain (Dominio alternativo)**.
4. Seleccione la dirección **DNS Server IP (IP del servidor DNS)**.
5. Seleccione el **Server Type (Tipo de servidor)** (ya sea **TSIG** o **Kerberos**).
6. (Solo implementaciones de TSIG) Seleccione la **TSIG Key (Clave TSIG)** para usar con TSIG.

   Asegúrese de que el archivo TSIG esté en el formato correcto y tenga una extensión de archivo .key.

   Si selecciona un tipo de autenticación Kerberos, sube una clave de autenticación a través de un archivo .key que contenga el archivo keytab de Kerberos sin codificar recuperado del servidor DNS.

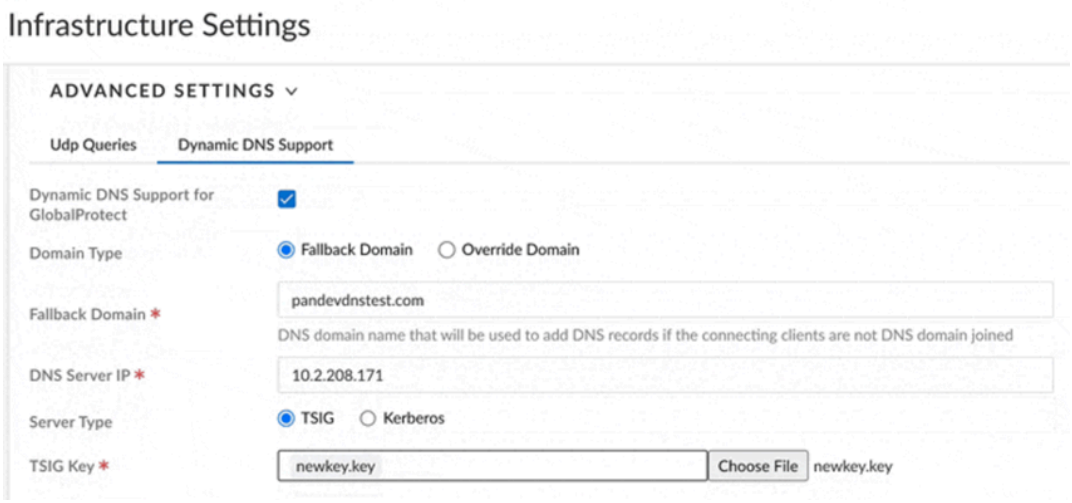
   El archivo TSIG debe estar en el siguiente formato:

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```

 ©2025 Palo Alto Networks, Inc.

7. (Solo implementaciones de Kerberos) Especifique las opciones de Kerberos a utilizar.
   - Introduzca la dirección IP del **Kerberos Domain Controller (Controlador de dominio Kerberos)**.
   - Introduzca la dirección IP del **Kerberos Admin Server (Servidor de gestión de Kerberos)**.
   - Introduzca el **Kerberos User Name (Nombre de usuario de Kerberos)**.
   - Introduzca la **Kerberos Key (Clave de Kerberos)** (el keytab) que se va a utilizar.

     Asegúrese de que la clave de Kerberos esté en el formato correcto.



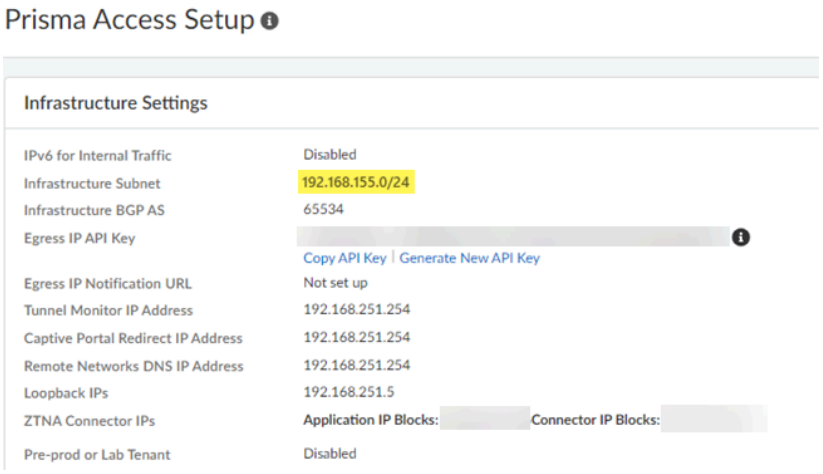
STEP 4 | Haga clic en **Save (Guardar)** para guardar sus cambios.

 ©2025 Palo Alto Networks, Inc.

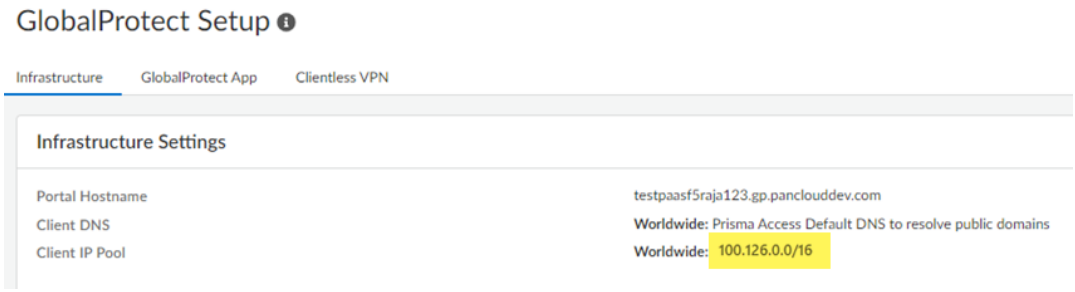
STEP 5 | Configurar zonas de búsqueda de reenvío y zonas de búsqueda inversa en su servidor DNS.

Consulte la documentación de su proveedor de IPAM para configurar estas zonas. Este paso requiere que introduzca la **Infrastructure Subnet (Subred de Infraestructura)** y el **Client IP Pool (grupo de direcciones IP del cliente)** de Prisma Access.

- Para encontrar la subred de infraestructura, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** y tome nota de la **Infrastructure Subnet (Subred de Infraestructura)**.



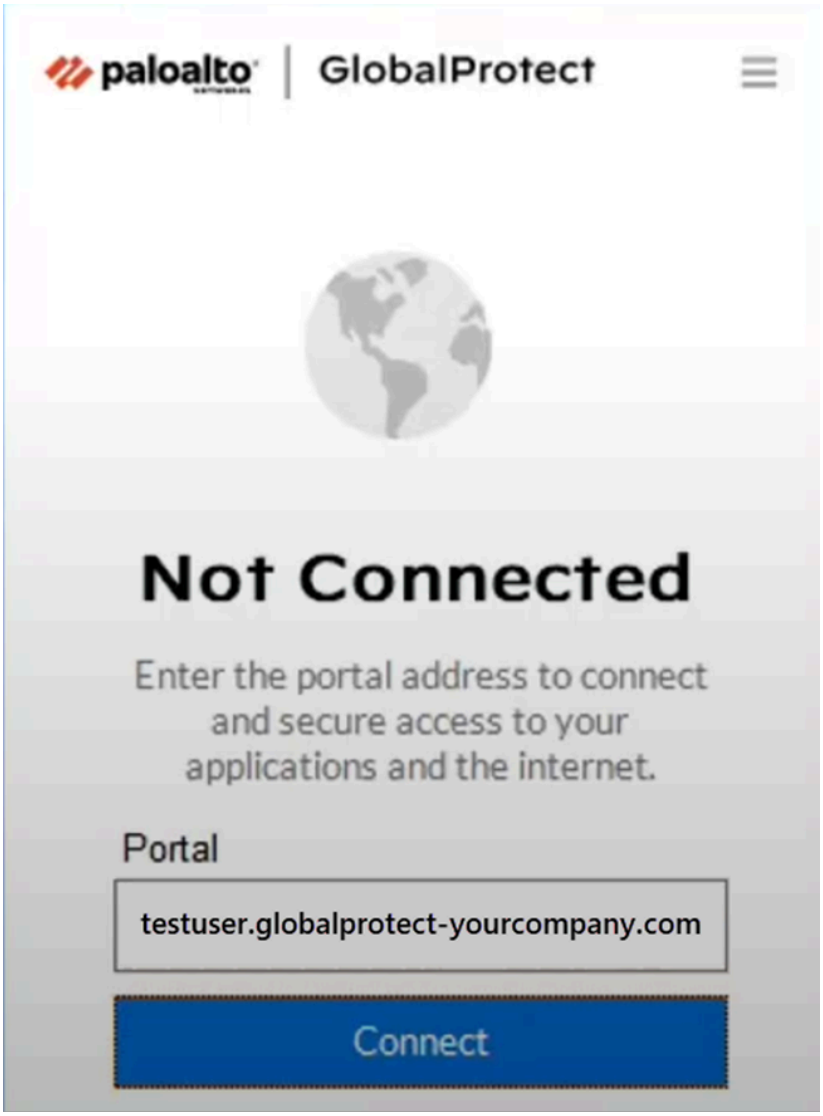
- Para encontrar el grupo de direcciones IP de usuarios móviles de GlobalProtect, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** y tome nota del **Client IP Pool (Grupo de IP de cliente)**.



 ©2025 Palo Alto Networks, Inc.

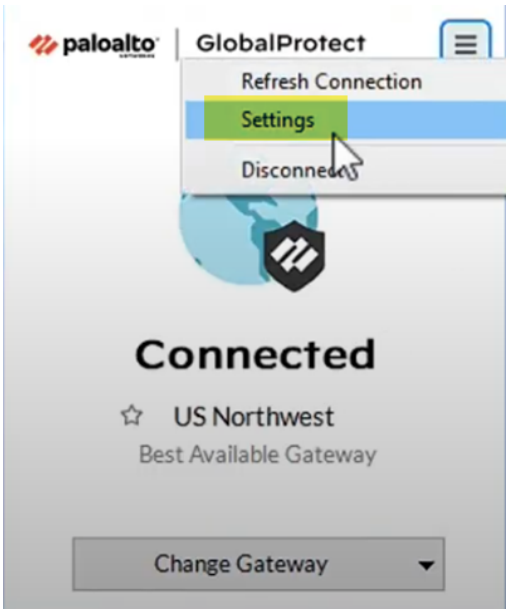
STEP 6 | Verifique que los registros DNS se estén actualizando en el servidor DNS de IPAM.

1. Abra una máquina cliente y conéctela a una puerta de enlace de GlobalProtect de Prisma Access.

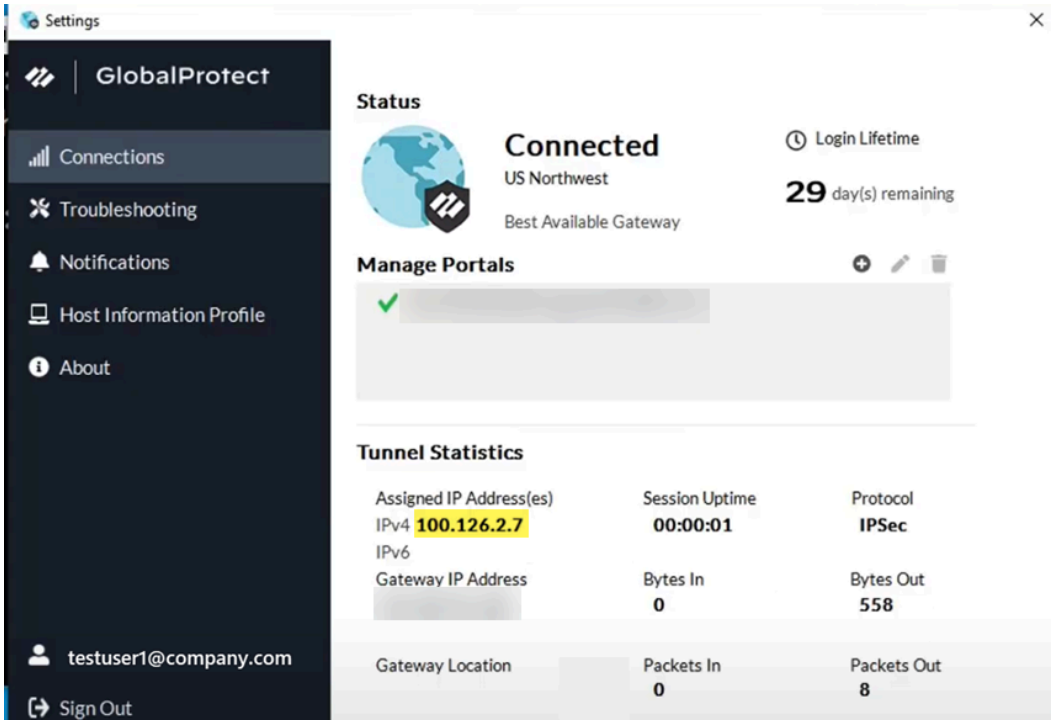


2. Seleccione la **Settings (Configuración)** de GlobalProtect y verifique la dirección IP de GlobalProtect que Prisma Access asignó al usuario.

 ©2025 Palo Alto Networks, Inc.

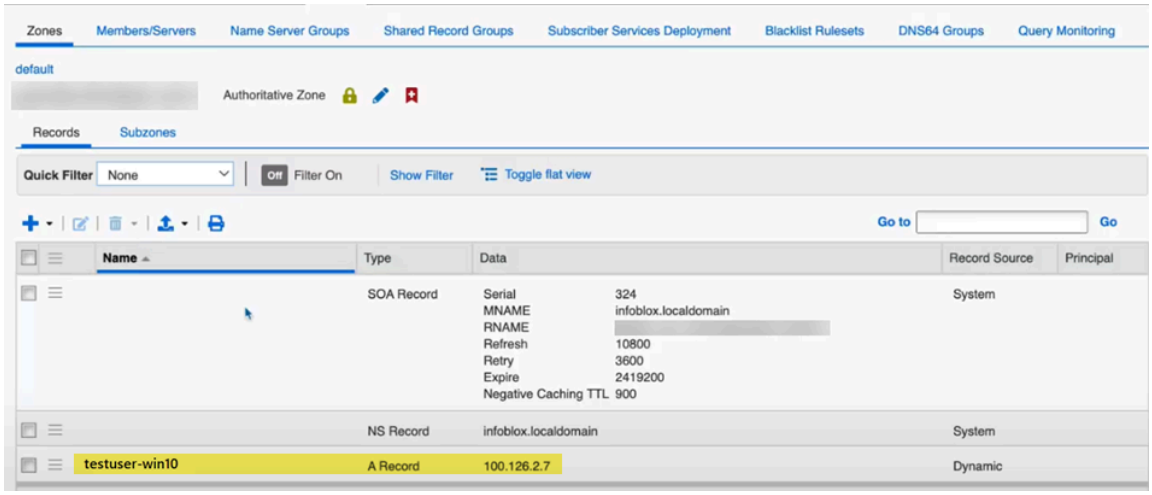


La(s) **Assigned IP Address(es) [Dirección(es) IP asignada(s)]** (100.126.2.7) muestra que la dirección IP proviene del grupo de direcciones IP de GlobalProtect (100.126.0.0/16).

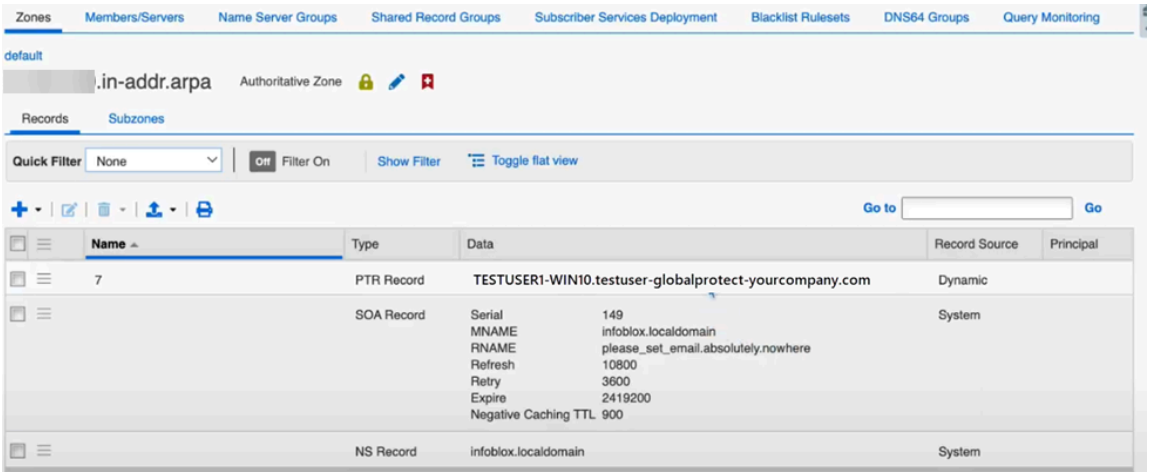


3. Desde el servidor DNS de IPAM, visualice el registro del usuario.
   En este ejemplo, el usuario se llama `testuser1-win10`.

 ©2025 Palo Alto Networks, Inc.



La búsqueda inversa de DNS también muestra el nombre de usuario en el registro PTR.



4. Cierre la sesión del usuario de GlobalProtect y verifique los registros para asegurarse de que el servidor DNS ha eliminado los registros del usuario.

Configurar actualizaciones de DNS dinámico para Prisma Access (Managed by Panorama)

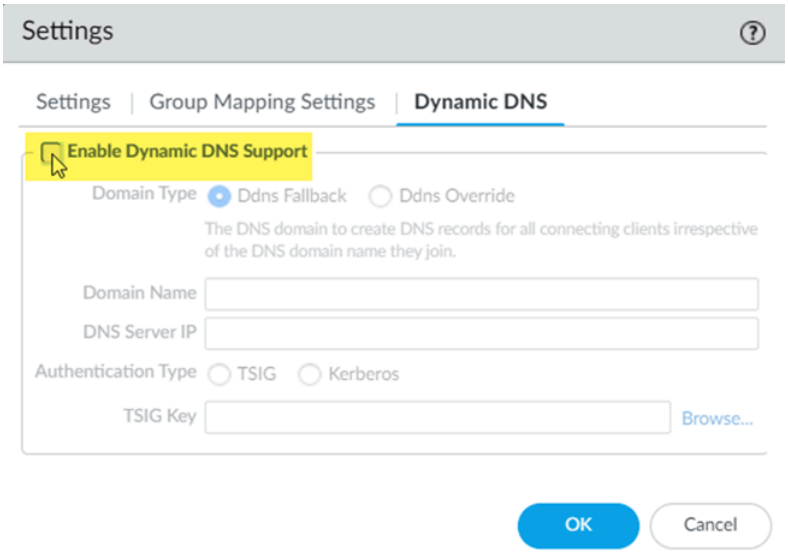
Para configurar actualizaciones dinámicas de DNS para Prisma Access (Managed by Panorama), complete estos pasos.

STEP 1 | Desde Panorama, vaya a **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles—GlobalProtect)** y haga clic en el engranaje para editar el archivo **Settings (Configuración)**.

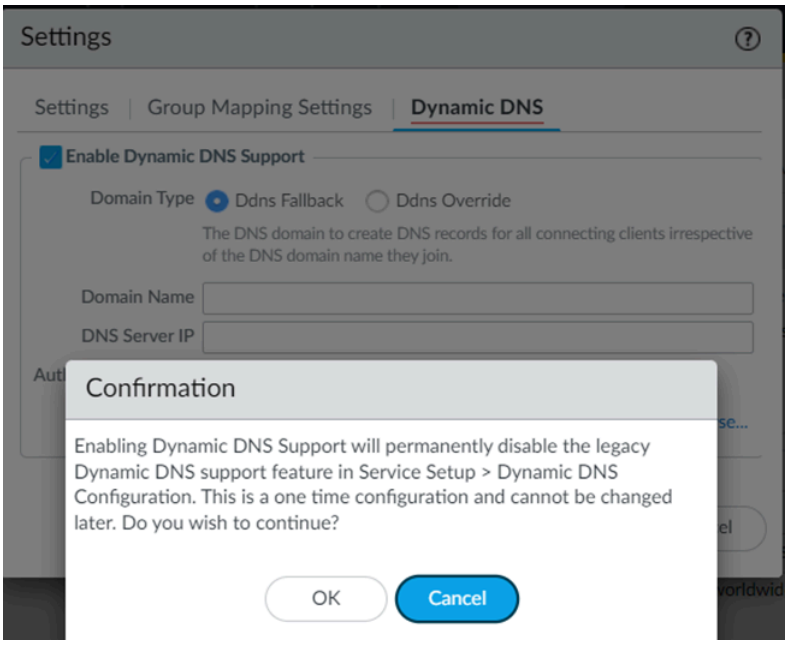
STEP 2 | Seleccione **Dynamic DNS (DNS dinámico)**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | **Enable Dynamic DNS Support (Habilitar compatibilidad con DNS dinámico)**



STEP 4 | Se le indica que, si tiene habilitada la compatibilidad con DNS dinámico heredada, a habilitar la compatibilidad actualizada se deshabilitará permanentemente la compatibilidad heredada. Haga clic en **OK (Aceptar)** para continuar.



STEP 5 | Configure los ajustes de **Dynamic DNS (DNS dinámico)**.

1. Seleccione **Enable Dynamic DNS Support (Habilitar la compatibilidad con DNS dinámico)**.
2. Seleccione el **Domain Type (Tipo de dominio)**.
   - **Ddns Fallback (Alternativa de Ddns)**: el dominio utilizado para los eventos nsupdate se revierte en el dominio especificado en el área **Domain Name (Nombre de dominio)**. Utilice esta opción si los clientes de GlobalProtect no están unidos a ningún dominio o

 ©2025 Palo Alto Networks, Inc.

si están unidos a un dominio que es el mismo que el que utiliza el servicio DDNS para actualizar los registros en el servidor DNS.

Si selecciona **Ddns Fallback (Alternativa de Ddns)** y los usuarios que no están conectados a un dominio inician sesión en GlobalProtect, su información se añade en la zona de Alternativa de Ddns que se crea en el servidor DNS.

Si los clientes de GlobalProtect que están iniciando sesión en GlobalProtect pertenecen a un dominio inesperado que no está configurado en el servidor DNS, nsupdate podría fallar; en este caso, seleccione **Ddns Override (Anulación de Ddns)** para sobrescribir el dominio desconocido con el dominio que es conocido por el servidor DNS.

- **Ddns Override (Anulación de ddns)**: Prisma Access utiliza solo el dominio especificado para actualizar el servidor DNS y anula todos los demás dominios. Si los clientes de GlobalProtect inician sesión en otro dominio, el servicio DDNS utiliza el dominio que especifique aquí para actualizar los registros DNS A y PTR.

3. Seleccione el dominio que se utiliza para actualizar los registros PTR para nombres de dominio o de reserva en el campo **Domain Name (Nombre de dominio)**.
4. Seleccione la dirección **DNS Server IP (IP del servidor DNS)**.
5. Seleccione el **Authentication Type (Tipo de autenticación)** (ya sea **TSIG** o **Kerberos**).
6. (Solo implementaciones de TSIG) Seleccione la **TSIG Key (Clave TSIG)** para usar con TSIG.

   Asegúrese de que el archivo TSIG esté en el formato correcto y tenga un tipo de archivo de .key.

   - Si está ejecutando una implementación gestionada de Panorama con una versión de complemento de la versión 5.2.0 o superior y elige un tipo de autenticación Kerberos, cargue una clave de autenticación a través de un archivo .key que tenga la cadena codificada en base64 de la clave Kerberos recuperada del servidor DNS, por ejemplo: `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcDluaXN0cmF0b3IAAAABAAAAAEAEgA`
   - Si está ejecutando una implementación gestionada de Panorama con una versión de complemento inferior a 5.1.0 y elige un tipo de autenticación Kerberos, cargue una clave de autenticación a través de un archivo .key que tenga el archivo keytab de Kerberos sin codificar recuperado del servidor DNS.

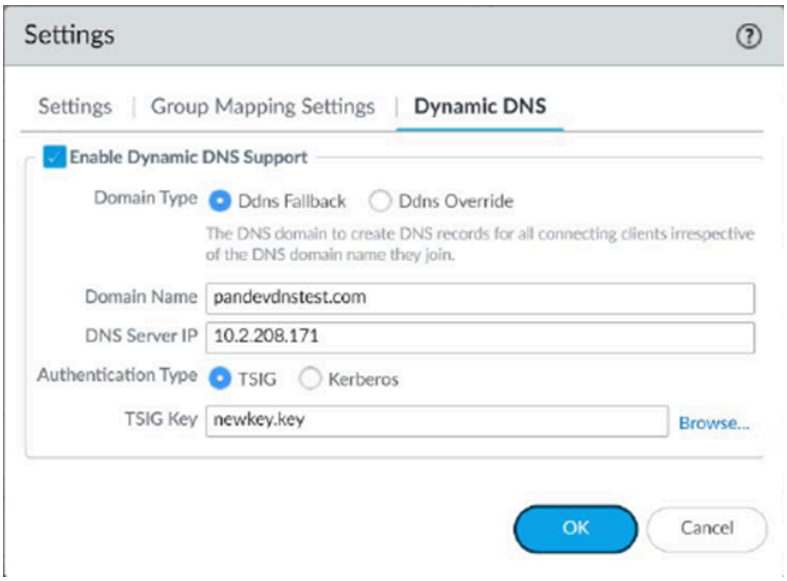
   El archivo TSIG debe estar en el siguiente formato:

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```

 ©2025 Palo Alto Networks, Inc.

7. (Solo implementaciones de Kerberos) Especifique las opciones de Kerberos a utilizar.
   - Introduzca la dirección IP del **Kerberos Domain Controller (Controlador de dominio Kerberos)**.
   - Introduzca la dirección IP del **Kerberos Admin Server (Servidor de gestión de Kerberos)**.
   - Introduzca el **Kerberos User Name (Nombre de usuario de Kerberos)**.
   - Introduzca la **Kerberos Key (Clave de Kerberos)** (el keytab) que se va a utilizar.

     Utilice la codificación base64 en la clave Kerberos antes de cargarla.



STEP 6 | Haga clic en **Save (Guardar)** para guardar sus cambios.

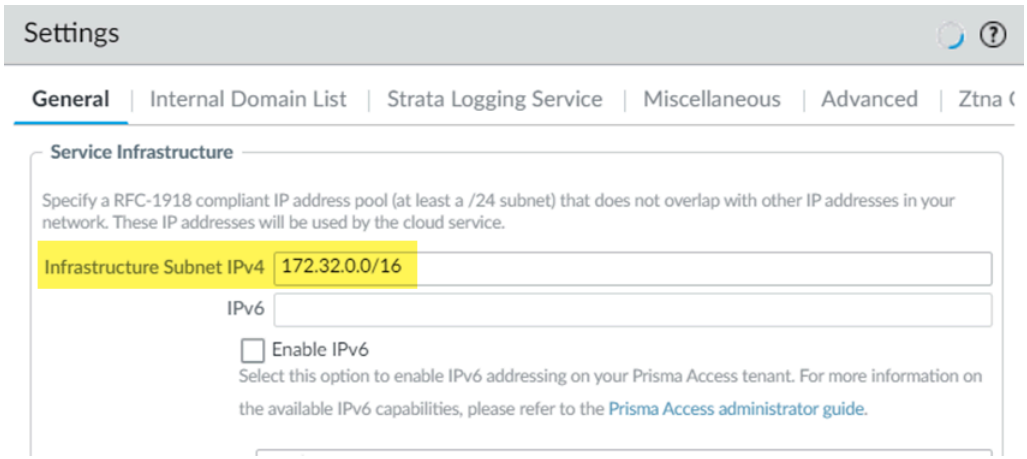
STEP 7 | Configurar zonas de búsqueda de reenvío y zonas de búsqueda inversa en su servidor DNS.

Consulte la documentación de su proveedor de IPAM para configurar estas zonas. Este paso requiere que introduzca la **Infrastructure Subnet (Subred de Infraestructura)** y el **Client IP Pool (grupo de direcciones IP del cliente)** de Prisma Access.

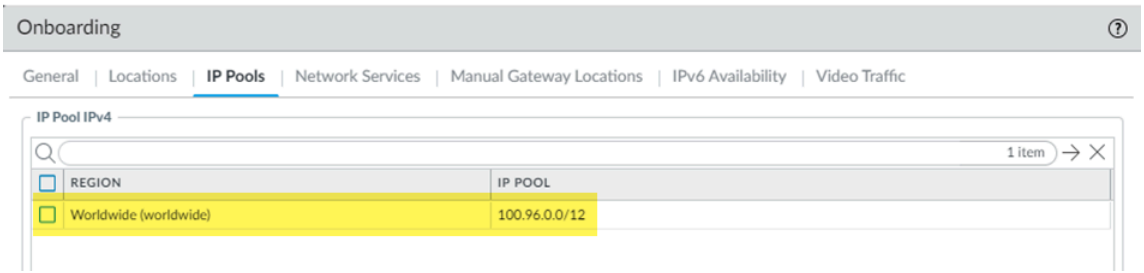
- Para encontrar la subred de infraestructura, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**, haga

 ©2025 Palo Alto Networks, Inc.

clic en el engranaje para editar la **Settings (Configuración)** y tome nota de la **Infrastructure Subnet IPv4 (Subred de infraestructura IPv4)**.



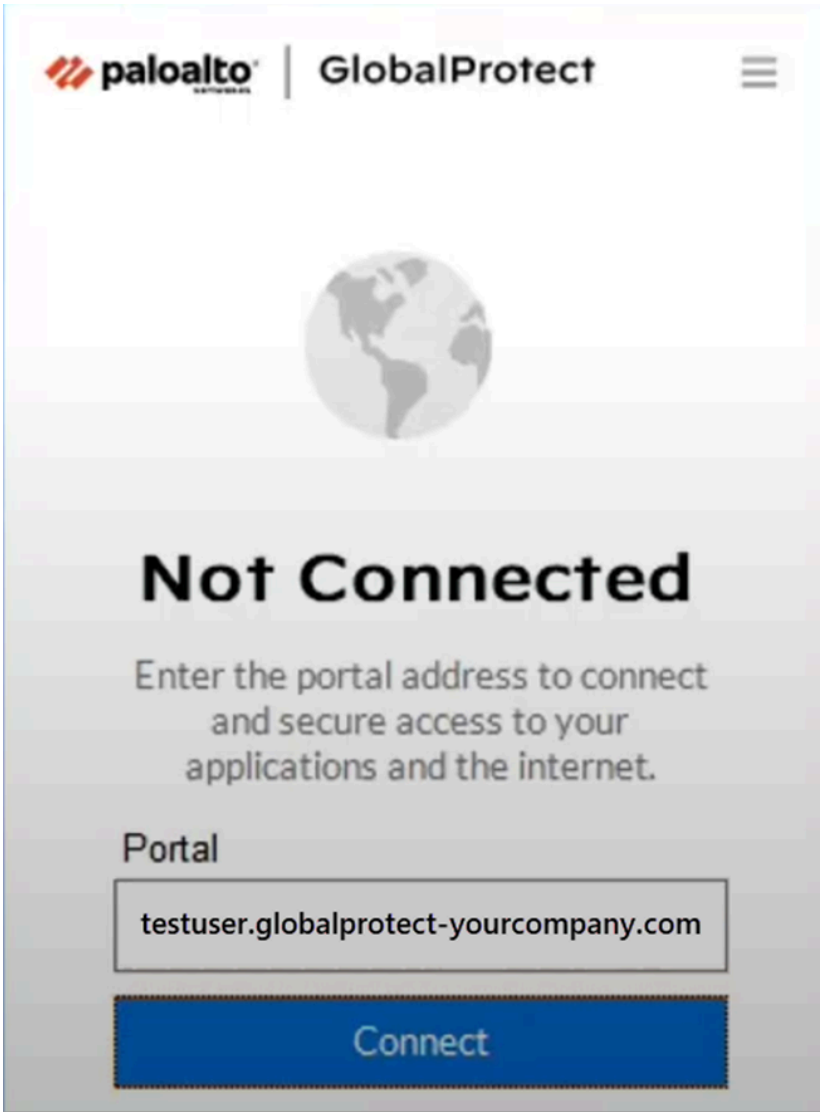
- Para encontrar el grupo de direcciones IP de usuarios móviles de GlobalProtect, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Mobile Users—GlobalProtect (Usuarios móviles—GlobalProtect)**, seleccione la opción **Hostname (Nombre de host)**, seleccione **IP Pools (Grupos de IP)** y tome nota del **IP Pool IPv4 (Grupo de IP IPv4)**.



 ©2025 Palo Alto Networks, Inc.

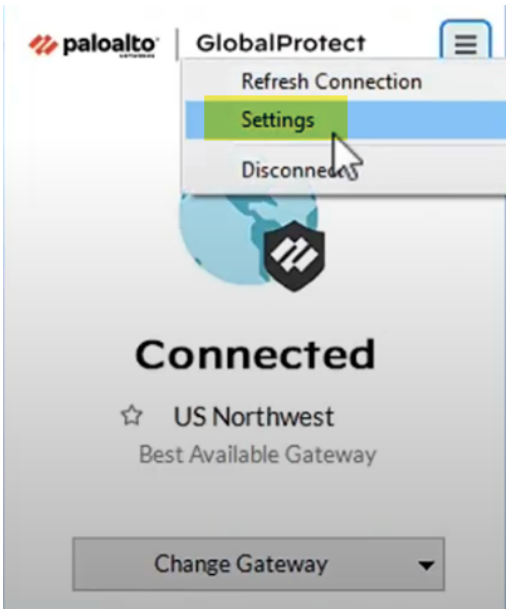
STEP 8 | Verifique que los registros DNS se estén actualizando en el servidor DNS de IPAM.

1. Abra una máquina cliente y conéctela a una puerta de enlace de GlobalProtect de Prisma Access.

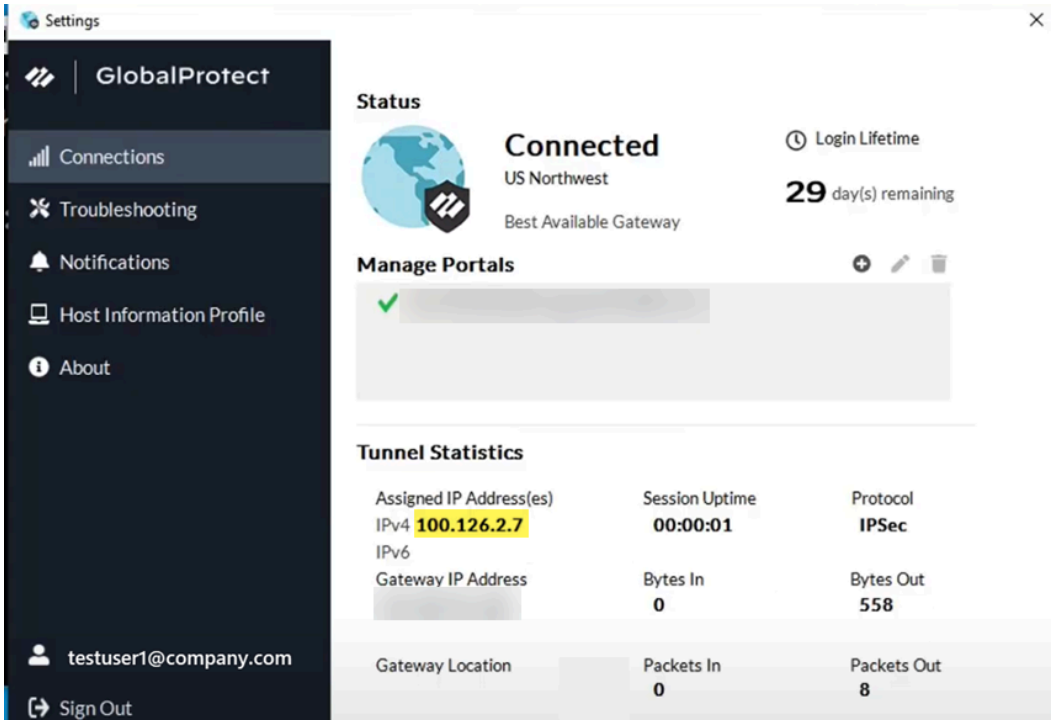


2. Seleccione la **Settings (Configuración)** de GlobalProtect y verifique la dirección IP de GlobalProtect que Prisma Access asignó al usuario.

 ©2025 Palo Alto Networks, Inc.

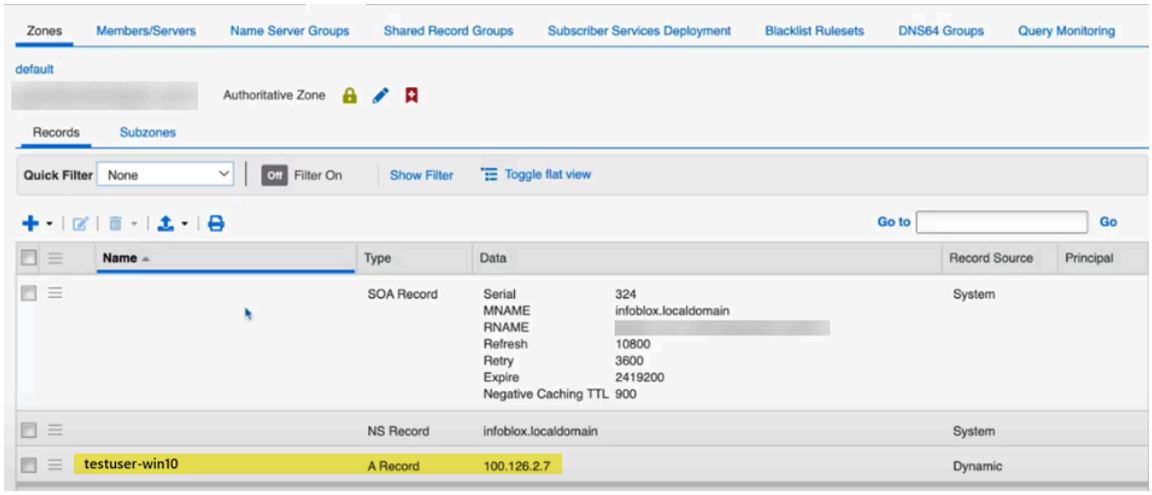


La(s) **Assigned IP Address(es) [Dirección(es) IP asignada(s)]** (100.126.2.7) muestra que la dirección IP proviene del grupo de direcciones IP de GlobalProtect (100.126.0.0/16).

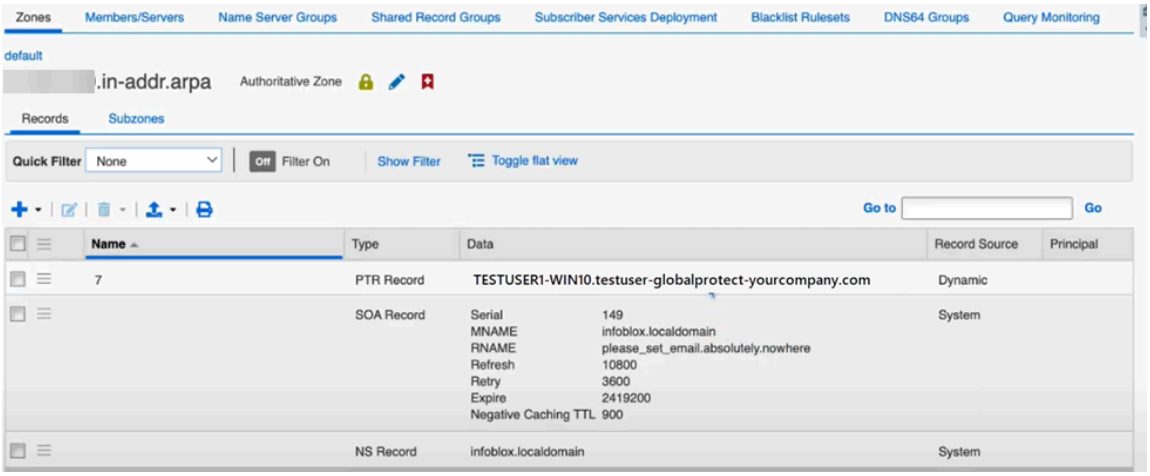


3. Desde el servidor DNS de IPAM, visualice el registro del usuario.
   En este ejemplo, el usuario se llama `testuser1-win10`.

 ©2025 Palo Alto Networks, Inc.



La búsqueda inversa de DNS también muestra el nombre de usuario en el registro PTR.



4. Cierre la sesión del usuario de GlobalProtect y verifique los registros para asegurarse de que el servidor DNS ha eliminado los registros del usuario.

