paloalto TECHDOCS

IPSec VPN Administration

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

August 16, 2024

Table of Contents

IPSec VPN Basics

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

Virtual private network (VPN) helps you to establish a secure network connection when using public networks. VPNs encrypt your internet traffic and hide your identity in the internet. This makes the location invisible and makes it more difficult for third parties to track your activities in the internet and steal data. A VPN connection is also secure against external attacks from bad actors in the internet as only you can access the data in the encrypted VPN tunnel.

VPNs create tunnels that allow users and systems to connect securely over a public network, as if they were connecting over a local area network (LAN). To set up a VPN tunnel, you need a pair of devices that can authenticate each other and encrypt the flow of information between them. The devices can be a pair of Palo Alto Networks firewalls, or a Palo Alto Networks firewall along with a VPN-capable device from another vendor.

There are many different types of VPNs, and one among them is the most common site-to-site VPN.

A site-to-site VPN is a private network that hides the private intranets and allow users of these secure networks to access each other's resources. Many organizations use site-to-site VPN for their businesses needs to connect two or more locations. For example, a site-to-site VPN would allow a company's headquarters at one geographical location to connect with a smaller branch at another geographical location. Site-to-site VPNs enhance the security and efficiency of organizational networks.

This guide helps you to understand the basics of site-to-site VPN, how to configure, monitor and troubleshoot the site-to-site VPN connections.

IPSec VPN

Where Can I Use This?	What Do I Need?
• Prisma Access (IPSec tunnel transport mode is not yet supported for Prisma Access) • PAN-OS	No license required

IPSec VPN provides a private and secure IP communication over a public network infrastructure (for example, the internet). With this technology, different sites or users in different geographical areas can communicate over a network and thus safely use their resources. IPSec provides data confidentiality and integrity, including authentication, integrity check, and encryption.

IPSec VPN is one of the two common VPN protocols, or sets of standards used to establish a VPN connection. At the IP layer, IPSec provides secure, remote access to an entire network (rather than just a single device).

IPSec VPNs come in two types:

- tunnel mode
- transport mode

Differences between IPSec and VPN

IP SECURITY (IPSec)	VPN
Provides IP hosts with methods for encrypting and authenticating data sent on the IP network.	Uses encryption to obscure all data sent between the VPN client and server.
By using IPSec, entities that have IP addresses can create a secure tunnel.	Many types of VPN protocols offer varying levels of security and other features. The most commonly used tunneling protocols in the VPN industry are Point-to-Point Tunnel Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), IPSec, Secure Socket Tunneling Protocol (SSTP), and OpenVPN.

IPSec Tunnel Modes

IPSec standards define two distinct modes of IPSec operations: tunnel and transport modes. The key difference between the transport and tunnel mode is where the policy rule is applied. Tunnel mode will add an ESP/AH header to the inner IP packet, and encapsulate it in a new outer IP packet. Hence, the entire inner IP packet including the IP header will be encrypted and authenticated. But, transport mode will add an ESP/AH header to the inner packet's payload, and move the inner packet's IP header out. This encrypts and authenticates the inner IP packet's payload only.

- *AH does not work with NAT since the integrity is calculated by using some fields of the IP header. The reason is that AH includes the outer IP header in the hash-based message authentication code (HMAC) calculation that causes NAT to break it.*
- *IPSec transport mode is used for end-to-end communications, for example between a client and a server, or between a workstation and a gateway if the gateway is being treated as a host. A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.*
- *While PAN-OS supports tunnel mode by default, support for transport mode is introduced beginning with PAN-OS 11.0 release.*

IPSec VPN Types

Site-to-Site (or Gateway-to-Gateway) VPN and Remote access (client-to-site) VPN are two distinct types of VPNs. Where client-to-site VPN represents a single user connection, site-to-site VPNs deal with remote connections between entire networks.

In a site-to-site VPN, the IPSec security method is used to create an encrypted tunnel from one customer network to a remote site of the customer. Palo Alto Networks VPN tunnels can also be used between partners.

Site-to-Site VPNs *do not allow for multiple endpoints.*

In remote access VPN, individual endpoints are connected to a private network to access the services and resources of that private network remotely. Remote Access VPN is most suitable for the business and home users as it allows multiple endpoints.

IPSec VPN Tunnels

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

The process of creating an IPSec tunnel first starts to establish a preparatory tunnel that is encrypted and secured, and then from within that secure tunnel negotiate the encryption keys and parameters for the IPSec tunnel.

The VPN negotiations take place in two defined phases: phase one and phase two. The main purpose of phase one is to set up a secure encrypted channel through which the two peers can negotiate. When phase one finishes successfully, the peers quickly move on to phase two for negotiations.

If the tunnel interface is in a zone different from the zone where the traffic will originate or depart, then define a policy rule to allow the traffic to flow from the source zone to the zone containing the tunnel interface. Configuring the IP address on the tunnel interface is optional. You would need this IP address if you intend to run dynamic routing protocols over the tunnel interface.

While IPSec incorporates many component technologies and offers multiple encryption options, the basic operation includes the following five main procedures:

- **Interesting Traffic or On-Demand**—The IPSec tunnel policy rule and the route table determines which type of traffic is considered to be “interesting” or is captured “on-demand” and, therefore, protected. How the PAN-OS VPN security policy gets implemented depends on the device platform. The access lists interpret IPSec policy rule to determine which traffic will be protected by IPSec.

  The IPSec tunnel comes up only when there is an interesting traffic destined to the tunnel. To manually initiate the tunnel, check the tunnel status and clear tunnels by referring to troubleshooting site-to-site VPN issues using the CLI.
- **IKE Phase 1**—IKE is a key management protocol standard used with IPSec. IKE authenticates each peer in an IPSec session, automatically negotiates two levels of SAs, and handles the exchange of session keys accomplished in two phases: phase 1 and phase 2.

  The main purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers.
- **IKE Phase 2**—IKE negotiates the stricter IPSec Security Associations (SA) parameters for the CHILD_SA between the peers.
- **IPSec Data Transfer**—Qualifying data is transferred between IPSec peers. Information is exchanged through IPSec sessions based on the method for defining interesting traffic. Packets are encrypted and decrypted at the IPSec peers using any encryption specified in the IPSec SA.
- **IPSec Tunnel Session Termination**—The IPSec session can be terminated because the traffic ended and the IPSec SA was deleted or the SA can timeout based on either SA lifetime setting.

The SA timeout can be after a specified number of seconds or a specified number of bytes passed through the connection.

The keys are discarded when SAs terminate, requiring IKE to perform a new phase two and, possibly, a new phase one negotiation. New SAs can be established before the current ones expire, maintaining uninterrupted data flows.

The IPSec session terminates through deletion or by timing out.

IPSec Tunnel Policy Rule Implementation on Palo Alto Networks Next-Generation Firewalls

Encapsulating a packet for secure transportation on the network is accomplished by means of the IPsec protocol. For example, in the case of a site-to-site VPN, a source host in a network transmits an IP packet. When that packet reaches the edge of the network, it makes contact with a VPN gateway. The VPN gateway that corresponds with that network encrypts the private IP packet and relays it over an ESP tunnel to a peer VPN gateway at the edge of the next network, the gateway of which decrypts the packet and delivers it to the destination host.

The policy-based VPNs have specific security rules, policy rules, or access-lists (such as source addresses, destination addresses, and ports) that are configured for permitting the interesting traffic through IPSec tunnels. These rules are referenced during the quick mode (or IPSec phase 2), and are exchanged in the first or the second messages as the proxy IDs. If the Palo Alto Networks firewall is not configured with the proxy ID settings, then the firewall sets the proxy ID with the default values (source ip = 0.0.0.0/0, destination ip = 0.0.0.0/0, application:any) and exchanges it with the peer during the first or the second message of the quick mode.

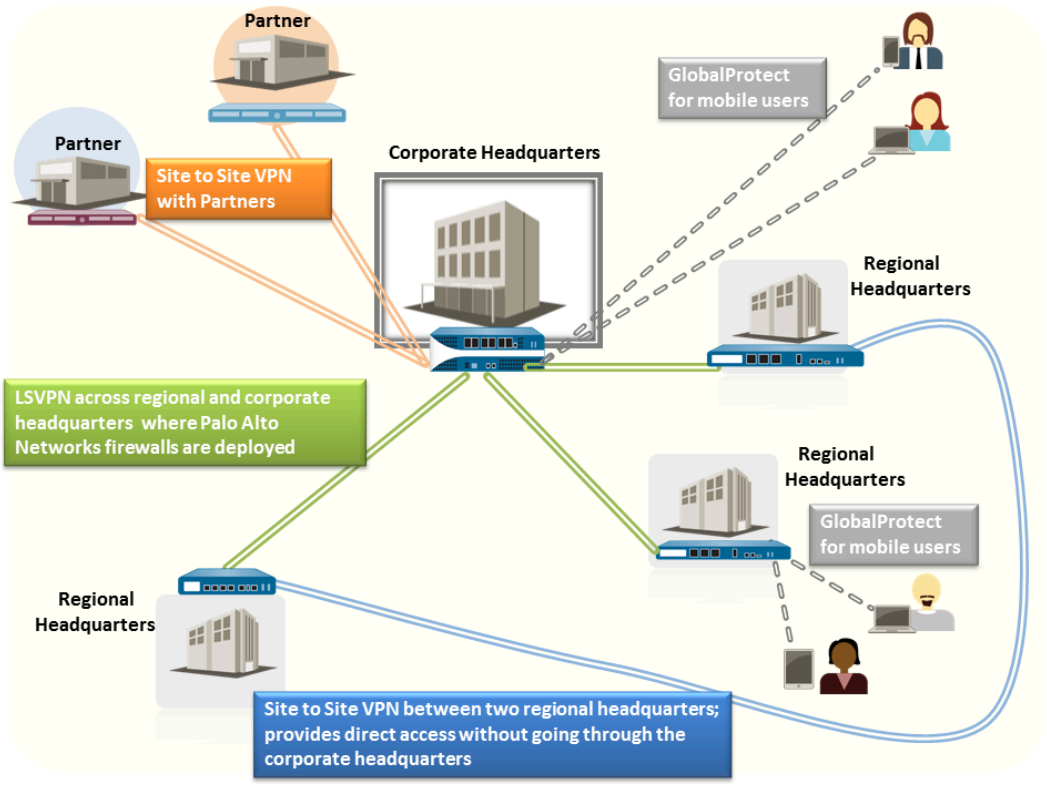
VPN Deployments

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

The Palo Alto Networks firewall supports the following VPN deployments:

- **Site-to-Site VPN**— A simple VPN that connects a central site and a remote site, or a hub and spoke VPN that connects a central site with multiple remote sites. The firewall uses the Internet Protocol Security (IPSec) set of protocols to set up a secure tunnel for the traffic between the two sites. See Site-to-Site VPN Overview.
- **Remote User-to-Site VPN**—A solution that uses the GlobalProtect agent to allow a remote user to establish a secure connection through the firewall. This solution uses SSL and IPSec to establish a secure connection between the user and the site. Refer to the GlobalProtect Administrator's Guide.
- **Large Scale VPN**— The Palo Alto Networks GlobalProtect Large Scale VPN (LSVPN) provides a simplified mechanism to roll out a scalable hub and spoke VPN with up to 1,024 satellite offices. The solution requires Palo Alto Networks firewalls to be deployed at the hub and at every spoke. It uses certificates for device authentication, SSL for securing communication between all components, and IPSec to secure data. See Large Scale VPN (LSVPN).
- **Remote Site VPN**—Remote sites use IPSec tunnels to secure users and devices in remote network locations. In addition, mobile users secured with GlobalProtect and users at remote sites access private applications using either IPSec tunnels (for service connections or ZTNA Connectors) or GRE tunnels (for Colo-Connect connections).

The following figure illustrates how various users, partners, and offices connect to the same corporate headquarters with different VPN deployments.



Internet Key Exchange (IKE) for VPN

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

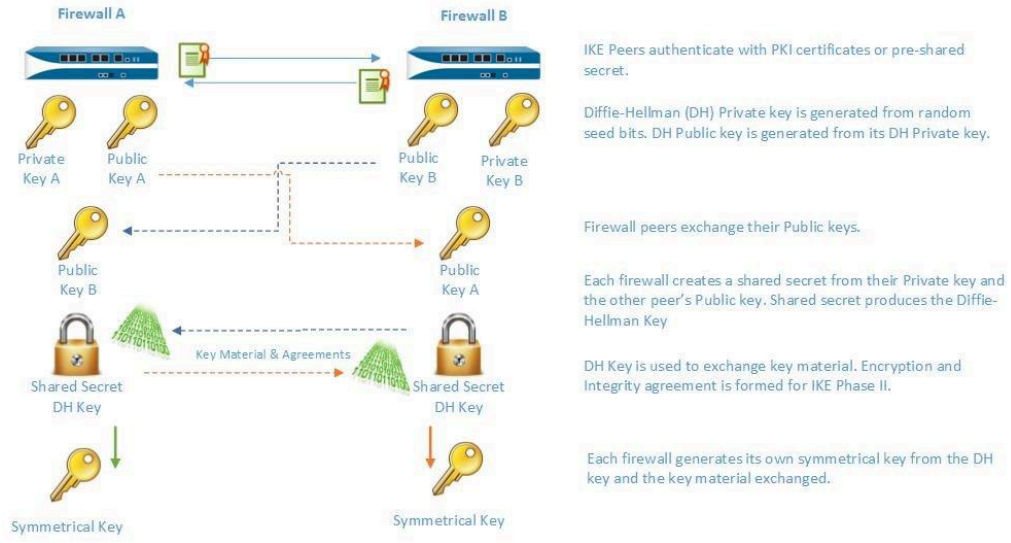
The IKE process allows the VPN peers at both ends of the tunnel to encrypt and decrypt packets using mutually agreed-upon keys or certificate and method of encryption. The IKE process occurs in two phases: IKE Phase 1 and IKE Phase 2.

- IKE Phase 1—Initially, a VPN peer will exchange the proposals for security services, such as, encryption algorithms, authentication algorithm, hash function. Both the VPN peers will form a security association which is a collection of parameters that the two devices use. When both the VPN peers of the tunnel agree to accept a set of security parameters, the IKE phase 1 is completed.

  There are two modes in IKE phase 1, main mode and aggressive mode.
- IKE Phase 2—Once the IKE phase 1 is completed successfully, IKE phase 2 is initiated. The security associations and services between the VPN peers are negotiated in IKE phase 2. The VPN peers of the tunnel will negotiate which protocol (Authentication Header or Encapsulation Security Protocol) and which algorithm to use.

  IKE Phase 2 operates only in quick mode.

Each of these phases uses keys and encryption algorithms that are defined using cryptographic profiles— IKE Crypto profile and IPSec Crypto profile—and the result of the IKE negotiation is a security association (SA). An SA is a set of mutually agreed-upon keys and algorithms that are used by both VPN peers to allow the flow of data across the VPN tunnel. The following illustration depicts the key exchange process for setting up the VPN tunnel:



IKE Gateway

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

The Palo Alto Networks firewalls or a firewall and another security device that initiate and terminate VPN connections across the two networks are called the IKE Gateways. To set up the VPN tunnel and send traffic between the IKE Gateways, each peer must have an IP address—static or dynamic—or FQDN. The VPN peers use pre-shared keys or certificates to authenticate each other mutually.

(In IKEv1) The peers must also negotiate the mode—main or aggressive—for setting up the VPN tunnel and the SA lifetime in IKE Phase 1. The main mode protects the identity of the peers and is more secure because more packets are exchanged when setting up the tunnel. Main mode is the recommended mode for IKE negotiation if both peers support it. Aggressive mode uses fewer packets to set up the VPN tunnel and is hence a faster but a less secure option for setting up the VPN tunnel.

(In IKEv2) IKEv2 negotiation process between the IKE gateways is much more efficient and simplified compared to IKEv1 negotiation. IKEv2 performs three types of exchanges: initial exchanges, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange. IKEv2 uses the following two exchanges during the initial exchange process each with two messages.

- IKE_SA_INIT exchange—Negotiates IKE SA parameters and exchanges keys.
- IKE_AUTH exchange—Authenticates the identity of the peer and establishes IPSec SAs.

After the four-message initial exchanges, IKEv2 sets up one IKE SA and one pair of IPSec SAs. To set up one IKE SA and one pair of IPSec SAs, IKEv1 goes through two phases that use a minimum of six messages.

To set up one more pair of IPSec SAs within the IKE SA, IKEv2 goes on to perform an additional two-message exchange—the CREATE_CHILD_SA exchange. One CREATE_CHILD_SA exchange creates one pair of IPSec SAs. IKEv2 also uses the CREATE_CHILD_SA exchange to re-key IKE SAs and Child SAs.

IKEv2 uses the INFORMATIONAL exchange for errors and notifications.

See Set Up an IKE Gateway for configuration details.

IKE Phase 1

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

In this phase, the firewalls use the parameters defined in the IKE Gateway configuration and the IKE Crypto profile to authenticate each other and set up a secure control channel. IKE Phase supports the use of pre-shared keys or digital certificates (which use public key infrastructure, PKI) for mutual authentication of the VPN peers. Pre-shared keys are a simple solution for

securing smaller networks because they don't require the support of a PKI infrastructure. Digital certificates can be more convenient for larger networks or implementations that require stronger authentication security.

When using certificates, make sure that the CA issuing the certificate is trusted by both gateway peers and that the maximum length of certificates in the certificate chain is 5 or less. With IKE fragmentation enabled, the firewall can reassemble IKE messages with up to five certificates in the certificate chain and successfully establish a VPN tunnel.

The IKE Crypto profile defines the following options that are used in the IKE SA negotiation:

- Diffie-Hellman (DH) group for generating symmetrical keys for IKE.

  The Diffie-Hellman algorithm uses the private key of one party and the public key of the other to create a shared secret, which is an encrypted key that both VPN tunnel peers share. The DH groups supported on the firewall are:

Group Number	Number of Bits
Group 1	(Not Recommended) 768 bits
Group 2	(Not Recommended) 1,024 bits (default)
Group 5	(Not Recommended) 1,536 bits
Group 14	2,048 bits
Group 15	(PAN-OS 10.2.0 and later releases) 3072-bit modular exponential group
Group 16	(PAN-OS 10.2.0 and later releases) 4096-bit modular exponential group
Group 19	256-bit elliptic curve group
Group 20	384-bit elliptic curve group
Group 21	(PAN-OS 10.2.0 and later releases) 521-bit random elliptic curve group

- Authentication algorithms—sha1, sha 256, sha 384, sha 512, or md5.
- Encryption algorithms—aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc, aes-256-cbc, or des.

  - *PAN-OS 10.0.3 and later releases support the aes-256-gcm and aes-128-gcm algorithms.*
  - *PAN-OS 10.1.0 and earlier releases support the des encryption algorithm.*

IKE Phase 2

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

After the tunnel is secured and authenticated, in Phase 2 the channel is further secured for the transfer of data between the networks. IKE Phase 2 uses the keys that were established in Phase 1 of the process and the IPSec Crypto profile, which defines the IPSec protocols and keys used for the SA in IKE Phase 2.

