

Site-to-Site VPN

- Site-to-site VPN, on page 1
- Types of site-to-site VPN topologies, on page 4
- License requirements for site-to-site VPN, on page 4
- Prerequisites for site-to-site VPN, on page 4
- Manage site-to-site VPNs, on page 5
- Configure a policy-based site-to-site VPN, on page 6
- Configure virtual tunnel interfaces, on page 19
- Monitor site-to-site topologies, on page 32
- History for site-to-site VPN, on page 36

Site-to-site VPN

A site-to-site VPN is a secure, encrypted VPN tunnel between two networks in different geographic locations. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. You can create site-to-site IPsec connections between managed devices, and between managed devices and other Cisco or third-party peers.

Site-to-site VPN features

Secure Firewall Threat Defense site-to-site VPN supports these features:

- IPsec IKEv1 & IKEv2 protocols.
- Certificates and automatic or manual preshared keys for authentication.
- IPv4 & IPv6 addresses. All combinations of inside and outside are supported.
- Static and dynamic interfaces.
- HA environments for both Firewall Management Center and Firewall Threat Defense.
- VPN alerts when the tunnel goes down and tunnel statistics.
- IKEv1 and IKEv2 back-up peer configuration for point-to-point extranet and hub-and-spoke VPNs.
- Extranet device as hub in 'Hub and Spokes' deployments.
- Dynamic IP address for a managed endpoint pairing with extranet device in 'Point to Point' deployments and for extranet device as an endpoint.

VPN topologies

VPN topology configuration requires specifying a unique name, a topology type, IKE version selection, and authentication method. The Secure Firewall Management Center configures site-to-site VPNs on Firewall 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.

In the Secure Firewall 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.

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.

IPsec and IKE

In the Secure Firewall 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 don't manage in Firewall Management Center. These include:

- Cisco devices that Secure Firewall Management Center supports, but for which your organization isn't 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 can't use Secure Firewall Management Center to create and deploy configurations to non-Cisco devices.

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

Guidelines for configuring site-to-site VPN in Secure Firewall Threat Defense devices

General guidelines

- Site-to-site VPN supports ECMP zone interfaces.
- Configure all nodes in a topology with either crypto ACL or a protected network. You cannot configure a topology with crypto ACL on one node and protected network on another.
- Configure a VPN connection across domains by using an extranet peer for the endpoint not in the current domain.
- You can backup Firewall Threat Defense VPNs using the Firewall Management Center backup.
- Configure unique local IKE identity for all tunnels across all your VPN topologies.
- Ensure that IKE ports 500 and 4500 are not already in use and that no active PAT translations exist on those ports before configuring a site-to-site VPN. Configuring a site-to-site VPN on ports that are already in use will cause the service to fail to start.
- When configuring a site-to-site VPN between two devices managed by the same Firewall Management Center, do not configure the devices as backup peers. Instead, configure one of the peer devices in the topology as an extranet device.
- If a spoke is part of multiple topologies with the same hub, for the Local Tunnel (IKE) Identity, we recommend that you use Key ID instead of an IP address.

  If the spoke uses an IP address as its local identity, the hub creates only one tunnel group. The spoke is then mapped to a specific virtual template interface, so the connection works with only one topology.

Limitations for configuring site-to-site VPN in Threat Defense devices

General limitations

- IKEv1 does not support CC/UCAPL-compliant devices. IKEv2 is recommended for these devices.
- VPN does not support network objects with a 'range' option.
- Firewall Threat Defense VPNs do not support PDF export and policy comparison.
- Tunnel status is not updated realtime, but at an interval of five minutes in the Firewall Management Center.
- You cannot use the double quote character (") in pre-shared keys, replace it if already in use.

Crypto ACL limitations

- Firewall Management Center supports only point-to-point VPN with crypto ACL and does not support tunnel health events.
- Firewall Management Center does not verify the device interface address verification for transport mode when you select a crypto ACL.
- There is no support for automatic mirror ACE generation. Mirror ACE generation for the peer is a manual process on either side.

Topology management limitations

- You cannot move a VPN topology between domains.
- There is no per-tunnel or per-device edit option for Firewall Threat Defense VPNs, you can edit only the whole topology.

Types of site-to-site VPN topologies

This table provides an overview of the different site-to-site VPN topology options available for secure network connectivity configuration.

Site-to-Site VPN Topology	Description	More Information
Route-Based VPN	Configure secure traffic dynamically between peers in a network based on routing over Virtual Tunnel Interfaces (VTIs).	Create a route-based site-to-site VPN, on page 24
Policy-Based VPN	Configure secure traffic between peers in a network based on a static policy using protected networks.	Configure a policy-based site-to-site VPN, on page 6

License requirements for site-to-site VPN

This topic lists the license requirements for setting up various types of site-to-site VPN connections.

License requirements for policy-based and route-based VPN

With the Base license, you can set up policy-based and route-based VPNs on your Firewall Threat Defense devices.

Depending on whether export-controlled functionality is enabled in your Smart License account, Firewall Management Center determines whether to allow or block the usage of strong crypto on devices. To verify if export-controlled functionality is enabled for your Smart License account, choose **System** (⚙) > **Licenses** > **Smart Licenses**.

Note If you use an evaluation license, or if you have not enabled the export-controlled functionality, you cannot use strong encryption for your VPN connections.

Prerequisites for site-to-site VPN

Supported interfaces

Topology Type	Interface Type

Policy-Based	• Physical interfaces
	  • Non-management
	  • Interface Mode must be either Routed or None
	• Subinterface interfaces
	• Redundant interfaces
	• Etherchannel interfaces
	• VLAN interfaces

Route-Based	Static Virtual Tunnel Interfaces



Note The maximum number of supported security associations (SA) depends on the maximum VPN peers for your platform. For more information about maximum VPN peers, refer the data sheet of the Secure Firewall Threat Defense device.

General prerequisites

- You must have administrator privileges.
- You must be in a leaf domain to perform the site-to-site VPN configurations.

Manage site-to-site VPNs

You can view, create, modify, and deploy site-to-site VPN configurations and manage their deployment status.

The **Site-to-Site VPN** page provides a snapshot of site-to-site VPN tunnels. You can view the status of the tunnels and filter the tunnels based on the device, topology, or tunnel type. The page lists 20 topologies per page and you can navigate between pages to view more topology details. You can click individual VPN topologies to expand and view details of the endpoints.

Before you begin

For certificate authentication of your site-to-site VPNs, you must prepare the devices by allocating trustpoints as described in Certificates.

Procedure

Select **Devices** > **VPN** > **Site to Site** to manage your Firewall Threat Defense site-to-site VPN configurations and deployments.

