

Gateway VPNs

The following topics describe how to manage your VPN deployment:

- Gateway VPN Basics, on page 1
- VPN Deployments, on page 2
- VPN Deployment Management, on page 4
- VPN Deployment Status, on page 15
- VPN Statistics and Logs, on page 15

Gateway VPN Basics

A virtual private network (VPN) is a network connection that establishes a secure tunnel between endpoints via a public source, such as the internet or other network. You can configure the Firepower System to build secure VPN tunnels between the virtual routers of Firepower managed devices. The system builds tunnels using the Internet Protocol Security (IPsec) protocol suite.

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. A connection consists of the IP addresses and host names of the two gateways, the subnets behind them, and the shared secrets for the two gateways to authenticate to each other.

The VPN endpoints authenticate to each other with either the Internet Key Exchange (IKE) version 1 or version 2 protocol to create a security association for the tunnel. The system uses either the IPsec authentication header (AH) protocol or the IPsec encapsulating security payload (ESP) protocol to authenticate the data entering the tunnel. The ESP protocol encrypts the data as well as providing the same functionality as AH.

If you have access control policies in your deployment, the system does not send VPN traffic until it has passed through access control. In addition, the system does not send tunnel traffic to the public source when the tunnel is down.

To configure and deploy VPN for Firepower, you must have a VPN license enabled on each of your target managed devices. Additionally, VPN features are only available on 7000 and 8000 Series devices.

IPsec

The IPsec protocol suite defines how IP packets across a VPN tunnel are hashed, encrypted, and encapsulated in the ESP or AH security protocol. The Firepower System uses the hash algorithm and encryption key of the Security Association (SA), which becomes established between the two gateways by the Internet Key Exchange (IKE) protocol.

Security associations (SA) establish shared security attributes between two devices and allow VPN endpoints to support secure communication. An SA allows two VPN endpoints to handle the parameters for how the VPN tunnel is secured between them.

The system uses the Internet Security Association and Key Management Protocol (ISAKMP) during the initial phase of negotiating the IPsec connection to establish the VPN between endpoints and the authenticated key exchange. The IKE protocol resides within ISAKMP.

The AH security protocol provides protection for packet headers and data, but it cannot encrypt them. ESP provides encryption and protection for packets, but it cannot secure the outermost IP header. In many cases, this protection is not required, and most VPN deployments use ESP more frequently than AH because of its encryption capabilities. Since VPN only operates in tunnel mode, the system encrypts and authenticates the entire packet from Layer 3 and up in the ESP protocol. ESP in tunnel mode encrypts the data as well as providing the latter's encryption capabilities.

IKE

The Firepower System uses the IKE protocol to mutually authenticate the two gateways against each other as well as to negotiate the SA for the tunnel. The process consists of two phases.

IKE phase 1 establishes a secure authenticated communication channel by using the Diffie-Hellman key exchange to generate a pre-shared key to encrypt further IKE communications. This negotiation results in a bidirectional ISAKMP security association. The system allows you to perform the authentication using a pre-shared key. Phase 1 operates in main mode, which seeks to protect all data during the negotiation, while also protecting the identity of the peers.

During IKE phase 2, the IKE peers use the secure channel established in phase 1 to negotiate security associations on behalf of IPsec. The negotiation results in a minimum of two unidirectional security associations, one inbound and one outbound.

VPN Deployments

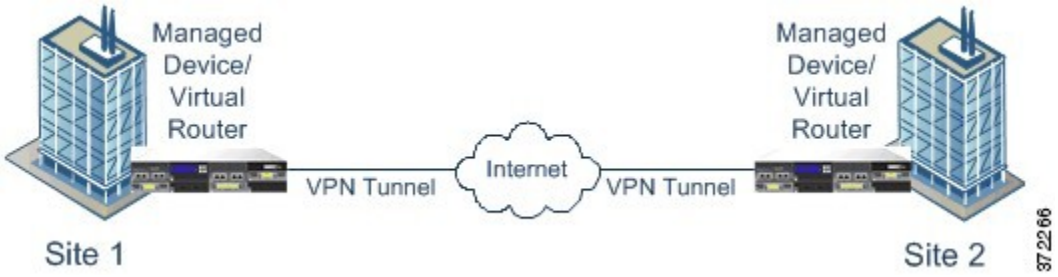
A VPN deployment specifies the endpoints and networks that are included in a VPN and how they connect to each other. After you configure a VPN deployment on the Firepower Management Center, you can then deploy it to your managed devices or devices managed by another Firepower Management Center.

