Configure Route-Based Site-to-Site VPN between Cisco Secure Management Center and AWS VPC

Revised: August 16, 2024

Configure Route-Based Site-to-Site VPN between Cisco Secure Management Center and AWS VPC

Introduction

The Secure Firewall Management Center (Management Center) features intuitive VPN wizards designed to streamline the configuration of site-to-site VPNs on managed Threat Defense devices.

These wizards also facilitate the setup of route-based site-to-site VPNs between Threat Defense devices and extranet devices. Extranet devices, which are not under the direct management of the management center, may comprise gateways located within public cloud infrastructures. Route-based VPNs use Virtual Tunnel Interfaces (VTIs)—routable logical interfaces that form the foundation of the VPN tunnel.

Is this Guide for You?

This guide is intended for network administrators who use the Management Center to establish a site-to-site VPN between a Threat Defense device located at the headquarters and an AWS Virtual Private Cloud (VPC).

Scenario

A medium-sized enterprise operates several branch offices, each with a set of instances hosted on AWS. This organization must establish a robust network infrastructure to facilitate secure and seamless communication across all locations. The solution involves configuring a site-to-site VPN that connects each branch's AWS VPC to the Threat Defense device at the organization's central headquarters. This connectivity is crucial because, by default, AWS VPC instances are isolated from external networks. The implementation of this VPN will enable the integration of the branches into the corporate network, ensuring centralized access and data security.

System Requirements

The following table shows the platforms for this feature.

Product	Version	Version Used in This Document
Cisco Secure Firewall Threat Defense (formerly Firepower Threat Defense/FTD)	6.7 and later	7.4.1
Cisco Secure Firewall Management Center (formerly Firepower Management Center/FMC)	6.7 and later	7.4.1
AWS Account	-	-

Benefits

The proposed solution offers significant benefits such as:

- Streamlined Setup: VTI offers a simplified approach to VPN configuration, removing the complexity of traditional crypto maps and access lists.
- Adaptive Routing: VTI accommodates dynamic routing protocols such as BGP, EIGRP, and OSPF, facilitating the automatic update of routes between VPN endpoints in response to changing network conditions.
- ISP Resilience: VTI enables the creation of secondary backup tunnels, enhancing connectivity reliability.
- Load balancing: VTI allows for the even distribution of VPN traffic through ECMP routing.

Prerequisites

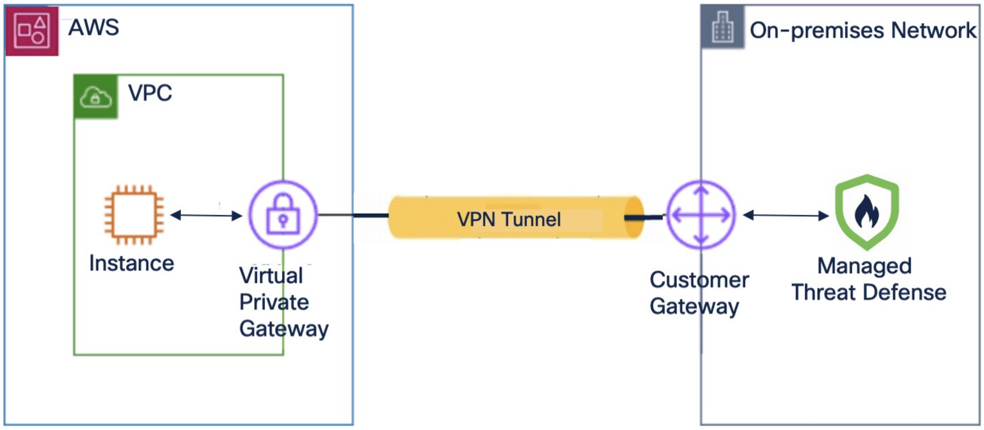
- Licenses: Management center Essentials (formerly Base) license must allow export-controlled functionality. Choose **System** > **Licenses** > **Smart Licenses** to verify this functionality in the Management Center.
- Configure an internet-routable, public IP address for the Threat Defense device.
- Assign appropriate logical names and IP addresses to the interfaces of the Threat Defense devices.
- Own an AWS account.

Components of a Site-to-Site VPN between Management Center and AWS

A site-to-site VPN between the Management Center and AWS consists of the following components:

- Virtual Private Gateway
- Customer Gateway Device (Managed Threat Defense)
- Customer Gateway

Figure 1: Site-to-Site VPN between an AWS VPC and an On-Premises Network



Virtual Private Gateway

A virtual private gateway is the VPN concentrator on the AWS side of the site-to-site VPN connection. You create a virtual private gateway and attach it to a virtual private cloud (VPC).

Customer Gateway

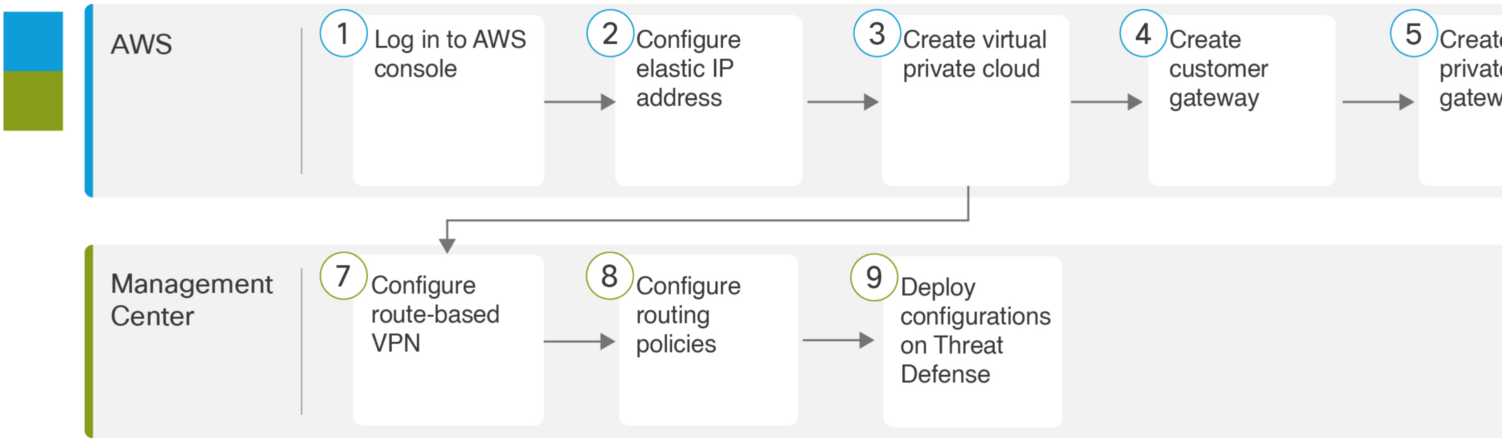
A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network. When you create a customer gateway, you provide information about your device to AWS.

Customer Gateway Device (Managed Threat Defense)

A customer gateway device is the Threat Defense device in the on-premises network of your central headquarters. You configure the device to work with the AWS site-to-site VPN connection.

End-to-End Procedure for Configuring Route-Based VPN between Management Center and AWS VPC

The following flowchart illustrates the workflow for configuring a route-based VPN between Management Center and AWS VPC.


AWS
1 Log in to AWS console
2 Configure elastic IP address
3 Create virtual private cloud
4 Create customer gateway
5 Create privat gatew
Management Center
7 Configure route-based VPN
8 Configure routing policies
9 Deploy configurations on Threat Defense

1 Configure an Elastic IP Address in AWS, on page 6
2 Configure Routing Policies in Management Center, on page 19
3 Create a Virtual Private Cloud in AWS, on page 6
4 Create a Customer Gateway in AWS, on page 9
5 Create a Virtual Private Gateway in AWS, on page 11
6 Create a VPN Connection in AWS, on page 12
7 Configure Route-Based VPN in Management Center, on page 15

Step	Description
1	Log in to AWS console.
2	Configure elastic IP address. See Configure an Elastic IP Address in AWS, on page 6.
3	Create virtual private cloud. See Create a Virtual Private Cloud in AWS, on page 6.
4	Create customer gateway. See Create a Customer Gateway in AWS, on page 9.
5	Create virtual private gateway. See Create a Virtual Private Gateway in AWS, on page 11.
6	Create AWS VPN connection. See Create a VPN Connection in AWS, on page 12.
7	Configure route-based VPN. See Configure Route-Based VPN in Management Center, on page 15.
8	Configure routing policies. See Configure Routing Policies in Management Center, on page 19.
9	Deploy configurations on Threat Defense device.

Configure an Elastic IP Address in AWS

Elastic IP address is a static public IPv4 address that is allocated to your AWS account.

Procedure

Step 1 Choose **Services** > **Networking & Content Delivery** > **VPC**.

Step 2 In the left pane, click **Elastic IPs**.

Step 3 Click **Allocate Elastic IP address**.

Step 4 Configure the following parameters in the **Allocate Elastic IP address** dialog box:

a) For **Network Border Group**, use the default value.

b) Click the **Amazon's pool of IPv4 addresses** radio button.

c) Click **Allocate**.

Create a Virtual Private Cloud in AWS

A VPC is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. When you create a VPC, AWS configures the IP address, subnets, route tables, network gateways, and security settings.