Compatibilidad con el registro de DNS dinámico para usuarios móviles: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Cortafuegos de nueva generación gestionados por Panorama con una licencia válida de Strata Logging Service y un complemento Cloud Services	☐ Licencia de Prisma Access ☐ Minimum Required Prisma Access Version: 3.1.1 Preferred o Innovation ☐ Compatible con dispositivos Panorama que ejecutan versiones 10.2 y posteriores (no compatible con dispositivos Panorama que ejecutan 10.1) ☐ Los endpoints de cliente deben estar unidos al dominio.

 ©2025 Palo Alto Networks, Inc.

Esta funcionalidad está disponible para implementaciones de Prisma Access que comienzan con Prisma Access (Managed by Panorama) 3.1.1.

Esta funcionalidad no está disponible para implementaciones de Prisma Access (Managed by Strata Cloud Manager).

Cuando un usuario móvil se conecta de forma remota a Prisma Access usando GlobalProtect, los servidores DNS de su empresa no se actualizan con la dirección IP asignada por la puerta de enlace de GlobalProtect. Antes de habilitar el DNS dinámico (DDNS), no existe ninguna asignación de direcciones IP del túnel con el nombre del endpoint, que se registran como registros de dirección y puntero (A y PTR). Por lo tanto, su administrador de TI o el software de gestión de usuarios no pueden asignar el nombre del endpoint remoto a la dirección IP.

Después de habilitar la función DDNS en Prisma Access, el complemento Cloud Services de Prisma Access comprueba los eventos de GlobalProtect en el Strata Logging Service cada 15 minutos para capturar el nombre de host del endpoint, el nombre de dominio y la dirección IP del túnel. Crea registros A y PTR de forma dinámica en el servidor DNS utilizando NSUPDATE.

Flujo de trabajo de DNS dinámico para usuarios móviles: GlobalProtect

Después de habilitar DDNS y cuando un usuario móvil inicia sesión con la aplicación GlobalProtect:

Lea las siguientes secciones para obtener una descripción general de cómo funciona el DDNS, las pautas y los requisitos, y cómo habilitarlo.

1. GlobalProtect establece un túnel SSL entre el endpoint de GlobalProtect y un servidor local o puerta de enlace de Prisma Access.
2. GlobalProtect envía el nombre de host, el nombre de dominio y la información de la dirección IP del túnel del dispositivo del usuario móvil a través del túnel al servidor local o puerta de enlace de Prisma Access.
3. La puerta de enlace local o Prisma Access reenvía esta información como eventos de GlobalProtect a Strata Logging Service.
4. El complemento Cloud Services de Prisma Access sondea el Strata Logging Service cada 15 minutos para actualizar el servidor DNS.

   Si el complemento no recibe los eventos de GlobalProtect desde Strata Logging Service, este vuelva a intentar la solicitud un máximo de cinco veces. Si las solicitudes de reintento no se realizaron correctamente, el complemento vuelve a intentar la operación cada 15 minutos un máximo de cuatro veces. Por lo tanto, el complemento puede recibir actualizaciones durante un intervalo de tiempo de una hora.

   Si desea actualizaciones más frecuentes, puede introducir el comando `debug plugins cloud_services set-gp-ddns-interval` para cambiar el intervalo de actualización a cinco minutos. No es necesario para actualizar el intervalo de tiempo. Si cambia el intervalo a cinco minutos, el complemento Cloud Services puede actualizar un máximo de 15.000 registros con una latencia de red de 50 ms y puede recibir actualizaciones durante un intervalo de tiempo de 20 minutos.

   - *No es necesario **Commit (Confirmar)** después de cambiar el intervalo de tiempo mediante el comando.*
   - *Estos números provienen de un entorno controlado y las condiciones de funcionamiento del mundo real pueden afectar estos números.*

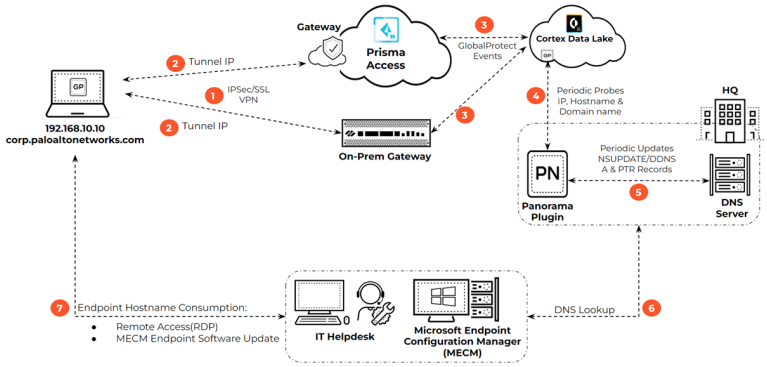
 ©2025 Palo Alto Networks, Inc.

5. Después de recibir las actualizaciones de Strata Logging Service, el complemento Cloud Services empaqueta los registros A y PTR como NSUPDATE y actualiza el servidor DNS principal cada 15 minutos.

   Si cambia el intervalo de tiempo a cinco minutos usando el comando `debug plugins cloud_services set-gp-ddns-interval`, el complemento actualiza el servidor DNS cada cinco minutos.

   Si el complemento no puede actualizar el servidor DNS a través de NSUPDATE, el complemento vuelve a intentar la operación de actualización un máximo de cinco veces. Si las actualizaciones no se realizaron correctamente, el complemento vuelve a intentar la operación de actualización cada 15 minutos, o cada cinco minutos si cambió el intervalo a cinco minutos, durante un máximo de cuatro veces. Por lo tanto, el complemento intenta actualizar los eventos que se registran durante un máximo de una hora (si usa un intervalo de 15 minutos) o 20 minutos (si usa un intervalo de cinco minutos), después de lo cual comienza de nuevo.
6. Una vez que los registros A y PTR de los usuarios móviles de GlobalProtect están disponibles en el servidor DNS, un administrador de TI o un software empresarial utiliza estos registros a través de una búsqueda de DNS o RDNS, y resuelve el nombre del endpoint o la dirección IP.
7. El administrador de TI o el software de gestión de endpoints utiliza esta información para gestionar el endpoint o enviar actualizaciones de software.

La siguiente figura ilustra este flujo de trabajo.



*Para ver los logs de errores de conexión, seleccione **Dashboard (Panel)** > **System Logs (Logs del sistema)** o **Monitor (Supervisar)** > **Logs** > **System (Sistema)** para **Mobile_User_Device_Group**.*

Directrices y requisitos de DNS dinámico

Antes de habilitar DDNS, asegúrese de que su implementación y servidor DNS cumplan con las siguientes pautas y requisitos:

- Los endpoints de cliente deben estar unidos al dominio.
- Actualice su cliente GlobalProtect a las siguientes versiones de la aplicación GlobalProtect según su sistema operativo:
  - Windows: 5.2.11 o posterior
  - Mac: 5.2.11 o posterior
  - Linux: 5.3.3 o posterior

 ©2025 Palo Alto Networks, Inc.

- Enable (Habilitar)Strata Logging Service si utiliza una puerta de enlace local distinta a Prisma Access.
- Se requiere un servidor DNS Infoblox con una versión mínima de 8.6.1 o posterior que admita actualizaciones de DDNS a través de NSUPDATE.
- Las implementaciones de varios inquilinos de Prisma Access no admiten DDNS.
- Guarde la clave de autenticación de su servidor DNS en formato base64 con una extensión de archivo .key. Puede cargar la clave solo en este formato en Prisma Access.
- Habilite NTP en su servidor DNS y asegúrese de que sea el mismo que el de Prisma Access.
- Cree zonas en Infoblox para direcciones PTR inversas y A directas.

Puede implementar DNS dinámico en una implementación independiente con cortafuegos de nueva generación y también con Prisma Access. Para los cortafuegos, se aplican todos los requisitos previos de esta sección y también debe tener una licencia válida de Strata Logging Service y utilice el complemento Cloud Services en Panorama *para el registro de logs.*

Habilitar DDNS para Usuarios móviles: GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para actualizar su servidor DNS con los registros A y PTR de sus usuarios móviles de GlobalProtect, complete los siguientes pasos.

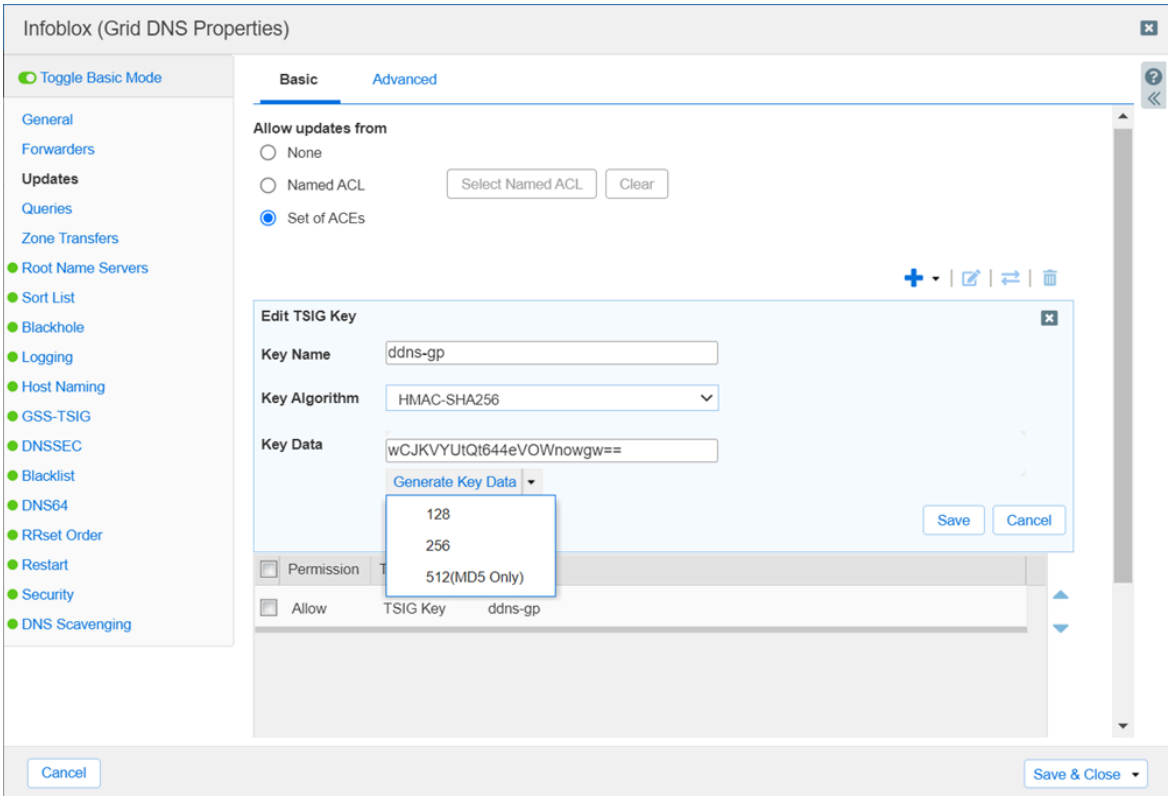
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Cree una clave de autenticación en su servidor DNS.

Este ejemplo utiliza Infoblox como servidor DNS.

1. Inicie sesión en su servidor DNS.
2. Seleccione **Data Management (Gestión de datos)** > **DNS** > **Grid DNS Properties (Propiedades de Grid DNS)** > **Updates (Actualizaciones)**.
3. Permitir actualizaciones desde el **Set of ACEs (Conjunto de ACE)**.
4. Añada una **TSIG Key (Clave TSIG)** después de completar los detalles.

   - *Seleccione el algoritmo de clave de **256** bits.*
   - ***Generate Key Data (Generar datos de clave)** para crear una nueva clave. Seleccione los datos de clave de **256** bits.*



5. Copie los datos clave a un archivo con el siguiente formato y guarde el archivo con la extensión .key.

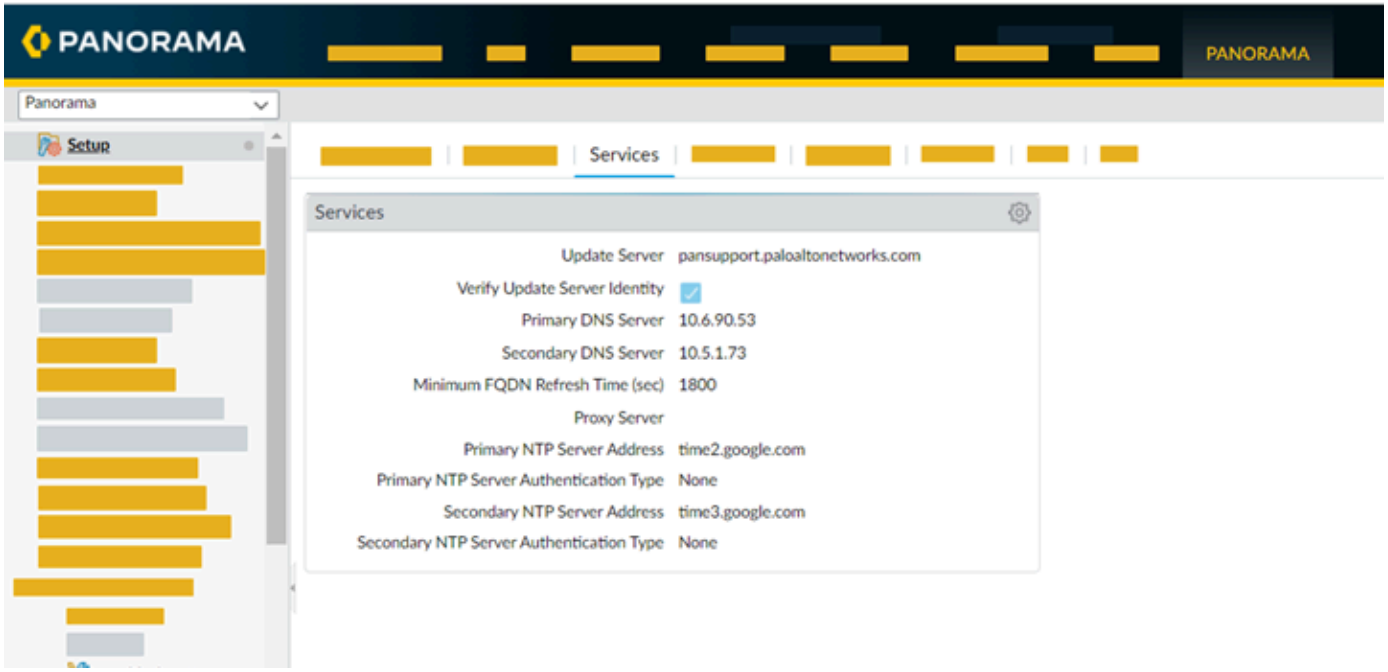
```
key "ddns-gp" { algorithm hmac-sha256; secret
 "wCJKVYUtQt644eVOWnowgw==";  };
```

Cargue esta clave al complemento Cloud Services de Prisma Access en un paso posterior.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | En su implementación de Prisma Access, especifique su servidor DNS como el servidor DNS principal.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Services (Servicios)**.
2. Debe **Edit (Editar)** la configuración y actualice los detalles del servidor DNS principal.

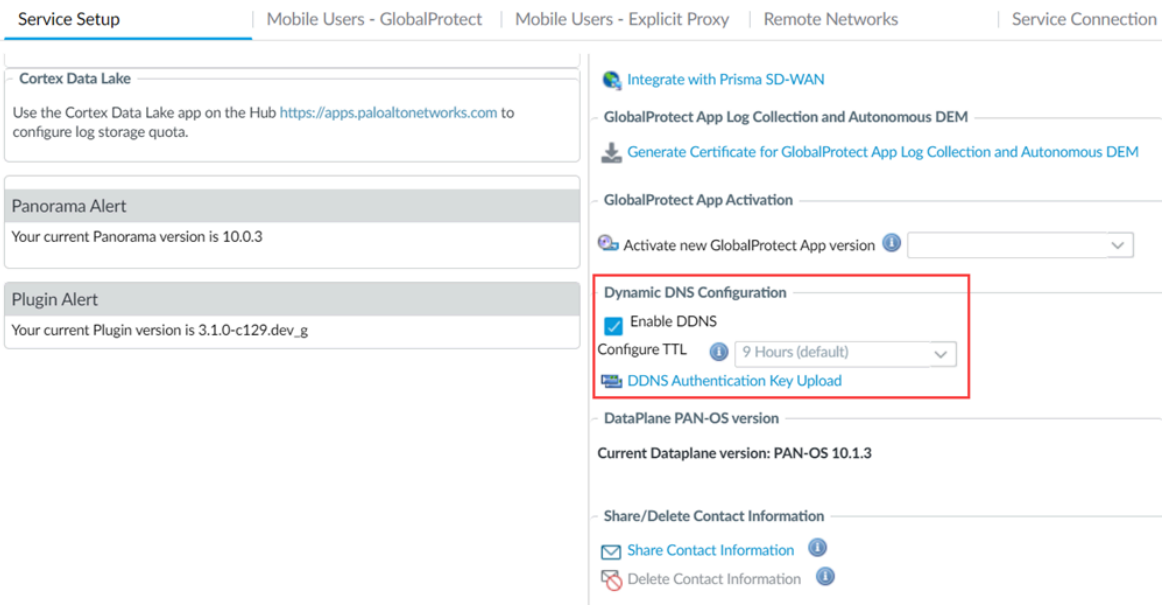


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configure los ajustes DDNS.

1. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.
2. Seleccione **Service Operations (Operaciones de servicio)** > **Dynamic DNS Configuration (Configuración de DNS dinámico)** y **Enable DDNS (Habilitar DDNS)**.
3. (Opcional) **Configure TTL (Configurar TTL)**, el valor de tiempo de vida (TTL), a la frecuencia que desee que Prisma Access actualice FDQN en su caché.

   El valor se establece en 9 horas de forma predeterminada.



4. Cargue la clave de autenticación DDNS que creó en el paso 1 desde su servidor DNS.

STEP 4 | **Commit to Panorama (Confirmar en Panorama)**.

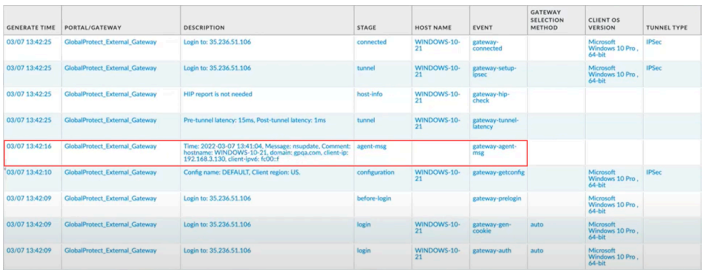
Verificar la configuración de DNS dinámico

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

Después de haber habilitado DDNS, supervise los logs y solucione cualquier problema revisando los siguientes componentes de Prisma Access.

Seleccionar **Monitor (Supervisar)** > **Logs** > **GlobalProtect**. El mensaje del agente de puerta de enlace contiene el nombre del host, el nombre de dominio y la información de la dirección IP del túnel. GlobalProtect envía el mensaje del agente solo si el endpoint es parte de un dominio o AD.

 ©2025 Palo Alto Networks, Inc.



GENERATE TIME	PORTAL/GATEWAY	DESCRIPTION	STAGE	HOST NAME	EVENT	GATEWAY SELECTION METHOD	CLIENT OS VERSION	TUNNEL TYPE
03/07 13:42:25	GlobalProtect_External_Gateway	Login to: 35.236.51.106	connected	WINDOWS-10-21	gateway-connected		Microsoft Windows 10 Pro , 64-bit	IPSec
03/07 13:42:25	GlobalProtect_External_Gateway	Login to: 35.236.51.106	tunnel	WINDOWS-10-21	gateway-setup-ipsec		Microsoft Windows 10 Pro , 64-bit	IPSec
03/07 13:42:25	GlobalProtect_External_Gateway	HIP report is not needed	host-info	WINDOWS-10-21	gateway-hip-check			
03/07 13:42:25	GlobalProtect_External_Gateway	Pre-tunnel latency: 15ms, Post-tunnel latency: 1ms	tunnel	WINDOWS-10-21	gateway-tunnel-latency			
03/07 13:42:16	GlobalProtect_External_Gateway	Time: 2022-03-07 13:41:04, Message: msupdate, Comment: hostname: WINDOWS-10-21, domain: gpqa.com, client-ip: 192.168.3.130, client-ipv6: fc00:f	agent-msg		gateway-agent-msg			
03/07 13:42:10	GlobalProtect_External_Gateway	Config name: DEFAULT, Client region: US.	configuration	WINDOWS-10-21	gateway-getconfig		Microsoft Windows 10 Pro , 64-bit	IPSec
03/07 13:42:09	GlobalProtect_External_Gateway	Login to: 35.236.51.106	before-login		gateway-prelogin		Microsoft Windows 10 Pro , 64-bit	
03/07 13:42:09	GlobalProtect_External_Gateway	Login to: 35.236.51.106	login	WINDOWS-10-21	gateway-gen-cookie	auto	Microsoft Windows 10 Pro , 64-bit	
03/07 13:42:09	GlobalProtect_External_Gateway	Login to: 35.236.51.106	login	WINDOWS-10-21	gateway-auth	auto	Microsoft Windows 10 Pro , 64-bit	

Verifique el comando `gp_ddns_support.log` en la CLI de Panorama para ver otros logs de DDNS.

Identificación y cuarentena de dispositivos en riesgo en una implementación de Prisma Access GlobalProtect

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

Prisma Access le permite identificar y poner en cuarentena los dispositivos comprometidos que están conectados con la aplicación GlobalProtect. Hace esto añadiendo manual o automáticamente dispositivos a una lista de cuarentena. Después de poner en cuarentena el dispositivo, puede bloquear el dispositivo en cuarentena para que no acceda a la red y asegurar una política coherente.

Cada ubicación de usuario móvil de Prisma Access envía y recibe su información de cuarentena entre el Panorama que gestiona Prisma Access y su conexión de servicio más cercana. Si tiene cortafuegos o puertas de enlace de nueva generación, debería hacer que la conexión de servicio redistribuya la información de la lista de cuarentena hacia y desde Panorama y los cortafuegos o puertas de enlace locales. También debería redistribuir la información de la lista de cuarentena de Panorama a la conexión de servicio para garantizar la aplicación coherente de políticas para todas las ubicaciones de usuarios móviles (puertas de enlace) en Prisma Access.

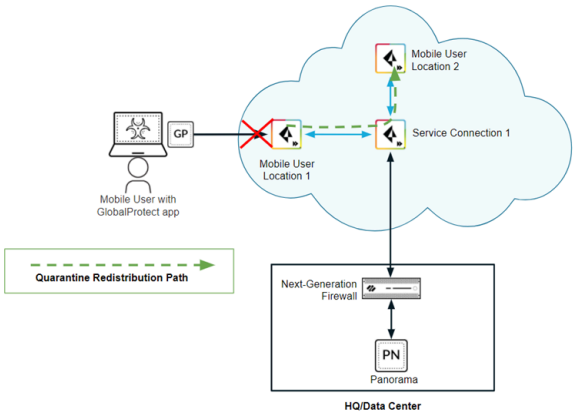
Casos de uso para la redistribución de listas de cuarentena

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

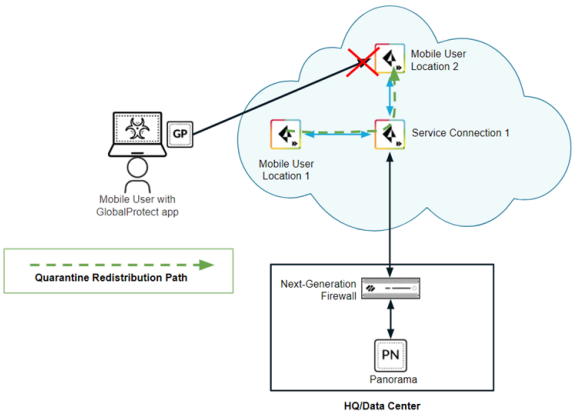
La siguiente sección describe algunos problemas comunes en las implementaciones de Prisma Access donde la redistribución de la lista de cuarentena es útil para la aplicación coherente de políticas para dispositivos comprometidos.

 ©2025 Palo Alto Networks, Inc.

- **Redistribución de la lista de cuarentena entre ubicaciones de usuarios móviles conectadas a la misma conexión de servicio**: en el siguiente ejemplo, un usuario móvil de GlobalProtect que está conectado a la ubicación de usuario móvil 1 se ve comprometido y se pone en cuarentena automáticamente. Prisma Access bloquea o restringe el dispositivo en cuarentena según la política.



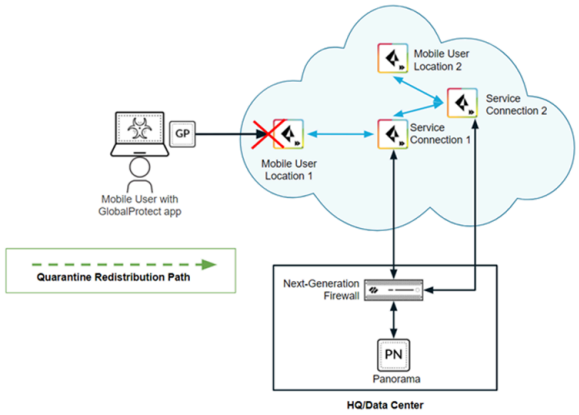
Una conexión de servicio (Conexión de servicio 1 en este ejemplo) redistribuye la información de la lista de cuarentena entre todas las ubicaciones de usuarios móviles a las que está conectada. Dado que la Ubicación de usuario móvil 2 recibe la información de la lista de cuarentena redistribuida a través de la Conexión de servicio 1, el intento del usuario móvil de GlobalProtect de conectarse a la Ubicación de usuario móvil 2 también se bloquea.



- **Redistribución de la lista de cuarentena entre ubicaciones de usuarios móviles conectadas a diferentes conexiones de servicio**: en el siguiente ejemplo, hay dos ubicaciones de usuarios móviles, pero se conectan a dos conexiones de servicio diferentes. Un usuario de GlobalProtect

 ©2025 Palo Alto Networks, Inc.

intentó conectarse a la ubicación de usuario móvil 1. Ubicación de usuario móvil 1 detecta que el endpoint del usuario de GlobalProtect está comprometido y lo pone en cuarentena.

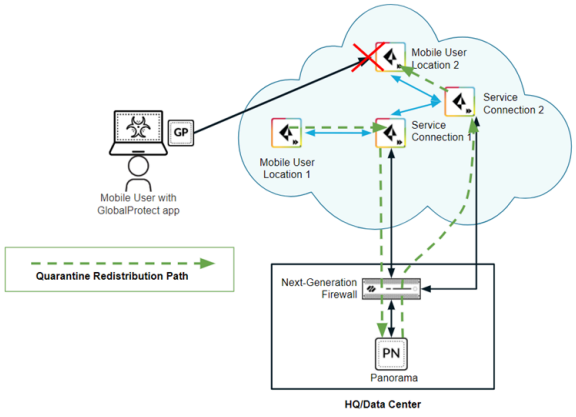


Para redistribuir la información de la lista de cuarentena de la Ubicación de usuario móvil 1 a la Ubicación de usuario móvil 2, realice las siguientes acciones:

- Redistribuir la información de la lista de cuarentena de la Conexión de servicio 1 a Panorama.
- Redistribuir la información de la lista de cuarentena de Panorama a Service Connection 2.

Con esta configuración, cuando el usuario de GlobalProtect se conecta a la Ubicación de usuario móvil 1 y se pone en cuarentena, la información de la lista de cuarentena se redistribuye desde la Ubicación de usuario móvil 1 a la Ubicación de usuario móvil 2 y se bloquea cualquier intento de conexión a la Ubicación de usuario móvil 2.

Esta configuración también es válida si el usuario de GlobalProtect se conecta a la Ubicación de usuario móvil 2 y está en cuarentena; la información de la lista de cuarentena se redistribuye de la Ubicación de usuario móvil 2 a la Ubicación de usuario móvil 1.



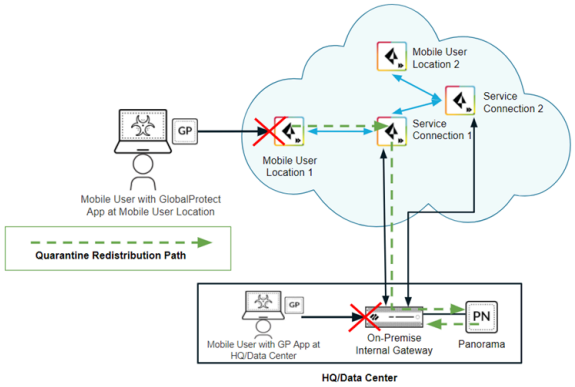
- **Redistribución de la lista de cuarentena entre Prisma Access y un cortafuegos o puerta de enlace de nueva generación**: en el siguiente ejemplo, un usuario de GlobalProtect intentó conectarse a la ubicación de usuario móvil 1. Ubicación de usuario móvil 1 detecta que el endpoint del usuario de GlobalProtect está comprometido y lo pone en cuarentena. A continuación, el usuario móvil se dirige a la sede de la empresa e intenta iniciar sesión

 ©2025 Palo Alto Networks, Inc.

nuevamente. La sede está protegida con un cortafuegos de nueva generación configurado como puerta de enlace GlobalProtect mediante detección de host interna.

La ubicación de usuario móvil 1 redistribuye la información de la lista de cuarentena a Panorama a través de la conexión de servicio 1, y Panorama redistribuye la información de la lista de cuarentena a la puerta de enlace interna local. Cuando el usuario intenta iniciar sesión desde la ubicación de la sede, GlobalProtect detecta que la puerta de enlace local está configurada como una puerta de enlace interna y se conecta a la puerta de enlace sin un túnel.

Dado que la información de la lista de cuarentena se ha redistribuido a la puerta de enlace local, el usuario queda bloqueado en la puerta de enlace según las políticas de usuario configuradas.



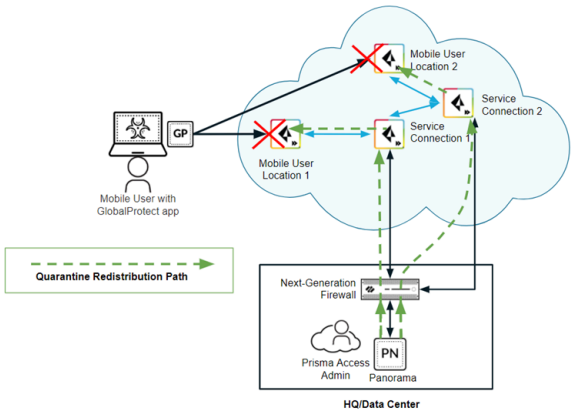
Si utiliza un cortafuegos o una puerta de enlace de última generación con Prisma Access, debe configurar Panorama para redistribuir la información de la lista de cuarentena al cortafuegos o puerta de enlace, a todas las conexiones de servicio y a Panorama.

- **El administrador pone en cuarentena manualmente al usuario móvil en Panorama**: en este ejemplo, el administrador de Prisma Access ha agregado manualmente un usuario móvil a la lista de cuarentena en el dispositivo Panorama que gestiona Prisma Access. El administrador ha configurado la redistribución entre Panorama, el cortafuegos de nueva generación y las conexiones de servicio. Panorama redistribuye la información de la lista de cuarentena actualizada al cortafuegos y a las conexiones de servicio. Luego, las conexiones de servicio redistribuyen la información de la lista de cuarentena a las ubicaciones de los usuarios móviles.

  El usuario móvil se conectó a la ubicación de usuario móvil 1. Una vez que la Ubicación del usuario móvil 1 recibe la información de la lista de cuarentena actualizada, el usuario se

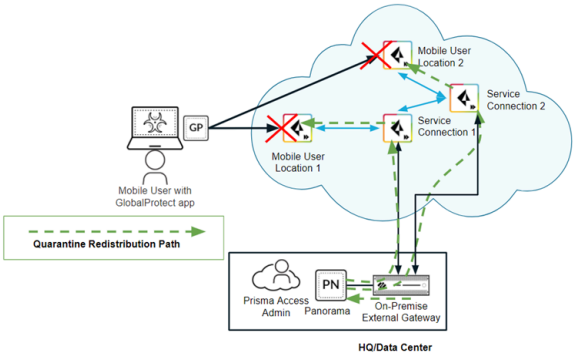
 ©2025 Palo Alto Networks, Inc.

desconecta. Si el usuario intenta conectarse a la Ubicación de usuario móvil 2, la conexión se bloquea y el usuario móvil recibe una notificación de cuarentena.



- **El usuario móvil se pone en cuarentena de forma automática o manual en la puerta de enlace local**: en este ejemplo, hay un cortafuegos de nueva generación que se ha configurado como puerta de enlace externa en la sede central o en la ubicación del centro de datos. El administrador ha puesto en cuarentena manualmente a un usuario móvil en la puerta de enlace externa. La puerta de enlace externa redistribuye la información de la lista de cuarentena desde la puerta de enlace externa a Panorama.

  Una vez que Panorama recibe la información de la lista de cuarentena actualizada de la puerta de enlace externa, redistribuye dicha información a las conexiones de servicio 1 y 2, que luego la redistribuyen a las ubicaciones de usuarios móviles 1 y 2. Si un usuario móvil intenta conectarse a la ubicación de usuario móvil 1 o 2, Prisma Access bloquea la conexión y el usuario recibe una notificación de cuarentena.



Configurar la redistribución de la lista de cuarentena en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Prisma Access

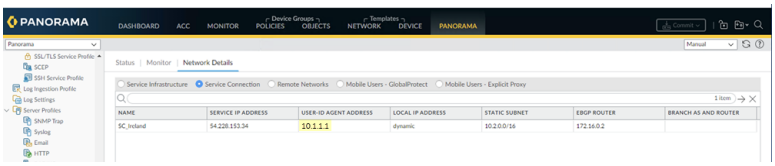
 ©2025 Palo Alto Networks, Inc.

Para redistribuir información de cuarentena hacia y desde conexiones de servicio, el Panorama que gestiona Prisma Access, y los cortafuegos de nueva generación, complete los siguientes pasos.

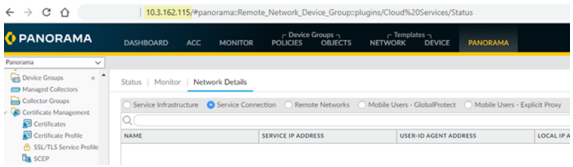
STEP 1 | Asegúrese de que la dirección IP de gestión de Panorama pueda comunicarse con la dirección del agente User-ID para todas las conexiones de servicio a las que desees redistribuir la información de la lista de cuarentena.

Se requiere comunicación entre la dirección del agente de User-ID de la conexión de servicio y la dirección IP de gestión de Panorama para que Prisma Access envíe y reciba información de la lista de cuarentena entre Panorama y las conexiones de servicio.

- Para encontrar la **User-ID Agent Address (Dirección de agente de User-ID)**, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **User-ID Agent Address (Dirección de agente de User-ID)**.



- Para encontrar la dirección IP de gestión del Panorama que gestiona Prisma Access, anote la dirección IP que se muestra en el navegador web cuando accede a Panorama.



STEP 2 | Permita a Prisma Access redistribuir información de la lista de cuarentena.

1. En Panorama, seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.
2. Para editar la configuración, haga clic en el engranaje.
3. En la pestaña **Advanced (Avanzado)**, seleccione **Enable Quarantine List Redistribution (Habilitar redistribución de la lista de cuarentena)**.

   Habilitar la redistribución de la lista de cuarentena permite a Prisma Access redistribuir la información de la lista de cuarentena recibida de una o más ubicaciones de usuarios móviles (puertas de enlace) a las conexiones de servicio.

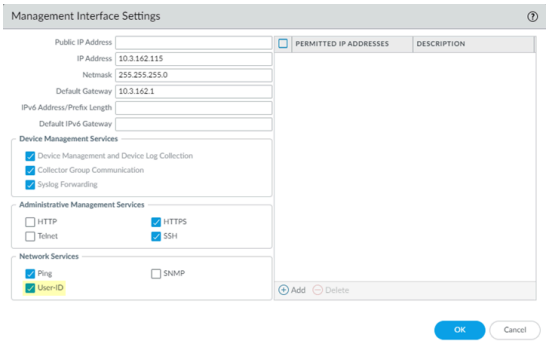


STEP 3 | Seleccione **Commit (Confirmar)** y **Push (Enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Configure Panorama para recibir información de la lista de cuarentena de Prisma Access configurando la configuración de la interfaz de gestión.

1. En el Panorama que gestiona Prisma Access, seleccione **Panorama** > **Setup (Configuración)** > **Interfaces**.
2. Seleccione la interfaz de **Management (Gestión)**
3. Seleccione **User-ID**.



STEP 5 | Configure un agente de redistribución de datos que redistribuya la información de la lista de cuarentena desde las conexiones de servicio a Panorama.

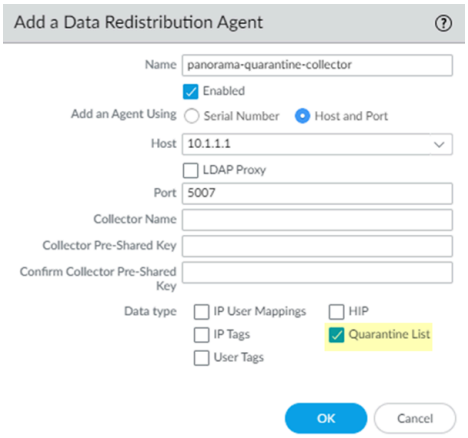
1. Desde el Panorama que gestiona Prisma Access, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles en la nube)** > **Service Connection (Conexión de servicio)**.
2. Toma nota de la **User-ID Agent Address (Dirección del agente de User-ID)** [**Panorama** > **Cloud Services (servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **User-ID Agent Address (Dirección de agente de User-ID)**] para cada conexión de servicio.
3. Seleccione **Panorama** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**.
4. Seleccione **Add (Añadir)** un agente de redistribución de datos, dale un **Name (Nombre)** y selecciona **Enabled (Habilitado)**.
5. Introduzca la **User-ID Agent Address (Dirección del agente de User-ID)** de la conexión del servicio como el **Host** y 5007 como el **Port (Puerto)**.

   Asegúrese de que su red no bloquee el acceso a este puerto entre Panorama y Prisma Access.
6. (Opcional) Si ha configurado esta conexión de servicio como un recopilador [**Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Collector Settings**

 ©2025 Palo Alto Networks, Inc.

(Configuración del recopilador)], introduzca el **Collector Name (Nombre del recopilador)** y la **Collector Pre-Shared Key (Clave precompartida de recopilador)**

7. Seleccione la **Quarantine List (Lista de cuarentena)**; luego, haga clic en **OK (Aceptar)**.



8. Repita el paso 5 para todas las conexiones de servicio en tu implementación de Prisma Access.

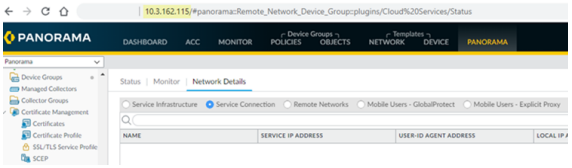
STEP 6 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** para guardar sus cambios localmente en el Panorama que gestiona Prisma Access.

 ©2025 Palo Alto Networks, Inc.

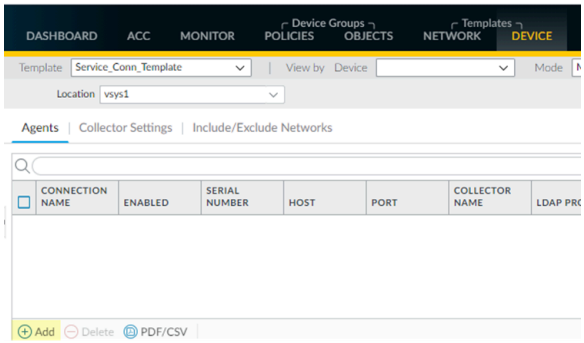
STEP 7 | Configure un agente de redistribución de datos que redistribuya la información de la lista de cuarentena desde Panorama a las conexiones de servicio.

1. Encuentra la dirección IP de gestión del Panorama que gestiona Prisma Access.

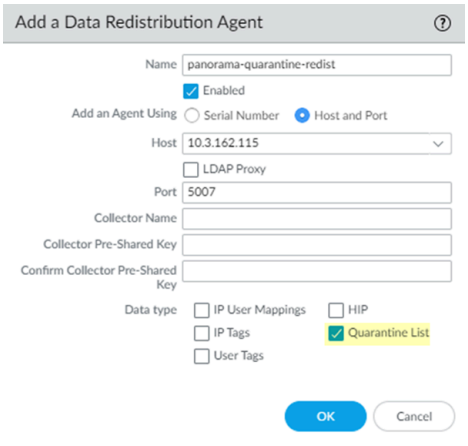
   Esta dirección se muestra en la barra de direcciones del navegador web cuando accede a Panorama.



