

**TECHDOCS**

# Administración de la VPN IPSec

---

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-support](http://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](http://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page [docs.paloaltonetworks.com/search.html](http://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](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2023-2023 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](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

June 9, 2023

---

# Table of Contents

<b>Conceptos básicos de VPN IPsec.....</b>	<b>5</b>
IPsec VPN.....	6
Modos de túnel IPsec.....	7
Tipos de VPN IPsec.....	8
Túneles VPN IPsec.....	9
Implementaciones de VPN.....	11
Intercambio de claves por red (IKE) para VPN.....	13
Puerta de enlace de IKE.....	13
IKE de fase 1.....	14
IKE de fase 2.....	15
IKEv2.....	17
<b>Comience con IPsec VPN (sitio a sitio).....</b>	<b>23</b>
Descripción general de VPN de sitio a sitio.....	24
Interfaz túnel.....	25
Monitorización de túnel.....	25
ID de proxy para VPN IPsec.....	26
Planifique la configuración de su túnel VPN IPsec.....	29
<b>Configuración de túneles VPN IPsec (sitio a sitio).....</b>	<b>31</b>
Configuración de una puerta de enlace de IKE.....	32
Exportación de un certificado para un peer para acceder usando Hash y URL.....	36
Importación de un certificado para Autenticación de puerta de enlace IKEv2.....	36
Cambio de la duración de la clave o del intervalo de autenticación IKEv2.....	37
Cambio del umbral de activación de cookies para IKEv2.....	38
Configuración de selectores de tráfico IKEv2.....	38
Definición de perfiles criptográficos.....	40
Definición de perfiles criptográficos IKE.....	40
Definición de perfiles criptográficos IPsec.....	41
Configuración de un túnel de IPsec.....	42
Configurar un túnel IPsec (modo túnel).....	42
Configurar un túnel IPsec (modo transporte).....	43
<b>Supervise su túnel VPN IPsec.....</b>	<b>45</b>
Definición de un perfil de supervisión de túnel.....	46
Ver el estado del túnel.....	47
Habilitación, deshabilitación, actualización o reinicio de una puerta de enlace IKE o túnel IPsec.....	50
Habilitación o deshabilitación de una puerta de enlace de IKE o un túnel IPsec.....	50

Actualización o reinicio de una puerta de enlace IKE o túnel IPSec.....	50
<b>Ejemplos de configuración de VPN de sitio a sitio.....</b>	<b>53</b>
VPN de sitio a sitio con rutas estáticas.....	54
VPN de sitio a sitio con OSPF.....	59
VPN de sitio a sitio con rutas estáticas y enrutamiento dinámico.....	66
<b>Solución de problemas.....</b>	<b>73</b>
Solucionar problemas de conexión de túnel VPN IPSec.....	74
Prueba de conectividad VPN.....	74
Interpretación de mensajes de error de VPN.....	75
Solucionar problemas de VPN de sitio a sitio mediante CLI.....	78
Mostrar comandos.....	78
Borrar comandos.....	79
Comandos de prueba.....	79
Comandos de depuración.....	80

# Conceptos básicos de VPN IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	No se requiere licencia

Las redes privadas virtuales (VPN) crean túneles que permiten a los usuarios y sistemas conectarse de manera segura a través de una red pública como si se estuvieran conectando a través de una red de área local (LAN). Para configurar un túnel VPN, hacen falta dos dispositivos que puedan autenticarse mutuamente y cifrar el flujo de información entre ellos. Los dispositivos pueden ser una pareja de cortafuegos de Palo Alto Networks, o bien un cortafuegos de Palo Alto Networks y un dispositivo de otro proveedor con capacidad para VPN.

Conozca los conceptos básicos de las VPN:

- [IPSec VPN](#)
- [Modos de túnel IPSec](#)
- [Tipos de VPN IPSec](#)
- [Túneles VPN IPSec](#)
- [Implementaciones de VPN](#)
- [Intercambio de claves por red \(IKE\) para VPN](#)

## IPSec VPN

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	No se requiere licencia

IPSec VPN proporciona una comunicación IP privada y segura a través de una infraestructura de red pública (por ejemplo, Internet). Con esta tecnología, diferentes sitios o usuarios en diferentes zonas geográficas pueden comunicarse a través de una red, y así utilizar sus recursos de forma segura. IPSec proporciona confidencialidad e integridad de datos, incluida la autenticación, la verificación de integridad y el cifrado.

VPN IPSec es uno de los dos protocolos VPN comunes, o conjuntos de estándares utilizados para establecer una conexión VPN. En la capa IP, IPSec proporciona acceso remoto y seguro a toda una red (en lugar de a un solo dispositivo).

Hay dos tipos de VPN IPSec:

- modo de túnel
- modo de transporte

### Diferencias entre IPSec y VPN

SEGURIDAD IP (IPSec)	VPN
Proporciona a los hosts de IP métodos para cifrar y autenticar los datos enviados en la red IP.	Utiliza el cifrado para ocultar todos los datos enviados entre el cliente VPN y el servidor.
Mediante el uso de IPSec, las entidades que tienen direcciones IP pueden crear un túnel seguro.	Muchos tipos de protocolos VPN ofrecen diferentes niveles de seguridad y otras características. Los protocolos de tunelización más utilizados en la industria de las VPN son el protocolo de túnel punto a punto (PPTP), el protocolo de túnel de capa dos (L2TP) o IPSec, el protocolo de túnel de socket seguro (SSTP) y OpenVPN.

## Modos de túnel IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>Prisma Access (El modo de transporte de túnel IPSec todavía no es compatible con Prisma Access)</li> <li>PAN-OS</li> </ul>	<p>No se requiere licencia</p>

Los estándares IPSec definen dos modos distintos de operaciones IPSec: modos de túnel y transporte. La diferencia principal entre el modo de transporte y el de túnel es dónde se aplica la regla de política. Cuando está en modo túnel, el paquete original se encapsula en otro encabezado IP, los paquetes pueden protegerse mediante el encabezado de autenticación (AH), la carga útil de seguridad encapsulada (ESP) o ambos en cualquiera de los modos.



- AH no funciona con NAT ya que la integridad se calcula utilizando algunos campos del encabezado IP. La razón es que AH incluye el encabezado IP externo en el cálculo del código de autenticación de mensajes basado en hash (HMAC) que hace que NAT lo rompa.*
- El modo de transporte IPSec se utiliza para comunicaciones de un extremo a otro, por ejemplo, entre un cliente y un servidor, o entre una estación de trabajo y una puerta de enlace, si la puerta de enlace se trata como un host. Un buen ejemplo sería una sesión cifrada de Telnet o Escritorio remoto desde una estación de trabajo a un servidor.*
- Si bien PAN-OS<sup>®</sup> admite el modo túnel de forma predeterminada, la compatibilidad con el modo transporte es la nueva opción introducida a partir de la versión PAN-OS 11.0.*

## Tipos de VPN IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	<p>No se requiere licencia</p>

La VPN de sitio a sitio (o puerta de enlace a puerta de enlace) y la VPN de acceso remoto (cliente a sitio) son dos tipos distintos de VPN. Mientras que la VPN de cliente a sitio representa una conexión de usuario único, las VPN de sitio a sitio se ocupan de las conexiones remotas entre redes integrales.

En una VPN de sitio a sitio, el método de seguridad IPSec se utiliza para crear un túnel cifrado desde la red de un cliente hasta un sitio remoto del cliente. Los túneles VPN de Palo Alto Networks también se pueden utilizar entre socios.



Las VPN de sitio a sitio *no permiten varios endpoints*.

En la **VPN de acceso remoto**, los endpoints individuales se conectan a una red privada para acceder a los servicios y recursos de esa red privada de forma remota. La VPN de acceso remoto es más adecuada para usuarios empresariales y domésticos, ya que permite varios endpoints.

## Túneles VPN IPsec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	No se requiere licencia

El proceso de creación de un túnel IPsec comienza primero por establecer un túnel de preparación que esté cifrado y protegido y, a continuación, desde dentro de ese túnel seguro, negociar las claves de cifrado y los parámetros para el túnel IPsec.

Las negociaciones de VPN se llevan a cabo en dos fases definidas como fase uno y fase dos. El objetivo principal de la fase uno es establecer un canal cifrado seguro a través del cual los dos peers puedan negociar. Cuando la fase uno termina con éxito, los peers pasan rápidamente a la fase dos para las negociaciones.

Si la interfaz de túnel se encuentra en una zona diferente a la zona en donde se originará o de donde saldrá el tráfico, defina una regla de política para permitir que el tráfico fluya desde la zona de origen a la zona que contiene la interfaz del túnel. La configuración de la dirección IP en la interfaz de túnel es opcional. Necesitaría esta dirección IP si tiene la intención de ejecutar protocolos de enrutamiento dinámico a través de la interfaz de túnel.

Si bien IPsec incorpora muchas tecnologías de componentes y ofrece múltiples opciones de cifrado, la operación básica incluye los siguientes cinco procedimientos principales:

- **Tráfico interesante o bajo demanda:** la regla de política de túnel IPsec y la tabla de rutas determinan qué tipo de tráfico se considera "interesante" o se captura "bajo demanda" y, por lo tanto, está protegido. [La forma en que se implementa la política de seguridad de VPN de PAN-OS](#) depende de la plataforma del dispositivo. Las listas de acceso interpretan la regla de políticas IPsec para determinar qué tráfico estará protegido por IPsec.

El túnel IPsec aparece solo cuando hay un tráfico interesante destinado al túnel. Para iniciar manualmente el túnel, compruebe el estado del túnel y borre los túneles consultando la [resolución de problemas de VPN de sitio a sitio mediante la CLI](#).

- **IKE de fase 1:** IKE es un estándar de protocolo de administración de claves que se utiliza con IPsec. IKE autentica cada peer en una sesión IPsec, negocia automáticamente dos niveles de SA y gestiona el intercambio de claves de sesión realizado en dos fases: fase 1 y fase 2.

El objetivo principal de la fase 1 de IKE es autenticar los peers de IPsec y configurar un canal seguro entre los peers.

- **IKE de fase 2:** IKE negocia los parámetros más estrictos de las asociaciones de seguridad (SA) de IPsec entre los peers.
- **Transferencia de datos IPsec:** los datos que cumplen los requisitos se transfieren entre peers IPsec. La información se intercambia a través de sesiones IPsec basadas en el método para definir el tráfico interesante. Los paquetes se cifran y descifran en los peers IPsec mediante cualquier cifrado especificado en la SA de IPsec.
- **Finalización de sesión de túnel IPsec:** la sesión IPsec se puede terminar porque el tráfico finalizó y se eliminó la SA IPsec o porque se puede agotar el tiempo de espera de la SA en función de la

configuración de duración de la asociación de seguridad. El tiempo de espera de SA puede ser después de un número indicado de segundos o un número determinado de bytes pasados a través de la conexión.

Las claves se descartan cuando se finalizan las SA, lo que requiere que IKE realice una nueva negociación de fase dos y, posiblemente, una nueva negociación de fase uno. Se pueden establecer nuevas asociaciones de seguridad antes de que caduquen las actuales, manteniendo flujos de datos ininterrumpidos.



*La sesión IPSec finaliza cuando estas se eliminan o cuando el tiempo de espera se agota.*

### **Implementación de reglas de políticas de túnel IPSec en cortafuegos de nueva generación de Palo Alto Networks**

La encapsulación de un paquete para su transporte seguro en la red se realiza mediante el protocolo IPsec. Por ejemplo, en el caso de una VPN de sitio a sitio, un host de origen en una red transmite un paquete IP. Cuando ese paquete llega al borde de la red, se pone en contacto con una puerta de enlace VPN. La puerta de enlace VPN que se corresponde con esa red cifra el paquete de IP privada y lo retransmite a través de un túnel ESP a una puerta de enlace VPN del mismo nivel en el borde de la siguiente red, cuya puerta de enlace descifra el paquete y lo entrega al host de destino.

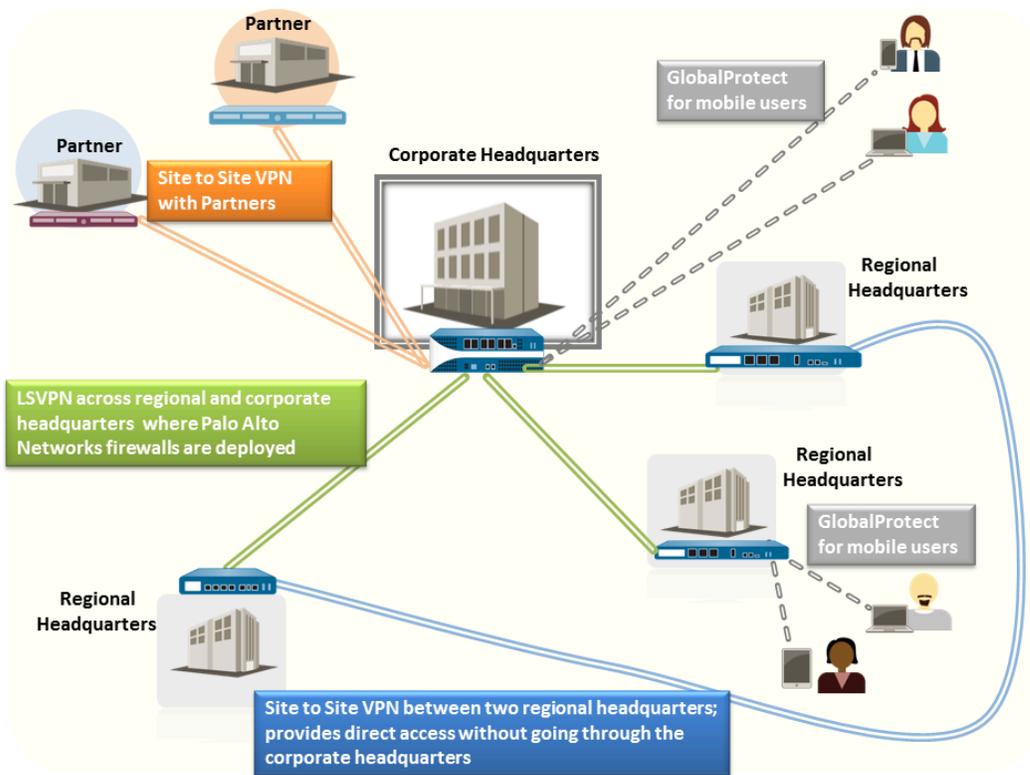
Las VPN basadas en políticas tienen reglas de seguridad específicas, reglas de políticas o listas de acceso (como direcciones de origen, direcciones de destino y puertos) que están configuradas para permitir el tráfico interesante a través de túneles IPSec. Se hace referencia a estas reglas durante el modo rápido (o fase 2 de IPSec) y se intercambian en el primer o segundo mensaje como el ID de proxy. Si el cortafuegos de Palo Alto Networks no está configurado con la configuración de ID de proxy, el cortafuegos establece el ID de proxy con los valores predeterminados (ip de origen = 0.0.0.0/0, ip de destino = 0.0.0.0/0, application:cualquiera) y lo intercambia con el peer durante el primer o el segundo mensaje del modo rápido.

## Implementaciones de VPN

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	<p>No se requiere licencia</p>

El cortafuegos de Palo Alto Networks admite las siguientes implementaciones de VPN:

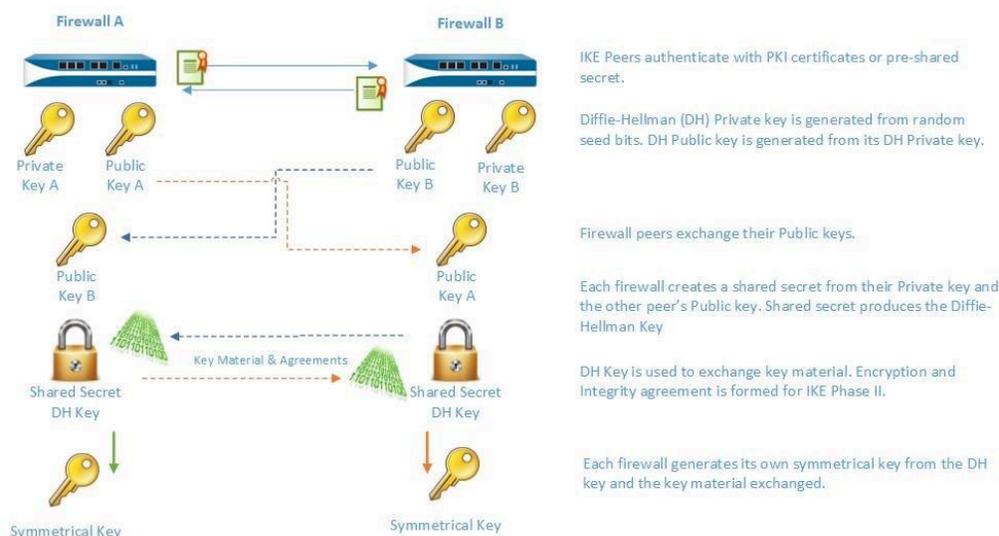
- **VPN de sitio a sitio:** Una VPN sencilla que se conecta a un sitio central y a un sitio remoto, o bien una VPN hub and spoke que se conecta a un sitio central con múltiples sitios remotos. El cortafuegos usa el conjunto de protocolos de seguridad de Internet (IPSec) para configurar un túnel seguro entre los dos sitios. Consulte [Descripción general de VPN de sitio a sitio](#).
- **VPN de usuario remoto a sitio:** Una solución que usa el agente GlobalProtect para permitir a un usuario remoto establecer una conexión segura a través del cortafuegos. Esta solución usa SSL e IPSec para establecer una conexión segura entre el usuario y el sitio. Consulte la [GlobalProtect Administrator's Guide](#) (Guía del administrador de GlobalProtect).
- **VPN a gran escala:** La VPN a gran escala de GlobalProtect de Palo Alto Networks (LSVPN) ofrece un mecanismo simplificado para implementar una VPN hub and spoke con un máximo de 1.024 oficinas satélite. Esta solución requiere que haya cortafuegos de Palo Alto Networks implementados en el concentrador y en todos los radios. Usa certificados para la autenticación de dispositivos, SSL para la protección entre todos los componentes e IPSec para proteger los datos. Consulte [Large Scale VPN \(LSVPN\)](#) (VPN a gran escala (LSVPN)).
- **VPN de sitio remoto:** los sitios remotos utilizan túneles IPSec para proteger a los usuarios y dispositivos en [ubicaciones de red remotas](#). Además, los usuarios móviles protegidos con GlobalProtect y los usuarios en sitios remotos acceden a aplicaciones privadas utilizando túneles IPSec (para [conexiones de servicio](#) o [conectores ZTNA](#)) o túneles GRE (para [conexiones Colo-Connect](#)).



