Use Cases for SD-WAN Capabilities in Cisco Secure Firewall

First Published: 2023-04-04

Last Modified: 2024-11-13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

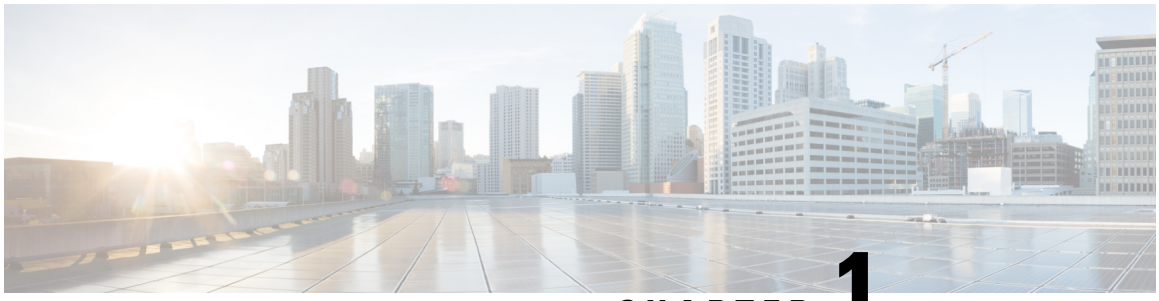
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Getting Started

This chapter provides you with a brief overview of the Cisco Secure Firewall features and the supported SD-WAN capabilities.

About This Publication

This guide details the primary use cases that uses the SD-WAN capabilities supported on Cisco Secure Firewall.

The approaches do not address all of the possible network needs; instead, they provide models on which you can pattern your network. You can choose not to use features presented in the examples, or you can add or substitute features that better suit your needs.

This guide assumes you are familiar with Cisco Secure Firewall. For more information on configurations, see Cisco Secure Firewall Management Center Administration Guide, 7.3 and Cisco Secure Firewall Management Center Device Configuration Guide, 7.3.

Cisco Secure Firewall

Cisco Secure Firewall is an exceptionally robust firewall solution with cutting-edge features such as Snort IPS, URL filtering, and malware defense.

This comprehensive offering greatly simplifies threat protection by enforcing consistent security policies across physical, private, and public cloud environments.

Furthermore, it grants extensive visibility into your network infrastructure, swiftly identifying the origin and activity of potential threats. Armed with this knowledge, you can promptly take action to stop attacks before they have a chance to disrupt your operations.

In addition to traditional firewall capabilities, it provides features as:

1. Application visibility and control
2. User identity awareness and control
3. Intrusion prevention and intrusion detection

4. SSL/TLS decryption
5. Reputation based blocking
6. File and malware protection
7. Virtual Private Network (VPN)

To further secure network deployments, Cisco Secure Firewall provides additional security capabilities in its later releases such as:

- Encrypted Visibility Engine (EVE) that enhance encrypted traffic inspection without the need to implement full main-in-the-middle (MITM) decryption.
- Elephant Flow Detection to detect and remediate elephant flows (flows that are typically larger than 1 GB/10 seconds) and avoid high CPU utilization and packet drops.
- Cisco Secure Dynamic Attribute Connector (CSDAC) that brings agility and intelligence into your security policy management by leveraging tags and labels for policy configuration rather than traditional IP/network-based policy configuration.

Overview of SD-WAN Capabilities

Software-Defined WAN (SD-WAN) solutions replace traditional WAN routers and are agnostic to WAN transport technologies. SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

As organizations expand their operations across multiple branch locations, ensuring secure and streamlined connectivity becomes paramount. Deploying a secure branch network infrastructure involves complex configurations, which can be time-consuming and prone to configuration errors if not handled properly. However, organizations can overcome these challenges by leveraging the Cisco Secure Firewall Management Center (management center) and the Cisco Secure Firewall Threat Defense (threat defense) devices for a simplified and secure branch deployment.

In this guide, we explore the concept of simplifying secure branch deployment using a robust firewall solution. By integrating a secure firewall as a foundational component of the branch network architecture, organizations can establish a strong security baseline while simplifying the deployment process. This approach enables organizations to enforce unified security policies, optimize traffic routing, and ensure resilient connectivity.

Some of the SD-WAN capabilities supported on the Cisco Secure Firewall are:

- **Simplified management:**
  - SASE: Umbrella auto tunnel deployment
  - Dynamic VTI (DVTI) hub spoke topology simplification
- **Application awareness:**
  - Direct Internet Access (DIA) for public cloud and guest user
  - Policy based routing (PBR) using applications as a match criteria
  - Local tunnel ID support for Umbrella

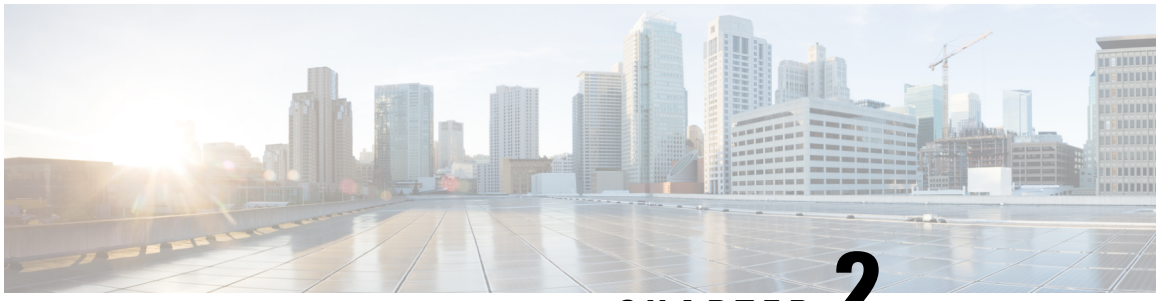
- **Increased usable bandwidth:**
  - ECMP support for load balancing across multiple ISPs and VTIs
  - Application-based load balancing using PBR
- **High availability with near zero network downtime:**
  - Dual ISP configuration
  - Optimal path selection based on application-based interface monitoring.
- **Secure Elastic Connectivity:**
  - Route-based (VTI) VPN tunnels between headquarters (hub) and branches (spokes)
  - IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP over VTI
  - DVTI hubs that support spokes with static or dynamic IP

Features

The following table lists some commonly used SD-WAN features:

Feature	Introduced in	More Information
SD-WAN Wizard	Release 7.6	Using SD-WAN Wizard for Secure Branch Network Deployment
Application monitoring using SD-WAN Summary dashboard	Release 7.4.1	SD-WAN Summary Dashboard
SD-WAN Summary Dashboard	Release 7.4	SD-WAN Summary Dashboard
Policy-based routing with user identity and SGTs	Release 7.4	Policy Based Routing
Policy-based routing using HTTP path monitoring	Release 7.4	Policy Based Routing
Loopback interface support for VTIs	Release 7.3	Configure Loopback Interfaces
Support for dynamic VTI (DVTI) with site-to-site VPN	Release 7.3	Dynamic VTI
Umbrella auto tunnel	Release 7.3	Deploy a SASE Tunnel on Umbrella
Support for IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP for VTIs	Release 7.3	BGP OSPF EIGRP

Feature	Introduced in	More Information
Route-based site-to-site VPN with hub and spoke topology	Release 7.2	Create a Route-based Site-to-Site VPN
Policy-based routing with path monitoring	Release 7.2	Policy Based Routing
Site to Site VPN Monitoring Dashboard	Release 7.1	Monitoring the Site-to-Site VPNs
Direct Internet Access/Policy Based Routing	Release 7.1	Policy Based Routing
Equal-Cost-Multi-Path (ECMP) zone with WAN interfaces	Release 7.1	ECMP
ECMP zone with VTI interfaces	Release 7.1	ECMP
Backup VTI for route-based site-to-site VPN	Release 7.0	Route Traffic Through a Backup VTI Tunnel
Support for static VTI (SVTI) with site-to-site VPN	Release 6.7	Static VTI



CHAPTER 2

Simplify Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI)

In this chapter, we delve into the practical application of the DVTI in a hub and spoke topology. The use case details the scenario, network topology, best practices, and prerequisites. It also provides a comprehensive end-to-end procedure for seamless implementation.

Route-based VPN in a Hub and Spoke Topology

The Secure Firewall Management Center supports routable logical interfaces called the Virtual Tunnel Interfaces (VTIs). You can use these interfaces to apply static and dynamic routing policies. When using VTI, you do not have to configure static crypto map access lists and map them to interfaces. You no longer have to track all remote subnets and include them in the crypto map access list.

You can create a VPN tunnel between peers using VTIs. VTIs support route-based VPN with IPsec profiles attached to the end of each tunnel. VTIs use static or dynamic routes. The threat defense device encrypts or decrypts the traffic from or to the tunnel interface and forwards it according to the routing table.

The management center supports a site-to-site VPN wizard with defaults to configure VTI or route-based VPN.

When it comes to implementing route-based VPN in a hub and spoke topology,Dynamic Virtual Tunnel Interface (DVTI) is configured on the hub and SVTI (Static Virtual Tunnel Interface) is configured on the spoke.

Dynamic VTI uses a virtual template for dynamic instantiation and management of IPsec interfaces. The virtual template dynamically generates a unique virtual access interface for each VPN session. Dynamic VTI supports multiple IPsec security associations and accepts multiple IPsec selectors proposed by the spoke.

Secure Firewall Threat Defense supports the configuration of a backup tunnel for the route-based (VTI) VPN providing link redundancy. When the primary VTI (primary tunnel) is unable to route the traffic, the traffic in the VPN is tunneled through the backup VTI (secondary tunnel).

Benefits

The benefits of using a VTI-based VPN in a hub and spoke topology are:

1. **Simplified Configuration:** VTI simplifies the configuration of VPN tunnels by providing a logical interface that represents the tunnel itself. This eliminates the need for complex crypto map or access list configurations typically associated with traditional VPN setups.
2. **Simplified Management:** It is easy to manage peer configurations for large enterprise hub and spoke deployments. Only one dynamic VTI is configured on the hub for multiple static VTIs configured on the spokes.
3. **Scalability:** VTI allows for easy scalability. Addition of new spokes does not require any additional VPN configuration on the hub. You may need to update NAT and routing configurations depending upon the setup.
4. **Dynamic Routing Support:** VTI supports dynamic routing protocols such as Open Shortest Path First (OSPF) allowing for the dynamic exchange of routing information between VPN endpoints. This enables efficient routing decisions based on real-time network conditions.
5. **Dual ISP Redundancy:** SVTI supports backup VTI tunnels.
6. **Load balancing:** SVTI supports load balancing of VPN traffic using ECMP.

Is This Use Case For You?

The intended audience for the DVTI hub and spoke configuration includes network architects, IT administrators, and networking professionals responsible for designing and managing the network infrastructure of an organization. This use case is valuable to those seeking to optimize network connectivity, ensure data security, and streamline network administration by implementing a centralized hub with secure tunnels connecting to remote spoke sites.

Scenario

A medium-sized company has multiple branch offices located in different cities, and they want to establish a secure and efficient network infrastructure to connect these branches with the central headquarters. The company's IT administrator, Alice, is responsible for configuring and managing the network.

What is at risk?

The current network configuration requires manual configuration of multiple point-to-point connections between each branch office and the central headquarters. This approach is time-consuming, error-prone, and makes it challenging to maintain consistency in network settings across all locations. Alice needs a solution that simplifies the configuration process and provides centralized control.

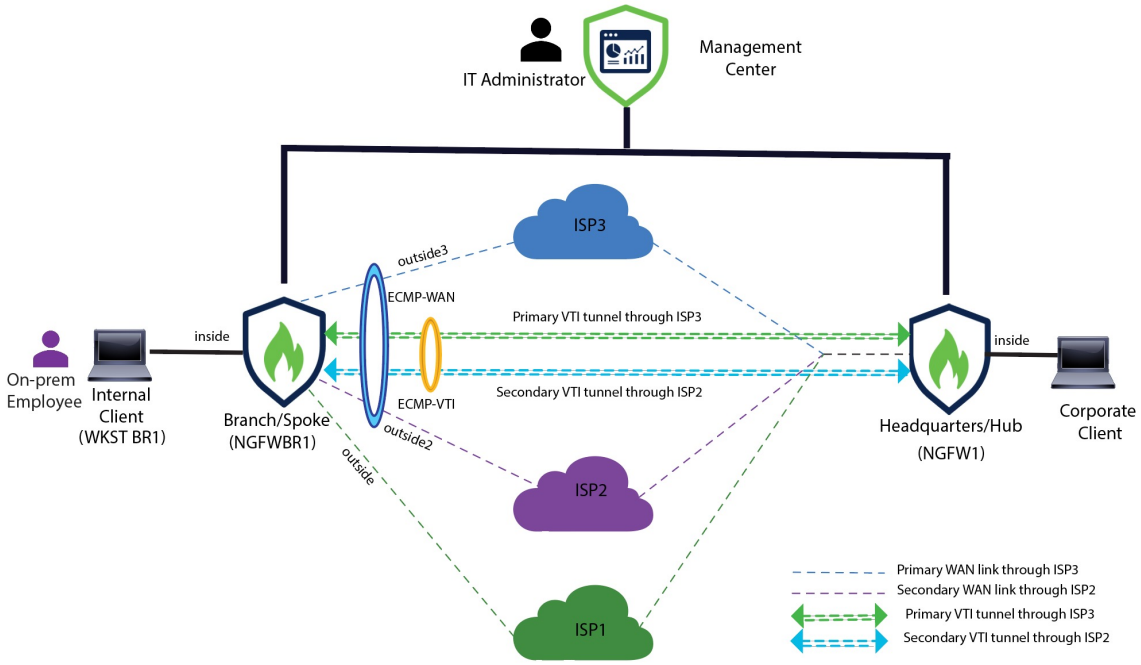
How does a route-based VPN between a branch(spoke) and headquarters (hub) solve the problem?

1. Centralized Configuration: Alice implements DVTI Hub and Spoke topology, centralizing configuration and management at the hub. This simplifies network settings across all locations.
2. Dynamic Routing: Alice sets up dynamic routing protocols (for example, OSPF) automating routing information exchange. Manual configuration of static routes is eliminated, simplifying network administration.
3. Rapid Provisioning: With DVTI, Alice can quickly provision new branch offices by configuring a spoke router and establishing a secure tunnel with the hub. This simplifies the provisioning process and supports network scalability.

By implementing DVTI, Alice simplifies network configuration, centralizes control, ensures consistency, and enables efficient provisioning and scalability in the corporate network.

Network Topology

In this hub spoke topology, a threat defense device is deployed at a branch location. In the figure below, the internal client or branch workstation is labelled WKST BR and the branch (spoke) threat defense is labelled NGFWBR1. The headquarters (hub) is labelled as NGFW1 and is connected to the corporate network. A VPN tunnel is configured between NGFWBR1 and NGFW1. An ECMP zone is configured on the primary and secondary static VTI interfaces on the branch node for link redundancy and loading balancing of VPN traffic.



Best Practices

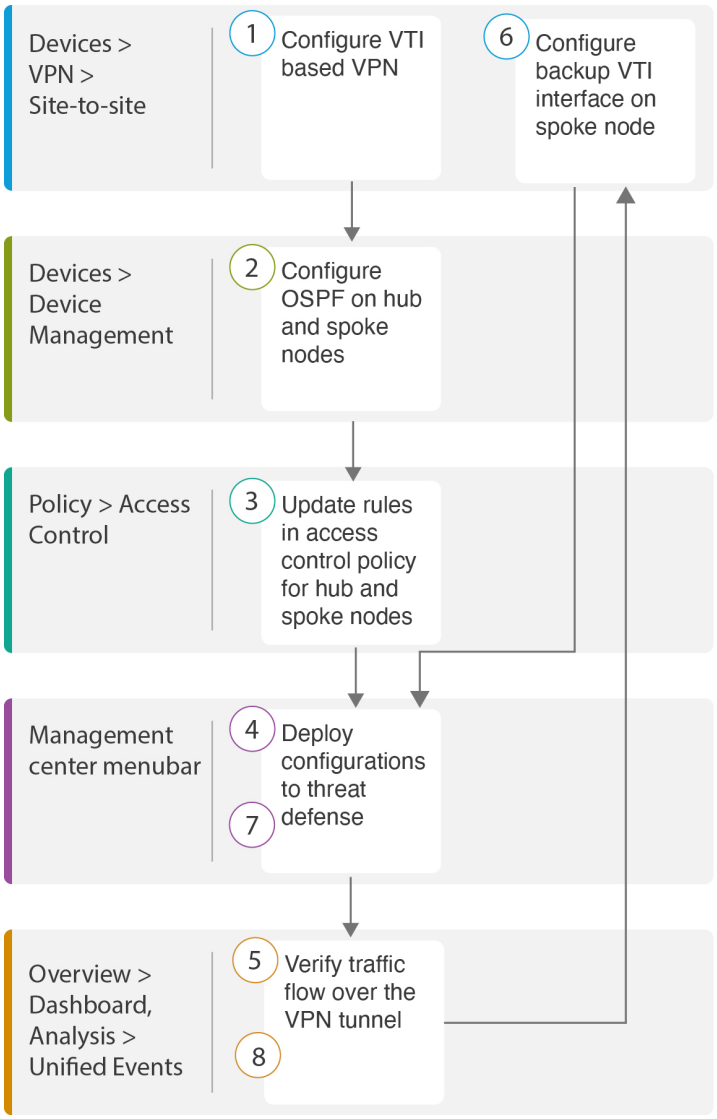
- Ensure that Secure Firewall Threat Defense is runing on version 6.7 and later.
- VTI is supported in routed mode only.
- Configure the Borrow IP for the dynamic interface from a loopback interface.
- Ensure to apply access rules on a VTI interface to control traffic through VTI.
- Configure ECMP zones for SVTIs to load balance VTI traffic.

Prerequisites

- Complete the Threat Defense Initial Configuration Using the Device Manager
- Assign Licenses to Devices
- Add routes for internet access. See Add a Static Route
- Configure NAT for Threat Defense
- Creating a Basic Access Control Policy

End-to-End Procedure for Configuring a Route-based VPN (Hub and Spoke Topology)

The following flowchart illustrates the workflow for configuring a route-based VPN for a hub spoke topology in Secure Firewall Management Center.



Step	Description
1	Configure a VTI based VPN. See • Create a Route-based Site-to-Site VPN, on page 10 • Configure the Endpoint for the Hub Node, on page 11

Step	Description
	• Configure the Endpoint for the Spoke Node, on page 12
2	Configure OSPF on the hub and spoke nodes. See • Configure OSPF on the Hub Node, on page 14 • Configure OSPF on the Spoke Node, on page 16
3	Updates rules in the access control policy for hub and spoke nodes. See Configure the Access Control Policy, on page 17.
4	Deploy configuration to threat defense. See Deploy Configuration, on page 20.
5	Verify traffic flow over VPN tunnel. See Verify Traffic Flow Over the VPN Tunnel, on page 20.
6	Configure backup VTI on spoke node. See Configure the Backup VTI Interface on the Spoke Node, on page 24.
7	Deploy the configuration on Threat Defense. SeeDeploy Configuration, on page 20 .
8	Verify traffic flow over secondary tunnel. See Verify the Primary and Secondary Tunnels, on page 26.

Create a Route-based Site-to-Site VPN

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

For managed spokes, you can configure a backup static VTI interface along with the primary VTI interface.

Procedure

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

Step 2 Enter the name as **Corporate-VPN** in the **Topology Name** field.

Step 3 Choose **Route Based (VTI)** as the topology type.

Step 4 Configure the endpoint for the hub node. See Configure the Endpoint for the Hub Node, on page 11.

Step 5 Configure the endpoint for the spoke node. See Configure the Endpoint for the Spoke Node, on page 12.

Step 6 The default settings are used in the **IKE**, **IPsec**, and **Advanced** tabs.

Step 7 Click **Save**.

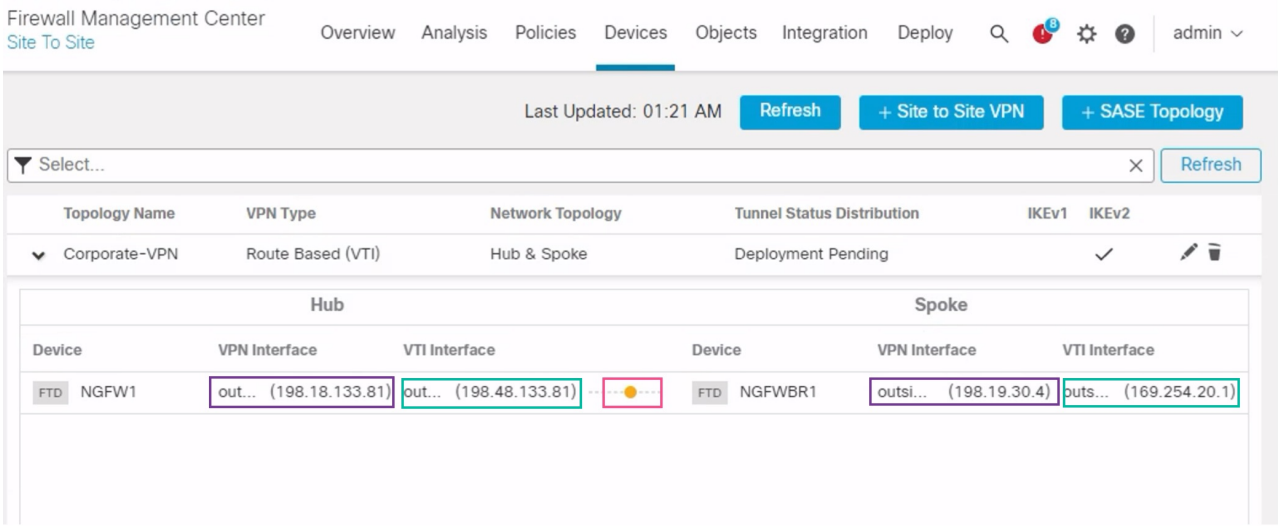
The Corporate-VPN topology is created successfully.

Step 8 You can view the VPN topology in the Site-to-site VPN listing page by navigating to **Devices** > **Site-to-site VPN**.

Note

Click **Refresh** if you do not see the VPN topology that you created.

Step 9 Expand the **Corporate-VPN** node to view all the tunnels in the topology. It displays the **NGFW1** hub and the **NGFWBR1** spoke with details of the physical source and VTI interfaces. Since the configuration has not yet been deployed, it displays **Deployment Pending** and the tunnel displays amber status.



What to do next

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

- A routing protocol to route the VTI traffic between the devices over the VTI tunnel. See Configure OSPF on the Hub Node, on page 14 and Configure OSPF on the Spoke Node, on page 16.
- An access control rule to allow encrypted traffic. See Configure the Access Control Policy, on page 17.

Configure the Endpoint for the Hub Node

When you specify the tunnel type as dynamic and configure the related parameters, the management center generates a dynamic virtual template. The virtual template dynamically generates the virtual access interface that is unique for each VPN session.

Procedure

Step 1 In the **Hub Nodes** section, click +. The **Add Endpoint** dialog box is displayed.

Step 2 Choose **NGFW1** as the hub from the **Device** drop-down list.

Note
The device must be running on software version 7.3 or later.

Step 3 Click **+** next to the **Dynamic Virtual Tunnel Interface** drop-down list to add a new dynamic VTI.

The **Add Virtual Tunnel Interface** dialog box appears with the following pre-populated default configurations.

- **Tunnel Type** is auto-populated with **Dynamic**.
- **Name** is auto-populated as <*tunnel_source interface logical name*>+ dynamic_vti +<*tunnel ID*>. For example, **outside_dynamic_vti_1** .
- The **Enabled** checkbox is checked by default.
- **Security Zone** –To define a security zone for this interface, choose **New…** from the drop-down list. In the **New Security Zone** dialog box, enter **Tunnel_Zone** as the name and click **OK**. Select **Tunnel_Zone** as the security zone for this tunnel interface**.**
- **Template ID** is auto-populated with a unique ID for the DVTI interface.
- **Tunnel Source** is the physical interface that is the source of the DVTI and is auto-populated by default. In this use case, we do not want to set an explicit tunnel source for the DVTI. Clear the selection by choosing **Select Interface** from the drop-down list.
- **IPsec Tunnel Mode** is set to IPv4, by default.
- **IP address** cannot be a static IP address as DVTI is a template interface. We recommend that you configure the Borrow IP for the dynamic interface from a loopback interface. To add a loopback interface, click **+** next to the **Borrow IP (IP unnumbered)** drop-down list. In the **Add Loopback Interface** dialog box:
  a. In the **General** tab, enter the **Name** as **HUB_Tunnel_IP** and **Loopback ID** as **1**.
  b. In the **IPv4** tab, enter the IP address as **198.48.133.81/32** .
  c. Click **OK** to save the loopback interface.

  The Borrow IP is set to **Loopback 1(HUB_Tunnel_IP)**.

Click **OK** to save the DVTI. A message is displayed that confirms the VTI is created successfully. Click **OK**.

The Dynamic Virtual Tunnel Interface is set to **outside_dynamic_vti_1(198.48.133.81)**.

Step 4 Select **GigabitEthernet 0/0 (outside)** from the **Tunnel Source** drop-down list. The IP address of the outside interface (**198.18.133.81)** is auto-populated in the next field.

Step 5 Expand **Advanced Settings** to view the default settings.

Step 6 Click **OK**.

NGFW1 is successfully configured as the hub node.

