



Set Up SD-WAN Branch Office with Dual ISPs Using Serial Numbers and Device Template

In this chapter, we show you how to set up your SD-WAN branch office with dual ISPs using device serial numbers and device templates. The use case details the scenario, network topology, best practices, and prerequisites. It also provides a comprehensive end-to-end procedure for seamless implementation.

- [Overview of SD-WAN Wizard and Device Templates, on page 1](#)
- [Is this Guide for You?, on page 2](#)
- [Sample Scenario, on page 2](#)
- [System Requirements, on page 2](#)
- [Prerequisites for SD-WAN Wizard and Device Templates, on page 2](#)
- [Guidelines and Limitations for SD-WAN Wizard and Device Templates, on page 3](#)
- [Network Topology Depicting Dual ISP with Hubs and Spokes, on page 3](#)
- [Workflow for Setting Up SD-WAN Branch Office with Dual ISPs Using Serial Number and Device Templates, on page 6](#)
- [Validate and Monitor Tunnel Statuses and Configurations of SD-WAN Topologies, on page 22](#)
- [Troubleshoot Device Templates and SD-WAN Topologies, on page 23](#)

Overview of SD-WAN Wizard and Device Templates

Onboarding multiple devices on a branch network and establishing a secure network infrastructure that connects these branches to the central headquarters is challenging. Manually configuring and deploying these devices within an SD-WAN topology is time-intensive and error-prone, potentially leading to inconsistencies in network settings and security vulnerabilities across different locations.

You can mitigate these issues by using the Cisco Secure Firewall Management Center (subsequently referred to as management center) and Cisco Secure Firewall Threat Defense (subsequently referred to as threat defense devices) devices. The Secure Firewall solution streamlines the deployment of secure branch networks with the new SD-WAN VPN wizard and device templates, which are available in management center Version 7.6.

The SD-WAN VPN wizard simplifies the configuration of VPN tunnels between your centralized headquarters and remote branch sites. It automates the VPN and routing setup for your SD-WAN overlay network.

Device templates facilitate the deployment of multiple branch devices with preprovisioned initial configurations. Using these templates, you can easily configure SD-WAN VPN connections and seamlessly add spokes to your SD-WAN topologies.

Is this Guide for You?

This guide is designed for network administrators responsible for onboarding branch office devices using their serial numbers with the Management Center. It provides detailed instructions for deploying these devices with preprovisioned configurations in a dual ISP SD-WAN topology.

Sample Scenario

Alex, a network administrator for an enterprise with multiple branch offices across various cities, wants to onboard several devices to a branch network with preconfigured settings and establish a secure network infrastructure that connects these branches to the central headquarters. Alex decides to use the new SD-WAN wizard and device templates in the management center. These new features streamline the process by providing centralized control, ensuring uniform configurations, and enabling efficient provisioning and scalability across the corporate network.

System Requirements

The following table displays the platforms and versions for this use case.

Product	Version	Version Used in This Document
Cisco Secure Firewall Management Center (formerly Firepower Management Center [FMC])	7.6 and later	7.6
Cisco Secure Firewall Threat Defense (formerly Firepower Threat Defense [FTD])	<ul style="list-style-type: none"> For hubs, Version 7.6.0 and later, and for spokes, Version 7.4.1 and later of the following models: <ul style="list-style-type: none"> Firepower 1000 Series Firepower 2100 Series Secure Firewall 3100 Series Secure Firewall 1200 Series 	Cisco Secure Firewall 1210CE Version 7.6

Prerequisites for SD-WAN Wizard and Device Templates

- [Prerequisites for Using the SD-WAN Wizard](#)
- [Requirements and Prerequisites for Device Management using Device Templates](#)
- [Licenses for Device Management using Device Templates](#)

Guidelines and Limitations for SD-WAN Wizard and Device Templates

- [Guidelines and Limitations for Using SD-WAN Wizard](#)
- [Guidelines and Limitations for Device Management using Device Templates](#)

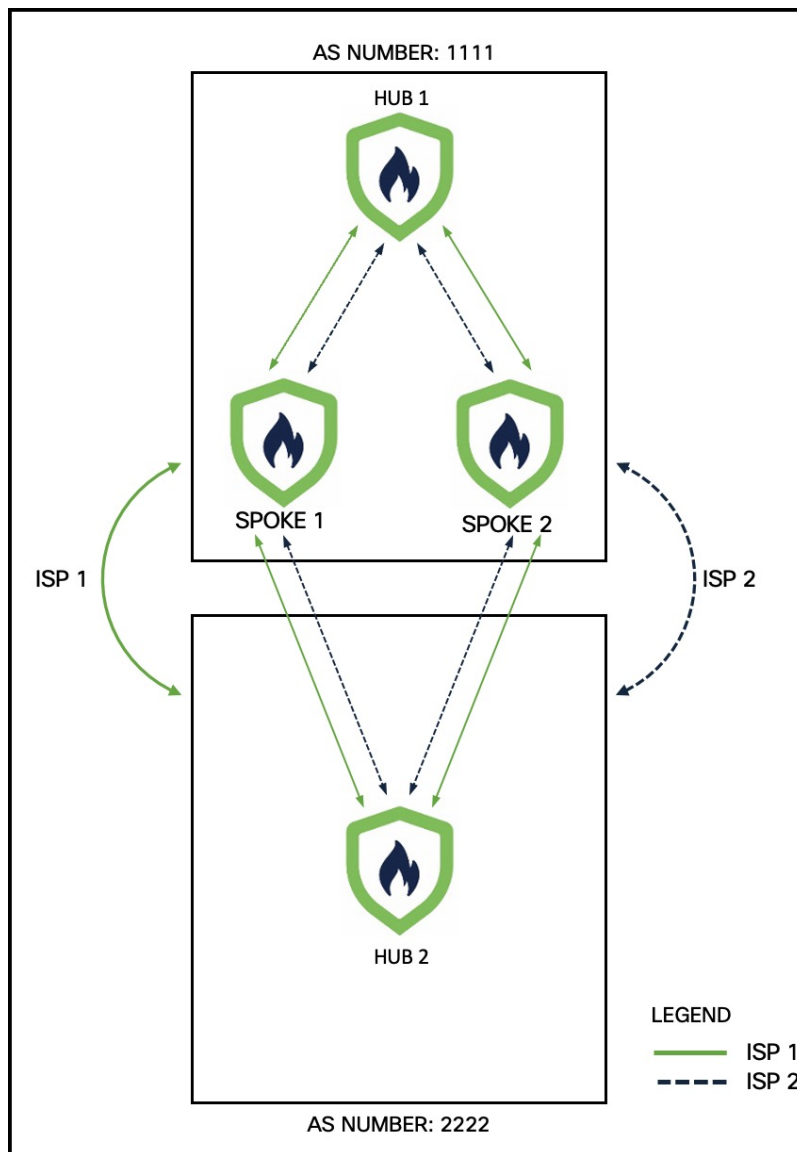
Network Topology Depicting Dual ISP with Hubs and Spokes

In the following sample dual-ISP topology, the hubs are in different regions. The hubs and spokes use External Border Gateway Protocol (eBGP) as the routing protocol to exchange routing information.