## Intercambio de claves por red (IKE) para VPN

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

El proceso IKE permite a los peers VPN en ambos extremos del túnel cifrar y descifrar paquetes usando claves o certificados acordados mutuamente y un método de cifrado. El proceso IKE se realiza en dos fases: **IKE de fase 1** y **IKE de fase 2**. Cada una de estas fases usa claves y algoritmos de cifrado que se definen usando perfiles criptográficos —perfil criptográfico IKE y perfil criptográfico IPsec—, y el resultado de la negociación IKE es una asociación de seguridad (SA). Una SA es un conjunto de claves y algoritmos acordados mutuamente usados por ambos peers VPN para permitir el flujo de datos a través del túnel VPN. La siguiente ilustración muestra el proceso de intercambio de claves para configurar un túnel VPN:



## Puerta de enlace de IKE

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

Los cortafuegos Palo Alto Networks o un cortafuegos y otro dispositivo de seguridad que inicien y terminen conexiones VPN entre dos redes se llaman gateways IKE. Para configurar el túnel VPN y enviar tráfico entre los gateways IKE, cada peer debe tener una dirección IP (estática o dinámica) o FQDN. Los peers VPN usan claves previamente compartidas o certificados para autenticarse mutuamente.

Los peers también deben negociar el modo (principal o agresivo) para configurar la duración del túnel VPN y la SA en IKE de fase 1. El modo principal protege la identidad de los peers y es más seguro porque se intercambian más paquetes al configurar el túnel. Si ambos peers lo admiten, el modo principal es el

recomendado para la negociación IKE. El modo agresivo usa menos paquetes para configurar el túnel VPN, por lo que es una opción más rápida, aunque menos segura, de configurar el túnel VPN.

Consulte [Configuración de una puerta de enlace de IKE](#) para obtener información detallada sobre la configuración.

## IKE de fase 1

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

En esta fase, los cortafuegos usan los parámetros definidos en la configuración del gateway IKE y el perfil criptográfico IKE para autenticarse mutuamente y establecer un canal de control. La fase IKE es compatible con el uso de claves compartidas previamente o certificados digitales (que usan infraestructuras de claves públicas, PKI) para la autenticación mutua de los peers VPN. Las claves previamente compartidas son una solución sencilla para proteger redes pequeñas, ya que no necesitan ser compatibles con una infraestructura PKI. Los certificados digitales pueden ser más adecuados para redes o implementaciones de mayor tamaño que requieren de mayor seguridad para la autenticación.

Al usar certificados, asegúrese de que la CA que emite el certificado es de confianza para ambos peers del gateway y que la longitud máxima de la cadena de certificados es 5 o menos. Con la fragmentación IKE habilitada, el cortafuegos puede volver a juntar mensajes IKE con hasta 5 certificados en la cadena de certificados y establecer correctamente el túnel VPN.

El perfil criptográfico IKE define las siguientes opciones que se usan en la negociación de SA IKE:

- Grupo Diffie-Hellman (DH) para la generación de claves simétricas para 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. Los grupos DH compatibles con el cortafuegos son:

Número de grupo	Número de bits
Grupo 1	768 bits
Grupo 2	1,024 bits (predeterminado)
Grupo 5	1,536 bits
Grupo 14	2,048 bits
Grupo 15	( <a href="#">PAN-OS 10.2.0 y versiones posteriores</a> ) Grupo exponencial modular de 3072 bits
Grupo 16	( <a href="#">PAN-OS 10.2.0 y versiones posteriores</a> ) Grupo exponencial modular de 4096 bits
Grupo 19	Grupo de curvas elípticas de 256 bits

Número de grupo	Número de bits
Grupo 20	Grupo de curvas elípticas de 384 bits
Grupo 21	(PAN-OS 10.2.0 y versiones posteriores) Grupo de curvas elípticas aleatorias de 512 bits

- Algoritmos de autenticación: sha1, sha 256, sha 384, sha 512 o md5.
- Algoritmos de cifrado: aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc, aes-256-cbc, o des.



- PAN-OS 10.0.3 y las versiones posteriores son compatibles con los algoritmos aes-256-gcm y aes-128-gcm.
- PAN-OS 10.1.0 y las versiones anteriores son compatibles con el algoritmo de cifrado des.

## IKE de fase 2

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

Una vez protegido y autenticado el túnel, en la fase 2 se aumenta la protección del canal para la transferencia de datos entre las redes. IKE de fase 2 usa las claves que se establecieron en la fase 1 del proceso y el perfil criptográfico IPsec, que define los protocolos y las claves IPsec usadas para la SA en el IKE de fase 2.

IPSEC usa los siguientes protocolos para habilitar una comunicación segura:

- Carga útil de seguridad encapsulada (ESP): Le permite cifrar el paquete de IP completo, así como autenticar la fuente y verificar la integridad de los datos. Mientras que ESP necesita que cifre y autentique el paquete, puede elegir solo cifrar o solo autenticar definiendo la opción de cifrado como Null; no se recomienda usar cifrado sin autenticación.
- Authentication header (AH): Autentica el origen del paquete y verifica la integridad de datos. AH no cifra la carga de datos y se desaconseja su uso en implementaciones en las que la privacidad de los datos es importante. AH se suele usar cuando el principal objetivo es verificar la legitimidad del peer y la privacidad de datos no es necesaria.

**Table 1: Algoritmos compatibles con autenticación y cifrado IPsec**

ESP	AH
-----	----

### Opciones de intercambio de Diffie Hellman (DH) compatibles

- Grupo 1: 768 bits
- Grupo 2: 1024 bits (predeterminado)
- Grupo 5: 1536 bits
- Grupo 14: 2048 bits

ESP	AH
<ul style="list-style-type: none"> <li>• (PAN-OS 10.2.0 y versiones posteriores) Grupo 15: Grupo exponencial modular de 15 a 3072 bits</li> <li>• (PAN-OS 10.2.0 y versiones posteriores) Grupo 15: Grupo exponencial modular de 16 a 4096 bits</li> <li>• Grupo 19: grupo de curvas elípticas de 256 bits</li> <li>• Grupo 20: grupo de curva elíptica de 384 bits</li> <li>• (PAN-OS 10.2.0 y versiones posteriores) Grupo 21: Grupo de curvas elípticas aleatorias de 21 a 512 bits</li> <li>• No-pfs: De manera predeterminada, secreto perfecto hacia adelante (PFS) está habilitado, lo que significa que se genera una nueva clave DH en IKE de fase 2 usando uno de los grupos enumerados arriba. Esta clave es independiente de las claves intercambiadas en IKE de fase 1 y ofrece una mejor transferencia de datos. Si selecciona no-pfs, la clave DH creada en la fase 1 no se renueva y se usa una única clave para las negociaciones con la SA IPSec. Ambos peers VPN deben estar habilitados o deshabilitados para PFS.</li> </ul>	

### Algoritmos de cifrado compatibles

• des	(PAN-OS 10.1.0 y versiones anteriores) Estándar de cifrado de datos (DES) con la fuerza de seguridad de 56 bits.
• 3des	Estándar de cifrado triple de datos (3DES) con una fuerza de seguridad de 112 bits.
• aes-128-cbc	Estándar de cifrado avanzado (AES) usando encadenamiento de bloques de cifras (CBC) con una fuerza de seguridad de 128 bits.
• aes-192-cbc	AES usando CBC con una fuerza de seguridad de 192 bits.
• aes-256-cbc	AES usando CBC con una fuerza de seguridad de 256 bits.
• aes-128-ccm	AES usando Counter CBC-MAC (CCM) con una fuerza de seguridad de 128 bits.
• aes-128-gcm	AES usando Modo Galois/Counter (GCM) con una fuerza de seguridad de 128 bits.
• aes-256-gcm	AES usando GCM con una fuerza de seguridad de 256 bits.

### Algoritmos de autenticación compatibles

• md5	• md5
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384

ESP	AH
<ul style="list-style-type: none"> <li>• sha512</li> </ul>	<ul style="list-style-type: none"> <li>• sha 512</li> </ul>

### Métodos de protección de túneles VPN IPsec (IKE de fase 2)

Los túneles VPN IPsec se pueden proteger usando claves manuales o automáticas. Asimismo, las opciones de configuración IPsec incluyen un grupo Diffie-Hellman para acordar claves, un algoritmo de cifrado y un hash para la autenticación de mensajes.

- **Clave manual:** La clave manual se suele usar si el cortafuegos Palo Alto Networks está estableciendo un túnel VPN con un dispositivo antiguo o si quiere reducir los gastos de la generación de claves de sesión. Si usa claves manuales, debe configurarse la misma en ambos peers.

Las claves manuales no son recomendables para establecer un túnel VPN porque las claves de sesión pueden verse comprometidas cuando transmitan la información de claves entre peers; si las claves ven comprometida su seguridad, la transferencia de datos deja de ser segura.

- **Clave automática:** La clave automática le permite generar claves de forma automática para configurar y mantener el túnel IPsec basado en algoritmos definidos en el perfil criptográfico IPsec.

## IKEv2

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

Una puerta de enlace de VPN IPsec usa IKEv1 o **IKEv2** para negociar la asociación de seguridad IKE (SA) y el túnel IPsec. IKEv2 se define en [RFC 5996](#).

A diferencia IKEv1, que usa Phase 1 SA y Phase 2 SA, IKEv2 usa una SA secundaria para Encapsulating Security Payload (ESP) o Authentication Header (AH), que se configura con una SA IKE.

Debe habilitarse NAT transversal (NAT-T) en ambos gateways si tiene NAT habilitada en un dispositivo situado entre dos gateways. Una puerta de enlace solo puede ver la dirección IP pública (enrutable globalmente) del dispositivo NAT.

IKEv2 ofrece las siguientes ventajas con respecto a IKEv1:

- Los extremos de túnel intercambian menos mensajes para establecer un túnel. IKEv2 usa cuatro mensajes; IKEv1 usa nueve mensajes (en el modo principal) o seis mensajes (en el modo agresivo).
- La funcionalidad NAT-T integrada mejora la compatibilidad entre proveedores.
- La comprobación de estado integrada restablece automáticamente un túnel si este deja de estar disponible. La comprobación de actividad sustituye la Detección de fallo del peer usada en IKEv1.
- Admite selectores de tráfico (uno por intercambio). Los selectores de tráfico se usan en las negociaciones IKE para controlar qué tráfico puede acceder al túnel.
- Admite intercambio de certificados de Hash y URL para reducir la fragmentación.
- Resiliencia ante ataques de denegación de servicio con validación de peers mejorada. Un número excesivo de SA medio abiertas puede activar la validación de cookies.

Antes de configurar IKEv2, debería estar familiarizado con los siguientes conceptos.

- [Comprobación de actividad](#)
- [Umbral de activación de cookies y validación de cookies estricta](#)
- [Selectores de tráfico](#)
- [Intercambio de certificados Hash y URL](#)
- [Duración de la clave de SA e intervalo de reautenticación](#)

Cuando haya realizado la [Configuración de una puerta de enlace de IKE](#), si elige IKEv2, realice las siguientes tareas opcionales relacionadas con IKEv2 como se requiere en su entorno:

- [Exportación de un certificado para un peer para acceder usando Hash y URL](#)
- [Importación de un certificado para Autenticación de puerta de enlace IKEv2](#)
- [Cambio de la duración de la clave o del intervalo de autenticación IKEv2](#)
- [Cambio del umbral de activación de cookies para IKEv2](#)
- [Configuración de selectores de tráfico IKEv2](#)

## Comprobación de actividad

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

La comprobación de actividad IKEv2 es similar a Detección de fallo del peer (DPD), que IKEv1 usa para determinar si un peer sigue disponible.

En IKEv2, la comprobación de actividad la logra cualquier transmisión de paquete IKEv2 o mensaje de información vacío que envíe el gateway al peer en un intervalo configurable (predeterminado: 5 segundos). En caso necesario, el remitente intenta la retransmisión hasta 10 veces. Si no recibe respuesta, el remitente cierra y elimina la IKE\_SA y las CHILD\_SA correspondientes. El remitente empezará de nuevo enviando otro mensaje IKE\_SA\_INIT.

## Umbral de activación de cookies y validación de cookies estricta

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

La validación de cookies siempre está habilitada para IKEv2; ayuda a proteger contra ataques DoS de media SA. Puede configurar el número de umbral global de SA a medio abrir que activará la validación de cookies. También puede activar gateways IKE individuales para garantizar que se realiza la validación de cookies para cada SA IKEv2 nueva.

- El **Cookie Activation Threshold (Umbral de activación de cookies)** es una configuración de sesión VPN global que limita el número de SA IKE a medio abrir simultáneas (el valor predeterminado es de 500). Si el número de SA IKE a medio abrir supera el **Cookie Activation Threshold**, el respondedor solicitará una cookie y el iniciador deberá responder con una IKE\_SA\_INIT que contenga una cookie

para validar la conexión. Si la cookie se valida correctamente, se puede iniciar otra SA. Un valor de cero significa que la validación de cookies siempre está activada.

El respondedor no mantiene un estado del iniciador ni realiza un intercambio de claves Diffie-Hellman hasta que el iniciador devuelva la cookie. La validación de cookies IKEv2 mitiga un ataque de denegación de servicio que podría intentar dejar numerosas conexiones a medio abrir.

El **Cookie Activation Threshold (Umbral de activación de cookies)** debe ser inferior que el valor de **Maximum Half Opened SA (SA semiabiertas máximas)**. Si ha [Cambio del umbral de activación de cookies para IKEv2](#) a un número más alto (por ejemplo, 65534) y el ajuste **Maximum Half Opened SA (SA medio abiertas máx.)** se mantiene en el valor por defecto de 65535, la validación de cookies está deshabilitada.

- Puede habilitar **Strict Cookie Validation** si desea que se realice la validación de cookies para cada SA IKEv2 que reciba la puerta de enlace, independientemente del umbral global. La **Strict Cookie Validation (Validación estricta de cookies)** afecta solo a la puerta de enlace que se está configurando y está deshabilitada por defecto. Si **Strict Cookie Validation (Validación estricta de cookies)** está deshabilitada, el sistema usa el **Cookie Activation Threshold (Umbral de activación de cookies)** para determinar si se necesita o no una cookie.

## Selectores de tráfico

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

En IKEv1, un cortafuegos que tiene una VPN basada en rutas necesita usar un ID de proxy local y remoto para configurar un túnel IPSec. Cada peer compara los ID de proxy con lo que se recibe realmente en el paquete para negociar IKE de fase 2 de forma correcta. El IKE de fase 2 consiste en negociar las SA para configurar un túnel IPSec. (Para obtener más información sobre los ID de proxy, consulte [Interfaz túnel](#)).

En IKEv2, puede realizar una [Configuración de selectores de tráfico IKEv2](#), que son componentes de tráfico de red que se usan durante la negociación IKE. Los selectores de tráfico se usan durante la CHILD\_SA (creación de túnel) de fase 2 para configurar el túnel y determinar qué tráfico está permitido a través del túnel. Los dos peers de puerta de enlace IKE deben negociar y acordar sus selectores de tráfico; de lo contrario, una parte estrecha su intervalo de direcciones para acuerdo. Una conexión IKE puede tener múltiples túneles; por ejemplo, puede asignar diferentes túneles a cada departamento para aislar su tráfico. La separación de tráfico también permite implementar funciones como QoS.

Los selectores de tráfico IPv4 e IPv6 son:

- **Dirección IP de origen:** Un prefijo de red, intervalo de dirección, host específico o un comodín.
- **Dirección IP de destino:** Un prefijo de red, intervalo de dirección, host específico o un comodín.
- **Protocolo:** un protocolo de transporte, como TCP o UDP.
- **Puerto de origen:** el puerto donde se ha originado el paquete.
- **Puerto de destino:** El puerto al que está destinado el paquete.

Durante la negociación IKE, puede haber múltiples selectores de tráfico para diferentes redes y protocolos. Por ejemplo, el Iniciador puede indicar que quiere enviar paquetes TCP desde 172.168.0.0/16 a través del túnel a su peer, destinado a 198.5.0.0/16. También quiere enviar paquetes UDP desde 172.17.0.0/16

a través del mismo túnel a la misma puerta de enlace, con destino a 0.0.0.0 (cualquier red). La puerta de enlace de peers debe coincidir con estos selectores de tráfico para que sepa qué esperar.

Es posible que una puerta de enlace inicie la negociación mediante un selector de tráfico que sea una dirección IP más específica que la dirección IP de la otra puerta de enlace.

- Por ejemplo, la puerta de enlace A ofrece una dirección IP de origen de 172.16.0.0/16 y la dirección IP de destino 192.16.0.0/16. Pero la puerta de enlace B se configura con 0.0.0.0 (cualquier origen) como la dirección IP de origen y 0.0.0.0 (cualquier destino) como la dirección IP de destino. Por lo tanto, la puerta de enlace B restringe la dirección IP de origen a 192.16.0.0/16 y la dirección de destino 172.16.0.0/16. Así, la restricción adapta la dirección del gateway A y los selectores de tráfico de las dos gateways están de acuerdo.
- Si la puerta de enlace B (configurada con dirección IP 0.0.0.0) es el Iniciador en lugar del Respondedor, la puerta de enlace A responderá con sus direcciones IP más específicas, y la puerta de enlace B restringirá sus direcciones para llegar a un acuerdo.