Configure the Endpoint for the Spoke Node

Procedure

Step 1 In the **Spoke Nodes** section, click **+**. The **Add Endpoint** dialog box is displayed.

Step 2 Choose **NGFWBR1** as the hub from the **Device** drop-down list.

Note
The device must be running on software version 7.3 or later.

Step 3 Click **+** next to the **Static Virtual Tunnel Interface** drop-down list to add a new static VTI.

The **Add Virtual Tunnel Interface** dialog box appears with the following pre-populated default configurations.

- **Tunnel Type** is auto-populated with **Static**.
- **Name** is auto-populated as <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*>. For example, **outside_static_vti_1** .
- The **Enabled** checkbox is checked by default.
- Select **Tunnel_Zone** from the Security Zone drop-down list.
- **Tunnel ID** is auto-populated with a value as 1.
- Select **GigabitEthernet0/4 (outside3)** from the **Tunnel Source** drop-down list. Select the IP address of the outside 3 interface as **198.19.30.4** from the drop-down list next to it.
- **IPsec Tunnel Mode** is set to IPv4, by default.
- **IP address** can either be a static IP address or a borrow IP. We recommend that you configure the Borrow IP for the static interface from a loopback interface. To add a loopback interface, click **+** next to the **Borrow IP (IP unnumbered)** drop-down list. In the **Add Loopback Interface** dialog box:
  a. In the **General** tab, enter the **Name** as **Spoke_Tunnel_IP** and **Loopback ID** as **1**.
  b. In the **IPv4** tab, enter the IP address as **169.254.20.1/32** .
  c. Click **OK** to save the loopback interface.

  The Borrow IP is set to **Loopback 1(Spoke_Tunnel_IP)**.

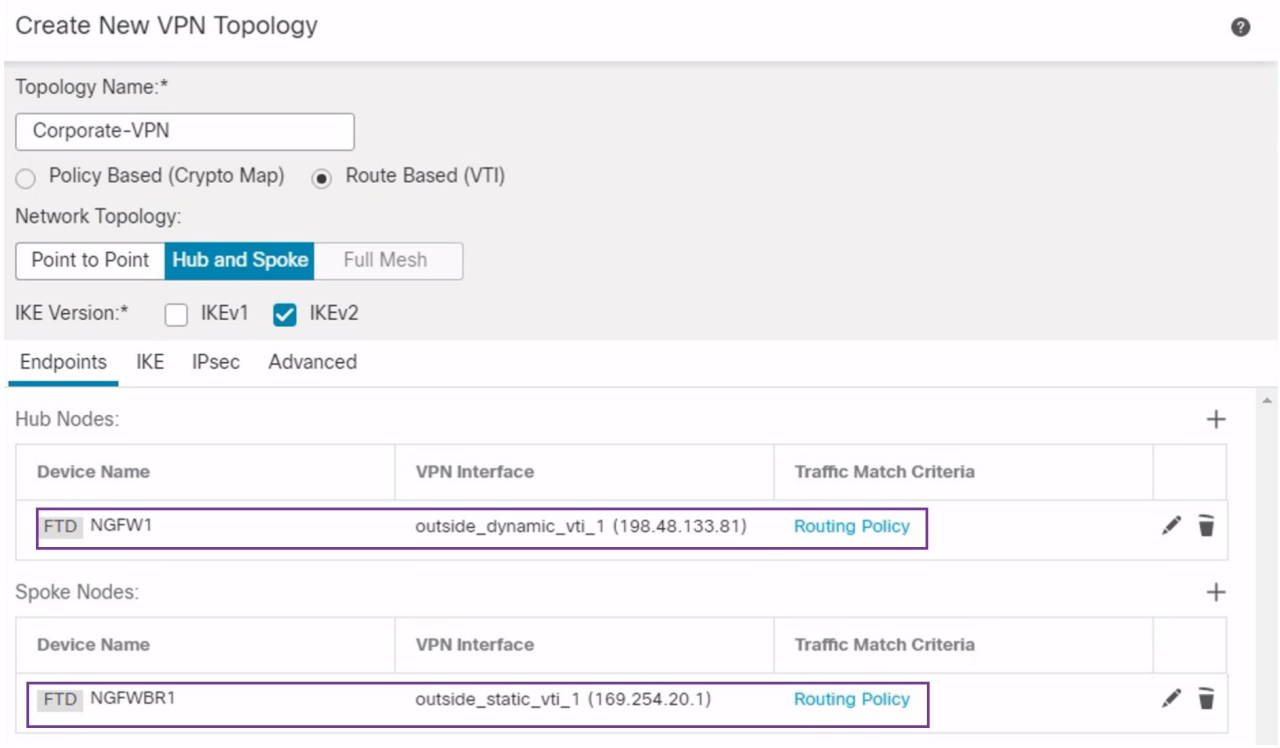
Click **OK** to save the SVTI. A message is displayed that confirms the VTI is created successfully. Click **OK**.

The Static Virtual Tunnel Interface is set to **outside_static_vti_1(169.254.20.1)**.

Step 4 Expand **Advanced Settings** to view the default settings. Both checkboxes must be checked.

Step 5 Click **OK**.

NGFWBR1 is successfully configured as the spoke node.



Configure OSPF on the Hub Node

OSPF is configured between Hub and Spoke device to allow traffic to be sent across the VPN tunnel. For reference, static routing is underlay, over which Spoke to Hub tunnel is established and OSPF is considered as overlay.

Procedure

Step 1 To edit the hub node, choose **Devices** > **Device Management** and click the **Edit** ( ) icon for the NGFW1 node.

Step 2 In the **Interfaces** tab, verify the **Loopback1** interface that was created earlier and serves as the IP address for the DVTI interface.

Step 3 Click **Routing**.

Step 4 Click **OSPF** in the left panel.

Step 5 Check the **Process 1** checkbox to enable an OSPF instance.

Step 6 Click the **Interface** tab.

Step 7 Click **+Add**. The **Add Interface** dialog box appears. Modify the following fields:

- **Interface**—Select the DVTI interface **outside_dynamic_vti_1** from the drop-down list.
- **Point-to-point**—Check the checkbox to transmit OSPF routes over VPN tunnels.

The rest of the fields use default values.

- Click **OK**.

A row is added in the **Interface** tab for **outside_dynamic_vti_1**.

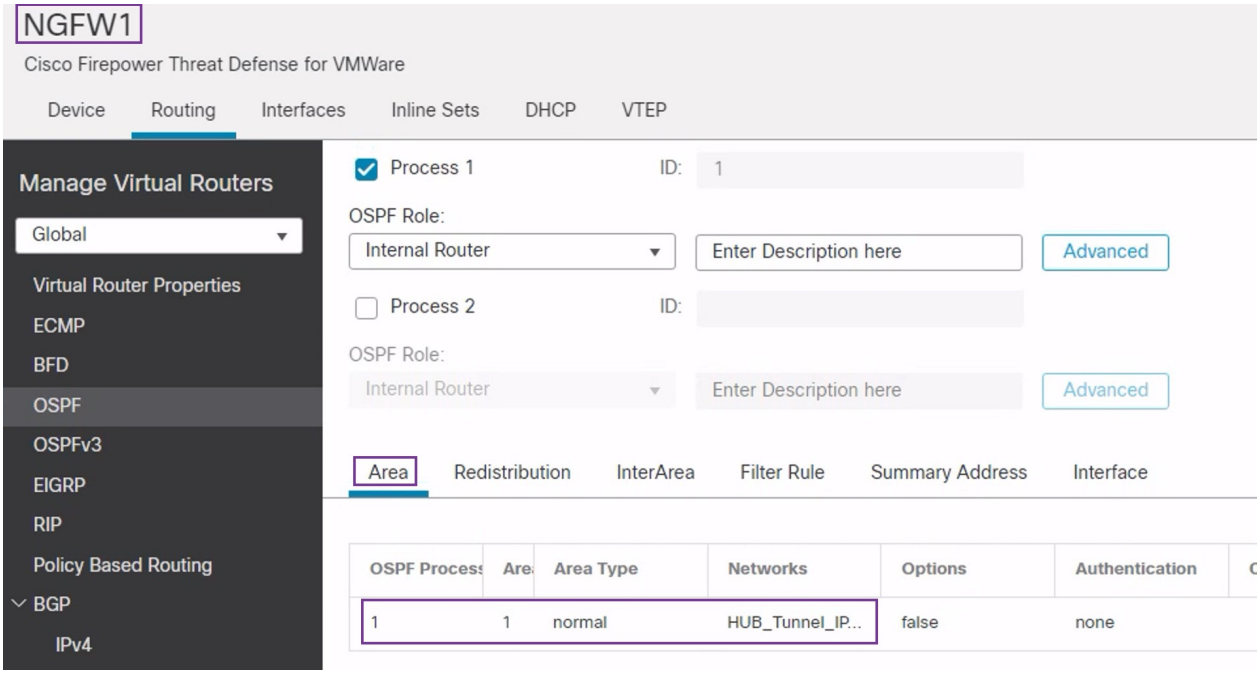
Step 8 Click the **Area** tab.

Step 9 Click **+Add**. The **Add Area** dialog box appears. Modify the following fields:

- **OSPF Process**—Choose the process ID as 1.
- **Area ID**—Ensure the value is 1.

  The rest of the fields use default values.
- **Available Network**— To add networks to be advertised over the tunnel:
  - To add a new network object, click +. Enter these details:
    - **Name**—Enter the name as **HUB_Tunnel_IP**.
    - **Network**—Select the **Host** option and enter the host IP as **198.48.133.81**.
    - Click **Save**.
  - Enter **HUB** in the search area of the **Available Network** field. The newly added network object (**HUB_Tunnel_IP**) is listed. Select the object and click **Add** to add it to the **Selected Network** list.
  - Enter **Corporate** in the search area of the **Available Network** field. The **Corporate_LAN** network object is listed. Select the object and click **Add** to add it to the **Selected Network** list.
- Click **OK**.

A row is added in the **Area** tab.



Step 10 Click **Save** to save the OSPF configuration for the hub node.

Configure OSPF on the Spoke Node

Procedure

Step 1 To edit the spoke node, choose **Devices** > **Device Management** and click the **Edit** (✎) icon for the NGFWBR1 node.

Step 2 In the **Interfaces** tab:

- Verify the details of **Tunnel1** interface that was created earlier in the spoke configuration.
- Verify the details of the **Loopback1** interface that was created earlier and serves as the IP address for Tunnel1.

Step 3 Click **Routing**.

Step 4 Click **OSPF** in the left panel.

Step 5 Check the **Process 1** checkbox to enable an OSPF instance.

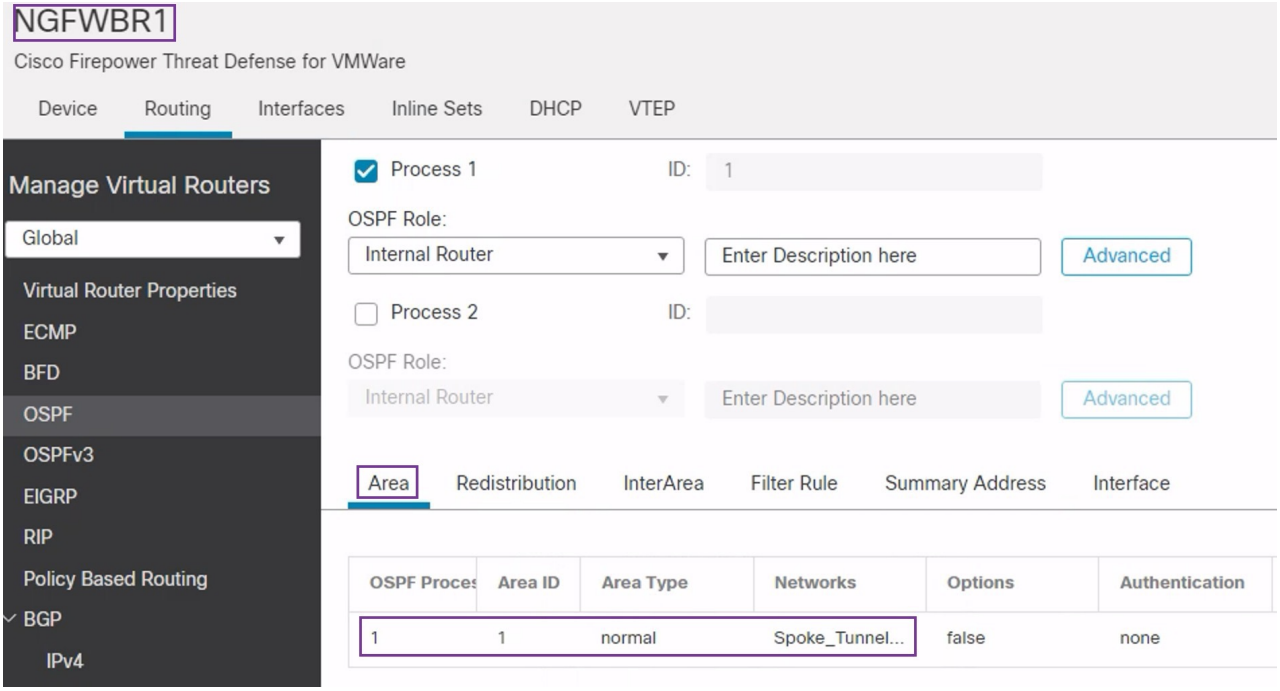
Step 6 Click the **Area** tab.

Step 7 Click **+Add**. The **Add Area** dialog box appears. Modify the following fields:

- **OSPF Process**—Choose the process ID as 1.
- **Area ID**—Ensure the value is 1.

  The rest of the fields use default values.
- **Available Network**— To add networks to be advertised over the tunnel:
  - To add a new network object, click +. Enter these details:
    - **Name**—enter the name as **Spoke_Tunnel_IP**.
    - **Network**—Select the **Host** option and enter the host IP as **169.254.20.1**.
    - Click **Save**.
  - Enter **Spoke** in the search area of the **Available Network** field. The newly added network object (**Spoke_Tunnel_IP**) is listed. Select the object and click **Add** to add it to the **Selected Network** list.
  - Enter **Branch** in the search area of the **Available Network** field. The **Branch_LAN** network object is listed. Select the object and click **Add** to add it to the **Selected Network** list.
- Click **OK**.

A row is added in the **Area** tab.



Step 8 Click **Save** to save the OSPF configuration for the spoke node.

Configure the Access Control Policy

Before proceeding, ensure that the VTI interfaces on **NGFW1** and **NGFWBR1** nodes are associated to a new zone labeled as **Tunnel_Zone**.

Navigate to **Policies > Access Control** to review the access control policies. The following access control policies must be updated for both the hub and spoke to allow the VPN traffic to and from the tunnel.

- **NGFW1**—Access control policy for the hub node (NGFW1)
- **Branch Access Control** —Access control policy for the spoke node (NGFWBR1)

Procedure

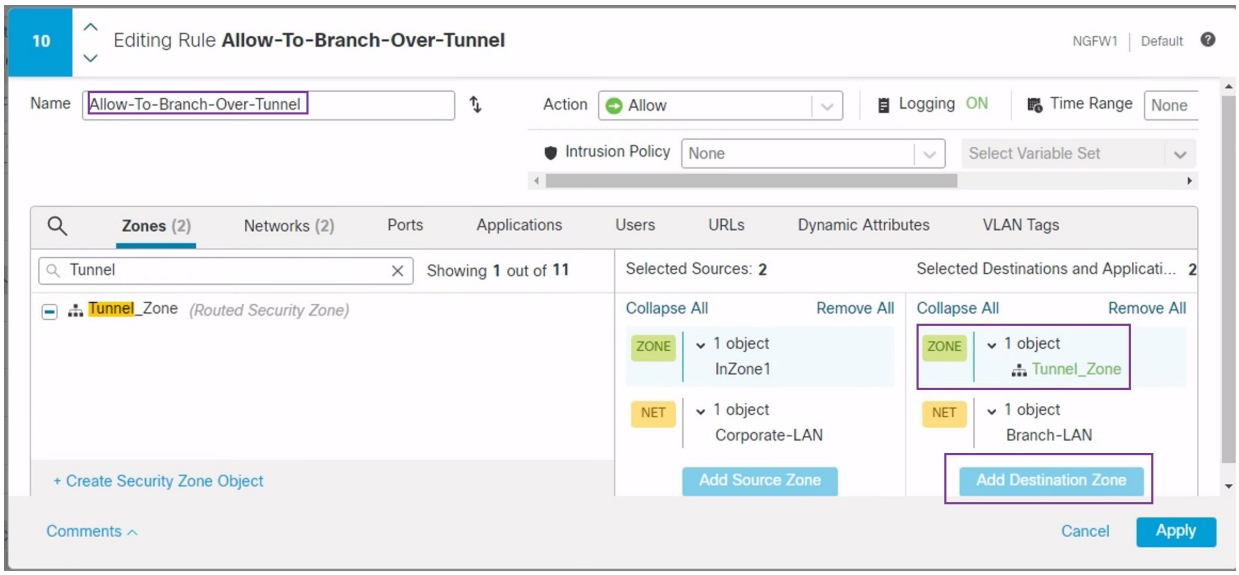
Step 1 To edit the hub node (NGFW1) AC policy, click the **Edit** (✎) icon.

The existing rules that must be modified for this use case are:

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

a. To edit the **Allow-To-Branch-Over-Tunnel** policy, click the **Edit** (✎) icon.

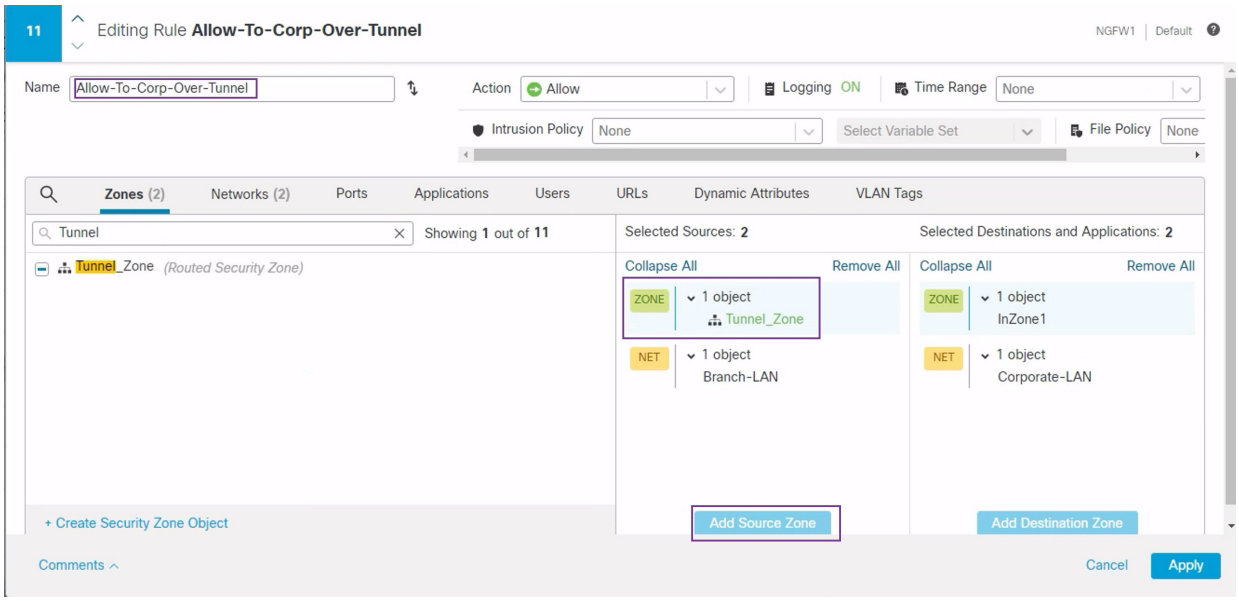
b. In the **Zones** tab, search for **Tunnel_Zone**, select it, and click **Add Destination Zone**.



c. Click **Apply** to save the rule.

d. To edit the **Allow-To-Corp-Over-Tunnel** policy, click the **Edit** (✎) icon.

e. In the **Zones** tab, search for **Tunnel_Zone**, select it, and click **Add Source Zone**.



f. Click **Apply** to save the rule.

g. Verify the updated rules in NGFW1.

h. Click **Save** the AC policy.

i. Click **Return to Access Conrol Policy Management** to return the policy page.

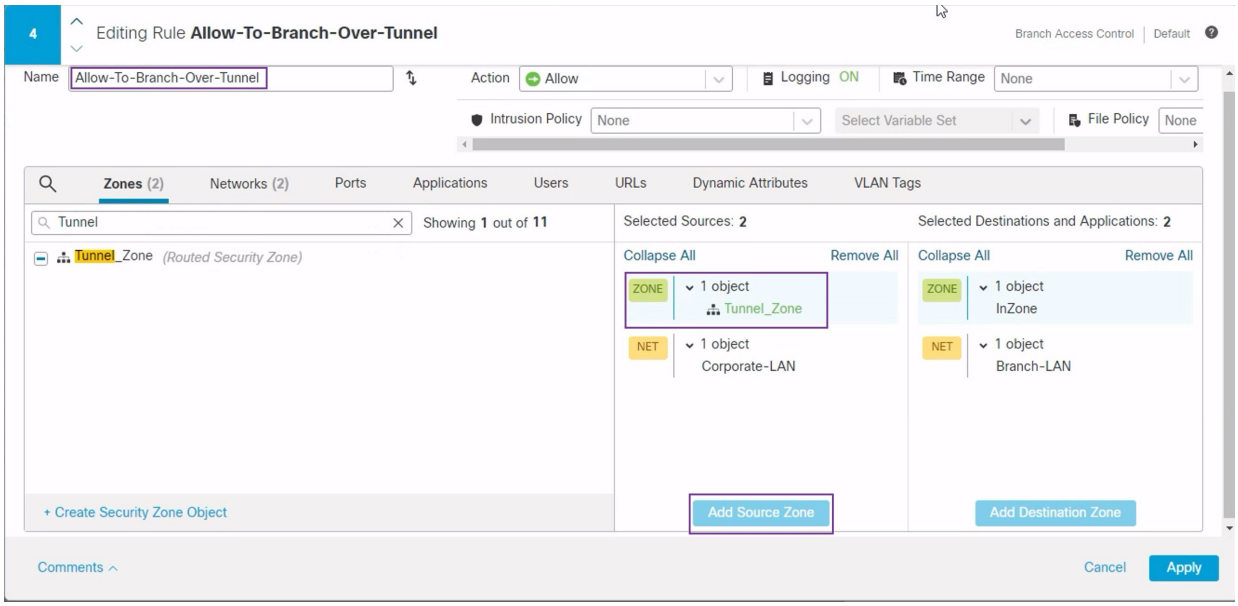
Step 2 To edit the spoke node (NGFWBR1) AC policy, click the **Edit** (✎) icon.

The rules that must be edited for this example are:

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

a. To edit the **Allow-To-Branch-Over-Tunnel** policy, click the **Edit** (✎) icon.

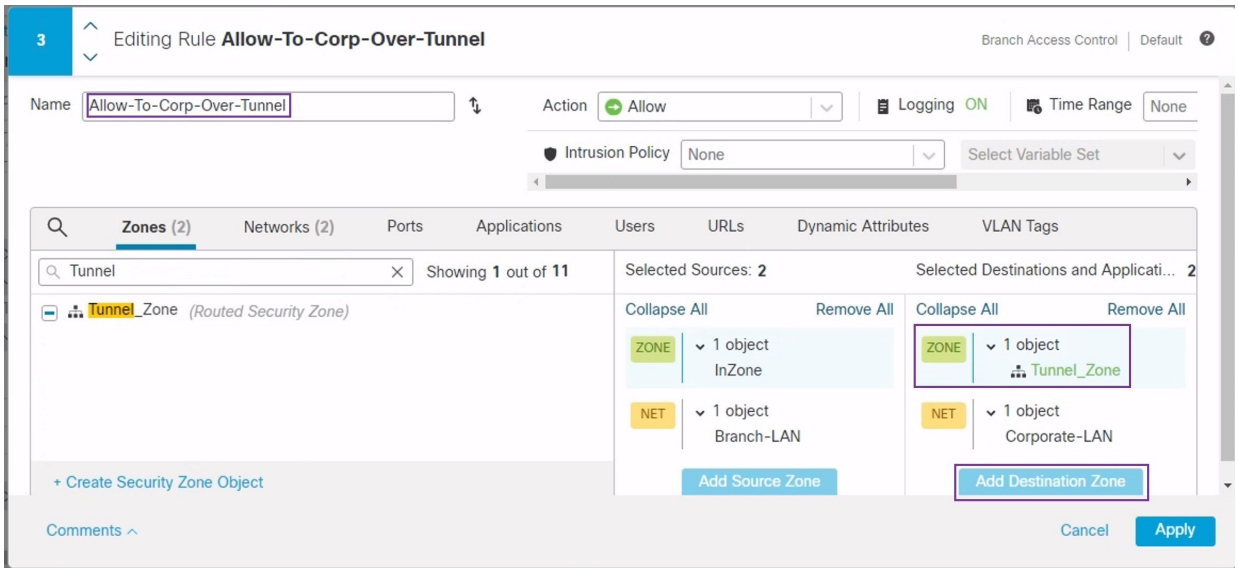
b. In the **Zones** tab, search for **Tunnel_Zone**, select it, and click **Add Souce Zone**.



c. Click **Apply** to save the rule.

d. To edit the **Allow-To-Corp-Over-Tunnel** policy, click the **Edit** (✎) icon.

e. In the **Zones** tab, search for **Tunnel_Zone**, select it, and click **Add Destination Zone**.



f. Click **Apply** to save the rule.

g. Verify the updated rules in NGFWBR1.

h. Click **Save** the AC policy.

