Site-to-Site VPNs for Firepower Threat Defense

About Firepower Threat Defense Site-to-site VPNs

Firepower Threat Defense site-to-site VPN supports the following features:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Certificates and automatic or manual preshared keys for authentication.
- IPv4 & IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 Site-to-Site VPN topologies provide configuration settings to comply with Security Certifications.
- Static and Dynamic Interfaces.
- Support for both Firepower Management Center and Firepower Threat Defense HA environments.
- VPN alerts when the tunnel goes down.
- Tunnel statistics available using the Firepower Threat Defense Unified CLI.
- Support for IKEv1 and IKEv2 back-up peer configuration for point-to-point extranet and hub-and-spoke VPNs.
- Support for extranet device as hub in 'Hub and Spokes' deployments.
- Support for dynamic IP address for a managed endpoint pairing with extranet device in 'Point to Point' deployments.

- Support for dynamic IP address for extranet device as an endpoint.
- Support for hub as extranet in 'Hub and Spokes' deployments.

VPN Topology

To create a new site-to-site VPN topology you must, at minimum, give it a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both. Also, determine your authentication method. Once configured, you deploy the topology to Firepower Threat Defense devices. The Firepower Management Center configures site-to-site VPNs on Firepower Threat Defense devices only.

You can select from three types of topologies, containing one or more VPN tunnels:

- Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.
- Hub and Spoke deployments establish a group of VPN tunnels connecting a hub endpoint to a group of spoke nodes.
- Full Mesh deployments establish a group of VPN tunnels among a set of endpoints.

IPsec and IKE

In the Firepower Management Center, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

Authentication

For authentication of VPN connections, configure a preshared key in the topology, or a trustpoint on each device. Preshared keys allow for a secret key, used during the IKE authentication phase, to be shared between two peers. A trustpoint includes the identity of the CA, CA-specific parameters, and an association with a single enrolled identity certificate.

Extranet Devices

Each topology type can include Extranet devices, devices that you do not manage in Firepower Management Center. These include:

- Cisco devices that Firepower Management Center supports, but for which your organization is not responsible. Such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.
- Non-Cisco devices. You cannot use Firepower Management Center to create and deploy configurations to non-Cisco devices.

Add non-Cisco devices, or Cisco devices not managed by the Firepower Management Center, to a VPN topology as "Extranet" devices. Also specify the IP address of each remote device.

Firepower Threat Defense Site-to-site VPN Guidelines and Limitations

- A VPN connection can only be made across domains by using an extranet peer for the endpoint not in the current domain.

- A VPN topology cannot be moved between domains.
- Network objects with a 'range' option are not supported in VPN
- Firepower Threat Defense VPNs are only be backed up using the Firepower Management backup.
- The Firepower Threat Defense VPNs do not currently support PDF export and policy comparison.
- There is no per-tunnel or per-device edit option for Firepower Threat Defense VPNs, only the whole topology can be edited.
- Device interface address verification will not be performed for Transport mode when Crypto ACL is selected.
- All nodes in a topology must be configured with either Crypto ACL or Protected Network. A topology may not be configured with Crypto ACL on one node and Protected Network on another.
- There is no support for automatic mirror ACE generation. Mirror ACE generation for the peer is a manual process on either side.
- While using Crypto ACL, there is no support for tunnel health events for VPN topologies. With Crypto ACL, there is no support for Hub, Spoke, and Full Mesh topologies; only point to point VPN is supported.
- Whenever IKE ports 500/4500 are in use or when there are some PAT translations that are active, the Site-to-Site VPN cannot be configured on the same ports as it fails to start the service on those ports.
- Tunnel status is not updated in realtime, but at an interval of 5 minutes in the Firepower Management Center.
- The character " (double quote) is not supported as part of pre-shared keys. If you have used " in a pre-shared key, ensure that you change the character after you upgrade to Firepower Threat Defense 6.30.