## Intercambio de certificados Hash y URL

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

IKEv2 admite el intercambio de certificados Hash y URL, que se usa durante una negociación IKEv2 de una SA. Almacene el certificado en un servidor HTTP, que se especifica mediante una URL. El peer recupera el certificado del servidor basándose en la recepción de la URL al servidor. El hash se usa para comprobar si el contenido del certificado es válido o no. Por tanto, los dos peers intercambian certificados con la CA HTTP en lugar de hacerlo entre sí.

La parte hash de Hash y URL reduce el tamaño del mensaje y de este modo Hash y URL es un modo de reducir la probabilidad de fragmentación de paquetes durante la negociación IKE. El peer recibe el certificado y el hash esperados, y por tanto la primera fase IKE ha validado el peer. La reducción de la fragmentación ayuda a proteger contra ataques de denegación de servicio.

Puede habilitar el intercambio de certificados hash y URL al configurar una puerta de enlace IKE al seleccionar **HTTP Certificate Exchange** e introducir la **Certificate URL**. El peer también debe usar el intercambio de certificados Hash y URL para que el intercambio se realice de forma correcta. Si el peer no puede usar Hash y URL, los certificados X.509 se intercambian de forma parecida a como lo hacen en IKEv1.

Si habilita el intercambio de certificados Hash y URL, debe exportar su certificado al servidor de certificados, si aún no está allí. Al exportar el certificado, el formato de archivo debería ser **Binary Encoded Certificate (DER)**. Consulte [Exportación de un certificado para un peer para acceder usando Hash y URL](#).

## Duración de la clave de SA e intervalo de reautenticación

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

En IKEv2, dos valores de perfil criptográfico IKE, **Key Lifetime (Periodo de tiempo de la clave)** y **IKEv2 Authentication Multiple (Múltiplo de autenticación IKEv2)**, controlan el establecimiento de los SA de IKE IKEv2. La duración de la clave es el tiempo de validez de una clave SA IKE negociada. Antes de que venza la clave, se deberá volver a asignar la clave de registro de SA; de no ser así, cuando llegue el vencimiento, la SA deberá comenzar una nueva asignación de claves SA IKE IKEv2. El valor predeterminado es de 8 horas.

El intervalo de reautenticación se obtiene al multiplicar la **Key Lifetime (Duración de la clave)** por el **IKEv2 Authentication Multiple (Múltiplo de autenticación IKEv2)**. La autenticación múltiple tiene como valor predeterminado 0, lo que desactiva la función de reautenticación.

El intervalo del múltiplo de autenticación es 0-50. De modo que si va a configurar una autenticación múltiple de 20, por ejemplo, el sistema volvería a autenticar cada 20 asignaciones de clave, es decir, cada 160 horas. Eso significa que la puerta de enlace podría crear SA secundarias durante 160 horas antes de tener que volver a autenticarse con IKE para recrear la SA IKE desde cero.

En IKEv2, las puertas de enlace del Iniciador y el Respondedor tienen su propio valor de duración de clave, y el gateway con la duración de clave más breve es la que solicitará la reasignación de claves de SA.



# Comience con IPSec VPN (sitio a sitio)

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	<p>No se requiere licencia</p>

Una conexión VPN ofrece acceso seguro a la información entre dos o más sitios. Para proporcionar acceso seguro a los recursos y una conectividad fiable, una conexión VPN necesita los siguientes componentes: Puerta de enlace IKE, interfaz de túnel, supervisión de túnel, Intercambio de claves de Internet (IKE) para la VPN e IKEv2.

Antes de [planificar la configuración de su túnel VPN IPSec](#), es importante que esté familiarizado con:

- [Interfaz túnel](#)
- [Monitorización de túnel](#)
- [ID de proxy para VPN IPSec](#)

## Descripción general de VPN de sitio a sitio

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	No se requiere licencia

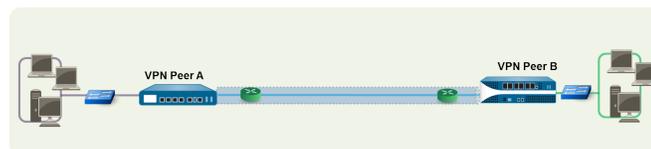
Una conexión VPN que permita conectar dos redes de área local (LAN) se llama VPN de sitio a sitio. Puede configurar VPN basadas en rutas para conectar cortafuegos de Palo Alto Networks en dos ubicaciones, o bien conectar cortafuegos de Palo Alto Networks a dispositivos de seguridad de terceros en otras ubicaciones. El cortafuegos también puede interoperar con dispositivos VPN basados en políticas de terceros; el cortafuegos de Palo Alto Networks es compatible con VPN basado en rutas.

El cortafuegos de Palo Alto Networks configura una VPN basada en rutas, donde el cortafuegos toma una decisión de enrutamiento basada en la dirección IP de destino. Si el tráfico se enruta a un destino específico a través de un túnel de VPN, se cifrará como tráfico VPN.

El conjunto de protocolos de seguridad de Internet (IPsec) se utiliza para configurar un túnel seguro para el tráfico VPN. Asimismo, la información de los paquetes de TCP/IP está protegida (y cifrada si el tipo de túnel es ESP). El paquete IP (encabezado y carga) está incrustado en otra carga de IP, se aplica un nuevo encabezado y se envía a través del túnel IPsec. La dirección IP de origen en el nuevo encabezado es la del peer VPN local y la dirección IP de destino es la del peer VPN del otro extremo del túnel. Cuando el paquete llega al peer VPN remoto (el cortafuegos en el otro extremo del túnel), el encabezado exterior se elimina y se envía el paquete original a su destino.

Para configurar el túnel VPN, primero deben autenticarse los peers. Tras autenticarse correctamente, los peers negocian los algoritmos y el mecanismo de cifrado para proteger la comunicación. El proceso de Intercambio de claves por red (IKE) se usa para autenticar a los peers de la VPN, y las asociaciones de seguridad (SA) IPsec se definen en cada extremo del túnel para proteger la comunicación VPN. IKE usa certificados digitales o claves compartidas previamente, así como las claves Diffie-Hellman para configurar las SA para el túnel de IPsec. Las SA especifican todos los parámetros obligatorios para el cifrado de la transmisión segura (incluyendo el índice de parámetros de seguridad [security parameter index, SPI], el protocolo de seguridad, las claves criptográficas y la dirección IP de destino), la autenticación de los datos, la integridad de los datos y la autenticación de los terminales.

La siguiente ilustración muestra un túnel de VPN entre dos sitios. Cuando un cliente que está protegido por el peer A de la VPN necesita contenido de un servidor ubicado en el otro sitio, el peer A de la VPN inicia una solicitud de conexión al peer B de la VPN. Si la política de seguridad permite la conexión, el peer A de la VPN usa los parámetros del perfil criptográfico IKE (IKE de fase 1) para establecer una conexión segura y autenticar al peer B de la VPN. A continuación, el peer A de la VPN establece el túnel VPN usando el perfil criptográfico IPsec, que define los parámetros del IKE de fase 2 para permitir la transferencia segura de datos entre los dos sitios.



## Interfaz túnel

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>Prisma Access</li> <li>PAN-OS</li> </ul>	No se requiere licencia

Para configurar un túnel VPN, la interfaz de capa 3 en cada extremo debe tener una interfaz de *túnel* lógica para que el cortafuegos se conecte y establezca un túnel VPN. Una interfaz de túnel es una interfaz lógica (virtual) que se utiliza para entregar tráfico entre los dos puntos de conexión. Si configura ID proxy, la ID proxy se considera en la capacidad total del túnel IPsec.

La interfaz de túnel debe pertenecer a una zona de seguridad para aplicar una regla de políticas; asimismo, debe estar asignada a un enrutador virtual para usar la infraestructura de enrutamiento existente. Compruebe que la interfaz de túnel y la interfaz física estén asignadas al mismo enrutador virtual, de modo que el cortafuegos pueda realizar una búsqueda de rutas y determinar el mejor túnel que puede usar.

Normalmente, la interfaz de capa 3 a la que está vinculada la interfaz de túnel pertenece a una zona externa, por ejemplo, la zona no fiable. Aunque la interfaz de túnel puede estar en la misma zona de seguridad que la interfaz física, puede crear una zona separada para la interfaz de túnel con el fin de lograr una mayor seguridad y mejor visibilidad. Si crea una zona separada para la interfaz de túnel (p. ej., una zona VPN), necesitará crear políticas de seguridad que habiliten el flujo del tráfico entre la zona VPN y la zona fiable.

Para enrutar el tráfico entre los sitios, una interfaz de túnel no requiere una dirección IP. Solo es necesaria una dirección IP si quiere habilitar la supervisión de túneles o si está usando un protocolo de enrutamiento dinámico para enrutar tráfico a través del túnel. Con enrutamiento dinámico, la dirección IP del túnel funciona como dirección IP de próximo salto para el enrutamiento de tráfico al túnel VPN.

Si está configurando el cortafuegos Palo Alto Networks con un peer de VPN que utiliza una VPN basada en políticas, debe configurar un ID de proxy local y remoto cuando configure el túnel IPsec. Cada peer compara los ID de proxy que tiene configurados con lo que se recibe en el paquete para permitir una negociación IKE de fase 2 correcta. Si se requieren varios túneles, configure varios ID de proxy exclusivos para cada interfaz de túnel; una interfaz de túnel puede tener un máximo de 250 ID de proxy. Cada ID de proxy se tendrá en cuenta a la hora de calcular la capacidad del túnel VPN IPsec del cortafuegos, y la capacidad del túnel varía en función del modelo de cortafuegos.

Consulte [Configuración de un túnel de IPsec](#) para obtener información detallada sobre la configuración.

## Monitorización de túnel

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Para un túnel VPN, puede comprobar la conectividad con una dirección IP de destino a través del túnel. El perfil de supervisión de la red del cortafuegos le permite verificar la conectividad (mediante ICMP) con una dirección IP de destino o un próximo salto en el intervalo de sondeo especificado, así como especificar una acción o fallo para acceder a la dirección IP supervisada.

Si no es posible alcanzar la dirección IP de destino, puede configurar el cortafuegos para que espere a que se recupere el túnel o configurar una conmutación por error automática a otro túnel. En cada caso, el cortafuegos genera un log de sistema que le alerta de un fallo del túnel y renegocia las claves IPsec para acelerar la recuperación.

Consulte [Supervise su túnel VPN IPsec](#) para obtener información detallada sobre la configuración.

## ID de proxy para VPN IPsec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

La identidad de proxy o ID de proxy hace referencia a un conjunto de tráfico que pertenece a una VPN IPsec que está sujeta a que la asociación de seguridad (SA) se negocie entre peers (o se configure una vez que la negociación se haya realizado correctamente).

Permite identificar y luego dirigir el tráfico:

- al túnel adecuado en el que coexisten varios túneles entre los mismos dos peers que comparten la misma puerta de enlace IKE.
- permite la coexistencia de SA únicas y compartidas con diferentes parámetros.

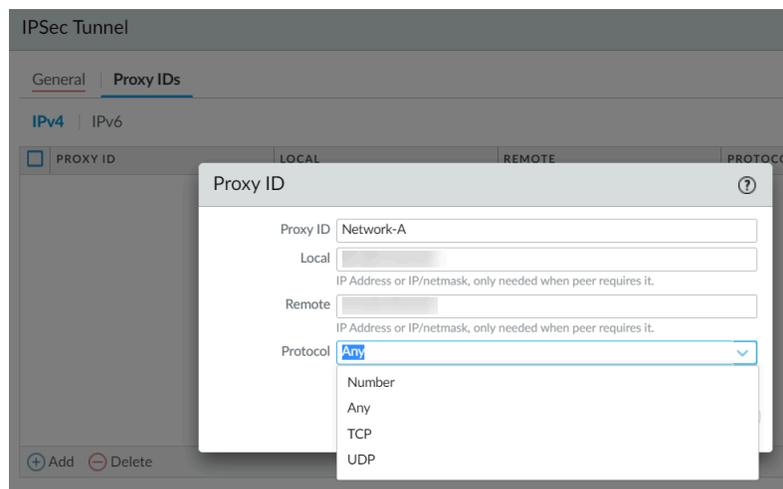


*Utilice los ID de proxy en las configuraciones en las que se configuran túneles VPN entre los mismos dos peers.*

Los ID de proxy ayudan a identificar qué tráfico pertenece a una VPN IPsec en particular. Esto permite que un sistema operativo instale los enlaces adecuados para dirigir el tráfico que coincide con la dirección de origen y destino en el ID de proxy (ID de cliente) y dirigirlo a la asociación de seguridad (SA) IPsec o VPN coincidente dentro y fuera de las asociaciones de seguridad (SA) IPsec coincidentes.

### Configuración del ID de proxy

Palo Alto Networks se encuentra entre los pocos proveedores que utilizan los ID de proxy. En la siguiente figura se muestra la ventana de ID de proxy de Palo Alto Networks junto con sus opciones.



Seleccione **Network (Red) > IPsec Tunnel (Túnel IPsec) > Proxy IDs (ID de proxy)**. Introduzca el nombre del ID de proxy, la dirección IP local, la dirección IP remota, si el peer lo requiere, y el tipo de protocolo junto con sus números de puerto local y remoto.



*Cada ID de proxy se considera un túnel VPN y, por lo tanto, se cuenta para la capacidad del túnel VPN IPsec del cortafuegos. Por ejemplo, el límite máximo para un túnel VPN IPsec de sitio a sitio es 1000 para PA-3020, 100 para PA-2050 y 25 para PA-200.*

Los ID de proxy se comportan de manera diferente con las versiones de IKE:

- **IKEv1:** los dispositivos de Palo Alto Networks son compatibles solo con coincidencias exactas de ID de proxy. Si los ID de proxy de los peers no coinciden, la VPN no funcionará correctamente.
- **IKEv2:** es compatible con la restricción del selector de tráfico cuando el ajuste de ID de proxy es diferente en las dos puertas de enlace de VPN.

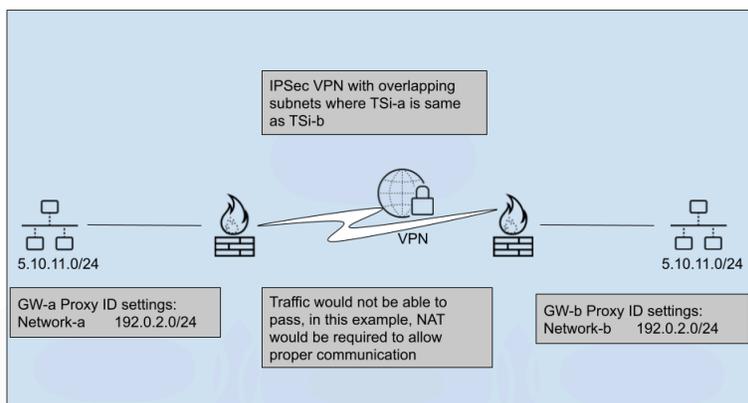
### Uso de los ID de proxy

En el ejemplo siguiente se muestran dos puertas de enlace de VPN: A y B.

La negociación de IKE la inicia VPN GW-az, i=iniciador, r=respondedor. VPN GW-a define el selector de tráfico TSi-a/TSr-a y VPN GW-b especifica el selector de tráfico TSi-b/TSr-b. Si bien TSr-a es el mismo que TSr-b y, por lo tanto, se puede ignorar, TSi-a puede ser diferente de TSi-b.

En este caso, el tráfico no se puede enrutar a través del túnel VPN, ya que existe la misma red en ambos lados del túnel.

Sin embargo, como se muestra a continuación, la única manera de resolver este problema es que ambas puertas de enlace de peers del mismo nivel creen las NAT para traducir una subred de red nueva y única a la red interna, de lo contrario, una de las partes tiene que cambiar la IP de la subred.



De esta manera, todo el tráfico de ambos lados se destinaría a la nueva dirección NAT en lugar de a la otra red similar. Ambas puertas de enlace tendrían que **realizar la NAT** para que esto funcione correctamente para eliminar cualquier confusión sobre qué red está en qué lado.

### Configuración de VPN IPsec para un firewall de Palo Alto Networks

Si el otro lado del túnel es un dispositivo VPN de terceros que no es un cortafuegos PAN-OS, entonces debe especificar un ID de proxy local y un ID de proxy remoto coincidentes: normalmente las subredes LAN locales y remotas.

Al configurar un ID de proxy de túnel IPsec para identificar redes IP locales y remotas para el tráfico que está sujeto a NAT, la configuración del ID de proxy para el túnel IPsec debe configurarse con la información de red IP posterior a NAT. La razón de esto es que la información de ID de proxy define las redes que se permitirán a través del túnel en ambos lados para la configuración de IPsec.

## Planifique la configuración de su túnel VPN IPsec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"><li>• Prisma Access</li><li>• PAN-OS</li></ul>	No se requiere licencia

Antes de configurar un túnel IPsec, es importante que decida los siguientes factores y planifique la configuración correcta de su túnel IPsec.

### **STEP 1 | Decida el tipo de VPN: Sitio a sitio o acceso remoto**

La VPN de sitio a sitio permite utilizar el método de seguridad IPsec para crear un túnel cifrado desde la red de un cliente hasta un sitio remoto del cliente. Sin embargo, la VPN de acceso remoto permite a los usuarios individuales conectarse a una red privada para acceder a sus servicios y recursos.

### **STEP 2 | Seleccione un método de seguridad para su VPN**

En una VPN de sitio a sitio, el método de seguridad IPsec se utiliza para crear un túnel cifrado desde la red de un cliente hasta un sitio remoto del cliente.

En la VPN de acceso remoto, los usuarios individuales están conectados a la red privada.

### **STEP 3 | Decida tu cliente VPN**

No es necesario configurar la VPN de sitio a sitio en cada cliente. La VPN de acceso remoto puede necesitar o no configuración en cada cliente.

### **STEP 4 | Decida la configuración de su túnel VPN**

La VPN de sitio a sitio no requiere que todos los usuarios inicien la configuración del túnel VPN. La VPN de acceso remoto requiere que cada usuario de acceso remoto inicie la configuración del túnel VPN.