Deploy Configuration

After you complete all the configurations, deploy them to the managed device.

Procedure

Step 1 On the management center menu bar, click **Deploy**. This displays the list of devices that are Ready for Deployment.

Step 2 Check the checkboxes adjacent to NGFWBR1 and NGFW1 on which you want to deploy configuration changes.

Step 3 Click **Deploy**. Wait till the deployment is marked Completed on the Deploy dialog box.

Step 4 If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Errors** or **Validation Warnings** window. To view complete details, click the Validation Errors or Validation Warnings link.

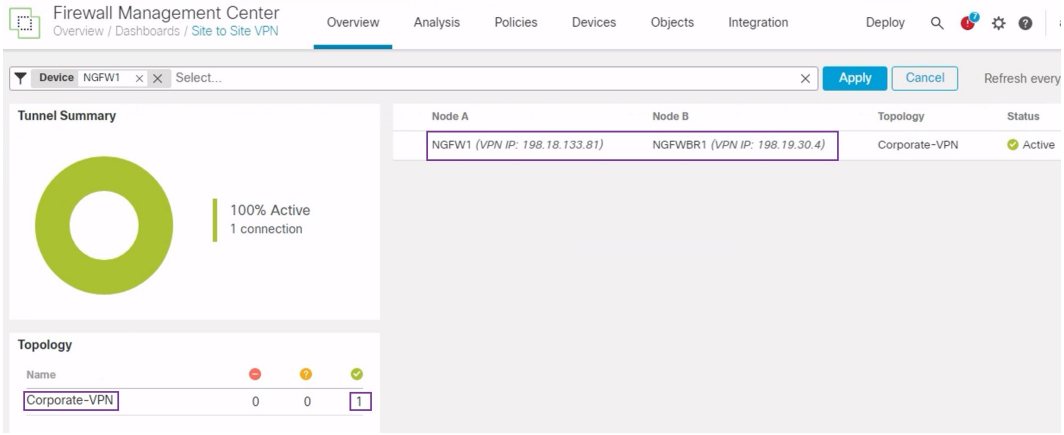
You have the following choices:

- Proceed with Deploy—Continue deploying without resolving warning conditions. You cannot proceed if the system identifies errors.
- Close—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

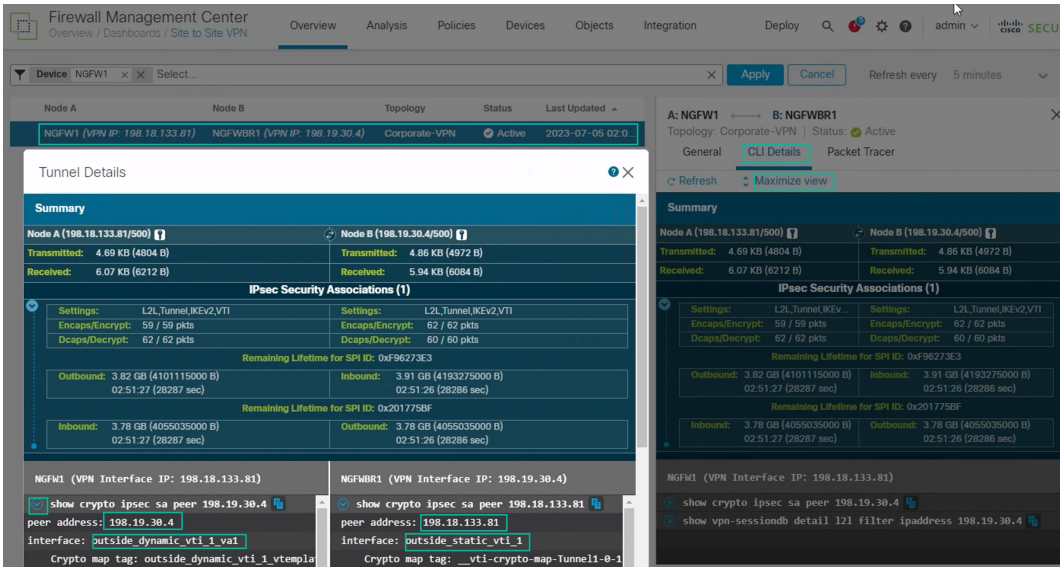
Verify Traffic Flow Over the VPN Tunnel

Perform the following verifications for the VPN tunnel.

- **Verify Tunnel Status on the Site-to-site VPN Dashboard**
  1. To verify that the VPN tunnel is up and green, choose **Overview** > **Dashboards** > **Site-to-site VPN**.



2. Hover over NGFW1. The **View Full Information** icon is displayed next to NGFW1.
3. Click the **View Full Information** icon.A side pane with tunnel details and additional actions appears.
4. Click the **CLI Details** tab in the side pane.
5. Click **Maximize View** to display a maximized dialog box that contains the details of the IPSec security associations.
6. You can expand the CLI for the show commands in the lower portion of the dialog box to view the VTI interfaces on the devices.

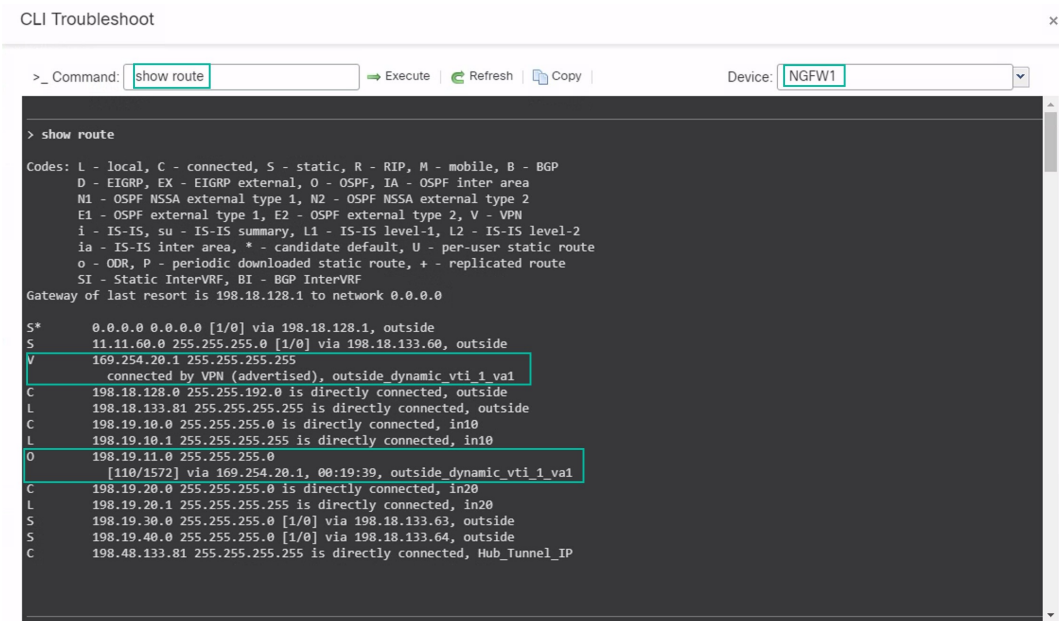


7. Click **Close** to terminate the Tunnel Details window.

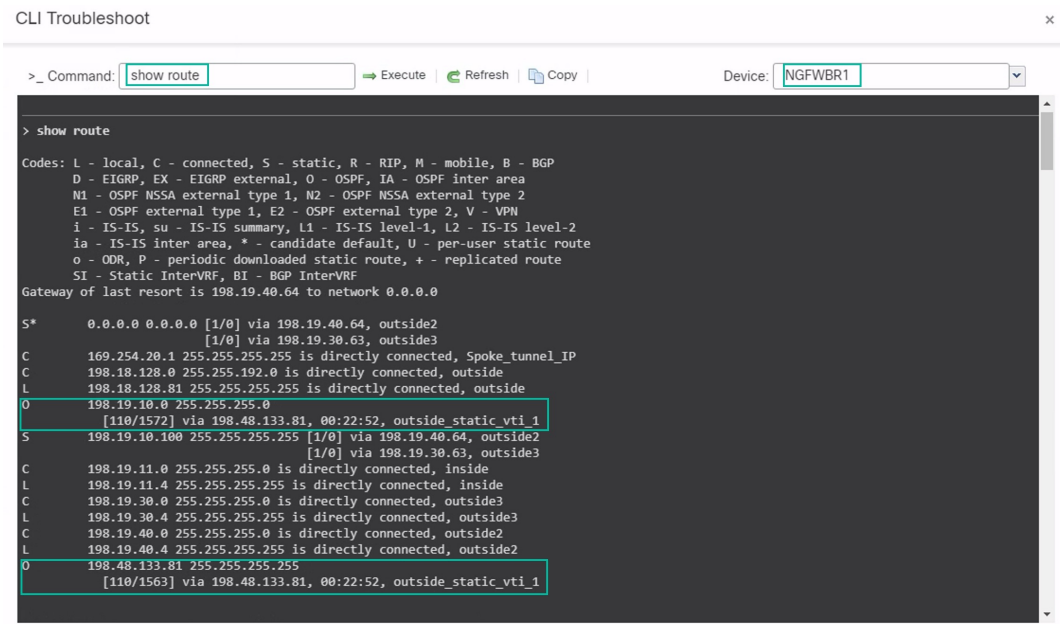
- **Verify Routing on the Hub and Branch Nodes**-To verify that the OSPF routes have been correctly learned on the **NGFW1** and **NGFWBR1.** nodes:

1. Choose **Devices** > **Device Management**.
2. To edit NGFW1, click the **Edit** (✎) icon.

3. Click the **Device** tab.
4. Click the **CLI** button in the **General** card. The **CLI Troubleshoot** window appears
5. Enter **show route** in the **Command** field and click **Execute** .
6. Review the routes on the NGFW1 node and confirm the VPN route for the spoke's VTI IP (169.254.20.1) and OSPF learnt route for the Branch_LAN (198.19.11.0/24) as displayed in the figure below.

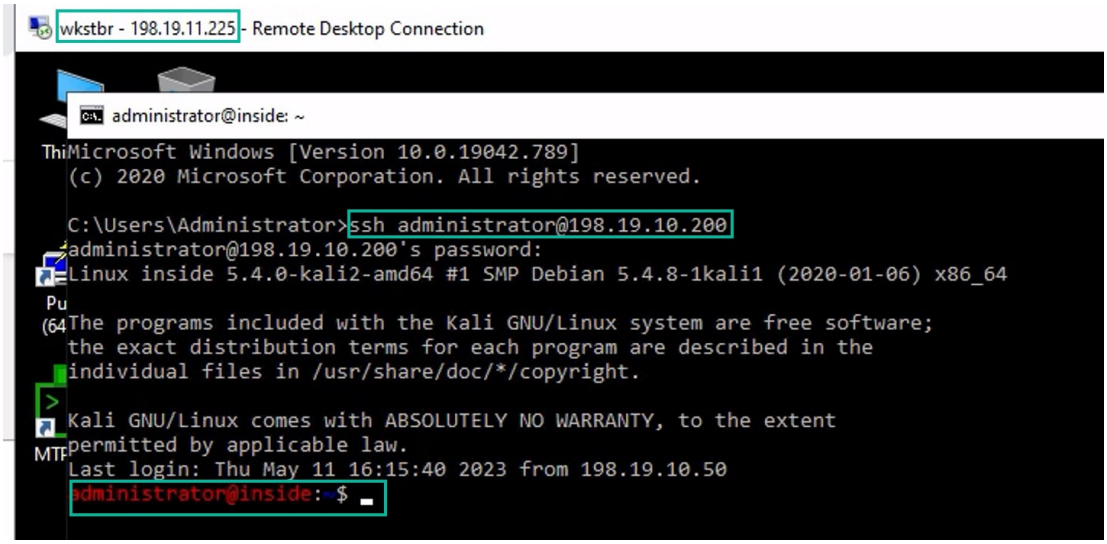


7. Repeat Steps 2 through 5 for the NGFWBR1 node.
8. Review the routes on the NGFWBR1 node. Confirm the OSPF routes learnt for the hub's VTI IP (198.48.133.81) and for the Corporate_LAN (198.19.10.0/24) as displayed in the figure below.



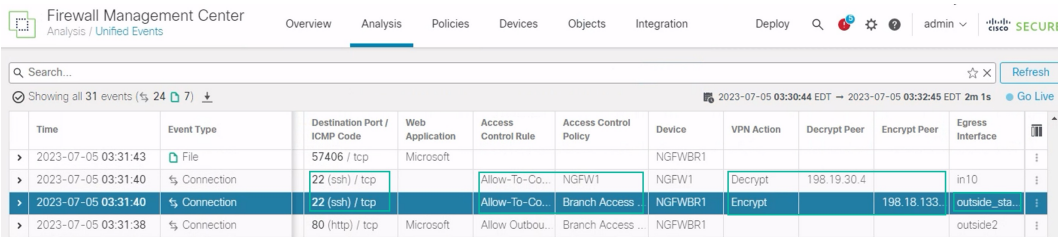
- **Verify Traffic between Protected Networks Behind the Spoke and Hub Nodes**

  Log into the WKST BR workstation (198.19.11.225) and SSH to the host (198.19.10.200) behind NGFW1. Ensure that you are able to SSH successfully to the host.



- **Verify Connectivity Between Branch and Spoke Nodes Using Unified Events**

  1. Choose **Analysis > Unified Events**.
  2. Add the **VPN Action, Encrypt Peer, Decrypt Peer**, and **Egress Interface** columns using the column picker.
  3. Reorder and resize the new columns along with the columns, **Destination Port/ICMP Code, Access Control Rule, Access Control Policy**, and **Device** as seen in the figure below.



4. To view the events related to the SSH connection from the **WKST BR** to **Corporate Host** choose the row with **22 (ssh/tcp)** in the **Destination Port/ICMP Code** column. Note the **Encrypt** action on **NGFWBR1** over the **outside_static_vti_1** interface followed by the **Decrypt** action on the **NGFW1** as shown in the figure above.

Configure the Backup VTI Interface on the Spoke Node

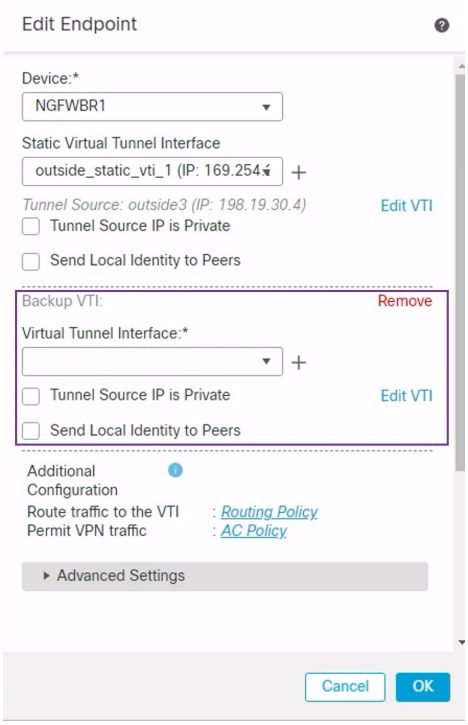
Secure Firewall Threat Defense supports the configuration of a backup tunnel for the route-based (VTI) VPN. When the primary VTI is unable to route the traffic, the traffic in the VPN is tunneled through the backup VTI.

Procedure

Step 1 Choose **Devices** > **Site-to-site VPN** to view the configured Corporate-VPN VPN topology and click the **Edit** (✎) icon. The Edit VPN Topology window appears.

Step 2 In the Spoke Nodes section, click the **Edit** (✎) icon for the **NGFWBR1** node. The **Edit Endpoint** dialog box appears.

Step 3 Click the **Add Backup VTI** link to add the secondary VTI tunnel. The link displays the Backup VTI section.



Step 4 Click **+** next to the **Virtual Tunnel Interface** drop-down list to add a new VTI.

The **Add Virtual Tunnel Interface** dialog box appears with the following pre-populated default configurations.

- **Tunnel Type** is auto-populated with **Static**.
- **Name** is auto-populated as <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*>. For example, **outside_static_vti_2** .
- The **Enabled** checkbox is checked by default.
- Select **Tunnel_Zone** from the Security Zone drop-down list.
- **Tunnel ID** is auto-populated with a value as 2.
- Select **GigabitEthernet0/3 (outside2)** from the **Tunnel Source** drop-down list. Select the IP address of the outside 3 interface as **198.19.40.4** from the drop-down list next to it.
- **IPsec Tunnel Mode** is set to IPv4, by default.
- **IP address** can either be a static IP address or a borrow IP. We recommend that you configure the Borrow IP for the static interface from a loopback interface. To add a loopback interface, click select **Loopback 1(Spoke_Tunnel_IP)** from the drop-down list.

Click **OK** to save the VTI. A message is displayed that confirms the VTI is created successfully. Click **OK**.

The Backup VTI Interface is set to **outside_static_vti_2(169.254.20.1)**.

Step 5 Click **OK** to save the spoke configuration.

Step 6 Click **Save** to save the VPN topology.

Configure an ECMP Zone for the Primary and Secondary VTI Interfaces

Configure ECMP on the primary and secondary static VTI interfaces on the branch node for link redundancy and for load balancing the VPN traffic.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Threat Defense device (**NGFWBR1**).

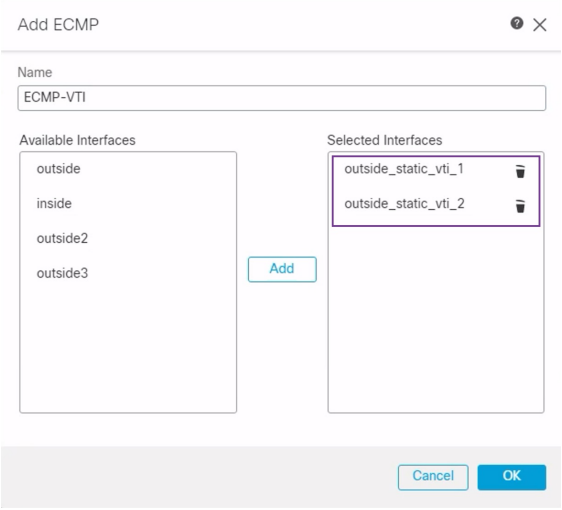
Step 2 Click the **Routing** tab on the interface view of NGFWBR1.

Step 3 Click **ECMP**.

Step 4 Click **Add**.

Step 5 In the **Add ECMP** box, enter a name, **ECMP-VTI** for the ECMP zone.

Step 6 To associate interfaces, select the interfaces **outside_static_vti_1** and **outside_static_vti_2** under the **Available Interfaces** box, and then click **Add**.



Step 7 Click **OK**.

The ECMP page now displays the newly created ECMP zone.

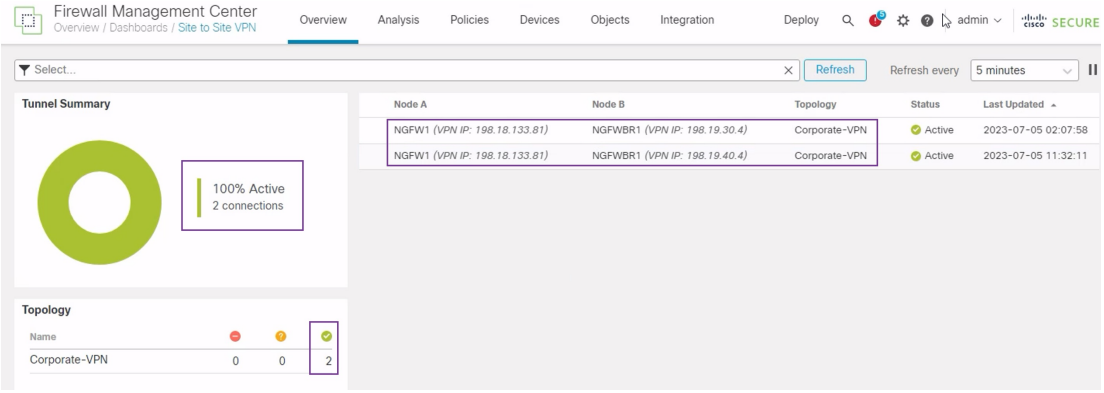
Step 8 Click **Save**.

Verify the Primary and Secondary Tunnels

Verify that both the primary and secondary VTI tunnels between the branch node and the hub node are configured, up, and active.

- **Verify Tunnel Status on the Site-to-site VPN Dashboard**

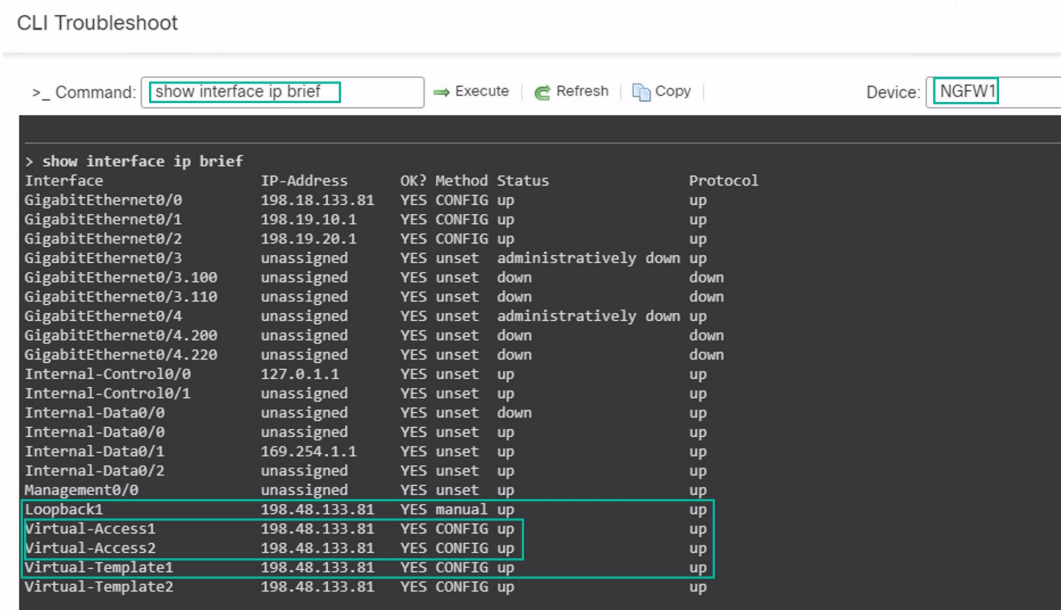
  To verify that the VPN tunnel is up and green, choose **Overview** > **Dashboards** > **Site-to-site VPN**.



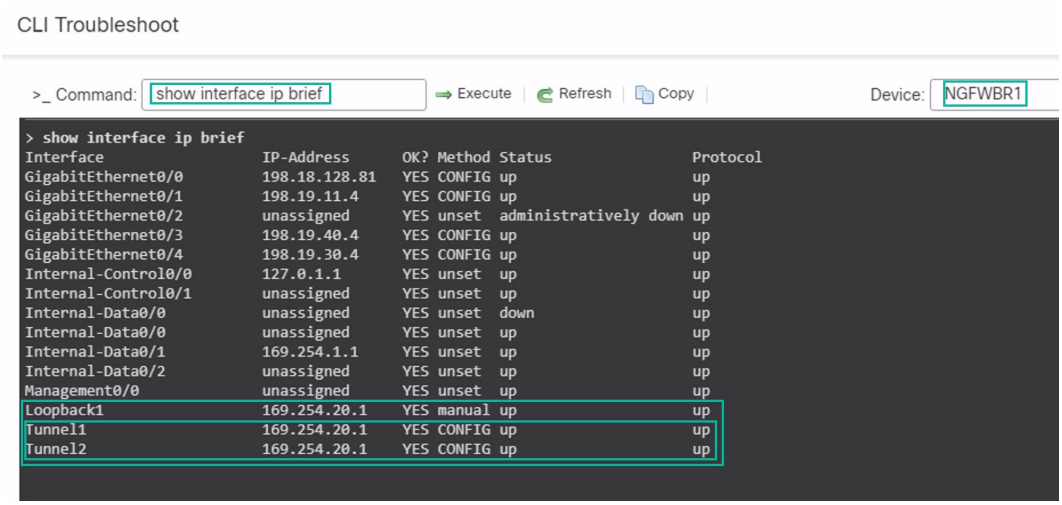
- **Verify Routing on the Hub and Branch Nodes**

  1. Choose **Devices** > **Device Management**.
  2. To edit NGFW1, click the Edit icon.
  3. Click the **Device** tab.
  4. Click the **CLI** button in the **General** card. The **CLI Troubleshoot** window appears
  5. Enter **show interface ip brief** in the **Command** field and click **Execute** to view the dynamic Virtual Access interfaces that were created from the DVTI on the hub.