The system supports three types of VPN deployments: point-to-point, star, and mesh.

Point-to-Point VPN Deployments

In a point-to-point VPN deployment, two endpoints communicate directly with each other. You configure the two endpoints as peer devices, and either device can start the secured connection. Each of the devices in this configuration must be a VPN-enabled managed device.

The following diagram displays a typical point-to-point VPN deployment.



Star VPN Deployments

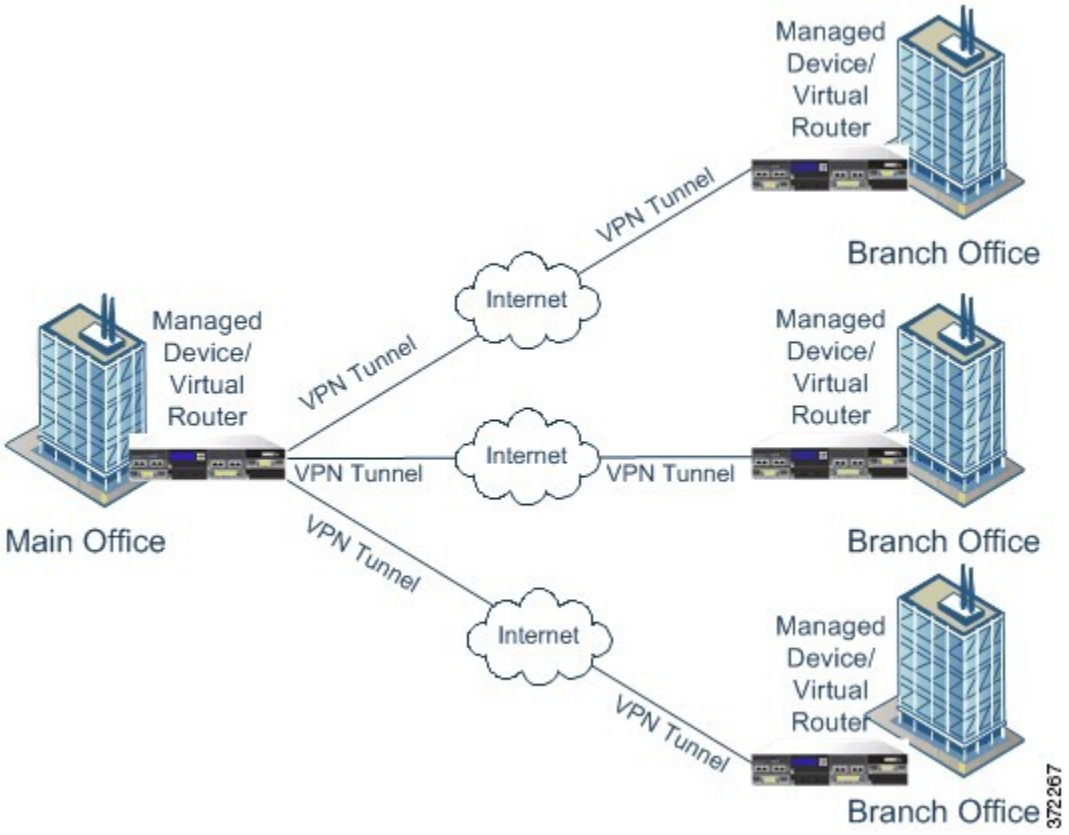
In a star VPN deployment, a central endpoint (hub node) establishes a secure connection with multiple remote endpoints (leaf nodes). Each connection between the hub node and an individual leaf node is a separate VPN tunnel. The hosts behind any of the leaf nodes can communicate with each other through the hub node.

Star deployments commonly represent a VPN that connects an organization's main and branch office locations using secure connections over the Internet or other third-party network. Star VPN deployments provide all employees with controlled access to the organization's network.

In a typical star deployment, the hub node is located at the main office. Leaf nodes are located at branch offices and start most of the traffic. Each of the nodes must be a VPN-enabled managed device.

Star deployments only support IKE version 2.