- Hub 1 is a Threat Defense hub device in a branch office with autonomous system (AS) number as 1111.
- Hub 2 is a Threat Defense hub device in a branch office with AS number as 2222.
- Spoke 1 and Spoke 2 are Threat Defense spoke devices in the branch with AS number as 1111.
- outside-isp1 is the VPN interface of each spoke to ISP 1.
- outside-isp2 is the VPN interface of each spoke to ISP 2.

Alex aims to onboard a Cisco Secure Firewall 1210CE Threat Defense device into an existing dual-ISP SD-WAN topology using the device's serial number and the preconfigured settings. Utilizing the new intuitive SD-WAN VPN wizard and device templates, he can efficiently create SD-WAN VPN topologies and streamline the onboarding process for the device in the SD-WAN topology. In our example, this device is Spoke 3.

Figure 1: Dual ISP Topology with Hubs in Different Regions



The topology has the following parameters:

Table 1: IP Addresses of Hubs and Spokes

Device	Management IP Address	Inside Interface	Outside Interface
Hub1	209.165.200.225	198.51.100.17/28	<ul style="list-style-type: none"> ISP1: 192.0.2.17/28 ISP2: 192.0.2.33/28

Device	Management IP Address	Inside Interface	Outside Interface
Hub2	209.165.200.226	198.51.100.33/28	<ul style="list-style-type: none"> • ISP1: 192.0.2.18/28 • ISP2: 192.0.2.34/28
Spoke 1	209.165.200.227	198.51.100.65/28	<ul style="list-style-type: none"> • ISP1: 192.0.2.19/28 • ISP2: 192.0.2.35/28
Spoke 2	209.165.200.228	198.51.100.129/28	<ul style="list-style-type: none"> • ISP1: 192.0.2.20/28 • ISP2: 192.0.2.36/28

Table 2: Loopback IP Addresses and IP Address Pools of Hubs

Device	Hub Loopback IP Addresses	IP Address Pools
Hub1	<ul style="list-style-type: none"> • Loopback1: 209.165.201.1 (Mask: 255.255.255.224) • Loopback2: 209.165.201.65 (Mask: 255.255.255.224) 	<ul style="list-style-type: none"> • IP_pool1_hub1: 209.165.201.2-209.165.201.30 (Mask: 255.255.255.224) • IP_pool2_hub1: 209.165.201.66-209.165.201.94
Hub2	<ul style="list-style-type: none"> • Loopback1: 209.165.201.33 (Mask: 255.255.255.224) • Loopback2: 209.165.201.97 (Mask: 255.255.255.224) 	<ul style="list-style-type: none"> • IP_pool1_hub2: 209.165.201.34-209.165.201.62 (Mask: 255.255.255.224) • IP_pool2_hub2: 209.165.201.98-209.165.201.126

Note that when you configure the hub IP address pools, ensure that you do not check the **Allow Overrides** check box in the **Add IPv4/IPv6 Pool** dialog box (**Objects > Object Management > Address Pools**). You can also create these address pools in the SD-WAN wizard.

Add IPv4 Pool

Name*

Description

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

☐ Allow Overrides

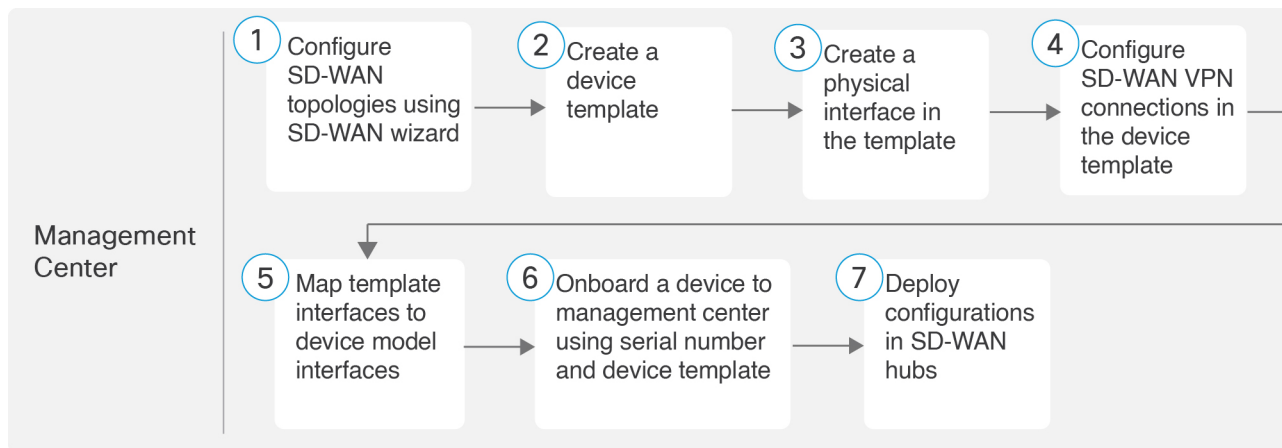
?

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

[Cancel](#) [Save](#)

Workflow for Setting Up SD-WAN Branch Office with Dual ISPs Using Serial Number and Device Templates

The following flowchart illustrates the workflow for setting up an SD-WAN branch office with dual ISPs using serial number and device templates.