The IPSec uses the following protocols to enable secure communication:

- Encapsulating Security Payload (ESP)—Allows you to encrypt the entire IP packet, and authenticate the source and verify the integrity of the data. While ESP requires that you encrypt and authenticate the packet, you can choose to only encrypt or only authenticate by setting the encryption option to Null; using encryption without authentication is discouraged.
- Authentication Header (AH)—Authenticates the source of the packet and verifies data integrity. AH doesn't encrypt the data payload and is unsuited for deployments where data privacy is important. AH is commonly used when the main concern is to verify the legitimacy of the peer, and data privacy isn't required.

Table 1: Algorithms Supported for IPSec Authentication and Encryption

ESP	AH
Diffie-Hellman (DH) exchange options supported	
• Group 1—768 bits • Group 2—1024 bits (default) • Group 5—1536 bits • Group 14—2048 bits • (PAN-OS 10.2.0 and later releases) Group 15—3072-bit modular exponential group • (PAN-OS 10.2.0 and later releases) Group 16—4096-bit modular exponential group • Group 19—256-bit elliptic curve group • Group 20—384-bit elliptic curve group • (PAN-OS 10.2.0 and later releases) Group 21—512-bit random elliptic curve group • no-pfs—By default, perfect forward secrecy is enabled, which means a new DH key is generated in IKE phase 2 using one of the groups listed above. This key is independent of the keys exchanged in IKE phase1 and provides better data transfer security. If you select no-pfs, the DH key created at phase 1 isn't renewed and a single key is used for the IPSec SA negotiations. Both VPN peers must be enabled or disabled for PFS.	
Encryption algorithms supported	

ESP	AH
• des	(PAN-OS 10.1.0 and earlier releases) Data Encryption Standard (DES) with the security strength of 56 bits.
• 3des	Triple Data Encryption Standard (3DES) with a security strength of 112 bits.
• aes-128-cbc	Advanced Encryption Standard (AES) using cipher block chaining (CBC) with a security strength of 128 bits.
• aes-192-cbc	AES using CBC with a security strength of 192 bits.
• aes-256-cbc	AES using CBC with a security strength of 256 bits.
• aes-128-ccm	AES using Counter with CBC-MAC (CCM) with a security strength of 128 bits.
• aes-128-gcm	AES using Galois/Counter Mode (GCM) with a security strength of 128 bits.
• aes-256-gcm	AES using GCM with a security strength of 256 bits.
Authentication algorithms supported	
• md5	• md5
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• sha512	• sha 512

Methods of Securing IPSec VPN Tunnels (IKE Phase 2)

IPSec VPN tunnels can be secured using manual keys or auto keys. In addition, IPSec configuration options include a Diffie-Hellman Group for key agreement, an encryption algorithm, and a hash for message authentication.

- **Manual Key**—Manual key is typically used if the Palo Alto Networks firewall is establishing a VPN tunnel with a legacy device, or if you want to reduce the overhead of generating session keys. If using manual keys, the same key must be configured on both peers.

  Manual keys aren't recommended for establishing a VPN tunnel because the session keys can be compromised when relaying the key information between the peers; if the keys are compromised, the data transfer is no longer secure.

- **Auto Key**— Auto Key allows you to generate keys automatically for setting up and maintaining the IPSec tunnel based on the algorithms defined in the IPSec Crypto profile.

IKEv2

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

An IPSec VPN gateway uses IKEv1 or IKEv2 to negotiate the IKE security association (SA) and IPSec tunnel. Palo Alto Networks IKEv2 implementation is based on RFC 7295.

Unlike IKEv1, which uses Phase 1 SA and Phase 2 SA, IKEv2 uses a child SA for Encapsulating Security Payload (ESP) or Authentication Header (AH), which is set up with an IKE SA.

NAT traversal (NAT-T) must be enabled on both gateways if you have NAT occurring on a device that sits between the two gateways. A gateway can see only the public (globally routable) IP address of the NAT device.

IKEv2 provides the following benefits over IKEv1:

- Tunnel endpoints exchange fewer messages to establish a tunnel. IKEv2 uses four messages; IKEv1 uses either nine messages (in main mode) or six messages (in aggressive mode).
- Built-in NAT-T functionality improves compatibility between vendors.
- Built-in health check automatically reestablishes a tunnel if it goes down. The liveness check replaces the Dead Peer Detection used in IKEv1.
- Supports traffic selectors (one per exchange). The traffic selectors are used in IKE negotiations to control what traffic can access the tunnel.
- Supports Hash and URL certificate exchange to reduce fragmentation.
- Resiliency against DoS attacks with improved peer validation. An excessive number of half-open SAs can trigger cookie validation.

Familiarize yourself with the IKEv2 basic concepts before configuring IKEv2.

After you Set Up an IKE Gateway, if you chose IKEv2, perform the following optional tasks related to IKEv2 as required by your environment:

- Export a Certificate for a Peer to Access Using Hash and URL
- Import a Certificate for IKEv2 Gateway Authentication
- Change the Key Lifetime or Authentication Interval for IKEv2
- Change the Cookie Activation Threshold for IKEv2
- Configure IKEv2 Traffic Selectors

Get Started with IPSec VPN (Site-to-Site)

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

A VPN connection provides secure access to information between two or more sites. To provide secure access to resources and reliable connectivity, a VPN connection needs the following components: IKE gateway, tunnel interface, tunnel monitoring, Internet Key Exchange (IKE) for VPN, and IKEv2.

Before you plan your IPSec VPN tunnel setup, its important you learn about:

- Tunnel Interface
- Proxy ID for IPSec VPN

Plan Your IPSec VPN Tunnel Setup

Before you set up an IPSec tunnel, it's important that you decide the following factors and plan your IPSec tunnel set up successfully.

1. **Decide on Type of VPN: Site-to-Site or Remote Access**

   The site-to-site VPN allows using the IPSec security method to create an encrypted tunnel from one customer network to a remote site of the customer. However, the remote access VPN allows individual users to connect to a private network to access its services and resources.

2. **Select a Security Method for your VPN**

   In site-to-site VPN, the IPSec security method is used to create an encrypted tunnel from one customer network to a remote site of the customer.

   In remote access VPN, individual users are connected to the private network.

3. **Decide on your VPN Client**

   The site-to-site VPN does not need setup on each client. Remote access VPN may or may not need setup on each client.

4. **Decide on your VPN Tunnel Setup**

   The site-to-site VPN does not require every user to initiate the VPN tunnel setup. Remote access VPN requires every remote access user to initiate the VPN tunnel setup.

5. **Decide on your Security Technology**

   While site-to-site VPN supports IPSec technology, Remote access VPN supports SSL as well as IPSec technology.

6. **Decide if you wish Single or Multiple Users on your VPN**

   In site-to-site VPN, multiple users are not allowed; In remote access VPN, however, multiple users are allowed.

Site-to-Site VPN Overview

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

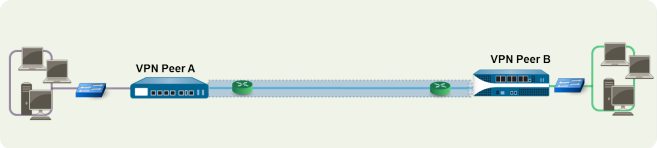
A VPN connection that allows you to connect two local area networks (LANs) is called a site-to-site VPN. You can configure route-based VPNs to connect Palo Alto Networks firewalls located at two sites or to connect a Palo Alto Networks firewall with a third-party security device at another location. The firewall can also interoperate with third-party policy-based VPN devices; the Palo Alto Networks firewall supports route-based VPN.

The Palo Alto Networks firewall sets up a route-based VPN, where the firewall makes a routing decision based on the destination IP address. If traffic is routed to a specific destination through a VPN tunnel, then it's handled as VPN traffic.

The Internet Protocol Security (IPSec) set of protocols is used to set up a secure tunnel for the VPN traffic, and the information in the TCP/IP packet is secured (and encrypted if the tunnel type is ESP). The IP packet (header and payload) is embedded in another IP payload, and a new header is applied and then sent through the IPSec tunnel. The source IP address in the new header is that of the local VPN peer and the destination IP address is that of the VPN peer on the far end of the tunnel. When the packet reaches the remote VPN peer (the firewall at the far end of the tunnel), the outer header is removed and the original packet is sent to its destination.

In order to set up the VPN tunnel, first the peers need to be authenticated. After successful authentication, the peers negotiate the encryption mechanism and algorithms to secure the communication. The Internet Key Exchange (IKE) process is used to authenticate the VPN peers, and IPSec security associations (SAs) are defined at each end of the tunnel to secure the VPN communication. IKE uses digital certificates or pre-shared keys, and the Diffie-Hellman keys to set up the SAs for the IPSec tunnel. The SAs specify all of the parameters that are required for secure transmission— including the security parameter index (SPI), security protocol, cryptographic keys, and the destination IP address—encryption, data authentication, data integrity, and endpoint authentication.

The following figure shows a VPN tunnel between two sites. When a client that is secured by VPN Peer A needs content from a server located at the other site, VPN Peer A initiates a connection request to VPN Peer B. If the security policy permits the connection, VPN Peer A uses the IKE Crypto profile parameters (IKE phase 1) to establish a secure connection and authenticate VPN Peer B. Then, VPN Peer A establishes the VPN tunnel using the IPSec Crypto profile, which defines the IKE phase 2 parameters to allow the secure transfer of data between the two sites.



Tunnel Interface

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

To set up a VPN tunnel, the Layer 3 interface at each end must have a logical *tunnel* interface for the firewall to connect to and establish a VPN tunnel. A tunnel interface is a logical (virtual) interface that is used to deliver traffic between the two endpoints. If you configure any proxy IDs, the proxy ID is counted toward any IPSec tunnel capacity.

The tunnel interface must belong to a security zone to apply a policy rule and it must be assigned to a virtual router in order to use the existing routing infrastructure. Ensure that the tunnel interface and the physical interface are assigned to the same virtual router so that the firewall can perform a route lookup and determine the appropriate tunnel to use.

Typically, the Layer 3 interface that the tunnel interface is attached to belongs to an external zone, for example the untrust zone. While the tunnel interface can be in the same security zone as the physical interface, for added security and better visibility, you can create a separate zone for the tunnel interface. If you create a separate zone for the tunnel interface, say a VPN zone, you'll need to create security policies to enable traffic to flow between the VPN zone and the trust zone.

To route traffic between the sites, a tunnel interface doesn't require an IP address. An IP address is only required if you want to enable tunnel monitoring or if you're using a dynamic routing protocol to route traffic across the tunnel. With dynamic routing, the tunnel IP address serves as the next hop IP address for routing traffic to the VPN tunnel.

If you're configuring the Palo Alto Networks firewall with a VPN peer that performs policy-based VPN, you must configure a local and remote proxy ID when setting up the IPSec tunnel. Each peer compares the proxy IDs configured on it with what is received in the packet to allow a successful IKE phase 2 negotiation. If multiple tunnels are required, configure unique proxy IDs for each tunnel interface; a tunnel interface can have a maximum of 250 proxy IDs. Each proxy ID counts toward the IPSec VPN tunnel capacity of the firewall, and the tunnel capacity varies by the firewall model.

See Set Up an IPSec Tunnel for configuration details.

Proxy ID for IPSec VPN

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

Proxy Identity or proxy ID refers to a set of traffic that belongs to an IPSec VPN which is subjected to the SA being negotiated between peers (or setup once the negotiation has succeeded).

It allows identifying and then directing the traffic:

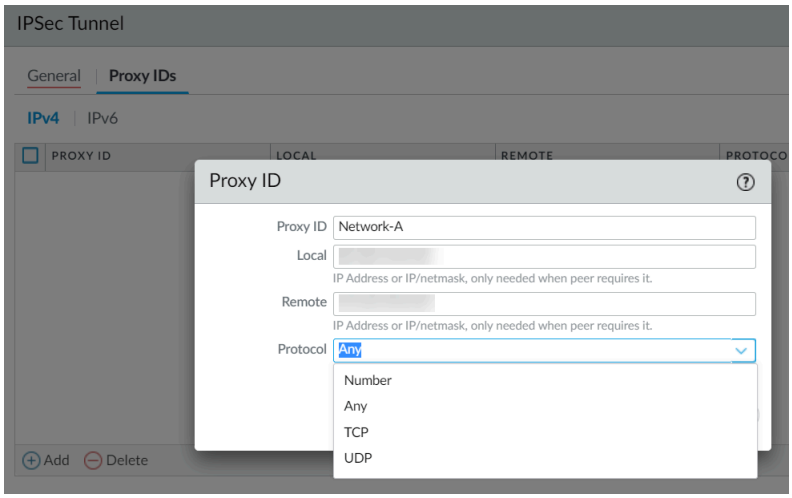
- to appropriate tunnel where multiple tunnels coexist between the same two peers that share the same IKE gateway.
- allows unique and shared SAs with different parameters to coexist.

Use proxy IDs in the configurations where VPN tunnels are set up between the same two peers.

Proxy IDs help identify what traffic belongs to a particular IPSec VPN. This lets an operating system install the appropriate hooks to direct traffic that matches the source and destination address in the proxy ID (client ID) and direct it into the matching IPSec SA or VPN into and out of the matching IPSec SAs.

Setting up the Proxy ID

Palo Alto Networks is among a few other vendors that use proxy IDs. The following figure shows the Palo Alto Networks proxy ID window along with its options.



Select **Network** > **IPSec Tunnel** > **Proxy IDs**. Enter the proxy ID name, local IP address, remote IP address if required by the peer, and the protocol type along with its local and remote port numbers.

Each proxy ID is considered to be a VPN tunnel and therefore is counted towards the IPSec VPN tunnel capacity of the firewall. For example, the maximum limit for a site-to-site IPSec VPN tunnel is 1000 for PA-3020, 100 for PA-2050, and 25 for PA-200.

Proxy IDs behave differently with IKE versions:

- **IKEv1**—Palo Alto Networks devices support only proxy ID exact matches. If proxy IDs for peers do not match, then the VPN does not work correctly.
- **IKEv2**—Supports traffic selector narrowing when proxy ID setting is different on the two VPN gateways.

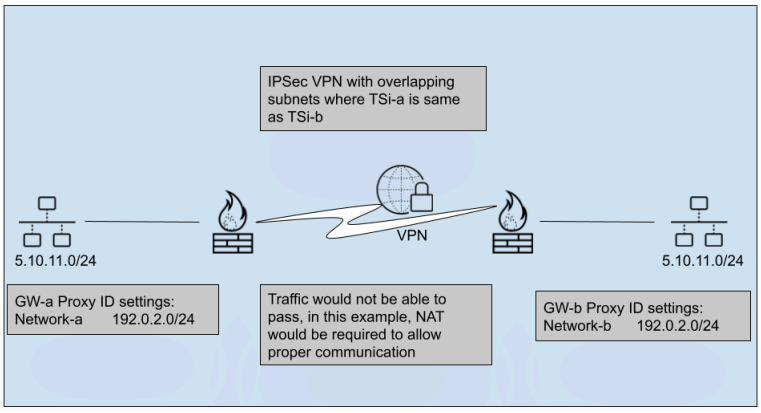
Using Proxy IDs

The following example shows two VPN gateways: A and B.

IKE negotiation is started by VPN GW-az, i=initiator, r=responder. VPN GW-a defines traffic selector TSi-a/TSr-a and VPN GW-b specifies traffic selector TSi-b/TSr-b. While TSr-a is the same as TSr-b and so it can be ignored, TSi-a can be different from TSi-b.

In this case, the traffic cannot route over the VPN tunnel since the same network exists on both sides of the tunnel.

However, as shown below, the only way to resolve this issue is for both peer gateways to create NATs to translate a new, unique network subnet to the internal network otherwise one side has to change the subnet IP.



This way, all traffic on either side would be destined to the new NAT address instead of the other similar network. Both gateways would have to perform NAT for this to work properly to remove any confusions about which network is on which side.

Configuring IPSec VPN for a Palo Alto Networks Firewall

If the other side of the tunnel is a third-party VPN device otherwise a non PAN-OS firewall, then you need to specify a matching local proxy ID and remote proxy ID: typically the local and remote LAN subnets.

When configuring an IPSec tunnel proxy ID to identify local and remote IP networks for traffic that is NATed, the proxy ID configuration for the IPSec tunnel must be configured with the post-NAT IP network information. The reason for this is that the proxy ID information defines the networks that will be allowed through the tunnel on both sides for the IPSec configuration.

Configure IPSec VPN Tunnels (Site-to-Site)

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

To set up site-to-site VPN:

- Make sure that your Ethernet interfaces, virtual routers, and zones are configured properly. For more information, see Configure Interfaces and Zones.
- Create your tunnel interfaces. Ideally, put the tunnel interfaces in a separate zone, so that tunneled traffic can use different policy rules.
- Set up static routes or assign routing protocols to redirect traffic to the VPN tunnels. To support dynamic routing (OSPF, BGP, RIP are supported), you must assign an IP address to the tunnel interface.
- Define IKE gateways for establishing communication between the peers across each end of the VPN tunnel; also define the cryptographic profile that specifies the protocols and algorithms for identification, authentication, and encryption to be used for setting up VPN tunnels in IKEv1 Phase 1. See Set Up an IKE Gateway and Define IKE Crypto Profiles.
- Configure the parameters that are needed to establish the IPSec connection for transfer of data across the VPN tunnel; See Set Up an IPSec Tunnel. For IKEv1 Phase-2, see Define IPSec Crypto Profiles.
- (Optional) Specify how the firewall will monitor the IPSec tunnels. See Monitor Your IPSec VPN Tunnel .
- Define Security policies to filter and inspect the traffic.

If there's a deny rule at the end of the security rulebase, intrazone traffic is blocked unless otherwise allowed. Rules to allow IKE and IPSec applications must be explicitly included above the deny rule.

If your VPN traffic is passing through (not originating or terminating on) a PA-7000 Series or PA-5200 Series firewall, configure a bidirectional Security policy rule to allow the ESP or AH traffic in both directions.

When these tasks are complete, the tunnel is ready for use. Traffic destined for the zones/addresses defined in a policy rule is automatically routed properly based on the destination route in the routing table, and handled as VPN traffic. For a few examples on site-to-site VPN, see Site-to-Site VPN Configuration Examples.

Set Up an IKE Gateway

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

To set up a VPN tunnel, the VPN peers or gateways must authenticate each other—using pre-shared keys or digital certificates—and establish a secure channel in which to negotiate the IPSec security association (SA) that will be used to secure traffic between the hosts on each side.

STEP 1 | Define the IKE Gateway.

1. Select **Network** > **Network Profiles** > **IKE Gateways**, **Add** a gateway, and enter the gateway **Name** (**General** tab).
2. Set the **Version** to **IKEv1 only mode**, **IKEv2 only mode**, or **IKEv2 preferred mode**. The IKE gateway begins its negotiation with its peer in the mode that you specify here. If you select **IKEv2 preferred mode**, the two peers will use IKEv2 if the remote peer supports it; otherwise they'll use IKEv1.

   The **Version** you select also determines which options are available for you to configure on the **Advanced Options** tab.

STEP 2 | Establish the local endpoint of the tunnel (gateway).