2. Asegúrese de que está en la plantilla **Service_Conn_Template**, luego seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**.



3. Seleccione **Add (Añadir)** un agente de redistribución de datos, dale un **Name (Nombre)** y selecciona **Enabled (Habilitado)**.
4. Introduzca la dirección IP de gestión del dispositivo Panorama como el **Host** y 5007 como el **Port (Puerto)**.



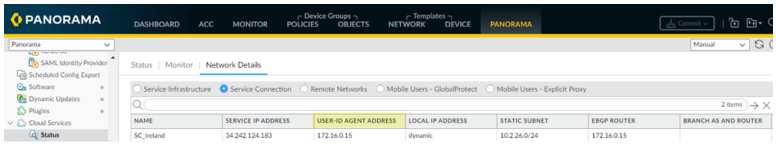
5. Seleccione la **Quarantine List (Lista de cuarentena)**; luego, haga clic en **OK (Aceptar)**.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Configura un agente de redistribución de datos que redistribuya la información de la lista de cuarentena desde las conexiones de servicio a las puertas de enlace de usuarios móviles.

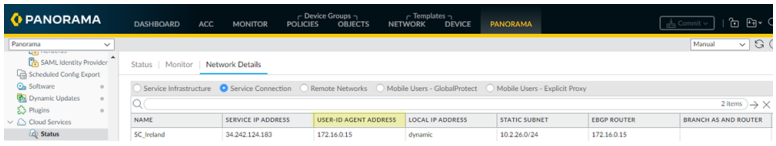
1. Desde el Panorama que gestiona Prisma Access, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles en la nube)** > **Service Connection (Conexión de servicio)**.
2. Tome nota de la **User-ID Agent Address (Dirección de agente de User-ID)** de la conexión del servicio desde la cual desea redistribuir la información de la lista de cuarentena.

   Dado que todas las conexiones de servicio tienen la misma información de lista de cuarentena redistribuida, seleccione cualquier conexión de servicio. También puede configurar más de una conexión de servicio.



3. Asegúrese de que está en **Mobile_User_Template**, luego seleccione**Device (dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**.
4. Seleccione **Add (Añadir)** un agente de redistribución de datos, dele un **Name (Nombre)** y seleccione **Enabled (Habilitado)**.
5. Introduzca la **User-ID Agent Address (Dirección del agente de User-ID)** de la conexión del servicio como el Host y **5007** como el Puerto.

   Asegúrese de que su red no bloquee el acceso a este puerto entre Panorama y Prisma Access.
6. (Opcional) Si ha configurado esta conexión de servicio como un recopilador [**Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Collector Settings (Configuración del recopilador)**], introduzca el **Collector Name (Nombre del recopilador)** y la **Collector Pre-Shared Key (Clave precompartida de recopilador)**.
7. Seleccione la **Quarantine List (Lista de cuarentena)**; luego, haga clic en **OK (Aceptar)**.



8. Seleccione **Commit and Push (Confirmar y enviar)** sus cambios.

STEP 9 | Vea la información de su lista de cuarentena seleccionando **Panorama** > **Device Quarantine (Cuarentena de dispositivos)**.

Consulte Ver la información del dispositivo en cuarentena en la Guía del Administrador de GlobalProtect para más detalles.

 ©2025 Palo Alto Networks, Inc.

Tráfico IPV6 de sinkhole en implementaciones de Usuarios móviles: GlobalProtect

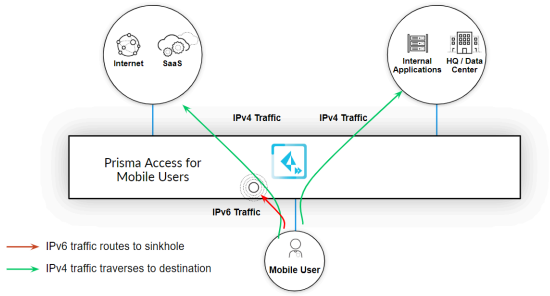
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

En un endpoint de pila dual que puede procesar tanto tráfico IPv4 como IPv6, la aplicación de GlobalProtect envía tráfico IPv4 de usuarios móviles para ser protegido a través del túnel VPN de GlobalProtect a Prisma Access. Sin embargo, el tráfico IPv6 de los usuarios móviles no se envía a Prisma Access de forma predeterminada y se envía al adaptador de red local en el endpoint en su lugar. Para reducir la superficie de ataque para amenazas basadas en IPv6, Palo Alto Networks recomienda que configure Prisma Access para desviar el tráfico IPv6. Debido a que los endpoints pueden volver automáticamente a una dirección IPv4, puede habilitar una experiencia de usuario segura y ininterrumpida para el tráfico de usuarios móviles a Internet.

La ruta IPv6 predeterminada tiene prioridad sobre otras rutas. Sin embargo, si existen rutas IPv6 más específicas a través de la interfaz de red física o si especifica la dirección de origen IPv6 de la interfaz física, dicho tráfico se enviará al adaptador de red local.

Además, Palo Alto Networks recomienda que configure GlobalProtect para deshabilitar completamente el tráfico de red en el adaptador de red local. Si tiene una implementación híbrida de Prisma Access con cortafuegos de nueva generación en las instalaciones configurados como puertas de enlace de GlobalProtect, puede configurar la funcionalidad de sinkhole IPv6 en la puerta de enlace de GlobalProtect en las instalaciones.

Puede configurar para que Prisma Access redirija todo el tráfico IPv6 de usuarios móviles. Cuando habilita esta funcionalidad, Prisma Access asigna una dirección IPv6 al endpoint de conexión además de una dirección IPv4; a continuación, enruta el tráfico IPv6 a Prisma Access y lo descarta mediante una política de seguridad integrada, como se muestra en la siguiente imagen.



Para configurar Prisma Access de manera que se desvíe todo el tráfico IPv6 de usuarios móviles, complete los siguientes pasos.

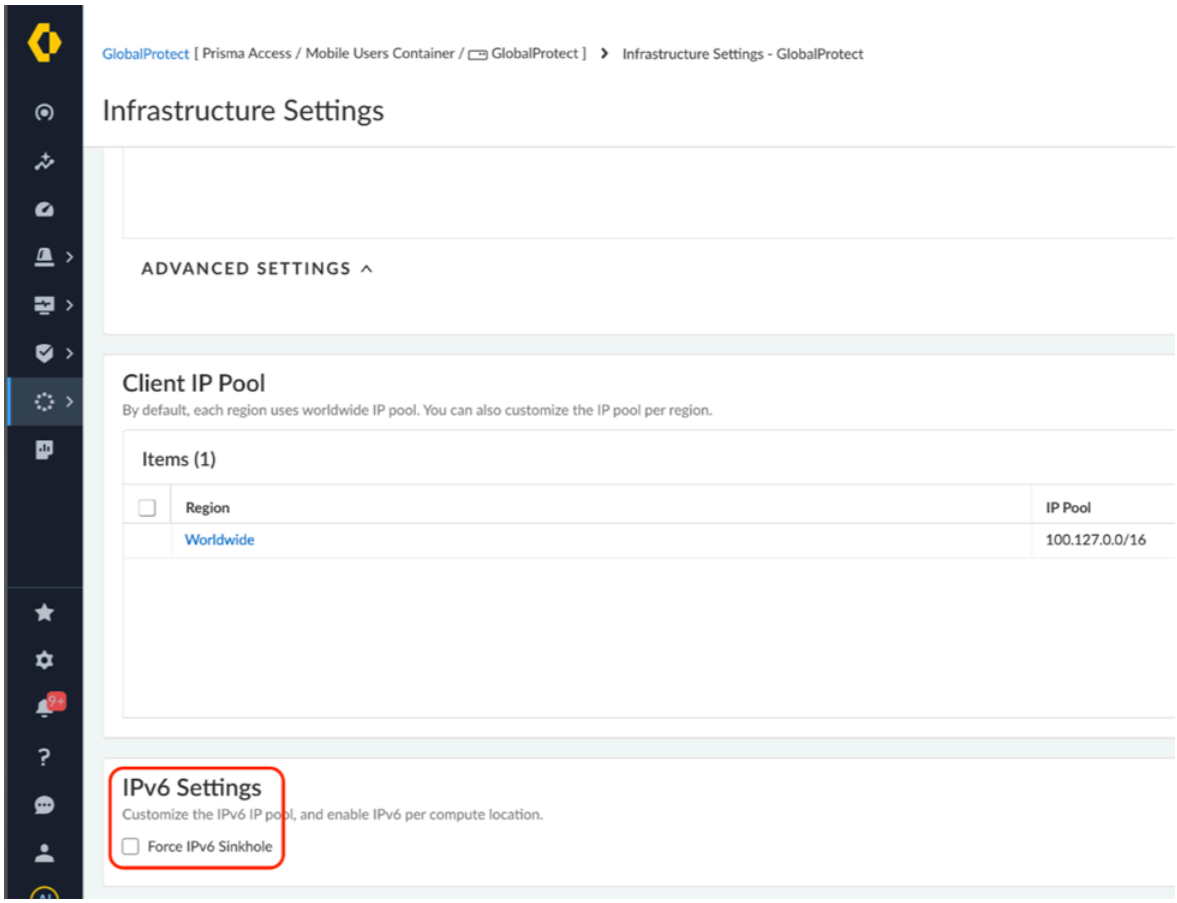
- Implementaciones de Prisma Access (Managed by Strata Cloud Manager):

  Vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)** > **GlobalProtect Setup (Configuración de GlobalProtect)** >

 ©2025 Palo Alto Networks, Inc.

Advanced Settings (Configuración avanzada) y seleccione **Force IPv6 Sinkhole (Forzar IPv6 Sinkhole)**.

Prisma Access utiliza fc00:0:0:0:0:0:0:0/64 como la dirección del sumidero.



- Implementaciones de Prisma Access (Managed by Panorama):

1. Abra una sesión de la CLI segura con privilegios de nivel de administrador mediante la misma dirección IP que utiliza para iniciar sesión en el Panorama que administra Prisma Access.
2. Introduzca `configurar` para introducir en modo de configuración.
3. Introduzca el comando **`set plugins cloud_services mobile-users ipv6 yes`**.

   Si necesita deshabilitar el comando en el futuro, introduzca **`set plugins cloud_services mobile-users ipv6 no`**.
4. Introduzca **`# commit`** para guardar los cambios localmente.
5. Escriba **`salir`** para salir del modo de configuración.
6. Introduzca **`commit-all shared-policy include-template yes device-group Mobile_User_Device_Group`** para confirmar y enviar sus cambios y hacerlos activos en Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Configurar GlobalProtect para desactivar el acceso directo a la red local

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Compatible con todos los endpoints de macOS y Windows GlobalProtect. Compatible con endpoints de Linux que comienzan con la versión 6.0.0 de la aplicación GlobalProtect.

Para asegurarse de que todo el tráfico de usuarios móviles se envía a Prisma Access, puede desactivar completamente las conexiones salientes, incluido el tráfico de subred local, para que no se envíen al adaptador local. Puede desactivar todas las conexiones salientes al adaptador local realizando cambios de configuración en la puerta de enlace de GlobalProtect.

Puede realizar estos pasos en Panorama o en un cortafuegos local que se haya configurado como una puerta de enlace GlobalProtect.

*Habilite la configuración **No direct access to local network (Sin acceso directo a la red local)** para reducir los riesgos en redes no fiables, como los puntos de acceso Wi-Fi fraudulentos.*

STEP 1 | Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**.

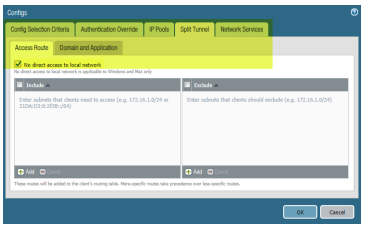
STEP 2 | Seleccione una puerta de enlace GlobalProtect existente o opte por **Add (Añadir)** una nueva.

STEP 3 | Seleccione **Agent (Agente)** > **Client Settings (Configuración de cliente)**.

STEP 4 | Seleccione la configuración **DEFAULT (PREDETERMINADA)** o **Add (Añadir)** para añadir una nueva.

STEP 5 | Seleccione **Split Tunnel (Túnel dividido)**; a continuación, seleccione **No direct access to local network (Sin acceso directo a la red local)**.

Deshabilitar el acceso a la red local hace que todo el tráfico, incluido el tráfico IPv4 e IPv6, se envíe al adaptador local. Además, no podrá acceder a los recursos de su subred local, como las impresoras. El tráfico de túnel dividido basado en la ruta de acceso, el dominio de destino y la aplicación aún funciona como se esperaba.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Solo implementaciones de Panorama y Prisma Access) Envíe sus cambios localmente para que estén activos en Panorama.

1. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)**.
2. Asegúrese de que su cambio sea parte del **Commit Scope (Ámbito de confirmación)**.
3. Haga clic en **OK (Aceptar)** para guardar los cambios en el ámbito de envío.
4. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 7 | Deberá **Commit (Confirmar)** y **Push (Enviar)** sus cambios para hacerlos activos en Prisma Access.

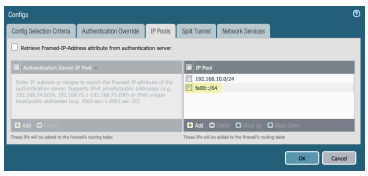
Configurar un sumidero IPv6 en la puerta de enlace local

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si tiene una implementación híbrida que utiliza cortafuegos de última generación configurados como puertas de enlace con Prisma Access, realice la siguiente tarea en la puerta de enlace local para eliminar el tráfico IPv6.

STEP 1 | Añada grupos de direcciones IP IPv6 a la configuración de su agente GlobalProtect.

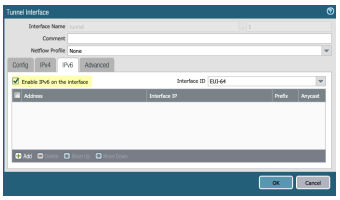
1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)**.
2. Seleccione una puerta de enlace GlobalProtect existente o opte por **Add (Añadir)** una nueva.
3. Seleccione **Agent (Agente)** > **Client Settings (Configuración del cliente)**.
4. Seleccione la configuración del agente para modificar o **Add (Añadir)** una nueva.
5. Seleccione **IP Pools (Grupos de IP)**; a continuación, seleccione **Add (Añadir)** para añadir un grupo de direcciones IPv6 para asignar al adaptador de red virtual en los endpoints que se conectan a los usos de la puerta de enlace de GlobalProtect para el tráfico de red móvil y haga clic en **OK (Aceptar)**.



 ©2025 Palo Alto Networks, Inc.

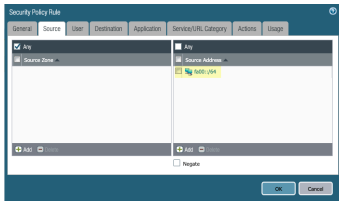
STEP 2 | Habilite IPv6 en la interfaz.

1. Seleccione **Device (Dispositivo)** > **Interface (Interfaz)** > **Tunnel (Túnel)** y seleccione la **Interface (Interfaz)** de túnel que utiliza para el tráfico del usuario móvil.
2. Seleccione **IPv6**, luego seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.

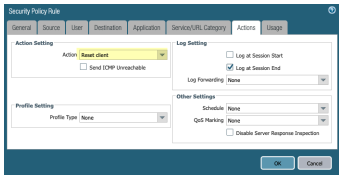


STEP 3 | Añada una política de seguridad para establecer una acción de restablecimiento TCP que terminará las sesiones con tráfico de origen IPv6 que coincida con los grupos de IP que configuró en el Paso 1.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)** para añadir una nueva política de seguridad.
2. Establezca la **Source Address (Dirección de origen)** en la regla para que coincida con los grupos de IP que configuró en el Paso 1.



3. Seleccione **Actions (Acciones)**; a continuación, seleccione una **Action Setting (Configuración de acción)** de **Reset Client (Restablecer cliente)** y haga clic en **OK (Aceptar)**.



STEP 4 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 5 | (Opcional) Realice esta tarea en todos los cortafuegos de puerta de enlace en su implementación.

Redistribuir la información de HIP con Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

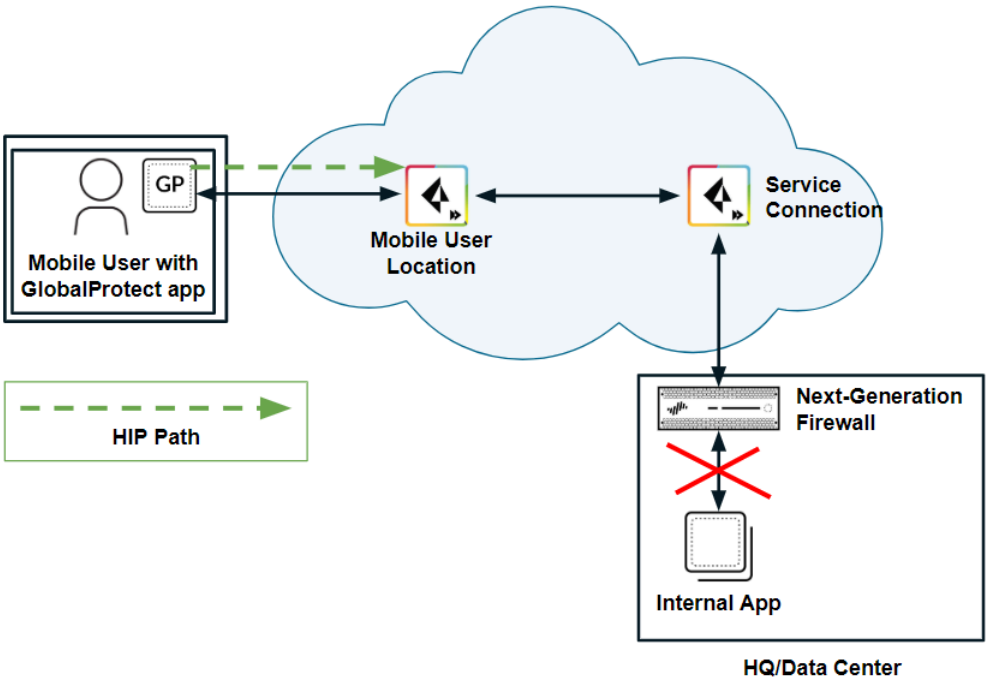
 ©2025 Palo Alto Networks, Inc.

Para garantizar la aplicación de forma coherente de las políticas de perfil de información de host (HIP) y simplificar la gestión de políticas, puede redistribuir la información de HIP recibida de usuarios móviles y usuarios de redes remotas que utilizan la aplicación GlobalProtect desde Prisma Access a otras puertas de enlace, cortafuegos y dispositivos Panorama de su empresa, incluido el Panorama que gestiona Prisma Access.

En la siguiente sección se describen algunas implementaciones comunes de Prisma Access en las que la redistribución de los HIP es útil para la aplicación coherente de políticas y la visualización de informes de HIP:

- **Redistribución HIP de Prisma Access a un cortafuegos de nueva generación**: si tiene un cortafuegos de nueva generación en el centro de datos o la ubicación de la sede de su organización y ha configurado ese cortafuegos con políticas de seguridad basadas en HIP, no puede aplicar esas políticas a los usuarios móviles de Prisma Access hasta que redistribuya la redistribución HIP de Prisma Access al cortafuegos.

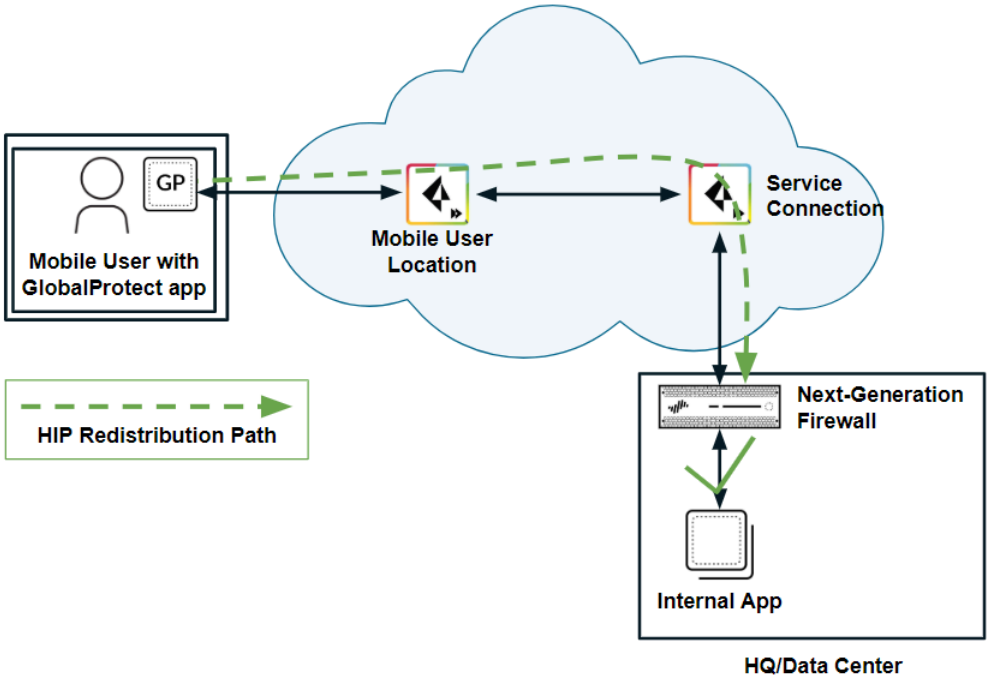
  La siguiente imagen muestra un usuario móvil cuyo endpoint está protegido con la aplicación GlobalProtect. El usuario intenta acceder a una aplicación interna en un centro de datos/sede cuyo acceso está controlado por un cortafuegos de nueva generación con políticas de seguridad basadas en HIP. Cuando el usuario inicia sesión en la aplicación GlobalProtect, la aplicación recopila información de HIP y la envía a Prisma Access; sin embargo, Prisma Access no redistribuye esta información al cortafuegos local. Dado que el cortafuegos no tiene la información HIP del usuario, bloquea el acceso del usuario a la aplicación.



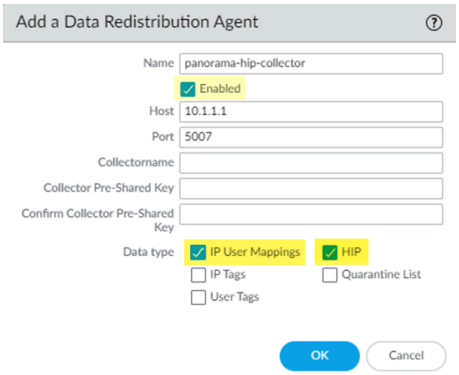
  La redistribución HIP le permite distribuir la información HIP de los usuarios móviles al cortafuegos local. A continuación, el cortafuegos puede comprobar la información de la CAD

 ©2025 Palo Alto Networks, Inc.

del usuario, comparándola con sus políticas de seguridad configuradas, y concederle acceso a la aplicación.



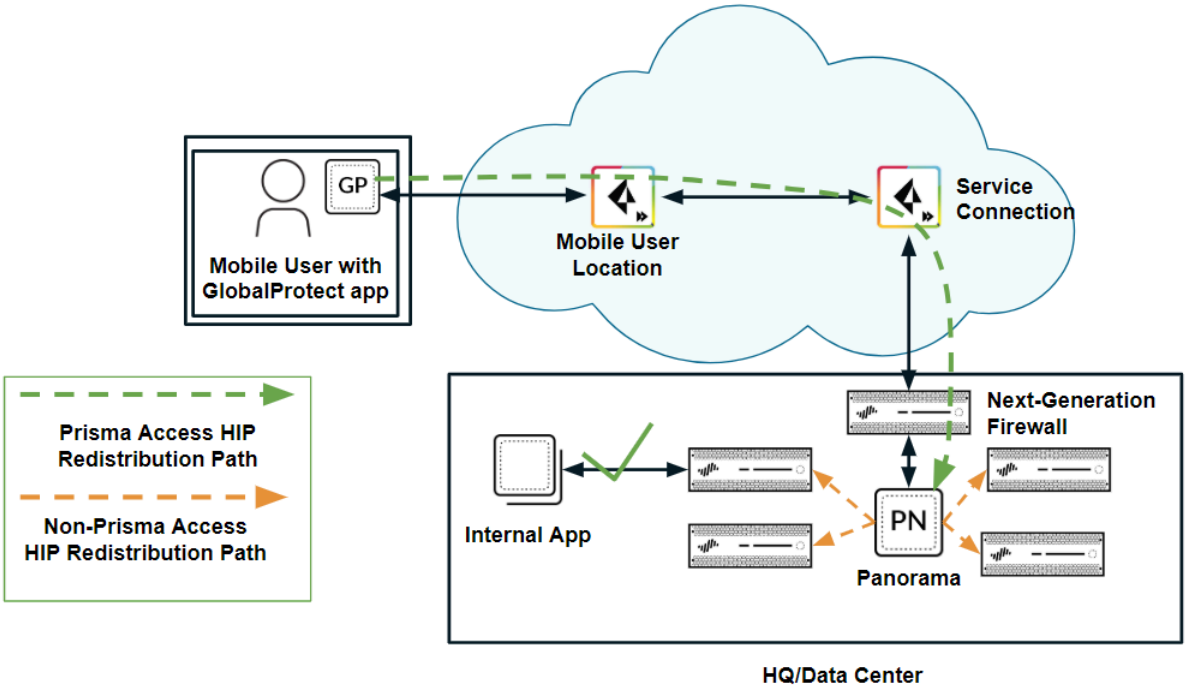
Para redistribuir la información HIP de Prisma Access al cortafuegos, permite que Prisma Access redistribuya la información HIP, luego **Add (Añadir)** un **User-ID Agent (Agente de User-ID)** (**Panorama** > **User Identification (Identificación de usuario)** > **User-ID Agents (Agentes de User-ID)** para dispositivos Panorama 9.1.*x* o **Panorama** > **Data Redistribution (Redistribución de datos)** para dispositivos Panorama 10.*x*) en el cortafuegos y especifique la **User-ID Agent Address (Dirección del agente de User-ID)** de Prisma Access [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **User-ID Address Agent (Agente de dirección de User-ID)**] como el **Host** (10.1.1.1 en el siguiente ejemplo) y **5007** como el **puerto**.



- **Redistribución HIP de Prisma Access a Panorama**: si tiene varios cortafuegos o puertas de enlace en su organización con políticas de seguridad basadas en HIP, puede redistribuir la información HIP de Prisma Access al Panorama que gestiona Prisma Access mediante la creación de un agente de User-ID en Panorama y especificando la **User-ID Agent Address (Dirección del agente de User-ID)** de Prisma Access como el **Host** del User-ID. A continuación,

 ©2025 Palo Alto Networks, Inc.

puede redistribuir los informes HIP de ese dispositivo Panorama a los demás dispositivos Panorama gestionados, puertas de enlace, cortafuegos y sistemas virtuales de su empresa, utilizando el mismo flujo de trabajo que utiliza para redistribuir la información de User-ID a los cortafuegos gestionados y hacer cumplir la política coherente para las aplicaciones y recursos internos, como se muestra en la siguiente imagen.



Alternativamente, puede configurar cada cortafuegos interno o puerta de enlace de su empresa para recopilar directamente la información HIP de Prisma Access, sin usar Panorama como ubicación central, creando un agente de User-ID en cada dispositivo. Tenga en cuenta, sin embargo, que Prisma Access utiliza conexiones de servicio para enviar información HIP, y el consumo de ancho de banda de la conexión de servicio podría aumentar si Prisma Access envía un gran número de informes HIP.

- **Redistribución HIP de un usuario en una red remota a Prisma Access**: los casos de uso anteriores mostraban a Prisma Access recopilando información HIP de usuarios móviles. Si desea aplicar políticas basadas en HIP en Prisma Access para un usuario en una ubicación de red remota, necesita una forma de distribuir la información HIP desde la aplicación GlobalProtect del usuario de red remota a Prisma Access.

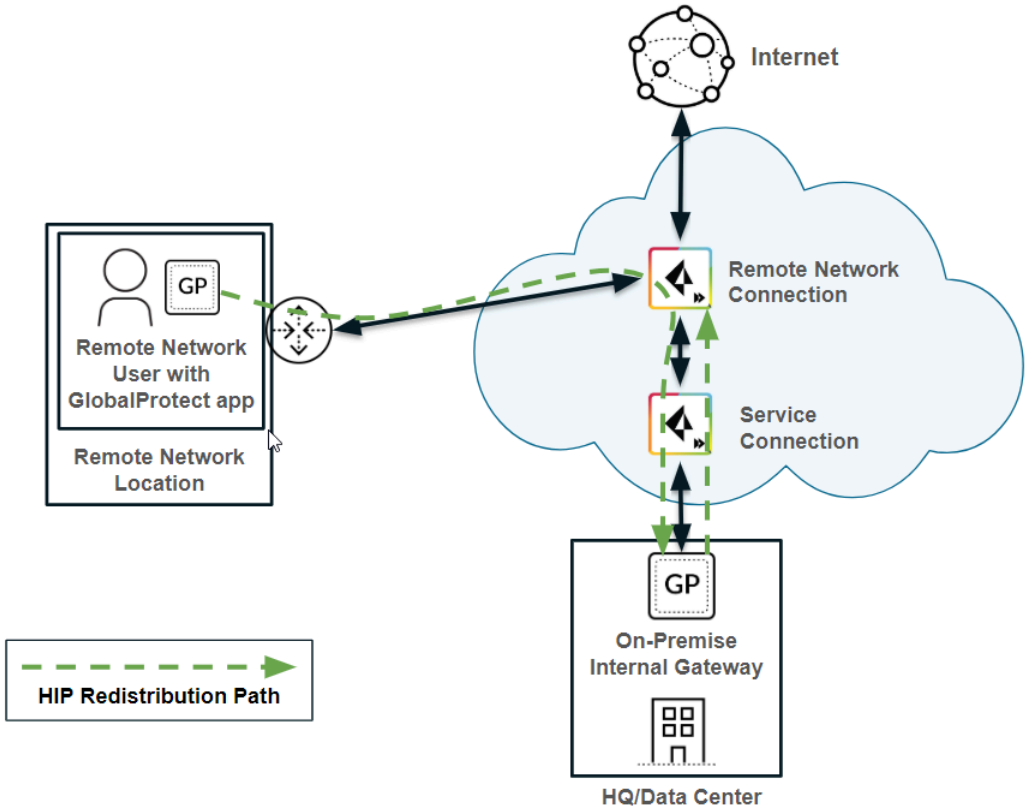
  El siguiente ejemplo muestra un usuario en una ubicación de red remota cuyo acceso a Internet se encuentra en la conexión de red remota. En Prisma Access, controle el acceso a Internet del usuario en la ubicación de red remota con políticas de seguridad creadas en el **Remote_Network_Device_Group** o en un grupo de dispositivos compartidos. Para hacer cumplir correctamente las políticas en la ubicación de red remota para el usuario, debe configurar Prisma Access para recuperar la información HIP del usuario desde la puerta de enlace interna.

  En este ejemplo, la puerta de enlace de GlobalProtect en el centro de datos/sede que está configurada como puerta de enlace interna mediante la detección interna comprueba la información HIP del usuario desde la aplicación GlobalProtect del usuario. La puerta de enlace

 ©2025 Palo Alto Networks, Inc.

interna detecta que el usuario se encuentra dentro de la ubicación remota de la red y recopila información de User-ID e HIP del usuario.

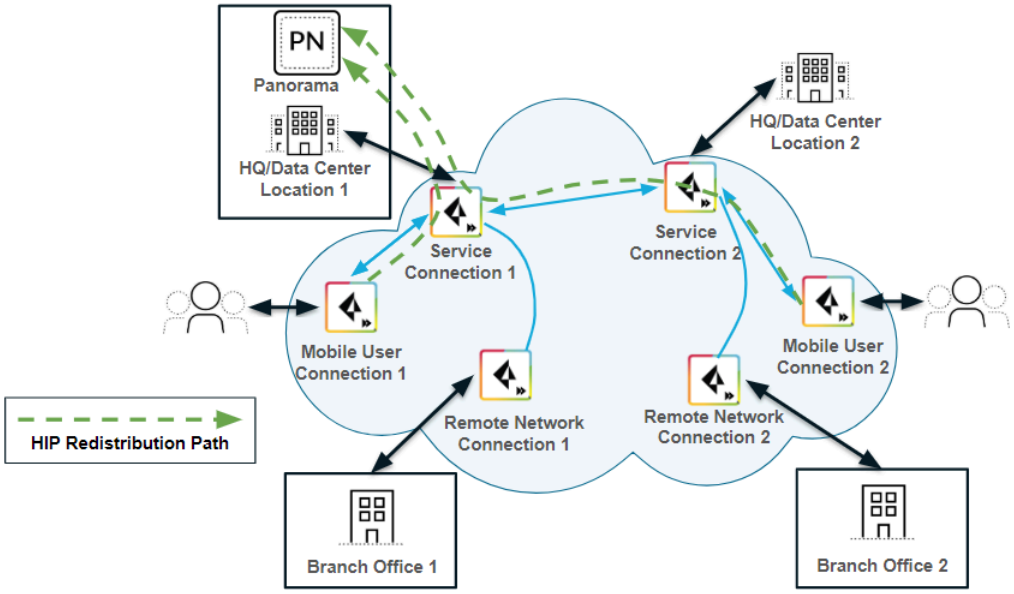
Para distribuir esta información HIP desde la puerta de enlace interna a Prisma Access, cree un agente de User-ID en Panorama y especifique la dirección IP de la puerta de enlace interna como host.



- Ver logs detallados de HIP **desde Panorama**: cuando los usuarios móviles inician sesión con la aplicación GlobalProtect, la aplicación envía la información de HIP a Prisma Access. Panorama recupera los resultados del log de Strata Logging Service para ver los resultados de los logs de coincidencias de HIP [**Monitor (Supervisar)** > **Logs** > **HIP Match (Coincidencia HIP)**];

 ©2025 Palo Alto Networks, Inc.

sin embargo, no puede ver informes detallados de HIP hasta que configure Panorama para redistribuir los detalles de los informes de HIP de Prisma Access a Panorama.

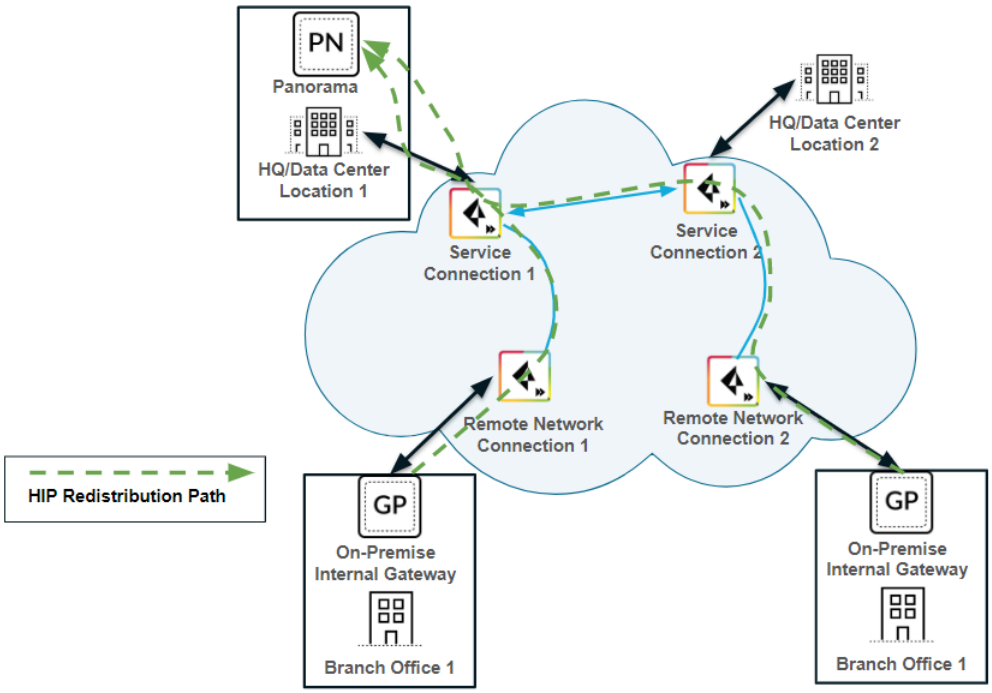


Para redistribuir información detallada de HIP de los usuarios móviles a Panorama, cree un agente de User-ID en Panorama y especifique la **User-ID Agent Address (Dirección del agente de User-ID)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service Connection (Conexión de servicio)** > **User-ID Agent Address (Dirección del agente de User-ID)**] como el host de User-ID.

Si ha configurado una puerta de enlace local como puerta de enlace interna en una ubicación de usuario remota, también puede enviar la información HIP para usuarios en redes remotas a Panorama creando un agente de ID de usuario en Panorama y especificando la dirección del **EBGP Router (Enrutador EBGP)** de red remota [**Panorama** > **Cloud Services (Servicios en la**

 ©2025 Palo Alto Networks, Inc.

nube) > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** > **EBGP Router (Enrutador EBGP)**] como host de User-ID.



Habilitar y configurar la redistribución HIP en Prisma Access:

- Configure la redistribución HIP en Prisma Access

Configure la redistribución HIP en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Cuando un usuario móvil cuyo endpoint tiene instalada la aplicación GlobalProtect se conecta a Prisma Access, Prisma Access recopila la información HIP del usuario de la aplicación GlobalProtect del endpoint, lo que hace que el informe HIP esté disponible en Prisma Access.

Para utilizar la redistribución de HIP, los usuarios deben tener la aplicación GlobalProtect instalada en su endpoint. Mientras que Prisma Access es compatible con VPN sin cliente, no puede redistribuir información HIP para usuarios de VPN sin cliente.

La redistribución de HIP es aplicable tanto a usuarios móviles como a usuarios en redes remotas. Sin embargo, para los usuarios en redes remotas, una puerta de enlace local debe detectar que el usuario es interno a la red de la organización utilizando la detección de hosts internos antes de que la puerta de enlace local pueda enviar información HIP a Prisma Access.

 ©2025 Palo Alto Networks, Inc.

En Prisma Access, configure la detección de hosts internos cuando configure la implementación de usuarios móviles.

Para garantizar la aplicación coherente de políticas, puede utilizar la redistribución de HIP para permitir que Prisma Access distribuya la información de HIP de los usuarios a otros dispositivos Panorama, puertas de enlace, cortafuegos y sistemas virtuales en su implementación, así como distribuir la información de HIP de esos dispositivos a Prisma Access en algunos casos. Esta capacidad le permite aplicar de manera coherente la aplicación de políticas basadas en HIP para el tráfico de los usuarios, incluidas las políticas para el tráfico destinado a Internet o para el tráfico que accede a una aplicación o recurso interno en la sede o centro de datos de su organización. La redistribución de la información HIP al dispositivo Panorama también te permite ver información HIP detallada de los usuarios de Prisma Access desde ese dispositivo.

Tenga en cuenta que las puertas de enlace internas y externas de GlobalProtect no admiten la redistribución HIP bidireccional. Por lo tanto, la práctica recomendada es utilizar su dispositivo Panorama como su punto de redistribución. En esta implementación, configuraría sus puertas de enlace internas y externas para enviar los informes HIP a Panorama y hacer que Panorama los reenvíe a sus cortafuegos para una aplicación coherente de políticas en su entorno.

- Strata Cloud Manager
- Panorama

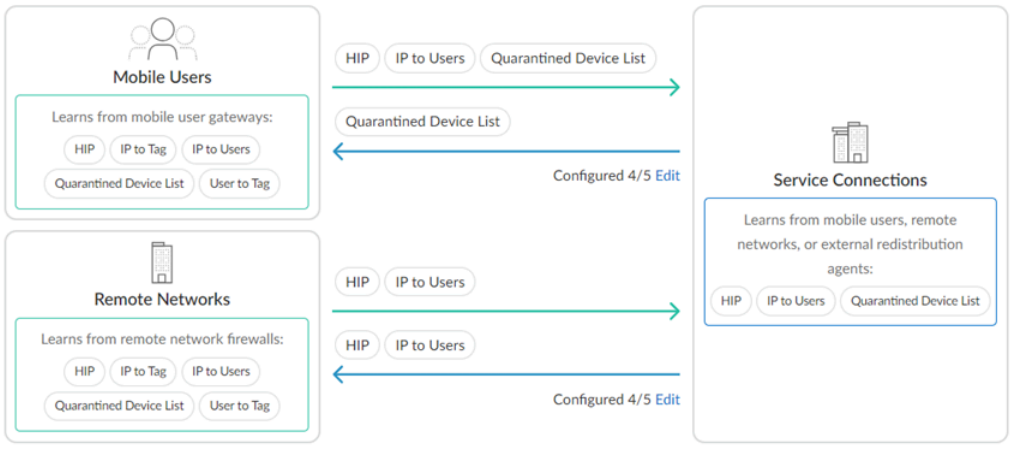
Configurar la redistribución HIP en Prisma Access (Strata Cloud Manager).