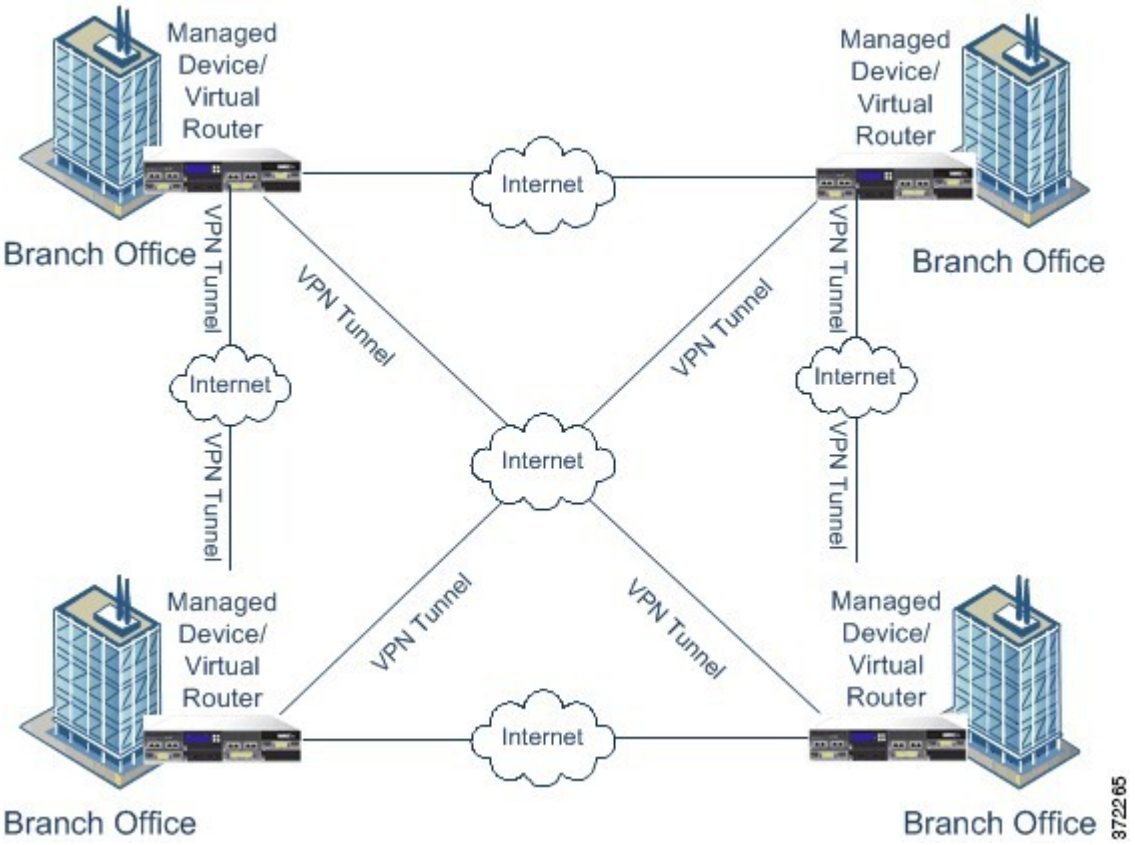
The following diagram displays a typical star VPN deployment.



Mesh VPN Deployments

In a mesh VPN deployment, all endpoints can communicate with every other endpoint by an individual VPN tunnel. The mesh deployment offers redundancy so that when one endpoint fails, the remaining endpoints can still communicate with each other. This type of deployment commonly represents a VPN that connects a group of decentralized branch office locations. The number of VPN-enabled managed devices you deploy in this configuration depends on the level of redundancy you require. Each of the endpoints must be a VPN-enabled managed device.

The following diagram displays a typical mesh VPN deployment.



VPN Deployment Management

On the VPN page (**Devices** > **VPN**), you can view all of your current VPN deployments by name and the endpoints contained in the deployment. Options on this page allow you to view the status of a VPN deployment, create a new deployment, deploy to managed devices, and edit or delete a deployment.

Note that when you register a device to a Firepower Management Center, deployed VPN deployments sync to the Firepower Management Center during registration.

Related Topics

Managing VPN Deployments, on page 10

VPN Deployment Options

When you create a new VPN deployment you must, at minimum, give it a unique name, specify a deployment type, and designate a preshared key. You can select from three types of deployment, each containing a group of VPN tunnels:

- Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.
- Star deployments establish a group of VPN tunnels connecting a hub endpoint to a group of leaf endpoints.
- Mesh deployments establish a group of VPN tunnels among a set of endpoints.