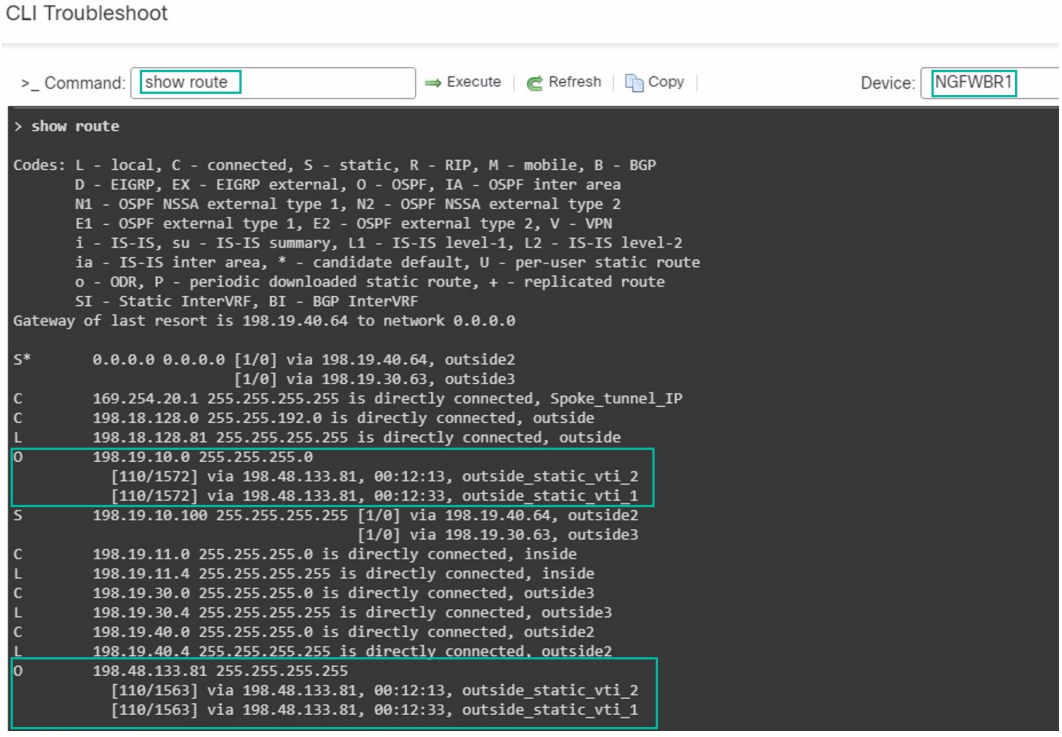
Note The Virtual-Access2 interface gets generated from the same DVTI when **NGFWBR1** connects to NGFW1 over the secondary VTI connection.



6. Repeat Steps 2 through 5 for the NGFWBR1 node to view the static VTI interfaces **Tunnel1** and **Tunnel2** as shown in the figure below.



7. Enter **show route** in the **Command** field and click **Execute** to view the routes after the addition of the secondary VTI tunnel.



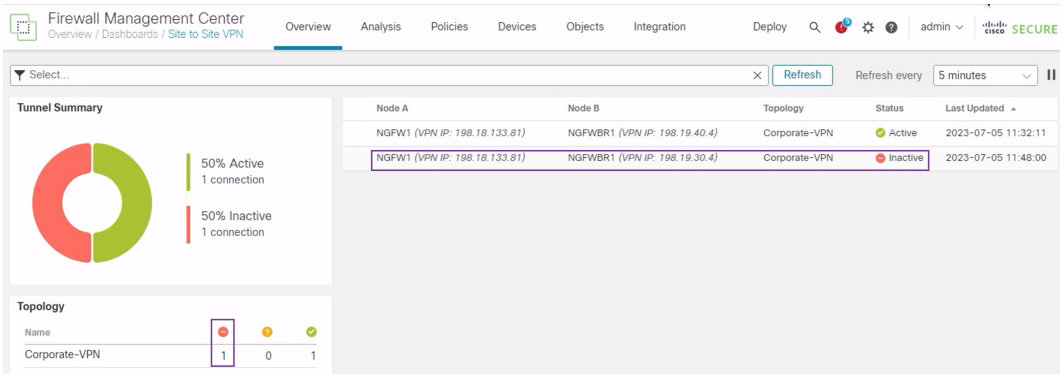
- Note that the **Corporate_LAN** (198.19.10.0/24) has been learnt over OSPF on both the primary (**outside_static_vti_1**) and secondary (**outside_static_vti_2**) VTIs.
- Note that the DVTI Tunnel IP (198.48.133.81) has also been learnt over OSPF on both the primary and secondary VTIs.

- **Verify Failover to Secondary Tunnel When the Primary Tunnel Goes Down**

1. In this example, to validate failover to the secondary tunnel, packet loss can be induced by restricting outbound traffic sourced from the outside3 interface going to internet either through an access control list on the upstream device or by shutting down the outside3 interface for threat defense from the management center.

Note Shutting down an interface is network intrusive and must not be tried in a production network.

2. In the Site-to-site VPN Dashboard, the primary tunnel is down as shown in the figure below.



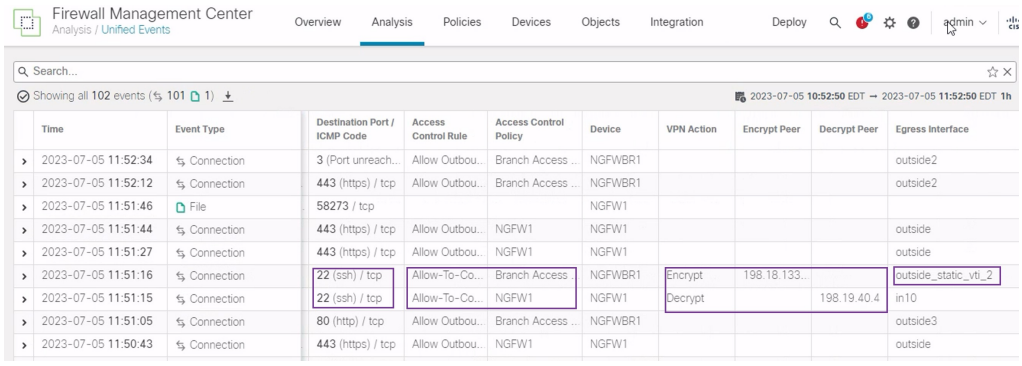
3. Initiate traffic from Branch to Hub. Log in to the WKST BR workstation and SSH to the host behind NGFW1. Ensure that you are able to SSH successfully to the host.

4. Verify the egress path of the traffic using the Unified Event Viewer:

   a. Choose **Analysis > Unified Events**.

   b. Add the **VPN Action, Encrypt Peer, Decrypt Peer**, and **Egress Interface** columns using the column picker.

   c. Reorder and resize the new columns along with the columns, **Destination Port/ICMP Code, Access Control Rule, Access Control Policy**, and **Device** as seen in the figure below.



   Notice that the egress interface on the **NGFWBR1** for the SSH (Port 22) is now displayed as the secondary interface (**outside_static_vti_2**).

Troubleshoot Route-based VPN Tunnels

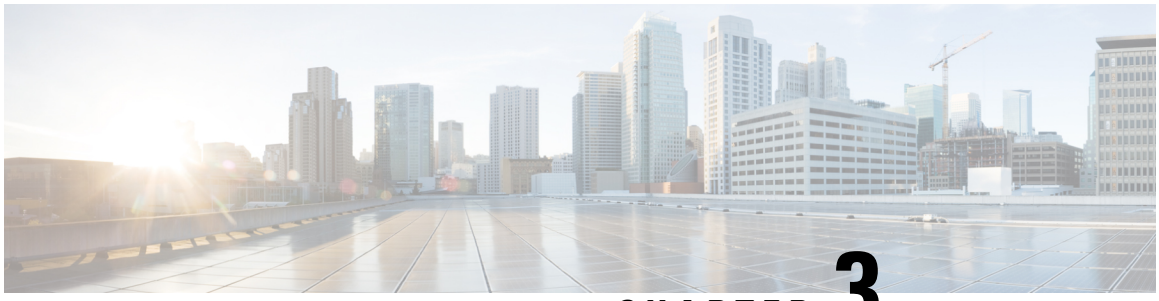
After the deployment, use the following CLI to debug issues related to route-based VPN tunnels on Secure Firewall Threat Defense.

Note Proceed with caution when you run debug commands on the threat defense device in production environments.You can set various debug levels on the device that may have verbose outputs.

How to...	CLI Command
Enable conditional debugging for a particular peer	**debug crypto condition peer <peer-IP>**
Debug the Virtual Tunnel Interface information	**debug vti 255**
Debug the IKEv2 protocol related transactions	**debug crypto ikev2 protocol 255**
Debug the IKEv2 platform related transactions	**debug crypto ikev2 platform 255**
Debug the common IKE related transactions	**debug crypto ike-common 255**
Debug the IPSec related transactions	**debug crypto ipsec 255**

Additional Resources

Resource	URL
Secure Firewall Threat Defense Release Notes	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
All New and Deprecated Features	http://www.cisco.com/go/whatsnew-fmc
Secure Firewall on Cisco.com	http://www.cisco.com/go/firewall
Secure Firewall on YouTube	https://www.youtube.com/cisco-netsec
Secure Firewall Essentials	https://secure.cisco.com/secure-firewall



CHAPTER 3

Route Application Traffic from the Branch to the Internet Using Direct Internet Access (DIA)

In this chapter, we delve into the practical application of Direct Internet Access (DIA) using two use cases. Each use case details the scenario, network topology, best practices, and prerequisites. It also provides a comprehensive end-to-end procedure for seamless implementation.

Direct Internet Access

Digital innovation is transforming the way businesses operate, communicate, and interact with customers. It has led to the creation of new applications and technologies to improve collaboration and customer experience and require high bandwidth and low latency connections.

Challenges with Traditional Networks

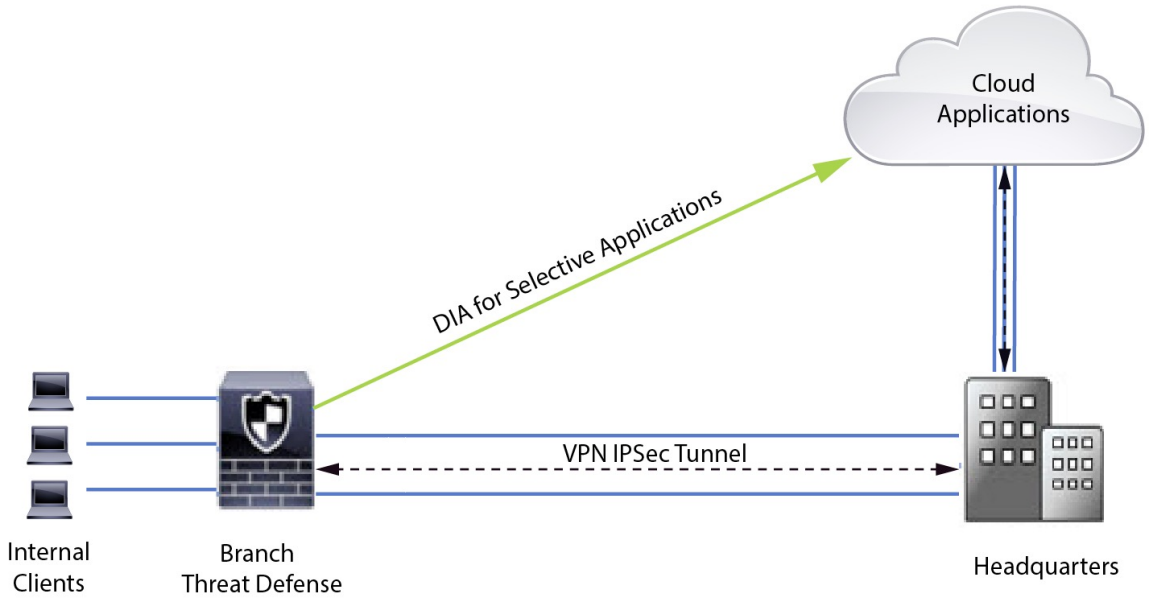
Traditionally, network deployments leverage a perimeter firewall on a central site to provide secure access to local and branch users. This architecture provides the desired connectivity, though it transports all internet traffic to the central site as encrypted traffic through a VPN tunnel resulting in packet latency, drops, and jitter. In addition, the network is constantly challenged with high costs and bandwidth utilization that is associated with deployment and complex network management.

Solution

One of the ways to overcome these challenges is to use Direct Internet Access (DIA). DIA is a component of the Simplified Branch feature of the Cisco Secure Firewall. DIA uses Policy Based Routing (PBR). DIA is also referred to as application aware routing.

In a DIA topology, application traffic from the branch office is routed directly to the internet thereby bypassing the latency of tunneling internet-bound traffic to the headquarters. The branch Secure Firewall Threat Defense is configured with an internet exit point. The PBR policy is applied on the ingress interface to identify the traffic based on the applications defined in the extended access control list. Correspondingly, the traffic is forwarded through the egress interfaces directly to the internet.

Figure 1: Direct Internet Access Through Specific Egress Interfaces



Why Policy based Routing?

You can use PBR to classify and securely break out traffic for specified applications. It also allows you to specify a path for certain traffic. You can configure a PBR policy in the Secure Firewall Management Center user interface to allow the applications to be directly accessed.

PBR and Path Monitoring

Typically, in PBR, traffic is forwarded through egress interfaces based on the priority value (interface cost) configured on them. In Secure Firewall Management Center version 7.2 and later versions, PBR uses path monitoring to collect performance metrics (RTT, jitter, packet loss, and MOS) of the egress interfaces. PBR uses these metrics to determine the best path (egress interface) for forwarding the traffic. Path monitoring periodically notifies PBR about the monitored interface when the metrics get modified. PBR retrieves the latest metric values for the monitored interfaces from the path monitoring database and updates the data path.

You must enable path monitoring for the interface, configure the monitoring type for the egress interface, and configure the application traffic to leverage path monitoring that uses the metrics values.

To understand path monitoring, see Scenario 2: Direct Internet Access With Path Monitoring, on page 37.

Benefits

Benefits of using DIA include

- Improved internet speeds and branch office user experience.
- Reduced complexity, making network management easier and cheaper.
- Cost-effective as it reduces bandwidth usage and eliminates the need for expensive hardware.
- Dynamic path selection using real-time metrics.
- Best egress path guaranteed without manual intervention.
- Continuous monitoring of link health and network state.
- Increased agility, allowing organizations to adapt quickly to changing business needs.

Is This Use Case For You?

The intended audience for this use case is network design engineers, network operations personnel, and security operations personnel who wish to implement Direct Internet Access within each remote site to allow local breakout of internet-bound traffic directly from the branch.

Components for Direct Internet Access

Some of the important components that the branch firewall uses for DIA are :

- **Trusted DNS Server**—Application detection in DIA feature relies on DNS snooping to resolve applications or a group of applications. To ensure that DNS requests are not resolved by rogue DNS servers and are indeed locked to the desired DNS servers, the management center allows you to configure a Trusted DNS server for Threat Defense.
- **Interface Priority**—Cisco Secure Firewall uses interface priority to determine the optimal internet path. Priority, lower the better, determines the preference of a particular ISP when sending the traffic out to the internet. The management center allows you to configure the interface priority for Threat Defense.
- **Network Service**—Object associated with a particular application that is used within policy based routing. This object is automatically created.
- **Network Service Group (NSG)**—Network Service Groups are a group of applications that the firewall uses to determine the path based on the configuration. Multiple network service objects can be part of a single NSG. The management center auto generates NSGs based on the extended access lists configured for policy based routing.

Best Practices

- Secure Firewall Threat Defense must run version 7.1 and higher.
- Trusted DNS servers must be configured to ensure DNS snooping is performed through trusted DNS servers to support application traffic flow.
- DNS requests passing through Threat Defense must be in a clear-text format and not encrypted to allow DNS snooping to facilitate PBR flows.
- ECMP zones must be configured for active/active load balancing of application traffic.
- ECMP is supported only in the routed firewall mode and a device can have a maximum of 256 ECMP zones.
- Only routed interfaces must be used. Each interface must belong to only a single ECMP zone.
- Make sure that interfaces belong to the virtual router where ECMP is being configured.
- Interfaces used in the ECMP zone configuration must have logical names defined within the interface configuration.
- Validate that no more than eight interfaces per ECMP zone are configured for PBR on Secure Firewall Threat Defense.
- Secure Firewall Threat Defense must not be deployed in a cluster because PBR is not supported in this mode.
- PBR must be configured for the global virtual router as it is not supported on user-defined virtual routers.
- Ensure that interfaces used in ingress and egress interface within PBR are either routed interfaces or non management-only interfaces and they belong to the global virtual router.

Prerequisites

- Complete the Threat Defense Initial Configuration Using the Device Manager
- Assign Licenses to Devices
- Add routes for internet access. See Add a Static Route
- Configure NAT for Threat Defense
- Creating a Basic Access Control Policy

Scenario 1: Direct Internet Access

Bob is an account manager and Ann is a help desk specialist. Both work at a branch office of a large corporation. Recently, they have been experiencing latency issues while using web conferencing tools like Webex and streaming platforms like YouTube.

What is at risk?

Network latency and network congestion results in reduced performance and user experience of web conferencing and streaming sessions. This may impact the productivity and efficiency of employees at the branch office, potentially leading to a negative impact on the overall business operations.

How does DIA with PBR solve the problem?

Alice, the IT administrator, used policy based routing in conjunction with DIA to reduce latency in the network.

Direct Internet Access allowed branch offices to access the internet directly, without routing traffic through a central site or data center. This reduced latency by providing a more direct and optimized internet connection for branch users.

Policy based routing separated Webex and YouTube traffic on different egress interfaces. This ensured that the traffic was directed through different paths, reducing the burden on a single interface and improving application performance.

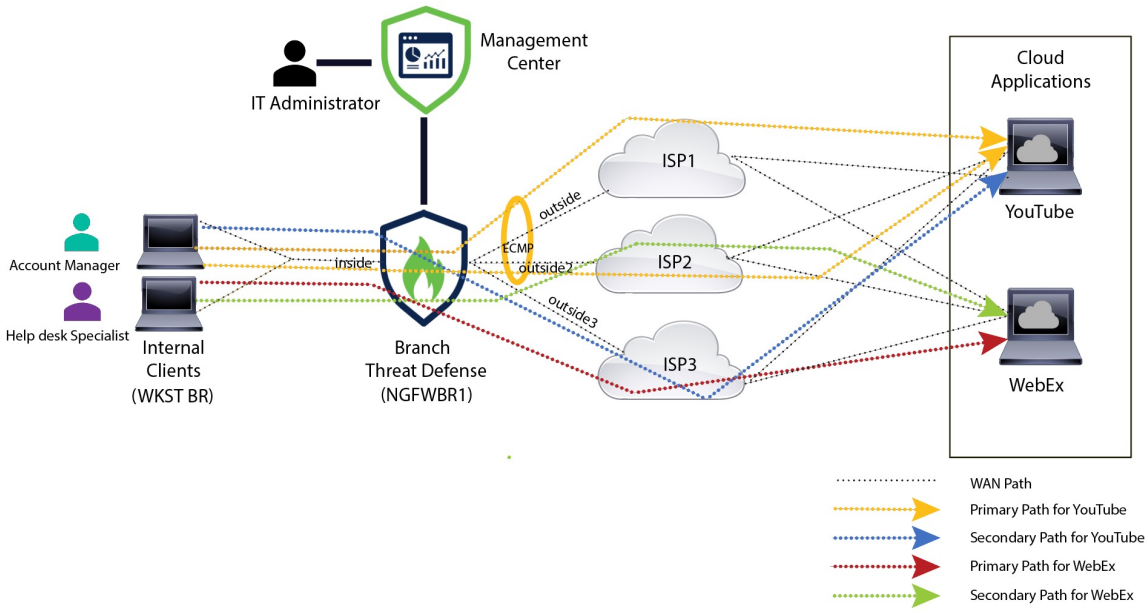
Network Topology for DIA

In this topology, a threat defense device is deployed at a branch location with three egress interfaces. The device is configured for DIA using PBR.

In the figure below, the internal client or branch workstation is labelled **WKST BR** and the branch threat defense is labeled **NGFWBR1**. The ingress interface of **NGFWBR1** is named **inside** and the egress interfaces are named **outside**, **outside2**, and **outside3** respectively.

Load balancing between the **outside** and **outside2** interfaces is achieved by configuring an ECMP zone and static routes.

Figure 2: Direct Internet Access Topology



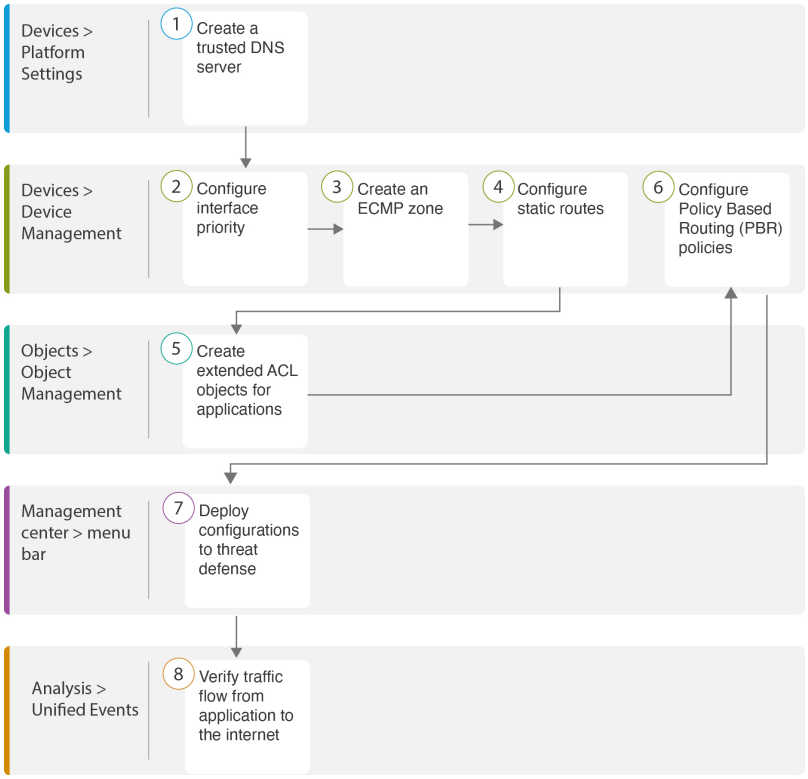
With DIA, users behind the branch firewall are allowed to access:

1. Social media application traffic (for example, **YouTube**) that is load balanced using two egress interfaces (**outside** and **outside2**). If both the interfaces fail, then traffic falls back to the third egress interface (**outside3**).

2. Collaboration application traffic (for example, **WebEx**) is forwarded through the **outside3** interface and if this link fails, traffic is forwarded through the **outside2** interface.

End-to-End Procedure for Configuring DIA

The following flowchart illustrates the workflow for configuring DIA in Secure Firewall Management Center.



Step	Description
1	(*Prerequisite*) Configure a Trusted DNS server. See Configure a Trusted DNS Server, on page 40.
2	(*Prerequisite*) Configure interface priority. See Configure Interface Priority, on page 41.
3	(*Prerequisite*) Create an ECMP zone. See Create an ECMP Zone, on page 41.
4	(*Prerequisite*) Configure static routes. See Configure an Equal Cost Static Route, on page 42.
5	Configure extended ACL objects for applications. See • Configure an Extended ACL Object for YouTube, on page 43 • Configure an Extended ACL Object for WebEx, on page 43

Step	Description
6	Configure PBR policies for applications. See • Configure a Policy Based Routing Policy for YouTube, on page 44 • Configure a Policy Based Routing Policy for WebEx, on page 45
7	Deploy the configuration on threat defense. See Deploy Configuration, on page 47.
8	Verify YouTube and WebEx traffic flow. See Verify Application Traffic Flow, on page 47.

Scenario 2: Direct Internet Access With Path Monitoring

Ann is a help desk specialist and works at a branch office of a large corporation. Ann has been experiencing connection drops and lags while using WebEx.

What is at risk?

WebEx meetings rely on real-time data transmission, including audio and video streams, between the meeting host and attendees. This real-time data is sensitive to network latency and packet loss. If the network experiences high packet loss, it can lead to audio and video quality issues such as freezing, lagging, or delays, which can negatively impact the meeting experience.

How PBR with path monitoring resolve the problem?

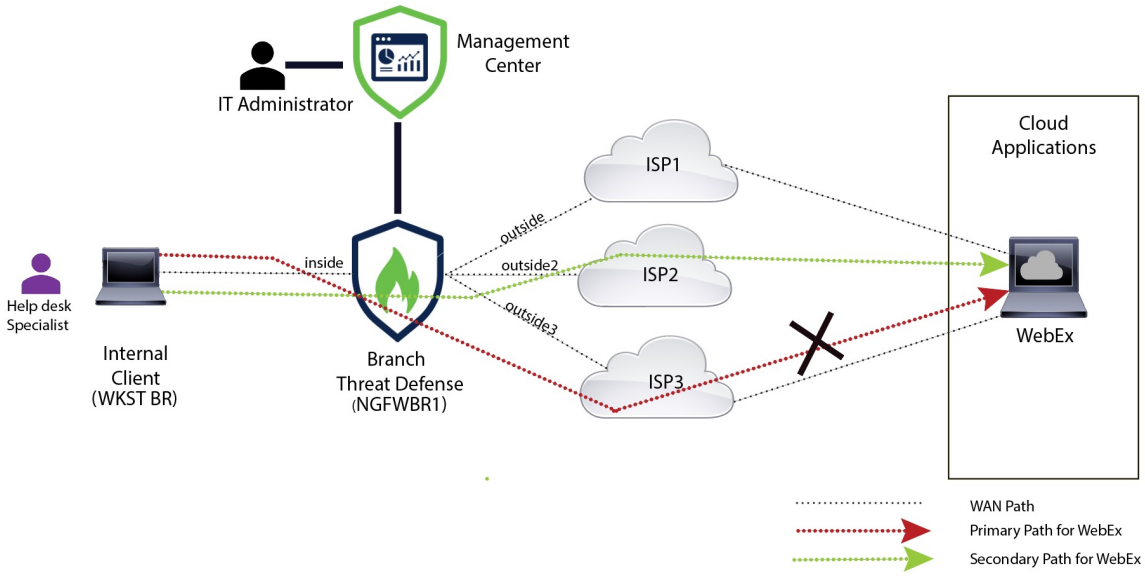
Alice, the IT administrator, used policy based routing with path monitoring to steer WebEx application traffic to the internet through the egress interface with minimal packet loss ensuring the best possible meeting experience for attendees.