### **STEP 5 | Decida su tecnología de seguridad**

Mientras que la VPN de sitio a sitio es compatible con la tecnología IPsec, la VPN de acceso remoto admite SSL así como la tecnología IPsec.

### **STEP 6 | Decida si desea usuarios individuales o múltiples en su VPN**

En la VPN de sitio a sitio, no se permiten múltiples usuarios; sin embargo, en la VPN de acceso remoto se permiten varios usuarios.



# Configuración de túneles VPN IPSec (sitio a sitio)

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	<p>No se requiere licencia</p>

Para configurar VPN de sitio a sitio:

- ❑ Asegúrese de que sus interfaces Ethernet, enrutadores virtuales y zonas están configurados correctamente. Si desea más información, consulte [Configuración de interfaces y zonas](#).
- ❑ Cree sus interfaces de túnel. Lo ideal sería colocar las interfaces de túnel en una zona separada para que el tráfico de túnel pueda usar políticas diferentes.
- ❑ Configure rutas estáticas o asigne protocolos de enrutamiento para redirigir el tráfico a los túneles VPN. Para admitir el enrutamiento dinámico (son compatibles OSPF, BGP, RIP), debe asignar una dirección IP a la interfaz del túnel.
- ❑ Defina puertos de enlace IKE para establecer comunicación entre peers a cada lado del túnel VPN; defina también el perfil criptográfico que especifica los protocolos y algoritmos para identificación, autenticación y cifrado que se usarán para configurar túneles VPN en IKEv1 de fase 1. Consulte [Configuración de un puerto de enlace de IKE](#) y [Definición de perfiles criptográficos de IKE](#).
- ❑ Configure los parámetros necesarios para establecer la conexión IPSec para transferencia de datos a través del túnel VPN; consulte [Configuración de un túnel de IPSec](#). En IKEv1 de fase 2, consulte la [Definición de perfiles criptográficos de IPSec](#).
- ❑ (Opcional) Especifique el modo en que el cortafuegos supervisará los túneles IPSec. Consulte [Supervise su túnel VPN IPSec](#).
- ❑ Defina las políticas de seguridad para filtrar e inspeccionar el tráfico.



*Si hay una regla de denegación en el extremo de la base de reglas de seguridad, el tráfico intrazona se bloquea, a menos que se permita de otro modo. Las reglas para permitir aplicaciones IKE e IPSec deben incluirse de manera explícita por encima de la regla de denegación.*



*Si el tráfico de su VPN atraviesa un cortafuegos serie PA-7000 o PA-5200 (no se origina ni finaliza en él), configure una regla de política de seguridad bidireccional para permitir el tráfico de ESP o AH en ambas direcciones.*

Cuando haya terminado estas tareas, el túnel estará listo para su uso. El tráfico destinado a zonas/direcciones definidas en una regla de políticas se enruta automáticamente correctamente basándose en la ruta de destino de la tabla de enrutamiento y se gestiona como tráfico VPN. Para ver algunos ejemplos de VPN de sitio a sitio, consulte [VPN de sitio a sitio Ejemplos de configuraciones](#).

## Configuración de una puerta de enlace de IKE

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Para configurar un túnel VPN, los peers o puertas de enlace VPN deben autenticarse mutuamente, utilizando claves previamente compartidas o certificados digitales, y establecer un canal seguro para negociar la asociación de seguridad (security association, SA) IPsec que se utilizará para proteger el tráfico entre los hosts en ambos lados.

### STEP 1 | Defina la [puerta de enlace de IKE](#).

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Gateways (Puertas de enlace de IKE)**, haga clic en **Add (Añadir)** para añadir una puerta de enlace e introduzca un **Name (Nombre)** para la puerta de enlace (pestaña **General**).
2. Establezca **Version (Versión)** en **IKEv1 only mode (Modo exclusivo IKEv1)**, **IKEv2 only mode (Modo exclusivo IKEv2)** o **IKEv2 preferred mode (Modo preferido IKEv2)**. La puerta de enlace IKE comienza su negociación con su peer en el modo que usted especifique aquí. Si selecciona **IKEv2 preferred mode** los dos peers usarán IKEv2 si el peer remoto lo admite; de lo contrario, usarán IKEv1.

La selección de **Version (Versión)** también determina qué opciones están disponibles en la pestaña **Advanced Options (Opciones avanzadas)**.

### STEP 2 | Establezca el endpoint local del túnel (puerta de enlace).

1. Seleccione el **Address Type (Tipo de dirección): IPv4 o IPv6**.
2. Seleccione la **Interface (Interfaz)** física de salida en el cortafuegos donde reside la puerta de enlace local.
3. En la lista **Local IP Address (Dirección IP local)**, seleccione la dirección IP que debe utilizar la conexión VPN como terminal; esta es la interfaz externa con una dirección IP del cortafuegos enrutable de forma pública.

### STEP 3 | Establezca el peer en el extremo más alejado del túnel (puerta de enlace).

En **Peer IP Address Type (Tipo de dirección IP del peer)**, seleccione una de las siguientes configuraciones e introduzca la información correspondiente para el peer:

- **IP:** introduzca un valor de **Peer Address (Dirección de peer)** como una dirección IPv4 o IPv6, o un objeto de dirección que sea una dirección IPv4 o IPv6.
- **FQDN:** introduzca un valor de **Peer Address (Dirección de peer)** como un FQDN o un objeto de dirección que utilice un FQDN. Si el objeto de dirección FQDN o FQDN se resuelve en más de una dirección IP, el cortafuegos selecciona la dirección preferida del conjunto de direcciones que coinciden con el tipo de dirección (IPv4 o IPv6) de la puerta de enlace IKE de la siguiente manera:
  - Si no se negocia ninguna asociación de seguridad (SA) IKE, la dirección preferida es la dirección IP con el valor más pequeño.

- Si la puerta de enlace de IKE utiliza una dirección dentro de un conjunto de direcciones ofrecidas, el cortafuegos selecciona esa dirección (sea o no la dirección más pequeña en el conjunto).
- Si la puerta de enlace de IKE utiliza una dirección que no está dentro de un conjunto de direcciones ofrecidas, el cortafuegos selecciona una nueva dirección, la más pequeña en el conjunto.
- **Dinámico:** seleccione **Dynamic (Dinámico)** si se desconoce la dirección IP del peer o el valor FQDN para que el par inicie la negociación.



*El uso de un objeto de dirección FQDN o FQDN reduce los problemas en entornos en los que el peer está sujeto a cambios dinámicos de dirección IP (y, de lo contrario, requeriría que vuelva a configurar esta dirección del peer de puerta de enlace IKE).*

### STEP 4 | Especifique cómo autenticar el peer.

Seleccione el método de **Authentication**. **Pre-Shared Key** o **Certificate**. Si selecciona una clave precompartida, vaya al siguiente paso. Si elige un certificado, vaya a el paso 6 para configurar la autenticación basada en certificados.

### STEP 5 | Configure una clave precompartida.

1. Introduzca una **Pre-shared Key (Clave precompartida)**, que es la clave de seguridad que se utilizará para autenticación a través del túnel. Vuelva a introducir el valor para **Confirm Pre-shared Key (Confirmar clave precompartida)**. Utilice un máximo de 255 caracteres ASCII o no ASCII.



*Genere una clave que sea difícil de averiguar con ataques por diccionario; use un generador de claves previamente compartidas en caso necesario.*

2. En **Local Identification**, seleccione uno de los siguientes tipos e introduzca el valor que considere oportuno: **FQDN (Nombre de host)**, **dirección IP**, **KEYID (cadena de ID de formato binario en HEX)** y **FQDN de usuario (dirección de correo electrónico)**. La identificación local define el formato y la identificación del gateway local. Si no especifica un valor, la dirección IP local se utiliza como valor de identificación local.
3. En **Peer Identification (Identificación de peer)**, seleccione uno de los siguientes tipos e introduzca el valor que considere oportuno: **FQDN (Nombre de host)**, **dirección IP**, **KEYID (cadena de ID de formato binario en HEX)** y **FQDN de usuario (dirección de correo electrónico)**. La identificación del peer define el formato y la identificación del gateway local. Si no especifica un valor, la dirección IP del peer se utiliza como valor de identificación del peer.
4. Vaya al paso 7 para configurar las opciones avanzadas de la puerta de enlace.

**STEP 6 |** Configuración de la autenticación basada en certificados.

Realice los pasos restantes de este procedimiento si ha seleccionado **Certificate (Certificado)** como el método de autenticación de la puerta de enlace del peer en el otro extremo del túnel.

1. Seleccione en **Local Certificate (Certificado local)** un certificado que ya se encuentre en el cortafuegos, haga clic en **Import (Importar)** para importar un certificado o bien haga clic en **Generate (Generar)** para crearlo.
  - Para implementar la función **Import (Importar)** de un certificado, realice la [Importación de un certificado para la autenticación de la puerta de enlace IKEv2](#) y regrese a esta tarea.
  - Si desea implementar la función **Generate (Generar)** para generar un nuevo certificado, [Genere un certificado en el cortafuegos](#) y regrese a esta tarea.
2. **(Opcional)** Marque **HTTP Certificate Exchange (Intercambio de certificados HTTP)** para configurar el hash y la URL (solo en IKE v. 2). Para un intercambio de certificados HTTP, introduzca la **Certificate URL (URL de certificado)**. Para obtener más información, consulte [Intercambio de certificado de hash y URL](#).
3. Seleccione el tipo de **Local Identification (Identificación local): Distinguished Name (Subject), FQDN (hostname) (Nombre distintivo [asunto], FQDN [nombre de host]), IP address (Dirección IP) o User FQDN (email address) (FQDN de usuario [dirección de correo electrónico])** e introduzca el valor. La identificación local define el formato y la identificación del gateway local.
4. Seleccione el tipo de **Peer Identification (Identificación de peer): Distinguished Name (Subject), FQDN (hostname) (Nombre distintivo [asunto], FQDN [nombre de host]), IP address (Dirección IP) o User FQDN (email address) (FQDN de usuario [dirección de correo electrónico])** e introduzca el valor. La identificación del peer define el formato y la identificación del gateway local.
5. Seleccione el tipo de **Peer ID Check (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 coincidan los caracteres tras el asterisco.
6. **(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 SA IKE correcta incluso aunque la identificación del peer no coincida con la identificación del peer en el certificado.
7. 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.
8. **(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.

**STEP 7 |** Configure las opciones avanzadas para la puerta de enlace.

1. (Opcional) Seleccione **Enable Passive Mode** en la sección Common Options (Opciones comunes) (**Advanced Options (Opciones avanzadas)**) para especificar que el cortafuegos solo responda a las solicitudes de conexión IKE y que nunca las inicie.
2. Si tiene un dispositivo que realice NAT entre puertas de enlace, seleccione **Enable NAT Traversal (Habilitar NAT transversal)** para utilizar la encapsulación UDP en los protocolos IKE y UDP, y permitirles pasar a través de dispositivos de NAT intermedios.
3. Si ha configurado **IKEv1 only mode (Modo de solo IKEv1)** en el paso 1, en la pestaña IKEv1
  - Seleccione el **Exchange Mode (Modo de intercambio): auto (automático), aggressive (agresivo) o main (principal)**. Si el cortafuegos está configurado para utilizar el modo de intercambio **auto (automático)**, acepta solicitudes de negociación tanto del modo **main (principal)** como del modo **aggressive (agresivo)**; sin embargo, siempre que sea posible, inicia los intercambios en el modo **main (principal)**.



*Si el modo de intercambio no se ha definido como **auto (automático)**, debe configurar ambos peers con el mismo modo de intercambio para permitir que cada peer acepte las solicitudes de negociación.*

- Seleccione un perfil existente o mantenga el perfil predeterminado en la lista **IKE Crypto Profile (Perfil criptográfico de IKE)**. De ser necesario, realice la [Definición de perfiles criptográficos IKE](#).
  - (Únicamente cuando utiliza autenticación basada en certificados y el modo de intercambio no está definido como **aggressive mode [modo agresivo]**) Haga clic en **Enable Fragmentation (Habilitar fragmentación)** para habilitar que el cortafuegos opere con fragmentación IKE.
  - Haga clic en **Dead Peer Detection (Detección de fallo del peer)** e introduzca un **Interval (Intervalo)** (el intervalo es de 2 a 100 segundos). Para **reintentar**, especifique el número de reintentos (el rango es de 2 a 100) antes de desconectarse del par IKE. La detección de fallo del peer identifica peers IKE inactivos o no disponibles enviando una carga de notificación IKE de fase 1 al peer y esperando a que la reconozca.
4. Si ha configurado **IKEv2 only mode (Modo de solo IKEv2)** o **IKEv2 preferred mode (Modo preferido IKEv2)** en el paso 1, en la pestaña IKEv2
    - Seleccione un perfil en **IKE Crypto Profile (Perfil criptográfico de IKE)**, que configura las opciones de la primera fase de IKE, como el grupo DH, el algoritmo de hash y la autenticación con ESP. Para obtener información sobre los perfiles criptográficos IKE, consulte [IKE de fase 1](#).
    - (Opcional) Habilite la **Strict Cookie Validation (Validación de cookies estricta)**. Consulte [Umbral de activación de cookies y validación de cookies estricta](#).
    - (Opcional) Seleccione **Enable Liveness Check (Habilitar comprobación de actividad)** e introduzca un **Interval (sec) (Intervalo [s])** (el valor predeterminado es 5) si desea que la puerta de enlace envíe una solicitud de mensaje a su peer de puerta de enlace, en el que solicite una respuesta. En caso necesario, el iniciador intenta la comprobación de actividad hasta diez veces. Si no recibe respuesta, el Iniciador cierra y elimina la IKE\_SA y las CHILD\_SA. El Iniciador empezará de nuevo enviando otro mensaje IKE\_SA\_INIT.

**STEP 8 |** Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

## Exportación de un certificado para un peer para acceder usando Hash y URL

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

IKEv2 permite el [Intercambio de certificados Hash y URL](#) como método para que el peer y el extremo remoto del túnel recuperen el certificado de un servidor donde ha exportado el certificado. Realice esta tarea para exportar su certificado a ese servidor. Ya debe haber creado un certificado utilizando **Device (Dispositivo) > Certificate Management (Gestión de certificados)**.

**STEP 1 |** Seleccione **Device (Dispositivo) > Certificates (Certificados)** y, si su plataforma admite varios sistemas virtuales, en **Location (Ubicación)**, seleccione el sistema virtual adecuado.

**STEP 2 |** En la pestaña **Device Certificates**, seleccione el certificado para exportar al servidor mediante la opción **Export**.



*El estado del certificado debe ser válido, no caducado. El cortafuegos no le impedirá exportar un certificado no válido.*

**STEP 3 |** Para **File Format**, seleccione **Binary Encoded Certificate (DER)**.

**STEP 4 |** Deje **Export private key** sin marcar. No es necesario exportar la clave privada para Hash y URL.

**STEP 5 |** Haga clic en **OK (Aceptar)**.

## Importación de un certificado para Autenticación de puerta de enlace IKEv2

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Realice esta tarea si está autenticando un peer para una puerta de enlace IKEv2 y no ha usado un certificado local existente en el cortafuegos, sino que quiere importar un certificado desde otra ubicación.

Para realizar esta tarea, se da por hecho que ha seleccionado **Network (Red) > IKE Gateways (Puertas de enlace de IKE)**, ha añadido una puerta de enlace y, en **Local Certificate (Certificado local)**, hizo clic en **Import (Importar)**.

**STEP 1 |** Importe un certificado.

1. Seleccione **Network (Red) > IKE Gateways (Puertas de enlace de IKE)**, haga clic en **Add (Añadir)** para añadir una puerta de enlace y en la pestaña **General**, en **Authentication (Autenticación)**, seleccione **Certificate (Certificado)**. En **Local Certificate (Certificado local)**, haga clic en **Import (Importar)**.

2. En la ventana Import Certificate (Importar certificado), introduzca un nombre en **Certificate Name (Nombre del certificado)** para el certificado que está importando.
3. Seleccione **Shared (Compartido)** si este certificado debe compartirse entre múltiples sistemas virtuales.
4. En **Certificate File (Archivo de certificado)**, utilice **Browse (Examinar)** para buscar el archivo del certificado. Haga clic en el nombre archivo y seleccione **Open (Abrir)**, lo que cumplimenta el campo **Certificate File (Archivo de certificado)**.
5. En **File Format**, seleccione una de las opciones siguientes:
  - **Base64 Encoded Certificate (PEM)**: contiene el certificado, pero no la clave. Es texto no cifrado.
  - **Encrypted Private Key and Certificate (PKCS12)**: contiene tanto el certificado como la clave.
6. Seleccione **Import private key** si la clave está en un archivo distinto del archivo de certificados. La clave es opcional, con la siguiente excepción:
  - Importe una clave si establece el **File Format (Formato de archivo)** en **PEM**. Introduzca un **Key file** al hacer clic en **Browse** y buscar el archivo de clave que desea importar.
  - Introduzca una **Passphrase** y seleccione **Confirm Passphrase**.
7. Haga clic en **OK (Aceptar)**.

**STEP 2** | Continúe con la siguiente tarea.

Paso [Configuración de la autenticación basada en certificados](#).

## Cambio de la duración de la clave o del intervalo de autenticación IKEv2

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> </ul>	No se requiere licencia

Esta tarea es opcional; el valor predeterminado de la duración de la asignación de claves de SA IKE IKEv2 es de 8 horas. La configuración predeterminada de la autenticación múltiple IKEv2 es 0, lo que significa que la función de reautenticación está deshabilitada. Para obtener más información, consulte la [Duración de la clave de SA e intervalo de reautenticación](#).

Para cambiar los valores predeterminados, realice la siguiente tarea. Un requisito previo es que ya exista un perfil IKE Crypto.

**STEP 1** | Cambie la duración de la clave de SA o el intervalo de autenticación para un perfil criptográfico IKE

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Crypto (Criptográfico IKE)** y seleccione el perfil Criptográfico IKE que se aplica a la puerta de enlace local.
2. Para la **Key Lifetime (Duración de la clave)**, seleccione una unidad (**Seconds [Segundos]**, **Minutes [Minutos]**, **Hours [Horas]** o **Days [Días]**) e introduzca un valor. El mínimo son 3 minutos.
3. Para **IKE Authentication Multiple (Múltiplo de autenticación IKE)**, introduzca un valor, que se multiplica por la duración para determinar el intervalo de reautenticación.

