



## Administering Firepower Threat Defense VPNs

- [Managing Firepower Threat Defense Site-to-site VPNs, on page 1](#)
- [Configuring Firepower Threat Defense Site-to-site VPNs, on page 2](#)
- [Monitoring Firepower Threat Defense VPNs, on page 9](#)

## Managing Firepower Threat Defense Site-to-site VPNs

### Procedure

Select **Devices > VPN > Site To Site** to manage your Firepower Threat Defense Site-to-site VPN configurations and deployments. Choose from the following:

- Add—To create a new VPN topology, click **Add** (+) **Add VPN > Firepower Threat Defense Device**, and continue as instructed in [Configuring Firepower Threat Defense Site-to-site VPNs, on page 2](#):

**Note** VPNs topologies can be created only on leaf domains.

- Edit—To modify the settings of an existing VPN topology, click **Edit** (pencil icon). Modifying is similar to configuring, continue as instructed above.

**Note** You cannot edit the topology type after you initially save it. To change the topology type, delete the topology and create a new one.

Two users should **not** edit the same topology simultaneously; however, the web interface does not prevent simultaneous editing.

- Delete—To delete a VPN deployment, click **Delete** (trash icon).
- View VPN status—This status applies to Firepower VPNs ONLY. Currently, no status is displayed for Firepower Threat Defense VPNs. To determine the status of the Firepower Threat Defense VPNs, see .
- Deploy—Click **Deploy**; see [Deploy Configuration Changes](#).

**Note** Some VPN settings are validated only during deployment. Be sure to verify that your deployment was successful.

## Configuring Firepower Threat Defense Site-to-site VPNs

### Procedure

- 
- Step 1** Choose **Devices > VPN > Site To Site**. Then **Add VPN > Firepower Threat Defense Device**, or edit a listed VPN Topology. .
- Step 2** Enter a unique **Topology Name**. We recommend naming your topology to indicate that it is a Firepower Threat Defense VPN, and its topology type.
- Step 3** Choose the **Network Topology** for this VPN.
- Step 4** Choose the IKE versions to use during IKE negotiations. **IKEv1** or **IKEv2**.  
Default is IKEv2. Select either or both options as appropriate; select IKEv1 if any device in the topology does not support IKEv2. You can also configure backup peer for point-to-point extranet VPNs. For more information, see [Firepower Threat Defense VPN Endpoint Options, on page 3](#).
- Step 5** Required: Add Endpoints for this VPN deployment by clicking **Add** (+) for each node in the topology. Configure each endpoint field as described in [Firepower Threat Defense VPN Endpoint Options, on page 3](#).
- For Point to point, configure **Node A** and **Node B**.
  - For Hub and Spoke, configure a **Hub Node** and **Spoke Nodes**
  - For Full Mesh, configure multiple **Nodes**
- Step 6** (Optional) Specify non-default IKE options for this deployment as described in [Firepower Threat Defense VPN IKE Options, on page 4](#)
- Step 7** (Optional) Specify non-default IPsec options for this deployment as described in [Firepower Threat Defense VPN IPsec Options, on page 5](#)
- Step 8** (Optional) Specify non-default Advanced options for this deployment as described in [Firepower Threat Defense Advanced VPN Deployment Options, on page 7](#).
- Step 9** Click **Save**.  
The endpoints are added to your configuration.
- 

### What to do next

Deploy configuration changes; see [Deploy Configuration Changes](#).



**Note** Some VPN settings are validated only during deployment. Be sure to verify that your deployment was successful.

## Firepower Threat Defense VPN Endpoint Options

### Navigation Path

**Devices > VPN > Site To Site.** Then **Add VPN > Firepower Threat Defense Device**, or edit a listed VPN Topology. Open the **Endpoint** tab.

### Fields

#### Device

Choose an endpoint node for your deployment:

- A Firepower Threat Defense device managed by this Firepower Management Center.
- A Firepower Threat Defense high availability container managed by this Firepower Management Center.
- An **Extranet** device, any device (Cisco or third-party) not managed by this Firepower Management Center.

#### Device Name

For Extranet devices only, provide a name for this device. We recommend naming it such that it is identifiable as an un-managed device.