The page lists the site-to-site VPNs topologies and indicates the status of tunnels using color codes:

- Active (Green)–There is an active IPsec Tunnel.
- Unknown (Amber)–No tunnel establishment event has been received from the device yet.
- Down (Red)–There are no active IPsec tunnels.
- Deployment Pending–Topology has not been deployed on the device yet.

Choose one of these actions:

- **Refresh**—View the updated status of the VPNs.
- **Add**—Create new policy based or route-based Site to Site VPNs.
- **Edit**—Modify the settings of an existing VPN topology.

  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 shouldn't edit the same topology simultaneously; however, the web interface doesn't prevent simultaneous editing.

- **Delete**—To delete a VPN deployment, click **Delete** ( ).
- Deploy—Choose **Deploy** > **Deploy**; see Deploy configuration changes.

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

Configure a policy-based site-to-site VPN

Configure a policy-based site-to-site VPN to establish secure communication channels between network endpoints using crypto maps and specified network topologies.

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** and click the **Policy Based (Crypto Map)** radio button, and choose the **Network Topology** for this VPN.

Step 3 Choose the IKE versions to use during IKE negotiations. Check the **IKEv1** or **IKEv2** check box.

Default is IKEv2. Select either or both options as appropriate; select IKEv1 if any device in the topology doesn't support IKEv2.

You can also configure a backup peer for point-to-point extranet VPNs. For more information, see Firewall Threat Defense VPN endpoint options, on page 7.

Step 4 Required: Add Endpoints for this VPN deployment by clicking **Add** (+) for each node in the topology.

Configure each endpoint field as described in Firewall Threat Defense VPN endpoint options, on page 7.

- 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 5 (Optional) Specify non-default IKE options for this deployment as described in Firewall Threat Defense VPN IKE options, on page 11

Step 6 (Optional) Specify non-default IPsec options for this deployment as described in Firewall Threat Defense VPN IPsec options, on page 14

Step 7 (Optional) Specify non-default Advanced options for this deployment as described in Firewall Threat Defense advanced site-to-site VPN deployment options, on page 16 and click **Save**.

The policy-based site-to-site VPN is configured with the specified endpoints, IKE settings, and topology options.

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.

Firewall Threat Defense VPN endpoint options

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 Firewall Threat Defense device managed by this Firewall Management Center
- A Firewall Threat Defense high availability container managed by this Firewall Management Center
- An **Extranet** device, any device (Cisco or third party) not managed by this Firewall 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 unmanaged 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. An endpoint with a dynamic interface can pair only with an extranet device and can't 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 Firewall 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 chose a managed device as an endpoint, choose a single IPv4 address or multiple IPv6 addresses from the drop-down list. These IP addresses are already assigned to this interface on the 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 uses.
- 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 Firewall Management Center and don't use this option if the peer is an extranet device.

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

Remote Node	Central Node
Bi-Directional	Bi-Directional

Certificate Map

Choose a preconfigured certificate map object, or click **Add** (+) to add a certificate map object. The certificate map defines what information is necessary in the received client certificate to be valid for VPN connectivity. See Certificate map objects for details.

Protected Networks

Caution Hub and Spoke topology—To avoid traffic drop for a dynamic crypto map, ensure that you don't select the protected network *any* for both the endpoints.

If the protected network is configured as *any*, on both the endpoints, the crypto ACL that works upon the tunnel is not generated.

Defines the networks that are protected by this VPN endpoint. Select the networks 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 Create a network object . Access control lists are generated from the choices made here.

- **Subnet/IP Address (Network)** —VPN endpoints can't have the same IP address and protected networks in a VPN endpoint pair cannot overlap. If protected networks for an endpoint contain IPv4 or IPv6 entries, the other endpoint's protected network must have at least one entry of the same type (IPv4 or IPv6). If it doesn't, the other endpoint's IP address must be of the same type and 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 By default, **Reverse Route Injection is enabled** check box is enabled in Firewall Management Center.

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

When you've selected Protected Networks as *Any* and observe default route traffic being dropped, disable the Reverse Route Injection. Choose **VPN** > **Site to Site** . Edit a VPN and then click **IPsec** > **Enable Reverse Route Injection** . Deploy the configuration changes to 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 list provides 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) enables routes to be automatically inserted into the routing process, for the 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 isn't 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.

Send Local Identity to Peers —Select this option to send local identity information to the peer device. Select one of the following **Local Identity Configuration** from the list and configure the local identity:

- **IP address**—Use the IP address of the interface for the identity.
- **Auto**—Use the IP address for pre-shared key and Cert DN for certificate-based connections.
- **Email ID**—Specify the email ID to use for the identity. The email address can be up to 127 characters.
- **Hostname**—Use the fully qualified hostname.
- **Key ID**—Specify the key-id to use for the identity. The key ID must be fewer than 65 characters.

The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels. The unique identity allows Firewall Threat Defense to have multiple IPsec tunnels behind a NAT to connect to the Cisco Umbrella Secure Internet Gateway (SIG).

For information about configuring a unique tunnel ID on Umbrella, see **Cisco Umbrella SIG User Guide**.

VPN Filter—Select an extended access list from the list or click **Add** to create a new extended access list object to filter the site-to-site VPN traffic.

The VPN filter provides more security and filters site-to-site VPN data using an extended access list. The extended access list object selected for the VPN filter lets you filter pre-encrypted traffic before entering the VPN tunnel and decrypted traffic that exits a VPN tunnel. The **sysopt permit-vpn** option, when enabled, would bypass the access control policy rules for the traffic coming from the VPN tunnel. When the **sysopt permit-vpn** option is enabled, the VPN filter helps in identifying and filtering the site-to-site VPN traffic.

Note The VPN filter is supported only on point to point, and hub and spoke topologies. It isn't supported on mesh topology.

For hub and spoke topology, you can choose to override the hub VPN filter on the spoke endpoints in case a different VPN filter needs to enabled on a specific tunnel.

Select the **Override VPN Filter on the Hub** option to override the hub VPN filter on the spokes. Select the **Remote VPN Filter** extended access list object or create an access list to override.

Note For an extranet device as a spoke, only the **Override VPN filter on the Hub** option is available.

For more information about sysopt permit-VPN, see Firewall Threat Defense advanced site-to-site VPN tunnel options , on page 18 .

NAT Traversal (NAT-T)

NAT-T allow seamless communication between the peer Firewall Threat Defense devices when there are NAT devices between these devices. You cannot disable NAT Traversal (NAT-T) per VPN using the Firewall Management Center UI. This option is available from Version 7.4.1. You can use FlexConfig to disable NAT-T. You can add the **crypto map** *map-name seq-num* **set nat-t-disable** command in the FlexConfig object. For example, **crypt map CSM_outside_map 1 set nat-t-disable**.