Step	Task	More Information
1	Configure SD-WAN topologies using SD-WAN wizard.	Configure SD-WAN

Step	Task	More Information
		Topologies Using the SD-WAN Wizard, on page 7
2	Create a device template.	Create a Device Template
3	Create a physical interface in the template.	Add a Physical Interface in the Template
4	Configure SD-WAN VPN connections in the device template.	Configure an SD-WAN VPN Connection in a Device Template
5	Map template interfaces to device model interfaces.	Map Template Interfaces to Device Model Interfaces, on page 15
6	Onboard a device to management center using serial number and device template.	Onboard a Device to Management Center Using a Serial Number and Device Template, on page 17
7	Deploy configurations in SD-WAN hubs.	-

Configure SD-WAN Topologies Using the SD-WAN Wizard

The SD-WAN wizard allows you to easily configure VPN tunnels between your centralized headquarters and remote branch sites. Using this wizard, for each spoke, you can use only one WAN interface per SD-WAN topology. However, for dual-ISP setups, you can configure a second SD-WAN topology with the second WAN interface.

This example describes how to configure two SD-WAN topologies:

- SDWAN-VPN1 with outside-isp1 as the spoke's VPN interface for ISP1
- SDWAN-VPN2 with outside-isp2 as the spoke's VPN interface for ISP2

Before you begin

Ensure that you review [Prerequisites for SD-WAN Wizard and Device Templates](#) and [Guidelines and Limitations for SD-WAN Wizard and Device Templates](#).

Procedure

Step 1 Choose **Devices > Site To Site**, and click **Add**.

Step 2 In the **Topology Name** field, enter **SDWAN-VPN1** as the name for the SD-WAN VPN topology.

Step 3 Click the **SD-WAN Topology** radio button and click **Create**.

Step 4 Configure a hub:

- a) Click **Add Hub**.
- b) From the **Device** drop-down list, choose a hub.
- c) Click + next to the **Dynamic Virtual Tunnel Interface (DVTI)** drop-down list to add a dynamic VTI for the hub.

The **Add Virtual Tunnel Interface** dialog box is prepopulated with default configurations. However, you must configure the following parameters:

1. From the **Tunnel Source** drop-down list, choose the physical interface that is the source of the dynamic VTI. Choose the IP address of this interface from the adjacent drop-down list.
2. From the **Borrow IP** drop-down list, choose a loopback interface. The dynamic VTI inherits this IP address.
 - For SDWAN-VPN1: For Hub1, we use Loopback1 (209.165.201.1) as the Borrow IP address.
 - For SDWAN-VPN2: For Hub1, we use Loopback2 (209.165.201.65) as the Borrow IP address.

For more information about the loopback IP addresses of the hubs, see [Table 2: Loopback IP Addresses and IP Address Pools of Hubs, on page 5](#).

- d) Click **OK**.
- e) In the **Hub Gateway IP Address** field, enter the public IP address of the hub's VPN interface or the tunnel source of the dynamic VTI to which the spokes connect.

This IP address is auto populated if the interface has a static IP address. If hub is behind a NAT device, you must manually configure the post-NAT IP address.

- For SDWAN-VPN1: For Hub1, the Hub Gateway IP Address is 192.0.2.17.
- For SDWAN-VPN2: For Hub1, the Hub Gateway IP Address is 192.0.2.33.

For more information about the IP addresses of the hubs and spokes, see [Table 1: IP Addresses of Hubs and Spokes, on page 4](#).

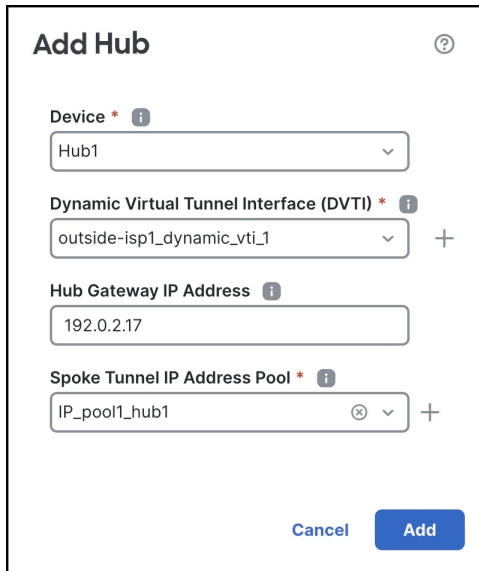
- f) From the **Spoke Tunnel IP Address Pool** drop-down list, choose an IP address pool or click + to create an address pool.

When you add spokes, the wizard auto generates spoke tunnel interfaces, and assigns IP addresses to these spoke interfaces from this IP address pool.

Note

Ensure that you do not check the **Allow Overrides** check box when you create an address pool in the **Add IP Pool** dialog box.

- g) Click **Add** to save the hub configuration.



Add Hub

Device * *i*
Hub1

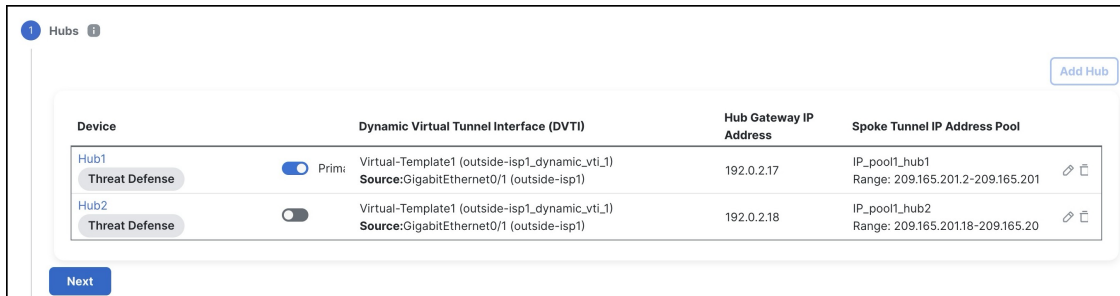
Dynamic Virtual Tunnel Interface (DVTI) * *i*
outside-isp1_dynamic_vti_1 +

Hub Gateway IP Address *i*
192.0.2.17

Spoke Tunnel IP Address Pool * *i*
IP_pool1_hub1 +

Cancel Add

- h) To add the secondary hub, repeat Step 4a to Step 4g.