**STEP 2** | Confirme los cambios.

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

## Cambio del umbral de activación de cookies para IKEv2

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Realice la siguiente tarea si quiere que el cortafuegos tenga un umbral diferente del ajuste predeterminado de 500 sesiones de SA a medio abrir antes de que requiera la validación de cookies. Para obtener más información sobre la validación de cookies, consulte el [Umbral de activación de cookies y validación de cookies estricta](#).

**STEP 1** | Cambie el umbral de activación de cookies.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y edite la configuración de sesión de VPN. En **Cookie Activation Threshold (Umbral de activación de cookies)**, introduzca el número máximo de SA a medio abrir permitidas antes de que el respondedor solicite una cookie del iniciador (intervalo: 0-65.535; predeterminado: 500).
2. Haga clic en **OK (Aceptar)**.

**STEP 2** | Confirme los cambios.

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

## Configuración de selectores de tráfico IKEv2

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

En IKE v. 2, puede configurar los [Selectores de tráfico](#), que son componentes del tráfico de red que se utilizan durante la negociación de IKE. Los selectores de tráfico se usan durante la CHILD\_SA (creación de túnel) de fase 2 para configurar el túnel y determinar qué tráfico está permitido a través del túnel. Los dos peers de puerta de enlace IKE deben negociar y acordar sus selectores de tráfico; de lo contrario, una parte estrecha su intervalo de direcciones para acuerdo. Una conexión IKE puede tener múltiples túneles; por ejemplo, puede asignar diferentes túneles a cada departamento para aislar su tráfico. La separación de tráfico también permite implementar funciones como QoS. Utilice el siguiente flujo de trabajo para configurar los selectores de tráfico.

**STEP 1** | Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** > **Proxy IDs (ID de proxy)**.

**STEP 2** | Seleccione la pestaña **IPv4** o **IPv6**.

**STEP 3** | Haga clic en **Add** e introduzca el **nombre** en el campo **Proxy ID**.

**STEP 4** | En el campo **Local**, introduzca la **Source IP Address (Dirección IP de origen)**.

**STEP 5 |** En el campo **Remote**, introduzca **Destination IP Address**.

**STEP 6 |** En el campo **Protocol (Protocolo)**, seleccione el protocolo de transporte (**TCP** o **UDP**).

**STEP 7 |** Haga clic en **OK (Aceptar)**.

## Definición de perfiles criptográficos

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>Prisma Access</li> <li>PAN-OS</li> </ul>	No se requiere licencia

Un perfil criptográfico especifica los cifrados usados para autenticación o cifrado entre dos peers IKE y la duración de esta clave. El periodo entre cada renegotiación se conoce como duración; cuando el tiempo especificado vence, el cortafuegos vuelve a negociar un nuevo conjunto de claves.

Para proteger las comunicaciones a través del túnel VPN, el cortafuegos requiere perfiles criptográficos IKE e IPSec para completar las negociaciones IKE de fase 1 y de fase 2, respectivamente. El cortafuegos incluye un perfil criptográfico predeterminado IKE y un perfil criptográfico predeterminado IPSec que están listos para utilizarse.

- [Definición de perfiles criptográficos IKE](#)
- [Definición de perfiles criptográficos IPSec](#)

## Definición de perfiles criptográficos IKE

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>Prisma Access</li> <li>PAN-OS</li> </ul>	No se requiere licencia

El perfil criptográfico IKE se utiliza para configurar algoritmos de cifrado y autenticación que sirven para el proceso de intercambio de claves en [IKE de fase 1](#), y una duración de las claves, que especifica el tiempo que serán válidas. Para invocar el perfil, debe vincularlo a la configuración de gateway IKE.



*Todas las puertas de enlace IKE configuradas en la misma interfaz o dirección IP local deben usar el mismo perfil criptográfico cuando el **tipo de dirección IP de peers** de la puerta de enlace IKE esté configurado como **Dynamic (Dinámico)** y esté aplicado el modo principal IKEv1 o IKEv2. Si los perfiles criptográficos son los mismos en las puertas de enlace, aunque la conexión inicial puede comenzar en una puerta de enlace diferente, la conexión cambiará a la puerta de enlace adecuada cuando se intercambien certificados o claves previamente compartidas, y los ID de peers.*

Independientemente de si el peer VPN es del mismo proveedor o no, los peers VPN deben tener configurados los mismos parámetros IKE para realizar una negociación IKE correcta.

Los siguientes parámetros deben coincidir para que la negociación de IKE se realice correctamente:

- DH Group para el intercambio de llaves
- Algoritmos de encriptación
- Algoritmos de autenticación

Por ejemplo, si ha configurado el peer 1 de VPN con **group20** para el grupo DH, **sha384** para la autenticación y **aes-256-gcm** para el cifrado. A continuación, el peer 2 de VPN con el que desea establecer el túnel IPSec también debe tener configurados los mismos valores.

- [PAN-OS 10.1 y posteriores y Prisma Access \(Gestionado por Panorama\)](#)
- [#unique\\_39](#)

## Definición de perfiles criptográficos IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• Prisma Access</li> <li>• PAN-OS</li> </ul>	No se requiere licencia

El perfil criptográfico IPSec se invoca en [IKE de fase 2](#). Especifica el modo en que se protegen los datos dentro del túnel cuando se usa IKE de clave automática para generar claves para las SA del IKE de forma automática.

Independientemente de si su peer de VPN es del mismo proveedor o no, los peers VPN deben tener los mismos parámetros IPSec configurados para poder realizar una negociación IPSec correcta.

La negociación IPSec será correcta cuando los siguientes parámetros coinciden entre los peers VPN:

- Protocolo IPSec (ESP o AH)
- Grupo DH (o PFS) para intercambio de claves
- Algoritmos de encriptación
- Algoritmos de autenticación

Por ejemplo, si configuró el peer 1 de VPN con **ESP** para protocolo IPSec, **group20** para grupo DH, **sha384** para autenticación y **aes-256-gcm** para cifrado. Luego, el peer 2 de VPN con el que desea establecer el túnel IPSec también debe configurarse exactamente con los mismos valores.

De forma predeterminada, el secreto directo perfecto (PFS) está habilitado en los túneles IPSec para generar una clave más aleatoria. PFS hace esto realizando un intercambio de claves adicional durante la negociación de SA IPSec, genera un nuevo secreto compartido y lo combina en las nuevas claves de SA IPSec. Al configurar PFS, asegúrese de que ambos peers VPN tengan la misma configuración de PFS. Cualquier fallo en la negociación de SA de IPSec resultará en la imposibilidad de establecer el túnel IPSec.

- [PAN-OS 10.1 y posteriores y Prisma Access \(Gestionado por Panorama\)](#)
- [Prisma Access \(Gestión de la nube\)](#)

## Configuración de un túnel de IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>Prisma Access (El modo de transporte de túnel IPSec todavía no es compatible con Prisma Access)</li> <li>PAN-OS</li> </ul>	No se requiere licencia

IPSec es un conjunto de protocolos utilizados para proteger las comunicaciones entre peers. En IPSec, puede configurar varios ajustes, como algoritmos de cifrado y autenticación y tiempos de espera de asociaciones de seguridad. Una de esas configuraciones es el modo IPSec: modo túnel o modo transporte.

Mientras configura un túnel IPSec, puede seleccionar el modo IPSec como túnel o modo de transporte para establecer una conexión segura. Es decir, puede seleccionar si cifrar o autenticar paquetes en [modo túnel](#) o [modo transporte](#). PAN-OS<sup>®</sup> es compatible con el modo túnel de forma predeterminada, autenticando o cifrando los datos (paquete IP) a medida que atraviesan el túnel. A partir de PAN-OS 11.0.0, puede utilizar el modo transporte.

### Diferencias entre modo túnel y de transporte

Modo de túnel	modo transporte
Cifra todo el paquete, incluido el encabezado IP. Se agrega un nuevo encabezado IP al paquete después del cifrado.	Cifra solo la carga útil, mientras que se conserva el encabezado IP original.
La supervisión del túnel utiliza la dirección IP de la interfaz del túnel.	La supervisión del túnel utiliza automáticamente la dirección IP de la interfaz física (dirección IP de la interfaz de la puerta de enlace) y la dirección IP de la interfaz del túnel se ignora.
Soporta doble encapsulación.	No hay soporte para doble encapsulación.
Este modo se usa comúnmente para comunicaciones de sitio a sitio.	Este modo se usa comúnmente para comunicaciones de host a host.

## Configurar un túnel IPSec (modo túnel)

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>Prisma Access</li> <li>PAN-OS</li> </ul>	No se requiere licencia

La configuración de los túneles de IPSec permite autenticar o cifrar los datos (paquetes de IP) cuando los atraviesan.

Si está configurando el cortafuegos para que funcione con un peer compatible con una VPN basada en políticas, debe definir los ID del proxy. Los dispositivos compatibles con VPN basadas en políticas usan reglas/políticas o listas de acceso de seguridad específicas (direcciones de origen, direcciones de destino y puertos) para permitir el tráfico interesante a través de un túnel IPSec. Se hace referencia a estas reglas durante la negociación IKE de fase 2 o modo rápido y se intercambian como ID de proxy en el primer o segundo mensaje del proceso. Por lo tanto, si configura el cortafuegos para que funcione con un peer de VPN basada en políticas, para que la negociación de fase 2 sea correcta, debe definir el ID del proxy, de modo que ambos peers tengan la misma configuración. Si el ID del proxy no está configurado porque el cortafuegos admite VPN basadas en rutas, se utiliza como tal los valores predeterminados siguientes: IP de origen: 0.0.0.0/0, ip de destino: 0.0.0.0/0 y aplicación: cualquiera; y cuando estos valores se intercambian con el peer, se produce un fallo al configurar la conexión VPN.

Para establecer un túnel IPSec correctamente, las negociaciones de IKE e IPSec deberán ser correctas:

- La negociación de IKE solo se realizará correctamente cuando ambos peers VPN intercambien los mismos parámetros de IKE configurados.
- La negociación de IPSec solo se realizará correctamente cuando ambos peers VPN intercambien los mismos parámetros de IPSec configurados.
- [\(PAN-OS 10.1 y posterior\)](#)
- [#unique\\_43](#)
- [#unique\\_44](#)

## Configurar un túnel IPSec (modo transporte)

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"><li>• PAN-OS</li></ul>	No se requiere licencia

El modo de transporte es nuevo a partir de la versión 11.0.0 de PAN-OS y admite:

- Solo dirección IPv4.
- Solo protocolo de carga útil de seguridad encapsulada (ESP).
- IKEv2 solamente.
- DH-grupo 20 para el grupo Diffie-Hellman (DH) y PFS.
- Solo AES con claves de 256 bits en modo GCM.

Puede elegir el modo IPSec según sus requisitos de red:

- Si desea cifrar los paquetes del protocolo del plano de gestión (como BGP) intercambiados entre el cortafuegos de próxima generación y el punto de conexión del túnel, debe configurar el modo de transporte IPSec. El modo transporte le permite cifrar el tráfico de control (como el protocolo de enrutamiento y los mensajes de señalización) con el protocolo más sólido. Con el modo transporte puede cifrar el tráfico punto a punto que pertenece a la dirección IP del cortafuegos.
- Si desea cifrar el tráfico del plano de datos intercambiado entre el cortafuegos de nueva generación y el endpoint del túnel, debe configurar el modo de túnel IPSec.

Puntos importantes a recordar antes de habilitar el modo transporte:

- No se puede seleccionar el modo de transporte cuando NAT-T está habilitado.
- No se puede configurar una puerta de enlace IKE en una interfaz de bucle invertido en un túnel IPSec con modo de transporte.
- El modo de transporte IPSec no utiliza la configuración de ID de proxy para la negociación. Por lo tanto, no puede configurar un ID de proxy en modo de transporte. Si intenta configurar el ID de proxy usando otro método, este se reemplazará por 0.0.0.0/0 de forma automática.
- Puede usar el modo transporte solo con un intercambio de clave **automático**.
- Si configura una puerta de enlace IKE sin un túnel IPSec, de manera predeterminada, IKE negocia una asociación de seguridad (SA) secundaria en modo túnel.
- En el modo de transporte IPSec sin encapsulación GRE, no enrute el tráfico de usuario a través de la interfaz de túnel asociada. Configure los protocolos de control (por ejemplo, sesiones de peering BGP) en una interfaz física (por ejemplo, ethernet1/1) en lugar de una interfaz de túnel. Mientras que el modo túnel IPSec para rutas BGP funciona con la interfaz de túnel, el modo transporte IPSec para rutas BGP funciona solo con la interfaz física.
- De forma predeterminada, el túnel IPSec funciona en modo **Tunnel (Túnel)**.
- Debe habilitar **Add GRE Encapsulation (Agregar encapsulación GRE)** en el modo **transporte** para encapsular paquetes de multidifusión.

Dado que PAN-OS 10.2 y las versiones anteriores no son compatibles con el modo transporte, cualquier cambio a versiones anteriores generará problemas de compatibilidad. Antes de degradar, debe eliminar manualmente cualquier túnel de modo transporte o cambiar al modo túnel. De lo contrario, la degradación resultará en un fracaso.

- [\(PAN-OS 11.0 y posterior\)](#)

# Supervise su túnel VPN IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"><li>• PAN-OS</li></ul>	No requiere licencia

Para ofrecer un servicio VPN ininterrumpido, puede usar la capacidad Detección de fallo del peer junto con la capacidad de supervisión del túnel en el cortafuegos. También puede supervisar el estado del túnel. Estas tareas de supervisión se describen en las siguientes secciones:

- [Definición de un perfil de supervisión de túnel](#)
- [Ver el estado del túnel](#)

Para solucionar problemas, puede implementar la [Habilitación/deshabilitación, actualización o reinicio de un puerto de enlace de KE o túnel IPSec](#).

## Definición de un perfil de supervisión de túnel

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Un perfil de supervisión de túnel le permite verificar la conectividad entre los peers VPN; puede configurar la interfaz de túnel para hacer ping a una dirección IP de destino con un intervalo determinado y especificar la acción si la comunicación a través del túnel está cortada.

**STEP 1 |** Seleccione **Network (Red) > Network Profiles (Perfiles de red) > Monitor (Supervisar)**. Hay un perfil de supervisión de túnel disponible para su uso.

**STEP 2 |** Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para el perfil.

**STEP 3 |** Seleccione la **Action (Acción)** que se realizará si no es posible alcanzar la dirección IP de destino.

- **Esperar recuperación:** El cortafuegos espera a que el túnel se recupere. Continúa usando la interfaz del túnel para las decisiones de enrutamiento como si el túnel siguiera activo.
- **Conmutación por error:** Desvía el tráfico a una ruta alternativa si hay alguna disponible. El cortafuegos deshabilita la interfaz del túnel y, por lo tanto, deshabilita cualquier ruta en la tabla de rutas que use la interfaz.

En ambos casos, el cortafuegos intenta acelerar la recuperación negociando nuevas claves IPSec.

**STEP 4 |** Especifique el **Interval (sec) (Intervalo [s])** y el **Threshold (Umbral)** para iniciar la acción especificada.

- El **Threshold (Umbral)** especifica el número de latidos que se perderán antes de que el cortafuegos realice la acción especificada (rango: 2 a 100; valor predeterminado: 5).
- **Interval (sec) (Intervalo [s])** especifica el tiempo (en segundos) entre latidos (rango: 2 a 10; valor predeterminado: 3).

**STEP 5 |** Adjunte el perfil de supervisión a la configuración de túnel IPSec. Consulte [Habilitación de la supervisión de túnel](#).

## Ver el estado del túnel

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>• PAN-OS</li> <li>• Cloud Management</li> </ul>	<ul style="list-style-type: none"> <li>❑ No se requiere licencia</li> <li>❑ AIOps para licencia NGFW Premium</li> </ul>

El estado del túnel informa si se han establecido las SA IKE de fase 1 y de fase 2 válidas, y de si está operativa la interfaz del túnel para el paso de tráfico.

Debido a que la interfaz del túnel es una interfaz lógica, no puede indicar el estado de un enlace físico. Por lo tanto, debe habilitar la supervisión de túnel para que la interfaz del túnel pueda verificar la conectividad a una dirección IP y determinar si la ruta sigue siendo utilizable. Si no se puede alcanzar la dirección IP, el cortafuegos esperará a la recuperación del túnel o una conmutación por error. Cuando se produce una conmutación por error, se anula el túnel existente y se inician cambios de enrutamiento para establecer un nuevo túnel y redirigir el tráfico.

- [PAN-OS](#)
- [Gestión de la nube](#)

## Ver el estado del túnel VPN IPsec

**STEP 1** | Seleccione **Network (Red) > IPsec Tunnels (Túneles IPsec)**.

**STEP 2** | Visualización del **Tunnel Status (Estado de túnel)**

- El color verde indica que el túnel de la SA IPsec es válido.
- El color rojo indica que la SA IPsec no está disponible o que ha caducado.

**STEP 3** | Vea el **IKE Gateway Status (Estado de la puerta de enlace de IKE)**.

- El color verde indica que la SA IKE de fase 1 es válida.
- El color rojo indica que la SA IKE de fase 1 no está disponible o ha caducado.

**STEP 4** | Vea el **Tunnel Interface Status (Estado de la interfaz del túnel)**

- El color verde indica que la interfaz del túnel está activa.
- El color rojo indica que la interfaz de túnel no está activa porque la supervisión del túnel está habilitada y el estado es desactivado.

Para solucionar problemas de un túnel VPN que aún no está activo, consulte [Interpretación de mensajes de error de VPN](#).