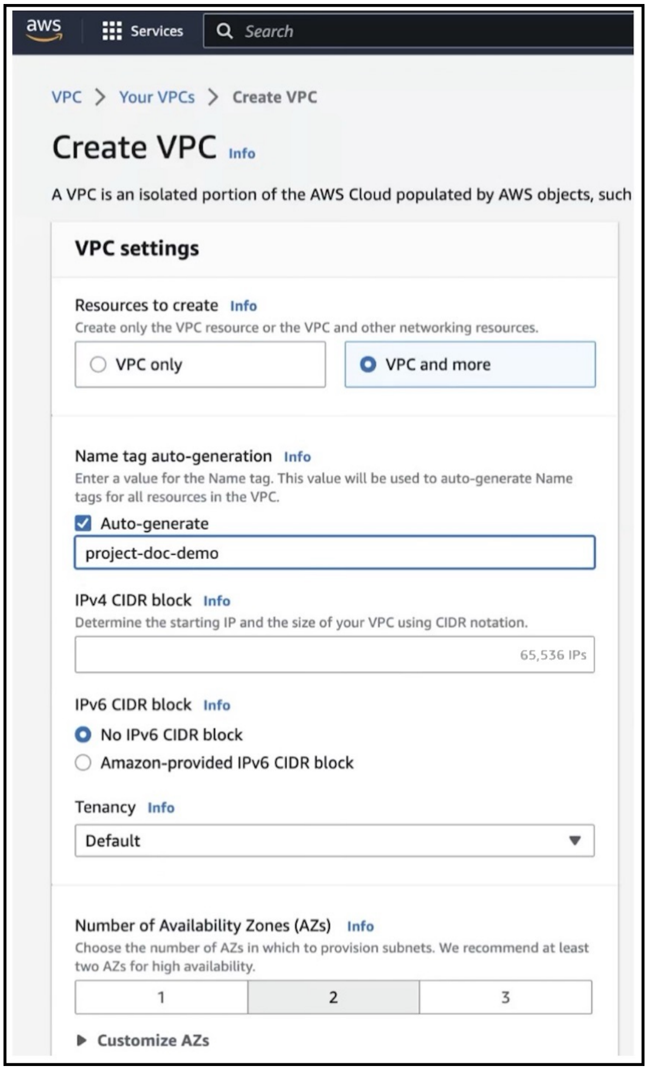
Procedure

Step 1 Choose **Services** > **Networking & Content Delivery** > **VPC**.

Step 2 In the left pane, click **VPC dashboard**.

Step 3 Click **Create VPC**.

Step 4 Configure the following parameters in the **Create VPC** dialog box:



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
project-doc-demo

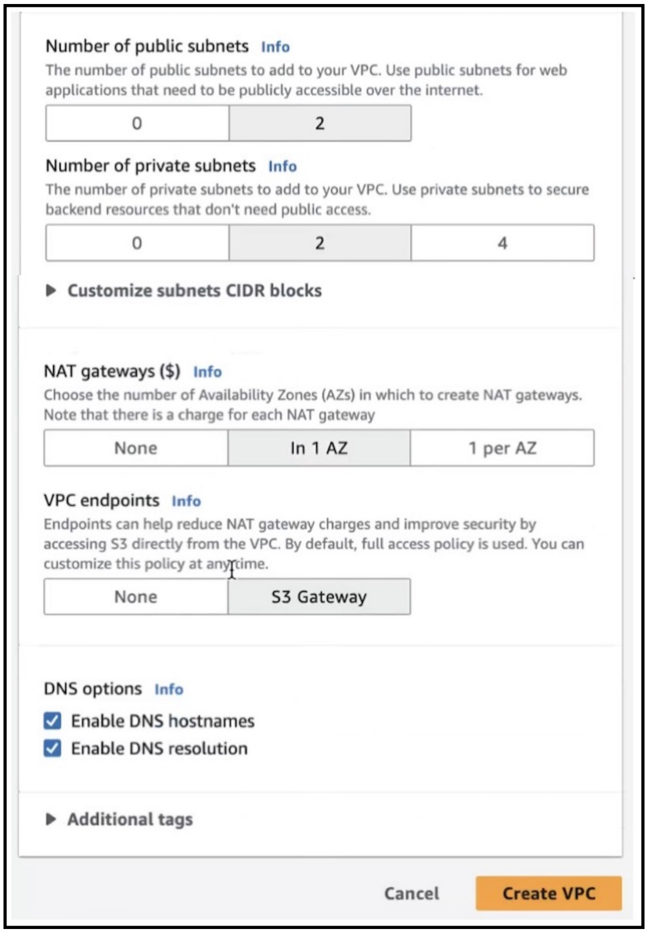
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
65,536 IPs

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default ▼

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1 | **2** | 3

▶ Customize AZs



Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 [✓ 2]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 [✓ 2] 4

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None [✓ In 1 AZ] 1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at anytime.

None [✓ S3 Gateway]

DNS options Info

☑ Enable DNS hostnames

☑ Enable DNS resolution

▶ Additional tags

Cancel Create VPC

a) Click the **VPC and more** radio button.

b) In the **Name tag** field, enter a name to identify the VPC.

c) In the **IPv4 CIDR block** field, enter an IP address.

The CIDR block size must be between /16 and /28.

d) From the **Tenancy** drop-down list, choose **Default**.

This option defines if instances that you launch into the VPC run on hardware that is shared with other AWS accounts or on hardware that is dedicated for your use only.

e) Choose **2** as the **Number of Availability Zones (AZs)** to provision subnets in at least two availability zones.

f) Choose values for **Number of public subnets** and **Number of private subnets** to configure your subnets.

g) Expand **Customize subnets CIDR blocks** to choose the IP address ranges for your subnets. You can also let AWS choose them for you.

h) (Optional) For **NAT gateways**, if resources in a private subnet need access to the public internet over IPv4, choose the number of AZs in which to create NAT gateways.

i) For **VPC endpoints**, choose **None** or**S3 Gateway**.

j) (Optional) Under **DNS options**, by default, both options are enabled by default.

k) Click **Create VPC**.

Associate a Subnet with a Route Table in AWS

You must associate each subnet in your VPC with the route table of your VPC.

Before you begin

Create a VPC in AWS.

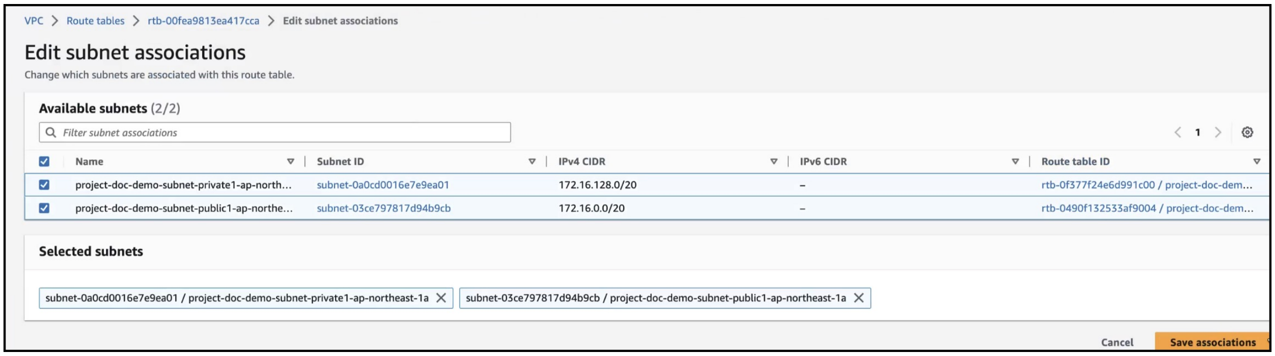
Procedure

Step 1 In the left pane, click **Route tables**.

Step 2 Select the route table assigned to your VPC.

Step 3 Click the **Subnet associations** tab.

Step 4 Click **Edit subnet associations**.



VPC > Route tables > rtb-00fea9813ea417cca > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

Filter subnet associations

☑	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	project-doc-demo-subnet-private1-ap-north...	subnet-0a0cd0016e7e9ea01	172.16.128.0/20	–	rtb-0f377f24e6d991c00 / project-doc-dem...
☑	project-doc-demo-subnet-public1-ap-northe...	subnet-03ce797817d94b9cb	172.16.0.0/20	–	rtb-0490f132533af9004 / project-doc-dem...

Selected subnets

subnet-0a0cd0016e7e9ea01 / project-doc-demo-subnet-private1-ap-northeast-1a

subnet-03ce797817d94b9cb / project-doc-demo-subnet-public1-ap-northeast-1a

Step 5 Check the private and public subnet check boxes.

Step 6 Click **Save associations**.

Create a Customer Gateway in AWS

Create a customer gateway to provide information about your device to AWS.

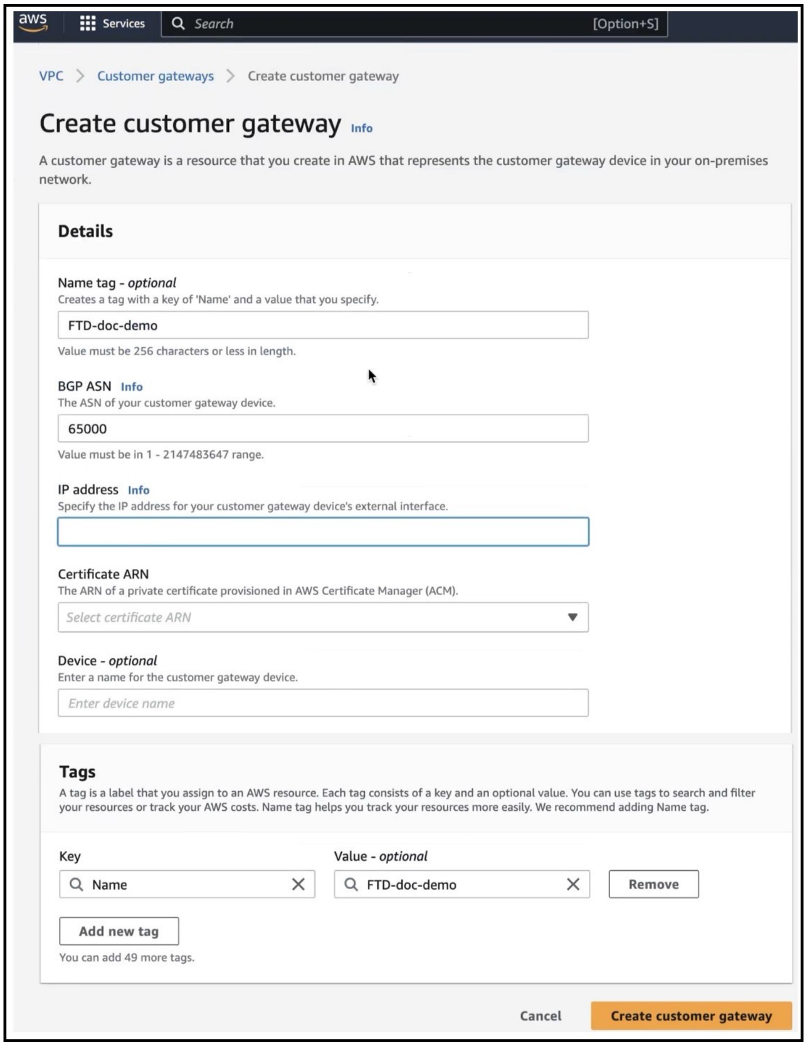
Procedure

Step 1 In the left pane, expand **Virtual Private network (VPN)**.