La redistribución de informes HIP está habilitada de forma predeterminada en **Strata Cloud Manager**. Para ver los detalles de la redistribución o para deshabilitarla, siga los pasos a continuación.

STEP 1 | En **Strata Cloud Manager**, seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Identify Services (Identificar Servicios)** > **Identify Redistribution (Identificar redistribución)**.

El diagrama de redistribución de identidad de Prisma Access muestra la configuración de redistribución de informes HIP predeterminada entre usuarios móviles y conexiones de servicio, así como entre redes remotas y conexiones de servicio.

Prisma Access Identity Redistribution Diagram



STEP 2 | Para deshabilitar la redistribución entre un segmento, haga clic en **Edit (Editar)** y luego haga clic en **Edit (Editar)** junto a la red remota de origen correspondiente.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Deshabilitar **HIP**.

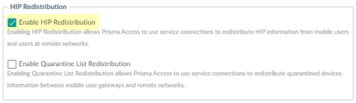
Configurar la redistribución HIP en Prisma Access (Panorama).

Para permitir que Prisma Access recopile y redistribuya información de HIP, complete la siguiente tarea.

STEP 1 | Permita a Prisma Access redistribuir la información de HIP.

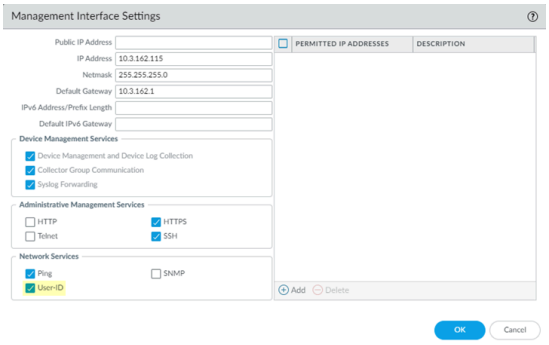
1. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.
2. Para editar la configuración, haga clic en el engranaje.
3. En **Advanced (Avanzado)** , seleccione **Enable HIP Redistribution (Habilitar la redistribución de HIP)**.

   La habilitación de la redistribución de HIP permite a Prisma Access redistribuir los informes de HIP recibidos de la aplicación GlobalProtect a los cortafuegos internos y a Panorama.



STEP 2 | Configurar Panorama para recibir informes de HIP de Prisma Access.

1. Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces**.
2. Seleccione la interfaz de **Management (Gestión)**
3. Seleccione **User-ID**.



STEP 3 | Configure Panorama para recopilar la asignación de User-ID de Prisma Access.

1. Desde el Panorama que gestiona Prisma Access, seleccione **Panorama** > **Data Redistribution (Redistribución de datos)** > **Agentes (Agentes)** (para dispositivos Panorama 10.*x*) o **Panorama** > **User Identification (Identificación de usuario)** > **User-ID Agents (Agentes de User-ID)** (para Dispositivos Panorama 9.1.*x*).
2. **Add (Añadir)** un agente de User-ID y asígnele un **Name (Nombre)**.
3. Introduzca uno de los siguientes valores en el campo **Host**, en función de los tipos de información de HIP que desee recopilar.
   - Para recopilar información de HIP para usuarios móviles, introduzca la **User-ID Agent Address (Dirección del agente de User-ID)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Service**

 ©2025 Palo Alto Networks, Inc.

Connection (Conexión de servicio) > **User-ID Agent Address (Dirección del agente de User-ID)**].

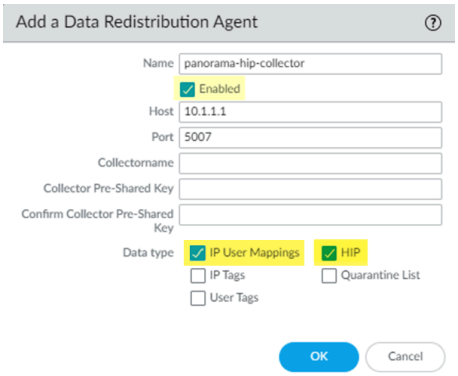
- Para recopilar información de HIP de los usuarios en ubicaciones de red remotas con una puerta de enlace interna, introduzca la dirección IP de la puerta de enlace interna.
- Para recopilar información de HIP de los usuarios que se encuentran en una conexión de red remota, introduzca la dirección del **EBGP Router (Enrutador EBGP)** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** > **EBGP Router (Enrutador EBGP)** como host de User-ID.

4. Introduzca **5007** en el campo del puerto.

   De forma predeterminada, el agente de User-ID utiliza el puerto 5007 para escuchar las solicitudes de información de HIP.

   Asegúrese de que su red no bloquee el acceso a este puerto entre Prisma Access y el servidor de Active Directory o el agente de User-ID.

5. Seleccione **Enabled (Habilitado)** para permitir que Panorama se comunique con el agente de User-ID.
6. Seleccione **IP User Mappings (Asignaciones de usuarios IP)** y **HIP** para permitir que Panorama reciba asignaciones de dirección IP a nombre de usuario y datos de GlobalProtect HIP de todas las ubicaciones de usuarios móviles.
7. Haga clic en **OK (Aceptar)**.



STEP 4 | Repita el paso 3 para cada conexión de servicio en la que desee configurar la recopilación de informes de HIP.

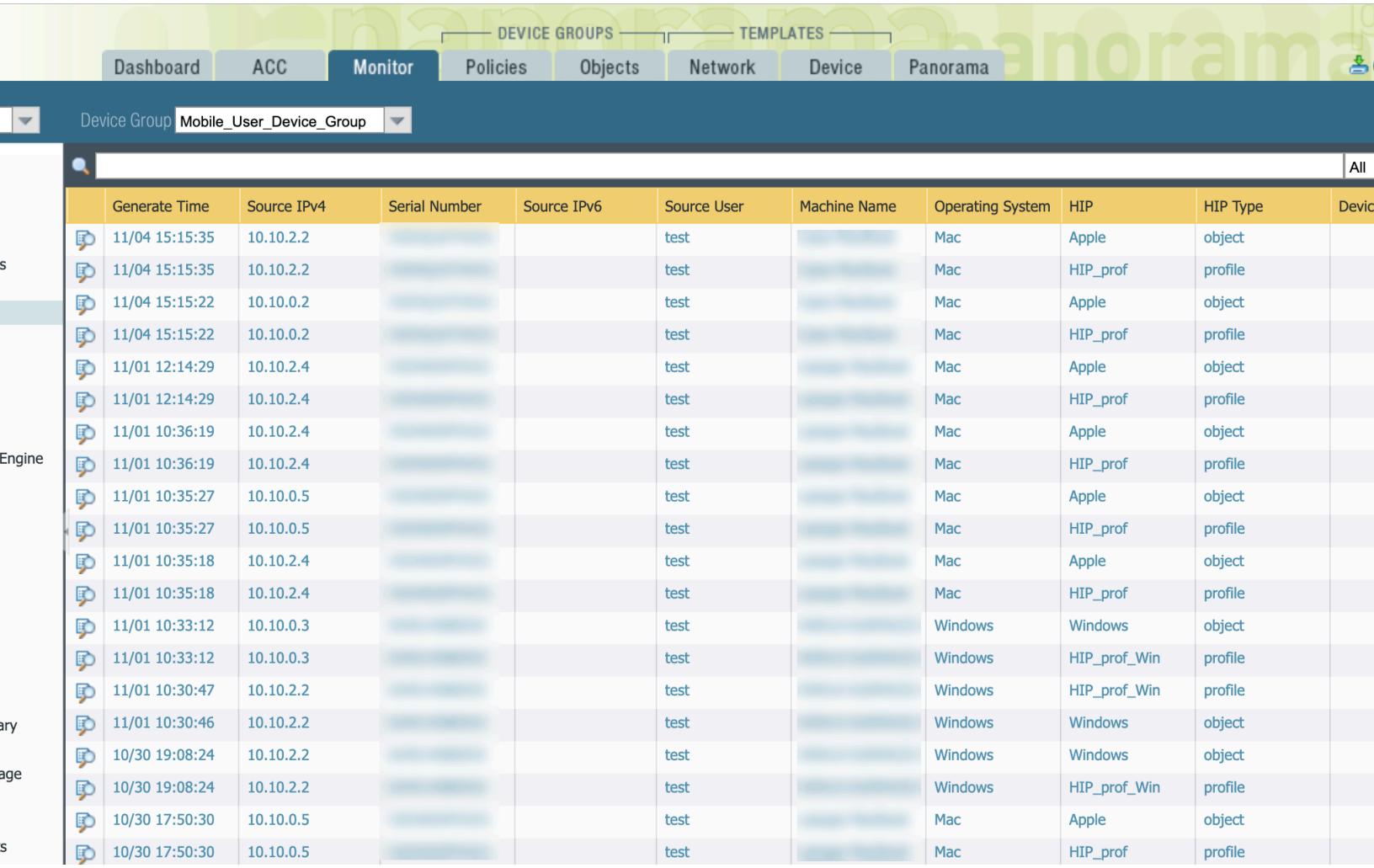
Ver informes de HIP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Después de configurar Prisma Access para recopilar y redistribuir información de HIP a Panorama, utilice el siguiente flujo de trabajo para ver la información de HIP en Panorama.

 ©2025 Palo Alto Networks, Inc.

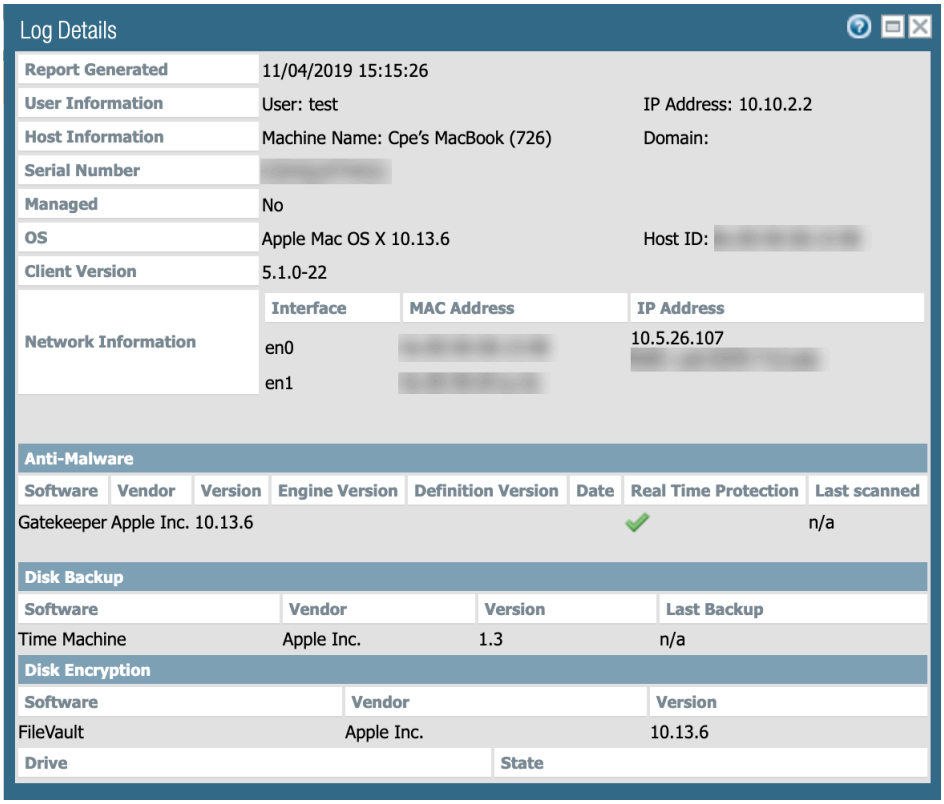
STEP 1 | Seleccione **Monitor (Supervisar)** > **Logs** > **HIP Match (Coincidencias HIP)** para ver la información de HIP.



Generate Time	Source IPv4	Serial Number	Source IPv6	Source User	Machine Name	Operating System	HIP	HIP Type	Devic
11/04 15:15:35	10.10.2.2			test		Mac	Apple	object	
11/04 15:15:35	10.10.2.2			test		Mac	HIP_prof	profile	
11/04 15:15:22	10.10.0.2			test		Mac	Apple	object	
11/04 15:15:22	10.10.0.2			test		Mac	HIP_prof	profile	
11/01 12:14:29	10.10.2.4			test		Mac	Apple	object	
11/01 12:14:29	10.10.2.4			test		Mac	HIP_prof	profile	
11/01 10:36:19	10.10.2.4			test		Mac	Apple	object	
11/01 10:36:19	10.10.2.4			test		Mac	HIP_prof	profile	
11/01 10:35:27	10.10.0.5			test		Mac	Apple	object	
11/01 10:35:27	10.10.0.5			test		Mac	HIP_prof	profile	
11/01 10:35:18	10.10.2.4			test		Mac	Apple	object	
11/01 10:35:18	10.10.2.4			test		Mac	HIP_prof	profile	
11/01 10:33:12	10.10.0.3			test		Windows	Windows	object	
11/01 10:33:12	10.10.0.3			test		Windows	HIP_prof_Win	profile	
11/01 10:30:47	10.10.2.2			test		Windows	HIP_prof_Win	profile	
11/01 10:30:46	10.10.2.2			test		Windows	Windows	object	
10/30 19:08:24	10.10.2.2			test		Windows	Windows	object	
10/30 19:08:24	10.10.2.2			test		Windows	HIP_prof_Win	profile	
10/30 17:50:30	10.10.0.5			test		Mac	Apple	object	
10/30 17:50:30	10.10.0.5			test		Mac	HIP_prof	profile	

©2025 Palo Alto Networks, Inc.

STEP 2 | Haga clic en el icono a la izquierda de un registro para ver información detallada de HIP.



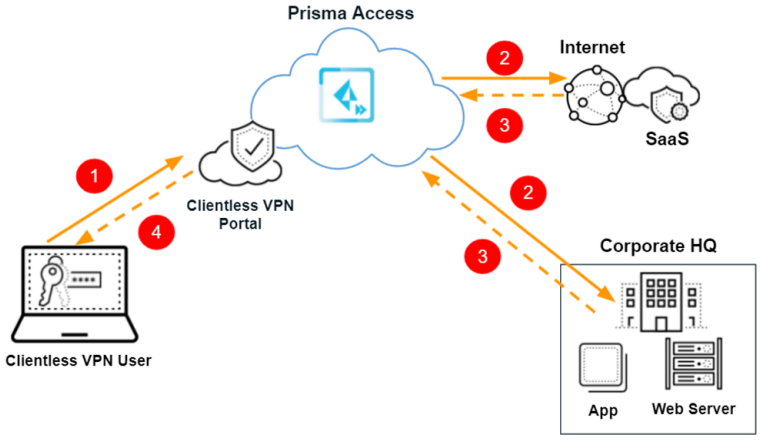
Soporte para codificación Gzip en VPN sin cliente

¿Dónde puedo usar esto?	¿Qué necesito?
• Panorama	• Licencia de Prisma Access

La VPN sin cliente de GlobalProtect proporciona acceso remoto seguro a aplicaciones web empresariales comunes. La VPN sin clinte de Prisma Access permite a los usuarios móviles acceder a sitios web comprimidos con Gzip para usar aplicaciones internas y SaaS. La compatibilidad con la codificación Gzip garantiza que la solicitud de codificación Gzip dentro del encabezado HTTP sea aceptada por el portal VPN sin cliente. Esto garantiza que el contenido de las páginas web comprimidas con Gzip se represente correctamente cuando se accede a través del portal VPN sin cliente.

El siguiente diagrama ilustra el soporte extendido para permitir a los usuarios acceder a aplicaciones internas y SaaS a través de VPN sin cliente en Prisma Access.

 ©2025 Palo Alto Networks, Inc.



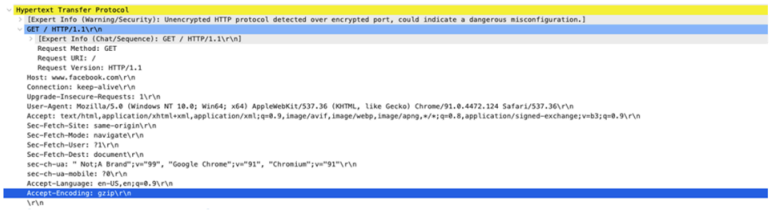
La VPN sin cliente puede determinar si usar codificación Gzip en función de la solicitud HTTP del cliente y la respuesta correspondiente de la aplicación. El valor **gzip** debe incluirse como uno de los valores de encabezado Accept-Encoding para que sea aceptado por la VPN sin cliente.

Por ejemplo, considere los siguientes escenarios cuando la VPN sin cliente usa codificación Gzip:

1. El navegador envía una solicitud HTTP al sitio web con los valores de encabezado Accept-Encoding establecidos en **gzip**, **deflate (desinflar)** y **br**, como se muestra en el siguiente ejemplo.



2. El portal VPN sin cliente en Prisma Access analiza la solicitud HTTP entrante del navegador y establece el valor de encabezado Aceptar codificación en **gzip** que indica compatibilidad con la codificación Gzip, como se muestra en el siguiente ejemplo.

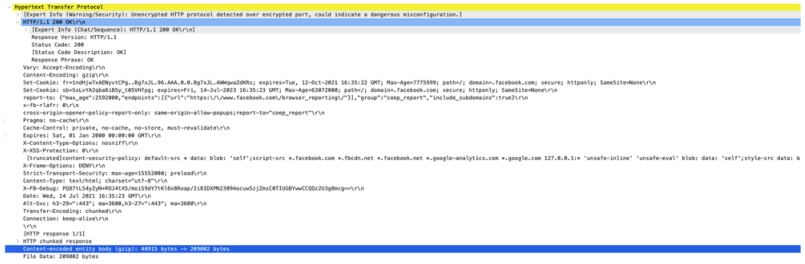


 ©2025 Palo Alto Networks, Inc.

3. Si el sitio web admite codificación Gzip en la respuesta HTTP, el sitio web envía el encabezado Content-Encoding como **gzip** que indica que el contenido está en formato Gzip, como se muestra en el siguiente ejemplo.



4. La VPN sin cliente reenvía la respuesta recibida del sitio web al navegador web en el mismo formato, como se muestra en el siguiente ejemplo.



Si la solicitud HTTP recibida por la VPN sin cliente no incluye **gzip** como uno de los métodos de codificación, la VPN sin cliente tampoco acepta la codificación Gzip.

Replicación de tráfico en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access ❑ Licencia de complemento de replicación de tráfico ❑ La replicación de tráfico requiere una versión mínima de 4.1 de Prisma Access para el tráfico de Usuarios móviles. ❑ La replicación de tráfico requiere una versión mínima de 5.0 de Prisma Access tanto para usuarios móviles como para tráfico de red remota. ❑ La compatibilidad con TLS 1.3 para redes remotas requiere una versión mínima de Prisma Access 5.2. ❑ PubSub requiere una versión de Prisma Access 5.2.1. como mínimo.

 ©2025 Palo Alto Networks, Inc.

Los registradores de red locales han sido una herramienta potente para que las organizaciones realicen análisis forenses y de filtraciones. Es común en topologías locales implementar una infraestructura paralela de puertos tap, puertos span o brokers de paquetes que entregarían una copia del tráfico que se utilizará para dicho análisis fuera de banda.

Sin embargo, junto con la adopción acelerada del trabajo híbrido y la nube, las organizaciones están migrando a las arquitecturas de SASE para abordar estos desafíos. La adhesión a las soluciones de seguridad en la nube de SASE creó puntos ciegos para estas herramientas de análisis forense, donde una copia del tráfico de un usuario remoto a una aplicación SaaS ya no está disponible.

La replicación de tráfico de Prisma Access añade visibilidad completa al análisis forense y post mortem que involucra arquitecturas SASE al poner a disposición una copia del tráfico que atraviesa Prisma Access. Algunos casos de uso comunes donde la replicación de tráfico es instrumental son:

- Análisis forense y de búsqueda de amenazas donde las capturas de paquetes proporcionan evidencia irrefutable del ataque y el enfoque que se utilizó
- El cumplimiento de la normativa específica cuando las capturas de paquetes necesitan almacenarse durante cierto tiempo
- Continuar utilizando cualquier herramienta preferida de terceros en la que su organización haya invertido
- Depuración de rendimiento de redes y aplicaciones a nivel de paquetes

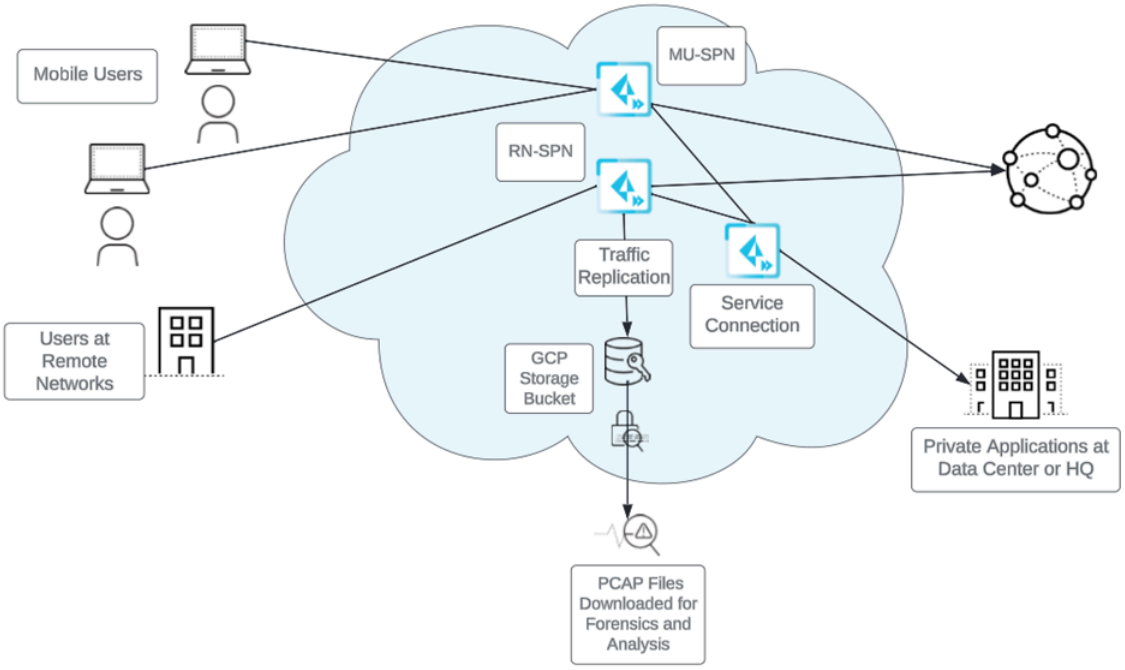
La replicación de tráfico proporciona acceso a las capturas de paquetes (pcaps) del tráfico del mundo real de los usuarios, permitiendo así la posibilidad de detectar y remediar amenazas que podrían abarcar varias sesiones o identificar y responder a comportamientos anómalos para reducir los riesgos y mantener la empresa segura.

Al habilitar la replicación de tráfico, Prisma Access crea depósitos de almacenamiento en la nube dedicados en cada ubicación de cómputo de Prisma Access donde está habilitada esta función y guarda continuamente archivos pcap que contienen una réplica del tráfico que atraviesa Prisma Access.

Para recibir notificaciones cuando se cargue un nuevo archivo pcap en el depósito de almacenamiento, puede suscribirse a las notificaciones Pub/Sub. El uso de notificaciones de Pub/Sub para nuevos archivos pcap elimina la necesidad de desarrollar herramientas que le notifiquen cuando hay una nueva carpeta o nuevos archivos en los depósitos.

Debe proporcionar una cuenta de servicio de Google Cloud que se utilizará para compartir derechos de solo lectura de estos depósitos de almacenamiento, lo que permite un acceso seguro a los archivos pcap. Se aplica un cifrado adicional de los archivos pcap en reposo, que implica una clave pública que se comparte a través de un certificado en Prisma Access. Solo usted tendría la clave privada para descifrar y recuperar los archivos pcap originales.

 ©2025 Palo Alto Networks, Inc.



Requisitos previos para la replicación del tráfico

Antes de comenzar a configurar la replicación de tráfico, tenga en cuenta los siguientes requisitos previos.

- Asegúrese de haber creado una cuenta de servicio en Google Cloud Platform (GCP).
- Asegúrese de haber creado una clave pública que se comparta a través de un certificado en la página **Objects (Objetos)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Custom Certificates (Certificados personalizados)** > **Generate (generar)** para usar en el descifrado SSL.
- La arquitectura recomendada requiere que el cómputo o el servicio que lea los archivos pcap de cada depósito de almacenamiento esté presente en la misma región GCP desde la que está leyendo el depósito. Aunque la lectura de archivos pcap desde un depósito de almacenamiento de una región GCP diferente o incluso fuera de la nube GCP podría funcionar, estos no son modelos de implementación compatibles.

Directrices de replicación del tráfico

Siga estas directrices para la replicación del tráfico:

- **Soporte TLS**: TLS 1.2 es compatible con la replicación de tráfico utilizada en implementaciones de usuarios móviles; TLS 1.2 y 1.3 son compatibles con la replicación de tráfico utilizada en implementaciones de redes remotas.
- **Algoritmos de túnel IPSec**: todos los algoritmos de túnel IPSec que son compatibles con implementaciones de usuarios móviles y redes remotas también son compatibles con replicación de tráfico.

Aprenda a configurar la replicación de tráfico:

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Replicación de tráfico en Prisma Access (Strata Cloud Manager)

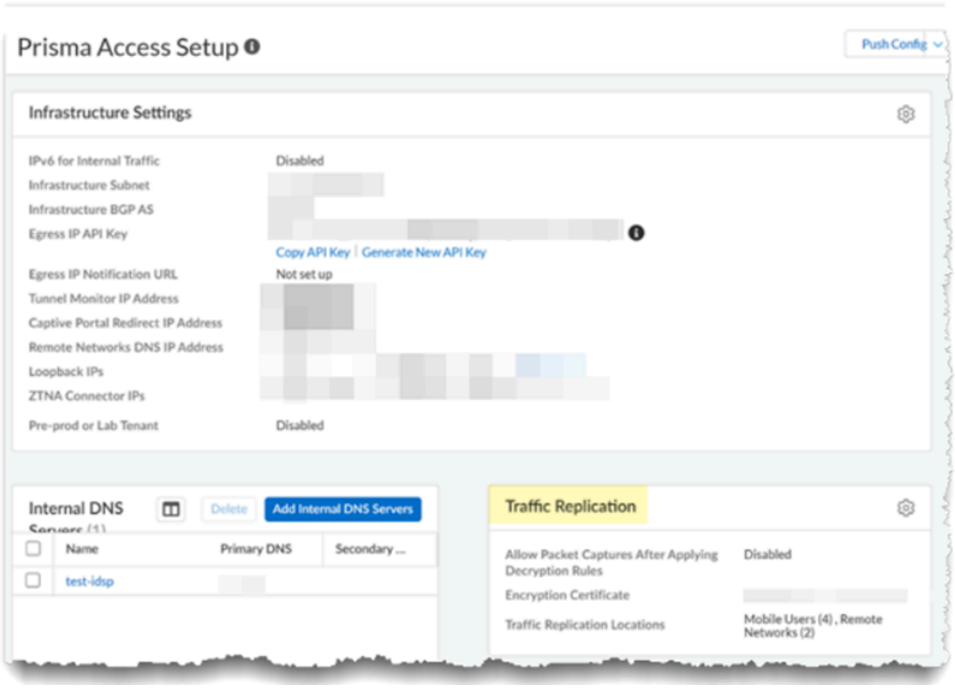
Para configurar la replicación de tráfico y acceder a los archivos de captura de paquetes (pcap), complete los siguientes pasos.

STEP 1 | Incorporación y configuración de Usuarios móviles: GlobalProtect para las ubicaciones en las que desea habilitar la replicación de tráfico y **Commit and Push (Confirmar y enviar)** sus cambios.

Debe tener habilitadas las ubicaciones de Usuarios móviles: GlobalProtect antes de habilitar la replicación de tráfico para esas ubicaciones.

STEP 2 | (Opcional) Aplique el descifrado SSL en las capturas de paquetes.

1. Vaya a Prisma Access (Managed by Strata Cloud Manager) y seleccione **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Traffic Replication (Replicación de tráfico)** y haga clic en el engranaje para editar **Settings (Configuración)**.



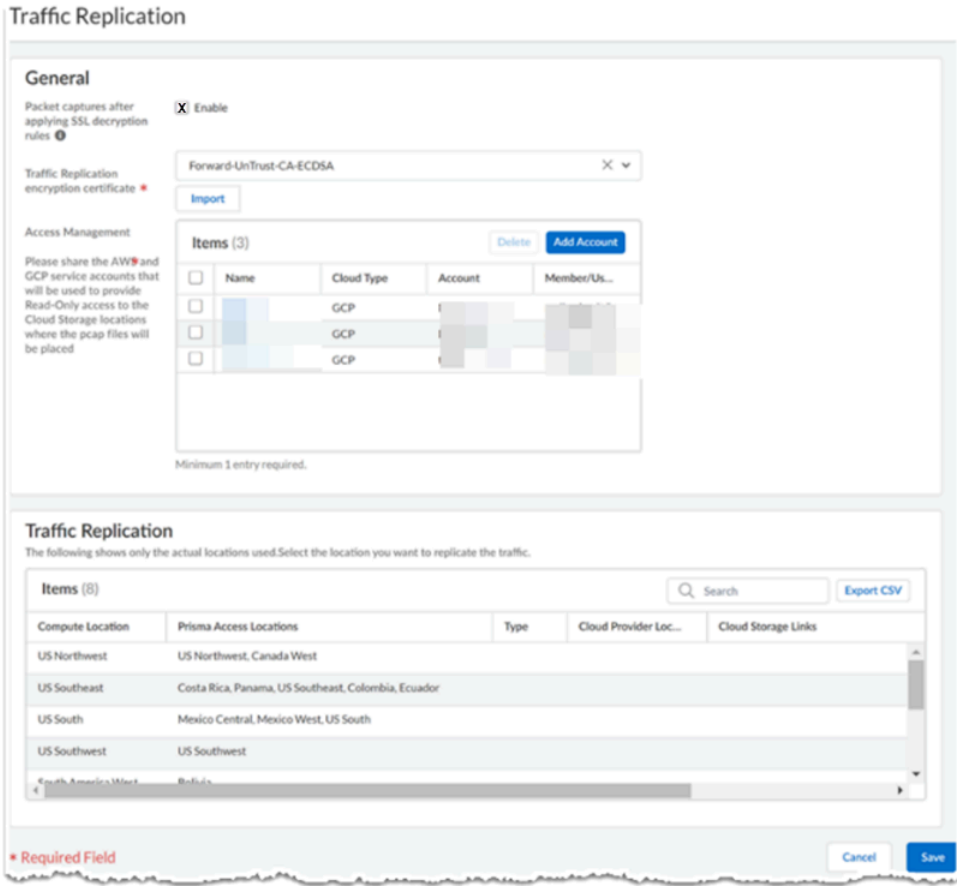
2. Habilitar **Packet captures after applying SSL decryption rules (Capturas de paquetes después de aplicar reglas de descifrado SSL)** para aplicar las políticas de descifrado SSL ya configuradas en los archivos pcap.

   Solo se descifrará el tráfico que coincida con la política de descifrado SSL en línea.

   Si selecciona esta opción, los archivos pcap usarán la mismas reglas de descifrado que haya especificado en la implementación. Si anula la selección de esta opción, no se

 ©2025 Palo Alto Networks, Inc.

realizará ningún descifrado en los archivos pcap, independientemente de las reglas de descifrado que haya configurado.



STEP 3 | Para el **Traffic Replication encryption certificate (Certificado de cifrado de replicación de tráfico)**, seleccione cualquier certificado que haya añadido en la página **Object (Objetos)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Custom Certificates (Certificados personalizados)** > **Generate (Generar)** o seleccione **Import (Importar** el certificado que se utilizará para el descifrado SSL.

El certificado consta de una clave pública y otra privada. Cargue la clave pública en Prisma Access; conserve la clave privada y utilícela para el descifrado cuando descarga los archivos pcap Comprimidos Del Depósito de almacenamiento. De esta manera, garantiza que solo su organización pueda acceder al depósito de almacenamiento donde se almacenan los archivos pcap.

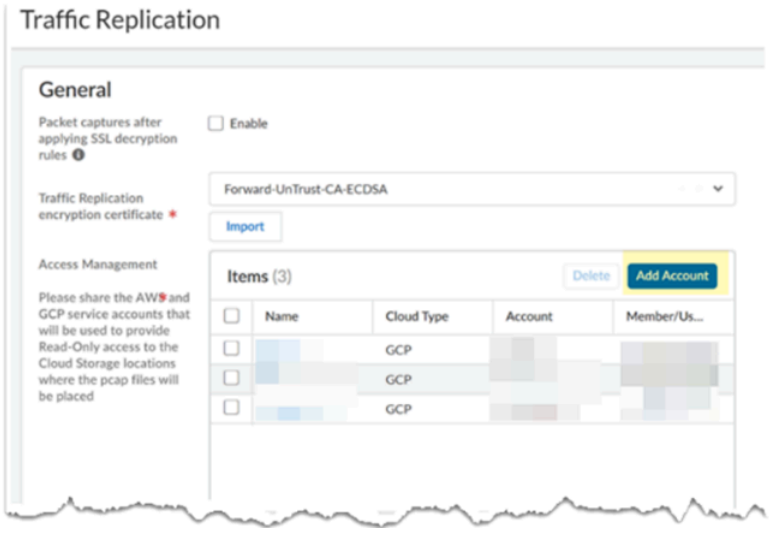
STEP 4 | Configure la cuenta de servicio de GCP que creó en el Paso 1.

La replicación de tráfico solo es compatible con las cuentas de GCP. Esta cuenta de servicio se utiliza para compartir el acceso de solo lectura a los depósitos de almacenamiento en los que se almacenan los archivos pcap en las ubicaciones en las que se ha habilitado la replicación de tráfico. Puede crear estas cuentas de servicio en su cuenta de GCP de forma normal Procedimientos de creación de cuentas de servicio de GCP. Es su responsabilidad controlar

 ©2025 Palo Alto Networks, Inc.

qué usuarios tienen acceso a estas cuentas de servicio. Cualquier usuario que tenga acceso a los archivos pcap y a la clave privada tendría acceso a los archivos pcap.

1. En el área **Access Management (Gestión de accesos)**, seleccione **Add Account (Añadir cuenta)** para añadir detalles de la cuenta para compartir el acceso de solo lectura a los depósitos de almacenamiento donde se almacenan los archivos pcap.



2. Introduzca los siguientes parámetros:
   - Dale a la cuenta un **Account Name (Nombre de cuenta)** único.
   - Especifique **GCP** como el **Type (Tipo)** para la cuenta.
   - Especifique la información de **Account (Cuenta)** de la cuenta de servicio de GCP que creó.
   - Introduzca el nombre de un **Member/User (Miembro/Usuario)** para la cuenta de servicio de GCP.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Si quiere añadir notificaciones de Pub/Sub que le notifiquen cuando se añade una carpeta nueva o archivos nuevos a un depósito, deberá configurar notificaciones de Pub/Sub en su cuenta de servicio de Google Cloud.

Prisma Access crea un único canal de Pub/Sub por inquilino para todas las ubicaciones de ese inquilino.

Las notificaciones de Pub/Sub son compatibles a partir de Prisma Access 5.2. Si ya tiene una cuenta y quiere añadir notificaciones de Pub/Sub, actualice a Prisma Access 5.2 y, luego, seleccione una de las siguientes opciones para añadir notificaciones de Pub/Sub:

- *Modifique la cuenta de servicio de Google Cloud existente que ya ha configurado en Prisma Access.*
- *Añada una nueva cuenta para la cuenta de servicio existente y especifique esa cuenta en su configuración de Prisma Access.*

  Si añade una nueva cuenta, debe deshabilitar la replicación de tráfico en la cuenta existente y habilitar la replicación de tráfico en la nueva cuenta.
- *Deshabilite y habilite la replicación de tráfico en la ubicación existente.*

Prisma Access envía mensajes de Pub/Sub con el encabezado `panw-traffic-replication-file- notifications-`<*tenantid*>, dónde <*tenantid*> es el identificador del inquilino que envía las notificaciones. Los mensajes tienen este formato:

```
Message { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1", "eventTime":
 "2024-04-24T23:12:59.xxxxxxx", "eventType": "OBJECT_FINALIZE",
 "notificationConfig": "projects/_/buckets/xxxx-xx-xxx-
xxxxxxxxx-us-west1/notificationConfigs/1", "objectGeneration":
 "xxxxxxxxxxxxxxxx", "objectId": "instance-group-
xxxxxxx/12345678_190000_xxxxx.zip", "payloadFormat": "NONE" } }
```

Donde:

- `objectGeneration` es el número de generación del objeto modificado.
- `objectID` es el nombre del objeto modificado.

STEP 6 | Configure la replicación de tráfico para una o varias ubicaciones de usuarios móviles.

1. En **Traffic Replication (Replicación de tráfico)**, seleccione las ubicaciones en las que desea habilitar la replicación de tráfico y, a continuación, seleccione **Mobile Users (Usuarios móviles)**.

   Seleccione la **Compute Location (Ubicación de cómputo)** que está asociada con **Prisma Access Locations (Ubicaciones de Prisma Access)**. La replicación de tráfico está habilitada para todos los clientes de usuarios móviles conectados a las ubicaciones seleccionadas.

STEP 7 | **Save (Guardar)** la configuración.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Confirmar y enviar sus cambios.

1. Seleccione **Manage (Gestionar)** > **Operations (Operaciones)** > **Push Config (Enviar configuración)**.
2. Seleccione **Mobile Users Container (Contenedor de usuarios móviles)** en el **Push Scope (Ámbito de envío)**, luego **Push Scope (Ámbito de envío)** y seleccione **Push (Enviar)** sus cambios.
3. Revise los objetivos de envío y seleccione **Push (Enviar)**.

STEP 9 | Compruebe el estado de la replicación del tráfico yendo a **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access** > **Traffic Replication (Replicación de tráfico)**.

STEP 10 | Descargar los archivos pcap.

Utilice la función **Cloud Storage Links (Enlaces de almacenamiento en la nube)** para acceder a los archivos pcap en sus depósitos de almacenamiento de GCP.

- Estos depósitos de almacenamiento admiten las mismas operaciones, comandos y consultas regulares que cualquier otro depósito de almacenamiento de GCP.
- Puede descargar datos pcap durante un máximo de 72 horas. Después de 72 horas, los archivos se eliminan permanentemente.
- Los archivos se cifran con su clave pública.
- El tamaño máximo del archivo es de 200 MB o 5 minutos de captura de paquetes, lo que sea menor.

1. Enumere los archivos de su servicio introduciendo `gsutil ls gs://<storage_bucket_link>/`, dónde <*storage_bucket_link*> es el enlace de almacenamiento de su cuenta de servicio de GCP donde se almacenan los archivos.
2. Descargue los archivos de su cuenta de servicio introduciendo la entrada `gs:// de la CP de gSutil<storage_bucket_link>/<file_name> <destination folder>`, donde:
   - <*storage_bucket_link*> es el enlace de almacenamiento de su cuenta de servicio de GCP donde se almacenan los archivos.
   - <*file_name*> es el nombre del archivo pcap.
   - <*destination folder*> es la carpeta donde desea que se descargue el archivo pcap.
3. Descomprima los archivos descargados.
4. Descifre los archivos descargados.

Replicación de tráfico en Prisma Access (Panorama)

Para configurar la replicación de tráfico y acceder a los archivos PCAP, siga estos pasos.

STEP 1 | Incorporación y configuración de Usuarios móviles: GlobalProtect (si configura la replicación de tráfico para usuarios móviles), Remote Networks (Redes remotas) (si configura la replicación de tráfico para redes remotas), o ambas (si configura la replicación de tráfico tanto para usuarios móviles como para redes remotas).

 ©2025 Palo Alto Networks, Inc.

STEP 2 | (Opcional) Aplique el descifrado SSL en las capturas de paquetes.