Note You must create the FlexConfig object with Deployment as 'EveryTime' and Type as 'Append'. This setting removes the command and adds it back for each deployment. If you configure Deployment as 'Once', then the command will be removed in the next deployment. You must be careful when you configure the FlexConfig object with this command. If Firewall Management Center changes the sequence number, the deployment will fail.

Firewall 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.

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 the required IKEv1 or IKEv2 policy objects from the predefined list or create new objects to use. You can choose multiple IKEv1 and IKEv2 policies. IKEv1 and IKEv2 support a maximum of 20

IKE policies, each with a different set of values. Assign a unique priority to each policy that you create. The lower the priority number, the higher the priority.
We recommend that you do NOT use values such as 10, 20 and so on because the default IKEv2 policy for remote access VPN can have these values as its priority value. Before deployment, verify that the priority values of the IKE policies (site-to-site and remote access VPN) do NOT conflict.
For details, see 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 Decide VPN authentication methods.

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 Firewall Management Center automatically defines the pre-shared key for this VPN. Specify the **Pre-shared Key Length**, the number of characters in the key. The range is 1 to 27.

  The character " (double quote) isn't supported as part of pre-shared keys. If you've used " in a pre-shared key, ensure that you change the character after you upgrade to Secure Firewall Threat Defense 6.30 or higher.

- **Pre-shared Manual Key**—Manually assign the pre-shared key for this VPN. Specify the **Key** and then reenter the same to **Confirm Key**.

  When you choose this option 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 preconfigured certificate enrollment object. This enrollment object generates 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 these requirements:

  - Ensure you've 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 Add certificate enrollment objects, and for instructions on enrolling the object on the endpoints see one of these as applicable:

    - Install a certificate using self-signed enrollment

- Install a certificate using EST enrollment
- Install a certificate using SCEP enrollment
- Install a certificate using manual enrollment
- Install 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 to this 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 Manage 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
EST	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 Secure Firewall 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 use 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 can't complete the site-to-site VPN connection.

Firewall Threat Defense VPN IPsec options

Configure the basic parameters for a point-to-point topology in a route-based VPN as described in Configure Endpoints for a Point to Point Topology and click the **IPsec** tab.



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. IPsec security negotiation uses the proposals defined in the crypto map entry 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 these 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. 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 you don't need to modify the end systems 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 fall back to tunnel mode if the peer doesn't 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 allowed. If the endpoints can't 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 an IKEv1 IPsec proposal object and Configure an IKEv2 IPsec proposal object for details.

Enable Security Association (SA) Strength Enforcement

Enabling this option ensures that the encryption algorithm used by the child IPsec SA isn't 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 Decide 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 isn't 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.

Note You can enable dummy Traffic Flow Confidentiality (TFC) packets at random lengths and intervals on an IPsec security association (SA). You must have an IKEv2 IPsec proposal set before enabling TFC.

Enabling TFC packets prevents the VPN tunnel from being idle. Thus the VPN idle timeout configured in the group policy doesn't work as expected when you enable the TFC packets.

Firewall Threat Defense advanced site-to-site VPN deployment options

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

Firewall Threat Defense VPN advanced IKE options

Advanced > IKE > ISAKAMP settings

IKE Keepalive

Enable or disables IKE Keepalives. You can set this option to EnableInfinite so that the device never starts the keepalive monitoring itself.

Threshold

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

Peer Identity Validation

During IKE tunnel establishment, the peer provides its identity: either an IP address, a Fully Qualified Domain Name (FQDN), or a Distinguished Name (DN). It also presents a certificate, which contains none, some, or all of these fields.

If IKE peer identity validation is enabled, the Firewall Threat Defense compares the peer's identity to the respective field in the certificate to see if the information matches. If the information matches, then the peer's identity is validated and the Firewall Threat Defense establishes the tunnel. If the information does not match, the tunnel is not established.

- **Do not check**—Firewall Threat Defense does not validate the peer identity.
- **Required**—Firewall Threat Defense validates the peer identity.
- **If supported by cert**—Firewall Threat Defense validates the peer identity only if the peer provides a certificate.

Enable Aggressive Mode

Select this negotiation method for exchanging key information if the IP address isn't known and DNS resolution might not be available on the devices. Negotiation is based on hostname and domain name.

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. This notification is disabled by default.

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's 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 doesn't match the traffic selectors for that SA. Sending this notification is disabled by default.

Firewall Threat Defense VPN advanced IPsec options

Advanced > IPsec > IPsec Settings

The advanced IPsec settings include these configuration options:

- **Enable Fragmentation Before Encryption**: This option lets traffic travel across NAT devices that don't support IP fragmentation. It doesn't impede the operation of NAT devices that do support IP fragmentation.
- **Path Maximum Transmission Unit Aging**: Check to enable Path Maximum Transmission Unit (PMTU) Aging, the interval to reset the PMTU of a Security Association (SA).
- **Value Reset Interval**: Enter the number of minutes at which the PMTU value of an SA is reset to its original value. The range is 10 to 30 minutes, default is unlimited.

Firewall Threat Defense advanced site-to-site VPN tunnel options

This topic lists the advanced site-to-site VPN tunnel options.

Navigation path

Overview > **Dashboards** > **Site to Site VPN**, 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 doesn’t appear 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**—Enabled by default. This parameter is a global setting that enables NAT-T for all endpoints within a topology. Check this check box to enable keepalive messages for NAT traversal. NAT traversal keepalive is used for the transmission of keepalive messages when there’s a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow.

  NAT traversal allows seamless communication between the peer Firewall Threat Defense devices when there are NAT devices between these devices. For hub and spoke topologies, this option is available only for the spoke.

  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)—By default, the Firewall Threat Defense applies access control policy inspection on the decrypted traffic. Enable this option to bypass the ACL inspection. The Firewall Threat Defense still applies the VPN Filter ACL and authorization ACL downloaded from the AAA server to the VPN traffic.

Enable or disable the option for all your VPN connections. If you disable this option, ensure that the traffic is allowed by the access control policy or prefilter policy.

Note For route-based VPNs, **sysopt permit-vpn** does not work. You must always create access control rules to allow route-based VPN traffic.

Certificate map settings

- **Use the certificate map configured in the Endpoints to determine the tunnel**—If this option is enabled (checked), the tunnel is 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 isn't 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 isn't 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 isn't 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.

Configure virtual tunnel interfaces

Firewall Management Center supports a routable logical interface called the Virtual Tunnel Interface (VTI).

