SITE-TO-SITE VPNS

EDU-210 Version A
PAN-OS® 9.0

EXTEND PREVENTION TO REMOTE SITES

- Site-to-site VPN
- Configuring site-to-site tunnels
- IPsec troubleshooting

Agenda

After you complete this module, you should be able to:

- Describe the three basic requirements for creating a VPN
- Configure the interface, IP addresses, and PSK for the IKE Gateway
- Configure the DH group, encryption methods, and authentication methods for an IKE Cryptographic Profile
- Configure a static route in the route table for the tunnel
- Troubleshoot your IPsec VPN issues from the responder side of the VPN tunnel

After you complete this module, you should be able to:

- Describe the three basic requirements for creating a VPN
- Configure the interface, IP addresses, and PSK for the IKE Gateway
- Configure the DH group, encryption methods, and authentication methods for an IKE Cryptographic Profile
- Configure a static route in the route table for the tunnel
- Troubleshoot your IPsec VPN issues from the responder side of the VPN tunnel

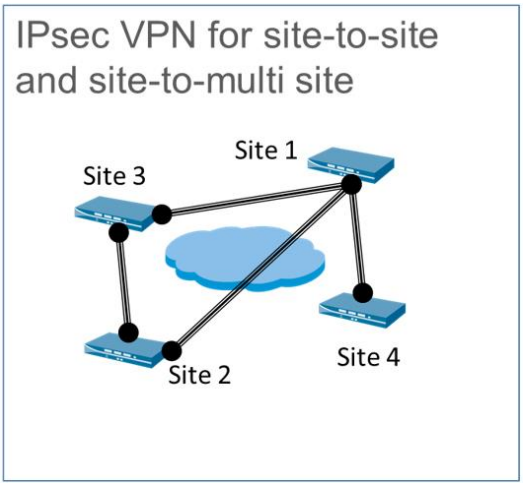
Site-to-site VPN

Configuring site-to-site tunnels

IPsec troubleshooting

Site-to-Site Overview

- PAN-OS® software implements route-based IPsec VPNs.
- The tunnel is represented by a logical tunnel interface.
- The tunnel interface is placed within a zone.
- The routing table chooses the tunnel settings.
- Multiple versions of Internet Key Exchange (IKE) are supported:
  - IKEv1
  - IKEv2



PAN-OS software implements IPsec VPNs as route-based tunnels, as opposed to policy-based designs. In a route-based VPN, the determining factor of which traffic will be tunneled is the final destination of that traffic. Route-based VPNs are easy to deploy and scale readily to large environments because they take advantage of dynamic routing protocols.

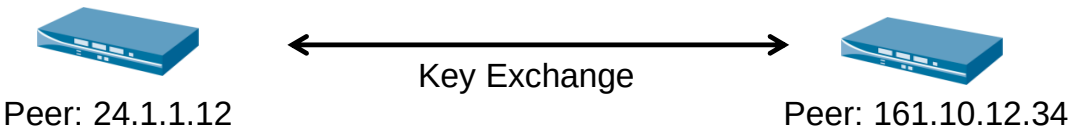
The firewall also can interoperate with third-party, policy-based VPN devices:

- A system that receives traffic destined for a remote private network looks up the next hop in the routing table, which is the standard procedure for traffic from another network.
- In the case of a remote network, the routing table points to a logical tunnel interface.
- The tunnel interface is not a real physical interface, but has all of the required information for the creation of an IPsec tunnel.
- After traffic is sent to the tunnel interface, the VPN is created and the traffic is forwarded through it.

IKEv1 is the more commonly used version. IKEv2 primarily is used to meet the requirements of the Network Device Protection Profile, or NDPP, Certification, Microsoft Azure compliance, and/or Suite B support. “IKEv2 preferred mode” provides the ability to fall back to IKEv1 after five retries (about 30 seconds).

IKE Phase 1

- IKE Phase 1 identifies the endpoints of the VPN.
- IKE Phase 1 uses peer IDs to identify the devices:
  - For devices with known addresses, the peer ID usually is the IP address.
  - A peer ID also can be a domain name or other string.
- Three settings (modes): Aggressive, Main, Auto



The creation of the IPsec tunnel has two phases. In the first phase, the IKE protocol authenticates the firewalls to each other and sets up a secure control channel. It uses the IKE-Crypto Profile for IKE negotiation.

With IKE Phase 1, each device is identified to the other by a peer ID. In most cases, this ID is just the public IP address of the device. In situations where the public ID is not static, this value can be replaced with a domain name or other text value.

IKE Phase 1 provides authentication of the endpoints of the tunnel and creates a secure channel for the next phase of the VPN.

Five pieces of information are passed during IKE Phase 1:

- Authentication method
- Diffie-Hellman key exchange
- Symmetric Key Algorithm – Bulk Data Encryption
- Hashing algorithm
- Lifetime

IKE Phase 2

- Each side of the tunnel has a proxy ID to identify traffic:
  - Support for multiple proxy IDs
- Networks are identified by proxy ID and can be either:
  - Masked network (e.g., 10.2.0.0/24)
  - Any network (0.0.0.0/0)

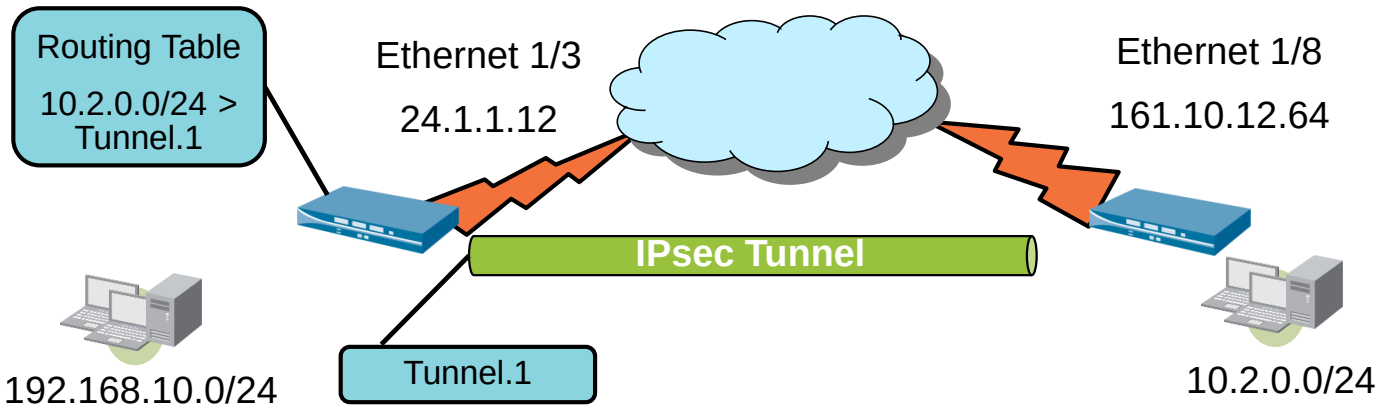
IKE Phase 2 creates the tunnel that will encapsulate data traffic. IKE Phase 1 was concerned with authenticating the endpoints, but IKE Phase 2 is concerned with data traffic that crosses the tunnel. Each side of the tunnel will have a proxy ID to identify the traffic it will be sending and what it expects to receive. These IDs either can be a specific network range or a generic network of 0.0.0.0/0. In either case, both sides need to know what the other side will be sending for the tunnel to work.