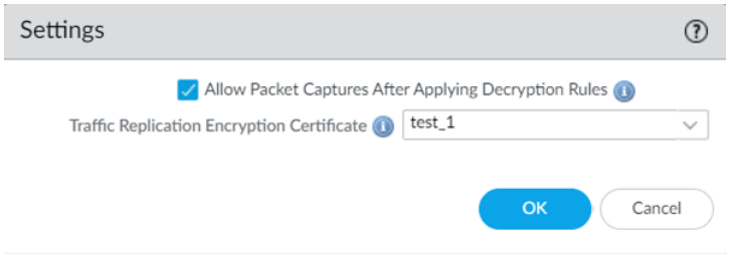
1. Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Traffic Replication (Replicación de tráfico)** y haga clic en el engranaje para editar **Settings (Configuración)**.
2. Seleccione **Allow packet captures after applying decryption rules (Permitir capturas de paquetes después de aplicar reglas de descifrado)** para aplicar las políticas de descifrado SSL ya configuradas en los archivos PCAP.

   Si selecciona esta opción, los archivos PCAP usarán la mismas reglas de descifrado que haya especificado en la implementación. Si anula la selección de esta opción, no se realizará ningún descifrado en los archivos PCAP, independientemente de las reglas de descifrado que haya configurado.

STEP 3 | Seleccione la opción **Traffic Replication Encryption Certificate (Certificado de cifrado de replicación de tráfico)** (clave pública) que creó en un paso anterior en **Mobile_User_Template** (para implementaciones de usuarios móviles) o **Remote_Network_Template** (para implementaciones de red remotas) para usar en el descifrado SSL.

Este paso es obligatorio. Puede seleccionar cualquier certificado que haya agregado en el área **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)** en **Mobile_User_Template** o **Remote_Network_Template**. Si habilita la replicación de tráfico para usuarios móviles y redes remotas, coloque el certificado en ambas **Mobile_User_Template** y **Remote_Network_Template**..

El certificado consta de una clave pública y otra privada. Cargue la clave pública en Prisma Access; conserve la clave privada y utilícela para el descifrado cuando descarga los archivos PCAP comprimidos del depósito de almacenamiento. De esta manera, garantiza que solo su organización pueda acceder al depósito de almacenamiento donde se almacenan los archivos PCAP.



STEP 4 | Configure la replicación de tráfico para una o más ubicaciones de Usuarios móviles: GlobalProtect, ubicaciones de redes remotas o ambas seleccionando la ubicación en el menú **Configuration (Configuración)** y seleccionando las ubicaciones en las que desea habilitar la replicación de tráfico y, a continuación, seleccionando **MU-GP**, **RN**, o ambas.

Seleccione la **Compute Location (Ubicación de cómputo)** que está asociada con **Prisma Access Locations (Ubicaciones de Prisma Access)**. La replicación del tráfico está habilitada para todos

 ©2025 Palo Alto Networks, Inc.

los clientes de Usuarios móviles: GlobalProtect, usuarios de redes remotas o ambos, que estén conectados a las ubicaciones seleccionadas.

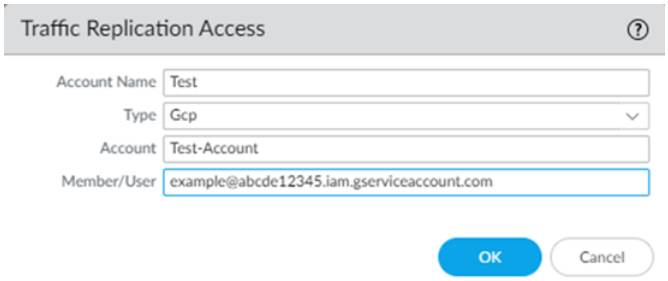


STEP 5 | Añada una cuenta que le permita acceder a los datos de captura de paquetes de replicación de tráfico (PCAP).

Esta cuenta de servicio se utiliza para compartir el acceso de solo lectura a los depósitos de almacenamiento en los que se almacenan los archivos PCAP en las ubicaciones en las que se ha habilitado la replicación de tráfico. Crea estas cuentas de servicio en su cuenta de GCP de forma normal Procedimientos de creación de cuentas de servicio de GCP. Es su responsabilidad controlar qué usuarios tienen acceso a estas cuentas de servicio. Cualquier usuario que tenga acceso a los archivos PCAP y a la clave privada tendría acceso a los archivos PCAP.

1. En el área **Traffic Replication Access (Acceso a la replicación de tráfico)**, seleccione **Add (Añadir)** para añadir una cuenta.
2. Introduzca los siguientes parámetros:
   - Dale a la cuenta un **Account Name (Nombre de cuenta)** único.
   - Especifique **GCP** como el **Type (Tipo)** para la cuenta.

     La replicación de tráfico solo es compatible con las cuentas de GCP.
   - Especifique la información de **Account (Cuenta)** de la cuenta de servicio de GCP que creó.
   - Introduzca el nombre de un **Member/User (Miembro/Usuario)** para la cuenta de servicio de GCP.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Si quiere añadir notificaciones de Pub/Sub que le notifiquen cuando se añade una carpeta nueva o archivos nuevos a un depósito, deberá configurar notificaciones de Pub/Sub en su cuenta de servicio de Google Cloud.

Prisma Access crea un único canal de Pub/Sub por inquilino para todas las ubicaciones de ese inquilino.

Las notificaciones de Pub/Sub son compatibles a partir de Prisma Access 5.2. Si ya tiene una cuenta y quiere añadir notificaciones de Pub/Sub, actualice a Prisma Access 5.2 y, luego, seleccione una de las siguientes opciones para añadir notificaciones de Pub/Sub:

- *Modifique la cuenta de servicio de Google Cloud existente que ya ha configurado en Prisma Access.*
- *Añada una nueva cuenta para la cuenta de servicio existente y especifique esa cuenta en su configuración de Prisma Access.*

  Si añade una nueva cuenta, debe deshabilitar la replicación de tráfico en la cuenta existente y habilitar la replicación de tráfico en la nueva cuenta.
- *Deshabilite y habilite la replicación de tráfico en la ubicación existente.*

Prisma Access envía mensajes de Pub/Sub con el encabezado `panw-traffic-replication-file- notifications-`<*tenantid*>, dónde <*tenantid*> es el identificador del inquilino que envía las notificaciones. Los mensajes tienen este formato:

```
Message { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1", "eventTime":
 "2024-04-24T23:12:59.xxxxxxx", "eventType": "OBJECT_FINALIZE",
 "notificationConfig": "projects/_/buckets/xxxx-xx-xxx-
xxxxxxxxx-us-west1/notificationConfigs/1", "objectGeneration":
 "xxxxxxxxxxxxxxxx", "objectId": "instance-group-
xxxxxxx/12345678_190000_xxxxx.zip", "payloadFormat": "NONE" } }
```

Donde:

- `objectGeneration` es el número de generación del objeto modificado.
- `objectID` es el nombre del objeto modificado.

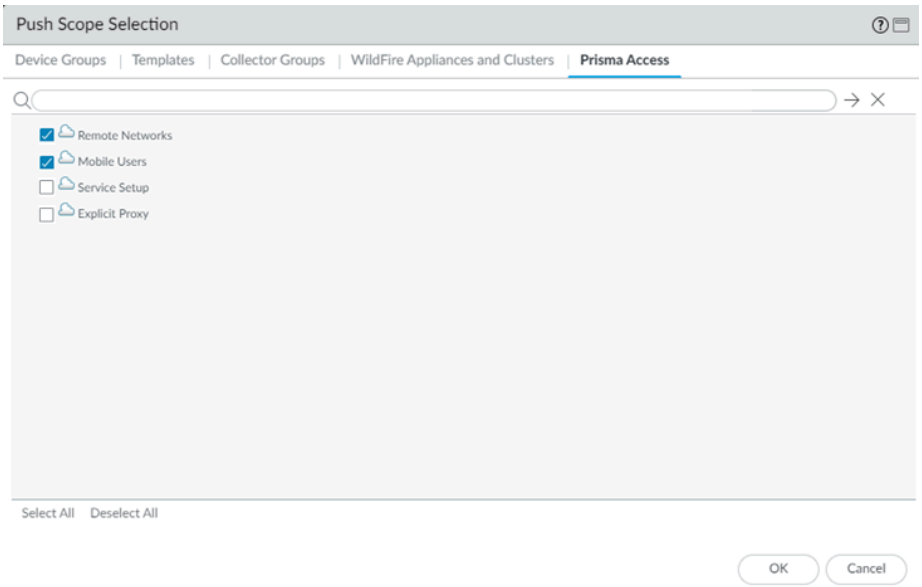
STEP 7 | Confirme e impulse sus cambios, asegurándose de que **Mobile Users (Usuarios móviles)** (para una implementación de usuario móvil), **Remote Networks (Redes remotas)** (para una implementación de redes remotas), o ambas se seleccionan en el **Push Scope (Ámbito de envío)**.

1. Haga clic en **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.
2. Debe **Edit Selections (Editar selecciones)** y, en la pestaña **Prisma Access**, asegurarse de que **Mobile Users (Usuarios móviles)** y **Remote Networks (Redes remotas)**

 ©2025 Palo Alto Networks, Inc.

estánseleccionas en el **Push Scope (Ámbito de envío)**, a continuación, haga clic en **OK (Aceptar)**.

Es posible que **Push Scope (Ámbito de envío)** no se seleccione automáticamente.



3. Haga clic en **Commit and Push (Confirmar y enviar)**.

STEP 8 | Compruebe el estado)de la replicación del tráfico yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Traffic Replication (Replicación de tráfico)**.



Storage Links (Enlaces de almacenamiento) es el nombre del depósito de almacenamiento de GCP donde puede acceder a los archivos PCAP, la **Cloud Provider Location (Ubicación del proveedor de nube)** es la ubicación donde se incorpora la instancia de GCP.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Descargue los archivos PCAP utilizando la clave privada que solo usted posee.

Utilice **Storage Links (Enlaces de almacenamiento)** para acceder a los archivos PCAP en sus depósitos de almacenamiento de GCP.

- Estos depósitos de almacenamiento admiten las mismas operaciones, comandos y consultas regulares que cualquier otro depósito de almacenamiento de GCP.
- Puede descargar datos PCAP durante un máximo de 72 horas. Después de 72 horas, los archivos se eliminan permanentemente.
- Los archivos se cifran con su clave pública.
- El tamaño máximo del archivo es de 200 MB o 5 minutos de captura de paquetes, lo que sea menor.

1. Enumere los archivos de su servicio introduciendo `gsutil ls gs://<storage_bucket_link>/`, dónde *<storage_bucket_link>* es el enlace de almacenamiento de su cuenta de servicio de GCP donde se almacenan los archivos.
2. Descargue los archivos de su cuenta de servicio introduciendo la entrada `gs:// de la CP de gSutil<storage_bucket_link>/<file_name> <destination folder>`, donde:
   - *<storage_bucket_link>* es el enlace de almacenamiento de su cuenta de servicio de GCP donde se almacenan los archivos.
   - *<file_name>* es el nombre del archivo PCAP.
   - *<destination folder>* es la carpeta donde desea que se descargue el archivo PCAP.
3. Descomprima los archivos descargados.
4. Descifre los archivos descargados usando la clave privada que solo usted posee.

 ©2025 Palo Alto Networks, Inc.

Implementaciones avanzadas de Redes remotas de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Las siguientes secciones le muestran las implementaciones avanzadas que están disponibles para Redes remotas de Prisma Access:

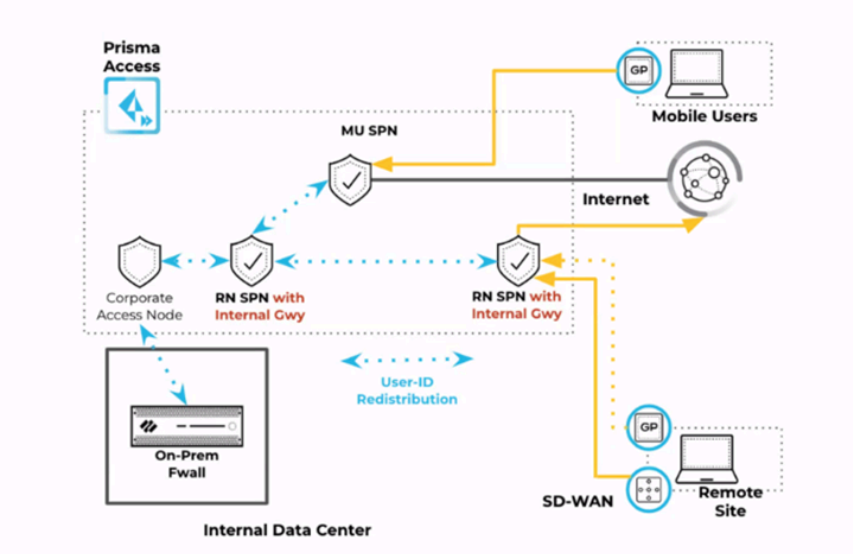
- Proporcionar acceso seguro entrante a ubicaciones de red remotas
- Crear una red de gran ancho de banda para un sitio remoto

Puerta de enlace interna de Prisma Access

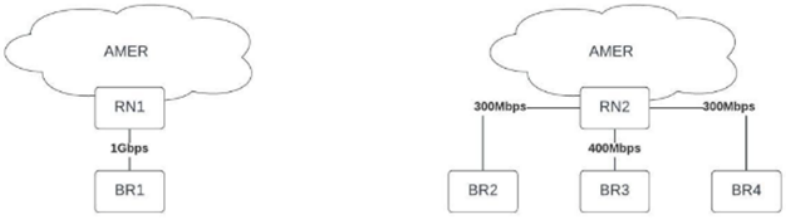
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia de usuario de Prisma Access y móvil ❑ Minimum Required Prisma Access Version: 5.1 ❑ Versión mínima de plano de datos requerida paraPrisma Access (Managed by Panorama): 10.2.4 ❑ Versión mínima requerida del cliente GlobalProtect: 6.0

Anteriormente, para generar asignaciones de usuarios de IP y HIP para hosts que ejecutan el software cliente GlobalProtect en Redes remotas de Prisma Access, es necesario implementar un NGFW local como puerta de enlace interna. Esta solución no es nativa de la nube. Con la puerta de enlace interna nativa de la nube de Prisma Access, puede evitar el uso de puertas de enlace internas locales y la puerta de enlace interna de Prisma Access genera las asignaciones de usuarios de IP y HIP localmente en redes remotas. Las redes remotas consumen asignaciones de IP de usuarios y HIP de la base de datos local para realizar verificaciones de postura en lugar de descubrirlas en otros cortafuegos.

 ©2025 Palo Alto Networks, Inc.

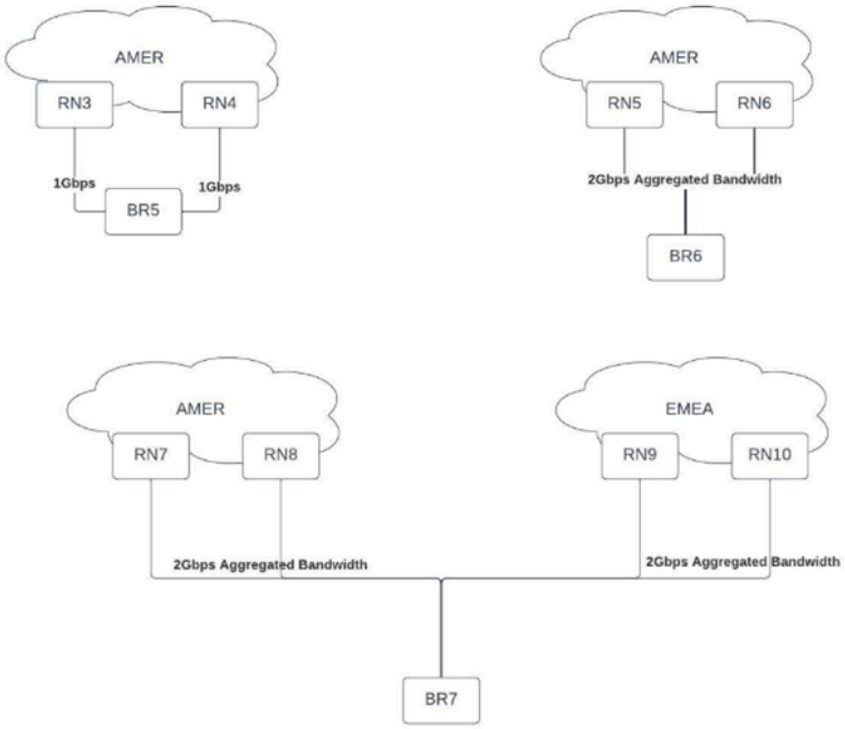


Tenga en cuenta que no puede implementar una puerta de enlace interna cuando un sitio remoto tiene varios túneles IPsec a diferentes sitios de red remotos (por ejemplo, un túnel activo/activo) o un sitio con gran ancho de banda. El siguiente diagrama muestra un ejemplo de un entorno compatible para una implementación de puerta de enlace interna.



El siguiente diagrama proporciona ejemplos de implementaciones en las que no se admiten puertas de enlace internas.

 ©2025 Palo Alto Networks, Inc.



Antes de establecer la puerta de enlace interna de Prisma Access, incorpore sus usuarios móviles.

- Strata Cloud Manager
- Panorama

Puerta de enlace interna de Prisma Access (Strata Cloud Manager)

Complete los siguientes pasos para configurar la puerta de enlace interna de Prisma Access.

STEP 1 | En Strata Cloud Manager, configurare GlobalProtect, añada configuraciones de aplicaciones e integre redes remotas.

Tenga en cuenta que no hay detección de host interno ni configuraciones de puerta de enlace interna en este momento.

STEP 2 | Tome nota de la **Remote Networks DNS IP Address (Dirección IP DNS de redes remotas)** de **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access**.

STEP 3 | Tome nota de las **Gateway FQDNs (FQDN de puerta de enlace)** de **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **Infrastructure (Infraestructura)** > **Infrastructure Settings (Configuración de la infraestructura)** > **Gateway FQDNs (FQDN de puerta de enlace)**.

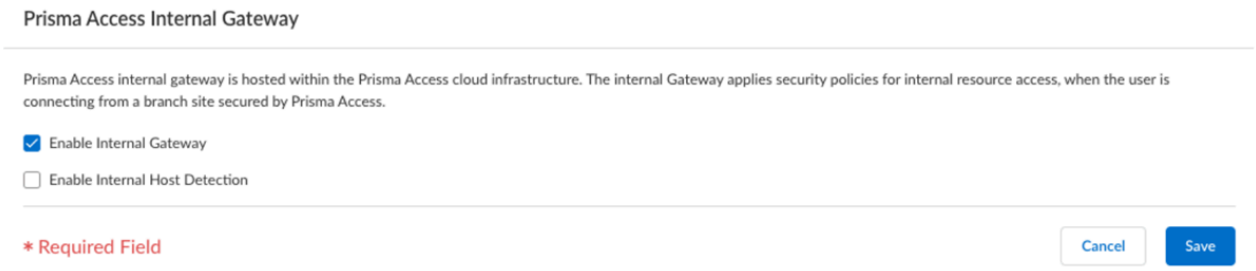
STEP 4 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)** > **Advanced Settings (Ajustes avanzados)**.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Edite la configuración de la **Prisma Access Internal Gateway (Puerta de enlace interna de Prisma Access)** para habilitar la puerta de enlace interna y seleccione **Save (Guardar)** para guardar los cambios.

(Opcional) Deberá **Enable Internal Host Detection (Habilitar la detección de host interno)** para IPv4 si no desea utilizar su propio servidor DNS. Puede habilitar la detección de host interno solo después de seleccionar **Enable Internal Gateway (Habilitar puerta de enlace interna)**.

Prisma Access admite la detección de host interno solo para el método de conexión método de conexión***Always On (Siempre activo)***.

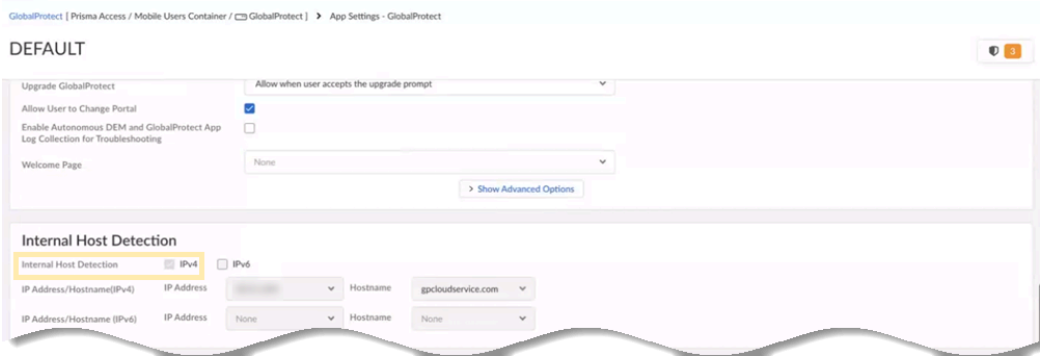


Cuando habilita la puerta de enlace interna, las instancias de red remotas actúan como puertas de enlace internas. Al habilitar la detección de host interno, Prisma Access crea registros PTR en los servidores proxy DNS de la red remota para el proceso de detección de host interno.

STEP 6 | Seleccione **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Aplicación de GlobalProtect)**.

STEP 7 | Seleccione una configuración de aplicación y vea los detalles de detección de host interno y los detalles de la puerta de enlace interna.

Al habilitar la puerta de enlace interna y la detección de host interno en el paso 5, Prisma Access permite la detección de host interno IPv4 y la puerta de enlace interna aquí también. Prisma Access rellena el valor **Remote Networks DNS IP Address (Dirección IP DNS de redes remotas)**, desde el paso 2, como la dirección IP.

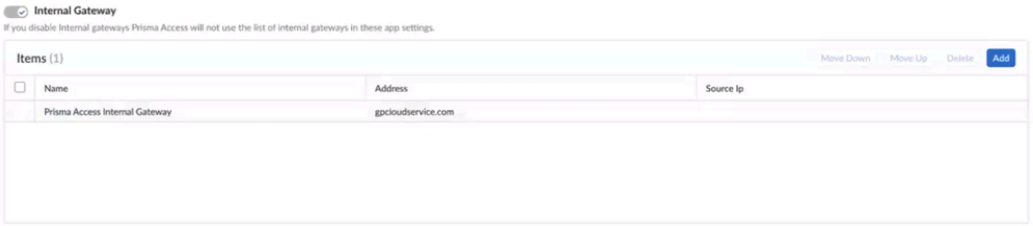


Tenga en cuenta que la detección de host interno IPv6 en los proxies DNS de Prisma Access no es compatible.

No es posible eliminar esta entrada de **Prisma Access Internal Gateway (Puerta de enlace interna de Prisma Access)**. Sin embargo, puede añadir las puertas de enlace internas implementadas automáticamente. Puede implementar sus propios servidores DNS en la red interna para la detección de host interno, pero asegúrese de añadir registros PTR para que la

 ©2025 Palo Alto Networks, Inc.

detección de host interno sea posible. Prisma Access anexa el valor **Gateway FQDNs (FQDN de puerta de enlace)**, desde el paso 3, a la dirección.



Puede ver los detalles de la dirección IP del servidor proxy DNS seleccionando **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Prisma Access**.

Si habilita **Internal Host Detection (Detección de host interno)**, verifique que la resolución DNS esté funcionando, realice una búsqueda inversa de DNS desde su red interna a la IP del servidor proxy DNS y asegúrese de que devuelva un FQDN que comience con **`any-igw`**.

STEP 8 | **Push (Enviar)** los cambios en los usuarios móviles y las redes remotas al mismo tiempo.

STEP 9 | Inicie sesión en el endpoint.

Cuando se conecta a GlobalProtect, primero se autentica con el portal de GlobalProtect. La detección de host interno activa GlobalProtect para conectarse a la puerta de enlace interna. A continuación, a medida que el agente de GlobalProtect sigue funcionando en el modo sin túnel, aparece la segunda autenticación y envía la información del host a la puerta de enlace interna en redes remotas.

Puerta de enlace interna de Prisma Access (Panorama)

STEP 1 | En Panorama, configurare GlobalProtect, añada configuraciones de aplicaciones e integre redes remotas.

Tenga en cuenta que no hay detección de host interno ni configuraciones de puerta de enlace interna en este momento.

STEP 2 | Vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** > **Settings (Configuración)**.

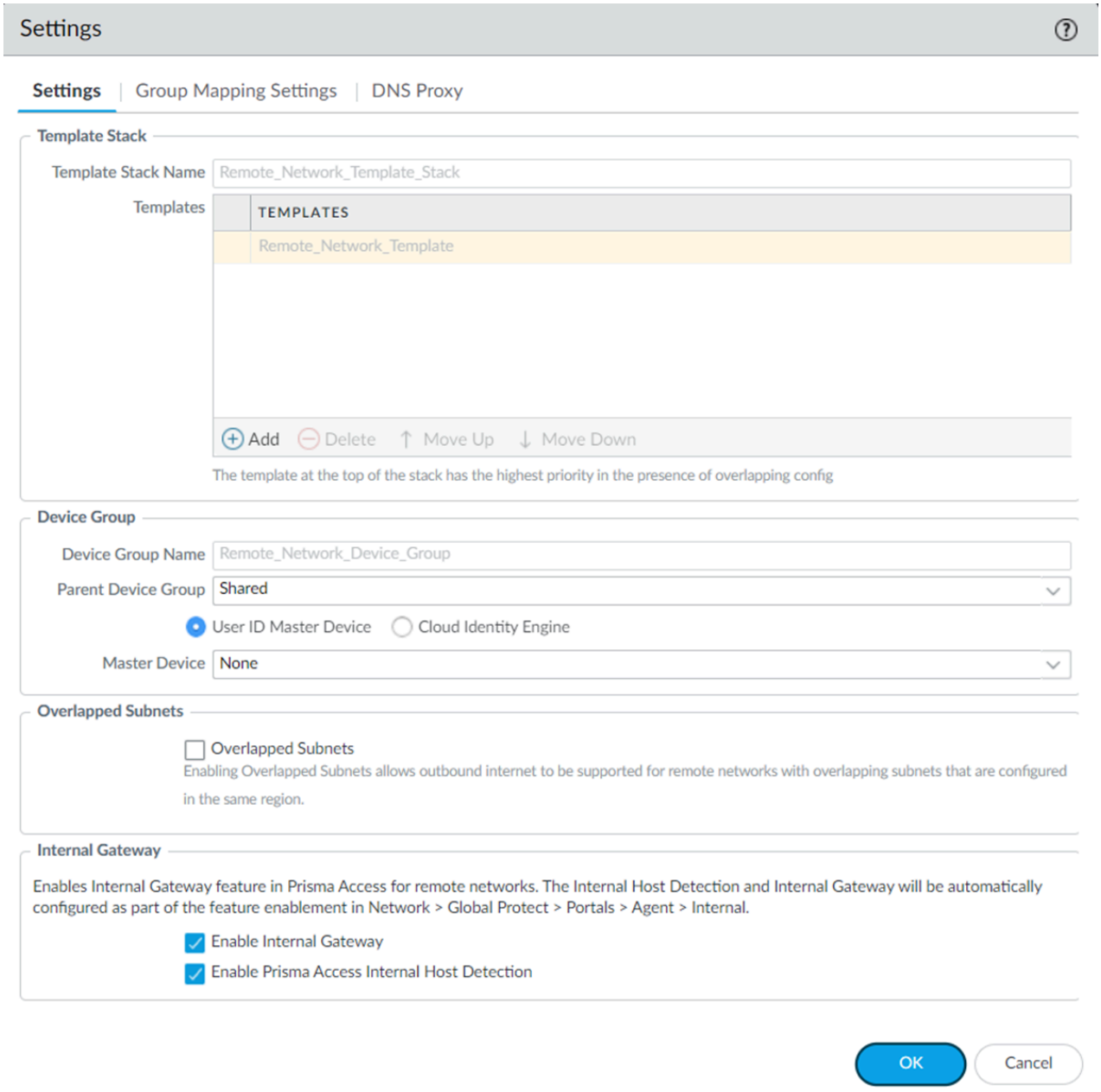
STEP 3 | Seleccione **Enable Internal Gateway (Habilitar puerta de enlace interna)** y guarde los cambios.

(Opcional) Puede **Enable Prisma Access Internal Host Detection (Habilitar la detección de host interno de Prisma Access)** para IPv4 si no desea utilizar su propio servidor DNS. Puede

 ©2025 Palo Alto Networks, Inc.

habilitar la detección de host interno solo después de seleccionar **Enable Internal Gateway (Habilitar puerta de enlace interna)**.

Prisma Access admite la detección de host interno solo para el método de conexión método de conexión***Always On (Siempre activo)***.



Cuando habilita la puerta de enlace interna, las instancias de red remotas actúan como puertas de enlace internas. Cuando habilita la detección de host interno, Prisma Access crea registros PTR en los servidores proxy DNS de la red remota para el proceso de detección de host interno.

Cuando habilita la puerta de enlace interna, Prisma Access crea una configuración de puerta de enlace interna en una plantilla de red remota.

 ©2025 Palo Alto Networks, Inc.

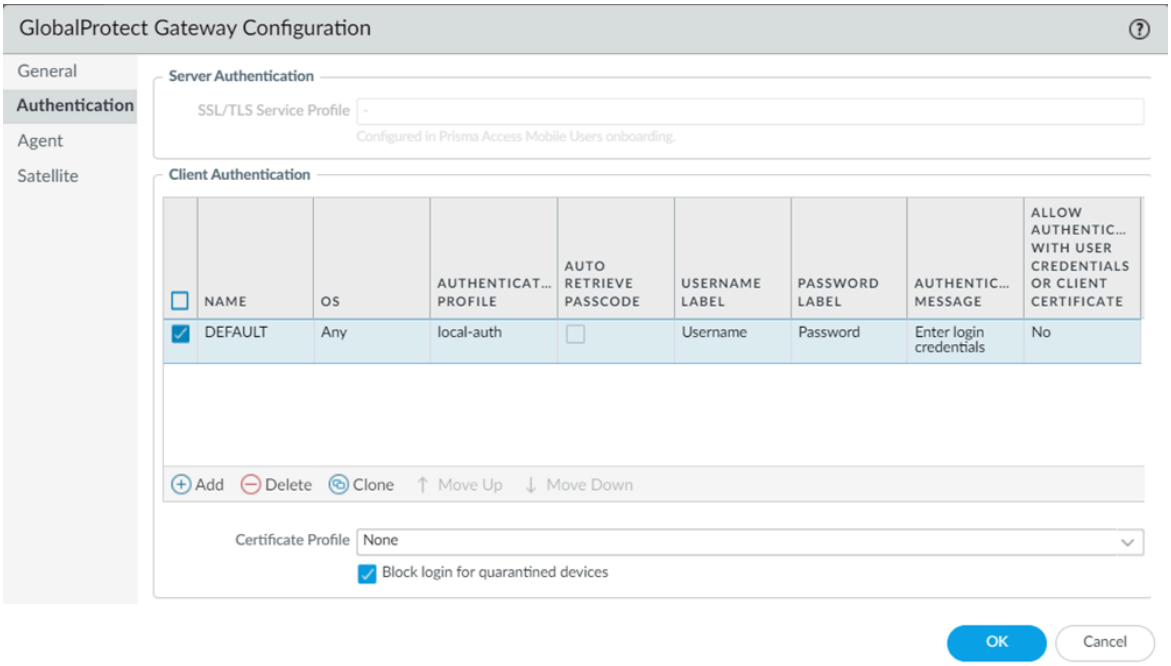
STEP 4 | Vaya a **Templates (Plantillas)** > **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y seleccione **Remote_Network_Template**.

Encontrará la plantilla **GlobalProtect_Internal_Gateway** creada para la puerta de enlace interna.

 ©2025 Palo Alto Networks, Inc.

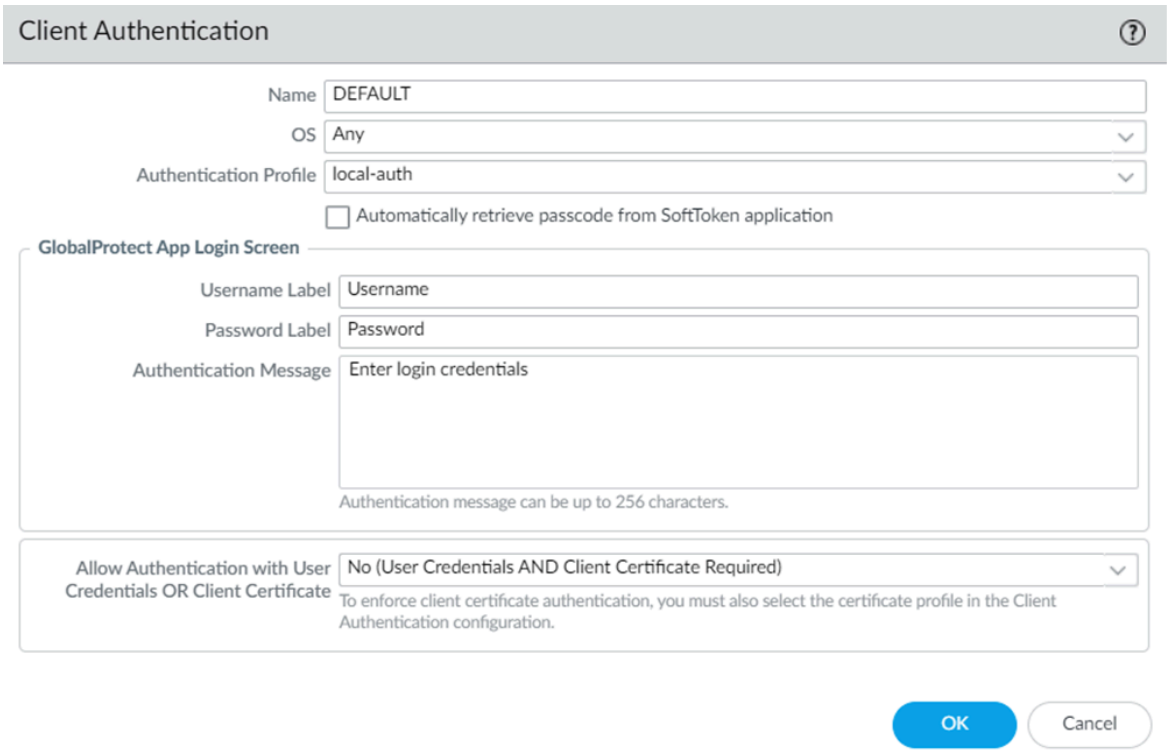
STEP 5 | Cree un perfil de autenticación para esta plantilla de red remota similar al perfil de autenticación en la plantilla de usuario móvil.

1. Seleccione la plantilla de red remota, plantilla **GlobalProtect_Internal_Gateway**, hipervínculo.
2. Vaya a **Authentication (Autenticación)** > **Client Authentication (Autenticación del cliente)**.

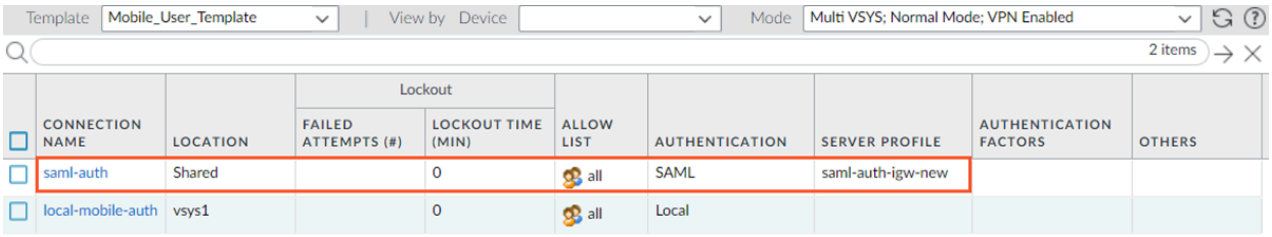


3. Edite los detalles del perfil de autenticación de la autenticación **DEFAULT (PREDETERMINADA)** del cliente.

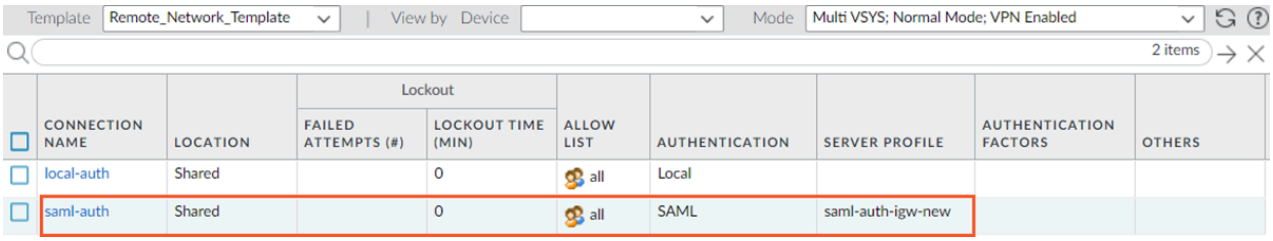
 ©2025 Palo Alto Networks, Inc.



Cree un perfil de autenticación igual al de la plantilla de usuario móvil. Puede encontrar el perfil de autenticación utilizado en la plantilla de usuario móvil en **Template (Plantilla)** > **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)**. Asegúrese de seleccionar **Mobile_User_Template**.



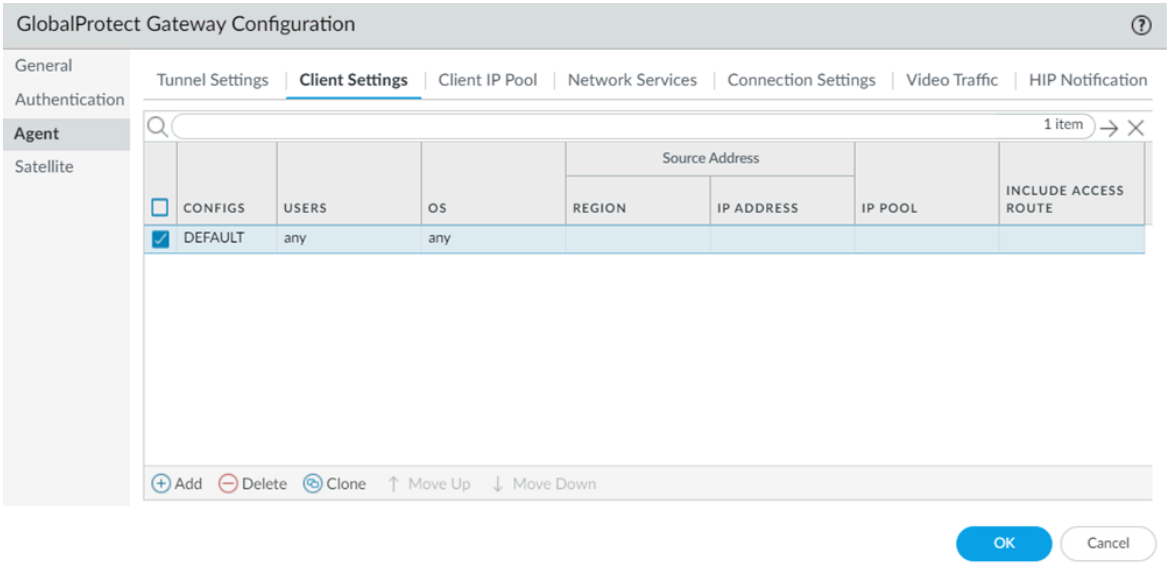
*También puede ver el perfil de autenticación de la plantilla de red remota seleccionando **Templates (Plantillas)** > **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)**. Seleccione **Remote_Network_Template**.*



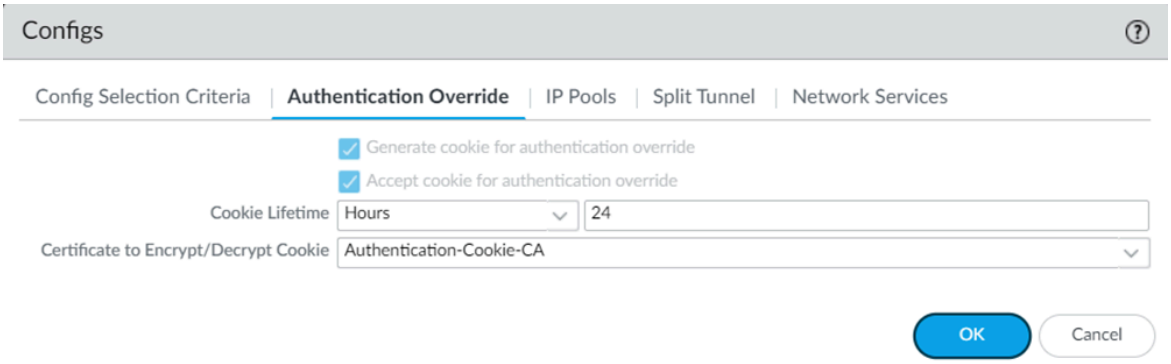
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Cree un certificado de dispositivo para la plantilla de red remota similar al certificado de dispositivo en la plantilla de usuario móvil.