Virtual tunnel interfaces

A virtual tunnel interface is a routable logical interface that

- does not require static mapping of IPsec sessions to a physical interface
- associates the IPsec tunnel endpoint with a virtual interface, and
- supports static and dynamic routing policies.

Virtual tunnel interface capabilities

Firewall Management Center supports VTIs as an alternative to policy-based VPN. VTIs support route-based VPN with IPsec profiles attached to the end of each tunnel. VTIs use static or dynamic routes. The device encrypts or decrypts the traffic from or to the tunnel interface and forwards it according to the routing table. Deployments become easier, and having VTI which supports route-based VPN with dynamic routing protocol also satisfies many requirements of a virtual private cloud. Firewall Management Center enables you to easily migrate from crypto-map based VPN configuration to VTI-based VPN.

You can configure route-based VPN with static VTI using the site-to-site VPN wizard. 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.

You can create VTI-based VPNs between:

- Two Firewall Threat Defense devices.
- A Firewall Threat Defense and public cloud.
- One Firewall Threat Defense and another Firewall Threat Defense with service provider redundancy.
- A Firewall Threat Defense and any other device with VTI interfaces.
- A Firewall Threat Defense and another device with policy-based VPN configuration.

For more information, see Static VTI, on page 20 .

Static VTI

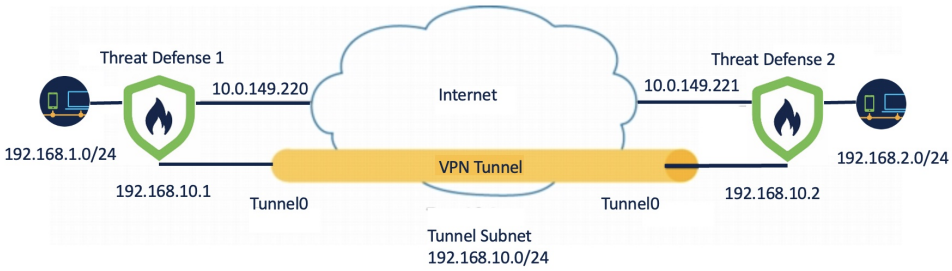
A static VTI is a virtual tunnel interface that

- uses tunnel interfaces to create a tunnel that is always-on between two sites
- requires defining a physical interface as a tunnel source, and
- supports a maximum of 1024 VTIs per device.

To create a static VTI interface in the Management Center, see Add a VTI interface, on page 23.

The figure shows a VPN topology using static VTIs.

Figure 1: Static VTI VPN topology



On Threat Defense 1:

- Static VTI IP address is 192.168.10.1
- Tunnel source is 10.0.149.220
- Tunnel destination is 10.0.149.221

On Threat Defense 2:

- Static VTI IP address is 192.168.10.2
- Tunnel source is 10.0.149.221
- Tunnel destination is 10.0.149.220

Benefits of SVTI

Static VTI provides these benefits:

- Minimizes and simplifies configuration.

  You do not have to track all remote subnets for a crypto map access list, and configure complex access lists or crypto maps.

- Provides a routable interface.

  Supports IP routing protocols such as BGP, and static routes.

- Supports backup VPN tunnels
- Supports load balancing using ECMP.
- Supports virtual routers.
- Provides differential access control for VPN traffic.

  You can configure a VTI with a security zone and use it in an AC policy. This configuration:

  - Allows you to classify and differentiate VPN traffic from clear-text traffic and permit VPN traffic selectively.
  - Provides differential access-control for VPN traffic across different VPN tunnels.

Guidelines for virtual tunnel interfaces

General configuration guidelines

- VTIs are only configurable in IPsec mode.
- You can use BGP or static routes for traffic using the tunnel interface.
- In an HA configuration with dynamic routing, the standby device cannot access the known subnets through the VTI tunnels as these tunnels are created with the active IP address.
- If NAT has to be applied, the IKE and ESP packets are encapsulated in the UDP header.
- Ensure that you remove unused transform sets from route-based IKE VPN configurations. If you have unused transform sets, the VPN tunnels may not come up and encapsulation and decapsulation will not happen. Use **show run crypto** and **show VPN-sessiondb detail l2l** commands to view the transform sets.

IPv6 address guidelines

- VTI supports IPv6 addresses.
- You can use an IPv6 address for the tunnel source interface and use the same address as the tunnel endpoint.
- The Firewall Management Center supports the following combinations of VTI IP (or internal networks IP version) over public IP versions: IPv6 over IPv6, IPv4 over IPv6, IPv4 over IPv4, and IPv6 over IPv4.
- VTI supports static and dynamic IPv6 addresses as the tunnel source and destination.

- The tunnel source interface can have IPv6 addresses and you can specify the tunnel endpoint address. If you don't specify the address, by default, the device uses the first IPv6 global address in the list as the tunnel endpoint.

IKE support and guidelines

- Static VTI supports IKE v1 and v2.
- IKE and IPsec security associations are 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 sends as its IKEv1 or IKEv2 identity.
- For IKEv1 in LAN-to-LAN tunnel groups, you can use names which aren't IP addresses, if the tunnel authentication method is digital certificates and/or the peer is configured to use aggressive mode.

MTU behavior

- MTU for VTIs is automatically set based on the underlying physical interface.

VTI scaling and guidelines

- Configure a maximum of 1024 static VTIs in a device.

  While calculating the VTI count, consider nameif subinterfaces, portchannel configurations, and platform VLAN limitations.
- If you configure more than 400 VTIs in a device in a high-availability setup, configure 45 seconds as the unit holdtime.

Routing protocol support

VTI supports multiple routing protocols for different IP versions.

- VTI supports IPv6 BGP.

ECMP configuration guidelines

- Configure spokes' static VTIs in an ECMP zone to load balance application traffic. If you do not configure the ECMP zone, the remaining paths act as backup paths when the primary path goes down.
- You can associate VTI interfaces with ECMP zones and configure ECMP static routes to achieve these benefits:
  - Load balancing (Active/Active VTIs)—Connection can flow over any of the parallel VTI tunnels.
  - Seamless connection migration—When a VTI tunnel becomes unreachable, the flows are seamlessly migrated to another VTI interface that is configured in the same zone.
  - Asymmetric routing—Forward traffic flow through one VTI interface and configure the reverse traffic flow through another VTI interface.

  For information on configuring ECMP, see ECMP routing methods.

Access control rule guidelines

- By default, all traffic sent through a VTI is encrypted.
- Access control rules can be applied on a VTI interface to control traffic through VTI.

- For route-based VPNs, Bypass Access Control policy for decrypted traffic (**sysopt connection permit-VPN**) does not work. You must always create access control rules to allow route-based VPN traffic.