Step 2 Click **Customer gateways**.

Step 3 Click **Create customer gateway**.

Step 4 Configure the following parameters in the **Create customer gateway** dialog box:



Create customer gateway Info

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

Details

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
FTD-doc-demo
Value must be 256 characters or less in length.

BGP ASN Info
The ASN of your customer gateway device.
65000
Value must be in 1 - 2147483647 range.

IP address Info
Specify the IP address for your customer gateway device's external interface.

Certificate ARN
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).
Select certificate ARN

Device - *optional*
Enter a name for the customer gateway device.
Enter device name

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*
Name	FTD-doc-demo

You can add 49 more tags.

a) In the **Name tag** field, enter a name to identify the customer gateway.

b) In the **BGP ASN** field, enter the BGP Autonomous System Number (ASN) of the Threat Defense device.

The range is 1 to 2,147,483,647. In our example, the ASN is 65000. You need this ASN when you configure BGP routing in the Management Center.

c) In the **IP address** field, enter the IP address of the Threat Defense device's external interface.

The IP address must be static. If your customer gateway device is behind a NAT device, use the IP address of your NAT device.

d) (Optional) In the **Certificate ARN** field, provide the Amazon Resource Name (ARN) of an AWS Certificate Manager (ACM) private certificate for the Threat Defense device to enable certificate-based authentication.

e) (Optional) In the **Device** field, enter the name of the Threat Defense device.

f) Click **Create customer gateway**.

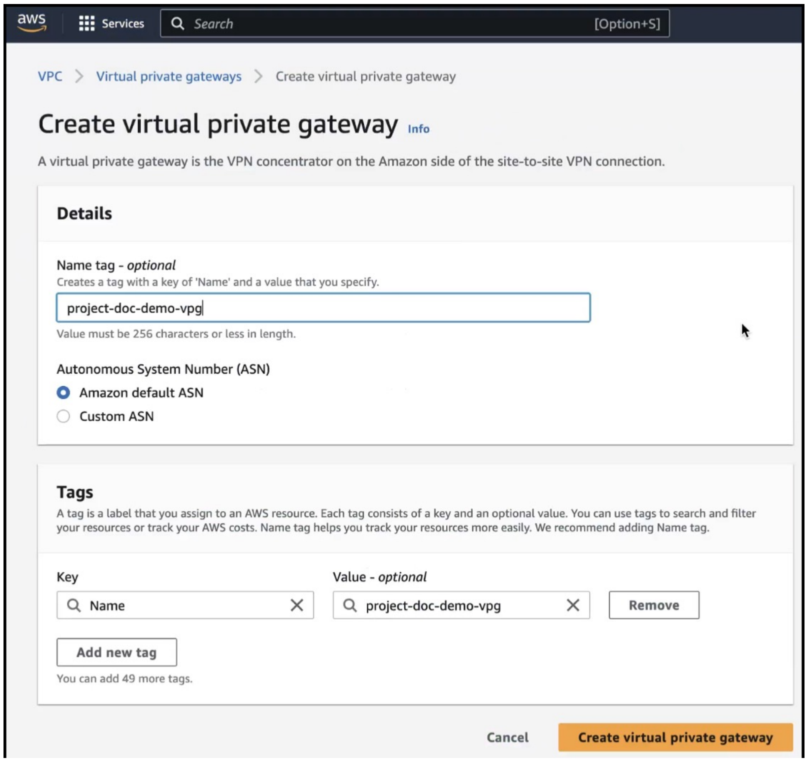
Create a Virtual Private Gateway in AWS

Procedure

Step 1 In the left pane, expand **Virtual private network (VPN)**.

Step 2 Click **Create virtual private gateway**.

Step 3 Configure the following parameters in the **Create virtual private gateway** dialog box:


aws
Services
Search
[Option+S]
VPC > Virtual private gateways > Create virtual private gateway

Create virtual private gateway Info

A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection.

Details

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

project-doc-demo-vpg

Value must be 256 characters or less in length.

Autonomous System Number (ASN)

● Amazon default ASN

○ Custom ASN

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*	
Name	project-doc-demo-vpg	Remove

Add new tag

You can add 49 more tags.

Cancel   Create virtual private gateway

a) In the **Name tag** field, enter a name for the virtual private gateway.

b) Click either the **Amazon default ASN** or the **Custom ASN** radio button.

   Note that the Amazon ASN is 64512.

c) For **Tags**, by default, the name is taken as the tag.

d) Click **Create Virtual Private Gateway**.

Attach a Virtual Private Gateway to the Virtual Private Cloud

After you create a virtual private gateway, you must attach it to the VPC.

Procedure

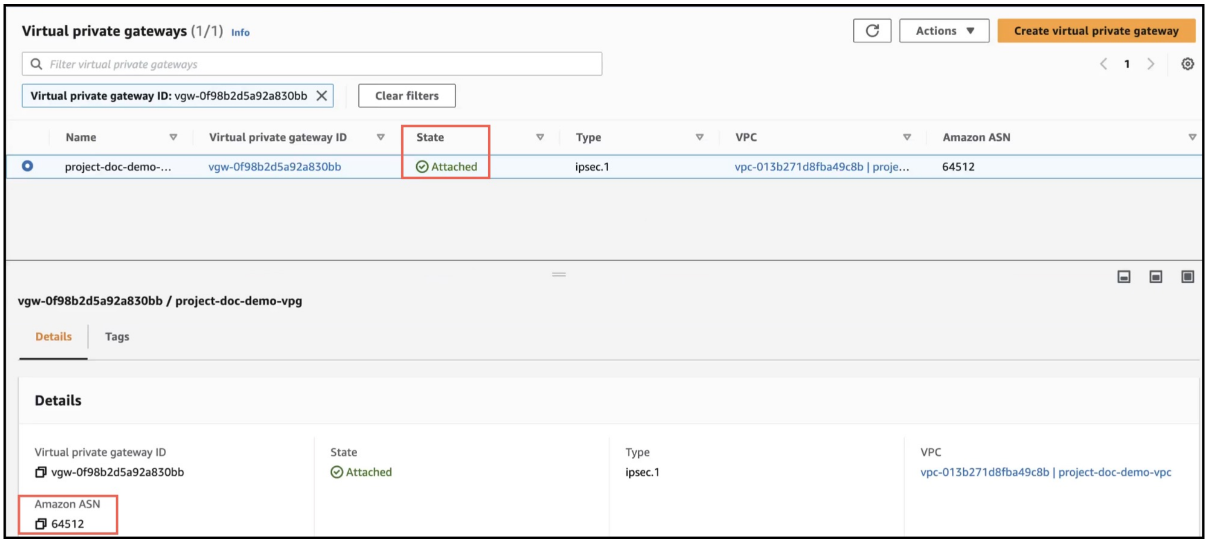
Step 1 Select the virtual private gateway that you created.

Step 2 Choose **Attach to VPC** from the **Actions** drop-down list.

Step 3 In the **Attach to VPC** dialog box, choose the VPC from the **Available VPCs** drop-down list.

Step 4 Click **Attach to VPC**.

Step 5 Verify if the **State** of the virtual private gateway is **Attached**.



Virtual private gateways (1/1) Info
Actions ▼
Create virtual private gateway
Filter virtual private gateways
Virtual private gateway ID: vgw-0f98b2d5a92a830bb ✕
Clear filters
1

	Name	Virtual private gateway ID	State	Type	VPC	Amazon ASN
●	project-doc-demo-...	vgw-0f98b2d5a92a830bb	✓ Attached	ipsec.1	vpc-013b271d8fba49c8b | proje...	64512

vgw-0f98b2d5a92a830bb / project-doc-demo-vpg

Details

Virtual private gateway ID	State	Type	VPC
vgw-0f98b2d5a92a830bb	✓ Attached	ipsec.1	vpc-013b271d8fba49c8b | project-doc-demo-vpc

Amazon ASN
64512

Create a VPN Connection in AWS

Before you begin

Ensure that you have a VPC, customer gateway, and a virtual private gateway.