Requirements and Prerequisites for Site-to-Site VPN

Model Support

FTD

Supported Domains

Leaf

User Roles

Admin

Managing Firepower Threat Defense Site-to-site VPNs

Procedure

Step 1 For certificate authentication for your VPNs, you must prepare the devices by allocating trustpoints as described in Firepower Threat Defense Certificate-Based Authentication.

Step 2 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 4:

  Note VPNs topologies can be created only on leaf domains.

- Edit—To modify the settings of an existing VPN topology, click **Edit** ( ). 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** ( ).
- 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 VPN Monitoring for Firepower Threat Defense.
- Deploy—Choose **Deploy** > **Deployment**; 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 Click **Policy Based (Crypto Map)** to configre a site-to-site VPN.

Step 4 Choose the **Network Topology** for this VPN.

Step 5 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 5.

Step 6 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 5.

- 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 7 (Optional) Specify non-default IKE options for this deployment as described in Firepower Threat Defense VPN IKE Options, on page 8

Step 8 (Optional) Specify non-default IPsec options for this deployment as described in Firepower Threat Defense VPN IPsec Options, on page 10

Step 9 (Optional) Specify non-default Advanced options for this deployment as described in Firepower Threat Defense Advanced Site-to-site VPN Deployment Options, on page 12.

Step 10 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.

If you get an alert that your VPN tunnel is inactive even when the VPN session is up, follow the VPN troubleshooting instructions to verify and ensure that your VPN is active. For information, see VPN Monitoring for Firepower Threat Defense and VPN Troubleshooting for Firepower Threat Defense.

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.

For 'Point to Point' deployments, you can also configure an endpoint with dynamic interface. Note that an endpoint with dynamic interface can pair only with an extranet device and cannot pair with an endpoint, which has a managed device.

You can configure device interfaces at **Devices** > **Device Management** > **Add/Edit device** > **Interfaces**.

IP Address

- If you choose an extranet device, a device **not** managed by the Firepower Management Center, specify an IP address for the endpoint.

  For an extranet device, select **Static** and specify an IP address or select **Dynamic** to allow dynamic extranet devices.

  If you have chosen point-to-point topology and only IKEv1, you can configure backup peer by entering the primary IP address and backup peer IP addresses separated by a comma.
- 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

Certificate Map

Choose a pre-configured certificate map object, or click **Add** (+) to add a certificate map object that defines what information is necessary in the received client certificate for it to be valid for VPN connectivity. See Firepower Threat Defense Certificate Map Objects for details.

Protected Networks

Caution In the Hub and Spoke topology, for a dynamic crypto map, ensure that you do not select the protected network *any* for both the endpoints to avoid traffic drop.

Defines the networks that are protected by this VPN Endpoint. The networks may be marked by selecting the list of Subnet/IP Address that define the networks that are protected by this endpoint. Click **Add** (+) to select from available Network Objects or add new Network Objects. 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.

Subnet/IP Address (Network) remains the default selection.

When you have selected Protected Networks as *Any* and observe default route traffic being dropped, disable the Reverse Route Injection under **VPN**> **Site to Site** > edit a VPN > **IPsec** > **Enable Reverse Route Injection**. Deploy the configuration changes; this will remove set reverse-route (Reverse Route Injection) from the crypto map configuration and remove the VPN-advertised reverse route that causes the reverse tunnel traffic to be dropped.

- **Access List (Extended)**—An extended access lists provide the capability to control the type of traffic that will be accepted by this endpoint, like GRE or OSPF traffic. Traffic may be restricted either by address or port. Click **Add** (+) to add access control list objects.

Note Access Control List is supported only in the point to point topology.

Advanced Settings

Enable Dynamic Reverse Route Injection— Reverse Route Injection (RRI) is the ability for routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. Dynamic RRI routes are created only upon the successful establishment of IPsec security associations (SA's)

Note

- Dynamic RRI is supported only on IKEv2, and not supported on IKEv1 or IKEv1 + IKEv2.
- Dynamic RRI is not supported on: originate-only peer, Full Mesh topology, and Extranet peer.
- In Point-to-Point, only one peer can have dynamic RRI enabled.
- Between Hub and Spoke, only one of the endpoints can have dynamic RRI enabled.
- Dynamic RRI cannot be combined with a dynamic crypto map.