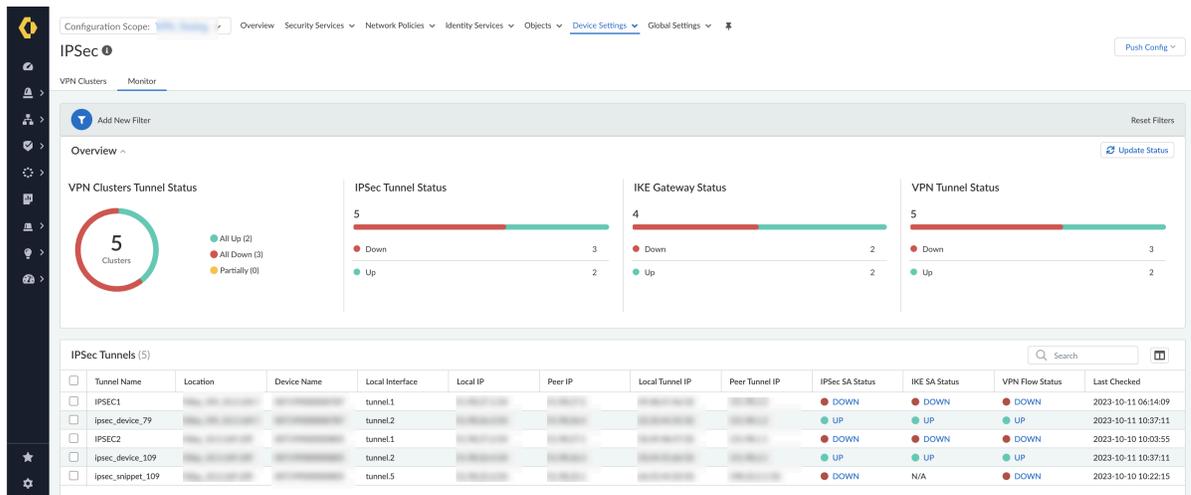
## Ver el estado del túnel VPN IPsec

**STEP 1** | Inicie sesión en Strata Cloud Manager.

**STEP 2 |** Seleccione **Manage (Gestionar) > Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access) > Device Settings (Configuración de dispositivo) > IPSec Tunnels (Túneles IPSec)** y seleccione **Monitor (Supervisar)**.

**STEP 3 |** Seleccione el **Configuration Scope (Ámbito de configuración)** para ver el estado del túnel VPN IPSec. Puede seleccionar una carpeta o cortafuegos de sus **Folders (Carpetas)** para supervisar el túnel VPN IPSec que creó en los cortafuegos:

- Para ver el estado de los túneles IPSec en todos los cortafuegos, seleccione la carpeta **All Firewalls (Todos los cortafuegos)**.
  - Para ver el estado de los túneles IPSec para el grupo de cortafuegos asociados con una carpeta, seleccione la carpeta específica.
  - Para ver el estado de los túneles IPSec en un cortafuegos específico, seleccione el cortafuegos.
-  • *Si ha creado el clúster VPN utilizando AutoVPN, no podrá supervisar el estado del túnel IPSec de dichos cortafuegos.*
- *Puede supervisar solo los cortafuegos locales y no los componentes gestionados por Prisma Access.*
  - *La supervisión está deshabilitada a nivel Global y de fragmento. Por lo tanto, puede crear un túnel IPSec en el ámbito de configuración global o de fragmento, pero puede supervisar el túnel IPSec solo en el nivel de carpeta o cortafuegos.*



Tunnel Name	Location	Device Name	Local Interface	Local IP	Peer IP	Local Tunnel IP	Peer Tunnel IP	IPSec SA Status	IKE SA Status	VPN Flow Status	Last Checked
IPSEC1			tunnel.1					DOWN	DOWN	DOWN	2023-10-11 06:14:09
ipsec_device_79			tunnel.2					UP	UP	UP	2023-10-11 10:37:11
IPSEC2			tunnel.1					DOWN	DOWN	DOWN	2023-10-10 10:03:55
ipsec_device_109			tunnel.2					UP	UP	UP	2023-10-11 10:37:11
ipsec_snippet_109			tunnel.5					DOWN	N/A	DOWN	2023-10-10 10:22:15

**STEP 4 |** Vea el **VPN Cluster Tunnel Status (Estado del túnel del clúster VPN)** que proporciona la representación gráfica del número de túneles que están activos, el número de túneles que están inactivos y el número de túneles que están parcialmente activos.

**STEP 5 |** Ver el **IPsec SA Status (Estado de SA de IPsec)** en **IPsec Tunnels (Túneles IPsec)**.

- El color verde [**UP (ARRIBA)**] indica un túnel de la SA IPsec válido. Seleccione **ARRIBA** para ver información detallada sobre el túnel IPsec.
- El color rojo [**DOWN (ABAJO)**] indica que la SA de IPsec no está disponible o ha caducado. Seleccione **ABAJO** para ver la información detallada para interpretar el motivo del error.

**STEP 6 |** Ver el **IKE SA Status (Estado SA de IKE)** en los **IPsec Tunnels (Túneles IPsec)**.

- El color verde [**UP (ARRIBA)**] indica una SA IKE de fase 1 válida. Seleccione **ARRIBA** para ver información detallada sobre la puerta de enlace IKE.
- El color rojo [**DOWN (ABAJO)**] indica que la SA IKE de fase 1 no está disponible o ha vencido. Seleccione **ABAJO** para ver la información detallada para interpretar el motivo del error.

**STEP 7 |** Vea el **VPN Flow Status (Estado del flujo de VPN)** para obtener información sobre el flujo de tráfico de VPN en **IPsec Tunnels (Túneles IPsec)**.

- El color verde [**UP (ARRIBA)**] indica que el túnel IPsec está activo. Seleccione **ARRIBA** para ver información detallada sobre el flujo de tráfico de VPN.
- El color rojo [**DOWN (ABAJO)**] indica que el túnel IPsec está inactivo. Seleccione **ABAJO** para ver la información detallada para interpretar el motivo del error.

**STEP 8 |** Seleccione **Add New Filter (Añadir nuevo filtro)**  y seleccione el campo para ver los resultados según el campo seleccionado. Por ejemplo, **Add New Filter (Añadir nuevo filtro)** seleccionando el **Device Name (Nombre del dispositivo)** de la lista para ver el estado del túnel IPsec para el dispositivo seleccionado.

Seleccione **Reset Filters (Restablecer filtros)**  para eliminar uno o más filtros.

**STEP 9 |** Seleccione **Update Status (Actualizar estado)** para actualizar todos los datos de supervisión del túnel IPsec presentes en ese nivel (cortafuegos, carpeta o todos los cortafuegos).

## Habilitación, deshabilitación, actualización o reinicio de una puerta de enlace IKE o túnel IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Puede habilitar, deshabilitar, actualizar o reiniciar una puerta de enlace IKE o túnel de VPN para facilitar la resolución de problemas.

- [Habilitación o deshabilitación de una puerta de enlace de IKE o un túnel IPSec](#)
- [Actualización o reinicio de una puerta de enlace IKE o túnel IPSec](#)

## Habilitación o deshabilitación de una puerta de enlace de IKE o un túnel IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No requiere licencia

Habilite o deshabilite una puerta de enlace de IKE o túnel IPSec para facilitar la resolución de problemas.

- Habilite o deshabilite una puerta de enlace IKE.
  - Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Gateways (Puertas de enlace de IKE)** y seleccione la puerta de enlace que desea habilitar o deshabilitar.
  - En la parte inferior de la pantalla, haga clic en **Enable** o **Disable**.
- Habilite o deshabilite un túnel IPSec.
  - Seleccione **Network (Red) > IPSec Tunnels (Túneles IPSec)** y seleccione el túnel que desea habilitar o deshabilitar.
  - En la parte inferior de la pantalla, haga clic en **Enable** o **Disable**.

## Actualización o reinicio de una puerta de enlace IKE o túnel IPSec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Puede actualizar o reiniciar una puerta de enlace IKE o un túnel IPSec. Los comportamientos de actualizar y reiniciar para un gateway IKE y túnel IPSec son los siguientes:

Fase	Actualizar	Reiniciar
Puerta de enlace IKE (IKE de fase 1)	<p>Actualiza las estadísticas en pantalla para la puerta de enlace IKE seleccionada.</p> <p>Equivale a emitir un segundo comando <b>show</b> en el CLI (tras un comando <b>show</b> inicial).</p>	<p>Reinicia la puerta de enlace IKE seleccionada.</p> <p><b>IKEv2:</b> También reinicia cualquier asociación de seguridad (SA) IPSec secundaria.</p> <p><b>IKEv1:</b> No reinicia las SA IPSec asociadas.</p> <p>Un reinicio interrumpe todas las sesiones existentes.</p> <p>Equivale a emitir una secuencia de comandos <b>clear, test, show</b> en la CLI.</p>
Túnel IPSec (IKE de fase 2)	<p>Actualiza las estadísticas en pantalla para el túnel IPSec seleccionado.</p> <p>Equivale a emitir un segundo comando <b>show</b> en el CLI (tras un comando <b>show</b> inicial).</p>	<p>Reinicia el túnel IPSec.</p> <p>Un reinicio interrumpe todas las sesiones existentes.</p> <p>Equivale a emitir una secuencia de comandos <b>clear, test, show</b> en la CLI.</p>

Tenga en cuenta que el resultado de reiniciar una puerta de enlace IKE depende de si se trata de IKEv1 o IKEv2.

- Actualice o reinicie una puerta de enlace IKE.
  1. Seleccione **Network (Red) > IPSec Tunnels (Túneles IPSec)** y seleccione el túnel para la puerta de enlace que desea actualizar o reiniciar.
  2. En la fila correspondiente a ese túnel, en la columna Status, haga clic en **IKE Info**.
  3. En la parte inferior de la pantalla Info IKE, haga clic en la acción que desea:
    - **Refresh:** actualiza las estadísticas en pantalla.
    - **Restart (Reiniciar):** borra las SA, de modo que el tráfico se descarta hasta que se inicie la negociación IKE de nuevo y se vuelva a crear el túnel.

- Actualice o reinicie un túnel IPSec.

Puede determinar que es necesario actualizar o reiniciar el túnel porque usa la supervisión de túneles para supervisar el estado del túnel, o usa un supervisor de red externo para supervisar la conectividad de red a través del túnel IPSec.

1. Seleccione **Network (Red) > IPSec Tunnels (Túneles IPSec)** y seleccione el túnel que desea actualizar o reiniciar.
2. En la fila de ese túnel, en la columna Status, haga clic en **Tunnel Info**.
3. En la parte inferior de la pantalla Información de túnel, haga clic en la acción que desea:
  - **Refresh (Actualizar)**: actualiza las estadísticas en pantalla.
  - **Restart (Reiniciar)**: borra las SA, de modo que el tráfico se descarta hasta que se inicie la negociación IKE de nuevo y se vuelva a crear el túnel.

# Ejemplos de configuración de VPN de sitio a sitio

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"><li>• PAN-OS</li></ul>	No se requiere licencia

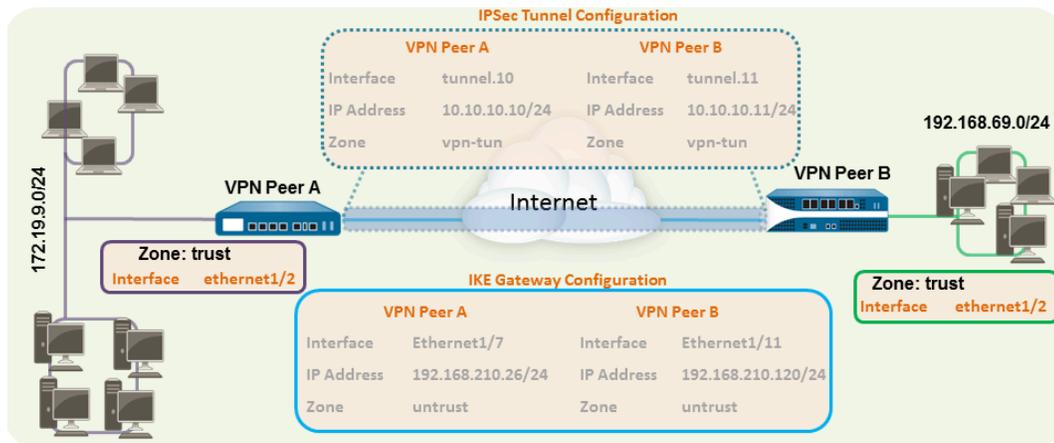
En las siguientes secciones se proporcionan instrucciones detalladas para configurar algunas implementaciones globales de VPN:

- [VPN de sitio a sitio con rutas estáticas](#)
- [VPN de sitio a sitio con OSPF](#)
- [VPN de sitio a sitio con rutas estáticas y enrutamiento dinámico](#)

## VPN de sitio a sitio con rutas estáticas

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Los siguientes ejemplos muestran una conexión VPN entre dos sitios que usan rutas estáticas. Sin enrutamiento dinámico, las interfaces de túnel en el peer A de la VPN y el peer B de la VPN no necesitan una dirección IP porque el cortafuegos usa automáticamente la interfaz del túnel como el próximo salto para el enrutamiento de tráfico a través de los sitios. Sin embargo, para habilitar la supervisión del túnel, se ha asignado una dirección IP estática a cada interfaz de túnel.



**STEP 1** | Configure una interfaz de capa 3.

Esta interfaz se usa para el túnel IKE de fase 1.

1. Seleccione **Network (Red) > Interfaces > Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la VPN.
2. Seleccione **Layer3 (Capa 3)** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
  - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
  - Si todavía no ha creado la zona, seleccione **New Zone (Nueva zona)** en **Security Zone (Zona de seguridad)**, defina un nombre para la zona en **Name (Nombre)** y, a continuación, haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.210.26/24.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** ethernet1/7
- **Security Zone (Zona de seguridad):** untrust (no fiable)
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 192.168.210.26/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** ethernet1/11
- **Security Zone (Zona de seguridad):** untrust (no fiable)
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 192.168.210.120/24

**STEP 2 |** Cree una interfaz de túnel y vincúlela a un enrutador virtual y una zona de seguridad.

1. Seleccione **Network (Red) > Interfaces > Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.1**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:
  - Si desea usar la zona de confianza como punto de finalización del túnel, selecciónela.
  - **(Recomendado)** Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Name (Nombre)** para una nueva zona, por ejemplo *vpn-tun*, y haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. **(Opcional)** Asigne una dirección IP a la interfaz de túnel, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz.

Con rutas estáticas, la interfaz del túnel no requiere una dirección IP. Para el tráfico destinado a una subred/dirección IP específica, la interfaz de túnel se convertirá automáticamente en el próximo salto. Plántese añadir una dirección IP si quiere habilitar la supervisión de túnel.

6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** tunnel.10 (túnel.10)
- **Zona de seguridad:** vpn\_tun
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 172.19.9.2/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** tunnel.11 (túnel.11)
- **Zona de seguridad:** vpn\_tun
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 192.168.69.2/24

**STEP 3 |** Configure una ruta estática, en el servidor virtual, a la subred de destino.

1. Seleccione **Network (Red) > Virtual Router (Enrutador virtual)** y haga clic en el enrutador que ha definido en el paso anterior.
2. Seleccione **Ruta estática**, haga clic en **Añadir** e introduzca una nueva ruta para acceder a la subred que se encuentra en el otro extremo del túnel.

En este ejemplo, la configuración para el peer A de VPN es:

- **Destino:** 192.168.69.0/24
- **Interface (Interfaz):** tunnel.10 (túnel.10)

La configuración para el peer B de VPN es:

- **Destino:** 172.19.9.0/24
- **Interface (Interfaz):** tunnel.11 (túnel.11)

**STEP 4 |** Configure los perfiles criptográficos (perfil criptográfico IKE para la fase 1 y perfil criptográfico IPSec para fase 2).

Complete esta tarea en ambos peers y asegúrese de definir valores idénticos.

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Crypto (Criptográfico de IKE)**. En este ejemplo, hemos usado el perfil predeterminado.
2. Seleccione **Red (Network) > Network Profiles (Perfiles de red) > IPSec Crypto (Criptográfico de IPSec)**. En este ejemplo, hemos usado el perfil predeterminado.

**STEP 5 |** Configure la puerta de enlace IKE.

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Gateway (Puerta de enlace de IKE)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** ethernet1/7
  - **Dirección IP local:** 192.168.210.26/24
  - **Tipo/Dirección IP del peer:** estática/192.168.210.120
  - **Claves previamente compartidas:** introduzca un valor
  - **Local identification (Identificación local):** None (Ninguna); significa que la dirección IP local se utilizará como el valor de identificación local.
- La configuración para el peer B de VPN es:
- **Interface (Interfaz):** ethernet1/11
  - **Local IP address (Dirección IP local):** 192.168.210.120/24
  - **Tipo/Dirección IP del peer:** estática/192.168.210.26
  - **Claves previamente compartidas:** introduzca el mismo valor que el del peer A
  - **Identificación local:** ninguna
3. Seleccione **Opciones de fase 1 avanzadas** y seleccione el perfil criptográfico de IKE que ha creado anteriormente para usar IKE de fase 1.

**STEP 6 |** Configure el túnel IPsec.

1. Seleccione **Network (Red) > IPsec Tunnels (Túneles IPsec)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Tunnel Interface (Interfaz del túnel):** tunnel.10 (túnel.10)
- **Type (Tipo):** Auto Key (Clave automática)
- **IKE Gateway (Puerta de enlace de IKE):** seleccione la puerta de enlace de IKE definida más arriba.
- **IPsec Crypto Profile (Perfil criptográfico de IPsec):** seleccione el perfil Criptográfico de IPsec definido en el paso 4.

La configuración para el peer B de VPN es:

- **Tunnel Interface (Interfaz de túnel):** tunnel.11 (túnel.11)
  - **Type (Tipo):** Auto Key (Clave automática)
  - **IKE Gateway (Puerta de enlace de IKE):** seleccione la puerta de enlace de IKE definida más arriba.
  - **IPsec Crypto Profile (Perfil criptográfico de IPsec):** seleccione el perfil criptográfico de IPsec definido en el paso 4.
3. **(Opcional)** Seleccione **Show Advanced Options (Mostrar opciones avanzadas)**, seleccione **Tunnel Monitor (Supervisor de túnel)** y especifique una dirección IP de destino para hacer ping y verificar la conectividad. Normalmente, se usa la dirección IP de la interfaz de túnel del peer de VPN.
  4. **(Opcional)** Para definir la acción que se realizará si no es posible establecer conectividad, consulte [Definición de un perfil de supervisión de túnel](#).