Crypto map guidelines

- VTI and crypto map configurations can coexist on the same physical interface if the peer address configured in the crypto map and the tunnel destination for the VTI are different.

Topology guidelines

Firewall mode guideline

Configure VTI only in routed mode.

Limitations for Virtual Tunnel Interfaces

This topic lists the limitations for configuring Virtual Tunnel Interfaces in Management Center.

General limitations

- VTIs do not support clustering.
- VTI tunnel interfaces are not supported for SNMP or Syslog in Platform Settings.

Static VTI limitations

- Only 20 unique IPSec profiles are supported.
- Dynamic VTI, OSPF, and QoS aren't supported.
- In policy-based routing, you can configure VTI only as an egress interface.
- You cannot configure a VTI interface as a network interface for a remote access VPN policy.

Backup VTI limitations

- Flow resiliency across tunnel failovers isn't supported. For example, the clear text TCP connection gets lost after a tunnel failover, and you need to reinitiate any FTP transfer that took place during the failover.
- Certificate authentication isn't supported in backup VTI.

Add a VTI interface

For configuring a route-based site-to-site VPN, you must create a VTI interface on the devices at both the nodes of the VTI tunnel.

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 Choose **Add Interfaces > Virtual Tunnel Interface**.

In the **Add Virtual Tunnel Interface** dialog box, configure these parameters:

a) (Optional) Choose a security zone from the **Security Zone** drop-down list to add the static VTI interface to that zone. In the **Priority** field, enter the priority to load balance the traffic across multiple VTIs.

If you want to perform traffic inspection based on a security zone, add the VTI interface to the security zone and configure an access control (AC) rule. To permit the VPN traffic over the tunnel, you need to add an AC rule with this security zone as the source zone.

The priority range is from 0 to 65535. The lowest number has the highest priority. This option is not applicable for dynamic VTI.

b) For a static VTI, enter a unique tunnel ID in the range of 0 to 10413 in the **Tunnel ID** field.

c) Choose the tunnel source interface from the **Tunnel Source** drop-down list.

The VPN tunnel terminates at this interface, a physical interface. Choose the IP address of the interface from the drop-down list. You can select the IP address irrespective of the IPsec tunnel mode. In case of multiple IPv6 addresses, select the address that you want to use as the tunnel endpoint.

d) Under **IPSec Tunnel Mode**, click the **IPv4** or **IPv6** radio button to specify the traffic type over the IPsec tunnel.

e) 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
We recommend that you use an IP from 169.254.x.x/16 range excluding the Firewall Threat Defense reserved range (169.254.1.x/24). Also, use /30 as net-mask to optimally use only two addresses for the two ends of the VTI tunnel. For example, 169.254.100.1/30.

Step 4 Click **OK**.

Step 5 Click **Save**.

Create a route-based site-to-site VPN

You can configure a route-based site-to-site VPN for the following two topologies:

- **Point to Point**: Configure VTIs on both nodes of the tunnel and use the wizard to configure the VPN.
- **Hub and Spoke**: Configure VTIs on the hub and the spokes.

You can configure an extranet device as the hub and managed devices as spokes. You can configure multiple hubs and spokes, and also configure backup hubs and spokes.

- For extranet hubs and spokes, you can configure multiple IPs as backup.
- For managed spokes, you can configure a backup static VTI interface along with the primary VTI interface.

For more information on VTI, see Virtual tunnel interfaces, on page 19.

Procedure

Step 1 Choose **Devices** > **VPN** > **Site to Site**.

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

Step 3 Enter a name for the VPN topology in the **Topology Name** field.

Step 4 Choose **Route Based (VTI)** and do one of the following:

- Select **Point to Point** as the network topology. To configure endpoints for a route-based **Point to Point** topology, see Configure endpoints for a point-to-point VPN topology, on page 25.
- Select **Hub and Spoke** as the network topology. To configure endpoints for a route-based **Hub and Spoke** topology, see Configure Endpoints for a Hub and Spoke Topology, on page 27.

Step 5 (Optional) Specify the **IKE**, **IPsec**, and **Advanced** options and click **Save**.

For more information, refer to these topics:

- Firewall Threat Defense VPN IKE options, on page 11
- Firewall Threat Defense VPN IPsec options, on page 14
- Firewall Threat Defense advanced site-to-site VPN deployment options, on page 16

What to do next

After you configure VTI interfaces and VTI tunnel on both the devices, you must configure:

- A routing policy to route the VTI traffic between the devices over the VTI tunnel. For more information, see Configure routing and AC policies for VTI, on page 30.
- An access control rule to allow encrypted traffic. Choose **Policies > Access Control**.

Configure endpoints for a point-to-point VPN topology

Configure these parameters to configure endpoints for a route-based site-to-site VPN for the **Point to Point** topology nodes:

Before you begin

Configure the basic parameters for a point-to-point topology in a route-based VPN as described in Create a route-based site-to-site VPN, on page 24 and click the **Endpoints** tab.

Procedure

Step 1 Under **Node A**, in the **Device** drop-down menu, select the name of the registered device (Firewall Threat Defense) or extranet as the first endpoint of your VTI tunnel.

For an extranet peer, specify the following parameters:

a. Specify the name of the device.

b. Enter the primary IP address in the **Endpoint IP address** field. If you configure a backup VTI, add a comma and, specify the backup IP address.

c. Click **OK** .

After configuring the above parameters for the extranet hub, specify the pre-shared key for the extranet in the **IKE** tab.

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

Step 2 For a registered device, you can specify the VTI interface for Node A from the **Virtual Tunnel Interface** drop-down list.

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

If you want to create a new interface on Node A, click the Add + icon and configure the fields as described in Add a VTI interface, on page 23 .

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**.

Step 3 If your Node A device is behind a NAT device, check the **Tunnel Source IP is Private** check box. In the **Tunnel Source Public IP Address** field, enter the tunnel source public IP address.

Step 4 **Send Local Identity to Peers** —Select this option to send local identity information to the peer device. Select one of the following **Local Identity Configuration** from the list and configure the local identity:

- **IP address** —Use the IP address of the interface for the identity.
- **Auto** —Use the IP address for pre-shared key and Cert DN for certificate-based connections.
- **Email ID** —Specify the email ID to use for the identity. The email ID can be up to 127 characters.
- **Hostname** —Use the fully qualified hostname.
- **Key ID** —Specify the key-id to use for the identity. The key ID must be fewer than 65 characters.

The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels. The unique identity allows Firewall Threat Defense to have multiple IPsec tunnels behind a NAT to connect to a Cisco Umbrella Secure Internet Gateway (SIG).

For information about configuring a unique tunnel ID on Umbrella, see **Cisco Umbrella SIG User Guide** .