Network Topology-DIA With Path Monitoring

In this topology, a threat defense device is deployed at a branch location with three egress interfaces. The device is configured for Direct Internet Access using Policy Based Routing.

In the figure below, the internal client or branch workstation is labeled **WKST BR** and the branch threat defense is labeled **NGFWBR1**. The ingress interface of **NGFWBR1** is named **inside** and the egress interfaces are named **outside**, **outside2**, and **outside3** respectively.

Figure 3: Direct Internet Access Topology (With Path Monitoring)



The **outside2**, and **outside3** egress interfaces are enabled with path monitoring. The PBR policy for WebEx is configured so that traffic is routed to the egress interface with minimal packet loss.

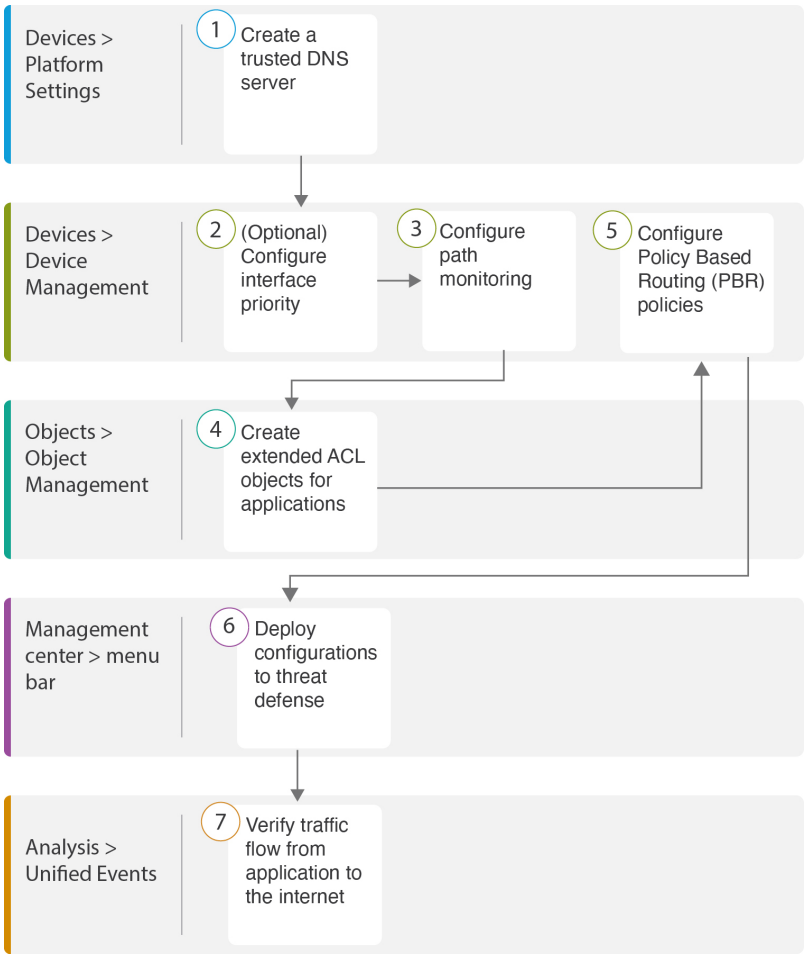
In this scenario, to validate path monitoring, packet loss can be induced by restricting outbound traffic that is sourced from the **outside3** interface going to internet either through an access control list on the upstream device or by shutting down the **outside3** interface for Secure Firewall Threat Defense from Firewall Management Center.

Note Shutting down an interface is network intrusive and must not be tried in a production network.

As a result of packet loss, the link that is associated with the **outside3** interface goes down. Collaboration application traffic is forwarded through the **outside2** interface instead of the **outside3** interface.

End-to-End Procedure for Configuring DIA With Path Monitoring

The following flowchart illustrates the workflow for configuring DIA with path monitoring in Secure Firewall Management Center.



Step	Description
1	(*Prerequisite*) Configure a Trusted DNS server. See Configure a Trusted DNS Server, on page 40.
2	[*Prerequisite (Optional)*] Configure interface priority. See Configure Interface Priority, on page 41.
3	Configure path monitoring. See Configure Path Monitoring Settings, on page 42.
4	Configure an extended ACL object for the application. See Configure an Extended ACL Object for WebEx, on page 43.
5	Configure a PBR policy for the application. See Configure a Policy Based Routing Policy With Path Monitoring for Webex, on page 46.
6	Deploy the configuration on threat defense. See Deploy Configuration, on page 47.
7	Verify WebEx traffic flow. See Verify Application Traffic Flow, on page 47.

Configure a Trusted DNS Server

Application detection in Direct Internet Access feature relies on DNS snooping to map the application domains to IPs in order to detect the application or a group of applications. To ensure that DNS requests are not resolved by rogue DNS servers and are indeed locked to desired DNS servers, Cisco Secure Firewall Management Center allows you to configure Trusted DNS Servers for Cisco Secure Firewall Threat Defense. Thus, the firewall only snoops the traffic that goes to trusted DNS servers. Apart from configuring the trusted DNS servers, you can include the already configured servers in DNS server group, DHCP pool, DHCP relay, and DHCP client as trusted DNS servers.

You can configure trusted DNS services for DNS snooping using the Trusted DNS Servers tab.

Note For an application-based PBR, you must configure trusted DNS servers. You must also ensure that the DNS traffic passes through threat defense in a clear-text format (encrypted DNS is not supported) so that domains can be resolved to detect applications.

Before you begin

- Ensure you have created one or more DNS server groups. For more information, see Creating DNS Server Group Objects.
- Ensure you have created interface objects to connect to the DNS servers.
- Ensure that the managed device has appropriate static or dynamic routes to access the DNS servers.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and edit a threat defense policy.

Step 2 Click the **Edit** ( ) icon.

Step 3 Click **DNS**.

Step 4 To configure the trusted DNS servers, click the **Trusted DNS Servers** tab.

Step 5 To choose **DNS_Server** from the existing host objects, under **Available Host Objects**, search for it using the search field, and click **Add** to include it to the **Selected DNS Servers** list.

Note
DNS_Server is the DNS server configured in this example.

Step 6 Click **Save**. The added DNS server is displayed in the **Trusted DNS Servers** page.

Step 7 Click **Policy Assignments** to ensure **NGFWBR1** is already in the **Selected Devices** list.

Step 8 Click **OK** to confirm the changes.

Step 9 Click **Save** to write the changes for platform settings.

Configure Interface Priority

Cisco Secure Firewall Threat Defense uses interface priority to determine the optimal internet path. Priority ranges from 0 to 65535, and determines the preference of a particular ISP when sending the traffic out to the internet. The traffic is forwarded based on the priority of the interfaces. Traffic is routed to the interface with the least priority value first. When an interface is not available, traffic is forwarded to the interface with the next lowest priority value. For example, let us assume that outside2 and outside3 are configured with priority values 10 and 20 respectively. The traffic is forwarded to outside2. If outside2 becomes unavailable, the traffic is then forwarded to outside3.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab on the interface view of NGFWBR1.

Step 3 Click **Policy Based Routing**.

Step 4 Click **Configure Interface Priority**.

Step 5 In the dialog box, provide the priority number against the interfaces.

When the priority value is the same for all the interfaces, the traffic is balanced among the interfaces.

Step 6 Click **Save**.

Create an ECMP Zone

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab on the interface view of NGFWBR1.

Step 3 Click **ECMP**.

Step 4 Click **Add**.

Step 5 In the **Add ECMP** box, enter a name, **ECMP-WAN** for the ECMP zone.

Step 6 To associate interfaces, select the interface under the **Available Interfaces** box, and then click **Add**.

Step 7 Click **OK**.

The ECMP page now displays the newly created ECMP zone.

Step 8 Click **Save**.

Configure an Equal Cost Static Route

You can assign interfaces of a virtual router, both global and user-defined, to an ECMP zone for the device.

Before you begin

- To configure an equal cost static route for an interface, ensure to associate it with an ECMP zone. See Create an ECMP Zone, on page 41.
- You cannot define a static route for interfaces with same destination and metric without associating the interfaces with an ECMP zone.

Procedure

Step 1 From the **Devices** > **Device Management** page and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab.

Step 3 From the drop-down list, select the virtual router whose interfaces are associated with an ECMP zone.

Step 4 To configure the equal cost static route for the interfaces, click **Static Route**.

Step 5 Click **Add Route** to add a new route, or click **Edit** (✎) for an existing route.

Step 6 From the **Interface** drop-down, select the interface belonging to the virtual router and an ECMP zone.

Step 7 Select the destination network from the **Available Networks** box and click **Add**.

Step 8 Enter a gateway for the network.

Step 9 Enter a metric value. It can be a number that ranges between 1 and 254.

Step 10 To save the settings, click **Save**.

Step 11 To configure equal cost static routing, repeat the steps to configure the static route for another interface in the same ECMP zone with the same destination network and metric value. Remember to provide a different gateway.

Configure Path Monitoring Settings

The PBR policy relies on flexible metrics, such as round trip time (RTT), jitter, mean opinion score (MOS), and packet loss of the interfaces to identify the best routing path for its traffic. Path monitoring collects these metrics on the specified interfaces. On the **Interfaces** page, you can configure interfaces with settings for path monitoring to send the probes for metrics collection.

Procedure

Step 1 Select **Devices** > **Device Management** and click **Edit** (✎) for the threat defense device (**NGFWBR1**).

Step 2 Click **Edit** (✎) for the interface you want to edit (**outside**).

Step 3 Click the **Path Monitoring** tab.

Step 4 Check the **Enable IP based Path Monitoring** check box.

Step 5 From the **Monitoring Type** drop-down list, select the relevant option. In this example, we use the default value, **Next-hop of default route out of interface (Auto)**.

Step 6 Click **Ok**.

Step 7 Repeat Steps 2 through 8 for the **outside2** and **outside3** interfaces.

Step 8 Click **Save**.

Configure an Extended ACL Object for YouTube

The access list is configured for YouTube traffic to be steered towards the internet from different egress interfaces with the help of policy based routing.

Procedure

Step 1 Select **Objects** > **Object Management** and choose **Access Lists** > **Extended** from the table of contents.

Step 2 Click **Add Extended Access List** to create an extended access list for social media traffic.

Step 3 In the Extended ACL Object dialog box, enter a name (**DIA_SocialMedia**) for the object.

Step 4 Click **Add** to create a new Extended Access List.

Step 5 Configure the following access control properties:

a. Select the **Action** to Allow (match) the traffic criteria.

b. Click the **Application** tab and search for **YouTube** in the **Available Applications** list.

c. Select **YouTube** and click **Add to Rule**.

d. Click **Add** to add the entry to the object.

e. Click **Save**.

Configure an Extended ACL Object for WebEx

The access list is configured for WebEx traffic to be steered towards the internet from different egress interfaces with the help of policy based routing.

Procedure

Step 1 Select **Objects** > **Object Management** and choose **Access Lists** > **Extended** from the table of contents.

Step 2 Click **Add Extended Access List** to create an extended access list for collaboration traffic.

Step 3 In the Extended ACL Object dialog box, enter a name (**DIA_Collaboration**) for the object.

Step 4 Click **Add** to create a new Extended Access List.

Step 5 Configure the following access control properties:

a. Select the **Action** to Allow (match) the traffic criteria.

b. Click the **Application** tab and search for **Webex** in the **Available Applications** list.

c. Select **Webex** and click **Add to Rule**.

d. Click **Add** to add the entry to the object.

e. Click **Save**.

Configure a Policy Based Routing Policy for YouTube

You can configure the PBR policy in the Policy Based Routing page by specifying the ingress interfaces, match criteria (Extended Access Control List), and egress interfaces to route YouTube traffic.

The YouTube traffic is load balanced between the **outside** and **outside2** interfaces and falls back to the **outside3** if both the links fail.

Procedure

Step 1 Select **Devices** > **Device Management**, and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab on the interface view of NGFWBR1.

Step 3 Click **Policy Based Routing**.

The Policy Based Routing page displays the configured policy. The grid displays the list of ingress interfaces and a combination of the policy-based route access list, and egress interfaces.

Step 4 To configure the policy, click **Add**.

Step 5 In the **Add Policy Based Route** dialog box, select **inside** from the **Ingress Interface** drop-down list.

Note
Only interfaces that have logical names and that belong to a global virtual router are listed in the drop-down.

Step 6 To specify the match criteria and the forward action in the policy, click **Add**.

Step 7 In the **Add Forwarding Actions** dialog box, do the following:

a) From the **Match ACL** drop-down, choose **DIA_SocialMedia**.

b) To select the configured interfaces, choose **Egress Interfaces** from the **Send To** drop-down list.

c) Choose **By Priority** from the **Interface Ordering** drop-down list.

Traffic is routed to the interface with the least priority value first. When the interface is not available, the traffic is then forwarded to the interface with the next lowest priority value. For example, let us assume that outside2 and outside3 are configured withpriority values 10 and 20 respectively. The traffic is forwarded to outside2. If outside2 becomes unavailable, the traffic is then forwarded to outside3.

d) In the **Available Interfaces** box, all the interfaces with their priority values are listed. Click the **Add** (+) icon to add the selected egress interface.

For our scenario:

1. From Available Interfaces, click the **Add** (+) icon adjacent to **outside** and **outside2** interfaces to move it to **Selected Egress Interfaces**.
2. Then click the **Add** (+) icon adjacent to **outside3** interface to move it to **Selected Egress Interfaces**.

e) Click **Save** to write the changes for the match criteria.
f) Review the configuration and click **Save** to write all the configuration changes for policy based routing.

Step 8 Click **Save**.

Configure a Policy Based Routing Policy for WebEx

You can configure the PBR policy in the Policy Based Routing page by specifying the ingress interfaces, match criteria (Extended Access Control List), and egress interfaces to route WebEx application traffic.

The WebEx application traffic is routed to **outside3** and falls back to the **outside2** if the primary link fails.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab on the interface view of NGFWBR1.

Step 3 Click **Policy Based Routing**.

The Policy Based Routing page displays the configured policy. The grid displays the list of ingress interfaces and a combination of the policy-based route access list, and egress interfaces.

Step 4 To edit the policy, click the **Edit** (✎) icon.

Step 5 To specify the match criteria and the forward action in the policy, click **Add**.

Step 6 In the **Add Forwarding Actions** dialog box, do the following:

a) From the **Match ACL** drop-down, choose **DIA_Collaboration**.
b) To select the configured interfaces, choose **Egress Interfaces** from the **Send To** drop-down list.
c) Choose **Order** from the **Interface Ordering** drop-down list.

The traffic is forwarded based on the sequence of the interfaces specified here.

d) In the **Available Interfaces** box, all the interfaces with their priority values are listed. Click the **Add** (+) icon to add the selected egress interface.

For our scenario:

1. From Available Interfaces, click the **Add** (+) icon adjacent to **outside3** interface to move it to **Selected Egress Interfaces**.

2. Then click the **Add** (+) icon adjacent to **outside2** interface to move it to **Selected Egress Interfaces**.

e) Click **Save** to write the changes for the match criteria.
f) Review the configuration and click **Save** to write all the configuration changes for policy based routing.

Step 7 Click **Save**.

Configure a Policy Based Routing Policy With Path Monitoring for Webex

You can configure the PBR policy with path monitoring in the Policy Based Routing page. In this example, WebEx application traffic is forwarded to the interface that has the least traffic loss.

Before you begin

To use the path monitoring metrics for configuring the traffic forwarding priority over egress interfaces, you must configure the path monitoring settings for the interfaces. See Configure Path Monitoring Settings, on page 42.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the threat defense device (**NGFWBR1**).
Step 2 Click the **Routing** tab on the interface view of NGFWBR1.
Step 3 Click **Policy Based Routing**.

The Policy Based Routing page displays the configured policy. The grid displays the list of ingress interfaces and a combination of the policy-based route access list, and egress interfaces.

Step 4 To configure the policy, click **Add**.
Step 5 In the **Add Policy Based Route** dialog box, select **inside** from the **Ingress Interface** drop-down list.

Note
Only interfaces that have logical names and that belong to a global virtual router are listed in the drop-down.

Step 6 To specify the match criteria and the forward action in the policy, click **Add**.
Step 7 In the **Add Forwarding Actions** dialog box, do the following:

a) From the **Match ACL** drop-down, choose **DIA_Collaboration**.
b) To select the configured interfaces, choose **Egress Interfaces** from the **Send To** drop-down list.
c) Choose **Minimal Packet Loss** from the **Interface Ordering** drop-down list.

The traffic is forwarded to the interface that has the minimal packet loss.

d) In the **Available Interfaces** box, all the interfaces are listed. From the list of interfaces, click the **Add** (+)icon to add the selected egress interface.

For our scenario:

1. From Available Interfaces, click the **Add** (+) icon adjacent to **outside3** interface to move it to **Selected Egress Interfaces**.
2. Then click the **Add** (+) icon adjacent to **outside2** interface to move it to **Selected Egress Interfaces**.

e) Click **Save** to write the changes for the match criteria.
f) Review the configuration and click **Save** to write all the configuration changes for policy based routing.

Step 8 Click **Save**.

Deploy Configuration

After you complete all the configurations, deploy them to the managed device.

Procedure

Step 1 On the management center menu bar, click **Deploy**.
Step 2 Check the checkbox adjacent to NGFWBR1 on which you want to deploy configuration changes.
Step 3 Click **Deploy**.
Step 4 If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Errors** or **Validation Warnings** window. To view complete details, click the Validation Errors or Validation Warnings link.

You have the following choices:

- Proceed with Deploy—Continue deploying without resolving warning conditions. You cannot proceed if the system identifies errors.
- Close—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

Verify Application Traffic Flow

Procedure

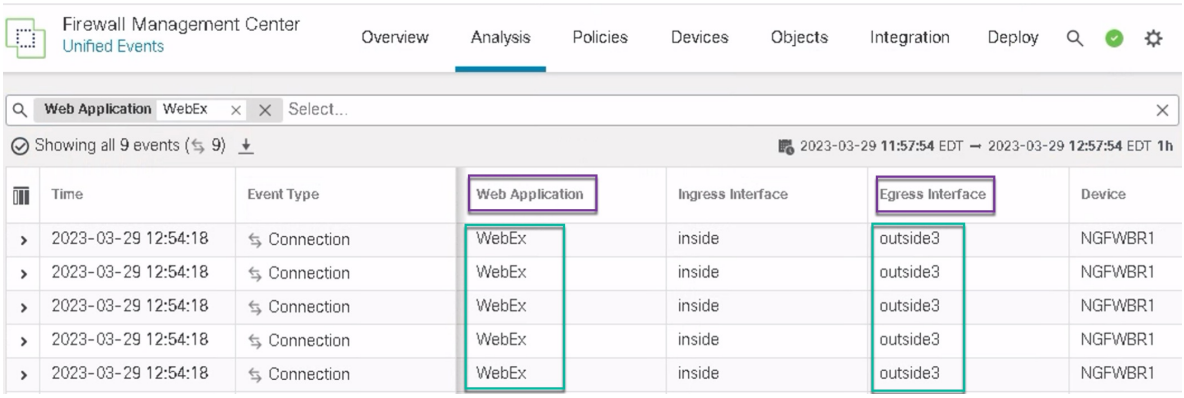
Step 1 In the management center interface, select **Analysis** > **Unified Events**.
Step 2 Customize the columns using the column picker by selecting the **Web Application** and **Egress Interface** and click **Apply**.
Step 3 Reorder the columns for ease of verification.
Step 4 Within the **Web Application** filter, enter the name **WebEx** and click **Apply** .
Step 5 Within the **Web Application** filter, enter the name **YouTube** and click **Apply** .

Step 6 Initiate traffic for the **YouTube** and **WebEx** applications on a host behind the Secure Firewall. In our scenario, launch the Google Chrome browser and navigate to https://youtube.com and https://webex.com in different tabs on the branch workstation **WKST BR1**.

Step 7 In the management center, verify the traffic flow for both the applications.

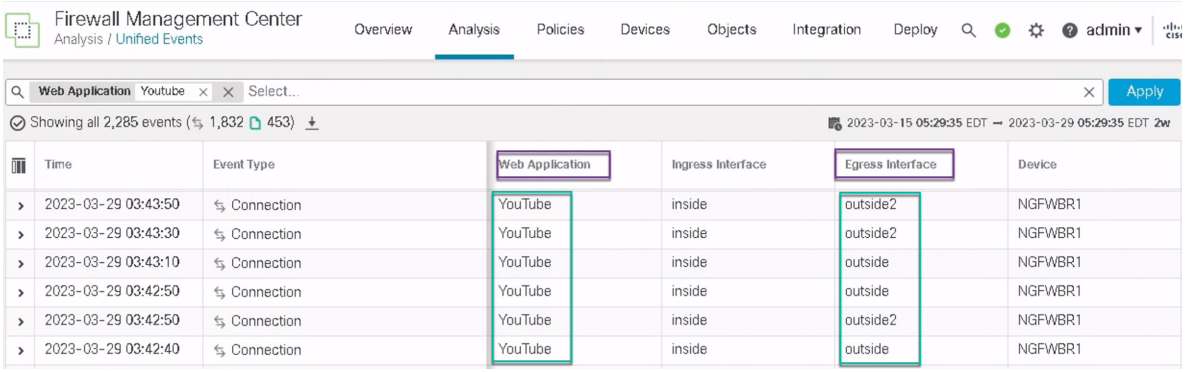
a. For DIA:

- **WebEx** application traffic is sent out through the **outside3** interface as per the configuration as seen in the figure below.



Time	Event Type	Web Application	Ingress Interface	Egress Interface	Device
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1

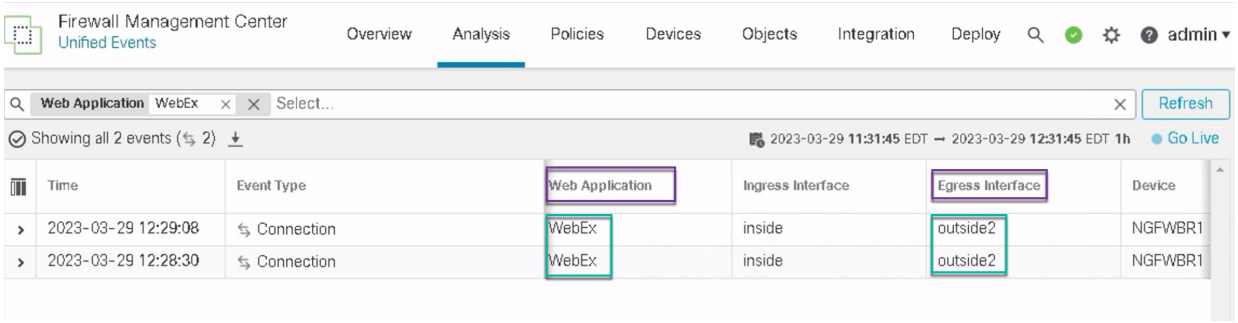
- **YouTube** application traffic is load balanced between the **outside** and **outside2** interfaces as per the configuration as seen in the figure below.



Time	Event Type	Web Application	Ingress Interface	Egress Interface	Device
2023-03-29 03:43:50	Connection	YouTube	inside	outside2	NGFWBR1
2023-03-29 03:43:30	Connection	YouTube	inside	outside2	NGFWBR1
2023-03-29 03:43:10	Connection	YouTube	inside	outside	NGFWBR1
2023-03-29 03:42:50	Connection	YouTube	inside	outside	NGFWBR1
2023-03-29 03:42:50	Connection	YouTube	inside	outside2	NGFWBR1
2023-03-29 03:42:40	Connection	YouTube	inside	outside	NGFWBR1

b. For DIA with path monitoring:

WebEx application traffic is sent out through the **outside2** interface as there is packet loss on the **outside3** interface as seen in the figure below.



Monitor and Troubleshoot Policy Based Routing

After the deployment, use the following CLI to monitor and troubleshoot issues related to policy based routing on Secure Firewall Threat Defense.