1. Seleccione la plantilla de red remota, **GlobalProtect_Internal_Gateway**, hipervínculo.
2. Vaya a **Agent (Agente)** > **Client Settings (Configuración del cliente)**.



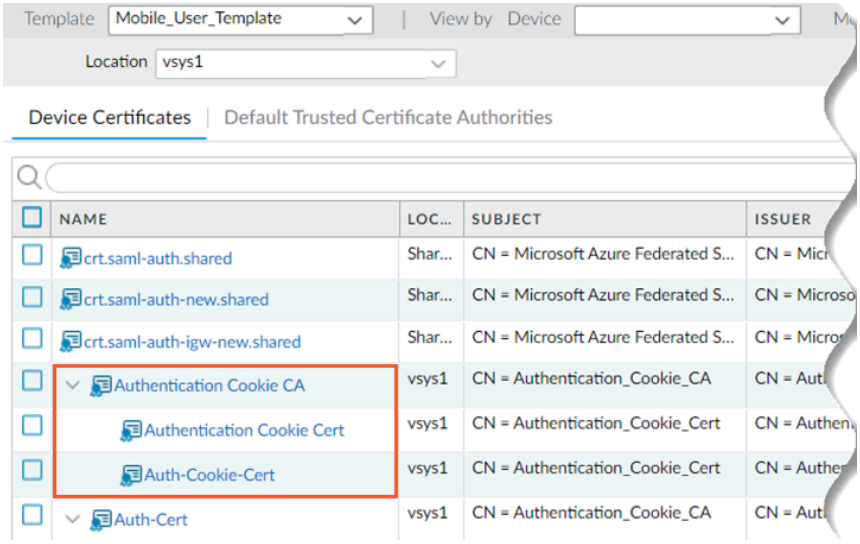
3. Seleccione la configuración **DEFAULT (PREDETERMINADA)** y vaya a la configuración **Authentication Override (Anulación de autenticación)**.
4. Edite la configuración **Certificate to Encrypt/Decrypt Cookie (Certificado para cifrar/descifrar cookies)** y cree un nuevo certificado de dispositivo.



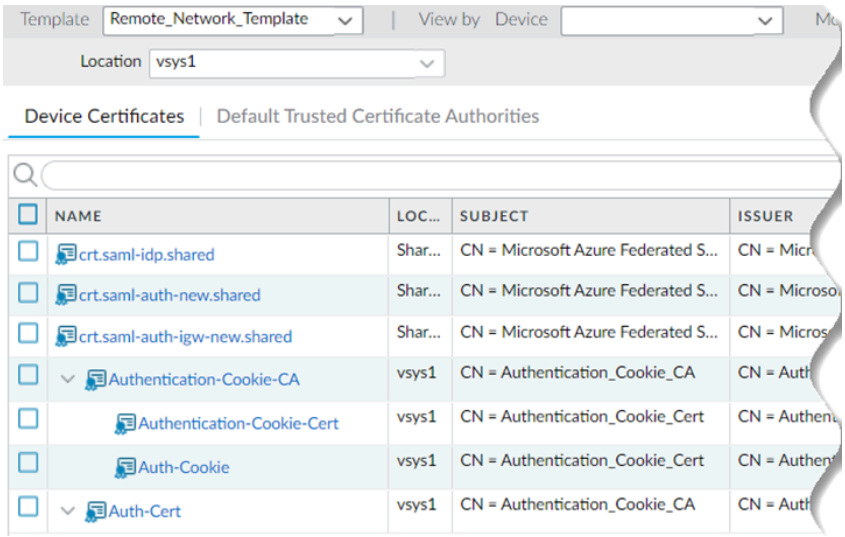
Cree un certificado de dispositivo igual al de la plantilla de usuario móvil. Puede encontrar el certificado del dispositivo utilizado en la plantilla de usuario móvil en **Template (Plantilla)** > **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Asegúrese de seleccionar **Mobile_User_Template**. La configuración **DEFAULT (PREDETERMINADA)** hace referencia al certificado **Authentication**

 ©2025 Palo Alto Networks, Inc.

Cookie CA (CA de cookie de autenticación). Siga la misma jerarquía que en **Mobile_User_Template** para una autenticación correcta.



*También puede ver el certificado del dispositivo para la plantilla de red remota seleccionando **Template (Plantilla)** > **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**. Seleccione **Remote_Network_Template**.*



STEP 7 | **Push (Enviar)** los cambios en los usuarios móviles y las redes remotas al mismo tiempo.

Proporcionar acceso seguro entrante a ubicaciones de red remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access que incluye Interconexión de red para el acceso de sitio a sitio y de usuario a sitio

 ©2025 Palo Alto Networks, Inc.

Si su organización aloja aplicaciones accesibles por internet en un sitio de red remoto, proporcionar acceso a esas aplicaciones expone su red a todas las amenazas que plantea un internet abierto. Esta sección describe cómo Prisma Access proporciona una forma de proporcionar acceso seguro a esas aplicaciones, cuándo debe implementarlo y cómo configurarlo.

- Asegurar el acceso entrante para sitios de red remotos
- Ejemplos de acceso entrante
- Directrices para utilizar el acceso entrante seguro
- Configurar acceso entrante seguro para sitios de red remotos

Asegurar el acceso entrante para sitios de red remotos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• La licencia de Prisma Access que incluye interconexión neta para acceso de sitio a sitio y usuario a sitio

Prisma Access para redes remotas permite el acceso saliente a aplicaciones conectadas a Internet. En algunos casos, su organización podría tener un requisito para proporcionar acceso entrante a una aplicación o sitio web en un sitio remoto, y proporcionar acceso seguro a esa aplicación para cualquier usuario conectado a Internet, no solo para los usuarios que están protegidos por Prisma Access. Por ejemplo:

- Aloja una aplicación o portal personalizado orientado al público en un sitio de red remoto.
- Tiene un entorno de laboratorio o de pruebas para el cual desea proporcionar acceso seguro.
- Tiene la necesidad de proporcionar acceso a una aplicación o sitio web a usuarios que no son miembros de un dominio organizacional.
- Tienes dispositivos IoT que requieren acceso a una aplicación interna de gestión de activos, seguimiento o estado.

Para hacer esto, crea una red remota que permita el acceso seguro entrante. Si necesita acceso saliente así como acceso entrante para un sitio de red remoto, cree dos redes remotas en la misma ubicación: una para el acceso entrante y otra para el acceso saliente.

Si bien esta solución puede proporcionar acceso para hasta 50.000 sesiones entrantes concurrentes por red remota, Palo Alto Networks no recomienda utilizar esta solución para proporcionar acceso a una aplicación o sitio web de alto volumen.

Ejemplos de acceso entrante

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access que incluye Net Interconnect para acceso de sitio a sitio y de usuario a sitio

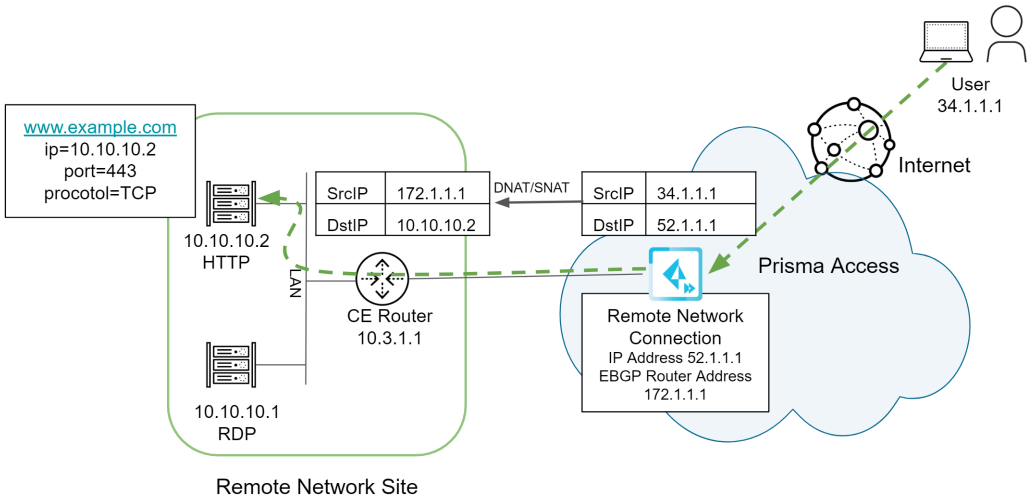
 ©2025 Palo Alto Networks, Inc.

Esta sección proporciona ejemplos de acceso entrante, junto con las direcciones IP que Prisma Access asigna en varias implementaciones.

El siguiente ejemplo muestra una configuración de muestra para habilitar el acceso entrante a una aplicación (www.example.com) en un sitio de red remoto. Asigna una dirección IP 10.10.10.2, un puerto 443 y un protocolo TCP a la aplicación. Luego introduce estos valores en Prisma Access cuando configura el acceso entrante. Después de guardar y confirmar los cambios, Prisma Access asigna una dirección IP pública a la aplicación que usted definió, en este caso 52.1.1.1.

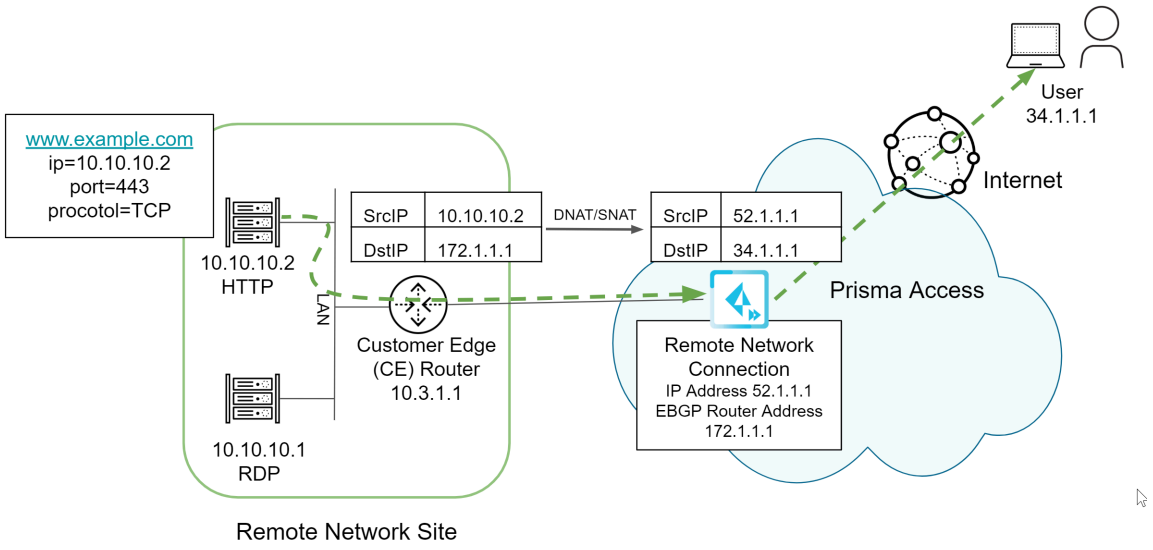
Prisma Access realiza la traducción de la dirección de red de origen (NAT de origen) en los paquetes de forma predeterminada. Si el dispositivo compatible con IPSec en su sitio de red remoto es capaz de realizar un retorno simétrico (como un cortafuegos de nueva generación de Palo Alto Networks), puede deshabilitar NAT de origen.

La siguiente imagen muestra el flujo de tráfico de los usuarios a las aplicaciones. Dado que la NAT de origen está habilitada, la dirección IP de origen en la tabla de enrutamiento cambia de la IP del dispositivo del usuario (34.1.1.1) a la dirección del **EBGP Router (Enrutador EBGP)** de la red remota [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** > **EBGP Router (Enrutador EBGP)**]. (172.1.1.1).

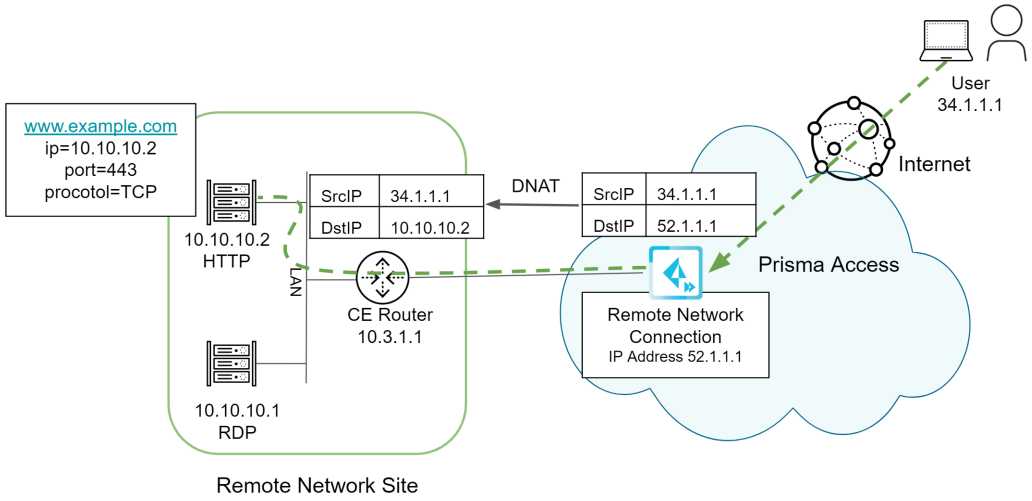


La siguiente imagen muestra la ruta de retorno del tráfico con NAT de origen habilitado.

 ©2025 Palo Alto Networks, Inc.

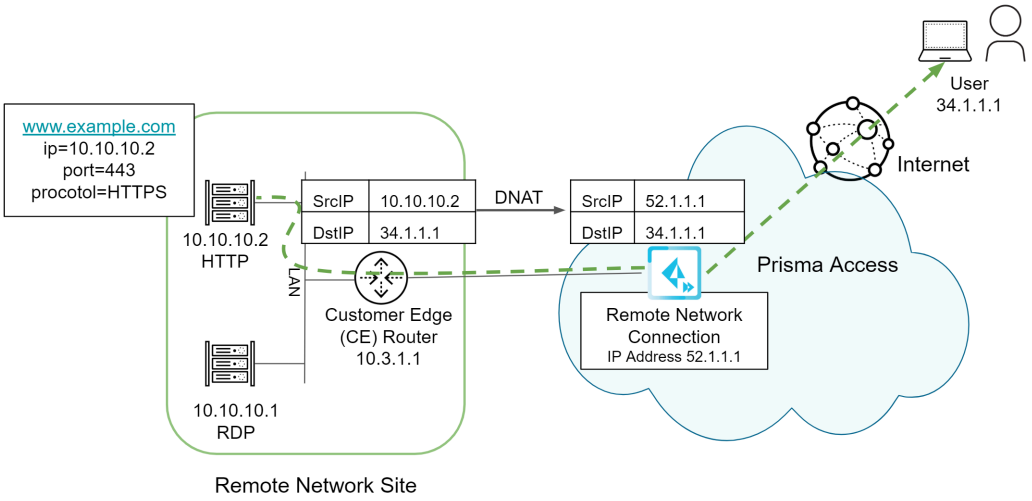


Si deshabilita el NAT de origen, Prisma Access todavía realiza NAT de destino, pero la dirección IP de origen de la solicitud no cambia.



Para el tráfico de retorno, SNAT está deshabilitado y la dirección de destino para todas las tablas de enrutamiento es la dirección IP del usuario (34.1.1.1).

 ©2025 Palo Alto Networks, Inc.



Si tiene un recurso que se encuentra en un sitio de red remoto que tiene habilitado el acceso entrante y desea que los usuarios de sitios de acceso no entrante tengan acceso a ese recurso, puede **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Permitir flujos entrantes a otras redes remotas a través de la red troncal de Prisma Access)** al configurar la red remota de acceso no entrante.

Si permite flujos de entrada desde otras redes remotas, debe habilitar NAT de origen.



Directrices para utilizar el acceso entrante seguro

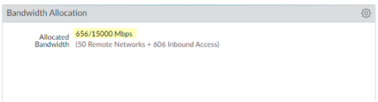
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licenciade Prisma Access que incluye Net Interconnect para acceso de sitio a sitio y de usuario a sitio

Utilice las siguientes pautas y restricciones al configurar una red remota para utilizar acceso entrante seguro:

- Cuando configura una red remota para acceso entrante, agrega unidades (Mbps) de su licencia para las direcciones IP que asigna (150 Mbps para 5 direcciones IP y 300 Mbps para 10 direcciones IP). Por este motivo, asegúrese de tener suficiente ancho de banda con licencia restante para integrar las redes remotas de acceso entrante antes de comenzar. Para verificar su ancho de banda disponible, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y vea su **Bandwidth**

 ©2025 Palo Alto Networks, Inc.

Allocation (Asignación de ancho de banda)con licencia. Esta área muestra el ancho de banda que ya ha asignado, junto con el ancho de banda total autorizado.



- El acceso entrante seguro utiliza un subconjunto de ubicaciones de Prisma Access.
- No es posible modificar una red remota existente para proporcionar acceso entrante seguro; en su lugar, cree una nueva red remota.
- La función de acceso entrante no está disponible en redes remotas que utilizan el equilibrio de carga ECMP.
- No se admite la traducción del puerto de la aplicación.
- La función importación masiva para integrar redes remotas no admite el acceso entrante. Utilice Panorama para incorporar nuevas redes remotas de acceso entrante.
- No utilice el acceso entrante a la red remota con reglas de reenvío de tráfico con conexiones de servicio.
- El tráfico saliente que se origina en la sucursal no está permitido en la red remota entrante.
- No se admite la autenticación de aplicaciones ni de User-ID.
- Prisma Access aplica los siguientes umbrales de limitación de velocidad para proporcionar protección contra inundaciones y mide la tasa en conexiones por segundo (CPS):

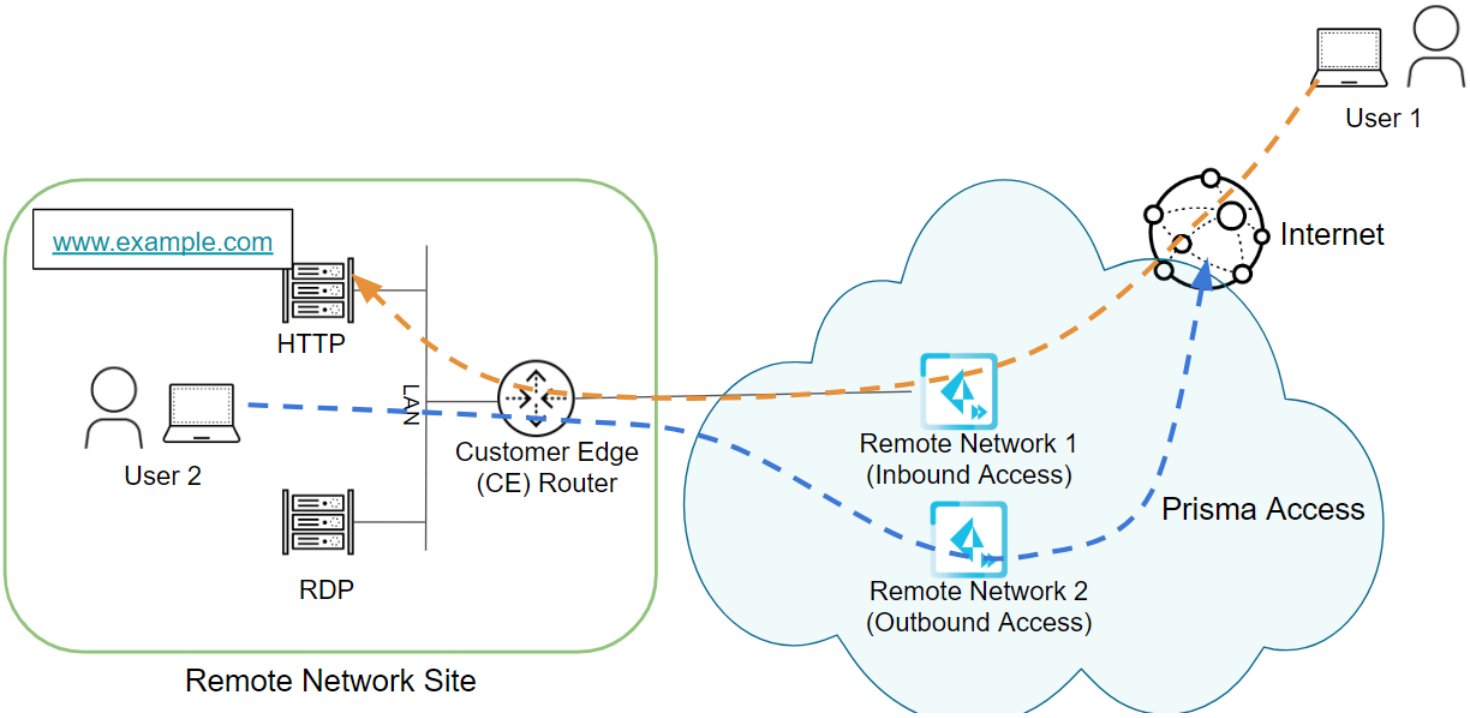
Tipo de protección contra inundaciones	Tasa de alarmas en CPS	Activar tasa en CPS
Congestión SYN	10000	15000
Congestión ICMP	20	20

Si necesita mayor protección contra inundaciones de nuevas sesiones, póngase en contacto con su equipo de Palo Alto Networks.

- Las redes remotas configuradas para acceso entrante seguro solo se pueden utilizar para ese propósito. Si necesita acceso saliente además de acceso entrante para un sitio de red remoto, cree dos sitios de red remotos en la misma ubicación (uno para acceso entrante y otro para acceso saliente), como se muestra en la siguiente figura. En este ejemplo, el Usuario 1 utiliza la

 ©2025 Palo Alto Networks, Inc.

Red remota 1 para el acceso entrante a www.example.com, mientras que el Usuario 2 utiliza la Red remota 2 para el acceso saliente a Internet desde la ubicación de red remota.



- Si tiene una implementación personalizada de Prisma Access en la que se excluye uno de los proveedores de la nube, es posible que no se admita el acceso entrante; en este caso, no puede elegir la ubicación durante la incorporación de la red remota.
- El acceso entrante seguro no es compatible con las licencias de evaluación.

Configurar acceso entrante seguro para sitios de red remotos

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access que incluye Interconexión de red para acceso sitio a sitio y usuario a sitio

Su implementación podría incorporar ancho de banda por ubicación de cómputo o por ubicación; cualquiera de los métodos es compatible para configurar el acceso entrante de red remoto. Cuando configura el acceso entrante para una red remota que asigna ancho de banda por ubicación de cómputo, especifique el ancho de banda según cada ubicación. Para crear una red remota que permita un acceso entrante seguro, complete uno de los siguientes flujos de trabajo:

- Para configurar el acceso entrante seguro para una implementación de red remota que asigna ancho de banda por ubicación de cómputo, complete este flujo de trabajo.
- Para configurar el acceso entrante seguro para una implementación de red remota que asigna ancho de banda por ubicación, complete este flujo de trabajo.

©2025 Palo Alto Networks, Inc.

Configurar el acceso entrante seguro para redes remotas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licencia de Prisma Access que incluye Interconexión de red para acceso de sitio a sitio y de usuario a sitio

Para hacer que las aplicaciones accesibles por internet estén disponibles desde un sitio de red remoto, primero haga una lista de las aplicaciones a las que desea proporcionar acceso y asigne una IP privada, un número de puerto y una combinación de protocolo para cada aplicación. Si utiliza la misma dirección IP para varias aplicaciones, la combinación de puerto/protocolo debe ser única para cada aplicación; si utiliza la misma combinación de puerto/protocolo para varias aplicaciones, cada dirección IP debe ser única.

Para comenzar la configuración, seleccione cuántas direcciones IP públicas desea asociar para las aplicaciones. Puede especificar ya sea 5 o 10 direcciones IP públicas por sitio de red remoto. Cada asignación de IP pública toma ancho de banda (unidades) de su licencia de Redes Remotas, además del ancho de banda que haya asignado para la ubicación de cómputo asociada a la red remota. 5 direcciones IP toman 150 Mbps de la asignación de licencias de red remota y 10 direcciones IP requieren 300 Mbps.

Después de elegir el número de direcciones IP públicas, accede a la aplicación, junto con su combinación asociada de IP privada, número de puerto y protocolo, para la que desea acceso seguro entrante.

Puede decidir cómo quiere asignar su aplicación a las direcciones IP públicas. De forma predeterminada, Prisma Access asigna las direcciones IP públicas a las aplicaciones que especifique, y se pueden asignar varias aplicaciones a una sola dirección IP. Si necesita asignar una sola aplicación a una sola dirección IP pública, puede seleccionar **Dedicated IP (IP dedicada)** durante la configuración del sistema. Puede configurar hasta 100 aplicaciones entrantes para cada grupo de direcciones IP públicas aprovisionadas (5 o 10).

- Strata Cloud Manager
- Panorama

Configurar el acceso entrante seguro para redes remotas (Strata Cloud Manager)

A continuación, se explica cómo hacer que una aplicación sea accesible desde un sitio de red remoto para todos los usuarios conectados a Internet (no solo usuarios de Prisma Access).

STEP 1 | Si aún no lo ha hecho, revise las directrices de red remota de acceso entrante.

STEP 2 | Reúna los detalles de la solicitud que necesitará para comenzar.

Haga una lista de las aplicaciones a las que desea proporcionar acceso y asigne una IP privada, un número de puerto y una combinación de protocolo para cada aplicación. Si utiliza la misma dirección IP para varias aplicaciones, la combinación de puerto/protocolo debe ser única para cada aplicación; si utiliza la misma combinación de puerto/protocolo para varias aplicaciones, cada dirección IP debe ser única.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | En Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)** > **Inbound Access (Acceso entrante)** > **Add Inbound Access (Añadir acceso entrante)**.

STEP 4 | Introduzca los datos necesarios.

Elija el **Number of Public IPs (Número de direcciones IP públicas)** que desea usar para las aplicaciones, ya sea cinco o diez.

Cada asignación de IP pública toma ancho de banda de su licencia de redes remotas, además del coste de la licencia para la red remota. 5 direcciones IP toman 150 MB de la asignación de licencias de red remota y 10 direcciones IP requieren 300 MB.

De Prisma Access versión 4.1, si tiene un recurso que se encuentra en un sitio de red remoto que tiene habilitado el acceso entrante y desea que los usuarios de sitios de acceso no entrante tengan acceso a ese recurso, puede **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Permitir flujos entrantes a otras redes remotas a través de la red troncal de Prisma Access)** al configurar la red remota de acceso no entrante.

A partir de la versión 5.0 de Prisma Access, puede permitir flujos entrantes a otras redes remotas a través de la red troncal del proveedor de servicios (SP) cuando configure la red remota de acceso no entrante.

La interconexión SP es compatible solo con lo siguiente:

- *Regiones de PGC*
- *Nuevas implementaciones de Prisma Access*
- *Tráfico de salida de proxy explícito*

STEP 5 | Añada las **Inbound Access Applications (Aplicaciones de acceso entrante)** para los que desea proteger el acceso.

Añada la combinación de IP privada / número de puerto / protocolo asociada para la aplicación.

STEP 6 | Decida cómo desea asignar las aplicaciones a las direcciones IP públicas.

De forma predeterminada, Prisma Access asigna las direcciones IP públicas a las aplicaciones que especifique, y se pueden asignar varias aplicaciones a una sola dirección IP. Si necesita asignar una sola aplicación a una sola dirección IP pública, puede **Assign Dedicated IP (Asignar IP dedicada)** durante la configuración del sistema. Puede configurar hasta 100 aplicaciones entrantes para cada grupo de direcciones IP públicas aprovisionadas (5 o 10).

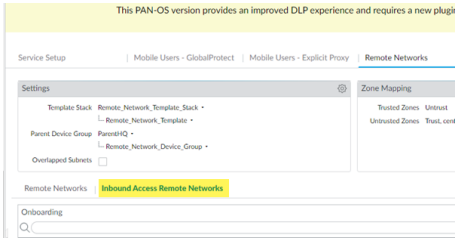
STEP 7 | Termine de configurar la red remota de acceso entrante como lo haría con un sitio de red remota normal.

Configurar el acceso entrante seguro para redes remotas (Panorama)

Si tiene una implementación de Prisma Access que asigna ancho de banda de red remota por ubicación de cómputo, configure el acceso entrante completando los pasos a continuación.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y seleccione **Inbound Access Remote Networks (Redes remotas de acceso entrante)**.



STEP 2 | **Add (Añadir)** una red remota para el acceso entrante.

STEP 3 | Especifique la configuración de la conexión de red remota de acceso entrante.

1. Introduzca un **Name (Nombre)** para la conexión de acceso entrante.
2. Introduzca un **Known (Conocido)**.

   El acceso entrante admite un subconjunto de ubicaciones.
3. Especifique un **Bandwidth (Ancho de banda)** para usar en la conexión de acceso entrante.

   El ancho de banda se asigna para las conexiones de acceso entrante por ubicación.
4. Especifique el **Number of Public IPs (Número de direcciones IP públicas)** para usar en la conexión de acceso entrante.

   Especifique 5 o 10 direcciones IP públicas. Cada asignación de IP pública toma ancho de banda (unidades) de su licencia de Redes Remotas, además del ancho de banda que haya asignado para la ubicación de cómputo asociada a la red remota.
5. Seleccione el túnel IPSec que se utilizará con la conexión de acceso entrante.
6. Seleccione si desea o no **Allow inbound flows to other Remote Networks over the Prisma Access Backbone (Permitir flujos de entrada a otras redes remotas a través de la red troncal de Prisma Access)**.

   Si tiene un recurso que se encuentra en un sitio de red remoto que tiene habilitado el acceso entrante y desea que los usuarios de sitios de acceso no entrante tengan acceso a ese recurso, puede **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Permitir flujos entrantes a otras redes remotas a través de la red troncal de Prisma Access)** al configurar la red remota de acceso no entrante. Si permite flujos de entrada desde otras redes remotas, debe habilitar NAT de origen.
7. (Opcional) Si tiene un enlace WAN secundario en esta ubicación, seleccione **Enable Secondary WAN (Habilitar WAN secundaria)** y proporcione un **IPSec Tunnel (Túnel IPSec)** que es diferente al túnel IPSec primario.

STEP 4 | Configure **Static Routes (Rutas estáticas)**, **BGP** y **QoS** para su implementación.

Esta configuración es la misma que la de una conexión de red remota de acceso no entrante.

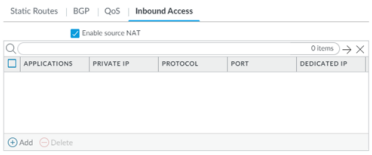
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Haga clic en el botón **Inbound Access (Acceso entrante)** para configurar las opciones de acceso entrante.

1. (Opcional) Para deshabilitar la NAT de origen, anule la selección **Enable Source NAT (Habilitar NAT de origen)**.

   De forma predeterminada, NAT de origen está habilitada. Si el dispositivo compatible con IPSec en su sitio de red remoto es capaz de realizar un retorno simétrico (como un cortafuegos de nueva generación de Palo Alto Networks), o si no ha seleccionado **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Permitir flujos de entrada a otras redes remotas a través de la red troncal de Prisma Access)**, anule la selección **Enable source NAT (Habilitar NAT de origen)**.

   *Usted debe **Enable source NAT (Habilitar NAT de origen)** en la pestaña **Inbound Access (Acceso entrante)** si selecciona esta casilla de verificación. La NAT de origen es un requisito para permitir flujos de entrada a otras redes remotas.*

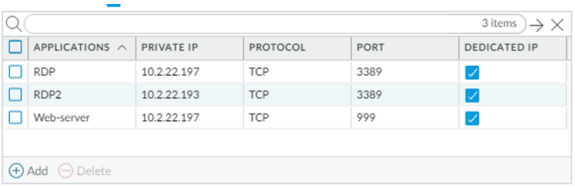
   

2. **Add (Añadir)** las aplicaciones para proporcionar acceso entrante seguro.

   Puede configurar hasta 100 aplicaciones entrantes para cada grupo de direcciones IP públicas aprovisionadas (5 o 10). Introduzca a una combinación única de dirección de **Private IP (IP privada)**, **Protocol (Protocolo)** y **Port (Puerto)** para cada aplicación. Es aceptable utilizar direcciones IP privadas y puertos duplicados para dos aplicaciones, siempre y cuando seleccione **TCP** para una aplicación y **UDP** para otra aplicación.

   Introduzca los siguientes valores.

   - Especifique el nombre de la **Application (Aplicación)**.
   - Especifique la dirección de **Private IP (IP privada)** que se utilizará con esta aplicación.
   - Especifique el parámetro **Protocol (Protocolo)** para usar con la aplicación (**TCP** o **UDP**).
   - Especifique el **Port (Puerto)** a usar con la aplicación.
   - Elija si desea dedicar una sola dirección IP pública a una sola aplicación; para ello, seleccione **Dedicated IP (IP dedicada)**.

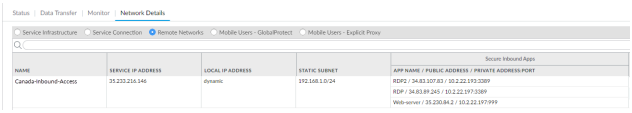
STEP 6 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 7 | **Save (Guardar)** y **Commit (Enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Espere aproximadamente 30 minutos para que Prisma Access genere las direcciones IP públicas; a continuación, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** y tome nota de la **Public Address (Dirección pública)** que se asocia con el **App Name (Nombre de la aplicación)** para la aplicación que ha creado.

Si seleccionó **Dedicated IP (IP dedicada)**, busque la aplicación única que está asociada con la **Public Address (Dirección pública)**.

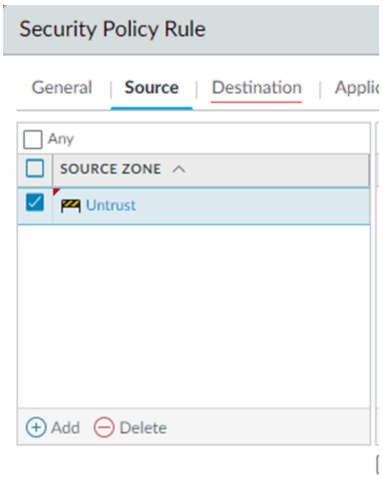


STEP 9 | Cree políticas de seguridad para permitir el tráfico de los usuarios entrantes de Internet.

Porque la política de seguridad predeterminada de Prisma Access solo permite el tráfico de desconfianza-a-desconfianza, debe configurar políticas de seguridad para permitir el tráfico de desconfianza-a-confianza para sus aplicaciones de acceso entrante. Palo Alto Networks recomienda que limite el tipo de acceso que permite a las aplicaciones que entran. Los siguientes ejemplos proporcionan acceso a servidores SSH, portales web y servidores RDP.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego haga clic en **Add (Añadir)** para añadir una política.

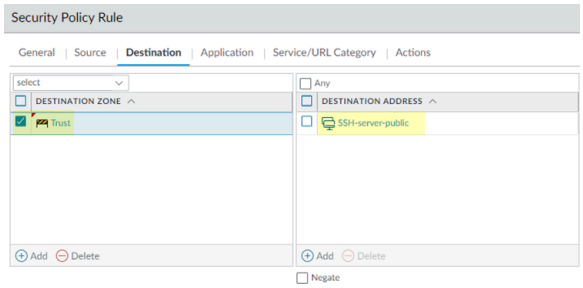
   Asegúrese de crear esta política en el grupo de dispositivos **Remote_Network_Device_Group**.
2. Seleccione el tráfico de **Source (Origen)** como **Untrust (No fiable)**.



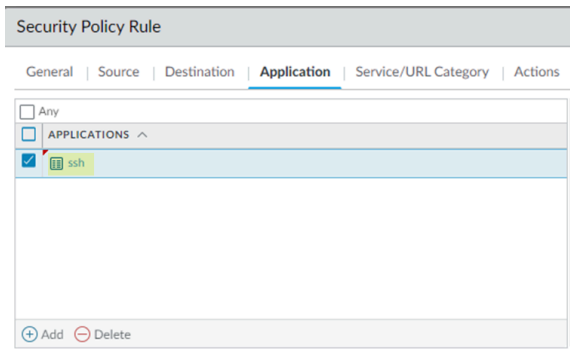
3. Cree una política para permitir el tráfico del servidor SSH seleccionando la opción **Destination Zone (Zona de destino)** para el tráfico de destino como **Trust (Confianza)** y especificando una **Destination Address (Dirección de destino)** de **SSH-server-public**. Se

 ©2025 Palo Alto Networks, Inc.

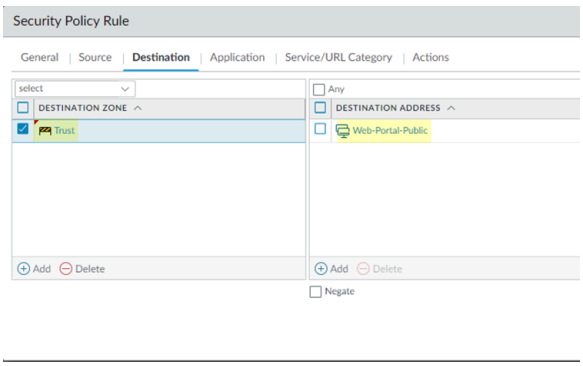
trata de un Objeto de dirección o grupo de direcciones que ha creado que tiene una lista de todas las direcciones IP públicas que se utilizan para el inicio de sesión SSH.



4. Seleccione una **Application (Aplicación)** de **ssh**.

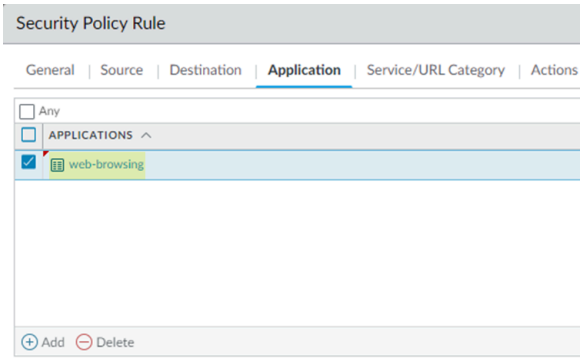


5. Seleccione una **Service/URL Category (Categoría de servicio/URL)** de **application-default** para permitir o denegar aplicaciones basadas solo en sus puertos predeterminados, según lo definido por Palo Alto Networks.
6. En **Actions (Acciones)**, seleccione **Allow (Permitir)**.
7. Haga clic en **OK (Aceptar)** para guardar la política.
8. Cree una política para permitir el acceso al portal web mediante la creación de una política en los pasos anteriores, pero sustituyendo la siguiente configuración en las pestañas **Destination (Destino)** y **Application (Aplicación)**:
   - Seleccione una **Destination Address (Dirección de destino)** de una dirección o grupo de direcciones de **Web-Portal-Public (Portal-Web-Público)**, que contiene todas las direcciones IP públicas del portal web.



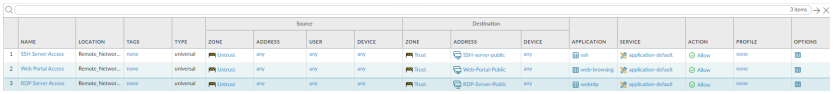
 ©2025 Palo Alto Networks, Inc.

- Seleccione una **Application (Aplicación)** de **web-browsing (navegación web)**.



9. Cree una política de seguridad para el acceso al servidor RDP, utilizando la misma configuración que para las otras políticas, pero creando un objeto Address (Dirección) o Address Group (Grupo de direcciones) llamado **RDP-Server-Public**, que contiene las direcciones IP públicas del servidor RDP, como la **Destination Address (Dirección de destino)** y **WebRDP** como la **Application (Aplicación)**.

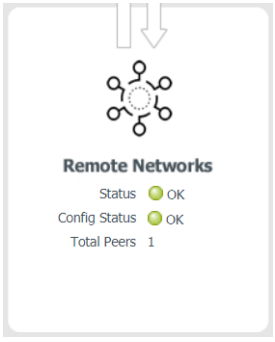
   Una vez completado, tiene tres políticas diferentes para permitir el acceso al servidor SSH, el acceso al portal web y el acceso al servidor RDP.



STEP 10 | **Save (Guardar)** y **Commit (Enviar)** sus cambios.

STEP 11 | Compruebe que la conexión de red remota esté operativa y procese correctamente el tráfico entrante.