1. Select the **Address Type**: **IPv4** or **IPv6**.
2. Select the physical, outgoing **Interface** on the firewall where the local gateway resides. Beginning with PAN-OS 11.1.5, the field accepts interfaces configured by using DHCPv6, PPPoEv6, or a 5G modem.
3. From the **Local IP Address** list, select the IP address that the VPN connection will use as the endpoint; this is the external-facing interface with a publicly routable IP address on the firewall.

STEP 3 | Establish the peer at the far end of the tunnel (gateway).

For **Peer IP Address Type**, select one of the following and enter the corresponding information for the peer:

- **IP**—Enter a **Peer Address** that is either an IPv4 or IPv6 address or enter an address object that is an IPv4 or IPv6 address.
- **FQDN**—Enter a **Peer Address** that is an FQDN string or an address object that uses an FQDN string. If the FQDN or FQDN address object resolves to more than one IP address,

the firewall selects the preferred address from the set of addresses that match the Address Type (IPv4 or IPv6) of the IKE gateway as follows:

- If no IKE security association (SA) is negotiated, the preferred address is the IP address with the smallest value.
- If the IKE gateway uses an address that is in the set of returned addresses, the firewall selects that address (whether or not it's the smallest address in the set).
- If the IKE gateway uses an address that isn't in the set of returned addresses, the firewall selects a new address, and it's the smallest address in the set.

- **Dynamic**—Select **Dynamic** if the peer IP address or FQDN value is unknown so that the peer will initiate the negotiation.

Using an FQDN or FQDN address object reduces issues in environments where the peer is subject to dynamic IP address changes (and would otherwise require you to reconfigure this IKE gateway peer address).

STEP 4 | Specify how to authenticate the peer.

Select the **Authentication** method: **Pre-Shared Key** or **Certificate**. If you choose a pre-shared key, proceed to the next step. If you choose a certificate, skip ahead to step 6, Configure certificate-based authentication.

STEP 5 | Configure a pre-shared key.

1. Enter a **Pre-shared Key**, which is the security key for authentication across the tunnel. Reenter the value to **Confirm Pre-shared Key**. Use a maximum of 255 ASCII or non-ASCII characters.

   Generate a key that is difficult to crack with dictionary attacks; use a pre-shared key generator, if necessary.

2. For **Local Identification**, choose from the following types and enter a value that you determine: **FQDN (hostname)**, **IP address**, **KEYID (binary format ID string in HEX)**, and **User FQDN (email address)**. Local identification defines the format and identification of the local gateway. If you don't specify a value, the local IP address is used as the local identification value.
3. For **Peer Identification**, choose from the following types and enter a value that you determine: **FQDN (hostname)**, **IP address**, **KEYID (binary format ID string in HEX)**, and **User FQDN (email address)**. Peer identification defines the format and identification of the peer gateway. If you don't specify a value, the peer IP address is used as the peer identification value.
4. Proceed to step 7 (Configure advanced options for the gateway).

STEP 6 | Configure certificate-based authentication.

Perform the remaining steps in this procedure if you selected **Certificate** as the method of authenticating the peer gateway at the opposite end of the tunnel.

1. Select a **Local Certificate**—one that is already on the firewall, **Import** a certificate, or **Generate** a new certificate.
   - If you need to **Import** a certificate, then first Import a Certificate for IKEv2 Gateway Authentication and then return to this task.
   - If you want to **Generate** a new certificate, then first generate a certificate on the firewall and then return to this task.
2. (Optional) Enable (select) the **HTTP Certificate Exchange** to configure Hash and URL (IKEv2 only). For an HTTP certificate exchange, enter the **Certificate URL**. For more information, see Hash and URL Certificate Exchange.
3. Select the **Local Identification** type—**Distinguished Name (Subject), FQDN (hostname)**, **IP address**, or **User FQDN (email address)**—and then enter the value. Local identification defines the format and identification of the local gateway.
4. Select the **Peer Identification** type—**Distinguished Name (Subject), FQDN (hostname)**, **IP address**, or **User FQDN (email address)**—and then enter the value. Peer identification defines the format and identification of the peer gateway.
5. Specify the type of **Peer ID Check**:
   - **Exact**—Ensures that the local setting and peer IKE ID payload match exactly.
   - **Wildcard**—Allows the peer identification to match as long as every character before the wildcard (*) matches. The characters after the wildcard need not match.
6. (Optional) **Permit peer identification and certificate payload identification mismatch** to allow a successful IKE SA even when the peer identification doesn't match the peer identification in the certificate.
7. Choose a **Certificate Profile**. A certificate profile contains information about how to authenticate the peer gateway.
8. (Optional) **Enable strict validation of peer's extended key use** to control strictly how the key can be used.

STEP 7 | Configure advanced options for the gateway.

1. (Optional) **Enable Passive Mode** in the Common Options (**Advanced Options**) to specify that the firewall only respond to IKE connection requests and never initiate them.
2. If you have a device performing NAT between the gateways, **Enable NAT Traversal** to use UDP encapsulation on IKE and UDP protocols, which enables them to pass-through intermediate NAT devices.
3. If you configured **IKEv1 only mode** in step 1, then on the IKEv1 tab:
   - Select the **Exchange Mode**: **auto**, **aggressive**, or **main**. When you set a firewall to use **auto** exchange mode, it can accept both **main** mode and **aggressive** mode negotiation requests; however, when possible, it will initiate exchanges in **main** mode.

     *If you don't set the exchange mode to **auto**, then you must configure both peers with the same exchange mode to allow each peer to accept negotiation requests.*
   - Select an existing profile or keep the default profile from the **IKE Crypto Profile** list. If needed, you can Define IKE Crypto Profiles.
   - (Only when using certificate-based authentication and when exchange mode isn't set to aggressive mode) Click **Enable Fragmentation** to enable the firewall to operate with IKE Fragmentation.
   - Click **Dead Peer Detection** and enter an **Interval** (range is 2 to 100 seconds). For **Retry**, specify the number of retries (range is 2 to 100) before disconnecting from the IKE peer. Dead peer detection identifies inactive or unavailable IKE peers by sending an IKE phase 1 notification payload to the peer and waiting for an acknowledgment.
4. If you configured **IKEv2 only mode** or **IKEv2 preferred mode** in step 1, then on the IKEv2 tab:
   - Select an **IKE Crypto Profile**, which configures IKE Phase 1 options such, as the DH group, hash algorithm, and ESP authentication. For information about IKE Crypto profiles, see IKE Phase 1.
   - (Optional) Enable **Strict Cookie Validation**. For information, see Change the Cookie Activation Threshold for IKEv2.
   - (Optional) **Enable Liveness Check** and enter an **Interval (sec)** (default is 5) if you want to have the gateway send a message request to its gateway peer, requesting a response. If necessary, the Initiator attempts the liveness check as many as 10 times. If it doesn't get a response, the Initiator closes and deletes the IKE_SA and CHILD_SA. The Initiator will start over by sending out another IKE_SA_INIT.

STEP 8 | Click **OK** and **Commit** your changes.

Export a Certificate for a Peer to Access Using Hash and URL

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

IKEv2 supports Hash and URL certificate exchange as a method of having the peer at the remote end of the tunnel fetch the certificate from a server where you've exported the certificate.

IKEv2 supports Hash and URL certificate exchange, which is used during an IKEv2 negotiation of an SA. You store the certificate on an HTTP server, which is specified by a URL. The peer fetches the certificate from the server based on receiving the URL to the server. The hash is used to check whether the content of the certificate is valid or not. Thus, the two peers exchange certificates with the HTTP CA rather than with each other.

The hash part of Hash and URL reduces the message size and thus Hash and URL is a way to reduce the likelihood of packet fragmentation during IKE negotiation. The peer receives the certificate and hash that it expects, and thus IKE Phase 1 has validated the peer. Reducing fragmentation occurrences helps protect against DoS attacks.

You can enable the Hash and URL certificate exchange when configuring an IKE gateway by selecting **HTTP Certificate Exchange** and entering the **Certificate URL**. The peer must also use the Hash and URL certificate exchange for the exchange to be successful. If the peer can't use Hash and URL, X.509 certificates are exchanged similarly to how they're exchanged in IKEv1.

If you enable the Hash and URL certificate exchange, you must export your certificate to the certificate server if it isn't already there. When you export the certificate, the file format should be **Binary Encoded Certificate (DER)**.

Perform this task to export your certificate to that server. You must have already created a certificate using **Device** > **Certificate Management**.

STEP 1 | Select **Device** > **Certificates**, and if your platform supports multiple virtual systems, for **Location**, select the appropriate virtual system.

STEP 2 | On the **Device Certificates** tab, select the certificate to **Export** to the server.

The status of the certificate should be valid, not expired. The firewall won't stop you from exporting an invalid certificate.

STEP 3 | For **File Format**, select **Binary Encoded Certificate (DER)**.

STEP 4 | Leave **Export private key** clear. Exporting the private key is unnecessary for Hash and URL.

STEP 5 | Click **OK**.

Import a Certificate for IKEv2 Gateway Authentication

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

Perform this task if you are authenticating a peer for an IKEv2 gateway and you didn't use a local certificate already on the firewall; you want to import a certificate from elsewhere.

This task presumes that you selected **Network** > **IKE Gateways**, added a gateway, and for **Local Certificate**, you clicked **Import**.

STEP 1 | Import a certificate.

1. Select **Network** > **IKE Gateways**, **Add** a gateway, and on the **General** tab, for **Authentication**, select **Certificate**. For **Local Certificate**, click **Import**.
2. In the Import Certificate window, enter a **Certificate Name** for the certificate you're importing.
3. Select **Shared** if this certificate is to be shared among multiple virtual systems.
4. For **Certificate File**, **Browse** to the certificate file. Click on the filename and click **Open**, which populates the **Certificate File** field.
5. For **File Format**, select one of the following:
   - **Base64 Encoded Certificate (PEM)**—Privacy Enhanced Mail is the most common format for X.509 certificates, CSRs, and cryptographic keys. PEM contains the certificate, but not the key.
   - **Encrypted Private Key and Certificate (PKCS12)**—PKCS12 is a binary format for storing a certificate chain and private key in a single file. PKCS12 files are used for importing and exporting certificates and private keys.
6. Select **Import private key** if the key is in a different file from the certificate file. The key is optional, with the following exception:
   - Import a key if you set the **File Format** to **PEM**. Enter a **Key file** by clicking **Browse** and navigating to the key file to import.
   - Enter a **Passphrase** and **Confirm Passphrase**.
7. Click **OK**.

STEP 2 | Continue to the next task.

Step Configure certificate-based authentication.

Change the Key Lifetime or Authentication Interval for IKEv2

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

In IKEv2, two IKE Crypto profile values, **Key Lifetime** and **IKEv2 Authentication Multiple**, control the establishment of IKEv2 IKE SAs. The key lifetime is the length of time that a negotiated IKE SA key is effective. Before the key lifetime expires, the SA must be re-keyed; otherwise, upon expiration, the SA must begin a new IKEv2 IKE SA re-key. The default value is 8 hours.

The reauthentication interval is derived by multiplying the **Key Lifetime** by the **IKEv2 Authentication Multiple**. The authentication multiple defaults to 0, which disables the reauthentication feature.

The range of the authentication multiple is 0-50. So, if you were to configure an authentication multiple of 20, for example, the system would perform reauthentication every 20 re-keys, which is every 160 hours. That means the gateway could perform Child SA creation for 160 hours before the gateway must reauthenticate with IKE to recreate the IKE SA from scratch.

In IKEv2, the Initiator and Responder gateways have their own key lifetime value, and the gateway with the shorter key lifetime is the one that will request that the SA be re-keyed.

This task is optional; the default setting of the IKEv2 IKE SA re-key lifetime is 8 hours. The default setting of the IKEv2 Authentication Multiple is 0, meaning the reauthentication feature is disabled.

To change the default values, perform the following task. A prerequisite is that an IKE Crypto profile already exists.

STEP 1 | Change the SA key lifetime or authentication interval for an IKE Crypto profile.

1. Select **Network** > **Network Profiles** > **IKE Crypto** and select the IKE Crypto profile that applies to the local gateway.
2. For the **Key Lifetime**, select a unit (**Seconds**, **Minutes**, **Hours**, or **Days**) and enter a value. The minimum is 3 minutes.
3. For **IKE Authentication Multiple**, enter a value, which is multiplied by the lifetime to determine the reauthentication interval.

STEP 2 | Commit your changes.

Click **OK** and **Commit**.

Change the Cookie Activation Threshold for IKEv2

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

Cookie validation is always enabled for IKEv2; it helps protect against half-SA DoS attacks. You can configure the global threshold number of half-open SAs that will trigger cookie validation. You can also configure individual IKE gateways to enforce cookie validation for every new IKEv2 SA.

- The **Cookie Activation Threshold** is a global VPN session setting that limits the number of simultaneous half-opened IKE SAs (default is 500). When the number of half-opened IKE SAs exceeds the **Cookie Activation Threshold**, the Responder will request a cookie, and the Initiator must respond with an IKE_SA_INIT containing a cookie to validate the connection. If the cookie validation is successful, another SA can be initiated. A value of zero means that cookie validation is always on.

  The Responder doesn't maintain a state of the Initiator, nor does it perform a Diffie-Hellman key exchange, until the Initiator returns the cookie. IKEv2 cookie validation mitigates a DoS attack that would try to leave numerous connections half open.

  The **Cookie Activation Threshold** must be lower than the **Maximum Half Opened SA** setting. If you change the cookie activation threshold for IKEv2 to a higher number (for example, 65534) and the **Maximum Half Opened SA** setting remained at the default value of 65535, cookie validation is disabled.
- You can enable **Strict Cookie Validation** if you want cookie validation performed for every new IKEv2 SA a gateway receives, regardless of the global threshold. **Strict Cookie Validation** affects only the IKE gateway being configured and is disabled by default. With **Strict Cookie**

Validation disabled, the system uses the **Cookie Activation Threshold** to determine whether a cookie is needed or not.

Perform the following task if you want a firewall to have a threshold different from the default setting of 500 half-opened SA sessions before cookie validation is required.

STEP 1 | Change the Cookie Activation Threshold.

1. Select **Device** > **Setup** > **Session** and edit the VPN Session Settings. For **Cookie Activation Threshold**, enter the maximum number of half-opened SAs that are allowed before the responder requests a cookie from the initiator (range is 0-65,535; default is 500).
2. Click **OK**.

STEP 2 | Commit your changes.

Click **OK** and **Commit**.

Configure IKEv2 Traffic Selectors

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

In IKEv1, a firewall that has a route-based VPN needs to use a local and remote Proxy ID in order to set up an IPSec tunnel. Each peer compares its proxy IDs with what it received in the packet to negotiate IKE Phase 2 successfully. IKE Phase 2 is about negotiating the SAs to set up an IPSec tunnel. (For more information on Proxy IDs, see Tunnel Interface.)

In IKEv2, you can configure traffic selectors, which are components of network traffic that are used during IKE negotiation. Traffic selectors are used during the CHILD_SA (tunnel creation) Phase 2 to set up the tunnel and to determine what traffic is allowed through the tunnel. The two IKE gateway peers must negotiate and agree on their traffic selectors; otherwise, one side narrows its address range to reach agreement. One IKE connection can have multiple tunnels; for example, you can assign different tunnels to each department to isolate their traffic. Separation of traffic also allows features such as QoS to be implemented.

The IPv4 and IPv6 traffic selectors are:

- **Source IP address**—A network prefix, address range, specific host, or wildcard.
- **Destination IP address**—A network prefix, address range, specific host, or wildcard.
- **Protocol**—A transport protocol, such as TCP or UDP.
- **Source port**—The port where the packet originated.
- **Destination port**—The port the packet is destined for.

During IKE negotiation, there can be multiple traffic selectors for different networks and protocols. For example, the Initiator might indicate that it wants to send TCP packets from 172.168.0.0/16 through the tunnel to its peer, destined for 198.5.0.0/16. It also wants to send UDP packets from 172.17.0.0/16 through the same tunnel to the same gateway, destined for 0.0.0.0 (any network). The peer gateway must agree to these traffic selectors so that it knows what to expect.

It's possible that one gateway will start negotiation using a traffic selector that is a more specific IP address than the IP address of the other gateway.

- For example, gateway A offers a source IP address of 172.16.0.0/16 and a destination IP address of 192.16.0.0/16. But gateway B is configured with 0.0.0.0 (any source) as the source IP address and 0.0.0.0 (any destination) as the destination IP address. Therefore, gateway B narrows down its source IP address to 192.16.0.0/16 and its destination address to 172.16.0.0/16. Thus, the narrowing down accommodates the addresses of gateway A and the traffic selectors of the two gateways are in agreement.
- If gateway B (configured with source IP address 0.0.0.0) is the Initiator instead of the Responder, gateway A will respond with its more specific IP addresses, and gateway B will narrow down its addresses to reach agreement.

Use the following workflow to configure traffic selectors.

STEP 1 | Select **Network** > **IPSec Tunnels** > **Proxy IDs**.

STEP 2 | Select the **IPv4** or **IPv6** tab.

STEP 3 | Click **Add** and enter the **Name** in the **Proxy ID** field.

STEP 4 | In the **Local** field, enter the **Source IP Address**.

STEP 5 | In the **Remote** field, enter the **Destination IP Address**.

STEP 6 | In the **Protocol** field, select the transport protocol (**TCP** or **UDP**).

STEP 7 | Click **OK**.

Define Cryptographic Profiles

Where Can I Use This?	What Do I Need?
• Prisma Access • PAN-OS	No license required

A cryptographic profile specifies the ciphers used for authentication and/or encryption between two IKE peers, and the lifetime of the key. The time period between each renegotiation is known as the lifetime; when the specified time expires, the firewall renegotiates a new set of keys.

For securing communication across the VPN tunnel, the firewall requires IKE and IPSec cryptographic profiles for completing IKE phase-1 and phase-2 negotiations, respectively. The firewall includes a default IKE Crypto profile and a default IPSec Crypto profile that are ready for use. If you don't want to use the default IKE or IPSec profiles or compliance suites provided, you can configure your own IKE or IPSec profile using the configuration steps provided in this chapter.

The cryptographic profiles (that is, IKE and IPSec profiles) provide information about the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites.

- Define IKE Crypto profiles—The IKE profiles specify the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites when you establish an IKE tunnel. These IKE parameters should match on the remote firewall for the IKE phase 1 negotiation to be successful.
- Define IPSec Crypto profiles —The IPSec profiles specify the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites when you establish an IPSec tunnel. These IPSec parameters should match on the remote firewall for the IKE phase 2 negotiation to be successful.

Define IKE Crypto Profiles

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • PAN-OS	• No license required • PAN-OS 10.1 and Later

The Internet Key Exchange (IKE) profiles provide information about the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites when you establish an IPSec tunnel.

The IKE Crypto profile is used to set up the encryption and authentication algorithms used for the key exchange process in IKE Phase 1, and lifetime of the keys, which specifies how long the keys are valid. To invoke the profile, you must attach it to the IKE Gateway configuration.