How ...	CLI Command
To log in to Secure Firewall Threat Defense Lina CLI	**system support diagnostic-cli**
To view the pre-defined network service objects that are pushed from the management center to threat defense during the deployment	• **show object network-service** • **show object network-service detail**
To view a particular network service object (NSG) related to configured applications	• **show object id YouTube** • **show object id WebEx**
To verify the network service group (NSG) pushed to Secure Firewall	**show run object-group network-service**
To view the route-map associated to policy based routing	**show run route-map**
To verify the interface configuration details like interface name and interface priority	**show run interface**
To verify the trusted DNS server configuration	**show dns**
To determine the path taken the traffic	**debug policy-route** **Important** Run the debug command with caution, especially in production environments as it may have verbose output based on the traffic.
To stop debugging the route	**undebug all**

To view the pre-defined network service objects, use the following command:

```
ngfwbr1# show object network-service
object network-service "ADrive" dynamic
 description Online file storage and backup.
 app-id 17
 domain adrive.com (bid=0) ip (hitcnt=0)
object network-service "Amazon" dynamic
 description Online retailer of books and most other goods.
 app-id 24
 domain amazon.com (bid=0) ip (hitcnt=0)
 domain amazon.jobs (bid=0) ip (hitcnt=0)
 domain amazon.in (bid=0) ip (hitcnt=0)
.
.
.
output snipped
.
.
.
object network-service "Logitech" dynamic
 description Company develops Computer peripherals and accessories.
 app-id 4671
 domain logitech.com (bid=0) ip (hitcnt=0)
object network-service "Lenovo" dynamic
 description Company manufactures/markets computers, software and related services.
 app-id 4672
 domain lenovo.com (bid=0) ip (hitcnt=0)
 domain lenovo.com.cn (bid=0) ip (hitcnt=0)
 domain lenovomm.com (bid=0) ip (hitcnt=0)
ngfwbr1#
```

To view specific network service objects such as YouTube and WebEx, use the following command:

```
ngfwbr1# show object id YouTube
object network-service "YouTube" dynamic
 description A video-sharing website on which users can upload, share, and view videos.
 app-id 929
 domain youtubei.googleapis.com (bid=592729) ip (hitcnt=0)
 domain yt3.ggpht.com (bid=709809) ip (hitcnt=102)
 domain youtube.com (bid=830871) ip (hitcnt=101)
 domain ytimg.com (bid=1035543) ip (hitcnt=93)
 domain googlevideo.com (bid=1148165) ip (hitcnt=466)
 domain youtu.be (bid=1247981) ip (hitcnt=0)
ngfwbr1# show object id WebEx
object network-service "WebEx" dynamic
 description Cisco's online meeting and web conferencing application.
 app-id 905
 domain files-prod-us-east-2.webexcontent.com (bid=182837) ip (hitcnt=0)
 domain webex.com (bid=290507) ip (hitcnt=30)
 domain avatar-prod-us-east-2.webexcontent.com (bid=452667) ip (hitcnt=0)
ngfwbr1#
```

To verify the NSG is pushed to Threat Defense, use the following command:

```
ngfwbr1# show run object-group network-service
object-group network-service FMC_NSG_292057776181
 network-service-member "WebEx"
object-group network-service FMC_NSG_292057776200
 network-service-member "YouTube"
ngfwbr1#
```

To verify the route map associated with PBR, use the following command:

```
ngfwbr1# show run route-map
!
route-map FMC_GENERATED_PBR_1678091359817 permit 5
```

```
 match ip address DIA_Collaboration
 set interface outside3 outside2

!
route-map FMC_GENERATED_PBR_1678091359817 permit 10
 match ip address DIA_SocialMedia
 set adaptive-interface cost outside outside2 outside3
!
ngfwbr1#
```

To verify the interface configuration and interface priority details, use the following command:

```
ngfwbr1# show run interface
!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
  zone-member ECMP-WAN
 ip address 198.18.128.81 255.255.192.0
 policy-route cost 10
!
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.11.4 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1678091359817
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 nameif outside2
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 zone-member ECMP-WAN
 ip address 198.19.40.4 255.255.255.0
 policy-route cost 10
!
interface GigabitEthernet0/4
 nameif outside3
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.30.4 255.255.255.0
 policy-route cost 20
!
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
 security-level 0
 no ip address
ngfwbr1#
```

To verify the trusted DNS configuration, use the following command:

```
ngfwbr1# show dns

DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 198.19.10.100: <ifc-not-specified> : N/A
Trusted Source Configured: 198.19.10.100: <ifc-not-specified> : N/A
DNS snooping IP cache: 0 in use, 37 most used
Address                                 Idle(sec) Timeout(sec) Hit-count          Branch(es)
ngfwbr1#
```

To debug policy route, use the following command:

```
ngfwbr1# debug policy-route
debug policy-route  enabled at level 1
ngfwbr1# pbr: policy based route lookup called for 198.19.11.225/58119 to 198.19.10.100/53
 proto 17 sub_proto 0 received on interface inside, NSGs, nsg_id=none
pbr: no route policy found; skip to normal route lookup
.
output-snipped
.
pbr: policy based route lookup called for 198.19.11.225/61482 to 63.140.48.151/443 proto 6
 sub_proto 0 received on interface inside
                                                                , NSGs, nsg_id=1
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1678091359817, sequence 5, permit; proceed with policy
routing
pbr: evaluating interface outside3
pbr: policy based routing applied; egress_ifc = outside3 : next_hop = 198.19.30.63

ngfwbr1#
```

The debug example above is for WebEx traffic. Note that the traffic is routed through the outside3 interface before PBR changes the route path to the outside2 interface.

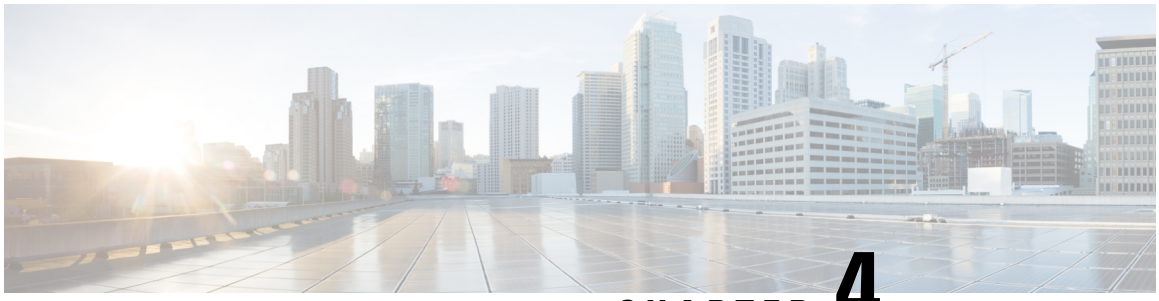
To stop the debug process, use the following command:

```
ngfwbr1# undebug all
```

Additional Resources

Resource	URL
Secure Firewall Threat Defense Release Notes	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
All New and Deprecated Features	http://www.cisco.com/go/whatsnew-fmc
Secure Firewall on Cisco.com	http://www.cisco.com/go/firewall
Secure Firewall on YouTube	https://www.youtube.com/cisco-netsec

Resource	URL
Secure Firewall Essentials	https://secure.cisco.com/secure-firewall



CHAPTER 4

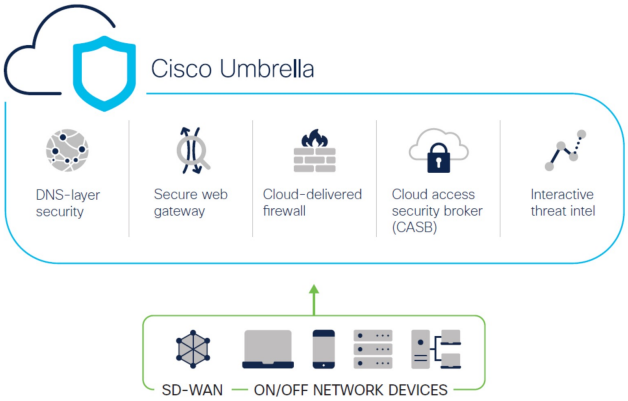
Secure Internet Traffic Using Umbrella Auto Tunnel

In this chapter, we delve into the practical application of the Umbrella auto tunnel. The use case details the scenario, network topology, best practices, and prerequisites. It also provides a comprehensive end-to-end procedure for seamless implementation.

Cisco Umbrella Auto Tunnel

Domain Name System (DNS) is an internet protocol often used in attacks. 90% of malware uses DNS (Source: Cisco Security Research Report). However, many organizations do not monitor their DNS or use DNS-focused security.

Figure 4: Cisco Umbrella



Cisco Umbrella is a cloud based secure internet gateway platform that provides multiple levels of defense against internet based threats. Umbrella integrates DNS layer security, Cloud Access Security Border (CASB) functionality, cloud-delivered firewall, and secure web gateway to deliver highly scalable security regardless of branch resources. Internet bound traffic can be sent securely automatically from the branch to the nearest Umbrella point of presence for inspection prior to being allowed or denied access to the internet.

From Release 7.3, the Secure Firewall Management Center supports Auto Tunnel configuration for Umbrella Secure Internet Gateway (SIG) integration that enables a network device to forward DNS and web traffic to Umbrella SIG for inspection and filtering through the SIG tunnel.

DNS and web policies defined within Cisco Umbrella can be applied to connections through Secure Firewall This enables you to apply and validate requests based on their domain names.

The management center provides a new simplified intuitive wizard-based interface to build this tunnel thus minimizing the configuration steps on Firewall Threat Defense and Cisco Umbrella.

The management center leverages uses Umbrella APIs to configure the network tunnels using parameters in the Cisco Umbrella Connection configuration. Then management center fetches the list of Umbrella datacenters and displays them in the user interface for selection as a hub in the SASE Topology. The network tunnel is deployed on the threat defense device and automatically created on Cisco Umbrella after the deployment is complete in the management center. This helps to apply uniform DNS and web policies for on premise users and roaming users.

Benefits

Benefits of securing internet traffic using Cisco Umbrella include :

- Securing users and applications at the DNS layer before any connections are established thus reducing consequent packet processing resulting in faster protection.
- Uniform DNS control policies are applied for hybrid users (on premise users and roaming users).
- Umbrella blocks web requests as well as requests to malware, ransomware, phishing attempts, and botnets even before a connection is established thereby stopping threats before they hit your network or endpoints. This results in a dramatic reduction in the number of infections and alerts you need to remediate.
- Eliminates the need for advanced firewall features such as URL filtering and TLS decryption.
- Auto tunnel setup requires minimal configuration in the management center.

- Automatic network tunnel configuration on the Umbrella dashboard.

Is This Use Case For You?

The intended audience for the Umbrella SASE Auto Tunnel Configuration is IT teams, network administrators, and security professionals who are responsible for managing and securing the network infrastructure of an organization. They are interested in exploring advanced solutions for secure remote access and simplifying the configuration and management of secure tunnels. The Umbrella SASE Auto Tunnel Configuration description would appeal to those seeking to enhance network security, streamline remote connectivity, and improve the overall user experience for their organization's remote workforce.

Scenario

Alice, the IT administrator is responsible for managing the organization's IT infrastructure and ensuring its security. Alice is aware of the growing threats in cyberspace and wants to implement robust security measures to prevent any potential cyber attacks such as malware, ransomware, and phishing.

Sally is an employee who works in the branch office and uses the organization's network to access the internet for work-related activities.

What is at risk?

Without proper security measures, employees may unknowingly access malicious websites and download harmful software, which can compromise the organization's network security and data privacy.

How does SIG integration solve the problem?

Alice implemented a two-layer security approach using a branch firewall and Cisco Umbrella. The firewall provided inbound security for the network from web and non-web based attacks. Umbrella provided outbound security by blocking malicious domains, IPs, and URLs at the DNS and web layers.

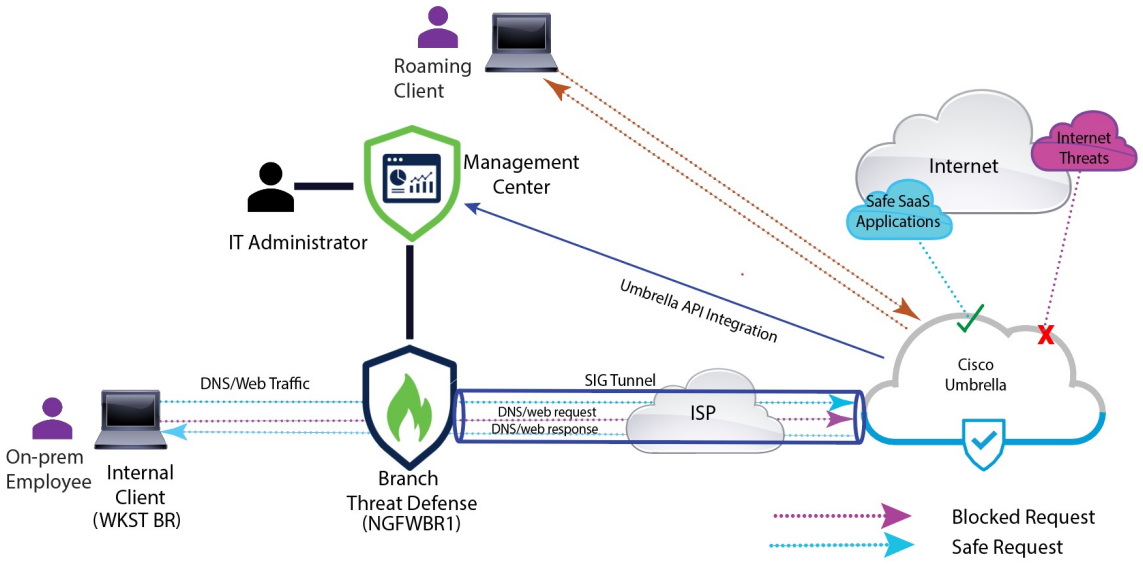
Sally notices that some websites are now being blocked by the firewall and Umbrella.

Both on-prem and remote users are subject to the same DNS and web policy defined within the Umbrella dashboard. As a result of this implementation, the organization's network is now more secure and protected against potential cyber attacks.

Network Topology

In this topology, a threat defense device is deployed at a branch location. In the figure below, the internal client or branch workstation is labelled WKST BR and the branch threat defense is labelled NGFWBR1. A SIG auto tunnel is configured between NGFWBR1 and Cisco Umbrella.

Figure 5: Network Topology for Umbrella Auto Tunnel Configuration



All DNS and web traffic is sent through the SIG tunnel to Cisco Umbrella to be validated and allowed or blocked based on the Umbrella DNS and web policy. This provides two layers of protection, one locally enforced by the Cisco Secure Threat Defense and the other cloud-delivered by Cisco Umbrella.

In the case of DNS traffic:

1. If Cisco Umbrella detects a DNS request for a domain that has not been classified, it will query the domain's reputation.
2. If the domain is classified as malicious, the DNS request is blocked, and the end user is prevented from accessing the website.
3. If the domain is classified as safe, the DNS request is resolved, and the website is accessible to the end user.

Best Practices for SASE Umbrella Tunnels

- Ensure that the base license is enabled with export-controlled features in the management center.
- We recommend that the threat defense interfaces facing the internet be named or prefixed with **outside**.
- Do not edit or delete the SASE topology if the deployment to Umbrella is running for that topology.
- To configure backup Umbrella DC, replicate the same topology with same threat defense endpoints using backup Umbrella DC.
- To configure backup interface on the threat defense endpoint, replicate the same topology with the same Umbrella DC with the same threat defense endpoint using VTI on the backup interface.

Prerequisites for Configuring Umbrella SASE Tunnels

- Complete the Threat Defense Initial Configuration Using the Device Manager

- Assign Licenses to Devices
- Add routes for internet access. See Add a Static Route.
- Configure NAT for Threat Defense
- Creating a Basic Access Control Policy
- You must have a Cisco Umbrella Secure Internet Gateway (SIG) Essentials subscription or a free SIG trial version.
- You must enable your Smart License account with the export-controlled features to deploy tunnels on Umbrella from the management center.
- Log into Umbrella at http://login.umbrella.com, and obtain the required information to establish a connection to Cisco Umbrella. Ensure the management center can reach management.api.umbrella.com.
- You must register your Cisco Umbrella organisation with the management center and configure the management key and the management secret in the Cisco Umbrella Connection advanced settings. This fetches the datacenter details from the Cisco Umbrella cloud. You must also configure the Organization ID, Network Device Key, Network Device Secret, and the Legacy Network Device Token in the Cisco Umbrella Connection general settings.

  For more information, see:

  - Configure Cisco Umbrella Connection Settings
  - Map Management Center Umbrella Parameters and Cisco Umbrella API Keys

- Ensure that Umbrella data center is reachable from the threat defense.
- Ensure the threat defense supports route-based VPN with local tunnel ID support (Version 7.1.0 and later). You can deploy a SASE tunnel with local tunnel ID support in management center version 7.3.0 and later.

Best Practices for SASE Umbrella Tunnels

- Ensure that the base license is enabled with export-controlled features in the management center.
- We recommend that the threat defense interfaces facing the internet be named or prefixed with **outside**.
- Do not edit or delete the SASE topology if the deployment to Umbrella is running for that topology.
- To configure backup Umbrella DC, replicate the same topology with same threat defense endpoints using backup Umbrella DC.
- To configure backup interface on the threat defense endpoint, replicate the same topology with the same Umbrella DC with the same threat defense endpoint using VTI on the backup interface.

Prerequisites for Configuring Umbrella SASE Tunnels

- Complete the Threat Defense Initial Configuration Using the Device Manager
- Assign Licenses to Devices

- Add routes for internet access. See Add a Static Route.
- Configure NAT for Threat Defense
- Creating a Basic Access Control Policy
- You must have a Cisco Umbrella Secure Internet Gateway (SIG) Essentials subscription or a free SIG trial version.
- You must enable your Smart License account with the export-controlled features to deploy tunnels on Umbrella from the management center.
- Log into Umbrella at http://login.umbrella.com, and obtain the required information to establish a connection to Cisco Umbrella. Ensure the management center can reach management.api.umbrella.com.
- You must register your Cisco Umbrella organisation with the management center and configure the management key and the management secret in the Cisco Umbrella Connection advanced settings. This fetches the datacenter details from the Cisco Umbrella cloud. You must also configure the Organization ID, Network Device Key, Network Device Secret, and the Legacy Network Device Token in the Cisco Umbrella Connection general settings.

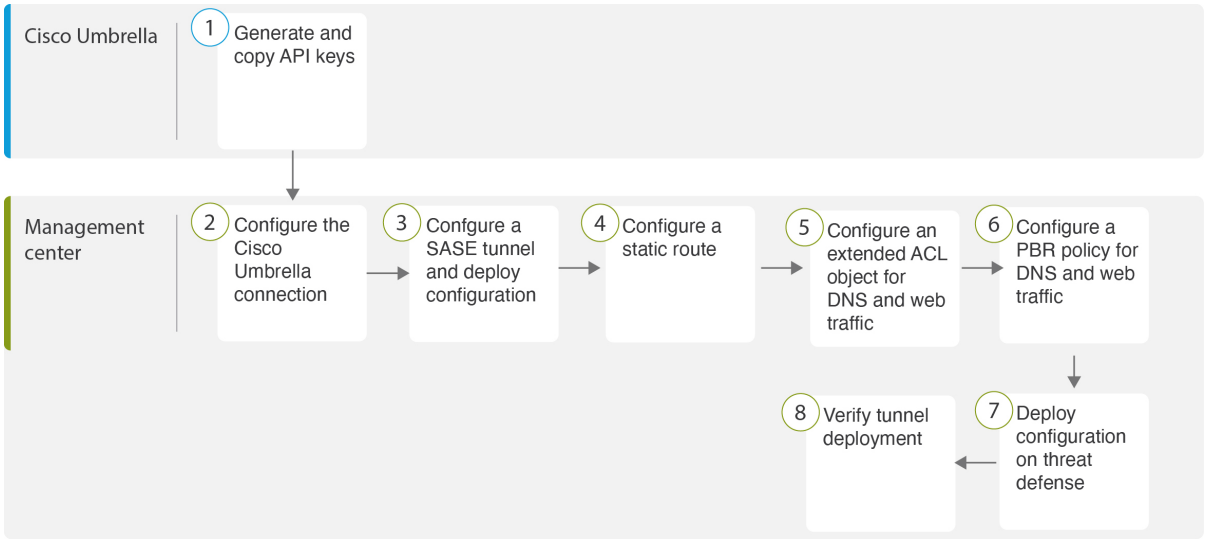
  For more information, see:

  - Configure Cisco Umbrella Connection Settings
  - Map Management Center Umbrella Parameters and Cisco Umbrella API Keys

- Ensure that Umbrella data center is reachable from the threat defense.
- Ensure the threat defense supports route-based VPN with local tunnel ID support (Version 7.1.0 and later). You can deploy a SASE tunnel with local tunnel ID support in management center version 7.3.0 and later.

End-to-end Procedure for Configuring Umbrella Auto Tunnel

The following flowchart illustrates the workflow for configuring the SASE tunnel in Secure Firewall Management Center.



Step	Description
1	(*Prerequisite*) Generate and copy the API keys in Cisco Umbrella. See Map Management Center Umbrella Parameters and Cisco Umbrella API Keys .
2	(*Prerequisite*) Configure the Cisco Umbrella connection. See Configure Cisco Umbrella Connection Settings.
3	Create the SASE tunnel and deploy the configuration on threat defense. See Configure a SASE Tunnel for Umbrella, on page 61.
4	Configure a static route. See Configure a Static Route, on page 65.
5	Configure an extended ACL object for DNS and web traffic. See Configure an Extended ACL for DNS and Web Traffic, on page 65
6	Configure a PBR policy for DNS and web traffic. See Configure a PBR Policy for DNS and Web Traffic , on page 66
7	Deploy configuration on threat defense. See Deploy Configuration, on page 20.
8	Verify tunnel deployment. See Verify SASE Umbrella Tunnel Deployment, on page 67.

Configure a SASE Tunnel for Umbrella

Before you begin

Ensure that you review Prerequisites for Configuring Umbrella SASE Tunnels, on page 58 and Best Practices for SASE Umbrella Tunnels, on page 58.

Procedure

Step 1 Log in to the management center, choose **Devices > VPN > Site To Site**.

Step 2 Click **+ SASE Topology** to open the SASE topology wizard.

Step 3 Enter a unique **Topology Name** For our example, enter **VPN-MumbaiUmbrella**.

Step 4 **Pre-shared Key**: This key is auto-generated according to the Umbrella PSK requirements.

The device and Umbrella share this secret key, and IKEv2 uses it for authentication. You can override the auto-generated key. If you want to configure this key, it must be between 16 and 64 characters in length, include at least one uppercase letter, one lowercase letter, one numeral, and have no special characters. Each topology must have a unique pre-shared key. If a topology has multiple tunnels, all the tunnels have the same pre-shared key.

Step 5 Choose a data center from the **Umbrella Data center** drop-down list. The Umbrella data centers are auto populated with the region and IP addresses.

Step 6 Click **Add** to add a threat defense node as an endpoint in the SASE topology.

a) Choose a threat defense device (**NGFWBR1**) from the **Device** drop-down list.

b) Choose a static VTI interface from the **VPN Interface** drop-down list.

To create a new static VTI interface (for example, **Outside_static_vti_1**), click **+**. The **Add Virtual Tunnel Interface** dialog box appears with the following pre-populated default configurations.

- Tunnel Type is set to **Static** by default.
- Name is <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*>. For example, Outside_static_vti_1.
- Tunnel is **Enabled** by default.
- Security zone is configured as **Outside** by default.
- Tunnel ID is auto-populated with an unique ID.
- Tunnel Source Interface is auto-populated with an interface with an 'outside' prefix.

  Note
  Ensure the tunnel source is set to **GigabitEthernet0/0**

  Note
  You can also set the Tunnel Source Interface to a different interface.

- IPsec tunnel mode is IPv4 by default.
- Unused IP address is picked from the 169.254.x.x/30 private IP address range. In our example, **169.254.2.1/30** is selected.

  Note
  When the /30 subnet is used, only two IP addresses are available. The first IP address is the auto tunnel VTI IP and the second IP address is used as the next hop IP while configuring the static route to the Umbrella DC. In our example, 169.254.2.1 is the VTI IP and 169.254.2.2 is used for the static route. See Configure a Static Route, on page 65.

- Click **OK**.

Choose **outside_static_vti_1** from the VPN Interface drop-down list.

c) Enter a prefix for the local tunnel ID in the **Local Tunnel ID** field.

The prefix can have a minimum of eight characters and a maximum of 100 characters. Umbrella generates the complete tunnel ID (<*prefix*>@<*umbrella-generated-ID*>-umbrella.com) after the management center deploys the tunnel on Umbrella. The management center then retrieves and updates the complete tunnel ID and deploys it on the threat defense device. Each tunnel has a unique local tunnel ID.

d) Click **Save** to add the endpoint device to the topology.

Step 7 Click **Next** to view the summary of the Umbrella SASE tunnel configuration.

- **Endpoints** pane: Displays the summary of the configured threat defense endpoints.
- **Encryption Settings** pane: Displays the encryption settings for the SASE tunnel.

Step 8 Check the **Deploy configuration on threat defense nodes** check box to trigger deployment of the network tunnels to the threat defense. This deployment only occurs after the tunnels are deployed on Umbrella. Local tunnel ID is required for the threat defense deployment.

Step 9 Click **Save**.

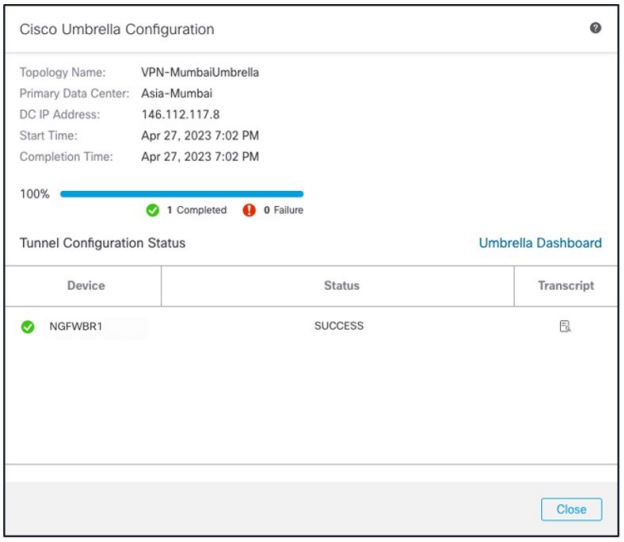
This action:

a. Saves the SASE topology in the management center.