Only Cisco managed devices can be used as endpoints in VPN deployments. Third-party endpoints are not supported.

You must define a pre-shared key for VPN authentication. You can specify a default key to use in all of the VPN connections you generate in a deployment. For point-to-point deployments, you can specify a preshared key for each endpoint pair.

In a multidomain deployment, you can configure a VPN deployment across domains; that is, you can assign endpoints to devices that belong to different domains. In such cases, you can view but not modify the ancestor deployment in the related descendant domains. When you drill down for deployment details, the system displays information for devices that belong to the current domain only.

Point-to-Point VPN Deployment Options

When configuring a point-to-point VPN deployment, you define a group of endpoint pairs and then create a VPN between the two nodes in each pair.

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

Name

Specify a unique name for the deployment.

Type

Click **PTP** to specify that you are configuring a point-to-point deployment.

Pre-shared Key

Define a unique pre-shared key for authentication. The system uses this key for all the VPNs in your deployment, unless you specify a pre-shared key for each endpoint pair.

Device

You can choose a managed device, including a device stack or device high-availability pair, as an endpoint for your deployment. For Cisco-managed devices not managed by the Firepower Management Center you are using, choose **Other** and then specify an IP address for the endpoint.

Virtual Router

If you chose a managed device as your endpoint, choose a virtual router that is currently applied to the selected device. You cannot choose the same virtual router for more than one endpoint.

Interface

If you chose a managed device as your endpoint, choose a routed interface that is assigned to the virtual router you specified.

IP Address

- If you chose a managed device as an endpoint, choose an IP address that is assigned to the specified routed interface.
- If the managed device is a device high-availability pair, you can choose only from a list of SFRP IP addresses.
- If you choose a managed device **not** managed by the Firepower Management Center, specify an IP address for the endpoint.

Protected Networks

Specify the networks in your deployment that are encrypted. Enter a subnet with CIDR block for each network. IKE version 1 only supports a single protected network.

Note that VPN endpoints cannot have the same IP address and that 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 entry, the other endpoint's protected network must have at least one entry of the same type (i.e., 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.

Internal IP

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

Public IP

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

Public IKE Port

If you checked the **Internal IP** check box, specify a single numerical value from 1 to 65535 for the UDP port on the firewall that is being port-forwarded to the internal endpoint. If the endpoint is a responder and the port on the firewall being forwarded is not 500 or 4500, you must specify this value.

Use Deployment Key

Check the check box to use the pre-shared key defined for the deployment. Clear the check box to specify a pre-shared key for VPN authentication for this endpoint pair.

Pre-shared Key

If you cleared the **Use Deployment Key** check box, specify a pre-shared key in this field.

Related Topics

Configuring Point-to-Point VPN Deployments, on page 11

Star VPN Deployment Options

When configuring a star VPN deployment, you define a single hub node endpoint and a group of leaf node endpoints. You must define the hub node endpoint and at least one leaf node endpoint to configure the deployment.

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

Name

Specify a unique name for the deployment.

Type

Click **Star** to specify that you are configuring a star deployment.

Pre-shared Key

Define a unique pre-shared key for authentication.

Device

You can choose a managed device, including a device stack or device high-availability pair, as an endpoint for your deployment. For Cisco-managed devices not managed by the Firepower Management Center you are using, choose **Other** and then specify an IP address for the endpoint.

Virtual Router

If you chose a managed device as your endpoint, choose a virtual router that is currently applied to the selected device. You cannot choose the same virtual router for more than one endpoint.

Interface

If you chose a managed device as your endpoint, choose a routed interface that is assigned to the selected virtual router.

IP Address

- If you chose a managed device as an endpoint, choose an IP address that is assigned to the specified routed interface.
- If the managed device is a device high-availability pair, you can choose only from a list of SFRP IP addresses.
- If you chose a managed device **not** managed by the Firepower Management Center, specify an IP address for the endpoint.

Protected Networks

Specify the networks in your deployment that are encrypted. Enter a subnet with CIDR block for each network.

Note that VPN endpoints cannot have the same IP address and that 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 entry, the other endpoint's protected network must have at least one entry of the same type (i.e., 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.