Five pieces of information are passed during IKE Phase 2:

- IPsec type/mode
- Diffie-Hellman: PFS
- Symmetric Key Algorithm – Bulk Data Encryption
- Hashing algorithm
- Lifetime (before rekey)

Note: You may be familiar with the idea of proxy ID under a different name: encryption domain. They are effectively the same thing.

Route-Based Site-to-Site VPN



This diagram shows how the traffic will traverse an established site-to-site tunnel.

Before you can set up VPNs, you must understand your network topology and be able to determine the required number of tunnels. For example:

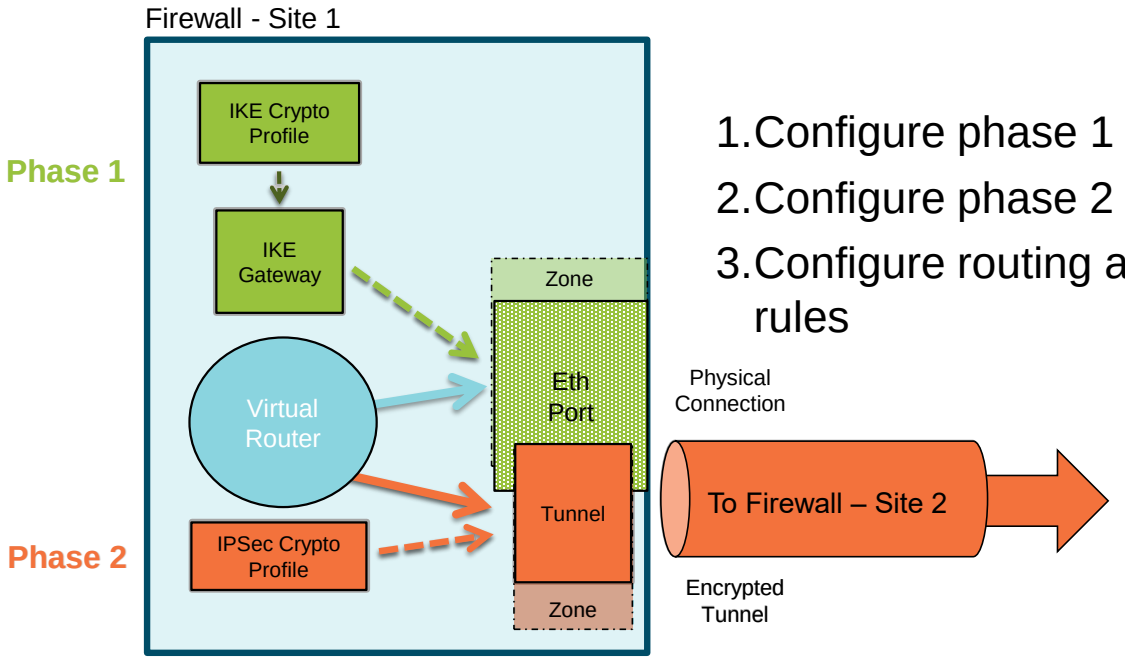
- A single VPN tunnel may be sufficient for connecting between a single central site and a remote site.
- Connections between a central site and multiple remote sites require VPN tunnels for each central-remote site pair.

Each tunnel is bound to a tunnel interface. When moving VPN traffic across the tunnel interface to the same virtual router as the incoming (cleartext) traffic. In this way, when a packet comes to the firewall, the route lookup function can determine the appropriate tunnel to use.

The tunnel interface appears to the system as a normal interface, and the existing routing infrastructure can be applied.

Each tunnel interface can have a maximum of 10 IPsec tunnels, which allows for the creation of IPsec tunnels for individual networks that are all associated with the same tunnel interface on the firewall.

VPN Tunnel Component Interaction



The diagram shows the various components that must be created to successfully configure an IPsec VPN tunnel. The arrows indicate the dependencies among some components.

The three basic requirements for creating a VPN in PAN-OS software are as follows:

1. Create the tunnel interface or Phase 1 objects:
   - Interface configuration can be performed in the web interface by selecting **Network** > **Interfaces** > **Tunnel**.
   - The new logical interface must be added to a Layer 3 zone and to a virtual router, just as any other logical Layer 3 interface would be handled.
2. Configure the IPsec tunnel or Phase 2 objects:
   - You can use the basic interface when you create a tunnel between PAN-OS devices with known IP addresses.
   - The only values needed are the tunnel interface to use, the local peer ID, the remote peer ID, and the pre-shared key, or PSK.
   - If the configuration is site-to-site with another Palo Alto Networks firewall, use the default Crypto Profiles.
   - If the configuration is site-to-site with a different vendor's firewall, configure the advanced settings in the Crypto Profiles to match.
3. Add a static route to the virtual router or enable an applicable routing protocol such as BGP, OSPF, or RIP:
   - Add a route table entry for the remote network that points to the tunnel interface used in Steps 1 and 2.
   - Create a route for the remote network using the tunnel interface.
   - No next-hop IP address is required when tunnel interfaces are used.
   - Be sure to create a security rule to allow tunneled traffic.