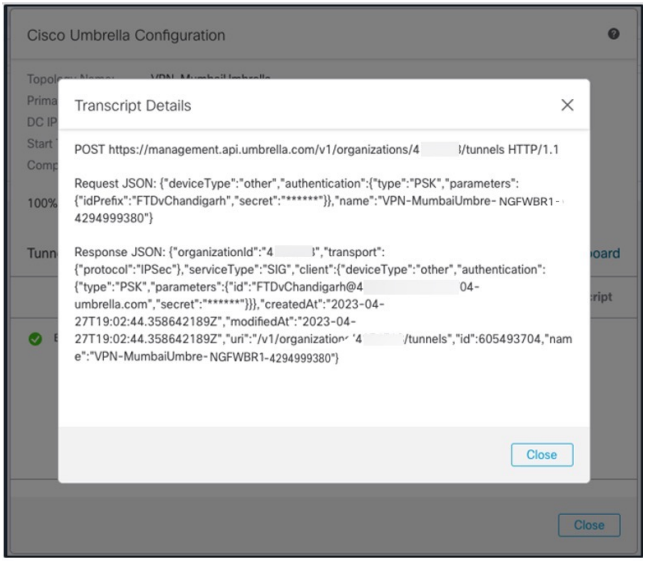
b. Triggers deployment of the network tunnels for each threat defense endpoint to Umbrella.

c. Triggers deployment of the network tunnels to the threat defense devices, if the option is enabled. This action commits and deploys all the updated configurations and policies, including non-VPN policies, since the last deployment on the device.

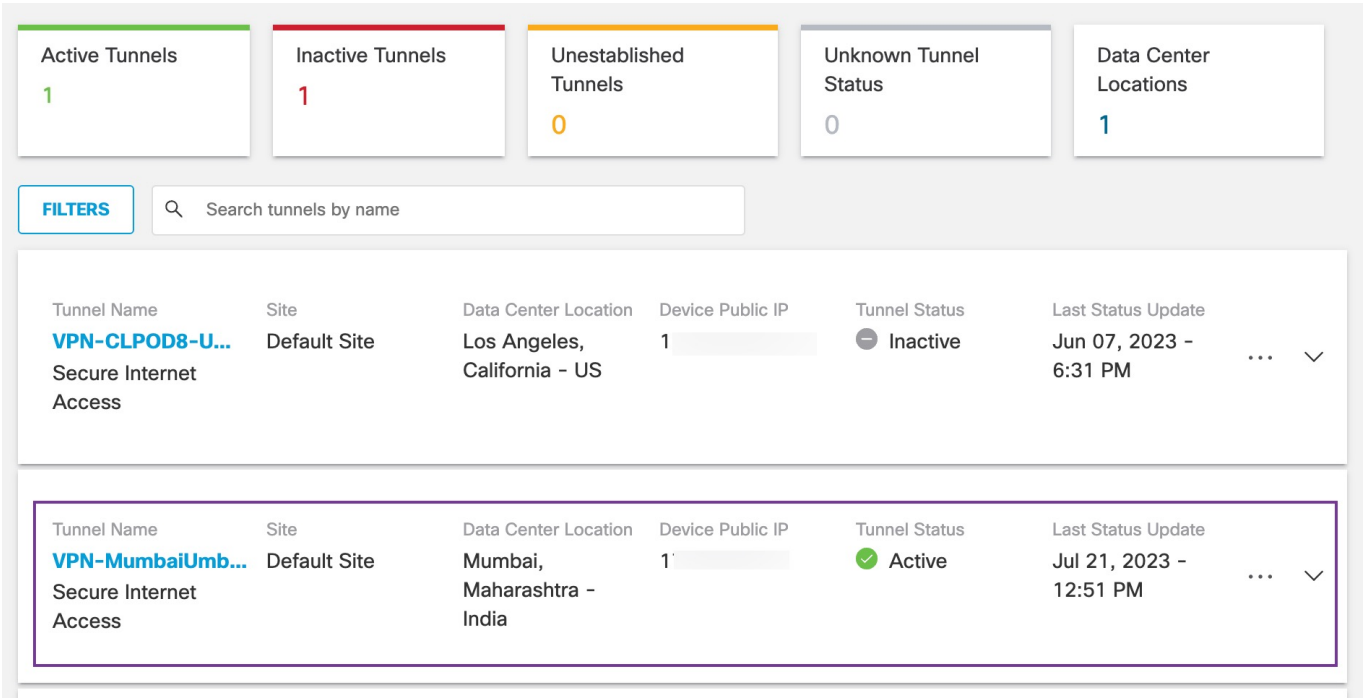
d. Opens the **Cisco Umbrella Configuration** window and displays the status of the tunnel deployment on Umbrella.



To view the details of the deployment, click the **Transcript** button to view the transcript details such as the APIs, request payload, and the response received from Umbrella.



Click the **Umbrella Dashboard** link to view the Network Tunnels page in Umbrella.



What to do next

For the traffic intended to flow through the SASE tunnel, configure a PBR policy with a specific match criteria to send the traffic through the VTI.

Configure a Static Route

You must configure a static route from the auto tunnel to the Umbrella DC.

Procedure

Step 1 From the **Devices** > **Device Management** page and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab.

Step 3 Click **Static Route**.

Step 4 Click **Add Route** to add a new route.

Step 5 Select **outside_static_vti_1** as the interface from the **Interface** drop-down list.

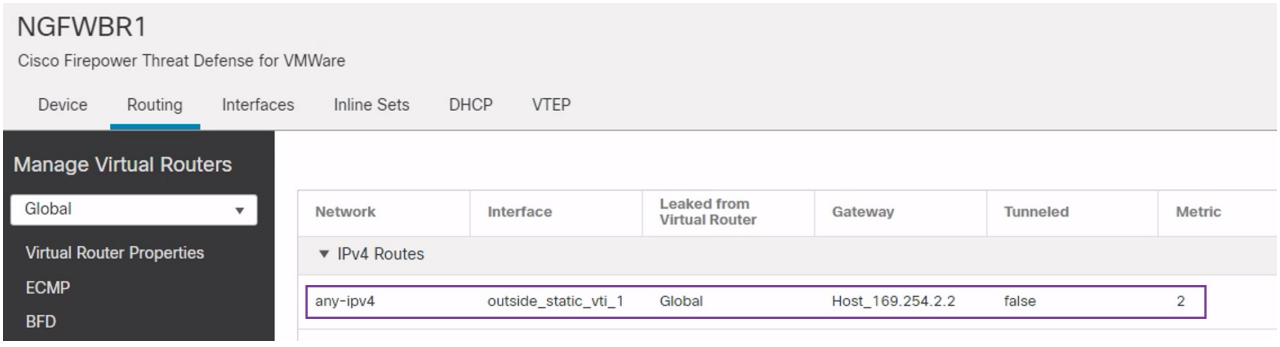
Step 6 Select **any-ipv4** as the the destination network from the **Available Networks** box and click **Add**.

Step 7 Enter a gateway for the network. For this example, enter **169.254.2.2**.

Step 8 Enter a metric value. It can be a number that ranges between 1 and 254. For this example, enter the value as 2.

Step 9 To save the settings, click **Save**.

The static route is created as seen in the figure below.



Configure an Extended ACL for DNS and Web Traffic

The access list is configured for DNS and web traffic to be steered towards the internet from the egress interface with the help of policy based routing.

Procedure

Step 1 Select **Objects** > **Object Management** and choose **Access Lists** > **Extended** from the table of contents.

Step 2 Click **Add Extended Access List** to create an extended access list for social media traffic.

Step 3 In the Extended ACL Object dialog box, enter a name (**LAN_to_Internet**) for the object.

Step 4 Click **Add** to create a new Extended Access List.

Step 5 Configure the following access control properties:

a. Select the **Action** to Allow (match) the traffic criteria.

b. Click the **Port** tab and search for **HTTP, HTTPS, DNS_over_UDP, DNS_over_TCP** in the **Available Ports** list.

c. Select the ports and click **Add to Destination**.

d. Click the **Network** tab and search for the branch LAN in the **Available Networks** list.

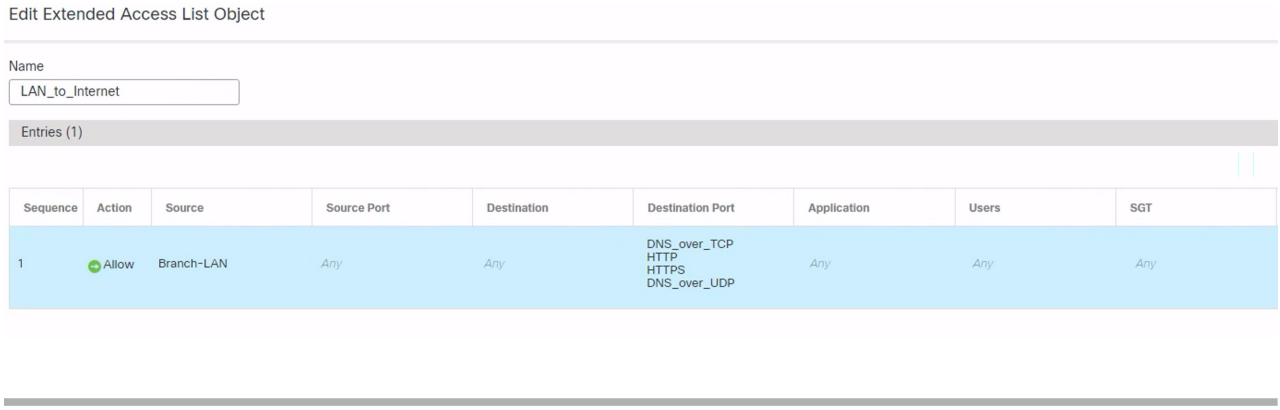
Note
In our example, the network is **Branch-LAN**.

e. Select **Branch-LAN** and click **Add to Source**.

f. Click **Add** to add the entry to the object.

g. Click **Save**.

The ACL object is created as seen in the figure below.



Configure a PBR Policy for DNS and Web Traffic

You can configure the PBR policy in the Policy Based Routing page by specifying the ingress interfaces, match criteria (Extended Access Control List), and egress interfaces to route DNS and web traffic.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the threat defense device (**NGFWBR1**).

Step 2 Click the **Routing** tab on the interface view of NGFWBR1.

Step 3 Click **Policy Based Routing**.

Step 4 In the **Add Policy Based Route** dialog box, select the **Ingress Interface** from the drop-down list.

Step 5 To specify the match criteria and the forward action in the policy, click **Add**.

Step 6 In the **Add Forwarding Actions** dialog box, do the following:

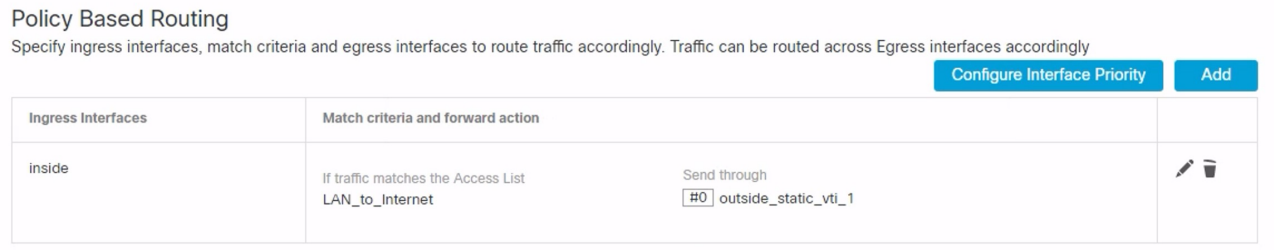
a) From the **Match ACL** drop-down, choose **LAN_to_Internet**.

b) To select the configured interfaces, choose **Egress Interfaces** from the **Send To** drop-down list.

c) From **Available Interfaces**, click the **Add** (+) icon adjacent to **Outside_static_vti_1** interface to move it to **Selected Egress Interfaces**.
d) Click **Save** to write the changes for the match criteria.
e) Review the configuration and click **Save** to write all the configuration changes for policy based routing.

Step 7 Click **Save**.

The PBR policy is created as seen in the figure below.



Deploy Configuration

After you complete all the configurations, deploy them to the managed device.

Procedure

Step 1 On the management center menu bar, click **Deploy**. This displays the list of devices that are Ready for Deployment.

Step 2 Check the checkboxes adjacent to NGFWBR1 and NGFW1 on which you want to deploy configuration changes.

Step 3 Click **Deploy**. Wait till the deployment is marked Completed on the Deploy dialog box.

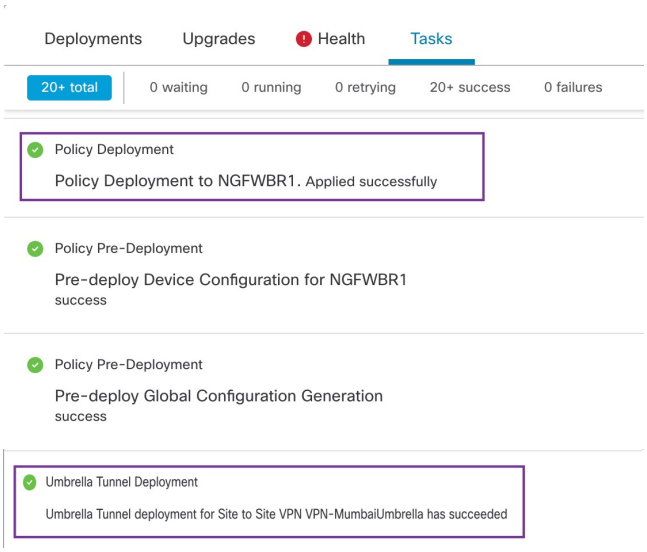
Step 4 If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Errors** or **Validation Warnings** window. To view complete details, click the Validation Errors or Validation Warnings link.

You have the following choices:

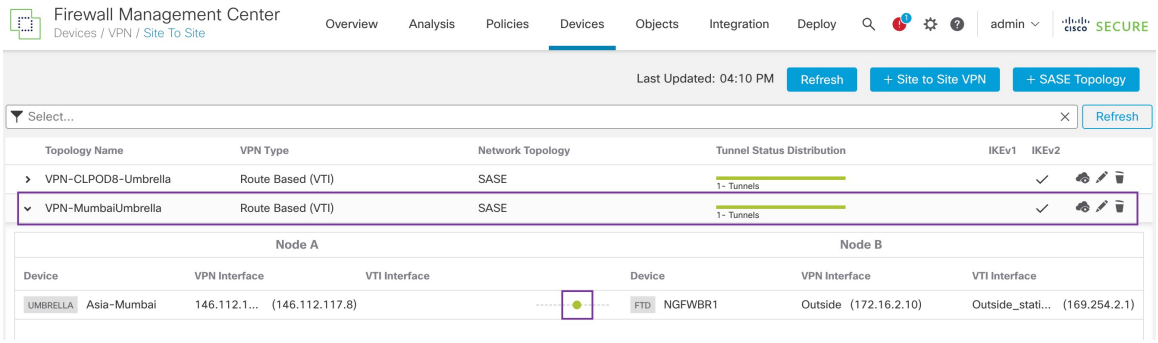
- Proceed with Deploy—Continue deploying without resolving warning conditions. You cannot proceed if the system identifies errors.
- Close—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

Verify SASE Umbrella Tunnel Deployment

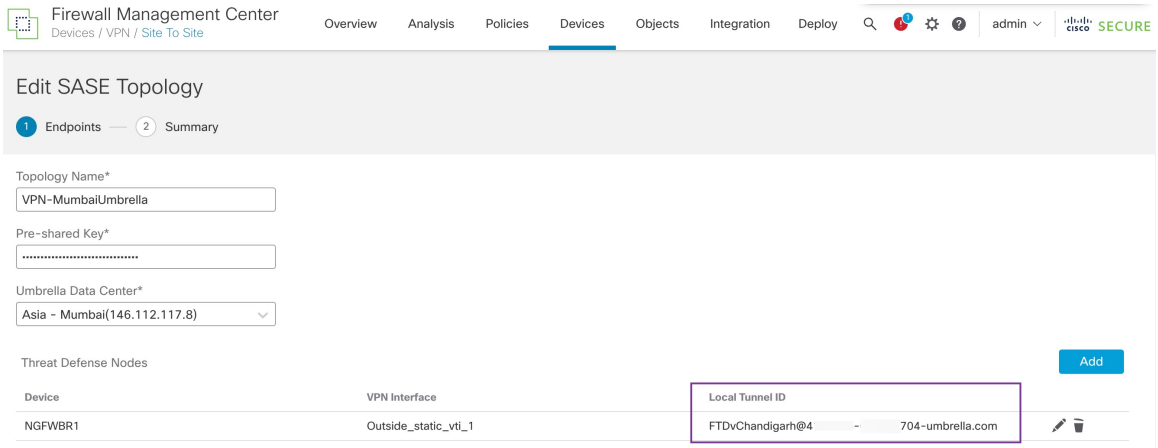
In the management center, go to **Notifications** > **Tasks** to view the status of the Umbrella tunnel deployment and policy deployment on the threat defense device (NGFWBR1).



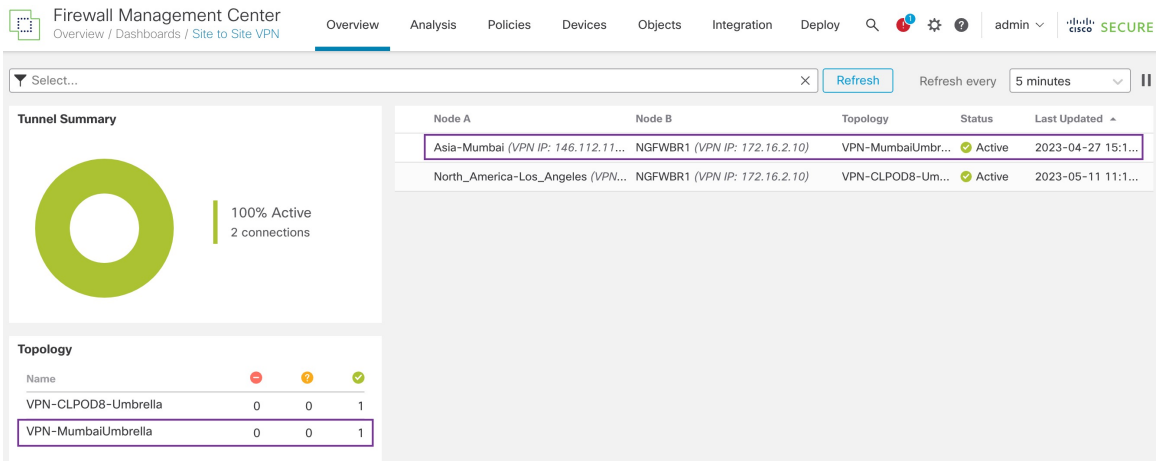
To check the SASE auto tunnel status in the management center, choose **Devices > VPN > Site To Site**.



To check the updated SASE topology in the management center, choose **Devices > VPN > Site To Site > Edit SASE Topology**. The local Tunnel ID is updated after the deployment to Umbrella.



To view the Site To Site VPN dashboard in the management center, choose **Overview > Dashboard > Site to Site VPN**.



Use the following CLI commands to verify SASE Umbrella Tunnel on threat defense:

- To verify the details of the SASE tunnel, use the following command:

```
> show running-config interface tunnel 1
!
interface Tunnel1
 nameif Outside_static_vti_1
 ip address 169.254.2.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 146.112.117.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

- To verify the IPSec profile and the associated proposal, use the following command:

```
> show running-config crypto ipsec
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256
 protocol esp integrity sha-256
crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set ikev2 local-identity email-id FTDvChandigarh@41xxxxx-xxxxxxxxx-umbrella.com
 set reverse-route
crypto ipsec security-association pmtu-aging infinite
```

- To verify the IKeV2 policy set, use the following command:

```
> show running-config crypto ikev2
crypto ikev2 policy 15
 encryption aes-gcm-256
 integrity null
 group 20 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable Outside
```

- To verify the tunnel statistics including Tx and Rx data, use the following command:

```
> show vpn-sessiondb l2l
Session Type: LAN-to-LAN
Connection    : 146.112.117.8
Index         : 19                    IP Addr       : 146.112.117.8
Protocol      : IKEv2 IPsecOverNatT
Encryption    : IKEv2: (1)AES-GCM-256  IPsecOverNatT: (1)AES-GCM-256
Hashing       : IKEv2: (1)none  IPsecOverNatT: (1)none
Bytes Tx      : 234                     Bytes Rx      : 446
```

```
Login Time   : 19:14:51 UTC Thu Apr 27 2023
Duration     : 0h:55m:16s
Tunnel Zone  : 0
```

- To check the tunnel status, use the following command:

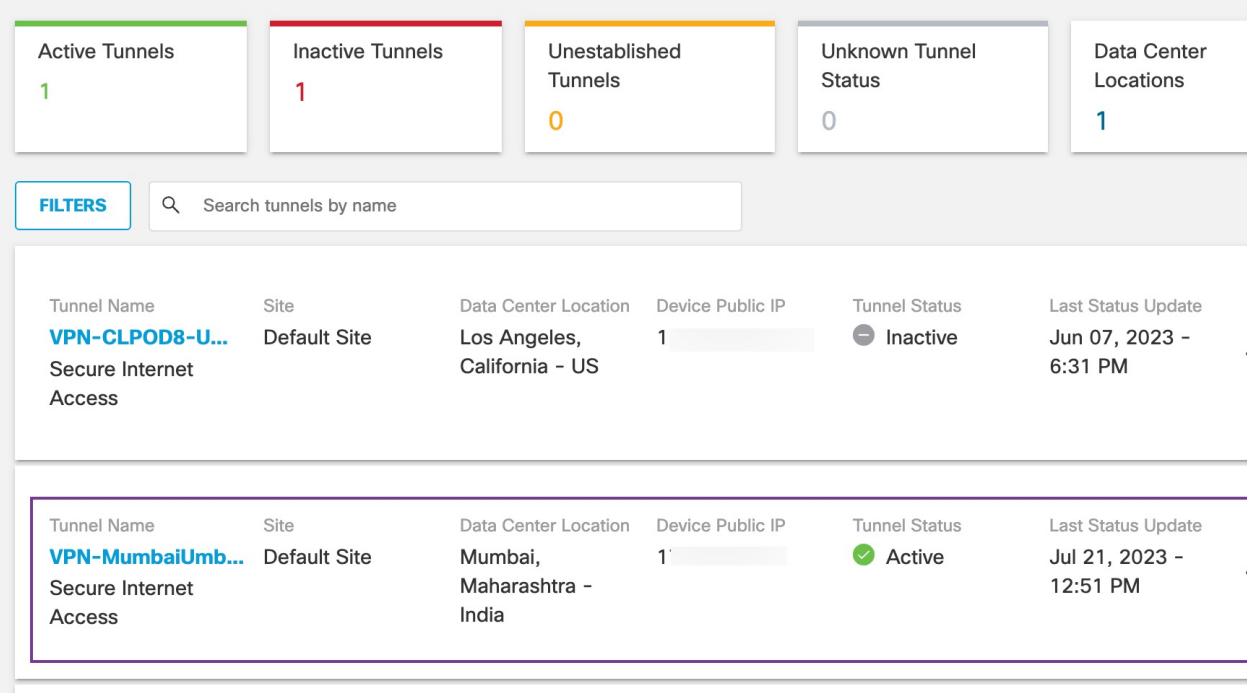
```
> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              203.0.113.130   YES unset  up                    up
TenGigabitEthernet0/0      172.16.2.10     YES manual up                    up
TenGigabitEthernet0/1      172.16.3.10     YES manual up                    up
TenGigabitEthernet0/2      unassigned      YES unset  administratively down up
Tunnel1                    169.254.2.1     YES manual up                    up
```

- To check the IPSec SA associated to the VTI tunnel, use the following command:

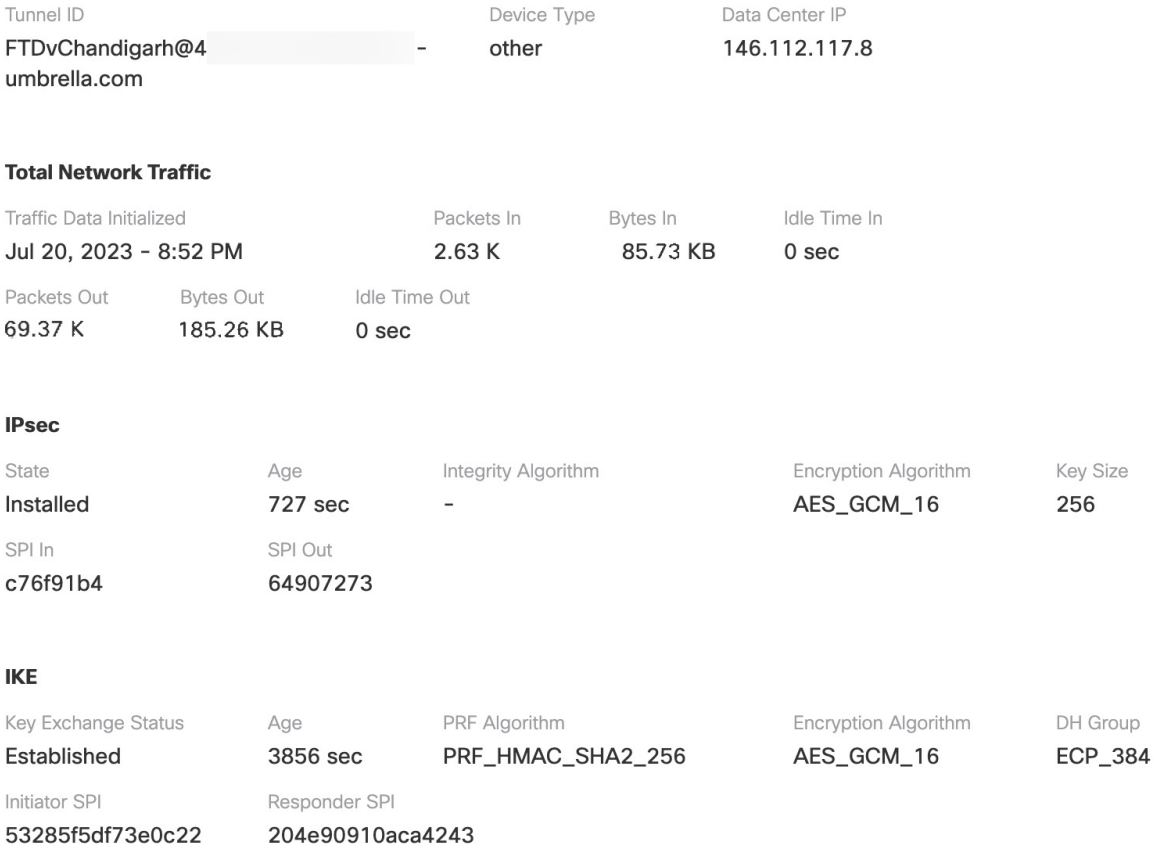
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.117.8


      #pkts encaps: 705, #pkts encrypt: 705, #pkts digest: 705
      #pkts decaps: 743, #pkts decrypt: 743, #pkts verify: 743
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 705, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

     local crypto endpt.: 198.18.128.81/4500, remote crypto endpt.: 146.112.117.8/4500

      path mtu 1500, ipsec overhead 63(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: C76F91B4
      current inbound spi : 64907273

    inbound esp sas:
      spi: 0x2BF92601 (737748481)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
         slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4331520/27987)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0xCA2DC006 (3391995910)
```

```
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4101072/27987)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
```

To view the SASE tunnel in Umbrella, log in to Cisco Umbrella and navigate to **Deployments** > **Core Identities** > **Network Tunnels**. The network tunnel from the threat defense to Umbrella is displayed as shown in the figure below.