*All IKE gateways configured on the same interface or local IP address must use the same crypto profile when the IKE gateway's **Peer IP Address Type** is configured as **Dynamic** and IKEv1 main mode or IKEv2 is applied. If the crypto profiles are the same on the gateways, although the initial connection might start off on a different gateway, the connection will shift to the proper gateway when pre-shared keys or certificates and peer IDs are exchanged.*

Regardless of whether your VPN peer is from the same vendor or not, the VPN peers must have the same IKE parameters configured in order to perform a successful IKE negotiation.

The following parameters need to match for a successful IKE negotiation:

- DH Group for key exchange
- Encryption algorithms
- Authentication algorithms

For example, if you have configured VPN peer 1 with **group20** for DH group, **sha384** for authentication, and **aes-256-gcm** for encryption. Then, VPN peer 2 with which you want to establish the IPSec tunnel also should have the same values configured.

Follow this procedure to create an IKE Crypto profile on a Palo Alto Networks firewall.

- PAN-OS and Prisma Access (Panorama Managed)
- Strata Cloud Manager

Define IKE Crypto Profiles (PAN-OS 10.1 and Later &)

STEP 1 | Create a new IKE profile.

1. Select **Network** > **Network Profiles** > **IKE Crypto** and select **Add**.
2. Enter a **Name** for the new profile.

STEP 2 | Specify the Diffie-Hellman (DH) Group for key exchange and the Authentication and Encryption algorithms.

Click **Add** in the corresponding sections (DH Group, Authentication, and Encryption) and select from the menus.

If you aren't certain what the VPN peers support, add multiple groups or algorithms in the order of most-to-least secure; the peers negotiate the strongest supported group or algorithm to establish the tunnel.

- DH Group—
  - (PAN-OS 10.2.0 and later releases) **group21** (on IKEv2 only mode)
  - **group20**
  - (PAN-OS 10.2.0 and later releases) **group16** (on IKEv2 only mode)
  - (PAN-OS 10.2.0 and later releases) **group15** (on IKEv2 only mode)
  - **group19**
  - **group14**
  - **group5**
  - **group2**
  - **group1**
- Authentication—
  - **sha512**
  - **sha384**
  - **sha256**
  - **sha1**
  - **md5**
  - (PAN-OS 10.0.3 and later releases) **non-auth**

  *If you select an AES-GCM algorithm for encryption, you must select the Authentication setting **non-auth** or the commit will fail. The hash is automatically selected based on the DH Group selected. DH Group 19 and below uses **sha256**; DH Group 20 uses **sha384**.*
- Encryption—
  - (PAN-OS 10.0.3 and later releases) **aes-256-gcm** (requires IKEv2; DH Group should be set to **group20**)
  - (PAN-OS 10.0.3 and later releases) **aes-128-gcm** (requires IKEv2 and DH Group set to **group19**)
  - **aes-256-cbc**
  - **aes-192-cbc**
  - **aes-128-cbc**
  - **3des**
  - (PAN-OS 10.1.0 and earlier releases) **des**

*Choose the strongest authentication and encryption algorithms that the peer can support. For the authentication algorithm, use SHA-256 or higher (SHA-384 or higher preferred for long-lived transactions). Don't use SHA-1 or MD5. For the encryption algorithm, use AES; DES and 3DES are weak and vulnerable. AES with Galois/Counter Mode (AES-GCM) provides the strongest security and has built-in authentication, so you must set Authentication to **non-auth** if you select **aes-256-gcm** or **aes-128-gcm** encryption.*

STEP 3 | Specify the duration for which the key is valid and the reauthentication interval.

For details, see SA Key Lifetime and Re-Authentication Interval.

1. In the **Key Lifetime** fields, specify the period (in seconds, minutes, hours, or days) for which the key is valid (range is 3 minutes to 365 days; default is 8 hours). When the key expires, the firewall renegotiates a new key. A lifetime is the period between each renegotiation.
2. For the **IKEv2 Authentication Multiple**, specify a value (range is 0-50; default is 0) that is multiplied by the **Key Lifetime** to determine the authentication count. The default value of zero disables the reauthentication feature.

STEP 4 | Commit your IKE Crypto profile.

Click **OK** and click **Commit**.

STEP 5 | Attach the IKE Crypto profile to the IKE Gateway configuration.

See Configure advanced options for the gateway.

Define IKE Crypto Profiles (Strata Cloud Manager)

Based on the IPSec device type you selected, Prisma Access provides a recommended set of ciphers and a key lifetime for the IKE Phase 1 key exchange process between:

- the private apps at your data center or headquarters location and Prisma Access—for a service connection
- the remote network site device and Prisma Access—for a remote network site

You can use the recommended settings, or customize the settings as needed for your environment.

- Select an **IKE Protocol Version** for your IPSec device and Prisma Access to use for IKE negotiation.

  If you select **IKEv1 Only Mode**, Prisma Access can use only the IKEv1 protocol for the negotiation. If you select **IKEv2 Only Mode**, Prisma Access can use only the IKEv2 protocol for the negotiation.

  If you select **IKEv2 Preferred Mode**, Prisma Access uses the IKEv2 protocol only if your IPSec device(for service connection)/branch IPSec device(for remote network site) also supports IKEv2. If your IPSec device does not support IKEv2, Prisma Access falls back to using the IKEv1 protocol.

- Add an **IKEv1 Crypto Profile** to customize the IKE crypto settings that define the encryption and authentication algorithms used for the key exchange process in IKE Phase 1.

  Prisma Access automatically uses a default IKE crypto profile based on the **Branch Device Type** that's being used to establish this tunnel.

  - **Encryption**—Specify the encryption algorithm used in the IKE SA negotiation.

    Prisma Access supports the following encryption algorithms: 3des (168 bits), aes-128-cbc (128 bits), aes-192-cbc (192 bits), aes-256-cbc (256 bits), and des (56 bits). You can also select null (no encryption).
  - **Authentication**—Specify the authentication algorithm used in the IKE SA negotiation.

    Prisma Access supports the following authentication algorithms: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits), and md5 (128 bits). You can also select null (no authentication).
  - **DH Group**—Specify the Diffie-Hellman (DH) groups used to generate symmetrical keys for IKE in the IKE SA negotiation. The Diffie-Hellman algorithm uses the private key of one party and the public key of the other to create a shared secret, which is an encrypted key that both VPN tunnel peers share.

    Prisma Access supports the following DH groups: Group 1 (768 bits), Group 2 (1024 bits—default), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 (256-bit elliptic curve group), and Group 20 (384-bit elliptic curve group). For the strongest security, select the group with the highest number.
  - **Lifetime**—Specify the unit and amount of time for which the IKE Phase 1 key is valid (default is 8 hours). For IKEv1, the security association (SA) is not actively re-keyed before the key lifetime expires. The IKEv1 Phase 1 re-key triggers only when the SA expires. For IKEv2, the SA must be re-keyed before the key lifetime expires. If the SA is not re-keyed upon expiration, the SA must begin a new Phase 1 key.
  - **IKEv2 Authentication Multiple**—Specify the value that is multiplied by the key lifetime to determine the authentication count (range is 0 to 50; default is 0). The authentication count is the number of times that the security processing node can perform IKEv2 IKE SA re-key before it must start over with IKEv2 re-authentication. The default value of 0 disables the re-authentication feature.

- Enable **IKE Passive Mode** so that Prisma Access only response to IKE connections and does not initiate them.

- **IKE NAT Traversal** is turned on by default.

  This means that UDP encapsulation is used on IKE and UDP protocols, enabling them to pass through network address translation (NAT) devices that are between the IPSec VPN tunnel endpoints.

Define IPSec Crypto Profiles

Where Can I Use This?	What Do I Need?
• Prisma Access	• No license required

Where Can I Use This?	What Do I Need?
• PAN-OS	• PAN-OS 10.1 and Later

The Internet Protocol Security (IPSec) profiles provide information about the algorithms that are used to authenticate, encrypt, and establish a shared secret between network sites when you establish an IPSec tunnel.

The IPSec Crypto profile is invoked in IKE Phase 2. It specifies how the data is secured within the tunnel when Auto Key IKE is used to generate keys automatically for the IKE SAs.

Regardless of whether your VPN peer is from the same vendor or not, the VPN peers must have the same IPSec parameters configured in order to perform a successful IPSec negotiation.

IPSec negotiation will be successful when the following parameters match between the VPN peers:

- IPSec Protocol (ESP or AH)
- DH Group (or PFS) for key exchange
- Encryption algorithms
- Authentication algorithms

For example, if you have configured VPN peer 1 with **ESP** for IPSec protocol, **group20** for DH group, **sha384** for authentication, and **aes-256-gcm** for encryption. Then, VPN peer 2 with which you want to establish the IPSec tunnel also should be configured exactly with the same values.

By default, perfect forward secrecy (PFS) is enabled on IPSec tunnels to generate a more randomized key. PFS does this by performing an additional key exchange during IPSec SA negotiation to generate a new shared secret and combines it into the new IPSec SA keys. When configuring PFS, ensure that both the VPN peers have the same PFS configuration. Any failure in IPSec SA negotiation will result in failure to establish the IPSec tunnel.

Follow this procedure to create an IPSec Crypto profile on a Palo Alto Networks firewall.

- PAN-OS and Prisma Access (Panorama Managed)
- Strata Cloud Manager

Define IPSec Crypto Profiles (PAN-OS 10.1 and Later &)

STEP 1 | Create a new IPSec profile.

1. Select **Network** > **Network Profiles** > **IPSec Crypto** and select **Add**.
2. Enter a **Name** for the new profile.
3. Select the **IPSec Protocol**—ESP or AH—that you want to apply to secure the data as it traverses across the tunnel.

   As a best practice, select ESP (Encapsulating Security Payload) over AH (Authentication Header) because ESP offers both confidentiality and authentication for the connection whereas AH offers only authentication.
4. Click **Add** and select the **Authentication** and **Encryption** algorithms for ESP, and **Authentication** algorithms for AH, so that the IKE peers can negotiate the keys for the secure transfer of data across the tunnel.

   If you aren't certain of what the IKE peers support, add multiple algorithms in the order of most-to-least secure as follows; the peers negotiate the strongest supported algorithm to establish the tunnel:

   - Encryption—**aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (the VM-Series firewall doesn't support this option), **aes-128-cbc**, **des** , **3des**.

     PAN-OS 10.1.0 and earlier releases support the Data Encryption Standard (DES) encryption algorithm.

     As a best practice, choose the strongest authentication and encryption algorithms the peer can support. For the authentication algorithm, use SHA-256 or higher (SHA-384 or higher preferred for long-lived transactions). Don't use SHA-1, MD5, or none. For the encryption algorithm, use AES; 3DES is weak and vulnerable.
   - Authentication—**sha512**, **sha384**, **sha256**, **sha1**, **md5**.

STEP 2 | Select the DH Group to use for the IPSec SA negotiations in IKE phase 2.

From **DH Group**, select the key strength you want to use: **group1**, **group2**, **group5**, **group14**, **group15**, **group16**, **group19**, **group20**, or **group21**. For the highest security, choose the group with the highest number.

*Beginning with PAN-OS 10.2.0 and later releases, **group15**, **group16**, and **group21** Diffie-Hellman (DH) groups are supported.*

If you don't want to renew the key that the firewall creates during IKE phase 1, select **no-pfs** (no perfect forward secrecy); the firewall reuses the current key for the IPSec security association (SA) negotiations.

STEP 3 | Specify the duration of the key—time and volume of traffic.

Using a combination of time and traffic volume allows you to ensure safety of data.

Select the **Lifetime** or time period for which the key is valid in seconds, minutes, hours, or days (range is 3 minutes to 365 days). When the specified time expires, the firewall will renegotiate a new set of keys.

Select the **Lifesize** or volume of data after which the keys must be renegotiated.

STEP 4 | Commit your IPSec profile.

Click **OK** and click **Commit**.

STEP 5 | Attach the IPSec Profile to an IPSec tunnel configuration.

See Set up key exchange.

Define IPSec Crypto Profiles (Strata Cloud Manager)

Based on the IPSec device type you selected, Prisma Access provides a recommended set of IPSec protocol and key lifetime settings to secure data within the IPSec tunnel between your:

- the private apps at your data center or headquarters location and Prisma Access in IKE Phase 2 for the Security Association (SA)—for a service connection
- branch device and Prisma Access in IKE Phase 2 for the Security Association (SA)—for a remote network site

You can use the recommended settings, or customize the settings as needed for your environment.

- Customize the **IPSec Crypto Profile** to define how data is secured within the tunnel when Auto Key IKE automatically generates keys for the IKE SAs during IKE Phase 2.

  Prisma Access automatically configures a default IPSec crypto profile based on the **Branch Device Type** vendor. You can either use the default profile or create a custom profile.

  - **IPSec Protocol**—Secure the data that traverses the VPN tunnel. The Encapsulating Security Payload (**ESP**) protocol encrypts the data, authenticates the source, and verifies the data integrity. The Authentication Header (**AH**) protocol authenticates the source and verifies the data integrity.

    If you use **ESP** as the IPSec protocol, also specify the **Encryption** algorithm used in the IPSec SA negotiation.

    Prisma Access supports the following encryption algorithms: aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits), and des (56 bits). You can also select null (no encryption).

- **Authentication**—Specify the authentication algorithm used in the IPSec SA negotiation.

  Prisma Access supports the following authentication algorithms: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits), and md5 (128 bits). If you set the IPSec Protocol to ESP, you can also select none (no authentication).

- **DH Group**—Specify the Diffie-Hellman (DH) groups for IKE in the IPSec security association (SA) negotiation.

  Prisma Access supports the following DH groups: Group 1 (768 bits), Group 2 (1024 bits—default), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 (256-bit elliptic curve group), and Group 20 (384-bit elliptic curve group). For the strongest security, select the group with the highest number. If you don't want to renew the key that Prisma Access creates during IKE phase 1, select **no-pfs** (no perfect forward secrecy). If you select this option, Prisma Access reuses the current key for the IPSec SA negotiation.

- **Lifetime**—Specify the unit and amount of time during which the negotiated key is valid (default is one hour).

- **Lifesize**—Specify the unit and amount of data that the key can use for encryption.

Set Up an IPSec Tunnel

Where Can I Use This?	What Do I Need?
• Prisma Access (IPSec tunnel transport mode is not yet supported for Prisma Access) • PAN-OS	No license required

IPSec is a suite of protocols used to secure communications between peers. IPSec provides strong cryptographic security services to protect sensitive data and ensures network privacy and integrity. IPSec can be configured to provide security for a wide range of network topologies, including site-to-site and remote access connections.

In IPSec, you can configure various settings, such as encryption and authentication algorithms and security associations timeouts. One such configuration is the IPSec mode—tunnel mode or transport mode.

Tunnel mode is commonly used in site-to-site VPNs where the communication between the complete networks or subnets needs to be protected. Transport mode is commonly used in end-to-end encryption between hosts. You can choose a tunnel or transport mode based on your network structure and data security requirements.

While configuring an IPSec tunnel, you can select the IPSec mode as tunnel or transport mode to establish a secure connection. That is, you can select whether to encrypt or authenticate packets in tunnel mode or transport mode. PAN-OS® supports tunnel mode by default, authenticating or encrypting the data (IP packet) as it traverses the tunnel. Beginning with PAN-OS 11.0.0, you can use transport mode.

Differences between Tunnel and Transport Mode

Tunnel Mode	Transport Mode
Encrypts the entire packet, including the IP header. A new IP header is added to the packet after encryption.	Encrypts only the payload, while the original IP header is retained.
Tunnel monitoring uses the tunnel interface IP address.	Tunnel monitoring automatically uses the IP address of the physical interface (gateway interface IP address), and the tunnel interface IP address is ignored.
Supports double encapsulation.	No support for double encapsulation.
Commonly used for site-to-site communications.	Commonly used for host-to-host communications.

Set Up an IPSec Tunnel (Tunnel Mode)

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • PAN-OS	• No license required • PAN-OS 10.1 and Later

The IPSec tunnel configuration allows you to authenticate and/or encrypt the data (IP packet) as it traverses the tunnel.

IPSec tunnel mode is the default mode. IPSec tunnel mode creates a secure connection between two endpoints by encapsulating packets in an additional IP header. This means, in tunnel mode, the IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer). Hence, tunnel mode provides better security by encrypting the entire original packet. Tunnel mode is commonly used for site-to-site communications.

If you're setting up the firewall to work with a peer that supports policy-based VPN, you must define Proxy IDs. Devices that support policy-based VPN use specific security rules/policies or access-lists (source addresses, destination addresses, and ports) for permitting interesting traffic through an IPSec tunnel. These rules are referenced during quick mode or IKE phase 2 negotiation, and are exchanged as proxy IDs in the first or the second message of the process. So, if you're configuring the firewall to work with a policy-based VPN peer, for a successful phase 2 negotiation you must define the proxy ID so that the setting on both peers is identical. If the proxy ID isn't configured, because the firewall supports route-based VPN, the default values used as proxy ID are source ip: 0.0.0.0/0, destination ip: 0.0.0.0/0 and application: any; and when these values are exchanged with the peer, it results in a failure to set up the VPN connection.

To establish an IPSec tunnel successfully, both IKE and IPSec negotiations should be successful:

- The IKE negotiation will be successful only when both VPN peers exchange compatible IKE parameters.
- The IKE Phase 2 (IPSec) negotiation will be successful only when both VPN peers exchange compatible IPSec parameters.
- PAN-OS
- Strata Cloud Manager
- Prisma Access (Panorama Managed)

Set Up an IPSec Tunnel (Tunnel Mode) (PAN-OS 10.1 and Later)

STEP 1 | Select **Network** > **IPSec Tunnels** and then **Add** a new tunnel configuration.

STEP 2 | On the **General** tab, enter a **Name** for the tunnel.

STEP 3 | Select the **Tunnel interface** on which to set up the IPSec tunnel.

To create a new tunnel interface:

1. Select **Tunnel Interface** > **New Tunnel Interface**. (You can also select **Network** > **Interfaces** > **Tunnel** and click **Add**.)
2. In the **Interface Name** field, specify a numeric suffix, such as **.2**.
3. On the **Config** tab, select the **Security Zone** list to define the zone as follows:

Use your trust zone as the termination point for the tunnel—Select the zone. Associating the tunnel interface with the same zone (and virtual router) as the external-facing interface on which the packets enter the firewall mitigates the need to create inter-zone routing.

Or:

Create a separate zone for VPN tunnel termination (Recommended)—Select **New Zone**, define a **Name** for the new zone (for example vpn-corp), and click **OK**.

1. For **Virtual Router**, select **default**.
2. (Optional) If you want to assign an IPv4 address to the tunnel interface, select the **IPv4** tab, and **Add** the IP address and network mask, for example 10.31.32.1/32.
3. Click **OK**.

STEP 4 | (Optional) Enable IPv6 on the tunnel interface.

1. Select the IPv6 tab on **Network** > **Interfaces** > **Tunnel** > **IPv6**.
2. Select **Enable IPv6 on the interface**.