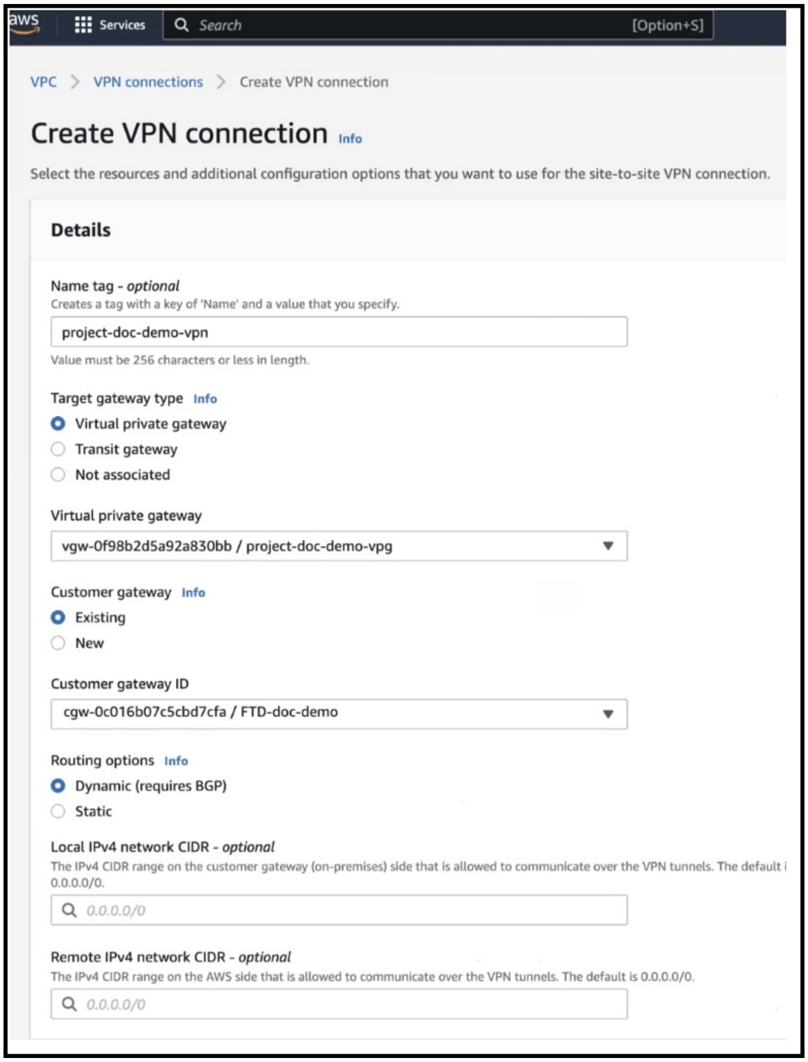
Procedure

Step 1 In the left pane, expand **Virtual private network (VPN)**.

Step 2 Click **Site-to-Site VPN connections**.

Step 3 Click **Create VPN connection**.

Step 4 Configure the following VPN parameters in the **Create VPN connection** dialog box:



VPC > VPN connections > Create VPN connection

Create VPN connection Info

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

Details

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
project-doc-demo-vpn
Value must be 256 characters or less in length.

Target gateway type Info
● Virtual private gateway
○ Transit gateway
○ Not associated

Virtual private gateway
vgw-0f98b2d5a92a830bb / project-doc-demo-vpg

Customer gateway Info
● Existing
○ New

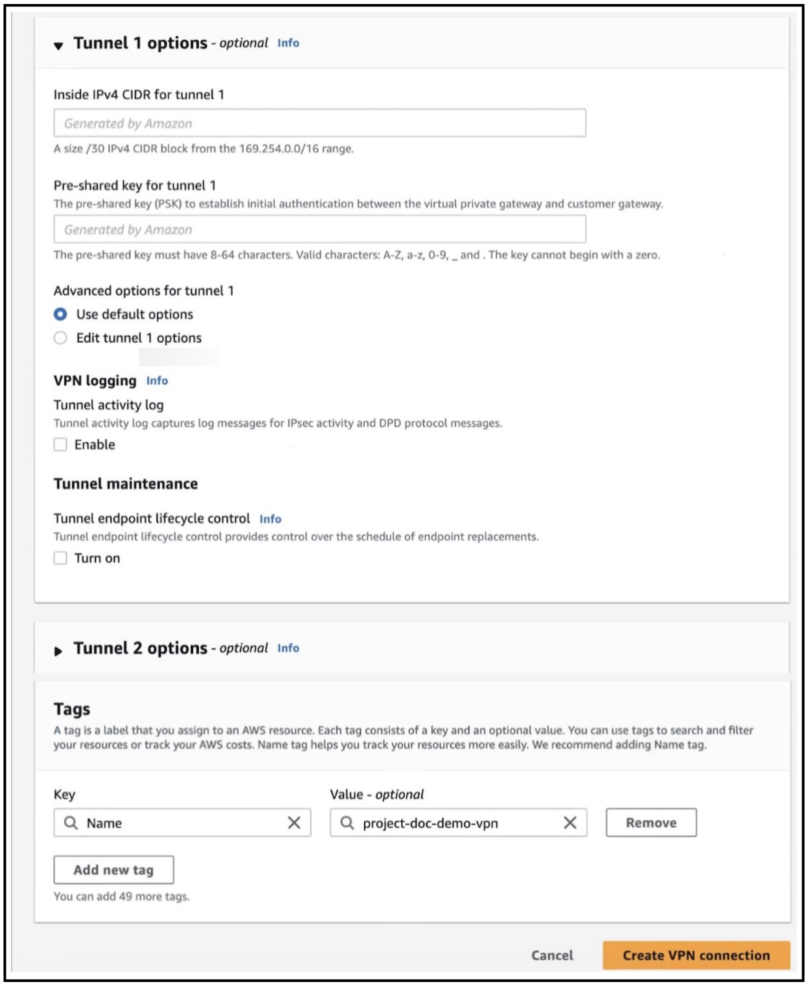
Customer gateway ID
cgw-0c016b07c5cbd7cfa / FTD-doc-demo

Routing options Info
● Dynamic (requires BGP)
○ Static

Local IPv4 network CIDR - *optional*
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default i
0.0.0.0/0.
0.0.0.0/0

Remote IPv4 network CIDR - *optional*
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.
0.0.0.0/0

a) In the **Name tag** field, enter a name for the VPN connection.
b) For **Target gateway type**, click the **Virtual private gateway** radio button.
c) Choose a virtual private gateway from the **Virtual private gateway** drop-down list.
d) For **Customer gateway**, click the **Existing** radio button and choose a customer gateway from the **Customer gateway ID** drop-down list.
e) For **Routing options**, click the **Dynamic (requires BGP)** radio button.
f) (Optional) For **Local IPv4 network CIDR**, enter the IP address of the protected network of the Threat Defense device or use the default value of 0.0.0.0/0.
g) (Optional) For **Remote IPv4 network CIDR**, enter the IP address of the AWS side network or use the default value of 0.0.0.0/0.
h) Expand **Tunnel 1 options** to configure the VPN tunnel parameters:



▾ **Tunnel 1 options** - *optional* Info

Inside IPv4 CIDR for tunnel 1

Generated by Amazon

A size /30 IPv4 CIDR block from the 169.254.0.0/16 range.

Pre-shared key for tunnel 1

The pre-shared key (PSK) to establish initial authentication between the virtual private gateway and customer gateway.

Generated by Amazon

The pre-shared key must have 8-64 characters. Valid characters: A-Z, a-z, 0-9, _ and . The key cannot begin with a zero.

Advanced options for tunnel 1

● Use default options

○ Edit tunnel 1 options

VPN logging Info

Tunnel activity log

Tunnel activity log captures log messages for IPsec activity and DPD protocol messages.

□ Enable

Tunnel maintenance

Tunnel endpoint lifecycle control Info

Tunnel endpoint lifecycle control provides control over the schedule of endpoint replacements.

□ Turn on

▸ **Tunnel 2 options** - *optional* Info

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*	
Name	project-doc-demo-vpn	Remove

Add new tag

You can add 49 more tags.

1. For **Inside IPv4 CIDR for tunnel 1**, AWS generates an IPv4 address.
2. In the **Pre-shared key for tunnel 1** field, enter a pre-shared key (PSK) for authentication between the virtual private gateway and the customer gateway. If you do not specify a PSK, AWS generates a PSK.

   You need this PSK to configure the VPN in the Management Center.
3. For **Advanced options for tunnel 1**, click the **Use default options** radio button.

i) (Optional) Expand **Tunnel 2 options** to configure the backup VPN tunnel parameters.