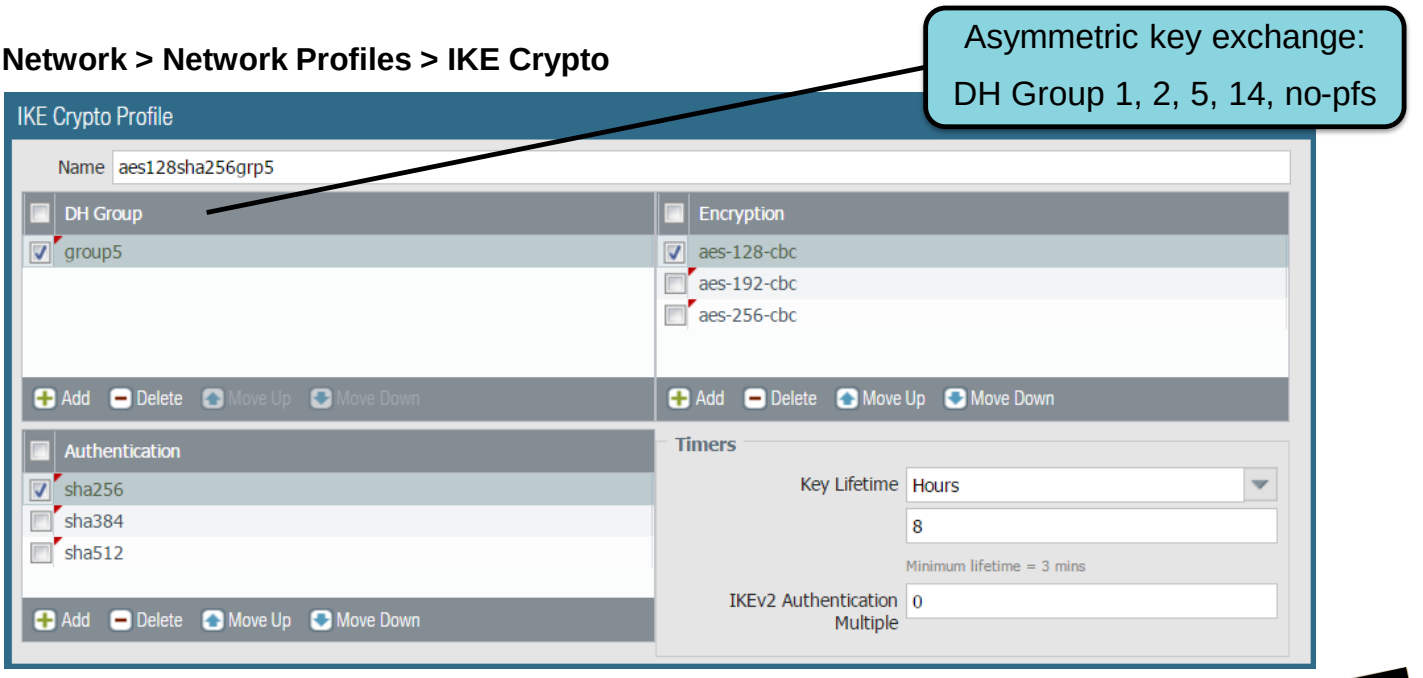
Site-to-site VPN

Configuring site-to-site tunnels

IPsec troubleshooting

Phase 1 Object: IKE Cryptographic Profiles

Network > Network Profiles > IKE Crypto



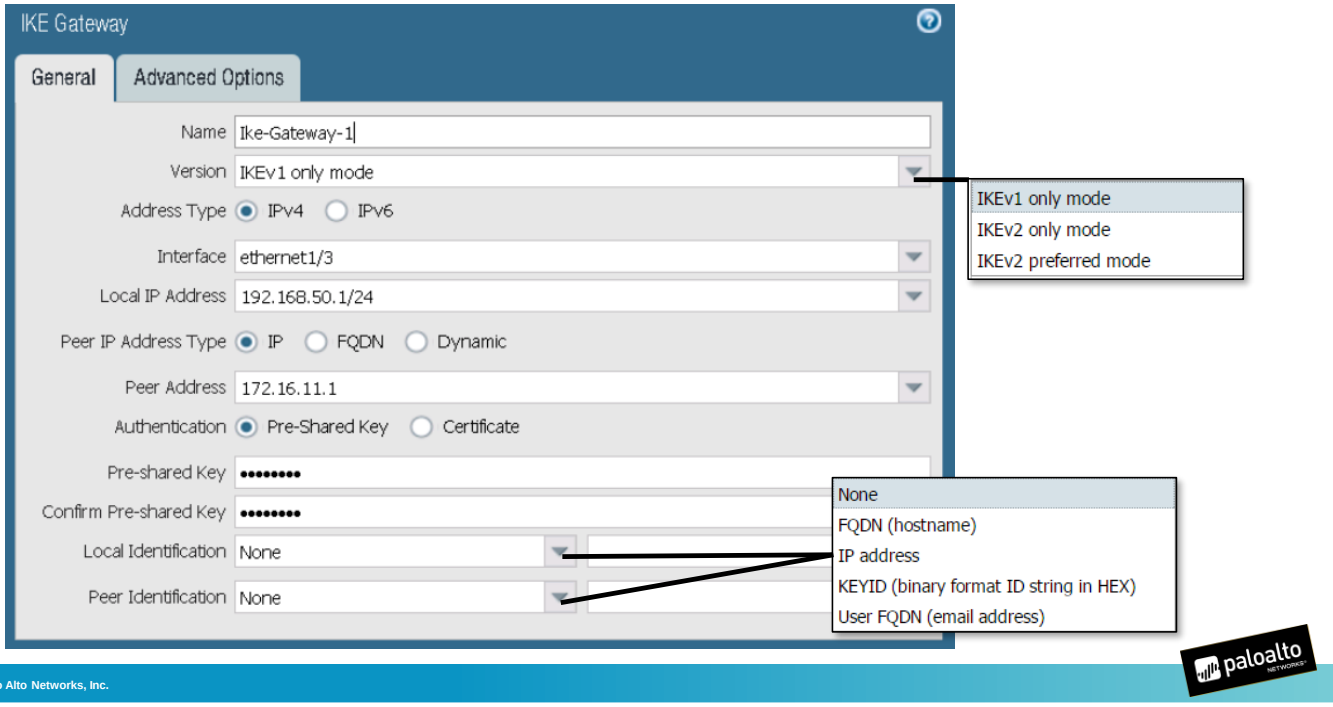
In IKE Phase 1, several possible cryptographic options can be chosen:

- Both sides of the tunnel must be able to agree on the same settings for all Phase 1 options for the Phase 1 security association, or SA, to be successful.
- For the **DH Group**, **Encryption**, and **Authentication** settings, multiple options can be selected for each.
- The panels show only the option selected by the administrator, even if more are available.
- Click **Add** to specify which methods will be attempted.
- To change the ordering in which an algorithm or group is listed, select the item and click the arrow icons in the panel. The listed order determines the order in which the algorithms are applied, and can affect tunnel performance.

Supported hashes are md5, sh1, sha256, sha384, and sha512.