Hubs *i* Add Hub

Device		Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
Hub1	<input checked="" type="checkbox"/> Threat Defense	Virtual-Template1 (outside-isp1_dynamic_vti_1) Source: GigabitEthernet0/1 (outside-isp1)	192.0.2.17	IP_pool1_hub1 Range: 209.165.201.2-209.165.201
Hub2	<input type="checkbox"/> Threat Defense	Virtual-Template1 (outside-isp1_dynamic_vti_1) Source: GigabitEthernet0/1 (outside-isp1)	192.0.2.18	IP_pool1_hub2 Range: 209.165.201.18-209.165.20

Next

- i) Click **Next**.

Step 5

To configure spokes, click **Add Spokes (Bulk Addition)**.

In the **Add Bulk Spokes** dialog box, configure the following parameters:

- Choose Spoke1 and Spoke2 from the **Available Devices** list and click **Add** to move the devices to **Selected Devices**.
- Use one of the following methods to select the VPN interfaces of the spokes:
 - Click the **Interface Name Pattern** radio button and specify a string to match the logical name of the internet or WAN interface of the spokes, for example, outside*, wan*. In our example, the string for the ISP1 interface is outside-isp1.

Note

If the spoke has multiple interfaces with the same pattern, the first interface that matches the pattern is selected for the topology.

- Click the **Security Zone** radio button and choose a security zone with the VPN interfaces of the spokes from the drop-down list, or click + to create a security zone.

- c. Click **Next**.

The wizard validates if the spokes have interfaces with the specified pattern. Only the validated devices are added to the topology.

- d. Click **Add**.

- e. Click **Next**.

For each spoke, the wizard automatically selects the hub's DVTI as the tunnel destination IP address.

Note

If the hub's tunnel source IP address is an IPv6 address, the wizard automatically selects the first IPv6 address of the spokes' selected interface. To edit the IPv6 address of a spoke's tunnel source, click the edit icon next to a spoke, choose an IPv6 address from the **IP Address** drop-down list, and click **Save**.

Step 6 Configure **Authentication Settings** for the devices in the SD-WAN topology:

You can use the default settings and proceed to [Step 7](#). If required, you can edit the settings later. In this example, we use pre-shared manual key for device authentication.

- a) From the **Authentication Type** drop-down list, choose a manual pre-shared key, an auto-generated pre-shared key, or a certificate for device authentication.
 - **Pre-shared Manual Key**—Specify the pre-shared key for the VPN connection.
 - **Pre-shared Automatic Key**—(Default value) The wizard automatically defines the pre-shared key for the VPN connection. Specify the key length in the **Pre-shared Key Length** field. The range is 1 to 127.
 - **Certificate**—When you use certificates as the authentication method, the peers obtain digital certificates from a CA server in your PKI infrastructure, and use them to authenticate each other.
- b) Choose one or more algorithms from the **Transform Sets** drop-down list.
- c) Choose one or more algorithms from the **IKEv2 Policies** drop-down list.

d) Click **Next**.

Step 7

Configure the **SD-WAN Settings**.

This step involves the auto generation of spoke tunnel interfaces, and BGP configuration of the overlay network.

- From the **Spoke Tunnel Interface Security Zone** drop-down list, choose a security zone or click + to create a security zone to which the wizard automatically adds the spokes' auto-generated Static Virtual Tunnel Interfaces (SVTIs).
- Check the **Enable BGP on the VPN Overlay Topology** check box to automate BGP configurations such as neighbor configurations between the overlay tunnel interfaces and basic route redistribution from the directly connected LAN interfaces of the hubs and spokes.
- In the **Autonomous System Number** field, enter an Autonomous System (AS) number.

AS number is a unique number for a network with a single routing policy. BGP uses AS numbers to identify networks. The spoke's BGP neighbor configuration is generated based on the corresponding hub's AS number. Range is from 0 to 65536.

- If all the hubs and spokes are in the same region, by default, **64512** is the AS number.
- If the primary and secondary hubs are in different regions, the primary hub and its spokes are configured with **64512** as the AS number, and the secondary hub is configured with a different AS number.

In our example, Hub1 and the spokes are in the same region with AS number as 1111. Hub2 is in a different region with AS number as 2222.

- In the **Community Tag for Local Routes** field, enter the BGP community attribute to tag the connected and redistributed local routes. This attribute enables easy route filtering. Make a note of this community string; you must use the same community string for the second SD-WAN VPN topology. In our example, this tag is 1.
- Check the **Redistribute Connected Interfaces** check box and choose an interface group from the drop-down list, or click + to create an interface group with connected inside or LAN interfaces for BGP route redistribution in the overlay topology.
- Check the **Secondary Hub is in different Autonomous System** check box. This check box is displayed only if you have a secondary hub in this topology.
- In the **Autonomous System Number** field, enter the AS number for the secondary hub. In our example, Hub2 is in a different region with AS number as 2222.
- In the **Community Tag for Learned Routes** field, enter the BGP community attribute to tag the routes learned from other SD-WAN peers over the VPN tunnel. This attribute is required only for eBGP configuration when the secondary hub has a different AS number. This field appears only if you have configured two hubs in the SD-WAN topology. Make a note of this community string, you must use the same community string for the second SD-WAN VPN topology. In our example, this tag is 2.
- Check the **Enable Multiple Paths for BGP** check box to allow multiple BGP routes to be used at the same time to reach the same destination. This option enables BGP to load-balance traffic across multiple links.

4 SD-WAN Settings

Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs. [View more](#)

Spoke Tunnel Interface Security Zone ⓘ

SZ-ISP1 ⓘ + ✎

Overlay Routing Configuration

BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ Enable BGP on the VPN Overlay Topology

Autonomous System Number * ⓘ

1111

Community Tag for Local Routes * ⓘ

1

☒ Redistribute Connected Interfaces ⓘ

Default inside* ⓘ +

☒ Secondary Hub is in different Autonomous System ⓘ

Autonomous System Number *

2222

Community Tag for Learned Routes * ⓘ

2

☒ Enable Multiple Paths for BGP

Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

Next You have unsaved changes

j) Click **Next**.

Step 8 Click **Finish** to save and validate the SD-WAN topology.

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.

Step 9 Repeat Step 1 to Step 8 to configure the SDWAN-VPN2 topology with the VPN interface for ISP2: outside-isp2.

What to do next

Configure a point-to-point route-based VPN topology between the two hubs using the route-based VPN wizard to ensure direct communication between these networks. For more information, see [Configure a Policy-based Site-to-Site VPN](#).

Create a Device Template

Before you begin

You must be an admin user to create a device template.