#### Interface

If you chose a managed device as your endpoint, choose an interface on that managed device.

#### IP Address

- If you choose an extranet device, a device **not** managed by the Firepower Management Center, specify an IP address for the endpoint.
- If you chose a managed device as an endpoint, choose a single IPv4 address or multiple IPv6 addresses from the drop-down list (these are the addresses already assigned to this interface on this managed device).
- All endpoints in a topology must have the same IP addressing scheme. IPv4 tunnels can carry IPv6 traffic and vice-versa. The Protected Networks define which addressing scheme the tunneled traffic will use.
- If the managed device is a high-availability container, choose from a list of interfaces.

#### This IP is Private

Check the check box if the endpoint resides behind a firewall with network address translation (NAT).



**Note** Use this option only when the peer is managed by the same Firepower Management Center and do not use this option if peer is from extranet.

### Public IP address

If you checked the **This IP is Private** check box, specify a public IP address for the firewall. If the endpoint is a responder, specify this value.

### Connection Type

Specify the allowed negotiation as bidirectional, answer-only, or originate-only. Supported combinations for the connection type are:

*Table 1: Connection Type Supported Combinations*

| Remote Node    | Central Node   |
|----------------|----------------|
| Originate-Only | Answer-Only    |
| Bi-Directional | Answer-Only    |
| Bi-Directional | Bi-Directional |

### Protected Networks

Defines a list of networks protected by this VPN endpoint. Click **Add** (+) to select from available Network Objects or add Network Objects inline. See [Creating Network Objects](#). Access Control Lists will be generated from the choices made here.

- **Subnet/IP Address (Network)**—VPN endpoints cannot have the same IP address and protected networks in a VPN endpoint pair cannot overlap. If a list of protected networks for an endpoint contains one or more IPv4 or IPv6 entries, the other endpoint's protected network must have at least one entry of the same type (that is, IPv4 or IPv6). If it does not, then the other endpoint's IP address must be of the same type and must not overlap with the entries in the protected network. (Use /32 CIDR address blocks for IPv4 and /128 CIDR address blocks for IPv6.) If both of these checks fail, the endpoint pair is invalid.



**Note** **Reverse Route Injection is enabled** by default in Firepower Management Center.

.

## Firepower Threat Defense VPN IKE Options

For the versions of IKE you have chosen for this topology, specify the **IKEv1/IKEv2 Settings**.



**Note** Settings in this dialog apply to the entire topology, all tunnels, and all managed devices.

### Navigation Path

**Devices > VPN > Site To Site.** Then **Add VPN > Firepower Threat Defense Device**, or edit a listed VPN Topology. Open the **IKE** tab.

### Fields

#### Policy

Choose a predefined IKEv1 or IKEv2 policy object or create a new one to use. For details, see [Firepower Threat Defense IKE Policies](#)

#### Key Type

- **Manual**—Manually assign the pre-shared key that is used for this VPN. Specify the **Key** and then re-enter to **Confirm Key**.
- **Automatic**—The Management Center automatically defines the pre-shared key that is used for this VPN. Specify the **Key Length**, the number of characters in the key, 1-27.

## Firepower Threat Defense VPN IPsec Options



**Note** Settings in this dialog apply to the entire topology, all tunnels, and all managed devices.

### Crypto-Map Type

A crypto map combines all the components required to set up IPsec security associations (SA). When two peers try to establish an SA, they must each have at least one compatible crypto map entry. The proposals defined in the crypto map entry are used in the IPsec security negotiation to protect the data flows specified by that crypto map's IPsec rules. Choose static or dynamic for this deployment's crypto-map:

- **Static**—Use a static crypto map in a point-to-point or full mesh VPN topology.
- **Dynamic**—Dynamic crypto-maps essentially create a crypto map entry without all the parameters configured. The missing parameters are later dynamically configured (as the result of an IPsec negotiation) to match a remote peer's requirements.

Dynamic crypto map policies apply only in a hub-and-spoke VPN configuration. In a point-to-point or full mesh VPN topology, you can apply only static crypto map policies. Emulate the use of dynamic crypto-maps in a point-to-point topology by creating a hub-and-spoke topology with two devices. Specify a dynamic IP address for the spoke, and enable dynamic crypto map on this topology.