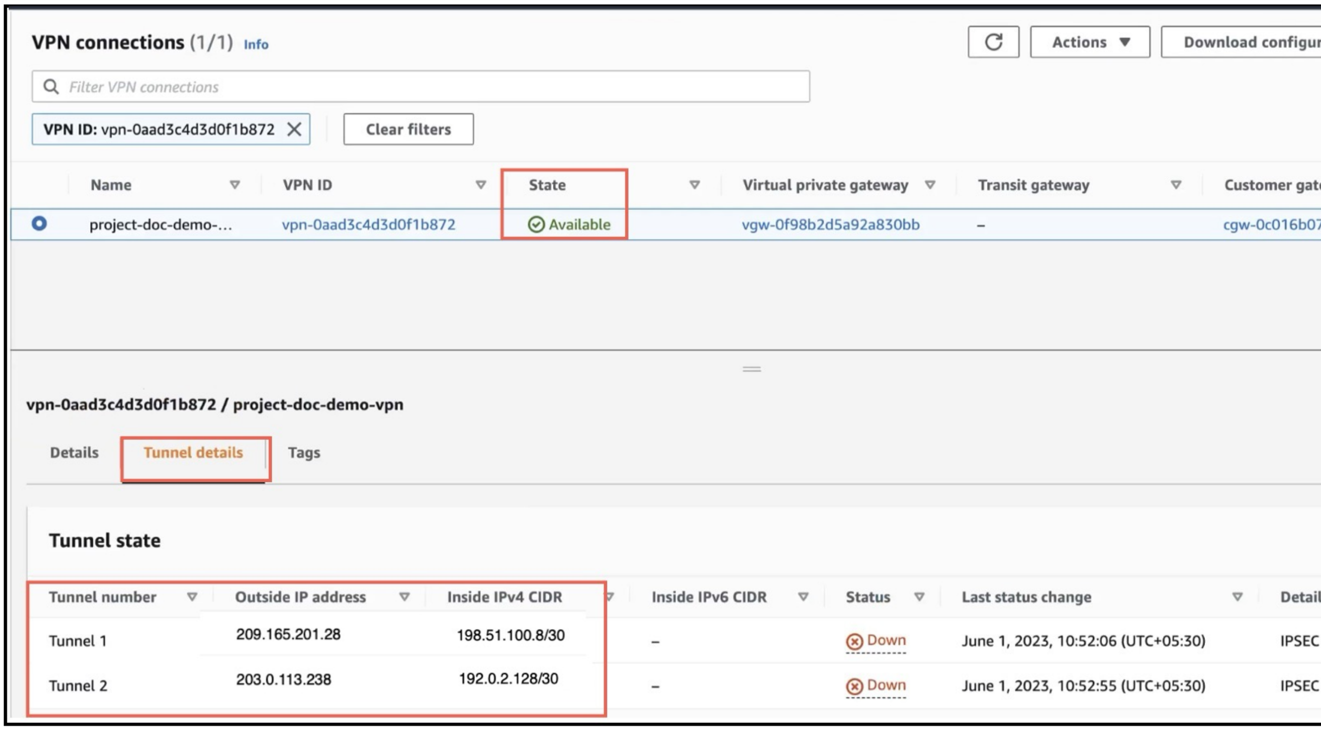
Note Ensure that you use the same PSK for both the tunnels.

Step 5 Click **Create VPN connection**.

After the VPN connection is created, the **State** changes from **Pending** to **Available**.

a) Select the VPN connection that you created to view the details.

b) Click the **Tunnel details** tab.



Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gat
project-doc-demo-...	vpn-0aad3c4d3d0f1b872	Available	vgw-0f98b2d5a92a830bb	–	cgw-0c016b07

vpn-0aad3c4d3d0f1b872 / project-doc-demo-vpn

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Detail
Tunnel 1	209.165.201.28	198.51.100.8/30	–	Down	June 1, 2023, 10:52:06 (UTC+05:30)	IPSEC
Tunnel 2	203.0.113.238	192.0.2.128/30	–	Down	June 1, 2023, 10:52:55 (UTC+05:30)	IPSEC

In the above example, note the following details:

Tunnel	Outside (Extranet) IP Address	AWS VTI IP Address	Threat Defense Device VTI IP Address
Tunnel 1	209.165.201.28	198.51.100.9/30	198.51.100.10/30
Tunnel 2	203.0.113.238	192.0.2.129/30	192.0.2.130/30

You need the above details when you configure the route-based VPN in the Management Center.

Configure Route-Based VPN in Management Center

Before you begin

Ensure that you note the inside and outside IP addresses of the VPN tunnel in AWS.

Procedure

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

Step 2 Click + **Site To Site VPN**.

Step 3 In the **Topology Name** field, enter a name for the VPN topology.

Step 4 Click the **Route Based (VTI)** radio button.

Step 5 Click the **Point to Point** tab.

Step 6 Check the **IKEv2** check box.

Step 7 Click the **Endpoints** tab.

Step 8 For **Node A**, configure the following parameters:

a) Choose a Threat Defense device from the **Device** drop-down list.

b) Choose a Static Virtual Tunnel Interface (SVTI) of the Threat Defense device from the **Virtual Tunnel Interface** drop-down list or click + to create an SVTI.

For more information about creating an SVTI, see Create a Static VTI for a Threat Defense Device in the Management Center, on page 17.

c) (Optional) Click **+ Add Backup VTI** to configure a backup VTI and configure the required parameters.

The **Tunnel Source** is the same for both the VTI tunnels. In our example, the backup VTI IP address is 192.0.2.130/30. See the IP address table in Create a VPN Connection in AWS, on page 12.

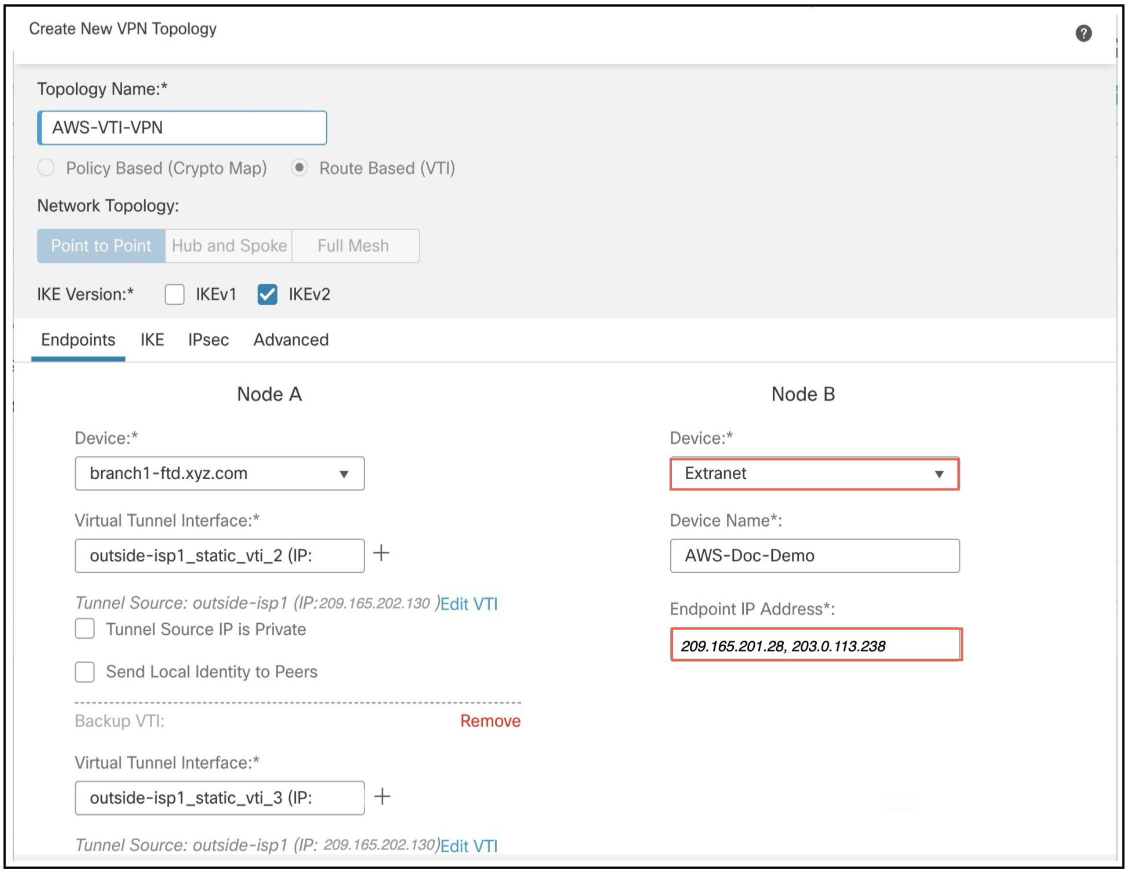
Step 9 For **Node B**, configure the following parameters:

a) From the **Device** drop-down list, choose **Extranet**.

b) In the **Device Name** field, enter the name of the extranet device.

c) In the **Endpoint IP Address** field, enter the IP addresses of the AWS VPN.

In our example, the IP address is 209.165.201.28 and 203.0.113.238.



Create New VPN Topology

Topology Name:* AWS-VTI-VPN

○ Policy Based (Crypto Map) ● Route Based (VTI)

Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Endpoints | IKE | IPsec | Advanced