Step 5 (Optional) Click **Add Backup VTI** to specify an extra VTI as the backup interface and configure the parameters.

Note
Ensure that both peers of the topology do not have the same tunnel source for the backup VTI. A device cannot have two VTIs with the same tunnel source and tunnel destination; hence, configure a unique tunnel source and tunnel destination combination.

Though the virtual tunnel interface is specified under Backup VTI, the routing configuration determines which tunnel to be used as primary or backup.

Step 6 In the **Connection Type** drop-down menu, select **Answer Only** or **Bidirectional** . If you have selected the IKE protocol version as IKEv1, one of the nodes must be **Answer Only** .

Answer Only : The device can only respond when a peer device initiates a connection, it cannot initiate any connection.

Bidirectional : The device can initiate or respond to a connection. This is the default option.

Step 7 Under **Additional Configuration** , do the following:

- To route traffic to the VTI, click **Routing Policy** . Firewall Management Center displays the **Devices** > **Routing** page.

  You can configure the Static or BGP routing for the VPN traffic.

- To permit VPN traffic, click **AC Policy** . Firewall Management Center displays the access control policy page of the device. Proceed to add an allow/block rule specifying the security zone of the VTI. If you configure a backup VTI, 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.

Step 8 Repeat the above procedure for Node B and click **OK** .

What to do next

- (Optional) Specify the **IKE** options for the deployment as described in Firewall Threat Defense VPN IKE options, on page 11.
- (Optional) Specify the **IPsec** options for the deployment as described in Firewall Threat Defense VPN IPsec options, on page 14.
- (Optional) Specify the **Advanced** options for the deployment as described in Firewall Threat Defense advanced site-to-site VPN deployment options, on page 16.
- Click **Save**.
- To route traffic to the VTI, choose **Devices** > **Device Management** , edit the threat defense device and click the **Routing** tab.

  You can configure the static routes or use BGP for routing the VPN traffic.
- To permit VPN traffic, choose **Policies** > **Access Control heading** > **Access Control**. Add a rule specifying the security zone of the VTI. For a backup VTI, ensure that you include the backup VTI in the same security zone as that of the primary VTI.

Configure Endpoints for a Hub and Spoke Topology

Configure the following parameters to configure endpoints for a route-based site-to-site VPN for the **Hub and Spoke** topology nodes:

Before you begin

Configure the basic parameters for a hub and spoke topology in a route-based VPN as described in Create a route-based site-to-site VPN, on page 24 and click the **Endpoints** tab.

Procedure

Step 1 **Add the Hub Nodes**:

a) Under **Hub Nodes**, click Add +.
b) In the **Device Name**, enter the name of the device.
c) In the **Endpoint IP address**, enter the primary IP address. If you are configuring a backup hubs, enter a comma and then specify the backup IP address.
d) Click the **IKE** tab and specify the pre-shared key provided on the extranet.
e) Click **OK**.

Add the Spoke Nodes:

- For extranet spokes, the configuration parameters are similar to the hubs.
- For the managed spoke nodes, configure the parameters similar to point-to-point nodes.

a) Under **Spoke Nodes**, click Add +.
b) In the **Device** drop-down menu, select the name of the registered device (Firewall Threat Defense).
c) Specify the interface settings:

- In the **Static Virtual Tunnel Interface** drop-down menu, select the VTI interface, which you had created on Firewall Threat Defense device that you've selected as the VTI endpoint.
- If you want to create a new interface, click the Add + icon and fill the fields as described in Add a VTI interface, on page 23.
- If you want to edit the configuration of an existing VTI, select the VTI in the **Static Virtual Tunnel Interface** drop-down field and click **Edit VTI**.

Step 2 If your endpoint device is behind a NAT device, check the **Tunnel Source IP is Private** check box. In the **Tunnel Source Public IP Address** field, enter the tunnel source public IP address.

Step 3 **Send Local Identity to Peers**—Select this option to send local identity information to the peer device. Select one of the following **Local Identity Configuration** from the list and configure the local identity:

- **IP address**—Use the IP address of the interface for the identity.
- **Auto**—Use the IP address for pre-shared key and Cert DN for certificate-based connections.
- **Email ID**—Specify the email ID to use for the identity. The email ID can be up to 127 characters.
- **Hostname**—Use the fully qualified hostname.
- **Key ID**—Specify the key-id to use for the identity. The key ID must be less than 65 characters.

The local identity is used to configure a unique identity per IKEv2 tunnel, instead of a global identity for all the tunnels. The unique identities allow Firewall Threat Defense to have multiple IPsec tunnels behind a NAT to connect to Cisco Umbrella Secure Internet Gateway (SIG).

For information about configuring a unique tunnel ID on Umbrella, see **Cisco Umbrella SIG User Guide**.

Step 4 (Optional) Click **Add Backup VTI** to specify an additional VTI as the backup interface.

Note

Ensure that both peers of the topology do not have backup VTI configured on the same tunnel source. For instance, if Peer A has two VTIs (primary and a backup) configured with a single tunnel source interface, say, 10.10.10.1/30, then Peer B also can't have its two VTIs with a single tunnel source IP, say 20.20.20.1/30.

Note
Though the virtual tunnel interface is specified under Backup VTI, the routing configuration determines which tunnel to be used as primary or backup.

You can do the following:

- To create a new backup interface, use the Add + icon.
- To edit the configuration of an existing Backup VTI, use **Edit VTI**.

Note
If the device is behind a NAT device, check the **Tunnel Source IP is Private** check box. In the **Tunnel Source Public IP Address** field, enter the tunnel source public IP address.

Step 5 Expand **Advance Settings** and in the **Connection Type** drop-down menu, select **Answer Only** or **Bidirectional**. If you've selected an IKE protocol version as IKEv1, one of the nodes must be **Answer Only**.

Step 6 For an extranet spoke, 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. If you are configuring a backup VTI, enter a comma and then specify the backup IP address.

c. Click the **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 7 Repeat the previous procedure to configure more spoke nodes.

Step 8 Click **OK**.

What to do next

- (Optional) Specify the **IKE** options for the deployment as described in Firewall Threat Defense VPN IKE options, on page 11.
- (Optional) Specify the **IPsec** options for the deployment as described in Firewall Threat Defense VPN IPsec options, on page 14.
- (Optional) Specify the **Advanced** options for the deployment as described in Firewall Threat Defense advanced site-to-site VPN deployment options, on page 16.
- Click **Save**.

Route traffic through a backup VTI tunnel

A backup VTI tunnel ensures traffic continuity by providing an alternative path when the primary VTI tunnel fails to route traffic in route-based VPN configurations.