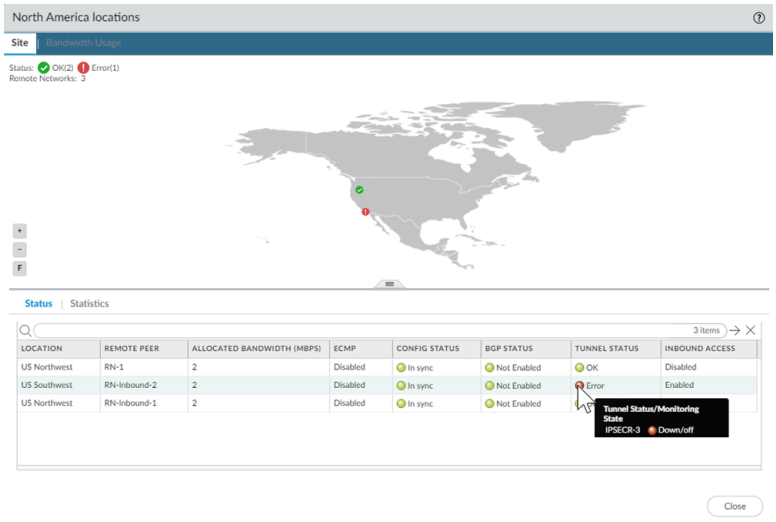
1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > > **Status (Estado)** > **Remote Networks (Redes remotas)** y coloque el cursor sobre las áreas **Status (Estado)** y **Config Status (Estado de configuración)** para ver el estado del túnel.



2. Si encuentra problemas, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > > **Monitor (Supervisar)** > **Remote Networks (Redes remotas)**,

 ©2025 Palo Alto Networks, Inc.

seleccione la ubicación del túnel de red remoto en el mapa y coloque el cursor sobre el **Tunnel Status (Estado del túnel)** para determinar la causa del error.



Configurar el acceso entrante seguro para sitios de red remotos para ubicaciones que asignan ancho de banda por ubicación

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access que incluye Interconexión de red para acceso de sitio a sitio y de usuario a sitio

Si tiene una implementación de Prisma Access que asigna ancho de banda de red remota por ubicación, configure el acceso entrante completando los siguientes pasos.

STEP 1 | Select **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks**, **Add** a connection, and configure the remote network, including routing and IPSec tunnel options.

Consulte Redes remotas de Prisma Access para obtener más detalles. Su implementación puede incorporar ancho de banda por ubicación de cómputo o por ubicación; cualquiera de los métodos es compatible para el acceso entrante.

Asegúrese de seleccionar una de las ubicaciones admitidas para el Acceso entrante.

©2025 Palo Alto Networks, Inc.

STEP 2 | Haga clic en la pestaña **Inbound Access (Acceso entrante)** para configurar las opciones de acceso entrante.

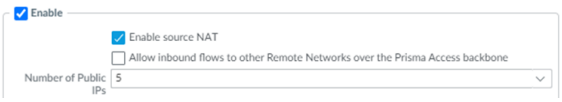
1. Seleccione **Enable (Habilitar)** para habilitar el acceso entrante a la red remota.

   Si seleccionó una ubicación que no es compatible con el acceso entrante, Prisma Access le solicita que seleccione uno compatible.

2. (Opcional) Para deshabilitar la NAT de origen, anule la selección **Enable Source NAT (Habilitar NAT de origen)**.

   De forma predeterminada, NAT de origen está habilitada. Si el dispositivo compatible con IPSec en su sitio de red remoto es capaz de realizar un retorno simétrico (como un cortafuegos de nueva generación de Palo Alto Networks), o si no ha seleccionado **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Permitir flujos de entrada a otras redes remotas a través de la red troncal de Prisma Access)**, anule la selección **Enable source NAT (Habilitar NAT de origen)**.

   *Usted debe **Enable source NAT (Habilitar NAT de origen)** en la pestaña **Inbound Access (Acceso entrante)** si selecciona esta casilla de verificación. La NAT de origen es un requisito para permitir flujos de entrada a otras redes remotas.*

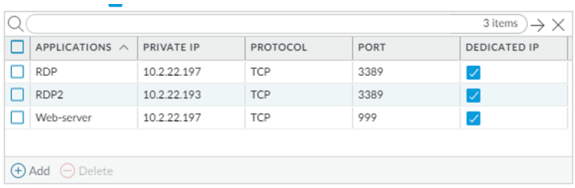


STEP 3 | **Add (Añadir)** las aplicaciones para proporcionar acceso entrante seguro.

Puede configurar hasta 100 aplicaciones entrantes para cada grupo de direcciones IP públicas aprovisionadas (5 o 10). Introduzca a una combinación única de dirección de **Private IP (IP privada)**, **Protocol (Protocolo)** y **Port (Puerto)** para cada aplicación. Es aceptable utilizar direcciones IP privadas y puertos duplicados para dos aplicaciones, siempre y cuando seleccione **TCP** para una aplicación y **UDP** para otra aplicación.

Introduzca los siguientes valores.

- Especifique el nombre de la **Application (Aplicación)**.
- Especifique la dirección de **Private IP (IP privada)** que se utilizará con esta aplicación.
- Especifique el parámetro **Protocol (Protocolo)** para usar con la aplicación (**TCP** o **UDP**).
- Especifique el **Port (Puerto)** a usar con la aplicación.
- Elija si desea dedicar una sola dirección IP pública a una sola aplicación; para ello, seleccione **Dedicated IP (IP dedicada)**.



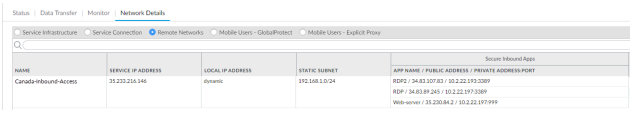
STEP 4 | Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | **Save (Guardar)** y **Commit (Enviar)** sus cambios.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Espere aproximadamente 30 minutos para que Prisma Access genere las direcciones IP públicas; a continuación, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** y tome nota de la **Public Address (Dirección pública)** que se asocia con el **App Name (Nombre de la aplicación)** para la aplicación que ha creado.

Si seleccionó **Dedicated IP (IP dedicada)**, busque la aplicación única que está asociada con la **Public Address (Dirección pública)**.

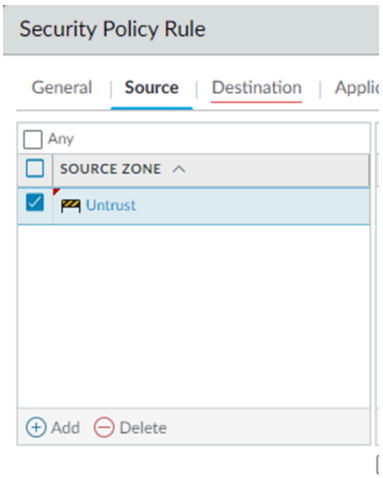


STEP 7 | Cree políticas de seguridad para permitir el tráfico de los usuarios entrantes de Internet.

Porque la política de seguridad predeterminada de Prisma Access solo permite el tráfico de desconfianza-a-desconfianza, debe configurar políticas de seguridad para permitir el tráfico de desconfianza-a-confianza para sus aplicaciones de acceso entrante. Palo Alto Networks recomienda que limite el tipo de acceso que permite a las aplicaciones que entran. Los siguientes ejemplos proporcionan acceso a servidores SSH, portales web y servidores RDP.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego haga clic en **Add (Añadir)** para añadir una política.

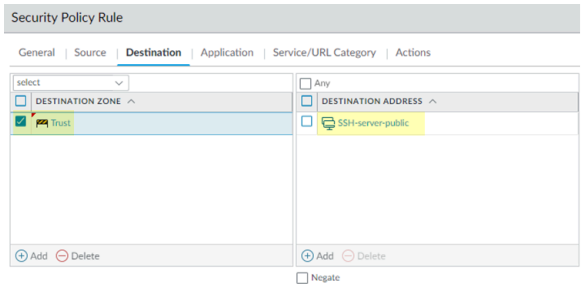
   Asegúrese de crear esta política en el grupo de dispositivos **Remote_Network_Device_Group**.
2. Seleccione el tráfico de **Source (Origen)** como **Untrust (No fiable)**.



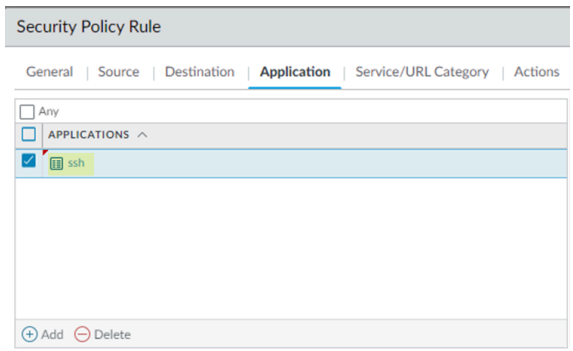
3. Cree una política para permitir el tráfico del servidor SSH seleccionando la opción **Destination Zone (Zona de destino)** para el tráfico de destino como **Trust (Confianza)** y especificando una **Destination Address (Dirección de destino)** de **SSH-server-public**. Se

 ©2025 Palo Alto Networks, Inc.

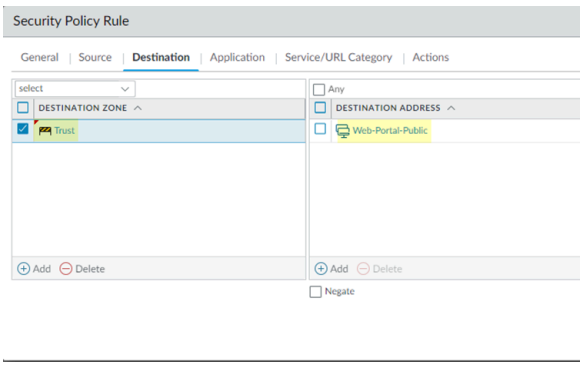
trata de un Objeto de dirección o grupo de direcciones que ha creado que tiene una lista de todas las direcciones IP públicas que se utilizan para el inicio de sesión SSH.



4. Seleccione una **Application (Aplicación)** de **ssh**.

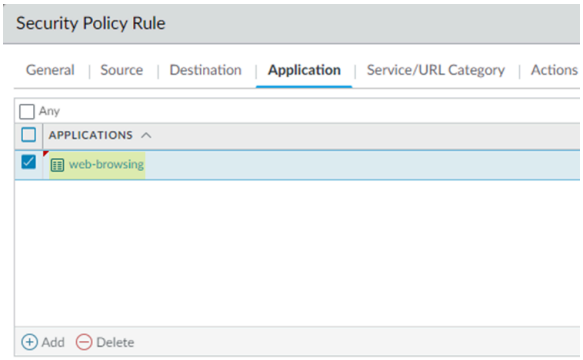


5. Seleccione una **Service/URL Category (Categoría de servicio/URL)** de **application-default** para permitir o denegar aplicaciones basadas solo en sus puertos predeterminados, según lo definido por Palo Alto Networks.
6. En **Actions (Acciones)**, seleccione **Allow (Permitir)**.
7. Haga clic en **OK (Aceptar)** para guardar la política.
8. Cree una política para permitir el acceso al portal web mediante la creación de una política en los pasos anteriores, pero sustituyendo la siguiente configuración en las pestañas **Destination (Destino)** y **Application (Aplicación)**:
   - Seleccione una **Destination Address (Dirección de destino)** de una dirección o grupo de direcciones de **Web-Portal-Public (Portal-Web-Público)**, que contiene todas las direcciones IP públicas del portal web.



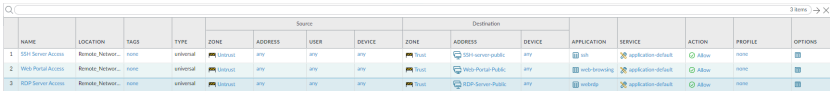
 ©2025 Palo Alto Networks, Inc.

- Seleccione una **Application (Aplicación)** de **web-browsing (navegación web)**.



9. Cree una política de seguridad para el acceso al servidor RDP, utilizando la misma configuración que para las otras políticas, pero creando un objeto Address (Dirección) o Address Group (Grupo de direcciones) llamado **RDP-Server-Public**, que contiene las direcciones IP públicas del servidor RDP, como la **Destination Address (Dirección de destino)** y **WebRDP** como la **Application (Aplicación)**.

   Una vez completado, tiene tres políticas diferentes para permitir el acceso al servidor SSH, el acceso al portal web y el acceso al servidor RDP.



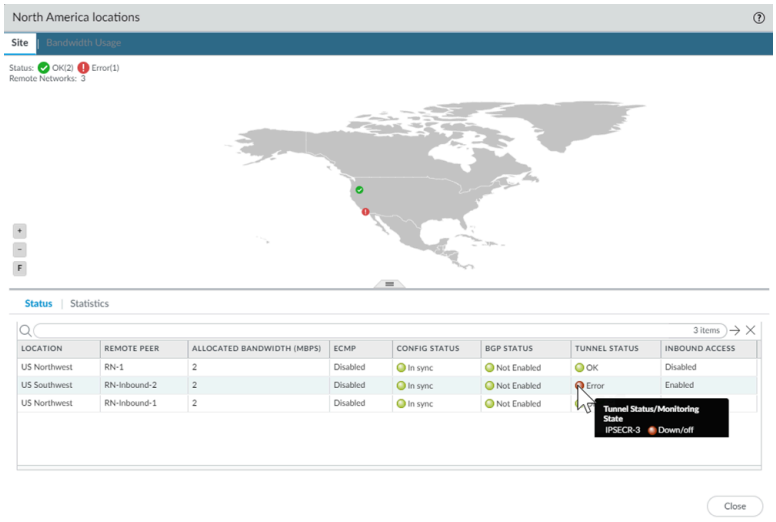
STEP 8 | **Save (Guardar)** y **Commit (Enviar)** sus cambios.

STEP 9 | Compruebe que la conexión de red remota esté operativa y procese correctamente el tráfico entrante.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > > **Status (Estado)** > **Remote Networks (Redes remotas)** y coloque el cursor sobre las áreas **Status (Estado)** y **Config Status (Estado de configuración)** para ver el estado del túnel.
2. Si encuentra problemas, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > > **Monitor (Supervisar)** > **Remote Networks (Redes remotas)**,

 ©2025 Palo Alto Networks, Inc.

seleccione la ubicación del túnel de red remoto en el mapa y coloque el cursor sobre el **Tunnel Status (Estado del túnel)** para determinar la causa del error.



Crear una red de gran ancho de banda para un sitio remoto

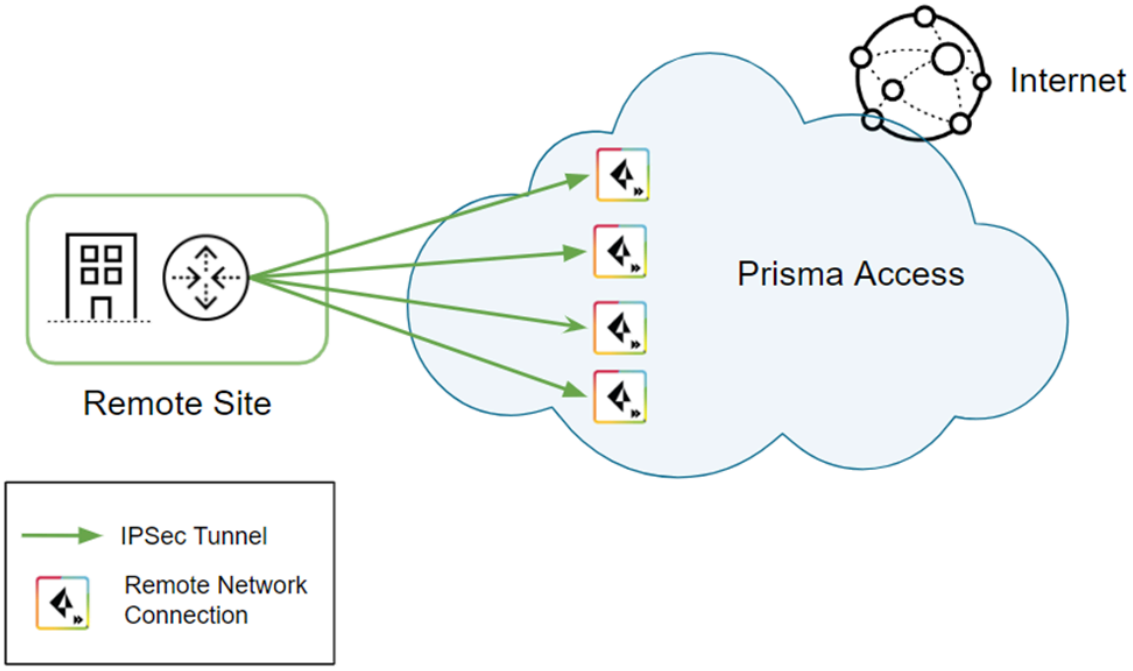
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Si desea proteger su sucursal o sitio para el acceso saliente a Internet con una conexión de alto ancho de banda a Prisma Access, puede equilibrar la carga del tráfico desde su sucursal o sitio utilizando varios túneles IPSec completando los pasos de esta sección.

El siguiente diagrama muestra cuatro conexiones de red remotas que utilizan el mismo sitio remoto. Antes de la incorporación, asigne 4 Gbps (4000 Mbps) a la ubicación de procesamiento, que en este ejemplo es Corea del Sur y corresponde al sitio remoto. 4000 Mbps proporciona cuatro nodos de terminación IPSec y cada nodo de terminación IPSec proporciona un máximo de 1000 Mbps de ancho de banda. Asigne a cada conexión de red remota su propio nodo de terminación IPSec durante el proceso de incorporación para utilizar el ancho de banda completo.

Este ejemplo muestra cuatro túneles. El número máximo de túneles que puede utilizar para una conexión de alto ancho de banda en Prisma Access se basa en el número máximo de túneles IPSec que admite el equipo local de su cliente (CPE) con el protocolo de equilibrio de carga que utiliza.

 ©2025 Palo Alto Networks, Inc.



Tenga en cuenta las siguientes restricciones y recomendaciones antes de implementar esta configuración:

- Utilice enrutamiento BGP para los túneles IPSec; no se admite el enrutamiento estático.
- Utilice esta configuración únicamente para acceso a Internet saliente.
- No utilice la supervisión de túneles en Prisma Access o en el CPE. La disponibilidad del túnel IPSec está determinada por el intercambio de tráfico BGP entre el CPE y la red remota de Prisma Access. Si un túnel IPSec deja de funcionar y se interrumpe la conexión BGP, las rutas conocidas a través de BGP en ese túnel se eliminan automáticamente del ECMP.
- Dado que utiliza BGP para determinar cuándo se cae un túnel, tenga en cuenta el valor HoldTime que ha configurado en su CPE. El temporizador de retención determina la cantidad de tiempo que el túnel estará inactivo antes de eliminar la ruta. Prisma Access utiliza el valor BGP HoldTime predeterminado de 90 segundos según lo define RFC 4271. Si configura un tiempo de retención más bajo para el CPE en BGP en el sitio de red remoto, BGP utiliza el valor de tiempo de retención más bajo. Palo Alto Networks recomienda un valor KeepAlive de 10 segundos y un valor HoldTime de 30 segundos para su CPE con esta implementación.

Para crear una conexión de red remota de alto ancho de banda, complete la siguiente tarea.

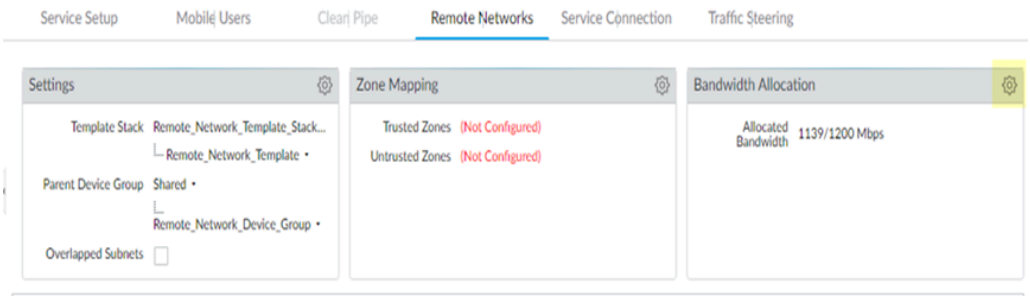
 ©2025 Palo Alto Networks, Inc.

STEP 1 | En Panorama, configure los túneles de red remota de Prisma Access.

1. (Opcional) Si aún no lo ha hecho, configure perfiles de puertas de enlace IKE, cifrado IKE y cifrado IPSec, y túneles IPSec para las conexiones de red remotas que cree.

   Tome nota de los perfiles criptográficos IKE e IPSec; especifique las mismas configuraciones en el CPE que utiliza para finalizar la conexión de red remota en la ubicación de red remota.
2. Determine el tipo de implementación de red remota que tiene.

   Las implementaciones de Prisma Access asignan ancho de banda mediante la asignación de ancho de banda por ubicación de cómputo o mediante la asignación de ancho de banda por ubicación.
3. Incorporar la red remota.
   - Para incorporar la red remota que asigna ancho de banda por ubicación de cómputo:
     1. Asigne ancho de banda a las ubicaciones que desea incorporar haciendo clic en el icono de engranaje en el área **Bandwidth Allocation (Asignación de ancho de banda)**.



     2. Introduzca la **Bandwidth Allocation (Asignación de ancho de banda)** que desea para cada **Compute Location (Ubicación de cómputo)** asociada con

 ©2025 Palo Alto Networks, Inc.

las **Prisma Access Locations (Ubicaciones de Prisma Access)** a las que desea incorporarse.

3. Espere a que el ancho de banda se refleje en el campo **Allocated Total (Total asignado)** en la parte superior de la página; luego, haga clic en **OK (Aceptar)**.

- Para incorporar la red remota que asigna el ancho de banda por ubicación, vaya al siguiente paso; asigne ancho de banda durante la incorporación de la red remota.

4. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)** y cree cuatro conexiones de redes remotas, especificando la siguiente configuración:

   - Seleccione la misma **Location (Ubicación)** para cada conexión.
   - Seleccione el **IPSec Termination Node (Nodo de terminación IPSec)**.

     Seleccione un nodo de terminación IPSec independiente para cada conexión de red remota.

     *Si tiene una implementación que asigna ancho de banda por ubicación, seleccione un **Bandwidth (Ancho de banda)** de **500 Mbps**.*

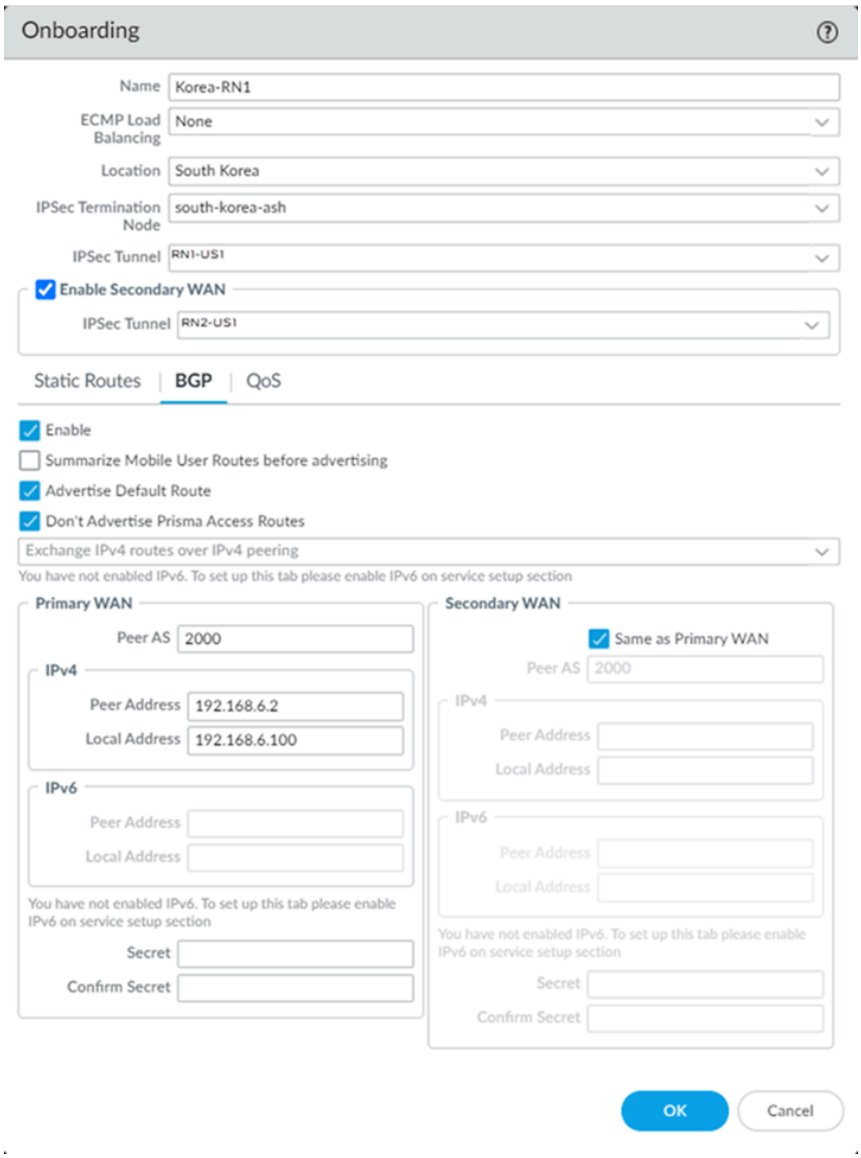
     El ancho de banda que seleccione no puede exceder la cantidad total de ancho de banda que tiene licencia. Utilice este ajuste para definir la cantidad de ancho de banda total con licencia que desea asignar a esta ubicación.
   - **Enable (Habilitar)** BGP, **Advertise Default Route (Anunciar ruta predeterminada)** y **Don't Advertise Prisma Access Routes (No anunciar rutas de Prisma Access)**.
   - Especifique el mismo **AS Peer (Peer de AS)** para todas las conexiones de red remotas.

     Este ejemplo muestra un **Peer AS (AS de Peer)** de 2000; en este ejemplo, se selecciona un **Peer AS (AS de Peer)** de 2000 para las cuatro conexiones.
   - (Opcional) si desea crear una red remota de respaldo, cree una seleccionando **Enable Secondary WAN (Habilitar WAN secundaria)**; luego, seleccione el **IPSec Tunnel (Túnel IPSec)** que creó para el túnel de respaldo.

   La configuración de una WAN secundaria no se admite en las siguientes implementaciones:

   - Si su WAN secundaria está configurada en modo activo-activo con el túnel IPSec primario.
   - Si el equipo de las instalaciones del cliente (CPE) está configurado en una configuración de enrutamiento multipath de igual coste (ECMP) con el túnel IPSec primario y secundario.

 ©2025 Palo Alto Networks, Inc.

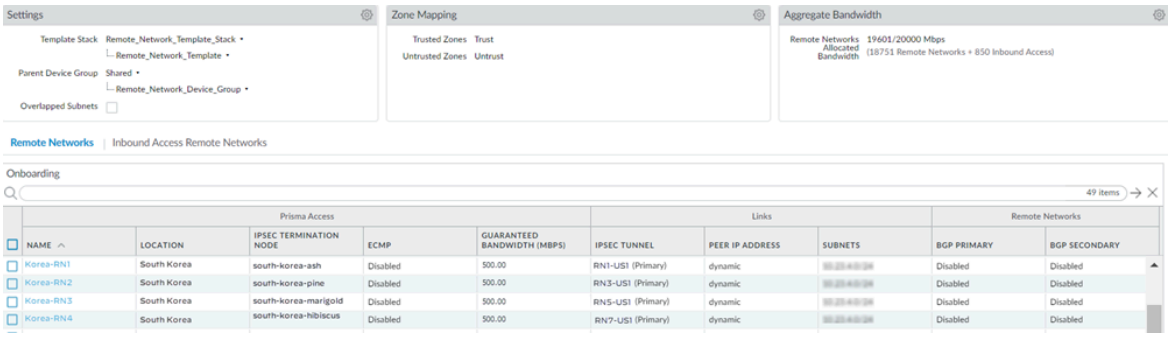


Cuando se complete, tendrá cuatro conexiones de red remotas de 1000 Mbps para la misma ubicación.

Dado que las implementaciones que asignan ancho de banda por ubicación tienen un ancho de banda máximo de 500 Mbps, esta configuración le proporcionará 500 Mbps para cada ubicación.

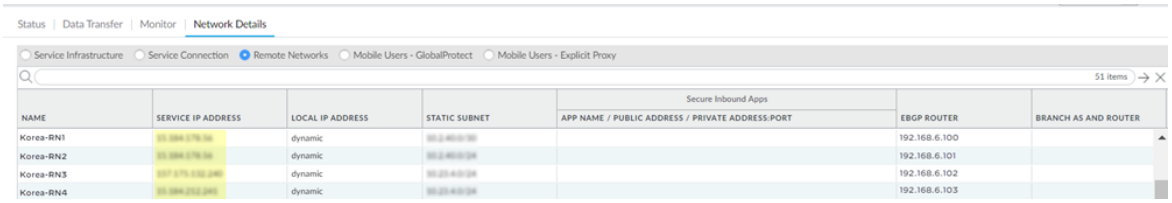
Si configuró túneles de respaldo, también tendrá cuatro túneles secundarios que se utilizarán para fines de conmutación por error.

 ©2025 Palo Alto Networks, Inc.



5. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado) (Estado)** > **Network Details (Detalles de la red)** > **Remote Networks (Redes remotas)** y tome nota de las direcciones de **Service IP Address (Dirección IP del servicio)** y **EBGP Router (Enrutador EBGP)**.

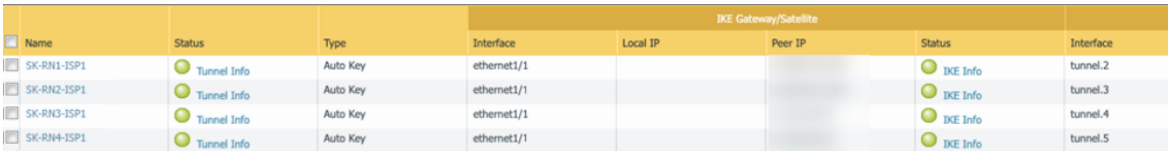
   Utiliza la **Service IP Address (Dirección IP del servicio)** como el dirección IP del peer cuando configura el túnel IPSec en el CPE en el sitio de red remoto, y utiliza estas direcciones y las direcciones del **EBGP Router (Enrutador EBGP)** cuando crea rutas estáticas en el CPE.



STEP 2 | En el CPE del sitio de red remota, configure los túneles de red remota.

- *La configuración en estos pasos utiliza cortafuegos de nueva generación de Palo Alto Networks; puede utilizar cualquier dispositivo CPE que admita túneles IPSec y ECMP para esta implementación.*
- *El equilibrio del ancho de banda depende del hash CPE para ECMP. Sin embargo, Prisma Access garantiza el retorno simétrico del tráfico.*

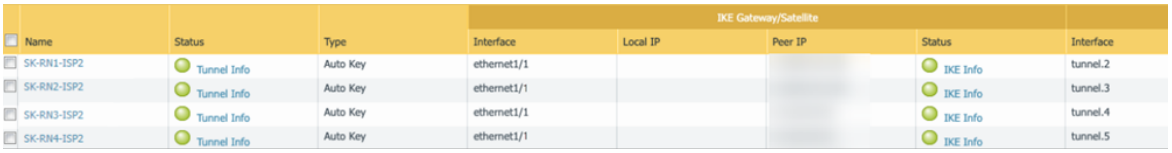
1. Cree cuatro túneles activos desde el CPE activo a cada una de las cuatro conexiones de red. Para la dirección **Peer IP (IP del peer)**, introduzca la **Service IP Address (Dirección IP del servicio)** de la red remota que recibió de Prisma Access en un paso anterior.



2. (Opcional) Si crea túneles de respaldo, créelos desde el CPE activo a cada una de las cuatro conexiones de red. Para la dirección de **Peer IP (IP del peer)**, introduzca la **Service**

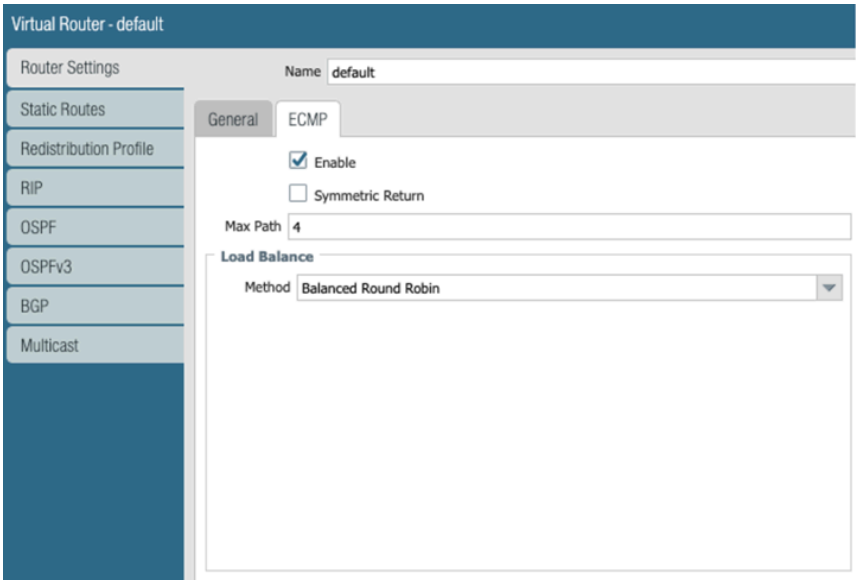
 ©2025 Palo Alto Networks, Inc.

IP Address (Dirección IP del servicio) de la red remota que recibió de Prisma Access en un paso anterior.



STEP 3 | Configure ECMP en el CPE en el sitio de red remoto.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. Seleccione el enrutador virtual **default (predeterminado)** o **Add (Añadir)** para añadir un nuevo enrutador virtual.
3. Seleccione **Router Settings (Configuración del enrutador)** > **Enable (Habilitar)** > **ECMP**, luego **Enable (Habilitar)** ECMP con una **Max Path (Ruta máxima)** de **4** y un **Method (Método)** de **Balanced Round Robin (Operación por turnos equilibrada)**.



STEP 4 | En el CPE del sitio de red remoto, cree rutas estáticas hacias las direcciones IP de **Service IP Address (Dirección IP del servicio)** y **EBGP Router (Enrutador EBGP)** de Prisma Access que recuperó en un paso anterior.

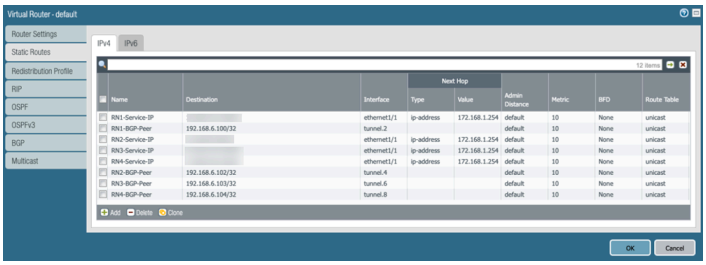
Como se indicó anteriormente, se requiere enrutamiento dinámico con BGP para esta configuración. Para facilitar la conexión BGP entre el CPE y el enrutador eBGP de Prisma Access, debe añadir una ruta estática para la dirección IP del enrutador eBGP en el CPE, y el

 ©2025 Palo Alto Networks, Inc.

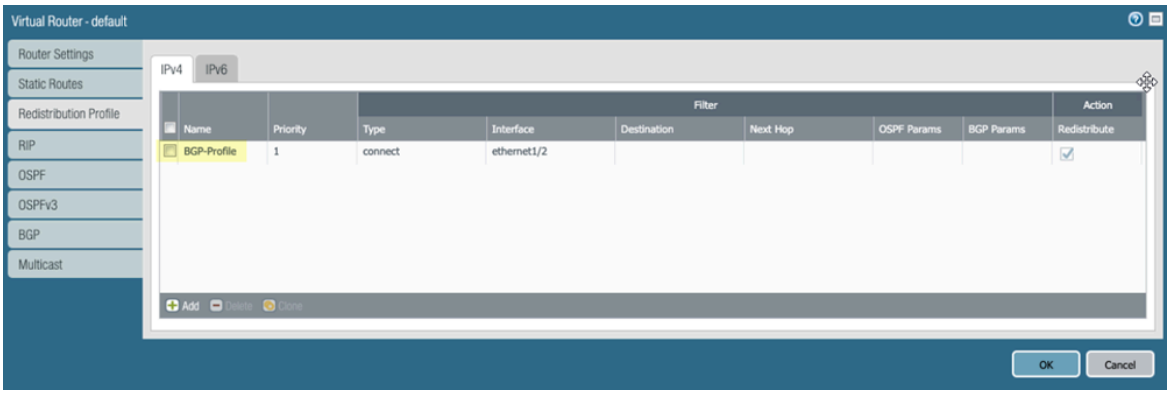
siguiente salto debe ser la interfaz de túnel en el CPE. Debe repetir este paso para todas las demás direcciones IP del enrutador eBGP de red remota en los túneles restantes.

El siguiente ejemplo muestra la ruta en el CPE activo. Si creó túneles de respaldo en un CPE en espera, cree la misma ruta en el CPE en espera.

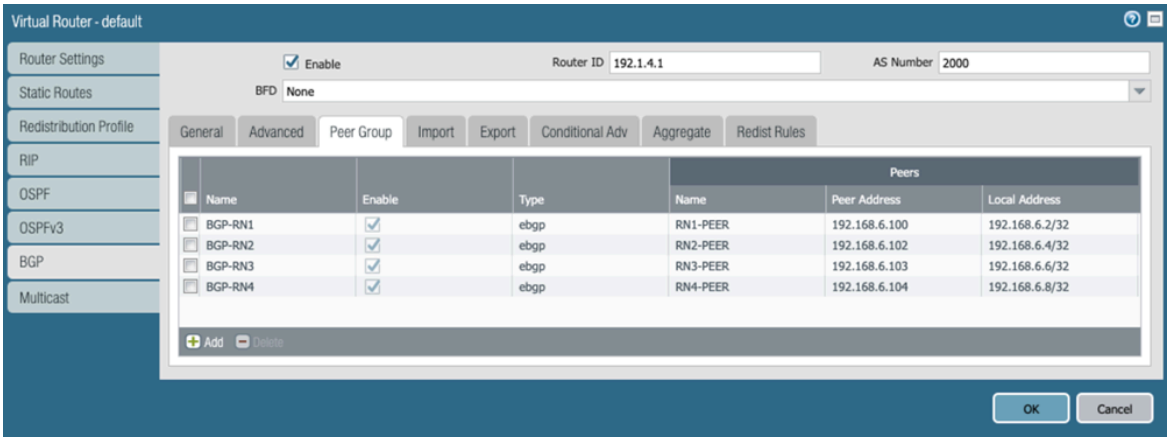
Si está configurando un cortafuegos de nueva generación de Palo Alto Networks, seleccione **Static Routes (Rutas estáticas)** > **IPv4** para añadir las rutas estáticas.



STEP 5 | Habilite la redistribución de ruta en el CPE seleccionando **Redistribution Profile (Perfil de redistribución)** > **IPv4** y luego **Add (Añadir)** un perfil de redistribución de ruta IPv4.

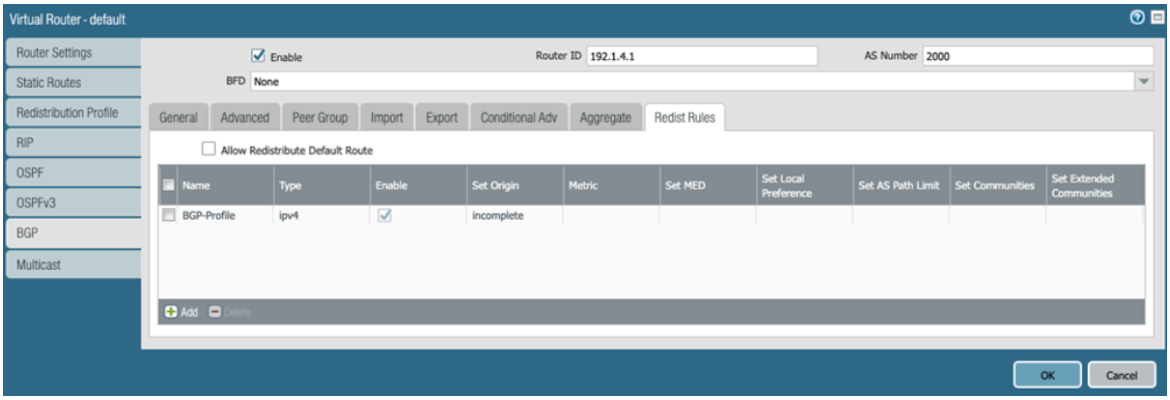


STEP 6 | Seleccione **BGP** > **Peer Group (Grupo de peers)**, **Enable (Habilitar)** BGP en la instancia del enrutador virtual y luego **Add (añadir)** peers BGP de la red remota.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Seleccione **BGP** > **Redist Rules (Reglas de redistribución)** y luego adjunte el perfil de redistribución de ruta que creó en un paso anterior.