### IKEv2 Mode

For IPsec IKEv2 only, specify the encapsulation mode for applying ESP encryption and authentication to the tunnel. This determines what part of the original IP packet has ESP applied.

- **Tunnel mode**—(default) Encapsulation mode is set to tunnel mode. Tunnel mode applies ESP encryption and authentication to the entire original IP packet (IP header and data), hiding the ultimate source and destination addresses and becoming the payload in a new IP packet.

The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPsec. This mode allows a network device, such as a router, to act as an IPsec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets


and forwards them along the IPsec tunnel. The destination router decrypts the original IP datagram and forwards it onto the destination system. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

- **Transport preferred**— Encapsulation mode is set to transport mode with an option to fallback to tunnel mode if the peer does not support it. In Transport mode only the IP payload is encrypted, and the original IP headers are left intact. Therefore, the admin must select a protected network that matches the VPN interface IP address.

This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. With transport mode, you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header is encrypted, which limits examination of the packet.

- **Transport required**— Encapsulation mode is set to transport mode only, falling back to tunnel mode is not allowed. If the endpoints cannot successfully negotiate transport mode, due to one endpoint not supporting it, the VPN connection is not made.

## Proposals

Click **Edit** () to specify the proposals for your chosen IKEv1 or IKEv2 method. Select from the available **IKEv1 IPsec Proposals** or **IKEv2 IPsec Proposals** objects, or create and then select a new one. See [Configure IKEv1 IPsec Proposal Objects](#) and [Configure IKEv2 IPsec Proposal Objects](#) for details.

## Enable Security Association (SA) Strength Enforcement

Enabling this option ensures that the encryption algorithm used by the child IPsec SA is not stronger (in terms of the number of bits in the key) than the parent IKE SA.

## Enable Reverse Route Injection

Reverse Route Injection (RRI) enables static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint.

## Enable Perfect Forward Secrecy

Whether to use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. If you select this option, also select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key in the Modulus Group list.

## Modulus Group

The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For a full explanation of the options, see [Deciding Which Diffie-Hellman Modulus Group to Use](#).

## Lifetime (seconds)

The number of seconds a security association exists before expiring. The default is 28,800 seconds.

## Lifetime (kbytes)

The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires. The default is 4,608,000 kilobytes. Infinite data is not allowed.

## ESPv3 Settings

### Validate incoming ICMP error messages

Choose whether to validate ICMP error messages received through an IPsec tunnel and destined for an interior host on the private network.

### Enable 'Do Not Fragment' Policy

Define how the IPsec subsystem handles large packets that have the do-not-fragment (DF) bit set in the IP header.

#### Policy

- Copy DF bit—Maintains the DF bit.
- Clear DF bit—Ignores the DF bit.
- Set DF bit—Sets and uses the DF bit.

### Enable Traffic Flow Confidentiality (TFC) Packets

Enable dummy TFC packets that mask the traffic profile which traverses the tunnel. Use the **Burst**, **Payload Size**, and **Timeout** parameters to generate random length packets at random intervals across the specified SA.

## Firepower Threat Defense Advanced VPN Deployment Options

The following list describes the advanced options you can specify in your deployment.



**Note** Settings in this dialog apply to the entire topology, all tunnels, and all managed devices.

### Advanced > IKE > ISAKMP Settings

#### IKE Keepalive

Enable or disables IKE Keepalives. Or set to EnableInfinite specifying that the device never starts keepalive monitoring itself.

#### Threshold

Specifies the IKE keep alive confidence interval. This is the number of seconds allowing a peer to idle before beginning keepalive monitoring. The minimum and default is 10 seconds; the maximum is 3600 seconds.

#### Retry Interval

Specifies number of seconds to wait between IKE keep alive retries. The default is 2 seconds, the maximum is 10 seconds.