You can deploy the backup VTI tunnel in these scenarios:

- Both peers having service provider redundancy backup.

  In this case, there are two physical interfaces, acting as the tunnel sources for the two VTIs of the peers.

- Only one of the peers has service provider redundancy backup.

  In this case, there's an interface backup on only one side of the peer and on the other end, there is only one tunnel source interface.

Before you begin

Ensure that you review the guidelines and limitations. For more information, refer to Guidelines for virtual tunnel interfaces, on page 21.

Procedure

Step 1 Create the VTI interface.

For more information, refer to Add a VTI interface, on page 23

Step 2 In the **Add Endpoint** dialog box of the **Create New VPN Topology** wizard, click **Add Backup VTI** to configure the respective backup interface for each peer.

For more information, refer to

- Configure endpoints for a point-to-point VPN topology, on page 25
- Configure Endpoints for a Hub and Spoke Topology, on page 27

Step 3 Choose **Devices > Device Management**, and edit the threat defense device and click **Routing** to configure the routing policy.

Step 4 Choose **Policies > Access Control** to configure the access control policy.

Configure routing and AC policies for VTI

After you configure VTI interfaces and the VTI tunnel on both the devices, you must configure these parameters:

- A routing policy to route VTI traffic between the devices over the VTI tunnel.
- An access control rule to allow encrypted traffic.

Procedure

Step 1 Configure routing for VTI interfaces.

For the VTI interfaces, you can configure static route or routing protocols such AS BGP.

a. Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

b. Click **Routing**.

c. Configure static route, or BGP.

Routing	Parameters	More Information
Static Route	• **Interface**—Select the VTI interface. For a backup tunnel, select the backup VTI interface. • **Selected Network**—Remote peer's protected network. • **Gateway**—Remote peer's tunnel interface IP address. For a backup tunnel, select the remote peer's backup tunnel interface IP address. • **Metric**—For a backup tunnel, configure a different metric to handle the failover of the traffic flow over the backup tunnel. **Note** DVTI does not support static routes.	Add a static route

BGP	• 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/IPv6 and click the **Neighbor** tab to configure the neighbors.
	  • **IP Address**—Remote peer's VTI interface IP address. For a backup tunnel, add a neighbor with the remote peer's backup VTI interface IP address.
	  • **Remote AS**—Remote peer's AS number.
	• Click the **Redistribution** tab, select the **Source Protocol** AS Connected to enable connected route redistribution.
		Configure BGP

Step 2 Add an access control rule to the access control policy on the device to allow encrypted traffic between the VTI tunnels with these settings:

a. Create the rule with the Allow action.

b. 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.

c. 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.

Monitor site-to-site topologies

This section provides information about the different ways to monitor your site-to-site topologies.

Monitor site-to-site VPNs using Site-to-Site VPN summary page

You can view a summary of your site-to-site VPN topologies in the **Site-to-Site VPN Summary** page. For each topology, you can view details such as VPN type, network topology, VPN interfaces, VPN devices, and tunnel statuses.

You can edit or delete the topology using the edit and delete buttons.

Monitor site-to-site VPNs using Site-to-Site VPN dashboard

The **Site-to-Site VPN** dashboard provides a snapshot and status of the site-to-site VPN tunnels. You can view the list of tunnels between peer devices and the status of each tunnel: Active, Inactive, or No Active Data. You can filter the data in the table according to the topology, device, and status. The dashboard shows live data and you can also configure the refresh interval.

Benefits of the dashboard

The dashboard provides these benefits:

- Identify problematic VPN tunnels and troubleshoot them.
- Verify connectivity between the site-to-site VPN peers devices.
- Monitor the health of the VPN tunnels to provide uninterrupted VPN connectivity between sites.
- Use Packet tracer to troubleshoot VPN tunnels.

Widgets of the dashboard

- **Tunnel Status Table**—A table listing the site to site VPNs configured using the Firewall Management Center
- **Tunnel Status Distribution Chart**—Aggregated status of the tunnels in a donut graph.

- **Topology Summary Listing**—Tunnel status summarized by topology.

Status of VPN tunnels

The different VPN tunnel statuses that you can view in the Site-to-Site dashboard are:

- **Inactive**—A policy-based (crypto map-based) VPN tunnel is inactive if all the IPSec tunnels are down. A VTI or tunnel is down if the tunnel encounters any configuration or connectivity issues.
- **Active**—In the Firewall Management Center, policy-based site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. A policy-based VPN tunnel is in the Active state if the Firewall Management Center identifies interesting traffic through the tunnel after the deployment. An IKE tunnel is up only if a minimum of one IPsec tunnel is up.

  Route-based VPN (VTI) tunnels do not require interesting traffic to be in the Active state. They are in the Active state if they are configured and deployed without errors.
- **No Active Data**—Policy-based tunnels remain in the No Active Data state until there is a traffic flow event through the tunnel for the first time. The No Active Data state also lists the policy-based and route-based VPNs that have been deployed with errors.

Limitations of the dashboard

- The table shows the list of site-to-site VPNs that are deployed. It does not show the tunnels that are created and not deployed.
- The table does not show the information about the backup tunnels of policy-based VPNs and backup VTIs.
- For cluster deployments, the table does not show director change in real-time data. It shows only the director information that existed when the VPN was deployed. The director change reflects in the table only after the tunnel AM redeployed after the change.

Tunnel status widget

This widget lists the site-to-site VPNs, configured using the Firewall Management Center and their tunnel statuses.

Features of the widget

Hover over a topology and click **View** ( ) to view these details about the topology:

- **General**—Displays more information about the nodes such as IP address and interface name.
- **CLI Details**—Displays the CLI outputs for the following commands:
  - **show crypto ipsec sa peer**: Displays the IPsec SAs built between Node A and B.
  - **show vpn-sessiondb l2l filter ipaddress** : Displays information about VPN sessions.

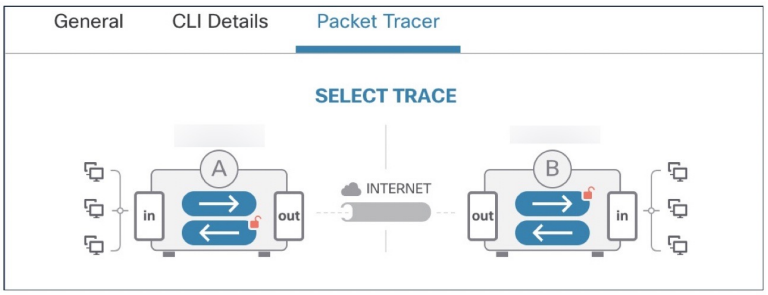
  For an extranet device, no command output appears.
- **Packet Tracer**—Use packet tracer to troubleshoot the VPN tunnels.