Procedure

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

Step 2 Click **Add Device Template**.

In the **Add Device Template** dialog box, configure the following parameters:

- In the **Name** field, enter the name for the template.
- (Optional) In the **Description** field, enter a description for the template.
- From the **Access Control Policy** drop-down list, choose an access control policy.

Step 3 Click **OK**.

Add a Physical Interface in the Template

By default, a device template enables the device to come up with the following physical interfaces:

- Management interface
- Inside interface
- Outside interface

For this dual ISP use case, we need two outside interfaces. To create a physical interface:

Procedure

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

Step 2 Click the edit icon of the template in which you want to add the physical interface.

Step 3 In the **Interfaces** tab, click **Add Physical Interface**.

Step 4 Choose a **Slot** and **Port Index** number from the drop-down list.

Step 5 Click **Create Interface**.

The screenshot shows a dialog box titled "Create Physical Interface" with a help icon. It contains three input fields: "Hardware Name" with the value "Ethernet", "Slot" with a dropdown menu showing "1", and "Port Index" with a dropdown menu showing "3". At the bottom, there are two buttons: "Cancel" and "Create Interface".

You can rename the outside interfaces of the device template. In this example, these interfaces are outside-isp1 and outside-isp2.

Configure an SD-WAN VPN Connection in a Device Template

You must configure an SD-WAN VPN connection to add spokes to SD-WAN topologies using the device template.

Before you begin

- Configure a minimum of one SD-WAN topology (**Devices > VPN > Site To Site**).
- Ensure that you review [Prerequisites for SD-WAN Wizard and Device Templates](#) and [Guidelines and Limitations for SD-WAN Wizard and Device Templates](#).

Procedure

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

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

Step 3 Click the **VPN** tab.

Step 4 Click **Add VPN Connection**.

Step 5 Choose an SD-WAN topology from the **VPN Topology** drop-down list.

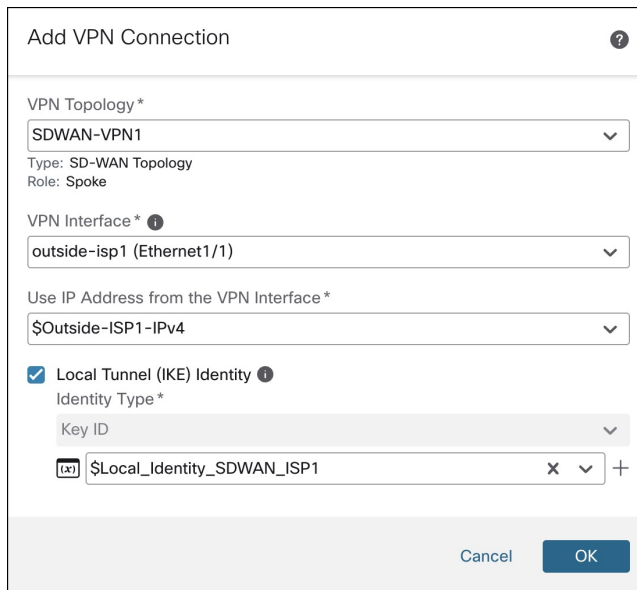
The **Add VPN Connection** dialog box expands and you can configure the following parameters:

- From the **VPN Interface** drop-down list, choose a WAN-facing or internet-facing physical interface to establish a VPN connection with the hub.

This list contains all the interfaces configured in the device template. In this example, the VPN interface is outside-isp1.

- Use IP Address from the VPN Interface**—This drop-down list is auto populated with the IP address variable. For IPv6 address, choose an IPv6 address from the drop-down list.
- Check the **Local Tunnel (IKE) Identity** check box to enable a unique and configurable identity for the VPN tunnel from the spoke to a remote peer.
- Identity Type**—Key ID is the only supported identity type. Choose a key ID variable from the drop-down list or click + to create a new key ID variable.

e) Click **OK**.



The 'Add VPN Connection' dialog box contains the following fields and options:

- VPN Topology ***: Dropdown menu with 'SDWAN-VPN1' selected.
- Type**: SD-WAN Topology
- Role**: Spoke
- VPN Interface ***: Dropdown menu with 'outside-isp1 (Ethernet1/1)' selected.
- Use IP Address from the VPN Interface ***: Dropdown menu with '\$Outside-ISP1-IPv4' selected.
- ☒ **Local Tunnel (IKE) Identity**
- Identity Type ***: Dropdown menu with 'Key ID' selected.
- Key ID**: Text field with '\$Local_Identity_SDWAN_ISP1' and a dropdown arrow.
- Buttons**: 'Cancel' and 'OK' buttons at the bottom right.

You can view the VPN connection in the **Site-to-Site VPN Connections** table.

Step 6 Click **Save**.

Step 7 Repeat Step 4 to Step 6 to configure another SD-WAN VPN connection using the second outside interface.

In this example, the second outside interface is outside-isp2, and there are two SD-WAN VPN connections:

- SDWAN-VPN1 with outside-isp1 as the VPN interface
- SDWAN-VPN2 with outside-isp2 as the VPN interface

SDWAN_Branch_Template		
Template for Cisco Firepower Threat Defense		
Interfaces	Inline Sets	Routing
DHCP	VPN	Template Settings
Site-to-Site VPN Connections		
VPN Topology	VPN Connections	Traffic Matching Criteria
SDWAN-VPN1 Type: SD-WAN Topology Role: Spoke	VPN Interface: outside-isp1 Local Tunnel IKE ID: \$Local_Identi...	Routing
SDWAN-VPN2 Type: SD-WAN Topology Role: Spoke	VPN Interface: outside-isp2 Local Tunnel IKE ID: \$Local_Identi...	Routing

Map Template Interfaces to Device Model Interfaces

For each model, you can specify which template interface corresponds to which model interface. You can map a template to one or more models as long as the interface configurations are valid for all the mapped

models. For example, if the template includes switch ports and VLAN interfaces, then that template can only be applied to a Firepower 1010.

Procedure

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

Step 2 Click **Add Model Mapping** for the template in which you want to create the model mapping. Alternatively, you can click the edit icon of the template and choose **Template Settings > Model Mapping**.

Step 3 Choose the **Device Model** from the drop-down list.

In this example, we choose a Cisco Firepower 1010 Threat Defense device.