**STEP 7 |** Cree reglas de políticas para permitir el tráfico entre los sitios (subredes).

1. Seleccione **Policies (Políticas) > Security (Seguridad)**.
2. Cree reglas para permitir el tráfico entre la zona no fiable y la zona vpn-tun y la zona vpn-tun y la zona no fiable para tráfico que se origine desde el origen especificado y las direcciones IP de destino.

**STEP 8 |** Confirme cualquier cambio de configuración pendiente.

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

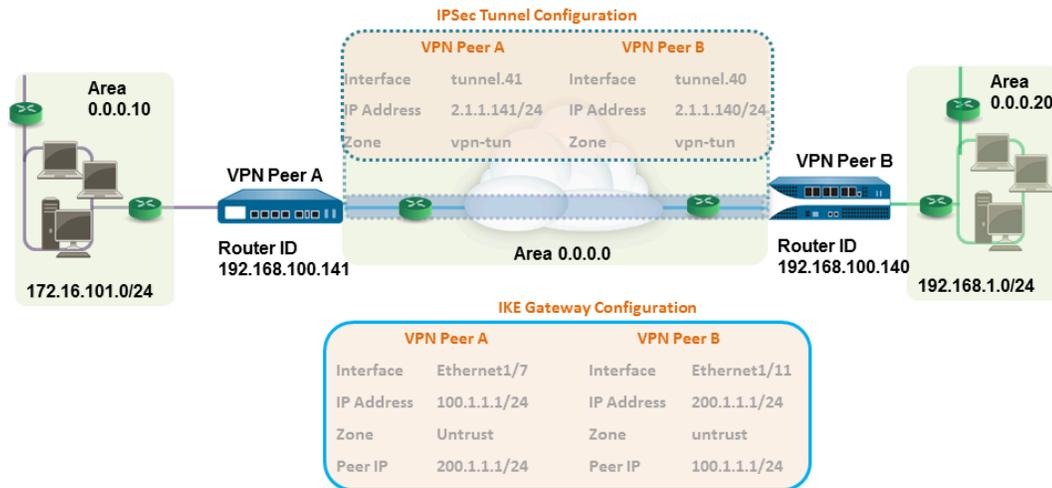
**STEP 9 |** [Prueba de conectividad VPN](#).

Consulte también [Ver el estado del túnel](#).

## VPN de sitio a sitio con OSPF

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

En este ejemplo, cada sitio usa OSPF para enrutamiento o tráfico dinámicos. La dirección IP del túnel en cada peer de VPN se asigna estáticamente y sirve como el próximo salto para el enrutamiento de tráfico entre dos sitios.



**STEP 1 |** Configure las interfaces de capa 3 en cada cortafuegos.

1. Seleccione **Network (Red) > Interfaces > Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la VPN.
2. Seleccione **Layer3 (Capa 3)** en la lista **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
  - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
  - Si todavía no ha creado la zona, seleccione **New Zone (Nueva zona)** en la lista **Security Zone (Zona de seguridad)**, defina un nombre para la nueva zona en **Name (Nombre)** y, a continuación, haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.210.26/24.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** ethernet1/7
- **Security Zone (Zona de seguridad):** untrust (no fiable)
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 100.1.1.1/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** ethernet1/11
- **Security Zone (Zona de seguridad):** untrust (no fiable)
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 200.1.1.1/24

**STEP 2 |** Cree una interfaz de túnel y vincúlela a un enrutador virtual y una zona de seguridad.

1. Seleccione **Network (Red) > Interfaces > Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.11**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:
  - Si desea usar la zona de confianza como punto de finalización del túnel, selecciónela.
  - **(Recomendado)** Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Name (Nombre)** para la nueva zona, por ejemplo vpn-tun, y haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. Asigne una dirección IP a la interfaz de túnel, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Add** en la sección IP e introduzca la dirección IP y la máscara de red/prefijo para asignarlos a la interfaz; por ejemplo, 172.19.9.2/24.

Esta dirección IP se usará como dirección IP de próximo salto para enrutar el tráfico al túnel y también puede usarse para supervisar el estado del túnel.

6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** tunnel.41 (túnel.41)
- **Zona de seguridad:** vpn\_tun
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 2.1.1.141/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** tunnel.40 (túnel.10)
- **Zona de seguridad:** vpn\_tun
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 2.1.1.140/24

**STEP 3 |** Configure los perfiles criptográficos (perfil criptográfico IKE para la fase 1 y perfil criptográfico IPSec para fase 2).

Complete esta tarea en ambos peers y asegúrese de definir valores idénticos.

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Crypto (Criptográfico de IKE)**. En este ejemplo, hemos usado el perfil predeterminado.
2. Seleccione **Red (Network) > Network Profiles (Perfiles de red) > IPSec Crypto (Criptográfico de IPSec)**. En este ejemplo, hemos usado el perfil predeterminado.

**STEP 4 |** Establezca la configuración OSPF en el enrutador virtual y adjunte las áreas OSPF con las interfaces apropiadas en el cortafuegos.

Para obtener más información sobre las opciones OSPF disponibles en el cortafuegos, consulte [Configuración de OSPF](#).

Use Broadcast como el tipo de enlace cuando haya más de dos enrutadores OSPF que necesiten intercambiar información de enrutamiento.

1. Seleccione **Network (Red) > Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador predeterminado o añada uno nuevo.
2. Seleccione **OSPF** (para IPv4) u **OSPFv3** (para IPv6) y seleccione **Enable (Habilitar)**.
3. En este ejemplo, la configuración OSPF para el peer A de VPN es:
  - **Router ID (ID de enrutador):** 192.168.100.141
  - **Area ID (ID de área):** 0.0.0.0 que se asigna a la interfaz del túnel.1 con el tipo de enlace: p2p
  - **Area ID (ID de área):** 0.0.0.10 que se asigna a la interfaz Ethernet1/1 con el tipo de enlace: Broadcast

La configuración OSPF para el peer B de VPN es:

- **Router ID (ID de enrutador):** 192.168.100.140
- **Area ID (ID de área):** 0.0.0.0 que se asigna a la interfaz del túnel.1 con el tipo de enlace: p2p
- **Area ID (ID de área):** 0.0.0.20 que se asigna a la interfaz Ethernet1/15 con el tipo de enlace: Broadcast

**STEP 5 |** Configure la puerta de enlace IKE.

Este ejemplo utiliza direcciones IP estáticas para ambos peers VPN. Normalmente, las sedes usan una dirección IP configurada estáticamente y las sucursales pueden usar direcciones IP dinámicas; las direcciones IP dinámicas no son las más indicadas para configurar servicios estables como VPN.

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Gateway (Puerta de enlace de IKE)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** ethernet1/7
- **Local IP address (Dirección IP local):** 100.1.1.1/24
- **Dirección IP del peer:** 200.1.1.1/24
- **Claves previamente compartidas:** introduzca un valor

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** ethernet1/11
- **Dirección IP local:** 200.1.1.1/24
- **Peer IP address (Dirección IP del peer):** 100.1.1.1/24
- **Claves previamente compartidas:** introduzca el mismo valor que el del peer A

3. Seleccione el perfil criptográfico IKE que ha creado anteriormente para usar IKE de fase 1.

**STEP 6 |** Configure el túnel IPsec.

1. Seleccione **Network (Red) > IPsec Tunnels (Túneles IPsec)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Tunnel Interface (Interfaz de túnel):** tunnel.41 (túnel.41)
- **Type (Tipo):** Auto Key (Clave automática)
- **IKE Gateway (Puerta de enlace de IKE):** seleccione la puerta de enlace de IKE definida más arriba.
- **Perfil criptográfico de IPsec:** seleccione la puerta de enlace de IKE definida en más arriba.

La configuración para el peer B de VPN es:

- **Tunnel Interface (Interfaz de túnel):** tunnel.40 (túnel.40)
  - **Type (Tipo):** Auto Key (Clave automática)
  - **IKE Gateway (Puerta de enlace de IKE):** seleccione la puerta de enlace de IKE definida más arriba.
  - **Perfil criptográfico de IPsec:** seleccione la puerta de enlace de IKE definida en más arriba.
3. Seleccione **Mostrar opciones avanzadas**, seleccione **Supervisor de túnel** y especifique una dirección IP de destino para hacer ping para verificar la conectividad.
  4. Para definir la acción que se realizará si no es posible establecer conectividad, consulte [Definición de perfiles supervisión de túnel](#).

**STEP 7 |** Cree reglas de políticas para permitir el tráfico entre los sitios (subredes).

1. Seleccione **Policies (Políticas) > Security (Seguridad)**.
2. Cree reglas para permitir el tráfico entre la zona no fiable y la zona vpn-tun y la zona vpn-tun y la zona no fiable para tráfico que se origine desde el origen especificado y las direcciones IP de destino.

**STEP 8 |** Verifique las adyacencias OSPF y las rutas desde el CLI.

Verifique que ambos cortafuegos puedan verse entre sí con estado completo. Confirme además la dirección IP de la interfaz del túnel del peer de VPN y el ID del enrutador OSPF. Use los siguientes comandos del CLI con cada peer de VPN:

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
         N/P:NSSA option, MC:multicast, E:AS external LSA capability, T:TOS capability
=====
virtual router:          vr1
neighbor address:       2.1.1.140
local address binding:  0.0.0.0
type:                   dynamic
status:                 full
neighbor router ID:     192.168.100.140
area id:                0.0.0.0
neighbor priority:      1
lifetime remain:        39
messages pending:       0
LSA request pending:   0
options:                0x42: O E
hello suppressed:      no

admin@FW-B> show routing protocol ospf neighbor

Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
         N/P:NSSA option, MC:multicast, E:AS external LSA capability, T:TOS capability
=====
virtual router:          vr1
neighbor address:       2.1.1.141
local address binding:  0.0.0.0
type:                   dynamic
status:                 full
neighbor router ID:     192.168.100.141
area id:                0.0.0.0
neighbor priority:      1
lifetime remain:        39
messages pending:       0
LSA request pending:   0
options:                0x42: O E
hello suppressed:      no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2

VIRTUAL ROUTER: vr1 (id 1)
=====
destination      nexthop          metric flags    age  interface      next-AS
2.1.1.0/24       0.0.0.0          10  Oi             6760 tunnel.41
172.16.101.0/24 0.0.0.0          10  Oi             6854 ethernet1/1
192.168.1.0/24   2.1.1.140       20  A Oo           6754 tunnel.40
total routes shown: 3

admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2

VIRTUAL ROUTER: vr1 (id 1)
=====
destination      nexthop          metric flags    age  interface      next-AS
2.1.1.0/24       0.0.0.0          10  Oi             20033 tunnel.40
172.16.101.0/24 2.1.1.141        20  AOo            6896 tunnel.40
192.168.1.0/24   0.0.0.0          10  Oi             8058 ethernet1/15
total routes shown: 3
```

**STEP 9** | Prueba de conectividad VPN.

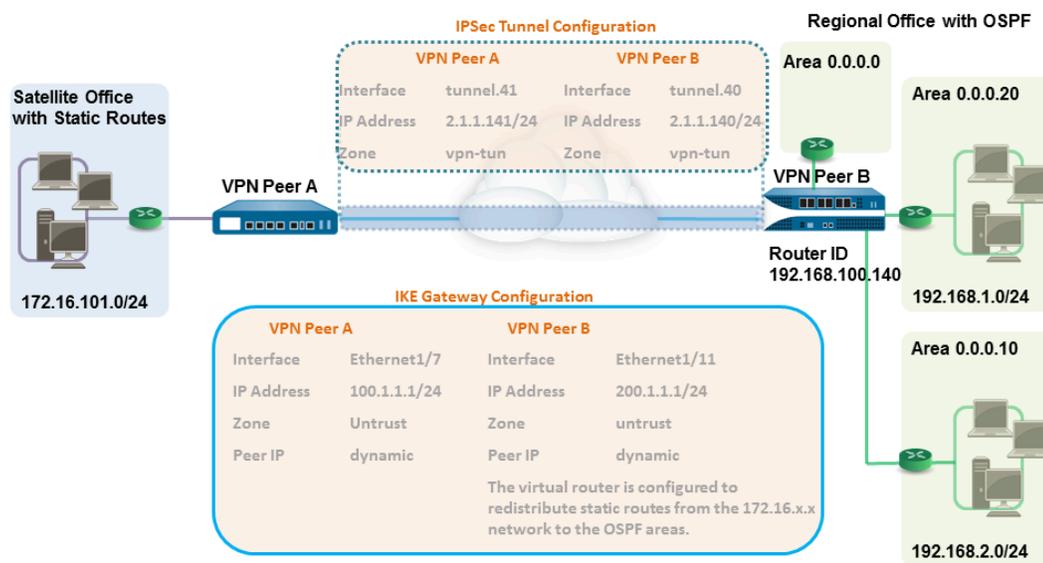
Consulte [Configuración de la supervisión del túnel](#) y [Ver el estado del túnel](#).

## VPN de sitio a sitio con rutas estáticas y enrutamiento dinámico

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

En este ejemplo, un sitio usa rutas estáticas y el otro sitio usa OSPF. Cuando el protocolo de enrutamiento no es el mismo entre ubicaciones, la interfaz del túnel en cada cortafuegos debe configurarse con una dirección IP estática. A continuación, permita el intercambio de información de enrutamiento, el cortafuegos que participa tanto en el proceso de enrutamiento estático como el dinámico debe configurarse con un Perfil de redistribución. Configurar el perfil de redistribución habilita al enrutador virtual para redistribuir y filtrar rutas entre protocolos (rutas estáticas, rutas conectadas y hosts) desde el sistema autónomo estático al sistema autónomo OSPF. Sin este perfil de redistribución, cada protocolo funciona por su cuenta y no intercambia ninguna información de ruta con otros protocolos que se ejecutan en el mismo enrutador virtual.

En este ejemplo, la oficina satélite tiene rutas estáticas y todo el tráfico destinado a la red 192.168.x.x se enruta al túnel .41. El enrutador virtual del peer B de VPN participa tanto en el proceso de enrutamiento dinámico como el estático y está configurado como un perfil de redistribución para propagar (exportar) las rutas estáticas al sistema autónomo OSPF.



**STEP 1 |** Configure las interfaces de capa 3 en cada cortafuegos.

1. Seleccione **Network (Red) > Interfaces > Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la VPN.
2. Seleccione **Layer3 (Capa 3)** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
  - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
  - Si todavía no ha creado la zona, seleccione **New Zone (Nueva zona)** en **Security Zone (Zona de seguridad)**, defina un nombre para la zona en **Name (Nombre)** y, a continuación, haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.210.26/24.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** ethernet1/7
- **Security Zone (Zona de seguridad):** untrust (no fiable)
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 100.1.1.1/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** ethernet1/11
- **Security Zone (Zona de seguridad):** untrust (no fiable)
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 200.1.1.1/24

**STEP 2 |** Configure los perfiles criptográficos (perfil criptográfico IKE para la fase 1 y perfil criptográfico IPSec para fase 2).

Complete esta tarea en ambos peers y asegúrese de definir valores idénticos.

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Crypto (Criptográfico de IKE)**. En este ejemplo, hemos usado el perfil predeterminado.
2. Seleccione **Red (Network) > Network Profiles (Perfiles de red) > IPSec Crypto (Criptográfico de IPSec)**. En este ejemplo, hemos usado el perfil predeterminado.

**STEP 3** | Configure la puerta de enlace IKE.

Con claves compartidas previamente, para añadir el escrutinio de autenticación al configurar el túnel IKE de fase 1, puede configurar atributos de identificación de peer y local, y un valor correspondiente con el que coincide en el proceso de negociación.

1. Seleccione **Network (Red) > Network Profiles (Perfiles de red) > IKE Gateway (Puerta de enlace de IKE)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** ethernet1/7
- **Local IP address (Dirección IP local):** 100.1.1.1/24
- **Tipo de IP de peer:** dinámica
- **Claves previamente compartidas:** introduzca un valor
- **Local identification (Identificación local):** seleccione **FQDN(hostname) (FQDN [nombre de host])** e introduzca un valor para el peer A de VPN.
- **Peer identification (Identificación del peer):** seleccione **FQDN(hostname) (FQDN [nombre de host])** e introduzca un valor para el peer B de VPN.

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** ethernet1/11
  - **Dirección IP local:** 200.1.1.1/24
  - **Peer IP address (Dirección IP de peer):** dynamic (dinámica)
  - **Claves previamente compartidas:** introduzca el mismo valor que el del peer A
  - **Identificación local:** seleccione **FQDN(nombre de host)** e introduzca un valor para el peer B de VPN.
  - **Identificación del peer:** seleccione **FQDN(nombre de host)** e introduzca un valor para el peer A de VPN.
3. Seleccione el perfil criptográfico IKE que ha creado anteriormente para usar IKE de fase 1.

**STEP 4 |** Cree una interfaz de túnel y vincúlela a un enrutador virtual y una zona de seguridad.

1. Seleccione **Network (Red) > Interfaces > Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, p. ej., **.41**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:
  - Si desea usar la zona de confianza como punto de finalización del túnel, selecciónela.
  - **(Recomendado)** Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Name (Nombre)** para la nueva zona, por ejemplo *vpn-tun*, y haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. Asigne una dirección IP a la interfaz de túnel, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Add** en la sección IP e introduzca la dirección IP y la máscara de red/prefijo para asignarlos a la interfaz; por ejemplo, 172.19.9.2/24.

Esta dirección IP se usará para enrutar el tráfico al túnel y supervisar el estado del túnel.

6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz):** tunnel.41 (túnel.41)
- **Zona de seguridad:** vpn\_tun
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 2.1.1.141/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz):** tunnel.42 (túnel.42)
- **Zona de seguridad:** vpn\_tun
- **Virtual Router (Enrutador virtual):** default (predeterminado)
- **IPv4:** 2.1.1.140/24

**STEP 5 |** Especifique la interfaz para enrutar el tráfico a un destino en la red 192.168.x.x.

1. En el peer A de VPN, seleccione el enrutador virtual.
2. Seleccione **Static Routes (Rutas estáticas)** y **Add (Añadir)** para añadir túnel.41 como la **Interface (Interfaz)** para el enrutamiento de tráfico con un **Destination (Destino)** en la red 192.168.x.x.

**STEP 6 |** Establezca la ruta estática y la configuración OSPF en el enrutador virtual y adjunte las áreas OSPF con las interfaces apropiadas en el cortafuegos.

1. En el peer B de VPN, seleccione **Network (Red) > Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador predeterminado o añada uno nuevo.
2. Seleccione **Static Routes (Rutas estáticas)** y **Add (Añadir)** para añadir la dirección IP del túnel como el próximo salto para el tráfico en la red 172.168.x.x.

Asigne la métrica de ruta deseada; el uso de un valor más bajo aumenta la prioridad para la selección de ruta en la tabla de reenvíos.

3. Seleccione **OSPF** (para IPv4) u **OSPFv3** (para IPv6) y seleccione **Enable (Habilitar)**.
4. En este ejemplo, la configuración OSPF para el peer B de VPN es:

- ID del enrutador: 192.168.100.140
- ID de área: 0.0.0.0 se asigna a la interfaz Ethernet1/12 con el tipo de enlace: Broadcast
- ID de área: 0.0.0.10 que se asigna a la interfaz Ethernet1/1 con el tipo de enlace: Broadcast
- ID de área: 0.0.0.20 se asigna a la interfaz Ethernet1/15 con el tipo de enlace: Broadcast

**STEP 7 |** Cree un perfil de redistribución para inyectar las rutas estáticas en el sistema autónomo OSPF.

1. Cree un perfil de redistribución en el peer B de VPN.
  1. Seleccione **Network (Red) > Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador que ha usado más arriba.
  2. Seleccione **Redistribution Profiles (Perfiles de redistribución)** y haga clic en **Add (Añadir)**.
  3. Introduzca un nombre para el perfil, seleccione **Redistr.** y asigne un valor de **Prioridad**. Si ha configurado múltiples perfiles, coincidirá primero el perfil con el valor de propiedad más bajo.
  4. Defina **Source Type (Tipo de origen)** como **static (estático)** y haga clic en **OK (Aceptar)**. Se usa la ruta estática definida en el paso 6 para la redistribución.
2. Inyecte las rutas estáticas en el sistema OSPF.
  1. Seleccione **OSPF > Export Rules (Reglas de exportación)** (para IPv4) u **OSPFv3 > Export Rules (Reglas de exportación)** (para IPv6).
  2. Haga clic en **Add (Añadir)** y seleccione el perfil de redistribución que ha creado.
  3. Seleccione cómo se llevan las rutas externas al sistema OSPF. La opción predeterminada, **Ext2**, calcula el coste total de la ruta usando solo métricas externas. Para usar métricas OSPF tanto internas como externas, use **Ext1**.
  4. Asigne una **Metric (Métrica)** (valor de coste) a las rutas inyectadas en el sistema OSPF. Esta opción le permite cambiar la métrica para la ruta inyectada al entrar en el sistema OSPF.
  5. Haga clic en **OK (Aceptar)**.

**STEP 8 |** Configure el túnel IPsec.

1. Seleccione **Network (Red) > IPsec Tunnels (Túneles IPsec)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

En este ejemplo, la configuración para el peer A de VPN es:

- **Tunnel Interface (Interfaz de túnel):** tunnel.41 (túnel.41)
- **Type (Tipo):** Auto Key (Clave automática)
- **IKE Gateway (Puerta de enlace de IKE):** seleccione la puerta de enlace de IKE definida más arriba.
- **Perfil criptográfico de IPsec:** seleccione la puerta de enlace de IKE definida en más arriba.

La configuración para el peer B de VPN es:

- **Tunnel Interface (Interfaz de túnel):** tunnel.40 (túnel.40)
  - **Type (Tipo):** Auto Key (Clave automática)
  - **IKE Gateway (Puerta de enlace de IKE):** seleccione la puerta de enlace de IKE definida más arriba.
  - **Perfil criptográfico de IPsec:** seleccione la puerta de enlace de IKE definida en más arriba.
3. Seleccione **Mostrar opciones avanzadas**, seleccione **Supervisor de túnel** y especifique una dirección IP de destino para hacer ping para verificar la conectividad.
  4. Para definir la acción que se realizará si no es posible establecer conectividad, consulte [Definición de perfiles supervisión de túnel](#).

**STEP 9 |** Cree reglas de políticas para permitir el tráfico entre los sitios (subredes).

1. Seleccione **Policies (Políticas) > Security (Seguridad)**.
2. Cree reglas para permitir el tráfico entre la zona no fiable y la zona vpn-tun y la zona vpn-tun y la zona no fiable para tráfico que se origine desde el origen especificado y las direcciones IP de destino.

**STEP 10** | Verifique las adyacencias OSPF y las rutas desde el CLI.

Verifique que ambos cortafuegos puedan verse entre sí con estado completo. Confirme además la dirección IP de la interfaz del túnel del peer de VPN y el ID del enrutador OSPF. Use los siguientes comandos del CLI con cada peer de VPN:

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

Options: 0x80:reserved, O:Opaque-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
         N/P:NSSA option, MC:multicast, E:AS external LSA capability, T:TOS capability
=====
virtual router:          vr1
neighbor address:       2.1.1.140
local address binding:  0.0.0.0
type:                   dynamic
status:                 full
neighbor router ID:     192.168.100.140
area id:                0.0.0.0
neighbor priority:      1
lifetime remain:        39
messages pending:       0
LSA request pending:    0
options:                0x42: O E
hello suppressed:       no

admin@FW-B> show routing protocol ospf neighbor

Options: 0x80:reserved, O:Opaque-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
         N/P:NSSA option, MC:multicast, E:AS external LSA capability, T:TOS capability
=====
virtual router:          vr1
neighbor address:       2.1.1.141
local address binding:  0.0.0.0
type:                   dynamic
status:                 full
neighbor router ID:     192.168.100.141
area id:                0.0.0.0
neighbor priority:      1
lifetime remain:        39
messages pending:       0
LSA request pending:    0
options:                0x42: O E
hello suppressed:       no
```