Internal IP

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

Public IP

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

Public IKE Port

If you checked the **Internal IP** check box, specify a single numerical value from 1 to 65535 for the UDP port on the firewall that is being port-forwarded to the internal endpoint. If the endpoint is a responder and the port on the firewall being forwarded is not 500 or 4500, you must specify this value.

Related Topics

Configuring Star VPN Deployments, on page 11

Mesh VPN Deployment Options

When configuring a mesh VPN deployment, you define a group of VPNs to link any two points for a given set of endpoints.

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

Name

Specify a unique name for the deployment.

Type

Click **Mesh** to specify that you are configuring a mesh deployment.

Pre-shared Key

Define a unique pre-shared key for authentication.

Device

You can choose a managed device, including a device stack or device high-availability pair, as an endpoint for your deployment. For Cisco-managed devices not managed by the Firepower Management Center you are using, choose **Other** and then specify an IP address for the endpoint.

Virtual Router

If you chose a managed device as your endpoint, choose a virtual router that is currently applied to the specified device. You cannot choose the same virtual router for more than one endpoint.

Interface

If you chose a managed device as your endpoint, choose a routed interface that is assigned to the specified virtual router.

IP Address

- If you chose a managed device as an endpoint, choose an IP address that is assigned to the selected routed interface.
- If the managed device is a device high-availability pair, you can choose only from a list of SFRP IP addresses.
- If you chose a managed device **not** managed by the Firepower Management Center, specify an IP address for the endpoint.

Protected Networks

Specify the networks in your deployment that are encrypted. Enter a subnet with CIDR block for each network. IKE version 1 only supports a single protected network.

Note that VPN endpoints cannot have the same IP address and that 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 entry, the other endpoint's protected network must have at least one entry of the same type (i.e., 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.

Internal IP

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

Public IP

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

Public IKE Port

If you checked the **Internal IP** check box, specify a single numerical value from 1 to 65535 for the UDP port on the firewall that is being port-forwarded to the internal endpoint. If the endpoint is a responder and the port on the firewall being forwarded is not 500 or 4500, you must specify this value.

Related Topics

Configuring Mesh VPN Deployments, on page 12

Advanced VPN Deployment Options

VPN deployments contain some common settings that can be shared among the VPNs in a deployment. Each VPN can use the default settings or you can override the default settings. Advanced settings typically require little or no modification and are not common to every deployment.

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

Other Algorithm Allowed

Check the check box to enable auto negotiation to an algorithm not listed in the Algorithm list, but proposed by the remote peer.

Algorithm

Specify the phase one and phase two algorithm proposals to secure data in your deployment. Choose **Cipher**, **Hash**, and Diffie-Hellman (**DH**) group authentication messages for both phases.

IKE Life Time

Specify a numerical value and choose a time unit for the maximum IKE SA renegotiation interval. You can specify a minimum of 15 minutes and a maximum of 30 days.

IKE v2

Check the check box to specify that the system uses IKE version 2. This version supports the star deployment and multiple protected networks.

Life Time

Specify a numerical value and select a time unit for the maximum SA renegotiation interval. You can specify a minimum of 5 minutes and a maximum of 24 hours.

Life Packets

Specify the number of packets that can be transmitted over an IPsec SA before it expires. You can use any integer between 0 and 18446744073709551615.

Life Bytes

Specify the number of bytes that can be transmitted over an IPsec SA before it expires. You can use any integer between 0 and 18446744073709551615.

AH

Check the check box to specify that the system uses the authentication header security protocol for the data to be protected. Clear the check box to use encryption service payload (ESP) protocol.

Related Topics

Configuring Advanced VPN Deployment Settings, on page 13

Managing VPN Deployments

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

Caution Adding or removing a VPN on a 7000 or 8000 Series device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.

Procedure

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

Step 2 Manage your VPN deployments:

- Add — To create a new VPN deployment, click **Add VPN** > **Firepower Device**, and continue as follows depending on deployment type:
  - Configuring Mesh VPN Deployments, on page 12
  - Configuring Point-to-Point VPN Deployments, on page 11
  - Configuring Star VPN Deployments, on page 11
- Edit — To modify the settings in an existing VPN deployment, click the edit icon ( ); see Editing VPN Deployments, on page 14.
- Delete — To delete a VPN deployment, click the delete icon ( ).
- Deploy—Click **Deploy**; see Deploy Configuration Changes.
- View VPN status — To view the status of an existing VPN deployment, click the status icon; see Viewing VPN Status, on page 15.