Phase 1 Object: IKE Gateway – General Tab

Network > Network Profiles > IKE Gateways



When you configure your IKE Gateway for simple deployments (e.g., tunnels between Palo Alto Networks devices), specify only the interface, IP addresses, and PSK.

Note: If the firewall interface used is configured with a dynamic IP address (e.g., in the case of a PPPoE DSL connection), the **Local IP Address** field must be set to **none**.

IKE certificate-based authentication often is required in VPN replacements where partner sites require certificate-authentication. The next-generation firewall can use IKE PKI certificate authentication for IP site-to-site VPNs.

Supported ID types are as follows:

- FQDN (hostname)
- IP address
- KeyID: ID string in HEX (binary format)
- Email address (User FQDN)

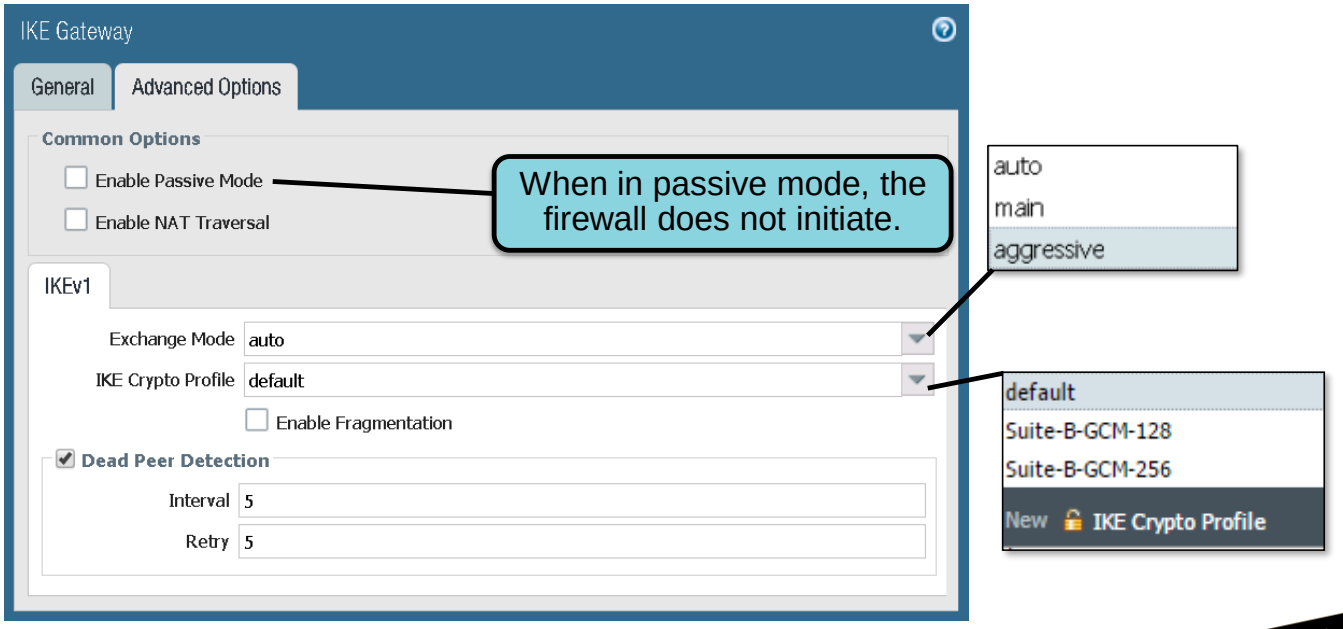
If no value is specified, the local IP address will be used as the **Local Identification** value.

IKE PKI feature limitations are as follows:

- The maximum level for the certificate chain is 5 (number of CA certificates, including trusted CA). If the level is exceeded, the error “certificate chain too long” is returned and the certificate chain build fails.
- CRL over LDAP is not supported.
- All IKE gateways configured on the same interface or local IP address must use the same Crypto Profile, and the peer ID must be different.

Phase 1 Object: IKE Gateway – Advanced Options

Network > Network Profiles > IKE Gateways > Advanced Options

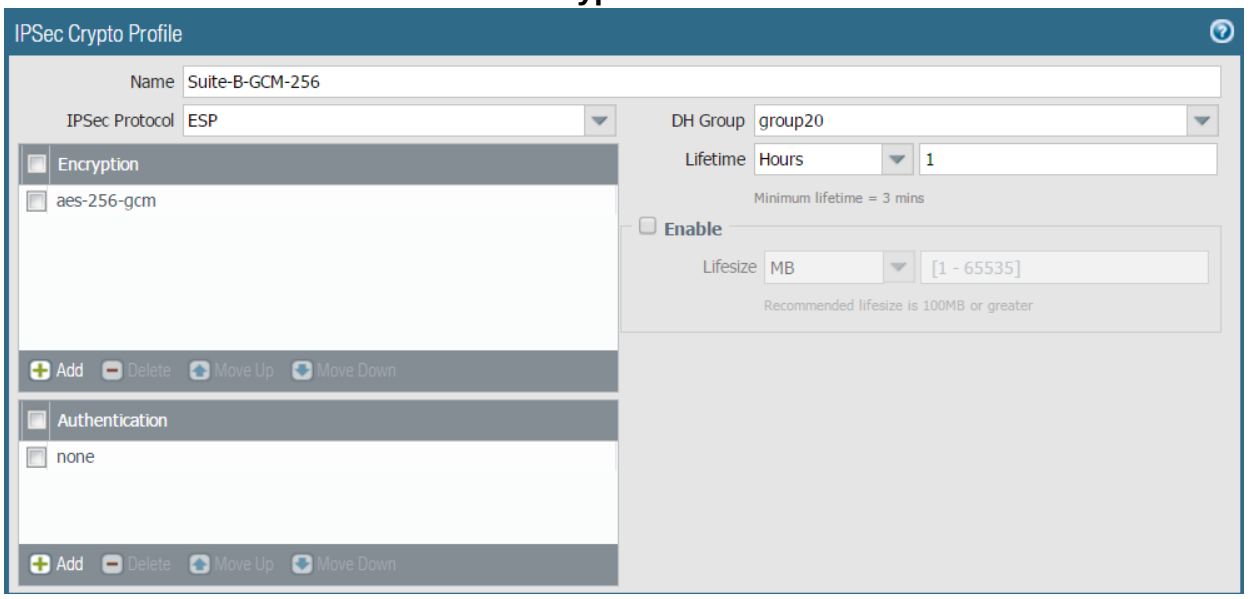


The administrator can use the **Advanced Options** tab to set all aspects of the IKEv1 Phase 1 connection:

- **Enable Passive Mode**: Select to have the firewall respond only to IKE connections and to never initiate them.
- **Enable NAT Traversal**: Select to have UDP encapsulation used on IKE and UDP protocols, which enables them to pass through intermediate NAT devices. Choose this option if NAT is configured on a device between the IPsec VPN terminating points.
- **Exchange Mode**: Select **auto**, **aggressive**, or **main**. In auto mode (default), the device can accept main mode and aggressive mode negotiation requests. However, whenever possible, it initiates negotiation and allows exchanges in main mode. You must configure the peer device with the same exchange mode to allow it to accept negotiation requests initiated from the first device.
- **IKE Crypto Profile**: Custom Crypto Profiles can be configured under the **IKE Crypto Profile** setting.
- **Enable Fragmentation**: Check to allow the local gateway to receive fragmented IKE packets. This option is available only if you have selected **main** as your **Exchange Mode**. The maximum fragmented packet size is 576 bytes.
- **Dead Peer Detection**: Select to enable and enter an interval (2 to 100 seconds) and delay before retrying the remote peer if the previous attempt failed (2 to 100 seconds). Dead peer detection, or DPD, identifies inactive or unavailable IKE peers and can help restore resources that are lost when a peer is unavailable. DPD needs to be supported by the remote firewall

Phase 2 Object: IPsec Cryptographic Profiles

Network > Network Profiles > IPSec Crypto

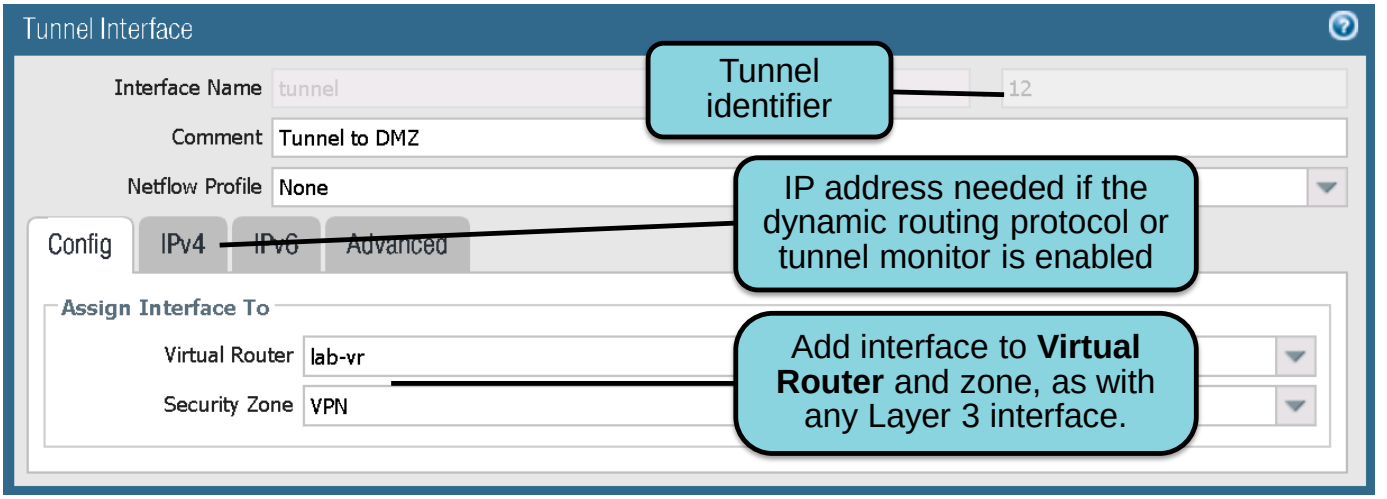


Use the **IPSec Crypto Profile** page to specify protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPsec negotiation:

- Multiple options can be selected for each of the **DH Group**, **Encryption**, and **Authentication** settings.
- The panels show only the option selected by the administrator, even if more are available.
- Click **Add** to specify which methods are attempted.
- To change the order in which an algorithm or group is listed, select the item and click the arrow icons in the panel.
- The listed order determines the order in which the algorithms are applied, and can affect tunnel performance.

VPN Tunnel Interface

Network > Interfaces > Tunnel Tab



A tunnel interface is a logical Layer 3 interface.

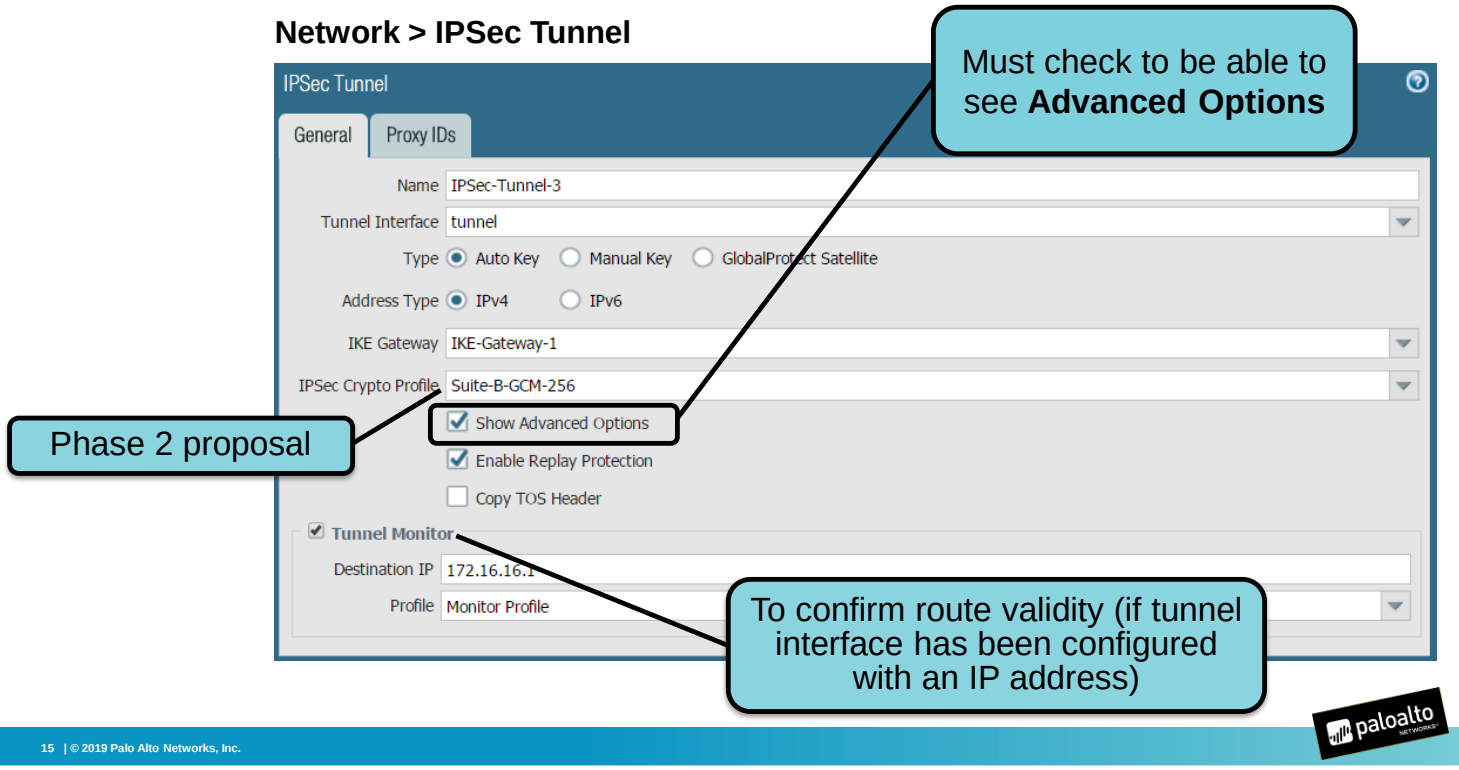
Each tunnel interface represents a specific VPN configuration. Any traffic that is routed to this interface is tunneled according to the configuration of the IPsec VPN object associated with the tunnel interface.