- **show routing route**

A continuación se muestra un ejemplo de salida en cada peer de VPN.

```
VPN PeerA
destination      next hop      metric  flags  age   interface  next-AS
192.168.1.0/24   2.1.1.141    20     A S    0     tunnel.41
192.168.2.0/24   2.1.1.141    20     A S    0     tunnel.41
172.16.101.0/24  0.0.0.0      1       A H    0     ethernet1/1
2.1.1.140/24     2.1.1.141    20     A S    0     tunnel.41

VPN PeerB
destination      next hop      metric  flags  age   interface  next-AS
192.168.1.0/24   0.0.0.0      10     A Oo   0     ethernet1/1
192.168.2.0/24   0.0.0.0      10     A Oo   0     ethernet1/15
172.16.101.0/24  2.1.1.140    20     A H    0     tunnel.40
2.1.1.141/24     2.1.1.140    10     A C    0     tunnel.40
```

**STEP 11** | Prueba de conectividad VPN.

Consulte [Configuración de la supervisión del túnel](#) y [Ver el estado del túnel](#).

# Solución de problemas

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"><li>• PAN-OS</li></ul>	No se requiere licencia

Este capítulo comparte tareas para probar la conectividad VPN e interpretar los mensajes de error de VPN si se encuentran. Utilice los comandos CLI para supervisar y solucionar problemas de conexiones VPN de sitio a sitio.

- [Solucionar problemas de conexión de túnel VPN IPSec](#)
- [Solucionar problemas relacionados con el túnel VPN IPSec de sitio a sitio mediante CLI](#)

## Solucionar problemas de conexión de túnel VPN IPsec

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Pruebe y solucione problemas de su conexión VPN IPsec para obtener su máximo rendimiento:

- [Prueba de conectividad VPN](#)
- [Interpretación de mensajes de error de VPN](#)

### Prueba de conectividad VPN

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Realice esta tarea para probar la conectividad VPN.

**STEP 1** | Inicie el IKE de fase 1 haciendo un ping a un host a través del túnel o usando el siguiente comando del CLI:

```
test vpn ike-sa gateway <gateway_name>
```

**STEP 2** | Introduzca el siguiente comando para probar si el IKE de fase 1 está configurado:

```
show vpn ike-sa gateway <gateway_name>
```

En el resultado, compruebe si se muestra la asociación de seguridad. De lo contrario, revise los mensajes del log del sistema para interpretar el motivo del fallo.

**STEP 3** | Inicie el IKE de fase 2 haciendo un ping a un host a través del túnel o usando el siguiente comando del CLI:

```
test vpn ipsec-sa tunnel <tunnel_name>
```

**STEP 4** | Introduzca el siguiente comando para probar si el IKE de fase 2 está configurado:

```
show vpn ipsec-sa tunnel <tunnel_name>
```

En el resultado, compruebe si se muestra la asociación de seguridad. De lo contrario, revise los mensajes del log del sistema para interpretar el motivo del fallo.

**STEP 5 |** Para ver la información del flujo de tráfico VPN, use el siguiente comando.

```
show vpn flow total tunnels configured:          1 filter - type
IPSec, state any total IPSec tunnel configured: 1 total
IPSec tunnel shown:                            1 name      id
state      local-ip      peer-ip      tunnel-i/f
-----
vpn-to-siteB      5      active
100.1.1.1      200.1.1.1      tunnel.41
```

## Interpretación de mensajes de error de VPN

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

La siguiente tabla enumera algunos de los mensajes de error de VPN más comunes que se registran en el log del sistema.

**Table 2: Mensajes de error de Syslog para problemas de VPN**

Si un error es este:	Pruebe a:
<p>La negociación IKE de fase 1 falló como iniciador, modo principal. Falló SA: x.x.x.x(500)-y.y.y.y(500) cookie:84222f276c2fa2e9:0000000000000000 por agotarse el tiempo de espera.</p> <p>O</p> <p>Falló la negociación IKE de fase 1. No se pudo encontrar la configuración de solicitud IKE de fase 1 para el peer IP x.x.x.x(1929)</p>	<ul style="list-style-type: none"> <li>Verificar si la dirección IP pública de cada peer VPN es precisa en la configuración del gateway IKE.</li> <li>Verifique si se puede hacer ping a las direcciones IP y que los problemas de enrutamiento no están provocando el fallo de conexión.</li> </ul>
<p>Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x(500) to y.y.y.y(500), ignored...</p> <p>O</p> <p>Falló la negociación IKE de fase 1. No se puede procesar la SA de payload del peer.</p>	<p>Comprobar el perfil criptográfico IKE para verificar que las propuestas en ambos lados tienen un cifrado, autenticación y propuesta de grupo DH comunes.</p>
<p>pfs group mismatched:my: 2peer: 0</p> <p>O</p>	<p>Comprobar la configuración del perfil criptográfico IPSec para verificar que:</p>

Si un error es este:	Pruebe a:
<p>La negociación IKE de fase 2 falló durante el proceso de la carga SA. No se encontró propuesta adecuada en la carga SA del peer.</p>	<ul style="list-style-type: none"> <li>• los dos peers VPN tienen el mismo valor de PFS: habilitado o deshabilitado</li> <li>• los grupos DH propuestos por cada peer tienen al menos un grupo DH en común</li> </ul>
<p>La negociación IKE de fase 2 falló al procesar el ID de proxy. Recibió id local x.x.x.x/x tipo IPv4 dirección de protocolo 0 puerto 0, recibió id remota y.y.y.y/y tipo IPv4 dirección de protocolo 0 puerto 0.</p>	<p>El peer de VPN de un extremo está usando una VPN basada en políticas. Debe configurar un ID de proxy en el firewall de Palo Alto Networks. Consulte <a href="#">Creación de una ID de proxy para identificar a los peers VPN</a>.</p>
<p>Commit error: Tunnel interface tunnel.x multiple binding limitation (xx) reached.</p>	<p>Debe haber alcanzado el número máximo de los ID de proxy admitidos en su cortafuegos. Verifique el número máximo de los ID de proxy admitidos en su cortafuegos antes de establecer un túnel IPsec.</p> <p>Le recomendamos que verifique el número máximo de ID de proxy admitidos en su cortafuegos antes de configurar los ID de proxy para los peers s VPN. Si tiene un caso de uso en el que desea implementar un túnel VPN IPsec con más ID de proxy de lo admitido en un cortafuegos, siga estos pasos:</p> <ul style="list-style-type: none"> <li>• Configure otro túnel con la misma configuración de fase 1 y fase 2.</li> <li>• Fusione (Supernet) la dirección IP para los ID de proxy. Por ejemplo, en lugar de usar 10.1.0.0/16, 10.2.0.0/16, cambie el rango a 10.0.0.0/8 para evitar entradas múltiples.</li> </ul>
<p>Proxy ID mismatch</p>	<p>La falta de coincidencia del <a href="#">ID de proxy</a> provocará que no se pueda establecer el túnel VPN IPsec de sitio a sitio. Por lo tanto, configure los ID de proxy idénticos en ambos peers VPN para establecer correctamente el túnel VPN IPsec de sitio a sitio.</p>

**Si un error es este:****Pruebe a:**

Por ejemplo: En una configuración de túnel IPsec de sitio a sitio, si un peer de VPN está configurado con una dirección IP para una máscara de red de /32 y el peer de VPN remoto está configurado con la misma dirección IP pero con una máscara de red diferente de /16, esto provocará un error al establecer el túnel VPN.



*El ID de proxy para otros proveedores de cortafuegos se conoce como Lista de acceso o Lista de control de acceso (ACL).*

Los ID de proxy en los peers VPN deben ser espejos exactos entre sí (es decir, opuestos), pero no deben coincidir.

Ejemplo de configuración de ID de proxy para peers VPN para establecer un túnel VPN IPsec:

Si el cortafuegos 1 de la VPN está configurado con 192.0.2.0/24 como ID local y 192.0.2.25/24 como ID de peer. Entonces, el cortafuegos 2 de la VPN debe configurarse con 192.0.2.25/24 como ID local y 192.0.2.0/24 como ID de igual.

## Solucionar problemas de VPN de sitio a sitio mediante CLI

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Utilice los siguientes comandos de la CLI para solucionar problemas de VPN de sitio a sitio de fase 1 y fase 2:

- [Mostrar comandos](#)
- [Borrar comandos](#)
- [Comandos de prueba](#)
- [Comandos de depuración](#)

### Mostrar comandos

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Si desea...	Use...
<ul style="list-style-type: none"> <li>Mostrar las estadísticas básicas de todos los túneles VPN.</li> </ul>	<code>&gt; show running tunnel flow info</code>
<ul style="list-style-type: none"> <li>Mostrar la SA de IKE para una puerta de enlace determinada</li> </ul>	<code>&gt; show vpn ike-sa gateway &lt;gateway&gt;   ma tch &lt;x.x.x.x/Y&gt;</code>
<ul style="list-style-type: none"> <li>Mostrar la SA de IKE para un túnel determinado</li> </ul>	<code>&gt; show vpn ike-sa tunnel &lt;tunnel&gt;</code>
<ul style="list-style-type: none"> <li>Mostrar contadores IPSec</li> </ul>	<code>&gt; show vpn flow</code>
<ul style="list-style-type: none"> <li>Mostrar la lista de todas las puertas de enlace IPSec y sus configuraciones.</li> </ul>	<code>&gt; show vpn gateway</code>
<ul style="list-style-type: none"> <li>Mostrar las SA de fase 1 de IKE</li> </ul>	<code>&gt; show vpn ike-sa</code>

Si desea...	Use...
<ul style="list-style-type: none"> <li>Mostrar las SA de fase 2 de IKE</li> </ul>	<pre>&gt; show vpn ipsec-sa</pre>
<ul style="list-style-type: none"> <li>Mostrar la lista de configuraciones de túnel IPsec de clave automática</li> </ul>	<pre>&gt; show vpn tunnel</pre>

## Borrar comandos

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Si desea...	Use...
<ul style="list-style-type: none"> <li>Elimine la SA de IKE IKEv1 para una puerta de enlace específica</li> </ul>	<pre>&gt; clear vpn ike-sa gateway &lt;gateway&gt;</pre>
<ul style="list-style-type: none"> <li>Elimine la SA IKE IKEv1 para un túnel específico</li> </ul>	<pre>&gt; clear vpn ike-sa tunnel &lt;tunnel&gt;</pre>
<ul style="list-style-type: none"> <li>Elimine la SA de IPsec IKEv1 para un túnel específico</li> </ul>	<pre>&gt; clear vpn ipsec-sa tunnel &lt;tunnel&gt;</pre>

## Comandos de prueba

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Si desea...	Use...
<ul style="list-style-type: none"> <li>Iniciar una negociación IKE con la puerta de enlace designada</li> </ul>	<pre>&gt; test vpn ike-sa gateway &lt;gateway&gt;</pre>
<ul style="list-style-type: none"> <li>Iniciar una negociación IPsec para el túnel designado</li> </ul>	<pre>&gt; test vpn ipsec-sa tunnel &lt;tunnel&gt;</pre>

## Comandos de depuración

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> <li>PAN-OS</li> </ul>	No se requiere licencia

Si desea...	Use...
<ul style="list-style-type: none"> <li>Activar la depuración para ver el registro de logs y el estado de forma detallada</li> </ul>	<pre data-bbox="711 520 1455 604">&gt; debug ike global on debug less mp-log ikemgr.log debug ike stat</pre>
<ul style="list-style-type: none"> <li>Capturar de paquetes para ver y capturar negociaciones en modo principal, agresivo y rápido.</li> </ul>	<pre data-bbox="711 680 1455 779">&gt; debug ike pcap on view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap</pre>
<ul style="list-style-type: none"> <li>Desactivar la depuración</li> </ul>	<pre data-bbox="711 863 1455 905">&gt; debug ike pcap off</pre>