Related Topics

Snort® Restart Scenarios

Configuring Point-to-Point VPN Deployments

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

Before you begin

If you are using managed devices as endpoints, create a virtual router and apply it to the appropriate device.

Note You cannot use the same virtual router for more than one endpoint. For more information, see Setting Up Virtual Routers

Procedure

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

Step 2 Click **Add VPN** > **Firepower Device**.

Step 3 Enter a unique **Name**.

Step 4 Verify that **PTP** is chosen as the **Type**.

Step 5 Enter a unique **Pre-shared Key**.

Step 6 Next to **Node Pairs**, click the add icon ( ).

Step 7 Configure the VPN deployment options described in Point-to-Point VPN Deployment Options, on page 5.

Step 8 Under **Node A**, next to **Protected Networks**, click the add icon ( ).

Step 9 Enter a CIDR block for the protected network.

Step 10 Click **OK**.

Step 11 Repeat step 8 through step 10 for **Node B**.

Step 12 Click **Save**.
The endpoint pair is added to your deployment.

Step 13 Click **Save** to finish configuring your deployment.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Configuring Star VPN Deployments

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

Before you begin

If you are using managed devices as endpoints, create a virtual router and apply it to the appropriate device.

Note You cannot use the same virtual router for more than one endpoint. For more information, see Setting Up Virtual Routers

Procedure

Step 1 Choose **Devices** > **VPN**.
Step 2 Click **Add VPN** > **Firepower Device**.
Step 3 Enter a unique **Name**.
Step 4 Click **Star** to specify the **Type**.
Step 5 Enter a unique **Pre-shared Key**.
Step 6 Next to **Hub Node**, click the edit icon ( ).
Step 7 Configure the VPN deployment options described in Star VPN Deployment Options, on page 6.
Step 8 Next to **Protected Networks**, click the add icon ( ).
Step 9 Enter an IP address for the protected network.
Step 10 Click **OK**.
Step 11 Click **Save**. The hub node is added to your deployment.
Step 12 Next to **Leaf Nodes**, click the add icon ( ).
Step 13 Repeat step 7 through step 10 to complete the leaf node, which has the same options as the hub node.
Step 14 Click **Save**.
The leaf node is added to your deployment.
Step 15 Click **Save** to finish configuring your deployment.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Configuring Mesh VPN Deployments

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

Before you begin

If you are using managed devices as endpoints, create a virtual router and apply it to the appropriate device.

Note You cannot use the same virtual router for more than one endpoint. For more information, see Setting Up Virtual Routers

Procedure

Step 1 Choose **Devices** > **VPN**.
Step 2 Click **Add VPN** > **Firepower Device**.
Step 3 Enter a unique **Name**.
Step 4 Click **Mesh** to specify the **Type**.
Step 5 Enter a unique **Pre-shared Key**.
Step 6 Next to **Nodes**, click the add icon ( ).
Step 7 Configure the VPN deployment options described in Mesh VPN Deployment Options, on page 8.
Step 8 Next to **Protected Networks**, click the add icon ( ).
Step 9 Enter a CIDR block for the protected network.
Step 10 Click **OK**.
The protected network is added.
Step 11 Click **Save**.
The endpoint is added to your deployment.
Step 12 Repeat step 6 through step 11 to add more endpoints.
Step 13 Click **Save** to complete your deployment.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Configuring Advanced VPN Deployment Settings

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

In a multidomain deployment, the system displays VPN deployments created in the current domain, which you can edit. It also displays VPN deployments created in ancestor domains if one of the endpoint devices belongs to your domain. You cannot edit VPN deployments created in ancestor domains. To view and edit VPN deployments created in a lower domain, switch to that domain.

Procedure

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

Step 2 Click the edit icon ( ).

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Click the **Advanced** tab.

Step 4 Configure the advanced settings, as described in Advanced VPN Deployment Options, on page 9.

Step 5 Next to **Algorithms**, click the add icon ( ).

Step 6 Chose **Cipher**, **Hash**, and Diffie-Hellman (**DH**) group authentication messages for both phases.

Step 7 Click **OK**.

Step 8 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Editing VPN Deployments

Caution Two users should **not** edit the same deployment simultaneously; however, note that the web interface does not prevent simultaneous editing.