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

Authentication Type

Site-to-site VPN supports two authentication methods, pre-shared key and certificate. For an explanation of the two methods, see Deciding Which Authentication Method to Use.

Note In a VPN topology that supports IKEv1, the **Authentication Method** specified in the chosen IKEv1 Policy object becomes the default in the IKEv1 **Authentication Type** setting. These values must match, otherwise, your configuration will error.

- **Pre-shared Automatic Key**—The Management Center automatically defines the pre-shared key that is used for this VPN. Specify the **Pre-shared Key Length**, the number of characters in the key, 1-27.

  The character " (double quote) is not supported as part of pre-shared keys. If you have used " in a pre-shared key, ensure that you change the character after you upgrade to Firepower Threat Defense 6.30 or higher.

- **Pre-shared Manual Key**—Manually assign the pre-shared key that is used for this VPN. Specify the **Key** and then re-enter it in **Confirm Key** to confirm.

  When this option is chosen for IKEv2, the **Enforce hex-based pre-shared key only** check box appears, check if desired. If enforced, you must enter a valid hex value for the key, an even number of 2-256 characters, using numerals 0-9, or A-F.

- **Certificate**—When you use certificates as the authentication method for VPN connections, peers obtain digital certificates from a CA server in your PKI infrastructure, and trade them to authenticate each other.

  In the **Certificate** field, select a pre-configured certificate enrollment object. This enrollment object is used to generate a trustpoint with the same name on the managed device. The certificate enrollment object should be associated with and installed on the device, post which the enrollment process is complete, and then a trustpoint is created.

  A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

  Before you select this option, note the following:

  - Ensure you have enrolled a certificate enrollment object on all the endpoints in the topology—A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. Certificate Enrollment Objects are used to enroll your managed devices into your PKI infrastructure, and create trustpoints (CA objects) on devices that support VPN connections. For instructions on creating a certificate enrollment object, see Adding Certificate Enrollment Objects, and for instructions on enrolling the object on the endpoints see one of the following as applicable:
    - Installing a Certificate Using Self-Signed Enrollment
    - Installing a Certificate Using SCEP Enrollment
    - Installing a Certificate Using Manual Enrollment
    - Installing a Certificate Using a PKCS12 File

Note For a site-to-site VPN topology, ensure that the same certificate enrollment object is enrolled in all the endpoints in the topology. For further details, see the table below.

- Refer the following table to understand the enrollment requirement for different scenarios. Some of the scenarios require you to override the certificate enrollment object for specific devices. See Managing Object Overrides to understand how to override objects.

Certificate Enrollment Types	Device identity certificate for all endpoints is from the same CA		Device identity certificate for all endpoints is from different CAs
	Device-specific parameters are NOT specified in the certificate enrollment object	Device-specific parameters are specified in the certificate enrollment object	
Manual	No override required	Override required	Override required
SCEP	No override required	Override required	Override required
PKCS	Override required	Override required	Override required
Self-signed	Not applicable	Not applicable	Not applicable

- Understand the VPN certificate limitations mentioned in Firepower Threat Defense VPN Certificate Guidelines and Limitations.

Note If you use a Windows Certificate Authority (CA), the default Application Policies extension is **IP security IKE intermediate**. If you are using this default setting, you must select the **Ignore IPsec Key Usage** option in the Advanced Settings section on the **Key** tab in the PKI Certificate Enrollment dialog box for the object you select. Otherwise, the endpoints cannot complete the site-to-site VPN connection.

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 are applicable to both hub-and-spoke and point-to-point VPN topologies. To apply dynamic crypto map policies, specify a dynamic IP address for one of the peers in the topology and ensure that the dynamic crypto-map is enabled on this topology. Note that in a full mesh VPN topology, you can apply only static crypto map policies.