Packet Tracer

Packet tracer allows you to troubleshoot VPN tunnels between two threat defense devices. You can check if the VPN connection between device A and device B is up. This tool performs these actions:

- Injects a packet into the device and tracks the packet flow from the ingress to the egress ports.
- Simulates traffic after you configure the ingress interfaces of the devices along with the protected networks.
- Evaluates the packet against modules such as flow and route lookups, ACLs, protocol inspection, NAT, and QoS.

Figure 2: Packet Tracer



For each device, the tool runs an encrypted trace and a decrypted trace (packet is treated as decrypted VPN traffic). You can run four different traces between the ingress and egress ports of the devices. Click the individual encrypt and decrypt options to enable or disable the trace.

When you run the trace, the tool executes the trace sequentially in the following order:

1. Encrypted trace of A.
2. Decrypted trace of B.
3. Encrypted trace of B.
4. Decrypted trace of A.

After the trace completes, you can view the output of the trace with the results of each module.

Note You cannot run a decrypt trace for route-based (VTI-based) VPNs.

To run the Packet Tracer:

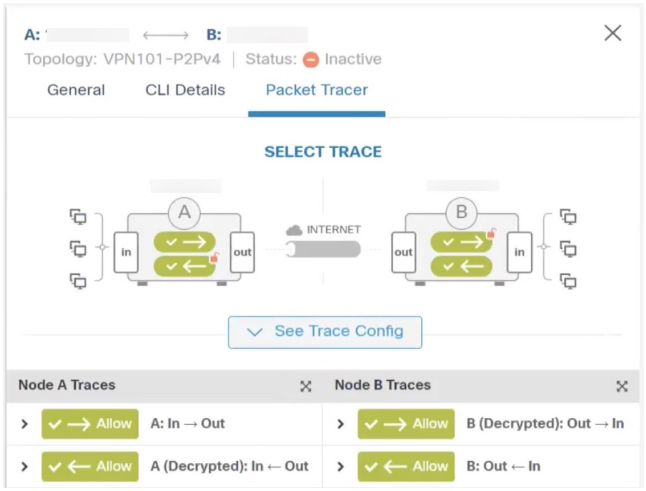
1. Click **See Detailed Config** to view the VPN interface name, VPN interface IP address, VTI interface name, and the VTI Interface IP address.
2. (Optional) Choose a protocol from the **Protocol** drop-down list. You can choose ICMP/8/0, TCP, or UDP.

   ICMP/8/0 is the default option. If you choose ICMP/8/0, 8 indicates the ICMP type as Echo Request and 0 indicates the ICMP code. If you choose TCP or UDP, choose the destination port from the **Destination Port** drop-down list. The range is from 0 to 65535.

3. Choose the ingress interface for both the devices on which to trace the packet from the **Ingress Interface** drop-down lists. Packet Tracer does not support loopback interfaces.
4. Enter an IP address from the same subnet as the ingress interface in the **Protected Network IP Address** fields.
5. Click **Trace Now**.

   After you initiate the trace, you can view if the trace is successful or not for each module. If the tunnel is down, the path appears in red. If the tunnel is up, the path appears in green. If a tunnel is down, click **Re-trace** to run the tool again. For a crypto-map based VPN, when the tunnel is inactive with no interesting traffic, the initial trace can be red. Click **Re-trace** to run the trace again.

Figure 3: Packet Tracer after a Successful Trace



Extranet Nodes: You can initiate a packet trace for VPN tunnels with one node as an extranet. For an extranet node, you cannot choose the ingress interface. The remaining steps for the packet trace are the same. You can't run trace on the extranet side.

For example, if Node A is a managed threat defense and Node B is an extranet:

- Configure the ingress interface for node A.
- Configure the protected network for Node A and B.
- Click **Trace Now**. The traces appear for Node A and not for Node B.

History for site-to-site VPN

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
IPsec flow offload	7.2	Any	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command.
Site-to-Site VPN Filter	7.1	Any	You can control site-to-site VPN traffic by using an access control policy.
Local tunnel ID support	7.1	Any	For each endpoint on a site-to-site VPN, you can configure a unique tunnel ID to be shared with the peers.
Multiple IKE Policy Support	7.1	Any	You can add multiple IKEv1 and IKEv2 policy objects for each endpoint.
Site-to-Site VPN Monitoring Dashboard	7.1	Any	Use the Site-to-Site VPN Monitoring dashboard to view and monitor the status of site-to-site VPN tunnels.
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	7.0	Any	When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel. Specifying a backup VTI provides resiliency, so that if the primary connection goes down, the backup connection might still be functional. For example, you could point the primary VTI to the endpoint of one service provider, and the backup VTI to the endpoint of a different service provider. You can add a backup VTI in the site-to-site VPN wizard by selecting route-based as the VPN type for a point-to-point connection.
Enhance the number of VTI from 100 per interface to 1024 per device	7.0	Any	Support for maximum number of VTIs is enhanced from 100 per physical interface to 1024 VTIs per device.
IPv6 Support	7.0	Any	You can configure IPv6 addressed VTIs. While only static IPv6 address is supported as the tunnel source and destination, IPv6 BGP isn't supported over VTI.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Removal and deprecation of weak ciphers	6.7	Any	Support has been removed for less secure ciphers. We recommend that you update your VPN configuration before you upgrade to Firewall Threat Defense 6.70 to supported DH and encryption algorithms to ensure the VPN works correctly. Update your IKE proposals and IPSec policies to match the ones supported in Firewall Threat Defense 6.70 and then deploy the configuration changes. These less secure ciphers have been removed or deprecated in Firewall Threat Defense 6.70 onwards: • **Diffie-Hellman GROUP 5** is deprecated for IKEv1 and removed for IKEv2 • Diffie-Hellman groups 2 and 24 have been removed. • **Encryption algorithms**: 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256 have been removed. **Note** **DES** is supported in evaluation mode or for users who do not satisfy export controls for strong encryption. **NULL** is removed in IKEv2 policy, but supported in both IKEv1 and IKEv2 IPsec transform-sets.
Dynamic RRI support	6.7	Any	Dynamic Reverse Route Injection is supported with IKEv2 based static crypto maps.
Backup peer for site-to-site VPN	6.6	Any	You can use the Firewall Management Center to add a backup peer to a site-to-site VPN connection. For example, if you have two ISPs, you can configure the VPN connection to fail over to the backup ISP if the connection to the first ISP becomes unavailable. New/modified pages: **Devices** > **VPN** > **Site to Site**. When adding or editing a point to point or hub and spoke FTD VPN topology to add an endpoint, the **IP Address** field supports comma-separated backup peers.