   This option allows you to route IPv6 traffic over an IPv4 IPSec tunnel and will provide confidentiality between IPv6 networks. The IPv6 traffic is encapsulated by IPv4 and then ESP. To route IPv6 traffic to the tunnel, you can use a static route to the tunnel, or use OSPFv3, or use a policy-based forwarding (PBF) rule.
3. Enter the 64-bit extended unique **Interface ID** in hexadecimal format, for example, 00:26:08:FF:FE:DE:4E:29. By default, the firewall will use the EUI-64 generated from the physical interface's MAC address.
4. To assign an IPv6 **Address** to the tunnel interface, **Add** the IPv6 address and prefix length, for example 2001:400:f00::1/64. If Prefix isn't selected, the IPv6 address assigned to the interface will be wholly specified in the address text box.
   1. Select **Use interface ID as host portion** to assign an IPv6 address to the interface that will use the interface ID as the host portion of the address.
   2. Select **Anycast** to include routing through the nearest node.

STEP 5 | Set up key exchange.

On the **General** tab, configure one of the following types of key exchange:

Set up Auto Key exchange

1. Select the IKE Gateway. To set up an IKE gateway, see Set Up an IKE Gateway.
2. (Optional) Select the default IPSec Crypto profile. To create a new IPSec Profile, see Define IPSec Crypto Profiles.

Set up Manual Key exchange

1. Specify the **Local SPI** for the local firewall. SPI is a 32-bit hexadecimal index that is added to the header for IPSec tunneling to assist in differentiating between IPSec traffic flows; it's used to create the SA required for establishing a VPN tunnel.
2. Select the **Interface** that will be the tunnel endpoint, and optionally select the IP address for the local interface that is the endpoint of the tunnel.
3. Select the protocol to be used—**AH** or **ESP**.
4. For AH, select the **Authentication** method and enter a **Key** and then **Confirm Key**.
5. For ESP, select the **Authentication** method and enter a **Key** and then **Confirm Key**. Then, select the **Encryption** method and enter a **Key** and then **Confirm Key**, if needed.
6. Specify the **Remote SPI** for the remote peer.
7. Enter the **Remote Address**, the IP address of the remote peer.

STEP 6 | Protect against a replay attack.

Anti-replay is a sub-protocol of IPSec and is part of the Internet Engineering Task Force (IETF) Request for Comments (RFC) 6479. The anti-replay protocol is used to prevent hackers from injecting or making changes in packets that travel from a source to a destination and uses a unidirectional security association in order to establish a secure connection between two nodes in the network.

After a secure connection is established, the anti-replay protocol uses packet sequence numbers to defeat replay attacks. When the source sends a message, it adds a sequence number to its packet; the sequence number starts at 0 and is incremented by 1 for each subsequent packet. The destination maintains the sequence of numbers in a *sliding window* format, maintains a record of the sequence numbers of validated received packets, and rejects all packets that have a sequence number that is lower than the lowest in the sliding window (packets that are too old) or packets that already appear in the sliding window (duplicate or replayed packets). Accepted packets, after they're validated, update the sliding window, displacing the lowest sequence number out of the window if it was already full.

1. On the General tab, select **Show Advanced Options** and select **Enable Replay Protection** to detect and neutralize against replay attacks.
2. Select the **Anti Replay Window** to use. You can select an anti-replay window size of 64, 128, 256, 512, 1024, 2048, or 4096. The default is 1024.

STEP 7 | (Optional) Preserve the Type of Service header for the priority or treatment of IP packets.

In the Show Advanced Options section, select **Copy TOS Header**. This copies the Type of Service (ToS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original ToS information.

If there are multiple sessions inside the tunnel (each with a different ToS value), copying the ToS header can cause the IPSec packets to arrive out of order.

STEP 8 | By default, IPSec tunnels come up in **Tunnel** mode if you don't configure IPSec mode. You can also select **IPSec Mode** as **Tunnel** in the **Show Advanced Options** section to establish an IPSec in tunnel mode.

STEP 9 | (Optional) Select **Add GRE Encapsulation** to enable GRE over IPSec.

Add GRE encapsulation in cases where the remote endpoint requires traffic to be encapsulated within a GRE tunnel before IPSec encrypts the traffic. For example, some implementations require multicast traffic to be encapsulated before IPSec encrypts it. Add GRE Encapsulation when the GRE packet encapsulated in IPSec has the same source IP address and destination IP address as the encapsulating IPSec tunnel.

STEP 10 | Enable Tunnel Monitoring.

You must assign an IP address to the tunnel interface for monitoring.

To alert the device administrator to tunnel failures and to provide an automatic failover to another tunnel interface:

1. Select **Tunnel Monitor**.
2. Specify a **Destination IP** address on the other side of the tunnel to determine if the tunnel is working properly.
3. Select a **Profile** to determine the action upon tunnel failure. To create a new profile, see Define a Tunnel Monitoring Profile.

STEP 11 | Create a Proxy ID to identify the VPN peers.

This step is required only if the VPN peer uses a policy-based VPN.

1. Select **Network** > **IPSec Tunnels** and click **Add**.
2. Select the **Proxy IDs** tab.
3. Select the **IPv4** or **IPv6** tab.
4. Click **Add** and enter the **Proxy ID** name.
5. Enter the **Local** IP address or subnet for the VPN gateway.
6. Enter the **Remote** address for the VPN gateway.
7. Select the **Protocol**:
   - **Number**—Specify the protocol number (used for interoperability with third-party devices).
   - **Any**—Allows TCP and/or UDP traffic.
   - **TCP**—Specify the local port and remote port numbers.
   - **UDP**—Specify the local port and remote port numbers.
8. Click **OK**.

STEP 12 | Commit your changes.

Click **OK** and **Commit**.

Set Up an IPSec Tunnel (Tunnel Mode) (Strata Cloud Manager)

Use the following steps to set up an IPSec tunnel for your service connection or a remote network site.

The first tunnel you create is the primary tunnel for the service connection or a remote network site. You can then repeat this workflow to optionally set up a secondary tunnel. When both tunnels are up, the primary tunnel takes priority over the secondary tunnel. If the primary tunnel for a service connection or a remote network site goes down, the connection falls back to the secondary tunnel until the primary tunnel comes back up.

Based on the IPSec device you use to establish the tunnel for your service connection or a remote network site, Prisma Access provides built-in, recommended IKE and IPSec security settings. You can use the recommended settings to get started quickly, or customize them as needed for your environment.

Add Primary and Secondary IPSec VPN Tunnels

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | For a service connection, go to **Settings** > **Prisma Access Setup** > **Service Connections** and **Set Up** the primary tunnel. For a remote network site, go to **Settings** > **Prisma Access Setup**

> **Remote Networks** and **Set Up** the primary tunnel. If you've already set up a primary tunnel, you can continue here to also add a secondary tunnel.

1. Give the tunnel a descriptive **Name**.
2. Select the **Branch Device Type** for the IPSec device at the HQ/DC (for a service connection) or at the remote network site that you're using to establish the tunnel with Prisma Access.
3. For the **Branch Device IP Address**, choose to use either a **Static IP** address that identifies the tunnel endpoint or a **Dynamic** IP address.

   (For a service connection) If you set the **Branch Device IP Address** to **Dynamic**, you must also add the IKE ID for the HQ/DC (**IKE Local Identification**) or for Prisma Access (**IKE Peer Identification**) to enable the IPSec peers to authenticate.

   Because you do not have the values to use for the Prisma Access IKE ID (**IKE Peer Identification**) until the service connection is fully deployed, you would typically want to set the IKE ID for the HQ/DC (**IKE Local Identification**) rather than the Prisma Access IKE ID.

   (For a remote network site) If you set the **Branch Device IP Address** to **Dynamic**, you must also add the IKE ID for the remote network site (**IKE Local Identification**) or for Prisma Access (**IKE Peer Identification**) to enable the IPSec peers to authenticate.

   Because you do not have the values to use for the Prisma Access IKE ID (**IKE Peer Identification**) until the remote network is fully deployed, you would typically want to set the IKE ID for the remote network site (**IKE Local Identification**) rather than the Prisma Access IKE ID.

STEP 3 | **Turn on Tunnel Monitoring**.

Enter a Tunnel Monitoring **Destination IP** address on the HQ/DC network for Prisma Access to use determine whether the tunnel is up and, if your IPSec device uses policy-based VPN, enter the associated **Proxy ID**.

The tunnel monitoring IP address you enter is automatically added to the list of branch subnetworks.

STEP 4 | **Save** the tunnel settings.

To continue:

- Set up and customize advanced crypto settings for IKE and IPSec. See More IKE Options and More IPSec Options.
- Enable Routing for Your Remote Network (Cloud Management).

Set Up an IPSec Tunnel (Tunnel Mode) ()

With Prisma Access, Palo Alto Networks deploys and manages the security infrastructure globally to secure your remote networks and mobile users.

- **Service Connections**—If your Prisma Access license includes it, you have the option to establish IPSec tunnels to allow communication between internal resources in your network

and mobile users and users in your remote network locations. You could, for example, create a service connection to an authentication server in your organization's HQ or data center.

Even if you don't require a service connection for your HQ or data center, we recommend that you create one to allow network communication between mobile users and remote network locations, and between mobile users in different geographical locations.

- **Remote Networks**—Use remote networks to secure remote network locations, such as branches, and users in those branches with cloud-based next-generation firewalls. You can enable access to the subnetworks at each remote network location using either static routes, dynamic routing using BGP, or a combination of static and dynamic routes. All remote network locations that you onboard are fully meshed.

See how to set up an IPSec tunnel for a service connection and a remote network.

Set up an IPSec Tunnel (Service Connection)

STEP 1 | Select or add a new **IPSec Tunnel** configuration to access the private apps at your data center or headquarters location:

- If you have added a template to the Service_Conn_Template_Stack (or modified the predefined Service_Conn_Template) that includes an IPSec Tunnel configuration, select that **IPSec Tunnel** from the drop-down. Note that the tunnel you are creating for each service connection connects Prisma Access to the IPSec-capable device at each corporate location. The peer addresses in the IKE Gateway configuration must be unique for each tunnel. You can, however, re-use some of the other common configuration elements, such as Crypto profiles.

  The IPSec Tunnel you select from a template must use Auto Key exchange and IPv4 only. In addition, make sure that the IPSec tunnel, IKE gateway, and crypto profile names are 31 characters or less.

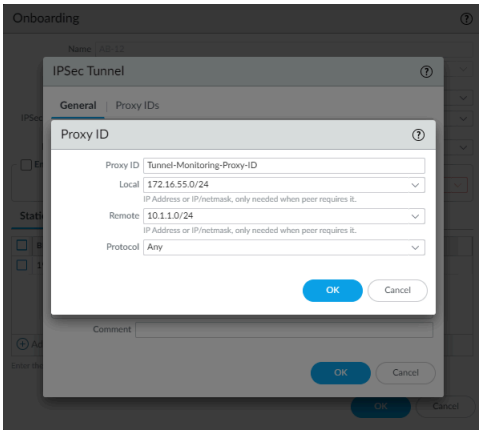
- To create a new IPSec Tunnel configuration, click **New IPSec Tunnel**, give it a **Name** and configure the IKE Gateway, IPSec Crypto Profile, and Tunnel Monitoring settings.
  - If the IPSec-capable device at your HQ or data center location uses policy-based VPN, on the **Proxy IDs** tab, **Add** a proxy ID that matches the settings configured on your local

IPSec device to ensure that Prisma Access can successfully establish an IPSec tunnel with your local device.

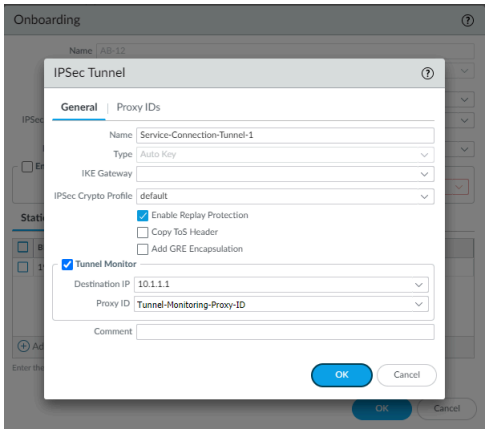
- Leave **Enable Replay Protection** selected to detect and neutralize against replay attacks.
- Select **Copy TOS Header** to copy the Type of Service (TOS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information.
- To enable tunnel monitoring for the service connection, select **Tunnel Monitor**.
  - Enter a **Destination IP** address.

    Specify an IP address at your HQ or data center site to which Prisma Access can send ICMP ping requests for IPSec tunnel monitoring. Make sure that this address is reachable by ICMP from the entire Prisma Access infrastructure subnet.
  - If you use tunnel monitoring with a peer device that uses multiple proxy IDs, specify a **Proxy ID** or add a **New Proxy ID** that allows access from the infrastructure subnet to your HQ or data center site.

    The following figure shows a proxy ID with the service infrastructure subnet (172.16.55.0/24 in this example) as the **Local** IP subnet and the HQ or data center's subnet (10.1.1.0/24 in this example) as the **Remote** subnet.



The following figure shows the Proxy ID you created being applied to the tunnel monitor configuration by specifying it in the **Proxy ID** field.



*You must configure a static route on your CPE to the Tunnel Monitor IP Address for tunnel monitoring to function. To find the destination IP address to use for tunnel monitoring from your data center or HQ network to Prisma Access, select **Panorama** > **Cloud Services** > **Status** > **Network Details**, click the **Service Infrastructure** radio button, and find the **Tunnel Monitor IP Address**.*

STEP 2 | BGP and hot potato routing deployments only—Select a service connection to use as the preferred backup (**Backup SC**).

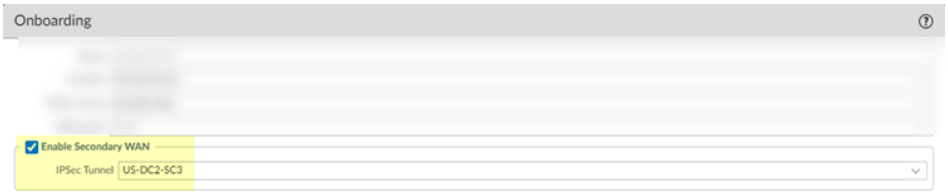
You can select any service connection that you have already added. Prisma Access uses the **Backup SC** you select as the preferred service connection in the event of a link failure. Selecting a backup service connection can prevent asymmetric routing issues if you have onboarded more than two service connections. This choice is available in Hot potato routing mode only.

STEP 3 | If you have a secondary WAN link at this location, select **Enable Secondary WAN** and then select or configure an **IPSec Tunnel** the same way you did to set up the primary IPSec tunnel.

If the primary WAN link goes down, Prisma Access detects the outage and establishes a tunnel to the headquarters or data center location over the secondary WAN link. If the primary WAN link becomes active, the link switches back to the primary link.

Configuring a Secondary WAN is not supported in the following deployments:

- If your secondary WAN is set up in active-active mode with the Primary IPSec tunnel.
- If your customer premises equipment (CPE) is set up in an Equal Cost Multipath (ECMP) configuration with the Primary and Secondary IPSec tunnel.



If you use static routes, tunnel failover time is less than 15 seconds from the time of detection, depending on your WAN provider.

If you configure BGP routing and have enabled tunnel monitoring, the shortest default hold time to determine that a security parameter index (SPI) is failing is the tunnel monitor, which removes all routes to a peer when it detects a tunnel failure for 15 consecutive seconds. In this way, the tunnel monitor determines the behavior of the BGP routes. If you do not configure tunnel monitoring, the hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271, which is the maximum wait time before Prisma Access removes a

route for an inactive SPI. If the peer BGP device has a shorter configured hold time, the BGP hold timer uses the lower value.

When the secondary tunnel is successfully installed, the secondary route takes precedence until the primary tunnel comes back up. If the primary and secondary are both up, the primary route takes priority.

If you use a different BGP peer for the secondary (backup) connection, Prisma Access does not honor the Multi-Exit Discriminator (MED) attributes advertised by the CPE. This caveat applies if you use multiple BGP peers on either remote network connections or service connections.

Set up an IPSec Tunnel (Remote Network)

STEP 1 | (Static routing or single-tunnel deployments only) Select or add a new **IPSec Tunnel** configuration to access the firewall, router, or SD-WAN device at the corporate location:

- Select one of the predefined IPSec templates in the Remote_Network_Template, or, if you have added a template to the Remote_Network_Template_Stack (or modified the predefined Remote_Network_Template) that includes an IPSec Tunnel configuration, select that **IPSec Tunnel** from the drop-down. Note that the tunnel you are creating for each remote network connection connects Prisma Access to the IPSec-capable device at each branch location.

  Use the following guidelines when configuring an IPSec tunnel:

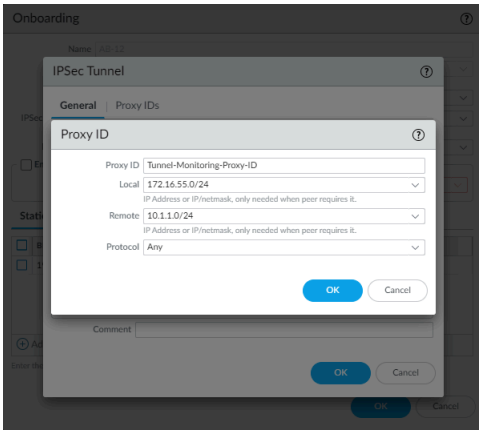
  - The peer addresses in the IKE Gateway configuration must be unique for each tunnel. You can, however, re-use some of the other common configuration elements, such as crypto profiles.
  - The IPSec Tunnel you select from a template must use Auto Key exchange and IPv4 only.
  - The IPSec tunnel, IKE gateway, and crypto profile names cannot be longer than 31 characters.
  - If you onboard multiple remote networks to the same location with dynamic IKE peers, you must use the same IKE crypto profile for all remote network configurations.
- To create a new IPSec Tunnel configuration, click **New IPSec Tunnel**, give it a **Name** and configure the IKE Gateway, IPSec Crypto Profile, and Tunnel Monitoring settings.
  - If the IPSec-capable device at your branch location uses policy-based VPN, on the **Proxy IDs** tab, **Add** a proxy ID that matches the settings configured on your local IPSec device

to ensure that Prisma Access can successfully establish an IPSec tunnel with your local device.

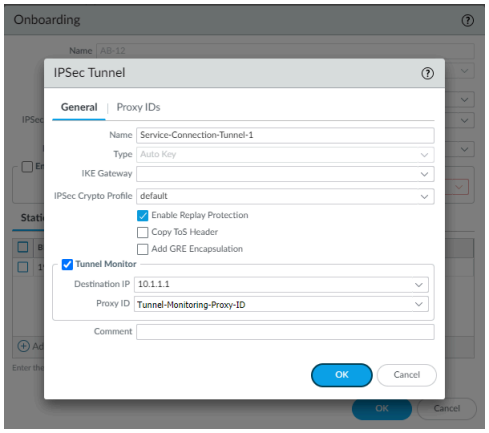
- Leave **Enable Replay Protection** selected to detect and neutralize against replay attacks.
- Select **Copy TOS Header** to copy the Type of Service (TOS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information.
- To enable tunnel monitoring for the service connection, select **Tunnel Monitor**.
  - Enter a **Destination IP** address.