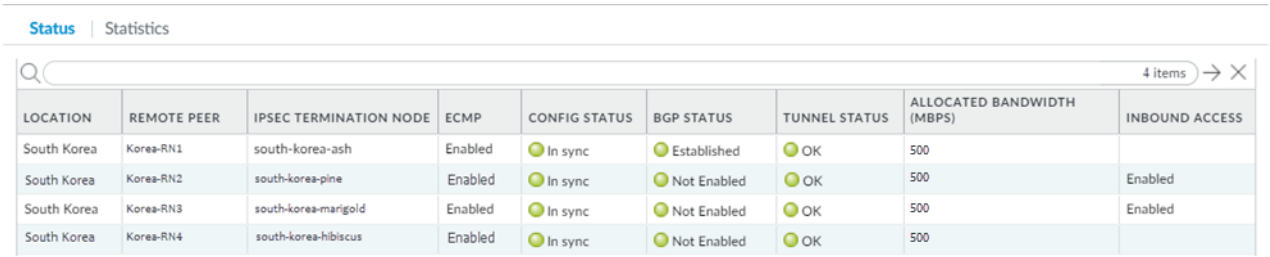


STEP 8 | Valide que el CPE esté pasando tráfico por sus cuatro túneles.

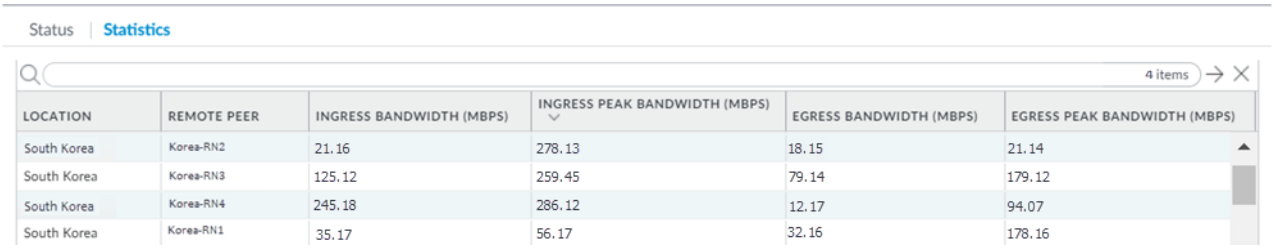
STEP 9 | Verifique el estado de las conexiones habilitadas para ECMP desde Prisma Access.

- Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Monitor (Supervisar)** > **Remote Networks (Redes remotas)**, seleccione la región donde implementó las conexiones ECMP y luego seleccione **Status (Estado)**.

  - *En esta área, **ECMP** se muestra como **No.** Esto está previsto porque no está configurando la función de equilibrio de carga ECMP de Prisma Access.*
  - *El ECMP es direccional desde CPE a Prisma Access y Prisma Access garantiza el retorno simétrico del tráfico desde el CPE.*



- Seleccione **Statistics (Estadísticas)** para ver qué tráfico pasa a través de cada túnel de red remota.



Cuando haya completado este flujo de trabajo, habrá creado una configuración de alto ancho de banda para la red remota. Tenga en cuenta que esta solución solo es compatible con el tráfico saliente.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Prisma Access para Clean Pipe

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Use *Prisma Access para Clean Pipe* para configurar de forma rápida y sencilla varias instancias de conexiones a Internet salientes limpias.

Esto no es compatible con Prisma Access (Managed by Strata Cloud Manager).

Descripción general de Prisma Access para Clean Pipe

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Para permitir que las organizaciones que gestionan la infraestructura de TI de otras organizaciones, como proveedores de servicios, MSSP o empresas de telecomunicaciones, protejan de manera rápida y sencilla el tráfico de Internet saliente para sus inquilinos, Palo Alto Networks ofrece Prisma Access para Clean Pipe. Un proveedor de servicios, MSSP, o Telco puede enrutar a sus clientes (configurados como inquilinos) a Prisma Access para Clean Pipe mediante una interconexión de socios. Una vez que el tráfico cruza la interconexión de socios, se enviará a una instancia de Clean Pipe dedicada al inquilino por motivos de seguridad y luego se enrutará a Internet.

Prisma Access para Clean Pipe también proporciona una API que puede usar para crear Clean Pipes de manera rápida y sencilla para sus inquilinos.

Casos de uso de Clean Pipe

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Utilice Prisma Access para Clean Pipe si cumple con todos los siguientes casos de uso:

- Gestiona una implementación de red con una gran cantidad de inquilinos.

  Por ejemplo, usted es un proveedor de servicios, una empresa de telecomunicaciones o un MSSP que administra y mantiene las redes de muchas organizaciones diferentes (hasta decenas de miles).
- Desea una forma para que cada inquilino en su implementación tenga protegido su tráfico de Internet saliente.
- Necesita una forma rápida y escalable de incorporar Clean Pipes para las organizaciones cuyas redes administra.
- Con excepción de la seguridad de internet saliente, no tiene requisitos adicionales para proteger a los usuarios móviles, las sedes centrales o las sucursales de las redes que administra.

  Si tiene requisitos de seguridad adicionales, le recomendamos crear varios inquilinos en Prisma Access en lugar de implementar Clean Pipe, que le permite crear y aplicar perfiles de seguridad para grupos separados de redes remotas y usuarios móviles.

 ©2025 Palo Alto Networks, Inc.

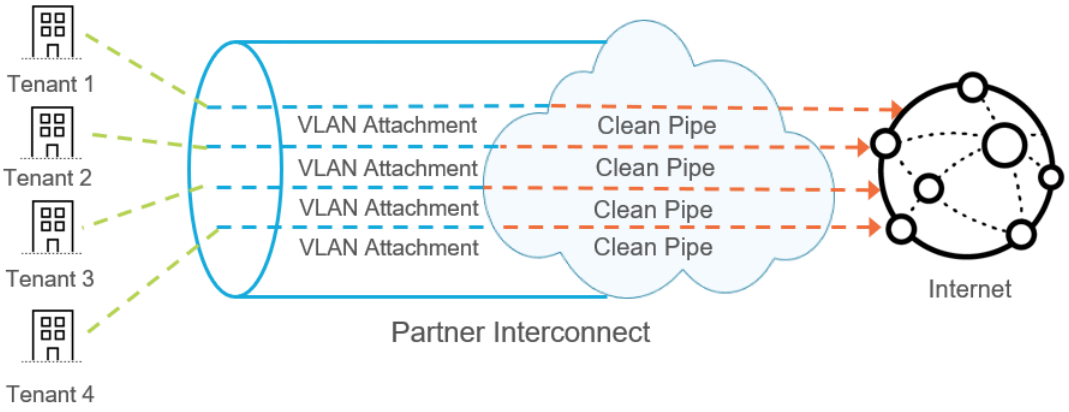
Ejemplos de Clean Pipe

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

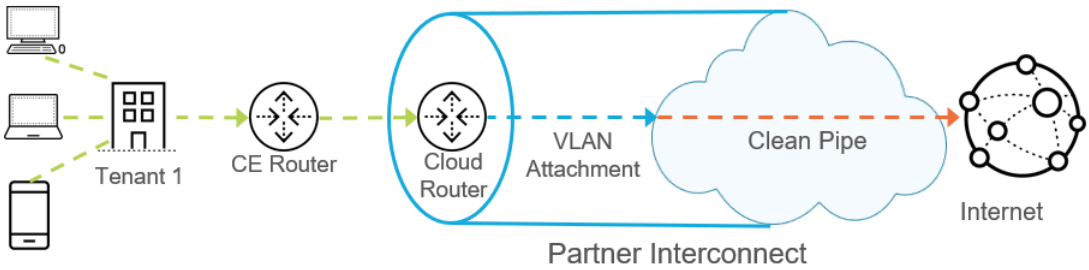
La siguiente figura proporciona un ejemplo de Clean Pipes configurada para un solo inquilino, con múltiples Clean Pipes configuradas para el inquilino.

En este ejemplo, el proveedor de servicios gestiona la conectividad a Internet de cuatro organizaciones y desea proteger el acceso a Internet saliente para ellas. El proveedor de servicios crea una interconexión de socios de Google Cloud Platform (GCP) y crea un archivo adjunto de VLAN para cada inquilino. El proveedor de servicios configura Prisma Access para Clean Pipe mediante Panorama para crear seguridad para el archivo adjunto de VLAN.

Este ejemplo muestra una sola Clean Pipe por inquilino. También puede crear varias Clean Pipe en un solo inquilino. Asegúrese de que cada Clean Pipe que especifique para un inquilino use una ubicación diferente.



La siguiente figura muestra una única Clean Pipe en más detalle para un inquilino que desea una conexión limpia a Internet. El enrutador Customer Edge (CE) proporciona conectividad WAN para el inquilino. El enrutador CE se conecta a un enrutador en la nube, y el enrutador en la nube proporciona conectividad para la interconexión de socios. El proveedor de servicios crea un archivo adjunto de VLAN para el inquilino y configura Prisma Access para Clean Pipe en Panorama, para proporcionar seguridad al archivo adjunto de VLAN que protege el tráfico basado en Internet del inquilino.



 ©2025 Palo Alto Networks, Inc.

Requisitos de interconexión de Clean Pipe y socios

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia de Prisma Access

Antes de empezar, tenga en cuenta los siguientes requisitos de implementación de Clean Pipe y tenga en cuenta las siguientes diferencias entre Prisma Access para Clean Pipe y otras implementaciones de Prisma Access:

- Debe tener un Prisma Access para la licencia de Clean Pipe.

  El Prisma Access para la licencia Clean Pipe es una licencia separada de otros productos Prisma Access. Sin embargo, los mismos requisitos para comprar e instalar Panorama y las licencias de Strata Logging Service se aplican a Clean Pipe.
- Prisma Access para Clean Pipe tiene los siguientes requisitos de interconexión de socios de GCP:
  - Debe poder crear una interconexión de socio en GCP.
  - Debes tener la capacidad de crear adjuntos de VLAN en GCP.
  - Para las interconexiones de socios de Capa 2 (L2), debe tener acceso al enrutador perimetral del cliente (CE) en el lado MSSP y poder realizar cambios de configuración en él.

  Para obtener más información sobre la configuración de GCP, consulte la documentación de GCP.
- Tenga en cuenta los requisitos mínimos de ancho de banda para la implementación de Clean Pipe.

  La licencia mínima que puede comprar es de 1000 Mbps. La asignación mínima de ancho de banda para cada inquilino de Clean Pipe es de 100 Mbps.

  Después de crear un inquilino, puede crear clean pipes en ese inquilino. Cada Clean Pipe debe tener un mínimo de 100 Mbps. Cada Clean Pipe comparte los dominios de acceso, las plantillas, la pila de plantillas y el grupo de dispositivos del inquilino.
- Si va a configurar varias Clean Pipe para un solo inquilino, se requiere que cada Clean Pipe sea una ubicación única. Si desea configurar dos adjuntos de VLAN para una sola ubicación de Clean Pipe en una configuración activa/de respaldo para la redundancia dentro de la zona, especifique la opción **REDUNDANT (REDUNDANTE)** al añadir una nueva instancia de Clean Pipe.
- Al crear una conexión dentro de un inquilino de Clean Pipe, haga coincidir la asignación de ancho de banda con la del adjunto de VLAN. No cree un adjunto de VLAN que tenga un ancho de banda mayor o menor que el ancho de banda de la conexión.
- Después de habilitar la multitenencia, no configure la implementación de Clean Pipe con ninguna de las otras pestañas del área Configuración, con la excepción del enlace **Generate API key (Generar clave de API)** en la pestaña **Service Setup (Configuración del servicio)**, que le permite generar una clave API para recuperar direcciones IP de Clean Pipe. Toda la configuración es única para Prisma Access para Clean Pipe y separada de otras implementaciones dePrisma Access, como Prisma Access para redes o Prisma Access para los usuarios.

 ©2025 Palo Alto Networks, Inc.

- No realice cambios en una configuración de Clean Pipe después de confirmarla. Si cambia una Clean Pipe después de que se haya confirmado, recibirá un error de confirmación cuando la vuelva a confirmar. En su lugar, elimine la tubería limpia existente y añada una nueva. Programe este cambio durante una ventana de tiempo de inactividad del sistema. Si ya ha realizado cambios y aún no se han confirmado, puede revertir los cambios editando la configuración de Clean Pipe a sus valores anteriores.
- Tenga en cuenta que las ubicaciones utilizadas por Clean Pipe difieren de otras implementaciones de Prisma Access. Prisma Access para Clean Pipe admite las siguientes ubicaciones:
  - asia-oriente1
  - asia-oriente2
  - asia-noreste1
  - asia-sur1
  - asia-sudeste1
  - australia-sureste1
  - europa-norte1
  - europa-oeste2
  - europa-oeste3
  - europa-oeste4
  - américa del norte-noreste1
  - américa del sur-este1
  - us-central1
  - ee. uu.-este1
  - ee. uu.-este4
  - ee. uu.-oeste1
  - ee. uu.-oeste2
- Tenga en cuenta las siguientes restricciones de red para Clean Pipe:
  - QoS para Clean Pipe solo se admite en la entrada (de Internet a la dirección de Clean Pipe).
  - User-ID no es compatible
  - Clean Pipe admite la afinidad de sesión en función de las direcciones IP de origen y destino y no se puede configurar.
  - Las políticas de confianza a confianza no son válidas para Clean Pipe, ya que el tráfico siempre está orientado a Internet. Utilice únicamente políticas de confianza a desconfianza.

 ©2025 Palo Alto Networks, Inc.

Completar la configuración de Clean Pipe

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Para completar la configuración de Prisma Access para Clean Pipe, realice la configuración en la Interconexión de socios y en Panorama.

Asegúrese de que puede acceder y configurar los enrutadores CE y en la nube en el lado de la interconexión de socios (acceso no principal) de la interconexión de socios.

STEP 1 | En el lado Interconexión de socios de la configuración, cree un archivo adjunto de VLAN utilizando la **Pairing Key (Clave de emparejamiento)** que ha recuperado de Panorama.

Para obtener más información acerca de la creación de archivos adjuntos de VLAN con Partner Interconnects y la configuración de enrutadores de borde de cliente (CE) para comunicarse con enrutadores en la nube, consulte la documentación de Google Cloud en https://cloud.google.com/interconnect/docs/

Asegúrese de que la ubicación y el ancho de banda que seleccione coincidan con la **Location (Ubicación)** que especificó en Panorama. El proveedor de servicios que utiliza para la interconexión de socios utiliza la clave de emparejamiento, junto con la ubicación y la capacidad de conexión solicitadas, para completar la configuración de su adjunto de VLAN.

STEP 2 | Después de que aparezca la conexión, vuelva a Panorama, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Network Details (Detalles de la red)** > **Clean Pipe** y tome nota de las direcciones **MSSP CE** y **Cloud Router IP (IP de enrutador en la nube)**.

Estos valores se rellenan después de introducir la **Pairing Key (Clave de emparejamiento)** en el otro lado del archivo adjunto de VLAN.



STEP 3 | Inicie sesión en el enrutador CE y realice la siguiente configuración.

1. Introduzca la dirección **CE MSSP** como dirección IP local.
2. Introduzca la dirección de **Cloud Router IP (IP del enrutador en la nube)** como la dirección IP del peer.
3. Introduzca un ASN BGP que coincida con el **BGP Peer ASN (ASN de par BGP)** que ingresó cuando configuró la Clean Pipe en Panorama.

   Asegúrese de introducir estos valores correctamente; no puede cambiarlos.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Compruebe el estado de Clean Pipe.

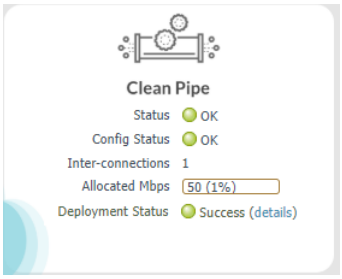
1. En Panorama, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)**, seleccione el **Tenant (inquilino)** del menú desplegable y compruebe el **Status (Estado)** de Clean Pipe.

   Consulte la lista de ubicaciones de Prisma Access para valores aceptables.

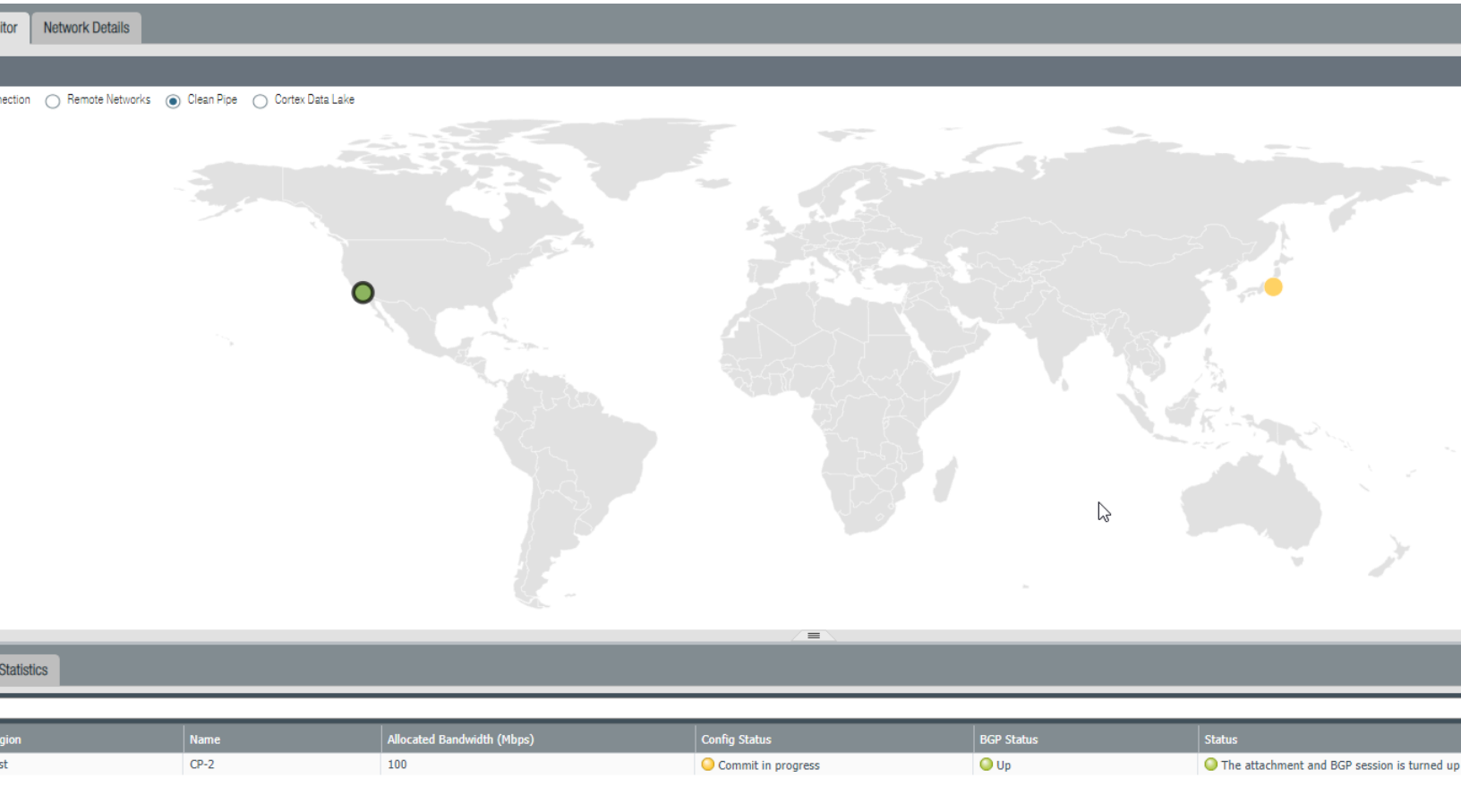
   El área de **Deployment Status (Estado de implementación)** le permite ver el progreso de los trabajos de incorporación y implementación antes de que se completen, así como

 ©2025 Palo Alto Networks, Inc.

ver más información sobre el estado de los trabajos completados. Consulte el progreso y estado de la implementación para obtener más detalles.



2. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Clean Pipe** y haga clic en la pestaña **Monitor (Supervisar)** para ver un mapa con el estado de las Clean Pipes implementadas.



Haga clic en las pestañas debajo del mapa para ver estadísticas adicionales para Clean Pipes.

Pestaña **Status (Estado)**:

- **Compute Region (Región de cómputo)**: la región de cómputo donde se implementa su infraestructura de servicios en la nube para la instancia de Clean Pipe.
- **Name (Nombre)**: el nombre de la instancia de clean pipe.
- **Allocated Bandwidth (Mbps) [Ancho de banda asignado (Mbps)]**: cantidad de ancho de banda asignado para la instancia de clean pipe.

 ©2025 Palo Alto Networks, Inc.

- **Config Status (Estado de configuración)**: el estado de su último envío de configuración al servicio. Si ha realizado un cambio localmente y aún no ha enviado la configuración a la nube, el estado se muestra **Out of sync (Fuera de sincronización)**. Pase el cursor sobre el indicador de estado para obtener información más detallada. Después de enviar y empujar la configuración a Prisma Access, el estado de configuración cambia a **In sync (En sincronización)**.
- **BGP Status (Estado de BGP)**: muestra información sobre el estado de BGP entre el cortafuegos o enrutador en la instancia de clean pipe y Prisma Access. Aunque es posible que vea pasar temporalmente el estado a través de los diversos estados de BGP [**idle (inactivo)**, **active (activo)**, **open send (abrir envío)**, **open pend (abrir pendiente)**, **open confirm (abrir confirmación)**], lo más común es que el estado de BGP muestre:
  - **Connect (Conectar)**: el enrutador en la instancia de clean pipe está tratando de establecer la relación de peers de BGP con el cortafuegos en la nube.
  - **Established (Establecido)**: se ha establecido la relación entre pares BGP.

    Este campo también mostrará si la conexión BGP está en un estado de error:
  - **Advertencia**: no se ha actualizado el estado del BGP en más de ocho minutos. Esto puede indicar un corte en el cortafuegos.

 ©2025 Palo Alto Networks, Inc.

  - **Error**: se desconoce el estado de BGP.
- **Status (Estado)**: estado operativo de la conexión entre Prisma Access y la instancia de clean pipe.

Pestaña **Statistics (Estadísticas)**

- **Region (Región)**: la región donde se implementa su infraestructura de servicios en la nube para la instancia de clean pipe.
- **Name (Nombre)**: el nombre de la instancia de clean pipe.
- **Allocated Bandwidth (Mbps) [Ancho de banda asignado (Mbps)]**: la cantidad de ancho de banda que asignó para la ubicación de red remota.
- **QoS**: seleccione **QoS** para mostrar una página que contiene estadísticas gráficas de QoS.
- **Avg Egress Bandwidth 5 Min (Mbps) [Ancho de banda de salida promedio 5 min (Mbps)]**: la cantidad promedio de ancho de banda de salida de clean pipe promediada durante 5 minutos.
- **Avg Egress Bandwidth 60 Min (Mbps) [Ancho de banda de salida promedio 60 min (Mbps)]**: la cantidad promedio de ancho de banda de salida de clean pipe promediada durante 60 minutos.
- **Avg Ingress Bandwidth 5 Min (Mbps) [Ancho de banda de entrada promedio 5 min (Mbps)]**: la cantidad promedio de ancho de banda de entrada de clean pipe promediada durante 5 minutos.
- **Avg Ingress Bandwidth 60 Min (Mbps) [Ancho de banda de entrada promedio 60 min (Mbps)]**: la cantidad promedio de ancho de banda de entrada de clean pipe promediada durante 60 minutos.
- **Egress Peak Bandwidth 1 Hour (Mbps) [Ancho de banda máximo de salida de 1 hora (Mbps)]**: la cantidad de ancho de banda máximo de salida para la instancia de clean pipe para la última hora.
- **Egress Peak Bandwidth 24 Hour (Mbps) [Ancho de banda máximo de salida de 24 horas (Mbps)]**: la cantidad de ancho de banda máximo de salida para la instancia de clean pipe para las últimas 24 horas.
- **Egress Peak Bandwidth 7 Days (Mbps) [Ancho de banda máximo de salida de 7 días (Mbps)]**: la cantidad de ancho de banda máximo de salida para la instancia de clean pipe para los últimos 7 días.
- **Egress Peak Bandwidth 30 Days (Mbps) [Ancho de banda máximo de salida de 30 días (Mbps)]**: la cantidad de ancho de banda máximo de salida para la instancia de clean pipe para los últimos 30 días.
- **Ingress Peak Bandwidth 1 Hour (Mbps) [Ancho de banda máximo de entrada de 1 hora (Mbps)]**: la cantidad de ancho de banda máximo de entrada para la instancia de clean pipe para la última hora.
- **Ingress Peak Bandwidth 24 Hour (Mbps) [Ancho de banda máximo de entrada de 24 horas (Mbps)]**: la cantidad de ancho de banda máximo de entrada para la instancia de clean pipe para las últimas 24 horas.

 ©2025 Palo Alto Networks, Inc.

- **Ingress Peak Bandwidth 7 Days (Mbps) [Ancho de banda máximo de entrada de 7 días (Mbps)]**: la cantidad de ancho de banda máximo de entrada para la instancia de clean pipe para los últimos 7 días.
- **Ingress Peak Bandwidth 30 Days (Mbps) [Ancho de banda máximo de entrada de 30 días (Mbps)]**: la cantidad de ancho de banda máximo de entrada para la instancia de clean pipe para los últimos 30 días.

Habilitar la multitenencia y crear un inquilino

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	• Licencia de Prisma Access

Para comenzar la configuración de Clean Pipe, cree una implementación multiinquilino en Panorama y cree uno o más inquilinos.

STEP 1 | Instalar y activar Prisma Access para Clean Pipe.

Prisma Access para Clean Pipe requiere una licencia separada, y su activación crea pestañas específicas de Clean Pipe en el complemento Cloud Services. El procedimiento que utiliza para instalar Prisma Access para Clean Pipe es el mismo que el procedimiento que se utiliza para activar e instalar una licencia de Prisma Access, incluyendo la instalación del complemento Cloud Services.

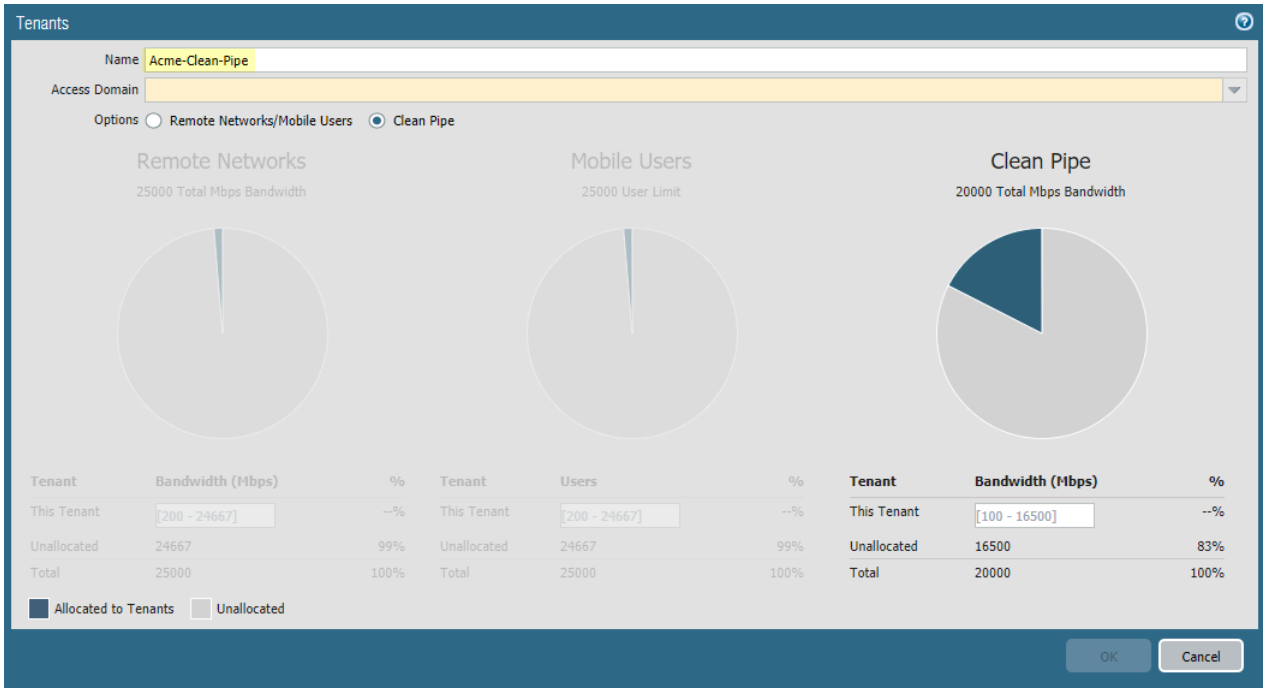
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Habilite la multitenencia si aún no lo ha hecho.

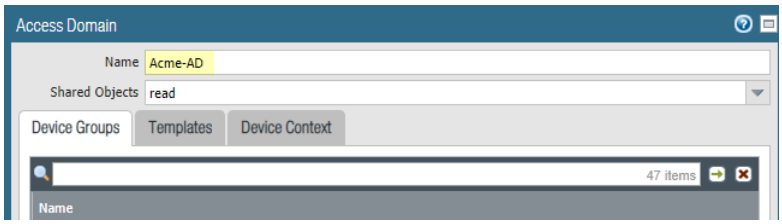
1. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)**.
2. Seleccione **Enable Multitenancy (Habilitar Multitenencia)** (ubicado en la parte superior derecha de la página).
3. Haga clic en **OK (Aceptar)**.

   La página **Tennants (Inquilinos)** se muestra.
4. En el área de **Options (Opciones)**, seleccione **Clean Pipe**.

   Para configurar un inquilino para redes remotas, usuarios móviles o ambos, consulte Gestionar varios inquilinos en Prisma Access.



5. Introduzca un **Name (Nombre)** para el primer inquilino.
6. Cree y configure un nuevo **Access Domain (Dominio de acceso)** para el primer inquilino y haga clic en **OK (Aceptar)**.



7. En el área **Clean Pipe**, introduzca un **Bandwidth (Mbps) [Ancho de banda (Mbps)]** para **This Tenant (Este inquilino)**.

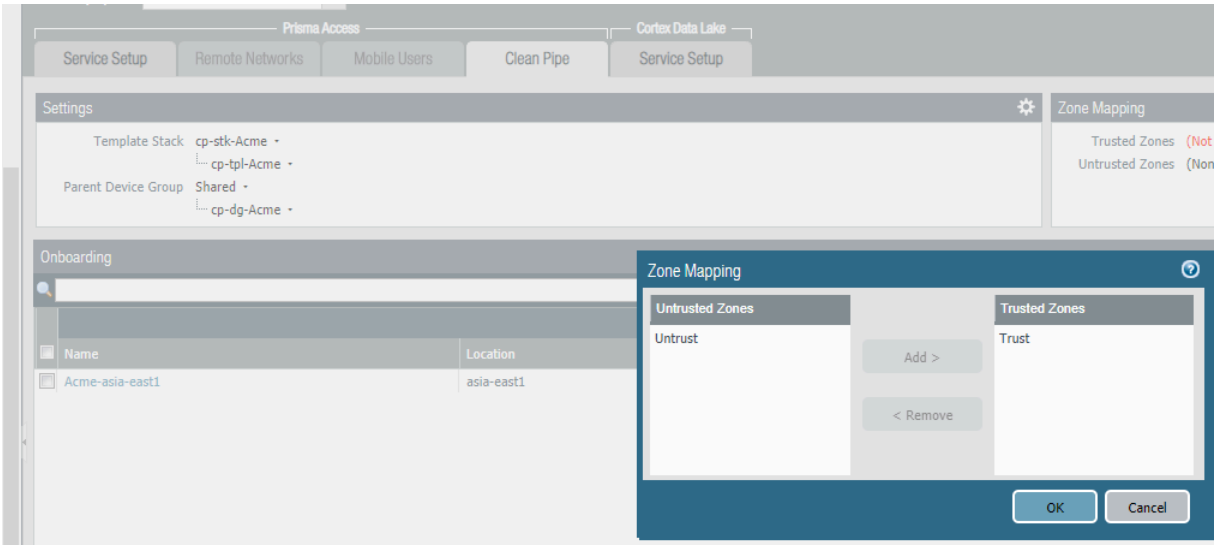
   Introduzca un mínimo de 100 Mbps para cada inquilino que cree.
8. Haga clic en **OK (Aceptar)**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cree zonas para el inquilino y asigne esas zonas para el inquilino.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.

   Asegúrese de haber seleccionado la **Template (Plantilla)** de Clean Pipe para el inquilino que creó (**cp-tpl-***tenant*).
2. Cree zonas para el inquilino (por ejemplo, **Trust (Confianza)** y **Untrust (No confianza)**.
3. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** y seleccione el **Tenant (Inquilino)** de la lista desplegable.
4. Seleccione la pestaña **Clean Pipe**.
5. Haga clic en el icono de engranaje junto a **Zone Mapping (Asignación de zona)** para editar la configuración.
6. Deberá **Add (Añadir)** y **Remove (Eliminar)** las zonas que creó para asignarlas a zonas de confianza y no confianza.



STEP 4 | Incorporar un nuevo Clean Pipe.

1. Seleccione **Panorama (Panorama)** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)**.
2. Deberá **Add (Añadir)** una nueva instancia de Clean Pipe para el inquilino, introduciendo la siguiente información:

   - **Name (Nombre)**: Especifique un nombre para la clean pipe.
   - **Bandwidth (Ancho de banda)**: seleccione el ancho de banda a asignar para clean pipe.

     Puedes incorporar instancias de Clean Pipe en incrementos de 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1000 Mbps, 2000 Mbps, 5000 Mbps y 10000 Mbps. La cantidad de ancho de banda que especifique debe estar dentro de la

 ©2025 Palo Alto Networks, Inc.

asignación de ancho de banda con licencia y debe coincidir con el ancho de banda de la conexión VLAN que cree en la Interconexión de socios.

- **Edge Availability Domain (Dominio de disponibilidad perimetral)**: seleccione el dominio de disponibilidad que desea para clean pipe. Puede elegir **1**, **2**, **CUALQUIERA** o **REDUNDANTE**.
  - Especifique **ANY (CUALQUIERA)** para un implementación de Clean Pipe no redundante.

    Asegúrese de que su proveedor de nube sea compatible con esta opción; también debe seleccionar **ANY (CUALQUIERA)** en el lado del proveedor de nube de la interconexión del socio. Si esa opción no está disponible para su proveedor de nube, elija otra opción.
  - Para especificar dos conexiones VLAN en la misma ubicación en una configuración activa/copia de seguridad en la misma ubicación, seleccione **REDUNDANT (REDUNDANTE)**.

    Prisma Access crea dos claves de emparejamiento para una configuración **REDUNDANT (REDUNDANTE)** (una para cada zona de disponibilidad) y añada el nombre del clean pipe con `zone1` para la primera zona de disponibilidad y `zone2` para la segunda zona de disponibilidad. Por ejemplo, si especifica un **Name**

 ©2025 Palo Alto Networks, Inc.

(Nombre) de **San Francisco**, Prisma Access crea dos zonas llamadas **San Francisco-zona1** y **San Francisco-zona2**.

Asegúrese de que configura la primera zona de disponibilidad (zona1) como la zona principal en su CPE.

También puede construir un par de clean pipes para una redundancia de un solo inquilino en diferentes ubicaciones; para hacerlo, especifique **1** para la primera clean pipe en una ubicación y **2** para la segunda clean pipe en una ubicación diferente.

- **BGP Peer ASN (ASN de par BGP)**: introduzca el número de sistema autónomo (ASN) de BGP.

  Puede especificar un ASN BGP privado o público.

  Tome nota de este valor; lo configura en el enrutador de borde del cliente (CE) cuando complete la configuración de Clean Pipe.
- **Location (Ubicación)**: seleccione la ubicación

  Recomendamos que utilice la misma ubicación que utiliza cuando crea el anexo VLAN para la interconexión del socio.
- Para habilitar QoS, seleccione **QoS**, luego seleccione el perfil de QoS que se utilizará con clean pipe. Formas de QoS de Clean Pipe en la entrada.



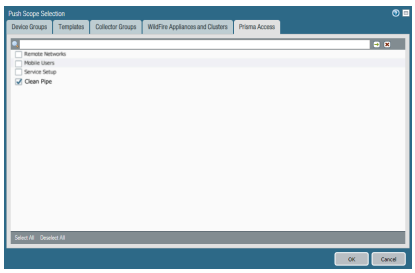
STEP 5 | Añada más instancias de Clean Pipe según sea necesario repitiendo el Paso 4.

Asegúrese de que cada Clean Pipe adicional utilice una ubicación diferente.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Confirme y envíe sus cambios para hacerlos activos en Prisma Access.

1. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y **Edit Selections (Editar selecciones)** en Push Scope.
2. Seleccione **Prisma Access**, luego seleccione **Clean Pipe**.



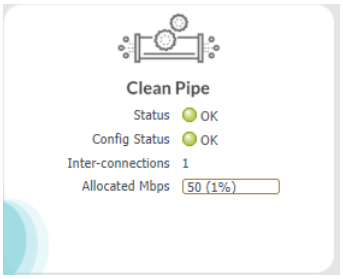
3. Haga clic en **OK (Aceptar)** para guardar los cambios en Push Scope.
4. Haga clic en **Commit (Confirmar)** y **Push (Enviar)** sus cambios.

STEP 7 | Verifique que su Clean Pipe se ha aprovisionado.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)**.
2. Seleccione el **Tenant (Inquilino)** de la lista desplegable en la parte superior de la página.
3. Haga clic en **Status (Estado)**.

   El estado de Clean Pipe se muestra.
4. Pase el ratón sobre el **Config Status (Estado de configuración)** de Clean Pipe y espere hasta que el estado cambie de **Provisioning in Progress (Aprovisionamiento en curso)** a **Provisioned (Aprovisionado)**.

   Este aprovisionamiento puede tardar hasta 30 minutos.



STEP 8 | Haga clic en la pestaña **Network Details (Detalles de la red)**, seleccione el botón de opción **Clean Pipe** y tome nota de la **Pairing Key (Clave de emparejamiento)**.

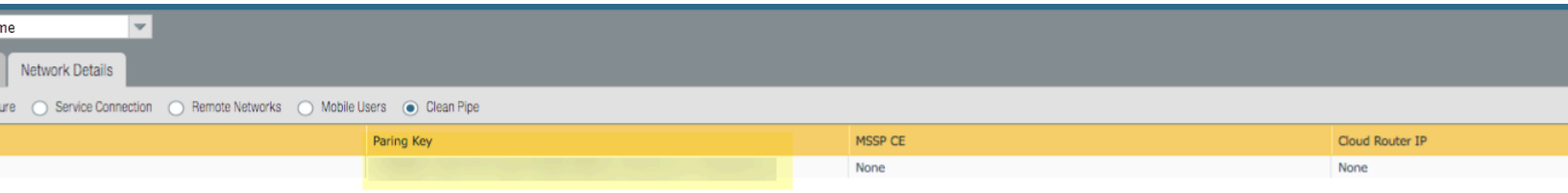
Los campos de **MSSP CE** y de la **Cloud Router IP (IP del enrutador en la nube)** están en blanco cuando comienza a configurar el Clean Pipe. Estos campos se completan después de que cree el Anexo VLAN cuando termina la configuración de Clean Pipe.

Si especificó una conexión **REDUNDANT (REDUNDANTE)**, Prisma Access crea dos claves de emparejamiento, una para cada zona de disponibilidad, y añade el nombre del clean pipe con `zone1` para la primera zona de disponibilidad y `zone2` para la segunda zona de disponibilidad. La siguiente captura de pantalla muestra la clean pipe de **San Francisco** con una configuración

 ©2025 Palo Alto Networks, Inc.

redundante; Prisma Access ha creado dos claves de emparejamiento, una para **SanFrancisco-zone1** y otra para **SanFrancisco-zone2**.

Asegúrese de que configura la primera zona de disponibilidad (zona1) como la zona principal en su CPE.



STEP 9 | Complete la configuración de Clean Pipe.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.