Step 4 Map the template interfaces to the device model interfaces by choosing the interface from the **Model Interface** drop-down list.

Note

Click **Clear Mapping** to remove the defined model mapping. Click **Reset Mappings** for default interface mapping in which the mapping is done based on the slot and port index order of the interface names.

Step 5 Click **Save**.

Note

Some configurations in the template may not be supported on all device models. Unsupported configurations, if any, are not applied to the device. The **Device Template Apply** Report provides details about such configurations.

Add Model Mapping ?

i Map the template-defined interfaces for each device model that you want to apply this template to.

Device Model *

Cisco Secure Firewall 1210CE Threat Defense ▼

⚠ If you are applying the template on a high-availability device, ensure that you reserve an interface for failover and another for state link.

[Clear Mappings](#)
[Reset Mappings **i**](#)

Template Interface	Template Interface Name	Model Interface
Ethernet1/1	outside	Ethernet1/1 ⊗ ▼
Ethernet1/2	inside	Ethernet1/2 ⊗ ▼

[Cancel](#)
[Save](#)

Onboard a Device to Management Center Using a Serial Number and Device Template

Zero-Touch Provisioning lets you register devices to the management center using serial number without any initial setup on the device. You can use a template to add a device, register the device with the management center and bring up the device with template configurations. You can register up to 25 devices at a time. For serial number registration, define all variables and overrides in a CSV file that you upload.

Before you begin

- Before you add a device using a serial number, you must integrate the management center with Cisco Security Cloud.

CDO onboards the on-prem management center after you integrate it with Cisco Security Cloud. CDO needs the management center in its inventory for zero-touch provisioning to operate. However, you do not need to use CDO directly. If you do use CDO, its management center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the management center, and cross-launching the management center.

1. Choose **Integration > Cisco Security Cloud**.

2. Click **Enable Cisco Security Cloud** to open a separate browser tab to log you into your Cisco Security Cloud account and confirm the displayed code. If you have multiple tenants, choose the tenant to which the management center must be onboarded.

3. Check the **Enable Zero-Touch Provisioning** check box.

If required, review and enable other options such as Policy Analyzer and Optimizer, Cisco XDR Automation, Cisco Security Cloud Support, and Cisco AI Assistant for Security.

4. Click **Save**.

- Ensure that the device is unconfigured or a fresh install. Zero-Touch Provisioning is meant for new devices only. Pre-configuration can disable zero-touch provisioning, depending on how you configure the device.
- Cable either the outside interface or the management interface of the device so it can reach the internet.
 - If you use the outside interface for zero-touch provisioning, do not cable the management interface. The IP address of the outside interface must be from DHCP.
 - If you use the management interface, configure a DHCP or static IP address. You can also configure a public IP address or FQDN for the management center if the device does not have a public IP address or FQDN. This configuration allows the device to initiate the management connection (**System > Configuration > Manager Remote Access**).
- Ensure that the management center is registered to the Smart Software Manager. A valid evaluation license is sufficient, but if it expires, you will not be able to add new devices until you successfully register.
- Create a device template. You must specify any required variables and network-object overrides for each device and ensure that model mapping is done for the target device model.

We recommend that you create a checklist to ensure that all configurations in the template have been entered correctly before applying the template on the device.

The following is a sample checklist:

- Check version, model, operation modes.
- Check list of variables and overrides.
- Check sanity of variable and override values.
- Check the model mappings.
- Check if parallel device template operations are in progress.



Note

If you are adding a device that will be managed by a data interface, ensure that you configure the template to be compatible with the connectivity parameters of the device. For more information, see [Configure a Template for Threat Defense Devices Managed Through the Data Interface](#).

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Click **Add > Device (Wizard)**.
- Step 3** In **Device registration method**, click **Serial Number** and click **Next**.

Add Device (Wizard)

1 Device registration method

Registration Key
Register device using registration key

Serial Number
Register one or more devices using the serial number (zero-touch provisioning)

Next

- Step 4** In **Initial device configuration**:

Add Device (Wizard)

1 Device registration method
Device registration method **Serial Number**

2 Initial device configuration

Choose initial device configuration method

☐ Basic ☒ **Device template**

Preconfigure settings using a template. A template is applied on a device after registration only if the device model and version support template application. If not, the template is not applied, and the initial deployment is skipped. For more information, see the [Online Help](#).

Device template *
SD-WAN_Branch_Template

Access control policy : sdwan-acl

Device models supported for the selected template
Firepower 1010E Threat Defense

This template requires devices to be managed using the Management interface. Ensure that the device's connection to Management Center is from the Management interface.

Previous Next

- Click the **Device template** radio button.
- From the **Device template** drop-down list, choose a device template for the device, and click **Next**.

- Step 5** In **Device details**:

- Download **SampleTemplate.csv**. This file includes parameters that must be defined for each device. For more information on the CSV template file parameters, see [CSV Template File](#).
- Drag & drop** your CSV template file or click **Browse** to select the CSV template file that you want to upload. A validation check is done on the file after you upload it.

After the CSV template file has been uploaded successfully, the content of the CSV template file is displayed in a table format.

Onboard a Device to Management Center Using a Serial Number and Device Template

See the following sample CSV template file containing parameters for onboarding the Cisco Firepower 1120 Threat Defense device.

```
DisplayName,SerialNumber,AdminPassword,$Local_Identity1_SDWAN_ISP1,$Local_Identity2_SDWAN_ISP2,$Local_Identity3_SDWAN_ISP1,$Local_Identity4_SDWAN_ISP2,Outside-isp1-ip4,Outside-isp2-ip4
Spoke3,FJC282917RQ,*****,,SDWAN-VPN2_isp1_Spoke,SDWAN-VPN2_isp2_Spoke,SDWAN-VPN1_isp1_Spoke,SDWAN-VPN1_isp2_Spoke,192.0.2.21/28,192.0.2.37/28
```

Add Device (Wizard)

2

Initial device configuration

Device template

SD-WAN_Branch_Template

3

Device details

Configure the public IP address or FQDN for the Management Center, except in scenarios where the Threat Defense device is publicly reachable, running a v

Configuration > Manager Remote Access.

CSV sample template file:

SampleTemplate.csv

>

You can onboard multiple Threat Defense devices by uploading a properly formatted .csv file containing the following information for each of these devices

✓

All entries are validated successfully.