    Specify an IP address at your branch location to which Prisma Access can send ICMP ping requests for IPSec tunnel monitoring. Make sure that this address is reachable by ICMP from the entire Prisma Access infrastructure subnet.
  - If you use tunnel monitoring with a peer device that uses multiple proxy IDs, specify a **Proxy ID** or add a **New Proxy ID** that allows access from the infrastructure subnet to your branch location.

    The following figure shows a proxy ID with the service infrastructure subnet (172.16.55.0/24 in this example) as the **Local** IP subnet and the branch location's subnet (10.1.1.0/24 in this example) as the **Remote** subnet.



The following figure shows the Proxy ID you created being applied to the tunnel monitor configuration by specifying it in the **Proxy ID** field.



*You must configure a static route on your CPE to the Tunnel Monitor IP Address for tunnel monitoring to function. To find the destination IP address to use for tunnel monitoring from your branch location to Prisma Access, select **Panorama** > **Cloud Services** > **Status** > **Network Details**, click the **Service Infrastructure** radio button, and find the **Tunnel Monitor IP Address**.*

STEP 2 | If you have a secondary WAN link at this location, select **Enable Secondary WAN**.

Be sure to create a unique IPSec tunnel for each remote network's secondary WAN; Prisma Access does not support reusing the same IPSec tunnel for secondary WANs in multiple remote networks.

Configuring a Secondary WAN is not supported in the following deployments:

- If your secondary WAN is set up in active-active mode with the Primary IPSec tunnel.
- If your customer premises equipment (CPE) is set up in an Equal Cost Multipath (ECMP) configuration with the Primary and Secondary IPSec tunnel.

If you use static routes, tunnel failover time is less than 15 seconds from the time of detection, depending on your WAN provider.

If you configure BGP routing and have enabled tunnel monitoring, the shortest default hold time to determine that a security parameter index (SPI) is failing is the tunnel monitor, which removes all routes to a peer when it detects a tunnel failure for 15 consecutive seconds. In this way, the tunnel monitor determines the behavior of the BGP routes. If you do not configure tunnel monitoring, the hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271, which is the maximum wait time before Prisma Access removes a route for an inactive SPI. If the peer BGP device has a shorter configured hold time, the BGP hold timer uses the lower value.

When the secondary tunnel is successfully installed, the secondary route takes precedence until the primary tunnel comes back up. If the primary and secondary are both up, the primary route takes priority.

If you use a different BGP peer for the secondary (backup) connection, Prisma Access does not honor the Multi-Exit Discriminator (MED) attributes advertised by the CPE. This caveat applies if you use multiple BGP peers on either remote network connections or service connections.

Set Up an IPSec Tunnel (Transport Mode)

Where Can I Use This?	What Do I Need?
• PAN-OS	• No license required • PAN-OS 11.0 and Later

Transport mode is new beginning with the PAN-OS 11.0.0 release and supports:

- IPv4 address only.
- Encapsulating Security Payload (ESP) protocol only.
- IKEv2 only.
- DH-group 20 for Diffie-Hellman (DH) group and PFS.
- Only AES with 256-bit keys in GCM mode.
- (PAN-OS 11.1.5 and later 11.1 versions) Proxy ID settings (using CLI commands) for IPSec negotiation.

You can choose the IPSec mode based on your networking requirements:

- If you want to encrypt the management plane protocol (such as BGP) packets exchanged between your next-generation firewall and the tunnel endpoint, then you must configure IPSec transport mode. Transport mode enables you to encrypt the control traffic (such as routing protocol and signalization messages) with the most robust protocol. With transport mode, you can encrypt the point-to-point traffic belonging to the firewall's IP address.
- If you want to encrypt the dataplane traffic exchanged between your next-generation firewall and the tunnel endpoint, then you must configure IPSec tunnel mode.

Important points to remember before enabling the transport mode:

- You can't select transport mode when NAT-T is enabled.
- You can't configure an IKE gateway on a loopback interface to an IPSec tunnel with transport mode.
- You can use transport mode only with an **auto-key** key exchange.
- If you configure an IKE gateway without an IPSec tunnel, by default IKE negotiates a tunnel mode child security association (SA).
- In IPSec transport mode without GRE encapsulation, don't route the user traffic through the associated tunnel interface. Configure the control protocols (like BGP peering sessions) on a physical interface (for example, ethernet1/1) instead of a tunnel interface. While IPSec tunnel mode for BGP routes works with the tunnel interface, IPSec transport mode for BGP routes works with the physical interface only.
- By default, the IPSec tunnel operates in **Tunnel** mode.
- You should enable **Add GRE Encapsulation** in **Transport** mode to encapsulate multicast packets.

Because PAN-OS 10.2 and earlier versions don't support transport mode, any downgrades to the previous versions will result in compatibility issues. Before downgrade, you must manually remove any transport mode tunnels or switch to tunnel mode. Otherwise, the downgrade will result in a failure.

To establish an IPSec tunnel successfully, both IKE and IPSec negotiations should be successful:

- The IKE negotiation will be successful only when both VPN peers exchange compatible IKE parameters.
- The IKE Phase 2 (IPSec) negotiation will be successful only when both VPN peers exchange compatible IPSec parameters.
- PAN-OS

Set Up an IPSec Tunnel (Transport Mode) (PAN-OS 11.0 and Later)

STEP 1 | Select **Network** > **IPSec Tunnels** and then **Add** a new tunnel configuration.

STEP 2 | On the **General** tab, enter a **Name** for the tunnel.

STEP 3 | Select the **Tunnel interface** on which to set up the IPSec tunnel.

To create a new tunnel interface:

1. Select **Tunnel Interface** > **New Tunnel Interface**. (You can also select **Network** > **Interfaces** > **Tunnel** and click **Add**.)
2. In the **Interface Name** field, specify a numeric suffix, such as **.2**.
3. On the **Config** tab, select the **Security Zone** list to define the zone as follows:

   Use your trust zone as the termination point for the tunnel—Select the zone. Associating the tunnel interface with the same zone (and virtual router) as the external-facing interface on which the packets enter the firewall mitigates the need to create inter-zone routing.

   Or:

   Create a separate zone for VPN tunnel termination (Recommended)—Select **New Zone**, define a **Name** for the new zone (for example vpn-corp), and click **OK**.
4. For **Virtual Router**, select **default**.
5. (Optional) If you want to assign an IPv4 address to the tunnel interface, select the **IPv4** tab, and **Add** the IP address and network mask, for example 10.31.32.1/32.

   When you configure transport mode without **GRE Encapsulation**, PAN-OS ignores any tunnel interface IP address configured on the tunnel interface. Hence, you don't need to configure an IP address for the tunnel interface (even if you enable the tunnel monitoring option). When you configure transport mode with **GRE Encapsulation**, PAN-OS uses the tunnel interface IP address for the GRE header. Therefore, you can use this method for dynamic and multicast routing (OSPF, BGP, and PIM).
6. Click **OK**.

STEP 4 | Set up key exchange.

On the **General** tab, configure Auto key exchange:

Set up Auto Key exchange

1. Select the IKE Gateway. To set up an IKE gateway, see Set Up an IKE Gateway.
2. (Optional) Select the default IPSec Crypto profile. To create a new IPSec Profile, see Define IPSec Crypto Profiles.

You can use transport mode only with an auto-key exchange.

STEP 5 | Protect against a replay attack.

Anti-replay is a sub-protocol of IPSec and is part of the Internet Engineering Task Force (IETF) Request for Comments (RFC) 6479. The anti-replay protocol is used to prevent hackers from

injecting or making changes in packets that travel from a source to a destination and uses a unidirectional security association in order to establish a secure connection between two nodes in the network.

After a secure connection is established, the anti-replay protocol uses packet sequence numbers to defeat replay attacks. When the source sends a message, it adds a sequence number to its packet; the sequence number starts at 0 and is incremented by 1 for each subsequent packet. The destination maintains the sequence of numbers in a *sliding window* format, maintains a record of the sequence numbers of validated received packets, and rejects all packets that have a sequence number that is lower than the lowest in the sliding window (packets that are too old) or packets that already appear in the sliding window (duplicate or replayed packets). Accepted packets, after they're validated, update the sliding window, displacing the lowest sequence number out of the window if it was already full.

1. On the General tab, select **Show Advanced Options** and select **Enable Replay Protection** to detect and neutralize against replay attacks.
2. Select the **Anti Replay Window** to use. You can select an anti-replay window size of 64, 128, 256, 512, 1024, 2048, or 4096. The default is 1024.

STEP 6 | (Optional) Preserve the Type of Service header for the priority or treatment of IP packets.

In the Show Advanced Options section, select **Copy TOS Header**. This copies the Type of Service (ToS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original ToS information.

In transport mode, the IP header before encapsulation is called the "inner," and the IP header after encapsulation is called the "outer". When you enable GRE Encapsulation, ToS is copied first to the GRE header, and then to the ESP header.

If there are multiple sessions inside the tunnel (each with a different ToS value), copying the ToS header can cause the IPSec packets to arrive out of order.

STEP 7 | In the **Show Advanced Options** section, select the **IPSec Mode** as **Transport** to establish an IPSec tunnel in transport mode.

STEP 8 | (Optional) Select **Add GRE Encapsulation** to enable GRE over IPSec.

Add GRE encapsulation in cases where the remote endpoint requires traffic to be encapsulated within a GRE tunnel before IPSec encrypts the traffic. For example, some implementations require multicast traffic to be encapsulated before IPSec encrypts it. Add GRE Encapsulation when the GRE packet encapsulated in IPSec has the same source IP address and destination IP address as the encapsulating IPSec tunnel.

As IPSec transport mode reuses the packet's IP header, it can't encapsulate multicast packets like OSPF. To encapsulate multicast packets, enable the **GRE Encapsulation** option of an IPSec tunnel to first convert the packet to a unicast GRE packet (the IP address of the tunnel interface will be used). Using a separate GRE tunnel to encapsulate the packet first and then forward it to the transport mode tunnel won't work. Due to IPSec transport mode's lack of support for double encapsulation, double encapsulation can't be used. The previously mentioned **GRE Encapsulation** option works because PAN-OS treats that as a single encapsulation.

STEP 9 | Enable Tunnel Monitoring.

Tunnel monitoring in transport mode automatically uses the IP address of the physical interface (gateway interface IP), ignoring tunnel interface IP addresses. Therefore, it isn't necessary to assign an IP address to the tunnel interface.

To alert the device administrator to tunnel failures and to provide an automatic failover to another tunnel interface:

1. Select **Tunnel Monitor**.
2. Specify a **Destination IP** address on the other side of the tunnel to determine if the tunnel is working properly.
3. Select a **Profile** to determine the action upon tunnel failure. To create a new profile, see Define a Tunnel Monitoring Profile.

STEP 10 | Commit your changes.

Click **OK** and **Commit**.

Monitor Your IPSec VPN Tunnel

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

Tunnel Monitoring

For a VPN tunnel, you can check connectivity to a destination IP address across the tunnel. The network monitoring profile on the firewall allows you to verify connectivity (using ICMP) to a destination IP address or a next hop at a specified polling interval, and to specify an action on failure to access the monitored IP address.

If the destination IP address is unreachable, you either configure the firewall to wait for the tunnel to recover or configure an automatic failover to another tunnel. In either case, the firewall generates a system log that alerts you to a tunnel failure and renegotiates the IPSec keys to accelerate recovery.

To provide uninterrupted VPN service, you can use the Dead Peer Detection capability along with the tunnel monitoring capability on the firewall. A DPD (Dead Peer Detection) profile provides information about the number of seconds to wait in between probes to detect if an IPSec peer site is alive or not. The liveness check for IKEv2 is similar to DPD, which IKEv1 uses as the way to determine whether a peer is still available.

You can also monitor the status of the tunnel. These monitoring tasks are described in the following sections:

- Define a Tunnel Monitoring Profile
- View the Tunnel Status

For troubleshooting purposes, you can Enable/Disable, Refresh or Restart an IKE Gateway or IPSec Tunnel.

Liveness Check

If there has only been outgoing traffic on all of the SAs associated with an IKE SA, it is essential to confirm the liveness of the other endpoint to avoid black holes. IKEv2 gateways can perform liveness checks to prevent sending messages to a dead peer. Receipt of a fresh cryptographically protected message on an IKE SA or any of its child SAs ensures the liveness of the IKE SA and all of its child SAs.

IKEv2 uses a liveness check (similar to Dead Peer Detection (DPD) in IKEv1) to determine whether a peer is still available. The liveness check option is enabled by default. Select **Network** > **Network Profiles** > **IKE Gateways** and **Advanced Options** to configure the interval (in seconds) in the **Liveness Check** for the IKE gateway. Note that you can configure the liveness check option only if you have selected **IKEv2 only mode** or **IKEv2 preferred mode** for the **Version** in the **IKE Gateway** (**Network** > **Network Profiles** > **IKE Gateways**) configuration. If you select **IKEv1 only mode** for the IKE Gateway **Version**, then the **Advanced Options** would display IKEv1 configuration parameters such as, **Exchange mode** and **Dead Peer Detection**.

In IKEv2, the liveness check is achieved by any IKEv2 packet transmission or a liveness check message that the gateway sends to the peer at a configurable interval, 5 seconds by default. If there is no response, the sender attempts the retransmission up to 10 times with increasing timeout (in seconds) for each retry as follows:

5 + 10 + 20 + 40 + 60 + 60 + 60 + 60 + 60 + 60 = 7 minutes and 15 seconds

If it doesn't get a response, the sender closes and deletes the IKE_SA and corresponding CHILD_SAs. The sender will start over by sending out another IKE_SA_INIT message.

After maximum retries are reached, the firewall will tear down phase 1 and phase 2 (child) SAs.

Define a Tunnel Monitoring Profile

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

A tunnel monitoring profile allows you to verify connectivity between the VPN peers; you can configure the tunnel interface to ping a destination IP address at a specified interval and specify the action if the communication across the tunnel is broken.

STEP 1 | Select **Network** > **Network Profiles** > **Monitor**. A default tunnel monitoring profile is available for use.

STEP 2 | Click **Add**, and enter a **Name** for the profile.

STEP 3 | Select the **Action** to take if the destination IP address is unreachable.

- **Wait Recover**—the firewall waits for the tunnel to recover. It continues to use the tunnel interface in routing decisions as if the tunnel were still active.
- **Fail Over**—forces traffic to a secondary path if one is available. The firewall disables the tunnel interface, and thereby disables any routes in the routing table that use the interface.

In either case, the firewall attempts to accelerate the recovery by negotiating new IPSec keys.

STEP 4 | Specify the **Interval (sec)** and **Threshold** to trigger the specified action.

- **Threshold** specifies the number of heartbeats to wait before taking the specified action (range is 2-100; default is 5).
- **Interval (sec)** specifies the time (in seconds) between heartbeats (range is 2-10; default is 3).

STEP 5 | Attach the monitoring profile to the IPSec tunnel configuration.

- When you **Add** a new tunnel configuration (**Network** > **IPSec Tunnels**), you can attach the monitoring profile that you created.
- On the General tab, select **Show Advanced Options** and enable **Tunnel Monitor**. You must assign an IP address to the tunnel interface for monitoring.
- Specify a **Destination IP** address on the other side of the tunnel to determine if the tunnel is working properly.
- Select the default tunnel monitoring **Profile** or the one you created to determine the action upon tunnel failure.

View the Tunnel Status

Where Can I Use This?	What Do I Need?
• PAN-OS • Strata Cloud Manager	❑ No license required ❑ AIOps for NGFW Premium license

The status of the tunnel informs you about whether or not valid IKE phase-1 and phase-2 SAs have been established, and whether the tunnel interface is up and available for passing traffic.

Because the tunnel interface is a logical interface, it can't indicate a physical link status. Therefore, you must enable tunnel monitoring so that the tunnel interface can verify connectivity to an IP address and determine if the path is still usable. If the IP address is unreachable, the firewall can take action accordingly, that is, the firewall will either wait for the tunnel to recover or failover. When a failover occurs, the existing tunnel is torn down, and routing changes are triggered to set up a new tunnel and redirect traffic. You can specify the number of heartbeats to wait before taking the specified action. You can also specify the interval between heartbeats to trigger the specified action. For tunnel monitoring, a monitor status of down is an indicator that the destination IP address being monitored is not reachable, and off indicates that the tunnel monitor is not configured.

You can view the following status of an IPSec VPN tunnel:

- IPSec tunnel status—Provides the connection status for an IPSec VPN session.
- IKE gateway status—Provides the IKE phase 1 SA status
- VPN flow or tunnel interface status—Provides the IPSec tunnel interface status

You can also execute the show commands in the command-line interface to view status information about active IPSec tunnels. The show commands display status output for all the IPSec tunnels, and it also displays tunnel information individually when you specify the tunnel ID.

- PAN-OS
- Strata Cloud Manager

View the Tunnel Status ()

STEP 1 | Select **Network** > **IPSec Tunnels**.

STEP 2 | View the **Tunnel Status**.

- Green indicates a valid IPSec SA tunnel.
- Red indicates that IPSec SA isn't available or has expired.

STEP 3 | View the **IKE Gateway Status**.

- Green indicates a valid IKE phase-1 SA.
- Red indicates that IKE phase-1 SA isn't available or has expired.

STEP 4 | View the **Tunnel Interface Status**.

- Green indicates that the tunnel interface is up.
- Red indicates that the tunnel interface is down, because tunnel monitoring is enabled and the status is down.

To troubleshoot a VPN tunnel that isn't yet up, see Interpret VPN Error Messages.

View the Tunnel Status (Strata Cloud Manager)

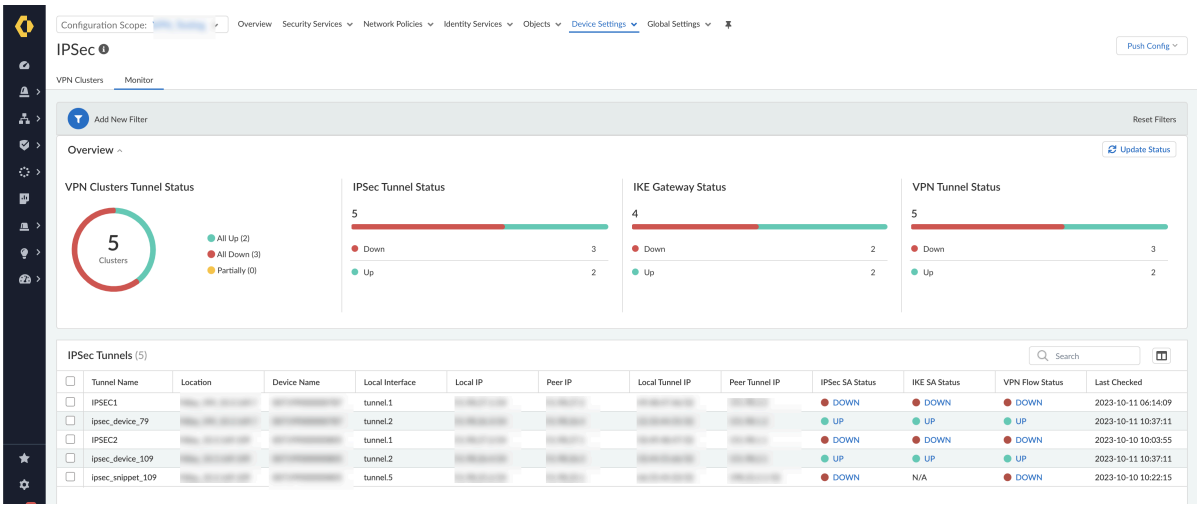
STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Device Settings** > **IPSec Tunnels** and select **Monitor**.