In a multidomain deployment, the system displays VPN deployments created in the current domain, which you can edit. It also displays VPN deployments created in ancestor domains if one of the endpoint devices belongs to your domain. You cannot edit VPN deployments created in ancestor domains. To view and edit VPN deployments created in a lower domain, switch to that domain.

Procedure

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

Step 2 Click the edit icon ( ).

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Modify the desired settings:

- Advanced settings; see Configuring Advanced VPN Deployment Settings, on page 13.
- Mesh deployment settings; see Configuring Mesh VPN Deployments, on page 12.
- Point-to-point deployment settings; see Configuring Point-to-Point VPN Deployments, on page 11.
- Star deployment settings; see Configuring Star VPN Deployments, on page 11.

Tip You cannot edit the deployment type after you initially save the deployment. To change the deployment type, you must delete the deployment and create a new one.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

VPN Deployment Status

After you configure a VPN deployment, you can view the status of your configured VPN tunnels. The VPN page displays a status icon for each VPN deployment once it has been deployed:

- The ( ) icon designates that all VPN endpoints are up.
- The ( ) icon designates that all VPN endpoints are down.
- The ( ) icon designates that some endpoints are up, while others are down.

You can click a status icon to view the deployment status along with basic information about the endpoints in the deployment, such as endpoint name and IP address. The VPN status updates every minute or when a status change occurs, such as an endpoint going down or coming up.

Related Topics

Viewing VPN Status, on page 15

Viewing VPN Status

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

In a multidomain deployment, the system displays VPN deployments created in the current domain. It also displays VPN deployments created in ancestor domains if one of the endpoint devices belongs to your domain. To view VPN deployments created in a lower domain, switch to that domain.

Procedure

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

Step 2 Click the VPN status icon next to the deployment where you want to view the status.

Step 3 Click **OK**.

VPN Statistics and Logs

After you configure a VPN deployment, you can view statistics about the data traversing your configured VPN tunnels. In addition, you can view the latest VPN system and IKE logs for each endpoint.

The system displays the following statistics:

Endpoint

The device path to the routed interface and IP address designated as the VPN endpoint.

Status

Whether the VPN connection is up or down.

Protocol

The protocol used for encryption, either ESP or AH.

Packets Received

The number of packets per interface the VPN tunnel receives during an IPsec SA negotiation.

Packets Forwarded

The number of packets per interface the VPN tunnel transmits during an IPsec SA negotiation.

Bytes Received

The number of bytes per interface the VPN tunnel receives during an IPsec SA negotiation.

Bytes Forwarded

The number of bytes per interface the VPN tunnel transmits during an IPsec SA negotiation.

Time Created

The date and time the VPN connection was created.

Time Last Used

The last time a user initiated a VPN connection.

NAT Traversal

If "Yes" is displayed, at least one of the VPN endpoints resides behind a device with network address translation.

IKE State

The state of the IKE SA: connecting, established, deleting, or destroying.

IKE Event

The IKE SA event: reauthentication or rekeying.

IKE Event Time

The time in seconds the next event should occur.

IKE Algorithm

The IKE algorithm being used by the VPN deployment.

IPsec State

The state of the IPsec SA: installing, installed, updating, rekeying, deleting, and destroying.

IPsec Event

Notification of when the IPsec SA event is rekeying.

IPsec Event Time

The time in seconds until the next event should occur.

IPsec Algorithm

IPsec algorithm being used by the VPN deployment.

Related Topics

Viewing VPN Statistics and Logs, on page 17

Viewing VPN Statistics and Logs

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	VPN	7000 & 8000 Series	Any	Admin/Network Admin

In a multidomain deployment, the system displays VPN deployments created in the current domain. It also displays VPN deployments created in ancestor domains if one of the endpoint devices belongs to your domain. To view VPN deployments created in a lower domain, switch to that domain.

Procedure

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

Step 2 Click the VPN status icon next to the deployment for which you want to view statistics.

Step 3 Click the view statistics icon ().

Step 4 Optionally, click **Refresh** to update the VPN statistics.

Step 5 Optionally, click **View Recent Log** to view the latest data log for each endpoint. To view the log for 7000 or 8000 Series devices in high-availability pairs and stacked devices, you can click the link for either the active/primary or backup/secondary device.