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

Lifetime Size
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 Site-to-site VPN Deployment Options

The following sections describes the advanced options you can specify in your S2S VPN deployment. These settings apply to the entire topology, all tunnels, and all managed devices.

Firepower Threat Defense VPN Advanced IKE Options

Advanced > IKE > ISAKAMP 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.

Note Enable or disable this option for all your VPN connections.

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 > IVEv2 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.

Firepower Threat Defense VPN Advanced IPsec Options

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.

Firepower Threat Defense Advanced Site-to-site VPN Tunnel Options

Navigation Path

Devices > VPN > Site To Site, then select **Add VPN > Firepower Threat Defense Device**, or edit a listed VPN Topology. Open the **Advanced** tab, and select **Tunnel** in the navigation pane.

Tunnel Options

Only available for Hub and Spoke, and Full Mesh topologies. This section will not display for Point to Point configurations.

- **Enable Spoke to Spoke Connectivity through Hub**—Disabled by default. Choosing this field enables the devices on each end of the spokes to extend their connection through the hub node to the other device.

NAT Settings

- **Keepalive Messages Traversal** —Elect 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.

Access Control for VPN Traffic

- **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** — Decrypted traffic is subjected to access control policy inspection by default. Enable this option to bypasses the ACL inspection; but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

  Enable or disable the option for all your VPN connections. If you disable this option, make sure that the traffic is allowed by the access control policy or pre-filter policy.

Certificate Map Settings

- **Use the certificate map configured in the Endpoints to determine the tunnel**—If this option is enabled (checked), the tunnel will be determined by matching the contents of the received certificate to the certificate map objects configured in the endpoint nodes.
- **Use the certificate OU field to determine the tunnel**—Indicates that if a node is not determined based on the configured mapping (the above option) if selected, then use the value of the organizational unit (OU) in the subject distinguished name (DN) of the received certificate to determine the tunnel.
- **Use the IKE identity to determine the tunnel**—Indicates that if a node is not determined based on a rule matching or taken from the OU (the above options) if selected, then the certificate-based IKE sessions are mapped to a tunnel based on the content of the phase1 IKE ID.
- **Use the peer IP address to determine the tunnel**—Indicates that if a tunnel is not determined based on a rule matching or taken from the OU or IKE ID methods (the above options) if selected, then use the established peer IP address.

About Virtual Tunnel Interfaces

Firepower Management Center supports a logical interface called Virtual Tunnel Interface (VTI). As an alternative to policy based VPN, a VPN tunnel can be created between peers with Virtual Tunnel Interfaces configured. This supports route-based VPN with IPsec profiles attached to the end of each tunnel. This allows dynamic or static routes to be used. Egressing traffic from the VTI is encrypted and sent to the peer, and the associated SA decrypts the ingress traffic to the VTI.

Using VTI does away with the requirement of configuring static crypto map access lists and mapping them to interfaces. You no longer have to track all remote subnets and include them in the crypto map access list. Deployments become easier, and having static VTI which supports route based VPN with dynamic routing protocol also satisfies many requirements of a virtual private cloud. FMC enables you to easily migrate from crypto-map based VPN configuration to VTI-based VPN.

You can configure route-based VPN in FMC, FTD Device REST API, and FDM by configuring a static Virtual Tunnel Interface. FMC supports a site-to-site VPN wizard with defaults to configure VTI or route-based VPN. Traffic is encrypted using static route or BGP.

You can create a routed security zone, add VTI interfaces to it, and define access control rules for the decrypted traffic control over the VTI tunnel.

VTI-based VPNs can be created between:

- Two FTD devices
- FTD and public cloud

- FTD and another FTD with service provider redundancy
- FTD and any other device with VTI interfaces configured
- FTD and another device with policy-based VPN configurations.

Guidelines and Limitations for Virtual Tunnel Interfaces

IPv6 Support

- IPv6 is not supported.