STEP 3 | Select the **Configuration Scope** to view the IPSec VPN tunnel status. You can select a folder or firewall from your **Folders** to monitor the IPSec VPN tunnel that you created on the firewalls:

- To view the status of the IPSec tunnels on all the firewalls, select the **All Firewalls** folder.
- To view the status of the IPSec tunnels for the group of firewalls associated with a folder, select the specific folder.
- To view the status of the IPSec tunnels on a specific firewall, select the firewall.

- *If you have created the VPN cluster using Auto VPN, then monitor those tunnels in the **Auto VPN** (**Manage** > **Configuration** > **NGFW and Prisma Access** > **Global Settings** > **Auto VPN**) page.*
- *You can monitor only on-premises firewalls and not the components managed by Prisma Access.*
- *Monitoring is disabled at the Global and snippet level. Therefore, you can create an IPSec tunnel in the global or snippet configuration scope, but you can monitor the IPSec tunnel only in the folder or firewall level.*



STEP 4 | View the **VPN Cluster Tunnel Status** that provides the graphical representation of the number of tunnels that are up, the number of tunnels that are down, and the number of tunnels that are partially up.

STEP 5 | View the **IPSec SA Status** in **IPSec Tunnels**.

- Green (**UP**) indicates a valid IPSec SA tunnel. Select **UP** to view detailed information about the IPSec tunnel.
- Red (**DOWN**) indicates that IPSec SA isn't available or has expired. Select **DOWN** to view the detailed information to interpret the reason for failure.

STEP 6 | View the **IKE SA Status** in **IPSec Tunnels**.

- Green (**UP**) indicates a valid IKE phase-1 SA. Select **UP** to view detailed information about the IKE gateway.
- Red (**DOWN**) indicates that IKE phase-1 SA isn't available or has expired. Select **DOWN** to view the detailed information to interpret the reason for failure.

STEP 7 | View the **VPN Flow Status** for VPN traffic flow information in **IPSec Tunnels**.

- Green (**UP**) indicates that the IPSec tunnel is up. Select **UP** to view detailed information about the VPN traffic flow.
- Red (**DOWN**) indicates that the IPSec tunnel is down. Select **DOWN** to view the detailed information to interpret the reason for failure.

STEP 8 | Select **Add New Filter**, and select the field to view the results based on the selected field. For example, **Add New Filter** by selecting the **Device Name** from the list, to view the IPSec tunnel status for the selected device.

Select **Reset Filters** Reset Filters to remove one or more filters.

STEP 9 | Select **Update Status** to update all the IPSec tunnel monitoring data present at that level (firewall, folder, or all firewalls).

Enable, Disable, Refresh, or Restart an IKE Gateway or IPSec Tunnel

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

You can enable, disable, refresh, or restart an IKE gateway or VPN tunnel to make troubleshooting easier.

Enable or Disable an IKE Gateway or IPSec Tunnel

Enable or disable an IKE gateway or IPSec tunnel to make troubleshooting easier.

- Enable or disable an IKE gateway.
  1. Select **Network** > **Network Profiles** > **IKE Gateways** and select the gateway you want to enable or disable.
  2. At the bottom of the screen, click **Enable** or **Disable**.

- Enable or disable an IPSec tunnel.
  1. Select **Network** > **IPSec Tunnels** and select the tunnel you want to enable or disable.
  2. At the bottom of the screen, click **Enable** or **Disable**.

Refresh or Restart an IKE Gateway or IPSec Tunnel

You can refresh or restart an IKE gateway or IPSec tunnel. The refresh and restart behaviors for an IKE gateway and IPSec tunnel are as follows:

Phase	Refresh	Restart
IKE Gateway (IKE Phase 1)	Updates the onscreen statistics for the selected IKE gateway. Equivalent to issuing a second `show` command in the CLI (after an initial `show` command).	Restarts the selected IKE gateway. **IKEv2**: Also restarts any associated child IPSec security associations (SAs). **IKEv1**: Doesn't restart the associated IPSec SAs. A restart is disruptive to all existing sessions. Equivalent to issuing a **`clear`**, **`test`**, **`show`** command sequence in the CLI.
IPSec Tunnel	Updates the onscreen statistics for the selected IPSec tunnel.	Restarts the IPSec tunnel.

Phase	Refresh	Restart
(IKE Phase 2)	Equivalent to issuing a second `show` command in the CLI (after an initial `show` command).	A restart is disruptive to all existing sessions. Equivalent to issuing a **`clear`**, **`test`**, **`show`** command sequence in the CLI.

Keep in mind that the result of restarting an IKE gateway depends on whether its IKEv1 or IKEv2.

- Refresh or restart an IKE gateway.
  1. Select **Network** > **IPSec Tunnels** and select the tunnel for the gateway you want to refresh or restart.
  2. In the row for that tunnel, under the Status column, click **IKE Info**.
  3. At the bottom of the IKE Info screen, click the action you want:
     - **Refresh**—Updates the statistics on the screen.
     - **Restart**—Clears the SAs, so traffic is dropped until the IKE negotiation starts over and the tunnel is recreated.

- Refresh or restart an IPSec tunnel.

  You might determine that the tunnel needs to be refreshed or restarted because you use the tunnel monitor to monitor the tunnel status, or you use an external network monitor to monitor network connectivity through the IPSec tunnel.
  1. Select **Network** > **IPSec Tunnels** and select the tunnel you want to refresh or restart.
  2. In the row for that tunnel, under the Status column, click **Tunnel Info**.
  3. At the bottom of the Tunnel Info screen, click the action you want:
     - **Refresh**—Updates the onscreen statistics.
     - **Restart**—Clears the SAs, so traffic is dropped until the IKE negotiation starts over and the tunnel is recreated.

Site-to-Site VPN Configuration Examples

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

This chapter discusses about some common site-to-site VPN deployments. In a real-time scenario, deployments can have challenges where different sites use different protocols to route the traffic. In the examples, we provide the step-by-step procedure on how to configure the Layer 3 interface on each firewall, create a tunnel interface and attach it to a virtual router and security zone, configure crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2), configure IKE gateway, configure IPSec tunnel, and create policy rules to allow traffic between the sites.

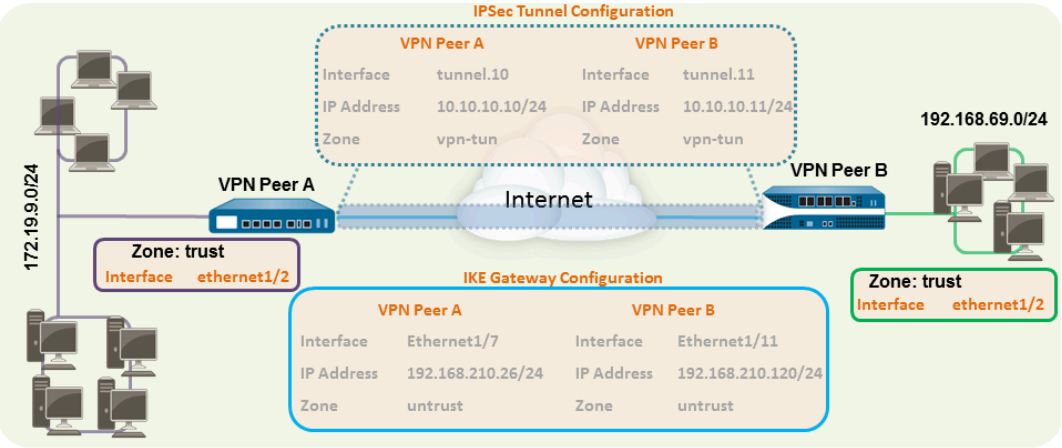
- Site-to-site VPN deployment with static routes—The static routing example deployment consist of different sites that use static routes for routing the traffic. Static routing does not use any protocols.

  Static routes require manual configuration on every router in the network, rather than the firewall entering dynamic routes in its route tables; even though static routes require that configuration on all routers, they may be desirable in small networks rather than configuring a routing protocol.
- Site-to-site VPN deployment with OSPF—The dynamic routing example deployment where the different sites involved in the deployment use only OSPF for routing the traffic dynamically. Dynamic routing uses various distance vector protocols. OSPF is one of the link state protocols used for dynamic routing to adjust routes.
- Site-to-site VPN deployment with Static and Dynamic Routing—The deployment where the routing protocol isn't the same between the sites. In this deployment example, one site uses static routes and the other site uses OSPF.

Site-to-Site VPN with Static Routing

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

The following example shows a VPN connection between two sites that use static routes. Without dynamic routing, the tunnel interfaces on VPN Peer A and VPN Peer B don't require an IP address because the firewall automatically uses the tunnel interface as the next hop for routing traffic across the sites. However, to enable tunnel monitoring, a static IP address has been assigned to each tunnel interface.



STEP 1 | Configure a Layer 3 interface.

This interface is used for the IKE phase-1 tunnel.

1. Select **Network** > **Interfaces** > **Ethernet** and then select the interface you want to configure for VPN.
2. Select **Layer3** from the **Interface Type**.
3. On the **Config** tab, select the **Security Zone** to which the interface belongs:
   - The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.
   - If you haven't yet created the zone, select **New Zone** from the **Security Zone**, define a **Name** for the new zone, and then click **OK**.
4. Select the **Virtual Router** to use.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.210.26/24.
6. To save the interface configuration, click **OK**.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—ethernet1/7
   - **Security Zone**—untrust
   - **Virtual Router**—default
   - **IPv4**—192.168.210.26/24

   The configuration for VPN Peer B is:

   - **Interface**—ethernet1/11
   - **Security Zone**—untrust
   - **Virtual Router**—default
   - **IPv4**—192.168.210.120/24

STEP 2 | Create a tunnel interface and attach it to a virtual router and security zone.

1. Select **Network** > **Interfaces** > **Tunnel** and click **Add**.
2. In the **Interface Name** field, specify a numeric suffix, such as **.1**.
3. On the **Config** tab, expand the **Security Zone** to define the zone as follows:
   - To use your trust zone as the termination point for the tunnel, select the zone.
   - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for a new zone (for example *vpn-tun*), and then click **OK**.
4. Select the **Virtual Router**.
5. (Optional) Assign an IP address to the tunnel interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface.

   With static routes, the tunnel interface doesn't require an IP address. For traffic that is destined to a specified subnet/IP address, the tunnel interface will automatically become the next hop. Consider adding an IP address if you want to enable tunnel monitoring.
6. To save the interface configuration, click **OK**.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—tunnel.10
   - **Security Zone**—vpn_tun
   - **Virtual Router**—default
   - **IPv4**—172.19.9.2/24

   The configuration for VPN Peer B is:

   - **Interface**—tunnel.11
   - **Security Zone**—vpn_tun
   - **Virtual Router**—default
   - **IPv4**—192.168.69.2/24

STEP 3 | Configure a static route, on the virtual router, to the destination subnet.

1. Select **Network** > **Virtual Router** and click the router you defined in the prior step.
2. Select **Static Route**, click **Add**, and enter a new route to access the subnet that is at the other end of the tunnel.

   In this example, the configuration for VPN Peer A is:

   - **Destination**—192.168.69.0/24
   - **Interface**—tunnel.10

   The configuration for VPN Peer B is:

   - **Destination**—172.19.9.0/24
   - **Interface**—tunnel.11

STEP 4 | Set up the crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2).

Complete this task on both peers and make sure to set identical values.

1. Select **Network** > **Network Profiles** > **IKE Crypto**. In this example, we use the default profile.
2. Select **Network** > **Network Profiles** > **IPSec Crypto**. In this example, we use the default profile.

STEP 5 | Set up the IKE Gateway.

1. Select **Network** > **Network Profiles** > **IKE Gateway**.
2. Click **Add** and configure the options in the **General** tab.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—ethernet1/7
   - **Local IP address**—192.168.210.26/24
   - **Peer IP type/address**—static/192.168.210.120
   - **Preshared keys**—enter a value
   - **Local identification**—None; this means that the local IP address will be used as the local identification value.
   - The configuration for VPN Peer B is:
   - **Interface**—ethernet1/11
   - **Local IP address**—192.168.210.120/24
   - **Peer IP type/address**—static/192.168.210.26
   - **Preshared keys**—enter same value as on Peer A
   - **Local identification**—None
3. Select **Advanced Phase 1 Options** and select the IKE Crypto profile you created earlier to use for IKE phase 1.

STEP 6 | Set up the IPSec Tunnel.

1. Select **Network** > **IPSec Tunnels**.
2. Click **Add** and configure the options in the **General** tab.

   In this example, the configuration for VPN Peer A is:

   - **Tunnel Interface**—tunnel.10
   - **Type**—Auto Key
   - **IKE Gateway**—Select the IKE Gateway defined above.
   - **IPSec Crypto Profile**—Select the IPSec Crypto profile defined in step 4.

   The configuration for VPN Peer B is:

   - **Tunnel Interface**—tunnel.11
   - **Type**—Auto Key
   - **IKE Gateway**—Select the IKE Gateway defined above.
   - **IPSec Crypto Profile**—Select the IPSec crypto defined in step 4.
3. (Optional) Select **Show Advanced Options**, select **Tunnel Monitor**, and specify a Destination IP address to ping for verifying connectivity. Typically, the tunnel interface IP address for the VPN Peer is used.
4. (Optional) To define the action on failure to establish connectivity, see Define a Tunnel Monitoring Profile.

STEP 7 | Create policy rules to allow traffic between the sites (subnets).

1. Select **Policies** > **Security**.
2. Create rules to allow traffic between the untrust and the vpn-tun zone and the vpn-tun and the untrust zone for traffic originating from specified source and destination IP addresses.

STEP 8 | Commit any pending configuration changes.

Click **Commit**.

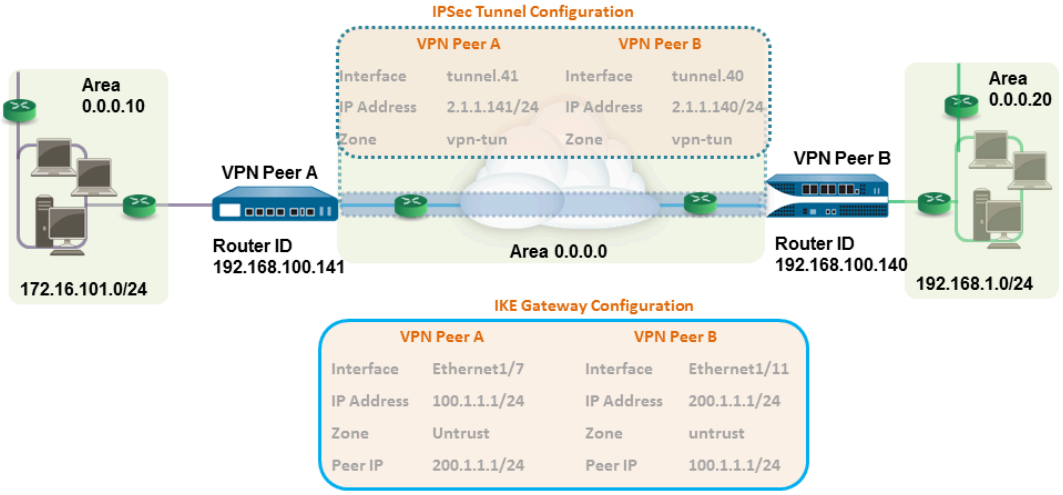
STEP 9 | Troubleshoot Your IPSec VPN Tunnel Connection.

See also View the Status of the Tunnels.

Site-to-Site VPN with OSPF

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

In this example, each site uses OSPF for dynamic routing of traffic. The tunnel IP address on each VPN peer is statically assigned and serves as the next hop for routing traffic between the two sites.



STEP 1 | Configure the Layer 3 interfaces on each firewall.

1. Select **Network** > **Interfaces** > **Ethernet** and then select the interface you want to configure for VPN.
2. Select **Layer3** from the **Interface Type** list.
3. On the **Config** tab, select the **Security Zone** to which the interface belongs:
   - The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.
   - If you haven't yet created the zone, select **New Zone** from the **Security Zone** list, define a **Name** for the new zone, and then click **OK**.
4. Select the **Virtual Router** to use.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.210.26/24.
6. To save the interface configuration, click **OK**.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—ethernet1/7
   - **Security Zone**—untrust
   - **Virtual Router**—default
   - **IPv4**—100.1.1.1/24

   The configuration for VPN Peer B is:

   - **Interface**—ethernet1/11
   - **Security Zone**—untrust
   - **Virtual Router**—default
   - **IPv4**—200.1.1.1/24

STEP 2 | Create a tunnel interface and attach it to a virtual router and security zone.

1. Select **Network** > **Interfaces** > **Tunnel** and click **Add**.
2. In the **Interface Name** field, specify a numeric suffix, such as, **.11**.
3. On the **Config** tab, expand **Security Zone** to define the zone as follows:
   - To use your trust zone as the termination point for the tunnel, select the zone.
   - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for the new zone (for example, vpn-tun), and then click **OK**.
4. Select the **Virtual Router**.
5. Assign an IP address to the tunnel interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask/prefix to assign to the interface, for example, 172.19.9.2/24.

   This IP address will be used as the next hop IP address to route traffic to the tunnel and can also be used to monitor the status of the tunnel.
6. To save the interface configuration, click **OK**.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—tunnel.41
   - **Security Zone**—vpn_tun
   - **Virtual Router**—default
   - **IPv4**—2.1.1.141/24

   The configuration for VPN Peer B is:

   - **Interface**—tunnel.40
   - **Security Zone**—vpn_tun
   - **Virtual Router**—default
   - **IPv4**—2.1.1.140/24

STEP 3 | Set up the crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2).

Complete this task on both peers and make sure to set identical values.

1. Select **Network** > **Network Profiles** > **IKE Crypto**. In this example, we use the default profile.
2. Select **Network** > **Network Profiles** > **IPSec Crypto**. In this example, we use the default profile.

STEP 4 | Set up the OSPF configuration on the virtual router and attach the OSPF areas with the appropriate interfaces on the firewall.

For more information on the OSPF options that are available on the firewall, see Configure OSPF.

Use Broadcast as the link type when there are more than two OSPF routers that need to exchange routing information.

1. Select **Network** > **Virtual Routers**, and select the default router or add a new router.
2. Select **OSPF** (for IPv4) or **OSPFv3** (for IPv6) and select **Enable**.
3. In this example, the OSPF configuration for VPN Peer A is:
   - **Router ID**: 192.168.100.141
   - **Area ID**: 0.0.0.0 that is assigned to the tunnel.1 interface with Link type: p2p
   - **Area ID**: 0.0.0.10 that is assigned to the interface Ethernet1/1 and Link Type: Broadcast

   The OSPF configuration for VPN Peer B is:
   - **Router ID**: 192.168.100.140
   - **Area ID**: 0.0.0.0 that is assigned to the tunnel.1 interface with Link type: p2p
   - **Area ID**: 0.0.0.20 that is assigned to the interface Ethernet1/15 and Link Type: Broadcast

STEP 5 | Set up the IKE Gateway.