DisplayName	SerialNumber	AdminPassword	DeviceGroup	\$Local_Identity1_SDWAN_ISP1	\$Local_Identity2_SDWAN_ISP2	\$Local_Identity3_SDWAN_ISP1	\$Local_Identity4_SDWAN_ISP2
Spoke3	FJC282917RQ	*****	-	SDWAN-VPN2_isp1_Spoke	SDWAN-VPN2_isp2_Spoke	SDWAN-VPN1_isp1_Spoke	SDWAN-VPN1_isp2_Spoke

Cancel

Add Device

Step 6 Click **Add Device** to initiate device registration.

The template configurations are applied after the device is successfully registered with the Management Center.

In the **Notifications > Tasks** window, you can view the messages related to the device registration, device discovery, and device template application.

The image displays two screenshots of the 'Tasks' window in a management center interface. Both screenshots show a top navigation bar with tabs for 'Deployments', 'Upgrades', 'Health', and 'Tasks' (which is selected). To the right of the tabs is a toggle for 'Show Pop-up Notifications' and an information icon. Below the tabs, a summary bar shows '20+ total' tasks, with sub-counts for '0 waiting', '0 running', '0 retrying', '20+ success', and '2 failures' (in the top screenshot) or '3 failures' (in the bottom screenshot). A search filter box is also present.

Top Screenshot Tasks:

- Discovery:** Spoke3 - Discovery from the device is successful. Duration: 1m 55s.
- SFTunnel:** Spoke3 - SFTunnel connection established successfully. Duration: -.
- Register:** Registration. Spoke3: Started device discovery. Duration: 42s.

Bottom Screenshot Tasks:

- Device Template Apply:** SD-WAN_Branch_Template - Application of device template is successful on all devices. Duration: 18s.
- Device Template Apply:** SD-WAN_Branch_Template - Application of device template is successful for device "Spoke3". Includes a 'Download Report' link. Duration: 17s.

A **Device Template Apply** report is generated after the apply template task is completed. This report is generated on both successful and unsuccessful application of the template on the device. You will see a link to this report in the **Notifications > Tasks** window.

Validate and Monitor Tunnel Statuses and Configurations of SD-WAN Topologies

View the Onboarded Device in the Device Management Page

After the device template is successfully applied on the device, you can view the Cisco Secure Firewall 1210CE device (Spoke 3) in the **Device Management** page.

All (6) Error (1) Warning (0) Offline (0) Normal (5) Deployment Pending (1) Upgrade (0) Short 3 (6)								
Collapse All				Download Device List Report				
<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	<div>Hub1</div> <div>209.165.200.225 - Routed</div>	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	sdwan-acl		
<input type="checkbox"/>	<div>Hub2</div> <div>209.165.200.226 - Routed</div>	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	sdwan-acl		
<input type="checkbox"/>	<div>Spoke1</div> <div>209.165.200.227 - Routed</div>	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	sdwan-acl		
<input type="checkbox"/>	<div>Spoke2</div> <div>209.165.200.228 - Routed</div>	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)	sdwan-acl		
<input type="checkbox"/>	<div>Spoke3</div> <div>209.165.200.229 - Routed</div>	Firewall 1210CE Threat Defense	7.6.0	N/A	Essentials	sdwan-acl		

Verify Tunnel Statuses in the Site-to-Site VPN Summary Page

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

After the device template is successfully applied on the device, the device (Spoke3) gets added to the SD-WAN topologies. You can view the VPN tunnels between the hubs and the spokes, and also the VPN tunnels between the hubs and the onboarded device, Spoke3.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2																								
SDWAN-VPN1	Route Based (VTI)	SD-WAN Topology	6- Tunnels		✓																								
<div>Hub</div> <div>Spoke</div> <table> <tr> <th>Device</th><th>VPN Interface</th><th>VTI Interface</th><th>Device</th><th>VPN Interface</th><th>VTI Interface</th></tr> <tr> <td>FTD Hub1</td><td>outside-isp1 (192.0.2.17)</td><td>outside-isp1_dyna... (209.165.201.1)</td><td>FTD Spoke3</td><td>outside-isp1 (192.0.2.21)</td><td>outside-isp1_stat... (209.165.201.3)</td></tr> <tr> <td>FTD Hub2</td><td>outside-isp1 (192.0.2.18)</td><td>outside-isp1_dyna... (209.165.201.17)</td><td>FTD Spoke3</td><td>outside-isp1 (192.0.2.21)</td><td>outside-isp1_stat... (209.165.201.19)</td></tr> <tr> <td>FTD Hub1</td><td>outside-isp1 (192.0.2.17)</td><td>outside-isp1_dyna... (209.165.201.1)</td><td>FTD Spoke2</td><td>outside-isp1 (192.0.2.20)</td><td>outside-isp1_stat... (209.165.201.4)</td></tr> </table>						Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface	FTD Hub1	outside-isp1 (192.0.2.17)	outside-isp1_dyna... (209.165.201.1)	FTD Spoke3	outside-isp1 (192.0.2.21)	outside-isp1_stat... (209.165.201.3)	FTD Hub2	outside-isp1 (192.0.2.18)	outside-isp1_dyna... (209.165.201.17)	FTD Spoke3	outside-isp1 (192.0.2.21)	outside-isp1_stat... (209.165.201.19)	FTD Hub1	outside-isp1 (192.0.2.17)	outside-isp1_dyna... (209.165.201.1)	FTD Spoke2	outside-isp1 (192.0.2.20)	outside-isp1_stat... (209.165.201.4)
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface																								
FTD Hub1	outside-isp1 (192.0.2.17)	outside-isp1_dyna... (209.165.201.1)	FTD Spoke3	outside-isp1 (192.0.2.21)	outside-isp1_stat... (209.165.201.3)																								
FTD Hub2	outside-isp1 (192.0.2.18)	outside-isp1_dyna... (209.165.201.17)	FTD Spoke3	outside-isp1 (192.0.2.21)	outside-isp1_stat... (209.165.201.19)																								
FTD Hub1	outside-isp1 (192.0.2.17)	outside-isp1_dyna... (209.165.201.1)	FTD Spoke2	outside-isp1 (192.0.2.20)	outside-isp1_stat... (209.165.201.4)																								
Viewing 1-6 of 6																													
SDWAN-VPN2	Route Based (VTI)	SD-WAN Topology	6- Tunnels		✓																								
<div>Hub</div> <div>Spoke</div> <table> <tr> <th>Device</th><th>VPN Interface</th><th>VTI Interface</th><th>Device</th><th>VPN Interface</th><th>VTI Interface</th></tr> <tr> <td>FTD Hub1</td><td>outside-isp2 (192.0.2.33)</td><td>outside-isp2_dyna... (209.165.201.33)</td><td>FTD Spoke3</td><td>outside-isp2 (192.0.2.37)</td><td>outside-isp2_stat... (209.165.201.35)</td></tr> <tr> <td>FTD Hub2</td><td>outside-isp2 (192.0.2.34)</td><td>outside-isp2_dyna... (209.165.201.49)</td><td>FTD Spoke3</td><td>outside-isp2 (192.0.2.37)</td><td>outside-isp2_stat... (209.165.201.51)</td></tr> <tr> <td>FTD Hub1</td><td>outside-isp2 (192.0.2.33)</td><td>outside-isp2_dyna... (209.165.201.33)</td><td>FTD Spoke2</td><td>outside-isp2 (192.0.2.36)</td><td>outside-isp2_stat... (209.165.201.36)</td></tr> </table>						Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface	FTD Hub1	outside-isp2 (192.0.2.33)	outside-isp2_dyna... (209.165.201.33)	FTD Spoke3	outside-isp2 (192.0.2.37)	outside-isp2_stat... (209.165.201.35)	FTD Hub2	outside-isp2 (192.0.2.34)	outside-isp2_dyna... (209.165.201.49)	FTD Spoke3	outside-isp2 (192.0.2.37)	outside-isp2_stat... (209.165.201.51)	FTD Hub1	outside-isp2 (192.0.2.33)	outside-isp2_dyna... (209.165.201.33)	FTD Spoke2	outside-isp2 (192.0.2.36)	outside-isp2_stat... (209.165.201.36)
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface																								
FTD Hub1	outside-isp2 (192.0.2.33)	outside-isp2_dyna... (209.165.201.33)	FTD Spoke3	outside-isp2 (192.0.2.37)	outside-isp2_stat... (209.165.201.35)																								
FTD Hub2	outside-isp2 (192.0.2.34)	outside-isp2_dyna... (209.165.201.49)	FTD Spoke3	outside-isp2 (192.0.2.37)	outside-isp2_stat... (209.165.201.51)																								
FTD Hub1	outside-isp2 (192.0.2.33)	outside-isp2_dyna... (209.165.201.33)	FTD Spoke2	outside-isp2 (192.0.2.36)	outside-isp2_stat... (209.165.201.36)																								