Limitations

- Only 20 unique IPSec profiles are supported.
- Only 100 VTIs are supported per physical interface.
- Dynamic VTI, OSPF, and QoS are not supported.
- Site-to-site VPN tunnels created with VTIs do not generate health alerts when the tunnel goes down. If you experience packet loss over a VPN with VTIs, check your VPN configuration.

General Configuration Guidelines

- VTIs are only configurable in IPsec mode.
- You can use dynamic or static routes for traffic using the tunnel interface.
- The MTU for VTIs is automatically set, according to the underlying physical interface.
- VTI supports IKE versions v1, v2, and uses IPsec for sending and receiving data between the tunnel's source and destination.
- If Network Address Translation has to be applied, the IKE and ESP packets will be encapsulated in the UDP header.
- IKE and IPsec security associations will be re-keyed continuously regardless of data traffic in the tunnel. This ensures that VTI tunnels are always up.
- Tunnel group name must match what the peer will send as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which are not IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.
- VTI and crypto map configurations can co-exist on the same physical interface, provided the peer address configured in the crypto map and the tunnel destination for the VTI are different.
- By default, all traffic sent through a VTI is encrypted.
- There are no security level configurations for VTI interfaces.
- Access list can be applied on a VTI interface to control traffic through VTI.

Multi-instance

VTI is supported in multi-instance.

Firewall Mode

VTI is supported in routed mode only.

Add a VTI Interface

For configuring a route-based site-to-site VPN, you must create a Virtual Tunnel Interface on the devices at both the nodes of the VTI tunnel. To create a new VTI interface, perform the following steps:

Procedure

Step 1 Choose **Devices** > **Device Management.**

Step 2 Click the **Edit** icon next to the device on which you want to create a VTI interface.

Step 3 From the **Add Interfaces** drop-down menu, choose **Virtual Tunnel Interface**.

Step 4 In the **Name** field, enter a name for the new VTI.

Step 5 Keep the **Enabled** checkbox checked (default) to enable the interface once you finish creating it.

Step 6 (Optional) Enter a description for the new VTI.

Step 7 (Optional) In the **Security Zone** drop-down menu, select a security zone to add the VTI interface to that zone. If you want to do traffic inspection based on security zone, you can add the VTI to the security zone and configure an access control rule. To permit the VPN traffic over the tunnel, you need to add an AC rule with this security zone as the source zone.

Step 8 In the **Tunnel ID** field, enter a unique tunnel ID in the range of 0-10413.

Step 9 In the **IP Address** field, enter the IP address and subnet to use for the tunnel endpoint. The VTI IP addresses of both endpoints of a route-based VPN must be in the same subnet.

Note Cisco recommends you to use IP from 169.254.x.x/16 range excluding the FTD reserved range (169.254.1.x/24). Also, use /30 as net-mask to optimally use only two addresses for two ends of the VTI tunnel. For example, 169.254.100.1/30.

Step 10 In the **Tunnel Source** drop-down menu, select the tunnel source interface.

Step 11 Click **OK**.

Create a Route-based Site-to-Site VPN

You can configure a route-based site-to-site VPN between two nodes. You need virtual tunnel interfaces at both the nodes of the tunnel in order to configure a VTI-based VPN.

For more information on VTI, see About Virtual Tunnel Interfaces, on page 15

Procedure

Step 1 Choose **Devices > Site To Site**.

Step 2 In the **Add VPN** drop-down menu, choose **Firepower Threat Defense Device**.

Step 3 In the Topology Name field, enter a name for the VPN topology that you are creating.

Step 4 Choose Route Based (VTI) as the topology type. Network topology is selected as Point to Point and IKE protocol version is selected as IKEv2 by default for the site-to-site configuration.

Step 5 Under **Node A** in the **Endpoints** tab, in the **Device** drop-down menu, select the name of the registered device (FTD) or Extranet to be used as the first endpoint of your VTI tunnel.