#### Identity Sent to Peers:

Choose the Identity that the peers will use to identify themselves during IKE negotiations:

- autoOrDN(default)—Determines IKE negotiation by connection type: IP address for preshared key, or Cert DN for certificate authentication (not supported).
- ipAddress—Uses the IP addresses of the hosts exchanging ISAKMP identity information.
- hostname—Uses the fully qualified domain name of the hosts exchanging ISAKMP identity information. This name comprises the hostname and the domain name.

**Enable Aggressive Mode**

Available only in a hub-and-spoke VPN topology. Select this negotiation method for exchanging key information if the IP address is not known and DNS resolution might not be available on the devices. Negotiation is based on hostname and domain name.

**Advanced > IKE > IKEv2 Security Association (SA) Settings**

More session controls are available for IKE v2 that limit the number of open SAs. By default, there is no limit to the number of open SAs:

**Cookie Challenge**

Whether to send cookie challenges to peer devices in response to SA initiate packets, which can help thwart denial of service (DoS) attacks. The default is to use cookie challenges when 50% of the available SAs are in negotiation. Select one of these options:

- Custom:
- Never (default)
- Always

**Threshold to Challenge Incoming Cookies**

The percentage of the total allowed SAs that are in-negotiation. This triggers cookie challenges for any future SA negotiations. The range is zero to 100%.

**Number of SAs Allowed in Negotiation**

Limits the maximum number of SAs that can be in negotiation at any time. If used with Cookie Challenge, configure the cookie challenge threshold lower than this limit for an effective cross-check.

**Maximum number of SAs Allowed**

Limits the number of allowed IKEv2 connections. Default is unlimited.

**Enable Notification on Tunnel Disconnect**

Allows an administrator to enable or disable the sending of an IKE notification to the peer when an inbound packet that is received on an SA does not match the traffic selectors for that SA. Sending this notification is disabled by default.

**Do not allow device reboot until all sessions are terminated**

Check to enable waiting for all active sessions to voluntarily terminate before the system reboots. This is disabled by default.

**Advanced > IPsec > IPsec Settings****Enable Fragmentation Before Encryption**

This option lets traffic travel across NAT devices that do not support IP fragmentation. It does not impede the operation of NAT devices that do support IP fragmentation.

**Path Maximum Transmission Unit Aging**

Check to enable PMTU (Path Maximum Transmission Unit) Aging, the interval to Reset PMTU of an SA (Security Association)

**Value Reset Interval**

Enter the number of minutes at which the PMTU value of an SA (Security Association) is reset to its original value. Valid range is 10 to 30 minutes, default is unlimited.

**Advanced > Tunnel > Tunnel Options****Enable Spoke to Spoke Connectivity through Hub****Advanced > Tunnel > NAT Settings****Keepalive Messages Traversal**

Select whether to enable NAT keepalive message traversal. NAT traversal keepalive is used for the transmission of keepalive messages when there is a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow. If you select this option, configure the interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The value can be from 5 to 3600 seconds. The default is 20 seconds.

**Interval**

Sets the NAT keepalive interval, from 5 to 3600 seconds. The default is 20 seconds.

## Monitoring Firepower Threat Defense VPNs

Monitor Firepower Threat Defense VPN activity in the following ways:

- System Messages

The Message Center is the place to start your monitoring. This feature allows you to view messages that are continually generated about system activities and status. To open the Message Center, click in the **System Status** icon, located to the immediate right of the **Deploy** button in the main menu. See [System Messages](#) for details on using the Message Center.

- VPN Health Events

These events are displayed along with other system events under **System > Health > Events > VPN Status**. See [Health Monitoring](#) for details on viewing system health events.

- System Logs

Currently the Firepower Management Center does not have the capability to read the Firepower Threat Defense VPN syslogs. These syslogs need to be forwarded to a third-party server for analysis and archiving. See [About Configuring Syslog](#) for details on configuring syslog servers and viewing the system logs.

- Unified CLI Commands, see *Command Reference for Firepower Threat Defense*

Use the show, clear, and debug commands on the Firepower Threat Defense device to monitor and troubleshoot VPN activity.

**Monitoring Guidelines**

- If more than 300 Firepower Threat Defense devices are configured in the Firepower Management Center, event handling issues may arise.
- Event loss between the Firepower Threat Defense device and the Firepower Management Center is possible if the connection is broken.