Node A

Device:* branch1-ftd.xyz.com

Virtual Tunnel Interface:* outside-isp1_static_vti_2 (IP: +

*Tunnel Source: outside-isp1 (IP:209.165.202.130)*Edit VTI

□ Tunnel Source IP is Private

□ Send Local Identity to Peers

Backup VTI: Remove

Virtual Tunnel Interface:* outside-isp1_static_vti_3 (IP: +

*Tunnel Source: outside-isp1 (IP: 209.165.202.130)*Edit VTI

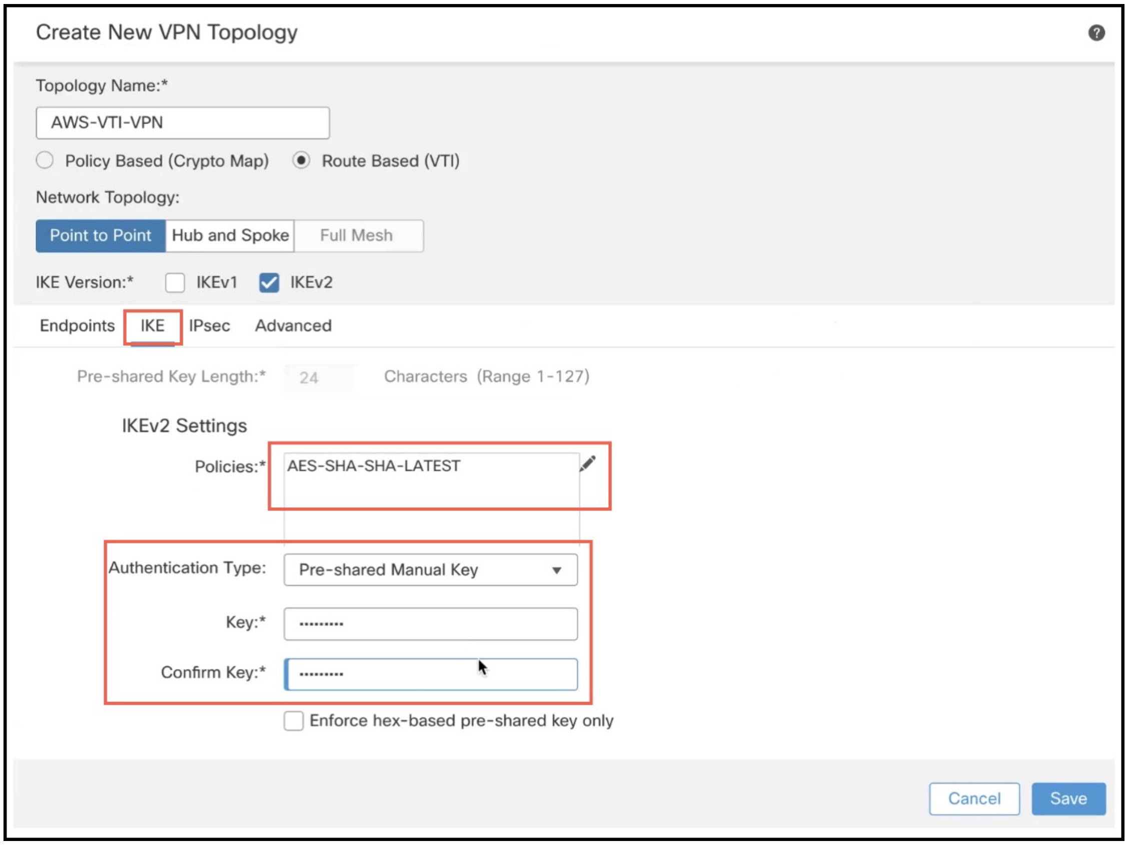
Node B

Device:* Extranet

Device Name*: AWS-Doc-Demo

Endpoint IP Address*: 209.165.201.28, 203.0.113.238

Step 10 Click the **IKE** tab to configure the following parameters:



Create New VPN Topology

Topology Name:* AWS-VTI-VPN

○ Policy Based (Crypto Map) ● Route Based (VTI)

Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Endpoints | IKE | IPsec | Advanced

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policies:* AES-SHA-SHA-LATEST

Authentication Type: Pre-shared Manual Key

Key:* ••••••••••

Confirm Key:* ••••••••••

□ Enforce hex-based pre-shared key only

a) For **IKEv2 Settings**, click the edit icon adjacent to **Policies** and choose **AES-SHA-SHA-LATEST** from the drop-down list. This protocol is the default IKE protocol of the AWS VPN.

b) From the **Authentication Type**drop-down list, choose **Pre-shared Manual Key**.

c) Enter a key in the **Key** and **Confirm Key** fields.

In our example, use the PSK that you configured in the AWS VPN.

Step 11 For **IPsec** and **Advanced** configuration, use the default values.

Step 12 Click **Save**.

You can view the topology in the **Site-to-Site VPN Summary** page (**Devices** > **Site To Site VPN**). After you deploy the configurations to all the devices, you can see the status of all the tunnels in this page.

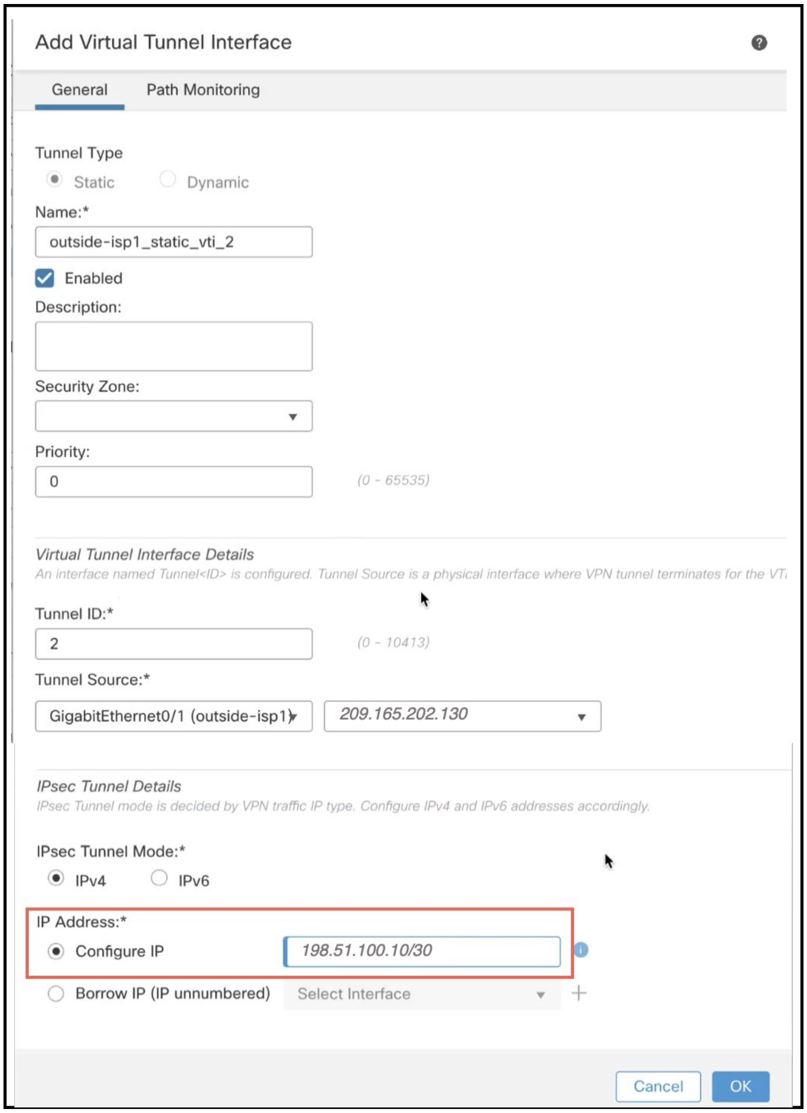
Create a Static VTI for a Threat Defense Device in the Management Center

Before you begin

Configure the basic parameters for a route-based point-to-point VPN topology as described in Configure Route-Based VPN in Management Center, on page 15, click the **Endpoints** tab, and choose a Threat Defense device from the **Device** drop-down list as **Node A**.

Procedure

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



Add Virtual Tunnel Interface

Tunnel Type

● Static ○ Dynamic

Name:* outside-isp1_static_vti_2

☑ Enabled

Description:

Security Zone:

Priority: 0 (0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VT

Tunnel ID:* 2 (0 - 10413)

Tunnel Source:* GigabitEthernet0/1 (outside-isp1) 209.165.202.130

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

● IPv4 ○ IPv6

IP Address:*

● Configure IP 198.51.100.10/30

○ Borrow IP (IP unnumbered) Select Interface

a) In the **Name** field, enter a name for the SVTI.

b) Check the **Enabled** check box.

c) (Optional) From the **Security Zone** drop-down list, choose a security zone for the static VTI.

d) In the **Priority** field, enter the priority for load-balancing the traffic across multiple VTIs.

   The range is from 0 to 65535. The lowest number has the highest priority.

e) In the **Tunnel ID** field, enter a unique tunnel ID.

   The range is from 0 to 10413.

f) From the **Tunnel Source** drop-down list, choose the tunnel source interface.

g) For **IPSec Tunnel Mode**, click the **IPv4** radio button to specify the traffic type over the IPsec tunnel.

h) In the **Configure IP** field, enter the IP address of the SVTI.

In our example, the SVTI IP address is 198.51.100.10/30. See the IP address table in Create a VPN Connection in AWS, on page 12.

i) Click **OK**.

Configure Routing Policies in Management Center

Configure an Underlay Routing Policy in the Management Center

To enable traffic to and from the AWS, you must configure an underlay routing policy. You can configure a static route or any dynamic routing protocol. In our example, we use a static route.

Procedure

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

Step 2 Click the edit icon adjacent to the interface that you want to edit.

Step 3 Click the **Routing** tab.

Step 4 In the left pane, click **Static Route** to configure a static route.

Step 5 Click **+Add Route**.

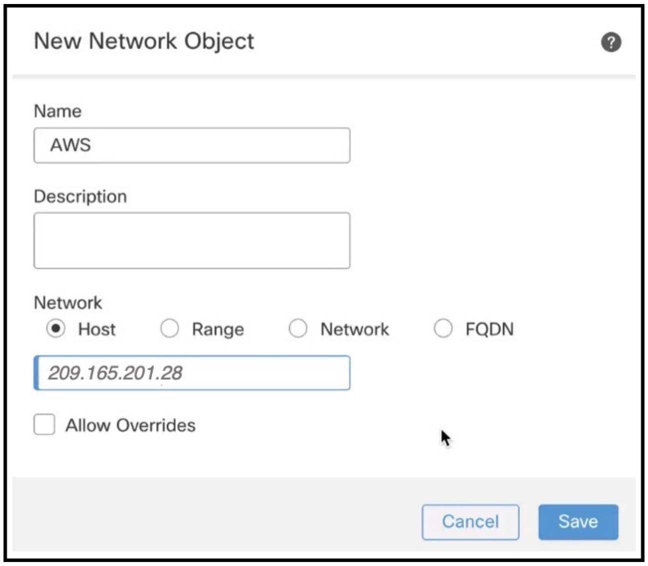
Step 6 Configure the following parameters in the **Add Static Route Configuration** dialog box:

a) Click the **IPv4** radio button.

b) From the **Interface** drop-down list, choose the outside interface of the Threat Defense device.

c) For **Available Network**, click **+** to create a network object for the AWS network.