The tunnel interface must be added to a Layer 3 security zone and a virtual router. Unlike with other Layer 3 logical interfaces, the tunnel interface does not need an IP address.

An address is required if dynamic routing protocols will be used across the VPN or if tunnel monitoring is desired.

Note: The **Interface Name** "tunnel" cannot be renamed.

Phase 2 Object: IPsec Tunnel



IKE Phase 2 negotiations determine the type of IPsec used and the internal networks that will connect using the tunnel.

Tunnel monitoring can be enabled if the underlying tunnel interface has been configured with an IP address. This feature sends ping traffic through the tunnel to verify full connectivity.

The monitor generates an alert if the route goes down, and has the added benefit of keeping the tunnel up even when no network traffic is being sent down it.

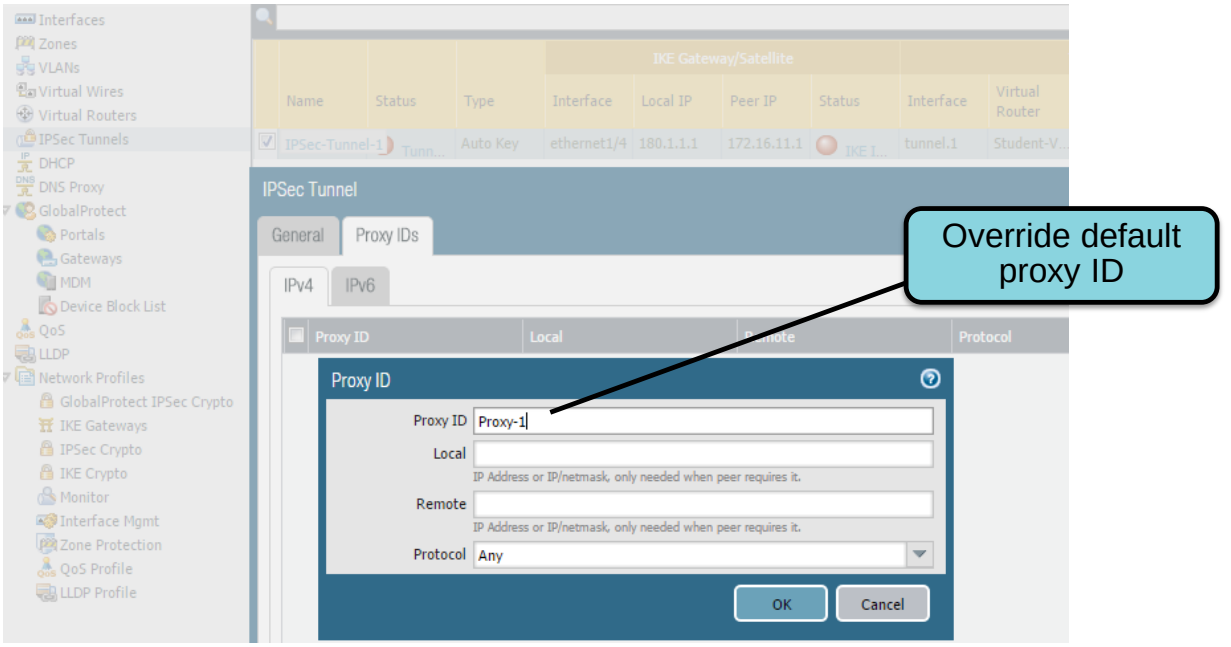
If tunnel monitoring is used, the Monitor Profile can define one of two actions:

- wait recover: If the remote IP is not reachable, the firewall continuously sends ping requests over the tunnel in an attempt to learn if the tunnel can recover and the destination IP becomes reachable. If the IP address is reachable, traffic routes across the tunnel again.
- fail-over: Traffic will fail over to a backup route path, if one is available. The firewall uses routing table lookup to determine routing for the duration of this session.

In both cases, the firewall tries to negotiate new IPsec keys to accelerate the recovery.

Phase 2 Object: IPsec Tunnel (Cont.)