You can also view details of the SD-WAN VPN tunnels in the Site-to-Site VPN dashboard. For more information, see [Verify Tunnel Statuses in the Site-to-Site VPN Dashboard](#).

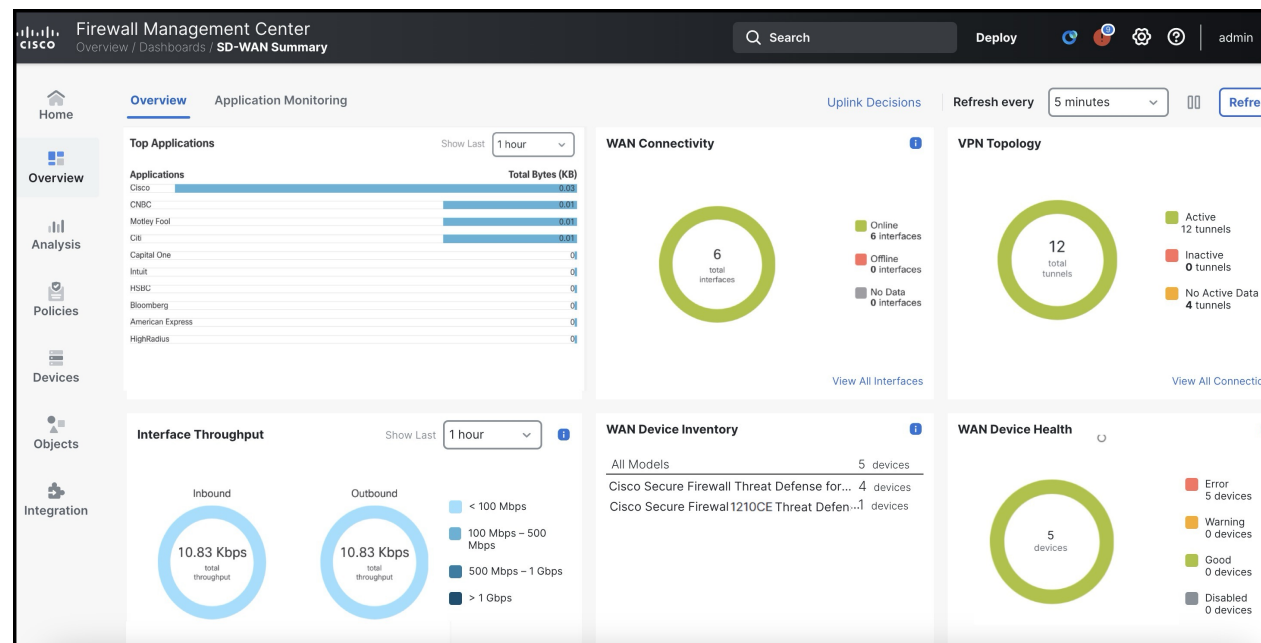
Monitor SD-WAN Topologies Using SD-WAN Summary Dashboard

To monitor your SD-WAN devices and their interfaces, choose **Overview > Dashboards > SD-WAN Summary**.

This dashboard helps you to:

- Identify issues with the underlay and overlay topologies.
- Troubleshoot VPN issues using the existing **Health Monitoring**, **Device Management**, and **Site-to-Site Monitoring** pages.
- Monitor application performance metrics of WAN interfaces. The threat defense steers application traffic based on these metrics.

Ensure that you review [Prerequisites for Using SD-WAN Summary Dashboard](#) to set up the dashboard.



Troubleshoot Device Templates and SD-WAN Topologies

- [Troubleshoot Device Templates](#)
- [Resolve Serial Number \(Zero-Touch Provisioning\) Registration Issues](#)
- [Troubleshoot SD-WAN Topologies](#)