d) Configure the following parameters in the **New Network Object** dialog box:



New Network Object

Name: AWS

Description:

Network: ● Host ○ Range ○ Network ○ FQDN

209.165.201.28

□ Allow Overrides

1. In the **Name** field, enter a name for the AWS network.

2. Click the **Host** radio button and enter the IP address of the AWS network.

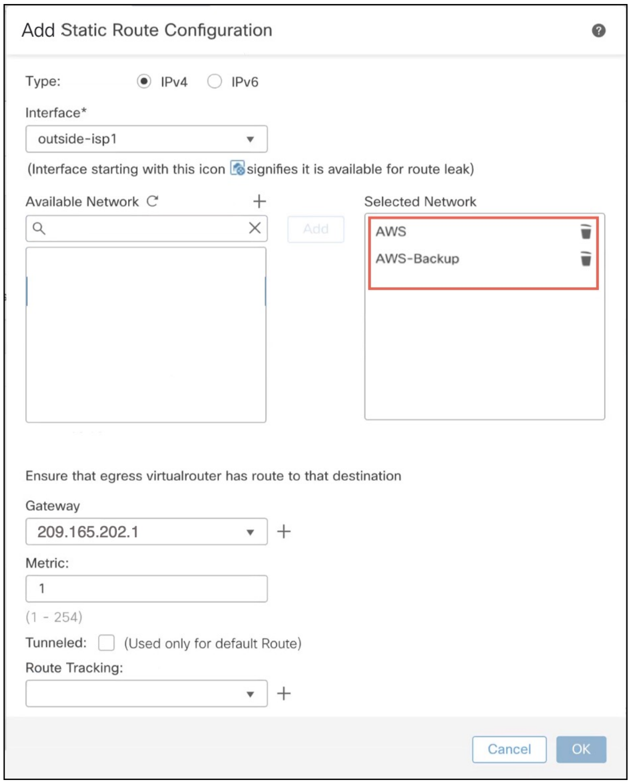
   In our example, the IP address of the AWS network is 209.165.201.28.

3. Click **Save**.

e) Repeat Step 6c to Step 6d to create a network object for the backup AWS network.

In our example, the IP address of the backup AWS network is 203.0.113.238.

f) Choose the AWS network and the backup AWS network from the **Available Network** list, and click **Add** to move it to the **Selected Network** list.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside-isp1

(Interface starting with this icon signifies it is available for route leak)

Available Network

Selected Network: AWS, AWS-Backup

Ensure that egress virtualrouter has route to that destination

Gateway: 209.165.202.1

Metric: 1

(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

g) In the **Gateway** field, enter the IP address of the Threat Defense device's gateway.

h) Click **OK**.

Configure an Overlay Routing Policy in the Management Center

You must configure an overlay routing policy for the VPN traffic. In our example, we configure a BGP routing policy.

Procedure

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

Step 2 Click the edit icon adjacent to the interface that you want to edit.

Step 3 Click the **Routing** tab.

Step 4 In the left pane, click **BGP** under **General Settings**.

Step 5 Check the **Enable BGP** check box.

Step 6 In the **AS Number** field, enter the AS number of the Threat Defense device that you configured for the AWS customer gateway.

In our example, it is 65000.

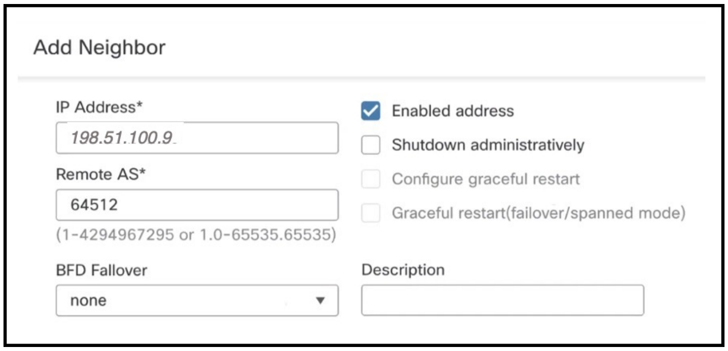
Step 7 Click **Save**.

Step 8 In the left pane, choose **BGP** > **IPv4**.

Step 9 Check the **Enable IPv4** check box.

Step 10 Click the **Neighbor** tab and click **+Add**.

Step 11 Configure the following parameters in the **Add Neighbor** dialog box:



Add Neighbor

IP Address*: 198.51.100.9

Remote AS*: 64512 (1-4294967295 or 1.0-65535.65535)

BFD Fallover: none

☑ Enabled address

□ Shutdown administratively

□ Configure graceful restart

□ Graceful restart(failover/spanned mode)

Description:

a) In the **IP Address** field, enter the AWS VTI IP address (Tunnel1) from the AWS VPN configuration.

In our example, the AWS IP address is 198.51.100.9.

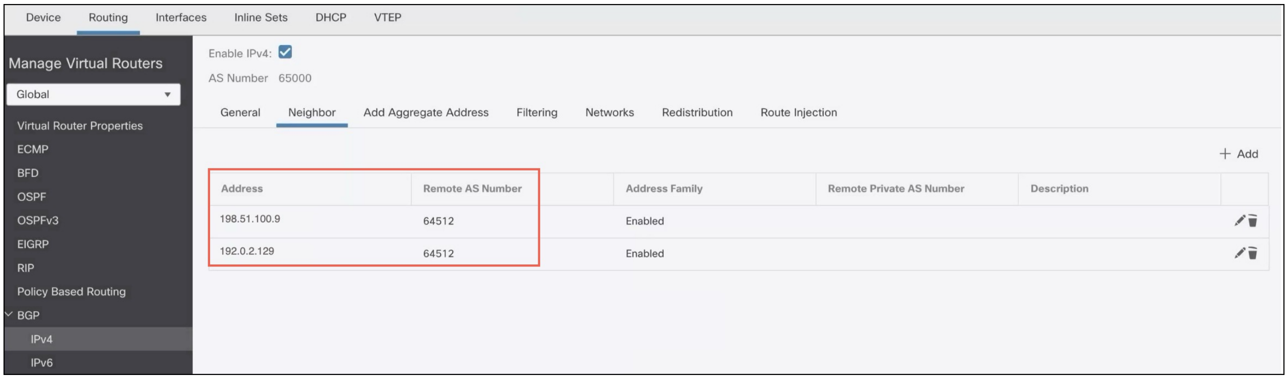
b) In the **Remote AS** field, enter the AWS AS number from the AWS VPN configuration.

In our example, the AWS AS number is 64512.

c) Click **OK**.

Step 12 Repeat Step 11a to Step 11c to add the backup AWS IP address (Tunnel2) as the neighbor.

In our example, the IP address is 192.0.2.129 and the AWS AS number is 64512.



Enable IPv4: ☑

AS Number 65000

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
198.51.100.9	64512	Enabled		
192.0.2.129	64512	Enabled		

Step 13 Click **Save**.

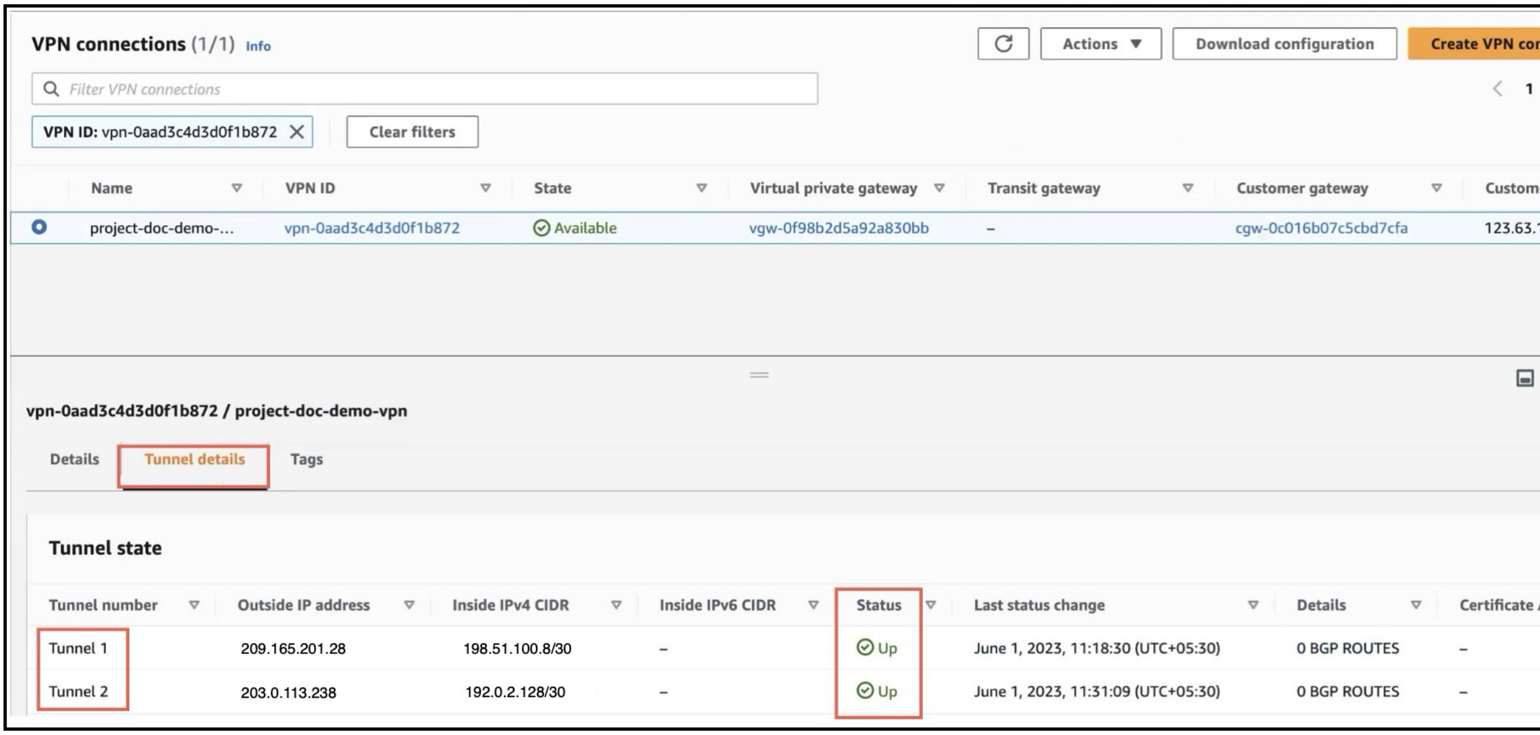
Verify the VTI Tunnel Statuses and Configurations

After deploying the configurations on the Threat Defense device, you can verify the VTI tunnel configuration and status on the device, the Management Center, and AWS.