Network > IPSec Tunnel > Proxy IDs

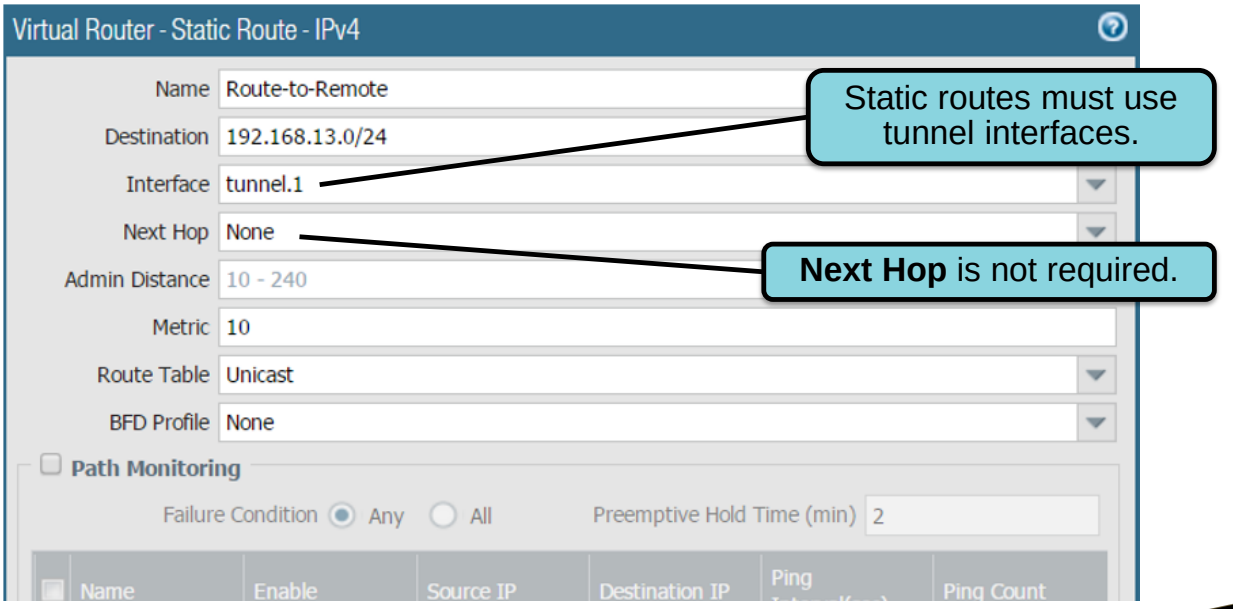


Palo Alto Networks implements route-based VPNs, so the default protected network IDs, or proxy IDs, are 0.0.0.0/0.

To aid in interoperability with third-party VPN solutions, the default proxy IDs may be replaced with one or more network strings.

Static Route for VPN

Network > Virtual Routers > Add > Static Routes > IPv4

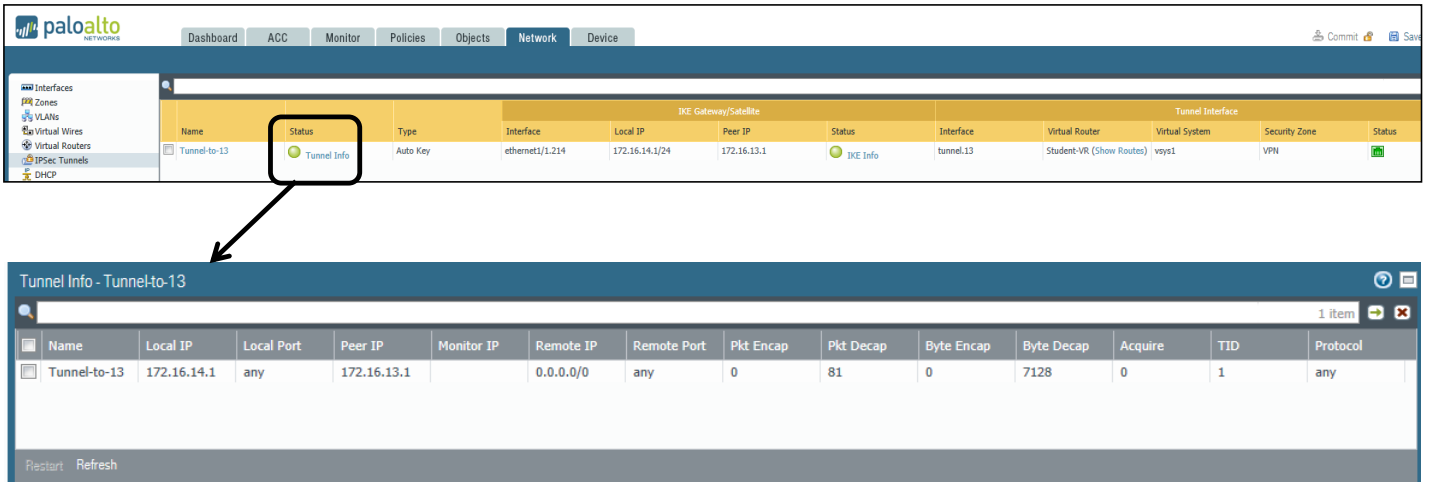


The last step is to add the route table entry for the tunnel:

- The entry is a static route for the remote private network.
- This route should point to the tunnel interface.
- No other configuration in the virtual router is required.
- This step is not required if dynamic routing is configured on the tunnel interface.

IPsec Tunnel Status: Check Connectivity

Network > IPSec Tunnels



Click **Tunnel Info** to display the details of the tunnel.

Site-to-site VPN

Configuring site-to-site tunnels

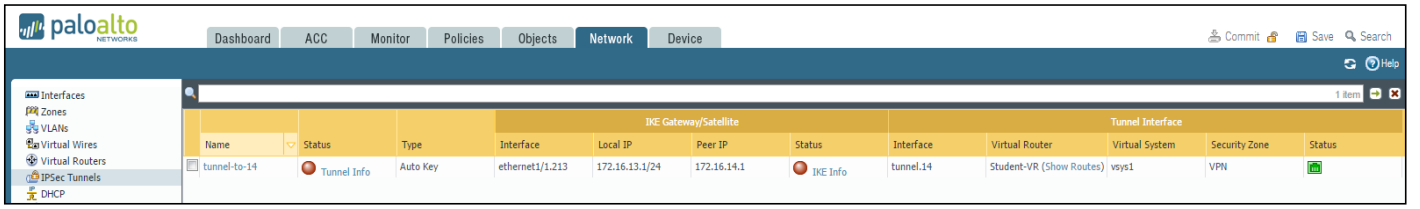
IPsec troubleshooting

IPsec Tunnel Status: Check Connectivity

Investigate the following links:

- Tunnel Info
- IKE Info
- Show Routes

Network > IPSec Tunnels



When you troubleshoot IPsec tunnels, begin by looking at the **IPSec Tunnel** page. Each tunnel entry will provide you with much useful troubleshooting information. Click the links to open up dialog boxes that contain status specific information.

To display the IPsec tunnel status on the firewall, go to **Network > IPSec Tunnels**:

- **Tunnel Status** (first status column): Green indicates an IPsec Phase 2 SA tunnel. Red indicates that IPsec Phase 2 SA is not available or has expired.
- **IKE Gateway Status**: Green indicates a valid IKE Phase 1 SA or IKEv2 IKE SA. Red indicates that IKE Phase 1 SA is not available or has expired.
- **Tunnel Interface Status**: Green indicates that the tunnel interface is up (because the tunnel monitor is disabled or because tunnel monitor status is UP and the monitoring IP address is reachable). Red indicates that the tunnel interface is down because the tunnel monitor is enabled and the remote tunnel monitoring IP address is unreachable.