This example uses static IP addresses for both VPN peers. Typically, the corporate office uses a statically configured IP address, and the branch side can be a dynamic IP address; dynamic IP addresses aren't best suited for configuring stable services such as VPN.

1. Select **Network** > **Network Profiles** > **IKE Gateway**.
2. Click **Add** and configure the options in the **General** tab.

   In this example, the configuration for VPN Peer A is:
   - **Interface**—ethernet1/7
   - **Local IP address**—100.1.1.1/24
   - **Peer IP address**—200.1.1.1/24
   - **Preshared keys**—enter a value

   The configuration for VPN Peer B is:
   - **Interface**—ethernet1/11
   - **Local IP address**—200.1.1.1/24
   - **Peer IP address**—100.1.1.1/24
   - **Preshared keys**—enter same value as on Peer A
3. Select the IKE Crypto profile that you created earlier to use for IKE phase 1.

STEP 6 | Set up the IPSec Tunnel.

1. Select **Network** > **IPSec Tunnels**.
2. Click **Add** and configure the options in the **General** tab.

   In this example, the configuration for VPN Peer A is:

   - **Tunnel Interface**—tunnel.41
   - **Type**—Auto Key
   - **IKE Gateway**—Select the IKE Gateway defined above.
   - **IPSec Crypto Profile**—Select the IKE Gateway defined above.

   The configuration for VPN Peer B is:

   - **Tunnel Interface**—tunnel.40
   - **Type**—Auto Key
   - **IKE Gateway**—Select the IKE Gateway defined above.
   - **IPSec Crypto Profile**—Select the IKE Gateway defined above.
3. Select **Show Advanced Options**, select **Tunnel Monitor**, and specify a Destination IP address to ping for verifying connectivity.
4. To define the action on failure to establish connectivity, see Define a Tunnel Monitoring Profile.

STEP 7 | Create policy rules to allow traffic between the sites (subnets).

1. Select **Policies** > **Security**.
2. Create rules to allow traffic between the untrust and the vpn-tun zone and the vpn-tun and the untrust zone for traffic originating from specified source and destination IP addresses.

STEP 8 | Verify OSPF adjacencies and routes from the CLI.

Verify that both the firewalls can see each other as neighbors with full status. Also confirm that the IP address of the VPN peer's tunnel interface and the OSPF Router ID. Use the following CLI commands on each VPN peer.

- **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:multicase, 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:multicase, 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
    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 | Troubleshoot Your IPSec VPN Tunnel Connection.

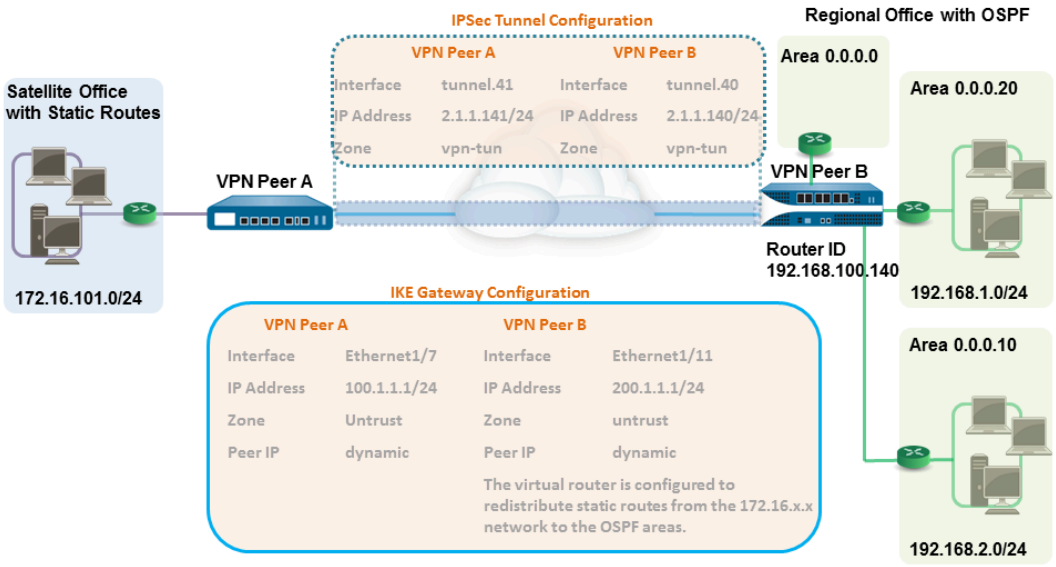
See Set Up Tunnel Monitoring and View the Status of the Tunnels.

Site-to-Site VPN with Static and Dynamic Routing

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

In this example, one site uses static routes and the other site uses OSPF. When the routing protocol isn't the same between the locations, the tunnel interface on each firewall must be configured with a static IP address. Then, to allow the exchange of routing information, the firewall that participates in both the static and dynamic routing process must be configured with a Redistribution profile. Configuring the redistribution profile enables the virtual router to redistribute and filter routes between protocols—static routes, connected routes, and hosts—from the static autonomous system to the OSPF autonomous system. Without this redistribution profile, each protocol functions on its own and doesn't exchange any route information with other protocols running on the same virtual router.

In this example, the satellite office has static routes and all traffic destined to the 192.168.x.x network is routed to tunnel.41. The virtual router on VPN Peer B participates in both the static and the dynamic routing process and is configured with a redistribution profile in order to propagate (export) the static routes to the OSPF autonomous system.



STEP 1 | Configure the Layer 3 interfaces on each firewall.

1. Select **Network** > **Interfaces** > **Ethernet** and then select the interface you want to configure for VPN.
2. Select **Layer3** from the **Interface Type**.
3. On the **Config** tab, select the **Security Zone** to which the interface belongs:
   - The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.
   - If you haven't yet created the zone, select **New Zone** from the **Security Zone**, define a **Name** for the new zone, and then click **OK**.
4. Select the **Virtual Router** to use.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.210.26/24.
6. To save the interface configuration, click **OK**.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—ethernet1/7
   - **Security Zone**—untrust
   - **Virtual Router**—default
   - **IPv4**—100.1.1.1/24

   The configuration for VPN Peer B is:

   - **Interface**—ethernet1/11
   - **Security Zone**—untrust
   - **Virtual Router**—default
   - **IPv4**—200.1.1.1/24

STEP 2 | Set up the crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2).

Complete this task on both peers and make sure to set identical values.

1. Select **Network** > **Network Profiles** > **IKE Crypto**. In this example, we use the default profile.
2. Select **Network** > **Network Profiles** > **IPSec Crypto**. In this example, we use the default profile.

STEP 3 | Set up the IKE Gateway.

With pre-shared keys, to add authentication scrutiny when setting up the IKE phase-1 tunnel, you can set up Local and Peer Identification attributes and a corresponding value that is matched in the IKE negotiation process.

1. Select **Network** > **Network Profiles** > **IKE Gateway**.
2. Click **Add** and configure the options in the **General** tab.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—ethernet1/7
   - **Local IP address**—100.1.1.1/24
   - **Peer IP type**—dynamic
   - **Preshared keys**—enter a value
   - **Local identification**—select **FQDN(hostname)** and enter the value for VPN Peer A.
   - **Peer identification**—select **FQDN(hostname)** and enter the value for VPN Peer B

   The configuration for VPN Peer B is:

   - **Interface**—ethernet1/11
   - **Local IP address**—200.1.1.1/24
   - **Peer IP address**—dynamic
   - **Preshared keys**—enter same value as on Peer A
   - **Local identification**—select **FQDN(hostname)** and enter the value for VPN Peer B
   - **Peer identification**—select **FQDN(hostname)** and enter the value for VPN Peer A
3. Select the IKE Crypto profile that you created earlier to use for IKE phase 1.

STEP 4 | Create a tunnel interface and attach it to a virtual router and security zone.

1. Select **Network** > **Interfaces** > **Tunnel** and click **Add**.
2. In the **Interface Name** field, specify a numeric suffix, say, **.41**.
3. On the **Config** tab, expand the **Security Zone** to define the zone as follows:
   - To use your trust zone as the termination point for the tunnel, select the zone.
   - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for the new zone (for example *vpn-tun*), and then click **OK**.
4. Select the **Virtual Router**.
5. Assign an IP address to the tunnel interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask/prefix to assign to the interface, for example, 172.19.9.2/24.

   This IP address will be used to route traffic to the tunnel and to monitor the status of the tunnel.
6. To save the interface configuration, click **OK**.

   In this example, the configuration for VPN Peer A is:

   - **Interface**—tunnel.41
   - **Security Zone**—vpn_tun
   - **Virtual Router**—default
   - **IPv4**—2.1.1.141/24

   The configuration for VPN Peer B is:

   - **Interface**—tunnel.42
   - **Security Zone**—vpn_tun
   - **Virtual Router**—default
   - **IPv4**—2.1.1.140/24

STEP 5 | Specify the interface to route traffic to a destination on the 192.168.x.x network.

1. On VPN Peer A, select the virtual router.
2. Select **Static Routes**, and **Add** tunnel.41 as the **Interface** for routing traffic with a **Destination** in the 192.168.x.x network.

STEP 6 | Set up the static route and the OSPF configuration on the virtual router and attach the OSPF areas with the appropriate interfaces on the firewall.

1. On VPN Peer B, select **Network** > **Virtual Routers**, and select the default router or add a new router.
2. Select **Static Routes** and **Add** the tunnel IP address as the next hop for traffic in the 172.168.x.x. network.

   Assign the desired route metric; using a lower the value makes higher priority for route selection in the forwarding table.
3. Select **OSPF** (for IPv4) or **OSPFv3** (for IPv6) and select **Enable**.
4. In this example, the OSPF configuration for VPN Peer B is:
   - Router ID: 192.168.100.140
   - Area ID: 0.0.0.0 is assigned to the interface Ethernet 1/12 Link type: Broadcast
   - Area ID: 0.0.0.10 that is assigned to the interface Ethernet1/1 and Link Type: Broadcast
   - Area ID: 0.0.0.20 is assigned to the interface Ethernet1/15 and Link Type: Broadcast

STEP 7 | Create a redistribution profile to inject the static routes into the OSPF autonomous system.

1. Create a redistribution profile on VPN Peer B.
   1. Select **Network** > **Virtual Routers**, and select the router you used above.
   2. Select **Redistribution Profiles**, and click **Add**.
   3. Enter a Name for the profile and select **Redist** and assign a **Priority** value. If you have configured multiple profiles, the profile with the lowest priority value is matched first.
   4. Set **Source Type** as **static**, and click **OK**. The static route you defined in step 6 will be used for the redistribution.
2. Inject the static routes into the OSPF system.
   1. Select **OSPF** > **Export Rules** (for IPv4) or **OSPFv3** > **Export Rules** (for IPv6).
   2. Click **Add**, and select the redistribution profile that you created.
   3. Select how the external routes are brought into the OSPF system. The default option, **Ext2** calculates the total cost of the route using only the external metrics. To use both internal and external OSPF metrics, use **Ext1**.
   4. Assign a **Metric** (cost value) for the routes injected into the OSPF system. This option allows you to change the metric for the injected route as it comes into the OSPF system.
   5. Click **OK**.

STEP 8 | Set up the IPSec Tunnel.

1. Select **Network** > **IPSec Tunnels**.
2. Click **Add** and configure the options in the **General** tab.

   In this example, the configuration for VPN Peer A is:

   - **Tunnel Interface**—tunnel.41
   - **Type**—Auto Key
   - **IKE Gateway**—Select the IKE Gateway defined above.
   - **IPSec Crypto Profile**—Select the IKE Gateway defined above.

   The configuration for VPN Peer B is:

   - **Tunnel Interface**—tunnel.40
   - **Type**—Auto Key
   - **IKE Gateway**—Select the IKE Gateway defined above.
   - **IPSec Crypto Profile**—Select the IKE Gateway defined above.
3. Select **Show Advanced Options**, select **Tunnel Monitor**, and specify a Destination IP address to ping for verifying connectivity.
4. To define the action on failure to establish connectivity, see Define a Tunnel Monitoring Profile.

STEP 9 | Create policy rules to allow traffic between the sites (subnets).

1. Select **Policies** > **Security**.
2. Create rules to allow traffic between the untrust and the vpn-tun zone and the vpn-tun and the untrust zone for traffic originating from specified source and destination IP addresses.

STEP 10 | Verify OSPF adjacencies and routes from the CLI.

Verify that both the firewalls can see each other as neighbors with full status. Also confirm that the IP address of the VPN peer's tunnel interface and the OSPF Router ID. Use the following CLI commands on each VPN peer.

- **`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:multicase, 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:multicase, 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`**

The following is an example of the output on each VPN peer.

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             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            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | Troubleshoot Your IPSec VPN Tunnel Connection.

See Set Up Tunnel Monitoring and View the Status of the Tunnels.

Troubleshooting

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

This chapter shares tasks for testing the VPN connectivity and interpreting VPN error messages if encountered. Use the CLI commands to monitor and troubleshoot site-to-site VPN connections.

Troubleshoot Your IPSec VPN Tunnel Connection

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

Test and troubleshoot your IPSec VPN connection for its maximum performance. Before testing the VPN connectivity familiarize yourself with the common VPN error messages.

The following table lists some of the common VPN error messages that are logged in the system log.

Table 2: Syslog Error Messages for VPN Issues

If an error is this:	Try this:

`IKE phase-1 negotiation is failed as initiator, main mode. Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`
or
`IKE phase 1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]`
	• Verify that the public IP address for each VPN peer is accurate in the IKE Gateway configuration.
	• Verify that the IP addresses can be pinged and that routing issues aren't causing the connection failure.

`Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...`
or
`IKE phase-1 negotiation is failed. Unable to process peer's SA payload.`
	Check the IKE Crypto profile configuration to verify that the proposals on both sides have a common encryption, authentication, and DH Group proposal.

`pfs group mismatched:my: 2peer: 0`
or
`IKE phase-2 negotiation failed when processing SA payload. No suitable proposal found in peer's SA payload.`
	Check the IPSec Crypto profile configuration to verify that:
	• PFS is either enabled or disabled on both VPN peers
	• the DH Groups proposed by each peer has at least one DH Group in common

`IKE phase-2 negotiation failed when processing Proxy ID. Received local id`	The VPN peer on one end is using a policy-based VPN. You must

If an error is this:	Try this:
`x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.`	configure a proxy ID on the Palo Alto Networks firewall. See Create a Proxy ID to identify the VPN peers.
`Commit error: Tunnel interface tunnel.x multiple binding limitation (xx) reached.`	You must have reached the maximum proxy IDs supported on your firewall. Check the maximum proxy IDs supported on your firewall before establishing an IPSec tunnel. We recommend you to check the maximum proxy IDs supported on your firewall before configuring proxy IDs for the VPN peers. If you have a use case where you want to implement an IPSec VPN tunnel with more than the maximum proxy IDs supported on a firewall, follow these steps: • Configure another tunnel with the same phase 1 and phase 2 configuration. • SuperNet the IP address for the proxy IDs. For example, instead of using 10.1.0.0/16, 10.2.0.0/16, supernet the range to 10.0.0.0/8 for avoiding multiple entries.
`Proxy ID mismatch`	Proxy ID mismatch will result in failure to establish the site-to-site IPSec VPN tunnel. Therefore, configure identical Proxy IDs on both VPN peers to establish the site-to-site IPSec VPN tunnel successfully. For example: In a site-to-site IPSec tunnel configuration, if one VPN peer is configured with an IP address for a netmask of /32 and the remote VPN peer is configured with the same IP address but with the different netmask of /16, it will result in failure establishing the VPN tunnel.

If an error is this:	Try this:
	Proxy ID for other firewall vendors are referred to as the Access List or Access Control List (ACL). Proxy IDs in the VPN peers should be exact mirrors of each other (that is, be opposite), but not match. Example proxy ID configuration for VPN peers to establish an IPSec VPN tunnel: If VPN firewall 1 is configured with 192.0.2.0/24 as local ID and 192.0.2.25/24 as peer ID. Then, VPN firewall 2 must be configured with 192.0.2.25/24 as local ID and 192.0.2.0/24 as peer ID.

Test VPN Connectivity

Perform this task to test VPN connectivity.

STEP 1 | Initiate IKE phase 1 by either pinging a host across the tunnel or using the following CLI command:

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

STEP 2 | Enter the following command to test if IKE phase 1 is set up:

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

In the output, check whether the security association displays. If it doesn't, review the system log messages to interpret the reason for failure.

STEP 3 | Initiate IKE phase 2 by either pinging a host from across the tunnel or using the following CLI command:

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


STEP 4 | Enter the following command to test if IKE phase 2 is set up:

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

In the output, check whether the security association displays. If it doesn't, review the system log messages to interpret the reason for failure.

STEP 5 | To view the VPN traffic flow information, use the following command:

```
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
```


Troubleshoot Site-to-Site VPN Issues Using CLI

Where Can I Use This?	What Do I Need?
• PAN-OS	No license required

Use the following CLI commands to troubleshoot phase 1 and phase 2 site-to-site VPN issues:

- Show Commands
- Clear Commands
- Test Commands
- Debug Commands

Show Commands

If you want to . . .	Use . . .
• Display the basic statistics of all VPN tunnels	`> show running tunnel flow info`
• Display the IKE SA for a given gateway	`> show vpn ike-sa gateway <gateway> | match <x.x.x.x/Y>`
• Display the IKE SA for a given tunnel	`> show vpn ike-sa tunnel <tunnel>`
• Display IPSec counters	`> show vpn flow`
• Display the list of all IPSec gateways and their configurations	`> show vpn gateway`
• Display IKE phase 1 SAs	`> show vpn ike-sa`
• Display IKE phase 2 SAs	`> show vpn ipsec-sa`
• Display the list of auto-key IPSec tunnel configurations	`>  show vpn tunnel`

Clear Commands

If you want to . . .	Use . . .
• Delete the IKEv1 IKE SA for a given gateway	`> clear vpn ike-sa gateway <gateway>`
• Delete the IKEv1 IKE SA for a given tunnel	`> clear vpn ike-sa tunnel <tunnel>`
• Delete the IKEv1 IPSec SA for a given tunnel	`> clear vpn ipsec-sa tunnel <tunnel>`

Test Commands

If you want to . . .	Use . . .
• Initiate an IKE negotiation with the designated gateway	`> test vpn ike-sa gateway <gateway>`
• Initiate an IPSec negotiation for the designated tunnel	`> test vpn ipsec-sa tunnel <tunnel>`

Debug Commands

If you want to . . .	Use . . .
• Turn on debugging to view detailed logging and status	`> debug ike global on debug less mp-log ikemgr.log debug ike stat`
• Packet capture to view and to capture main, aggressive, and quick mode negotiations.	`> debug ike pcap on view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap`
• Turn off debugging	`> debug ike pcap off`