Verify Tunnel Statuses in AWS

To verify the VPN tunnels in AWS:

1. Choose **Virtual private network (VPN) > Site-to-Site VPN connections**.
2. Click the radio button adjacent to the VPN.
3. Click the **Tunnel details** tab. The **Status** of the tunnels should be **Up**.



	Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Custom
●	project-doc-demo-...	vpn-0aad3c4d3d0f1b872	✓ Available	vgw-0f98b2d5a92a830bb	–	cgw-0c016b07c5cbd7cfa	123.63.1

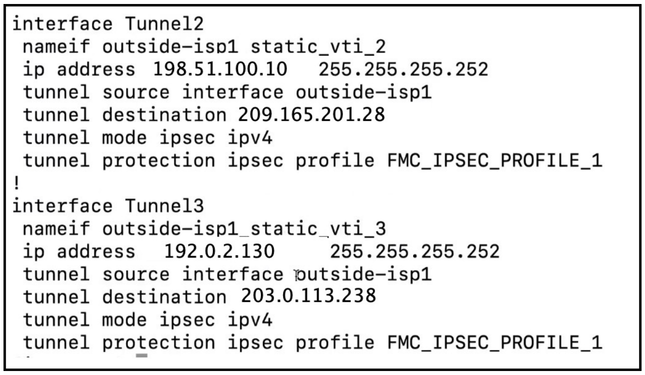
vpn-0aad3c4d3d0f1b872 / project-doc-demo-vpn

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate A
Tunnel 1	209.165.201.28	198.51.100.8/30	–	✓ Up	June 1, 2023, 11:18:30 (UTC+05:30)	0 BGP ROUTES	–
Tunnel 2	203.0.113.238	192.0.2.128/30	–	✓ Up	June 1, 2023, 11:31:09 (UTC+05:30)	0 BGP ROUTES	–

Verify Tunnel and Routing Configuration on the Threat Defense Device

- To verify the interface configuration on the Threat Defense device, use the **show running-config interface** command.

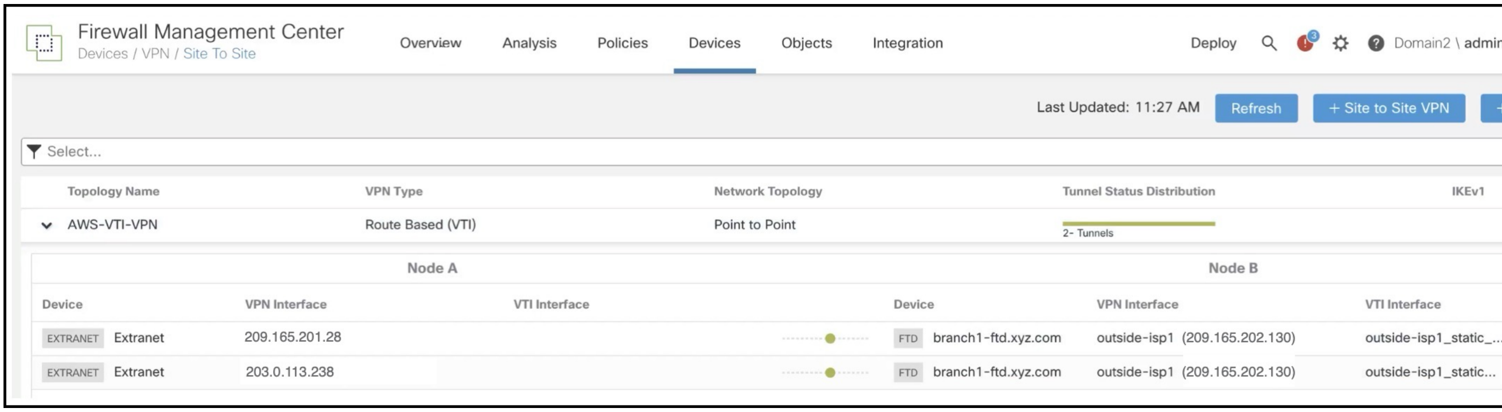


```
interface Tunnel2
 nameif outside-isp1 static_vti_2
 ip address 198.51.100.10   255.255.255.252
 tunnel source interface outside-isp1
 tunnel destination 209.165.201.28
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
!
interface Tunnel3
 nameif outside-isp1_static_vti_3
 ip address  192.0.2.130     255.255.255.252
 tunnel source interface outside-isp1
 tunnel destination 203.0.113.238
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

- To verify the BGP configuration of the Threat Defense device, use the **show bgp** command.

Verify Tunnel Status in Site-to-Site VPN Summary Page

To verify the status of the VPN tunnels, choose **Device** > **VPN** > **Site To Site**.



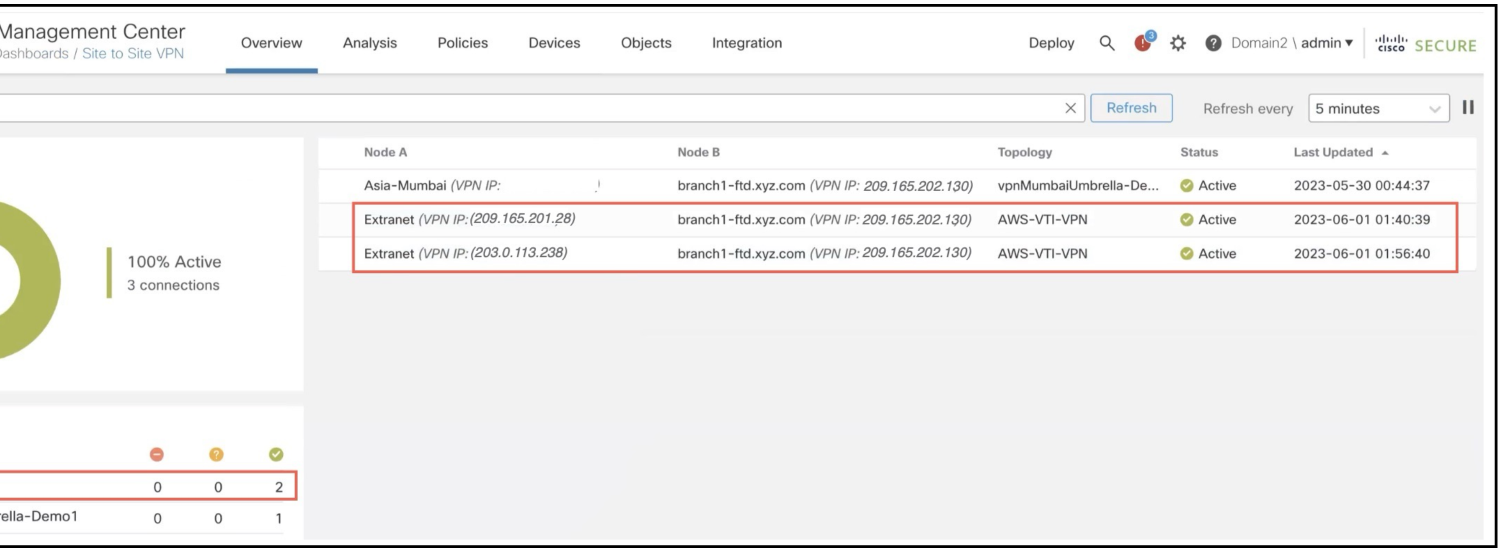
Last Updated: 11:27 AM

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1
AWS-VTI-VPN	Route Based (VTI)	Point to Point	2- Tunnels	

Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet	209.165.201.28		FTD branch1-ftd.xyz.com	outside-isp1 (209.165.202.130)	outside-isp1_static_...
EXTRANET Extranet	203.0.113.238		FTD branch1-ftd.xyz.com	outside-isp1 (209.165.202.130)	outside-isp1_static...

Verify Tunnel Status in Site-to-Site VPN Dashboard

To view details of the VPN tunnel, choose **Overview** > **Dashboards** > **Site to Site**



Node A	Node B	Topology	Status	Last Updated ▲
Asia-Mumbai *(VPN IP:*	branch1-ftd.xyz.com *(VPN IP: 209.165.202.130)*	vpnMumbaiUmbrella-De...	✓ Active	2023-05-30 00:44:37
Extranet *(VPN IP: (209.165.201.28)*	branch1-ftd.xyz.com *(VPN IP: 209.165.202.130)*	AWS-VTI-VPN	✓ Active	2023-06-01 01:40:39
Extranet *(VPN IP: (203.0.113.238)*	branch1-ftd.xyz.com *(VPN IP: 209.165.202.130)*	AWS-VTI-VPN	✓ Active	2023-06-01 01:56:40

100% Active
3 connections

	⊖	?	✓
	0	0	2
rella-Demo1	0	0	1

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.