Note: Tunnels will be established only when relevant traffic attempts to cross. You can use the **`test vpn`** command to initiate a tunnel manually.

VPN Error Messages

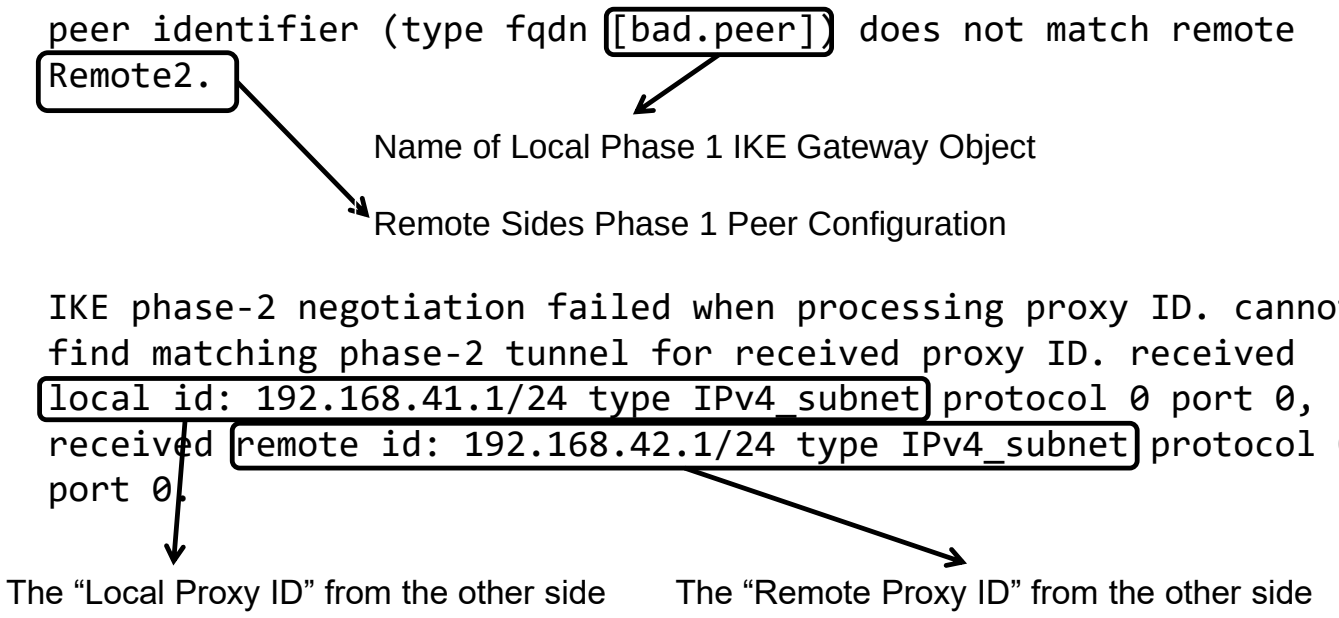
Issue	Initiator Error	Responder Error
Wrong IP/no connection	P1 - Timeout	P1 - Timeout
No matching P1 proposal	P1 - Timeout	No suitable proposal (P1)
Mismatched peer ID	P1 - Timeout	Peer identifier does not match
No matching P2 proposal	No proposal chosen	No suitable proposal (P2)
PFS group mismatch	P2 - Timeout	PFS group mismatch
Mismatched proxy ID	P2 - Timeout	Cannot find matching phase-2 tunnel

Remember always to troubleshoot IPsec VPN issues from the responder. The initiator does not receive detailed error messages. This behavior is by design and is not linked to any particular vendor's implementation.

The more common configuration issues include:

- Wrong IP: The remote gateway IP address is wrong or there is no IP connectivity between the two public interfaces. The Responder will show an error stating that it received a request for a tunnel that is not configured.
- No matching P1 or P2 proposal: The peers cannot find matches for the five parameters of the IKE Phase 1 or Phase 2 proposals.
- Mismatched peer ID: The value entered for peer IDs does not match.
- PFS group mismatch: Both sides have PFS enabled, but with different DH groups.
- Mismatched proxy ID: The values for local and remote proxy ID are not correct. This error most commonly happens during interoperation with policy-based VPNs.

Reading VPN Error Messages (System Log)



The error messages for peer and proxy ID mismatches contain the information sent by the initiating peer. This information can be compared to the local configuration to determine where the error is:

- Phase 1 gateways: The error message refers to the IKE gateway object and shows the peer ID sent by the initiator.
- Phase 2 proxy ID: The error message shows the local and remote proxy IDs sent by the initiator.

Module Summary

Now that you have completed this module, you should be able to:

- Describe the three basic requirements for creating a VPN
- Configure the interface, IP addresses, and PSK for the IKE Gateway
- Configure the DH group, encryption methods, and authentication methods for an IKE Cryptographic Profile
- Configure a static route in the route table for the tunnel
- Troubleshoot your IPsec VPN issues from the responder side of the VPN tunnel

Now that you have completed the module, you should be able to:

- Describe the three basic requirements for creating a VPN
- Configure the interface, IP addresses, and PSK for the IKE Gateway
- Configure the DH group, encryption methods, and authentication methods for an IKE Cryptographic Profile
- Configure a static route in the route table for the tunnel
- Troubleshoot your IPsec VPN issues from the responder side of the VPN tunnel

Questions?

Review Questions

1. Which three options are aspects of the basic requirements to create a VPN in a PAN-OS release? (Choose three.)
    a. add a static route to the virtual router
    b. create the tunnel interface
    c. configure the IPsec tunnel
    d. identify proxy ID errors
2. True or false? When you create a static route for the VPN, no next hop IP address is required.
    a. true
    b. false
3. Which two options are true regarding a VPN tunnel interface? (Choose two.)
    a. The tunnel interface always requires an IP address.
    b. A tunnel interface is a logical Layer 3 interface.
    c. The tunnel interface must be added to a Layer 3 security zone.
    d. The interface name “tunnel” can be renamed to anything you want, up to 20 characters in length.
4. True or false? IPsec is a set of protocols used to set up a secure tunnel for the VPN traffic.
    a. true
    b. false

Site-to-Site VPN Lab (Pages 223-232 in the Lab Guide)

- Create a Site-to-Site VPN Tunnel
- Assign the Tunnel to a VPN Zone
- Create a Security Policy Rule to Allow Traffic from the Partner's Trust Network
- Ping to Activate VPN

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, b, c
2. a (true)
3. b, c
4. a (true)