Step 6 For a registered device, you can specify the interface for Node A:

- In the **Virtual Tunnel Interface** drop-down menu, select the VTI interface, which you had created on FTD device that you have selected as Node A.
- If you want to create a new interface on Node A, click the + icon and fill the fields as described in Add a VTI Interface, on page 17.
- If you want to edit the configuration of an existing VTI, select the VTI in the **Virtual Tunnel Interface** drop-down field and click **Edit VTI**.

  Note The selected tunnel interface is the source interface for Node A and it becomes the tunnel destination for Node B.

Step 7 If your Node A device is behind a NAT device, check the **Tunnel Source IP is Private** checkbox . In the **Tunnel Source Public IP Address** field, enter the tunnel source public IP address.

Step 8 In the **Connection Type** drop-down menu, select **Answer Only** or **Birectional**. If you have selected IKE protocol version as IKEv1, one of the nodes must be **Answer Only**.

Step 9 Under **Additional Configuration**, do the following:

- To route traffic to the VTI, click **Routing Policy**. FMC displays the **Devices** > **Routing** page. You can configure the Static or BGP routing for the VPN traffic.
- To permit VPN traffic, click **AC Policy**. FMC displays the access control policy page of the device. Proceed to add allow/block rule specifying the security zone of the VTI. If a backup VTI is being configured, ensure to include the backup tunnel to the same security zone as that of the primary VTI. No specific settings is required for the backup VTI in the AC policy page.

Step 10 For an extranet peer, specify the following parameters:

a) In the **Device Name**, enter the name of the device.
b) In the **Endpoint IP address**, enter the primary IP address.
c) Click **IKE** tab and specify the pre-shared key provided on the extranet.

Note The AWS VPC has **AES-SHA-SHA-LATEST** as the default policy. Therefore, if the remote peer connects to AWS VPC, from the **Policy** drop-down list, select **AES-SHA-SHA-LATEST** to establish the VPN connection without the need to change the default value in AWS .

Step 11 Repeat the above procedure for Node B.

Additional Configurations for VTI

After you configure VTI interfaces and VTI tunnel on both the devices, you must configure a routing policy to route VTI traffic between the devices over the VTI tunnel. You must also configure an access control rule to allow encrypted traffic.

Routing Configuration for VTI

Static Route

Configure static routing on both the devices (both the ends) to route the traffic flow between the devices over the VTI tunnel.

If backup tunnel is configured for the VPN, configure a static route with a different metric to handle the failover of the traffic flow over the backup tunnel.

Ensure that you configure the following when you configure a static route:

- **Interface**—Select the VTI interface used in the VPN.
- **Selected Network**—Select the remote peer's protected network (added as a network object).
-

For more information about static routing, see Add a Static Route.

Border Gateway Protocol (BGP)

Configure BGP on both the devices to share routing information and to route traffic flow between the devices over the tunnel with the following settings:

- Under **General Settings** > **BGP**, enable BGP, provide the AS number of the local device, and add Router Id (if you choose Manual).
- Under **BGP**, enable IPv4 and configure neighbors on the Neighbor tab.
  - **IP Address**—Specify the remote peer's VTI interface IP address as the neighbor's IP address.
  - **Remote AS**—Specify the remote peer's AS number.

For more information about BGP configuration, see Configure BGP.

AC Policy Rule

Add an access control rule to the access control policy on the device to allow encrypted traffic between the VTI tunnels with the following settings:

- Create the rule with the Allow action.
- Select the VTI security zone of the local device as the Source Zone and the VTI security zone of the remote peer as the Destination Zone.
- Select the VTI security zone of the remote peer as the Source Zone and the VTI security zone of the local device as the Destination Zone.

For more information about configuring an access control rule, see Create and Edit Access Control Rules.

Note If backup VTI is configured, ensure to include the backup tunnel to the same security zone as that of the primary VTI. No specific settings are required for the backup VTI in the AC policy page.

History for Site-to-Site VPNs