Expand the section to view the details of the tunnel.



Troubleshoot Umbrella Auto Tunnels

After the deployment, use the following CLI to debug issues related to Umbrella auto tunnels on Secure Firewall Threat Defense.

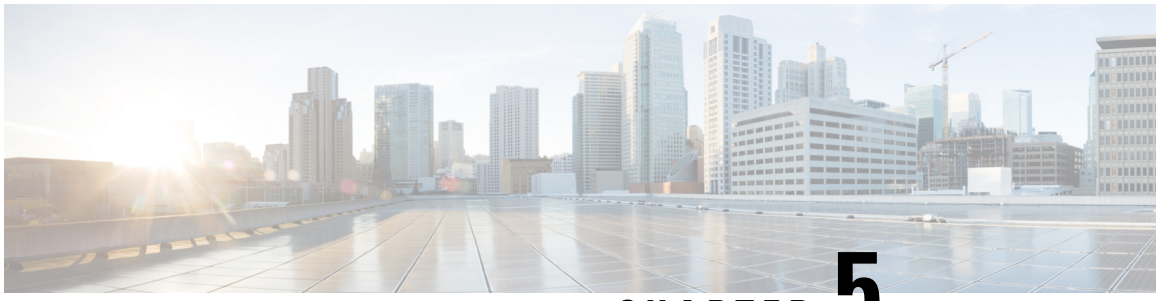
Note Proceed with caution when you run debug commands on the threat defense device in production environments.You can set various debug levels on the device that may have verbose outputs.

How to...	CLI Command
Enable conditional debugging for a particular peer	**debug crypto condition peer <peer-IP>**
Debug the Virtual Tunnel Interface information	**debug vti 255**
Debug the IKEv2 protocol related transactions	**debug crypto ikev2 protocol 255**
Debug the IKEv2 platform related transactions	**debug crypto ikev2 platform 255**
Debug the common IKE related transactions	**debug crypto ike-common 255**

How to...	CLI Command
Debug the IPSec related transactions	**debug crypto ipsec 255**

Additional Resources

Resource	URL
Secure Firewall Threat Defense Release Notes	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
All New and Deprecated Features	http://www.cisco.com/go/whatsnew-fmc
Secure Firewall on Cisco.com	http://www.cisco.com/go/firewall
Secure Firewall on YouTube	https://www.youtube.com/cisco-netsec
Secure Firewall Essentials	https://secure.cisco.com/secure-firewall



CHAPTER 5

Empower Remote Workers with Secure Connectivity: DIA, Umbrella Auto Tunnel, and DVTI in Action

In this chapter, we delve into the practical application of using DIA, Umbrella auto tunnel, and DVTI. The use case details the scenario, network topology, and the end-to-end procedure for seamless implementation.

Enhancing Connectivity and Security for Remote Workers with DIA, Umbrella SASE Auto Tunnel, and DVTI

In today's interconnected and remote work environment, organizations face the challenge of providing seamless connectivity, secure access, and optimized performance for their distributed workforce. This use case explores the implementation of DIA (Direct Internet Access), Umbrella SASE auto tunnel, and DVTI (Dynamic Virtual Tunnel Interface) technologies to overcome network connectivity issues, enhance collaboration, protect sensitive information, and empower the remote users to work efficiently from any location.

Is This Use Case For You?

The intended audience for this use case is IT professionals, network administrators, and decision-makers responsible for managing and securing the network infrastructure, as well as organizations looking to optimize connectivity and security for their remote workforce. It provides insights into the implementation of DIA, Umbrella SASE auto tunnel, and DVTI technologies and highlights the benefits they offer in addressing the challenges faced by remote workers.

Scenario

Sally works as a remote sales representative for a global company that relies heavily on real-time collaboration and data access. She frequently travels to different client locations, but faces challenges in accessing sales data and communicating with colleagues.

What is at risk?

The company's existing network infrastructure is unable to provide seamless connectivity and secure access across multiple locations, resulting in delays, data inconsistency, and communication breakdowns.

How does a solution consisting of DIA, Umbrella auto tunnel, and DVTI in a hub and spoke topology solve the problem?

To address the challenges faced by remote workers like Sally, her company implements a comprehensive solution using DIA, Umbrella SASE auto tunnel, and DVTI.

1. **DIA:** DIA allows Sally to connect directly to the internet without routing through the corporate network. This provides her with faster and more reliable internet access, enabling quick access to cloud-based applications and services. It offloads network traffic from the corporate network, reducing congestion and optimizing performance.
2. **Umbrella Auto tunnel:** By leveraging the Umbrella Auto Tunnel configuration, Sally's company ensures that uniform security policies are applied to traffic regardless of whether Sally is remotely connected or behind a branch firewall. It eliminates the need for manual configuration of VPN connections and reduces the complexity and potential errors associated with traditional tunnel setups. This technology offers simplicity, convenience, and enhanced security for Sally and other remote workers in the organization
3. **DVTI:** DVTI in a hub and spoke topology enables the dynamic creation of secure IPsec tunnels between the branch office and the corporate network. These tunnels encrypt data transmission, ensuring secure access to corporate resources while working remotely. DVTI also optimizes network performance by intelligently routing traffic through the most efficient path and providing redundancy for uninterrupted connectivity.

By combining DIA, Umbrella SASE auto tunnel, and DVTI, Sally's company enhances her connectivity, security, and productivity as a remote worker. She can access cloud applications quickly, collaborate seamlessly with colleagues, and enjoy a secure and reliable connection to corporate resources, regardless of her location. The IT team benefits from centralized security management, reduced network complexity, and improved visibility into remote workers' activities.

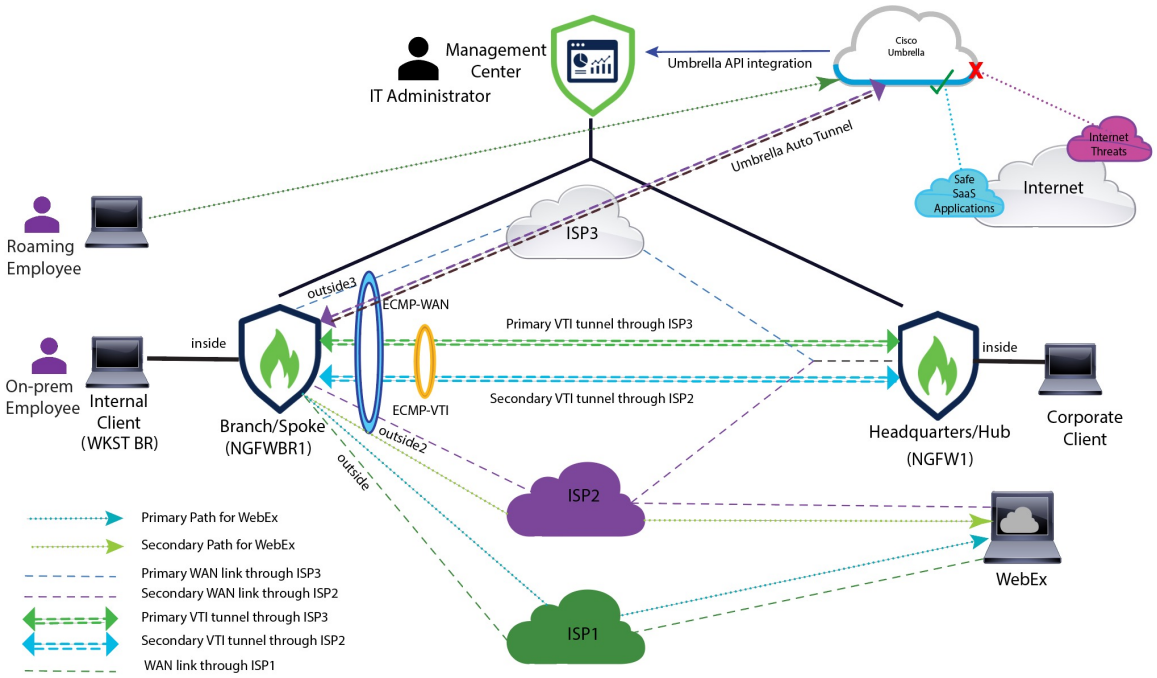
Topology

In this topology, the internal client or branch workstation is labeled as WKST BR that is connected to the branch threat defense labeled as NGFWBR1. The headquarters threat defense is labeled NGFW1. The corporate network is reachable through NGFW1. The ingress interface of NGFWBR1 is named inside and the egress interfaces are named outside, outside2, and outside3 respectively.

A Umbrella auto tunnel is configured between NGFWBR1 and Cisco Umbrella.

All DNS and web traffic is sent through the Umbrella auto tunnel to Cisco Umbrella to be allowed or blocked based on the Umbrella DNS and web policy. This provides two layers of protection, one locally enforced by the Cisco Secure Threat Defense and the other cloud-delivered by Cisco Umbrella.

For the hub spoke configuration, a VPN tunnel is configured between NGFWBR1 and NGFW1. An ECMP zone is configured on the primary and secondary static VTI interfaces on the branch node for link redundancy and loading balancing of VPN traffic.



End-to-end Procedure for Configuring DIA, Umbrella Auto Tunnel, and DVTI

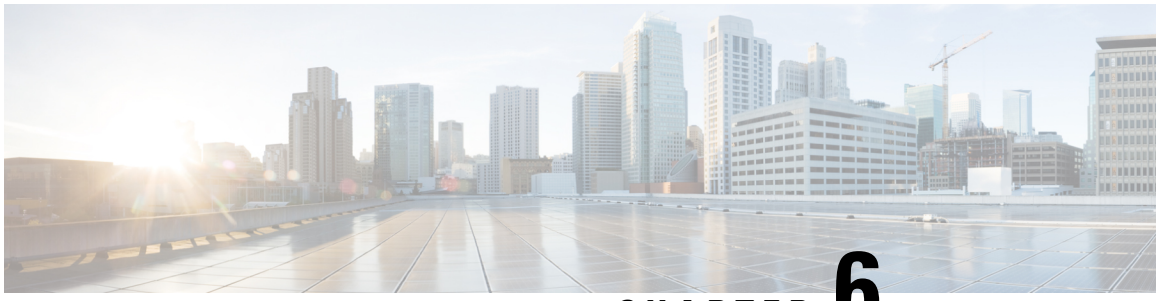
To configure the solution with DIA, Umbrella SASE auto tunnel, and DVTI:

- **Configure Direct Internet Access**: End-to-End Procedure for Configuring DIA With Path Monitoring, on page 38
- **Configure Umbrella SIG Auto Tunnel**:End-to-end Procedure for Configuring Umbrella Auto Tunnel, on page 60
- **Configure DVTI Hub and Spoke Topology**: End-to-End Procedure for Configuring a Route-based VPN (Hub and Spoke Topology), on page 9

Additional Resources

Resource	URL
Secure Firewall Threat Defense Release Notes	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
All New and Deprecated Features	http://www.cisco.com/go/whatsnew-fmc

Resource	URL
Secure Firewall on Cisco.com	http://www.cisco.com/go/firewall
Secure Firewall on YouTube	https://www.youtube.com/cisco-netsec
Secure Firewall Essentials	https://secure.cisco.com/secure-firewall



CHAPTER 6

Set Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates

In this chapter, we show you how to set up your SD-WAN branch office with dual ISPs using device registration keys 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.

Introduction

Onboarding multiple devices on a branch network and establishing a secure network infrastructure that connects these branches to the central headquarters is very 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 across different locations and security vulnerabilities.

You can mitigate these issues by using the Cisco Secure Firewall Management Center and Cisco Secure Firewall Threat Defense devices. The Secure Firewall solution streamlines the deployment of secure branch

networks with the new SD-WAN VPN wizard and device templates, 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 registration keys with the Management Center. It provides detailed instructions for deploying these devices with pre-provisioned configurations in a dual ISP SD-WAN topology. Note that this deployment does not support Threat Defense Virtual.

Scenario

Alex, a network administrator for a medium-sized enterprise with multiple branch offices across various cities, wants to onboard several devices on 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 shows 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)	7.4.1 and later of the following models: • Firepower 1000 series • Firepower 2100 series • Secure Firewall 3100 series • Secure Firewall 1200 series	Firepower 1120 Version 7.6

Prerequisites

- 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

- Guidelines and Limitations for Using SD-WAN Wizard
- Guidelines and Limitations for Device Management using Device Templates

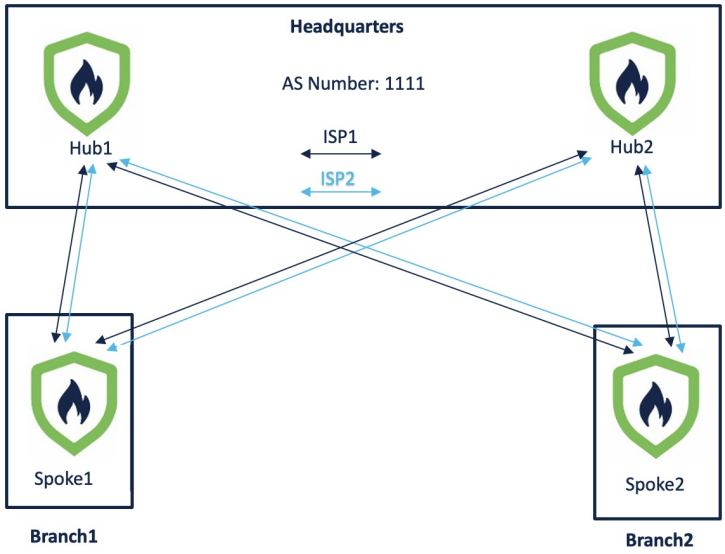
Network Topology

In the following dual ISP topology, the hubs and the spokes are in a single region, with AS number as 64512. The hubs and spokes use Internal Border Gateway Protocol (iBGP) as the routing protocol to exchange routing information.

- Hub1 and Hub2 are Threat Defense hub devices at the headquarters.
- Spoke1 and Spoke2 are Threat Defense spoke devices at the branches.
- outside-isp1 is the VPN interface of each spoke to ISP1.
- outside-isp2 is the VPN interface of each spoke to ISP2.

Alex aims to onboard a Cisco Firepower 1120 Threat Defense device into an existing dual ISP SD-WAN topology with preconfigured device 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 into the SD-WAN topology.

Figure 6: Dual ISP Topology with Two Hubs and Two Spokes in the Same Region



The topology has the following parameters:

Table 1: IP Adresses of Hubs and Spokes

Device	Management IP Address	Inside Interface	Outside Interface
Hub1	209.165.200.225	198.51.100.17/28	• ISP1: 192.0.2.17/28 • ISP2: 192.0.2.33/28
Hub2	209.165.200.226	198.51.100.33/28	• ISP1: 192.0.2.18/28 • ISP2: 192.0.2.34/28
Spoke1	209.165.200.227	198.51.100.65/28	• ISP1: 192.0.2.19/28 • ISP2: 192.0.2.35/28
Spoke2	209.165.200.228	198.51.100.129/28	• ISP1: 192.0.2.20/28 • ISP2: 192.0.2.36/28

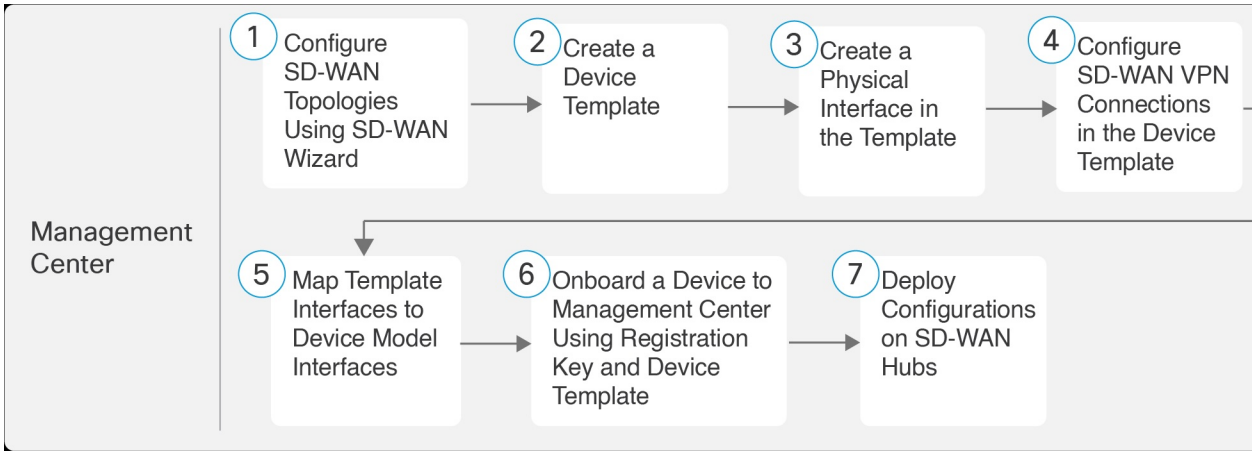
Table 2: Loopback IP Addresses and IP Address Pools of Hubs

Device	Hub Loopback IP Addresses	IP Address Pools
Hub1	• Loopback1: 209.165.201.1/255.255.255.224 • Loopback2: 209.165.201.65/255.255.255.224	• 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	• Loopback1: 209.165.201.33/255.255.255.224 • Loopback2: 209.165.201.97/255.255.255.224	• 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 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.

End-to-End Procedure for Setting Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates

The following flowchart illustrates the workflow for setting up an SD-WAN branch office with dual ISPs using registration key 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 84
2	Create a device template	Create a Device Template, on page 89
3	Create a physical interface in the template.	Add a Physical Interface in the Template, on page 90
4	Configure SD-WAN VPN connections in the device template.	Configure an SD-WAN VPN Connection in a Device Template, on page 91
5	Map template interfaces to device model interfaces.	Map Template Interfaces to Device Model Interfaces, on page 92
6	Onboard a device to management center using registration key and device template.	Onboard a Device to the Management Center Using a Registration Key and Device Template, on page 94
7	Deploy configurations on 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.

In this example, we 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, on page 81 and Guidelines and Limitations, on page 81.

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 from the drop-down list. The dynamic VTI inherits this IP address.
   - For SDWAN-VPN1: For Hub1, we use Loopback1 (209.165.201.1) as the Borrow IP.
   - For SDWAN-VPN2: For Hub1, we use Loopback2 (209.165.201.65) as the Borrow IP.

   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 83.

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 Adresses of Hubs and Spokes , on page 82.

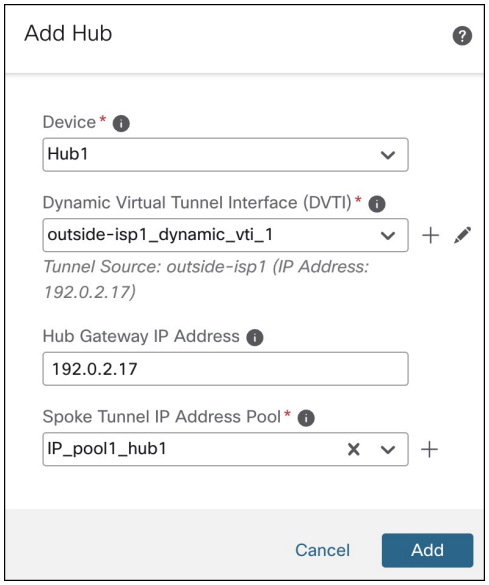
f) From the **Spoke Tunnel IP Address Pool** drop-down list, choose an IP address pool or click + to create an address pool.

Note

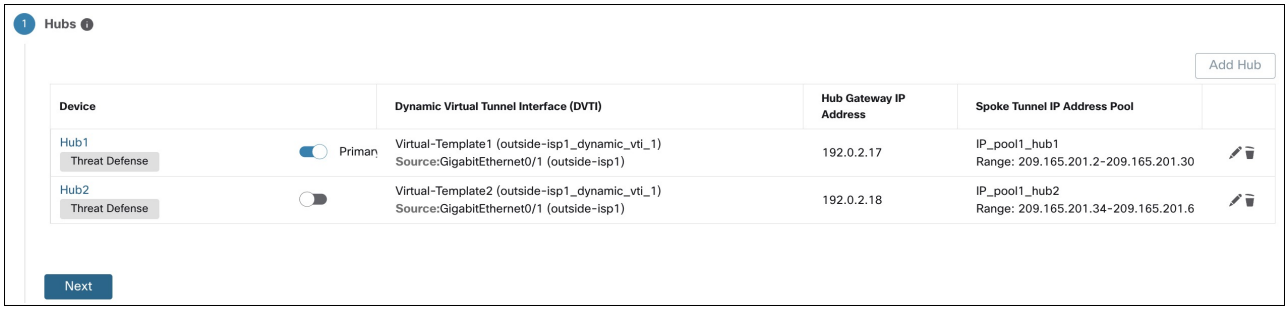
Ensure that you do not check the **Allow Overrides** check box when you create an address pool in the **Add IP Pool dialog box**.

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

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



h) (Optional) To add a secondary hub, repeat Step 4a to Step 4g.



i) Click **Next**.

Step 5 To configure spokes, click **Add Spokes (Bulk Addition)**. In the **Add Bulk Spokes** dialog box, configure the following parameters:

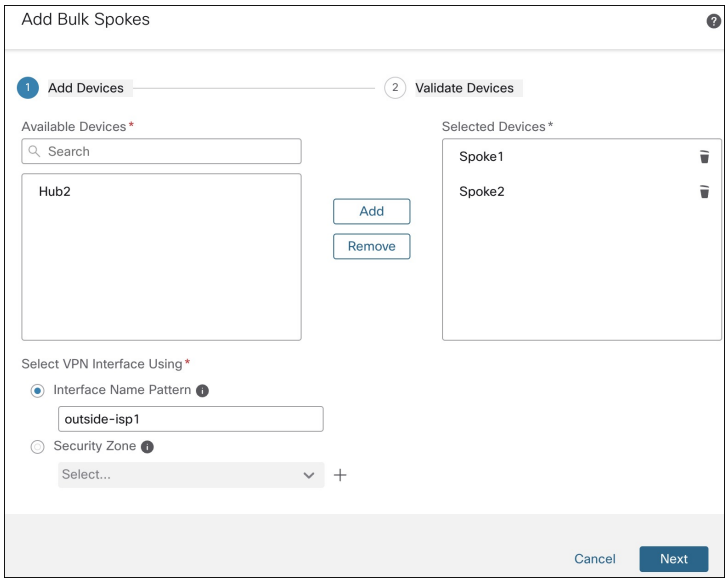
a. Choose Spoke1 and Spoke2 from the **Available Devices** list and click **Add** to move the devices to **Selected Devices**.

b. 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.

  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:

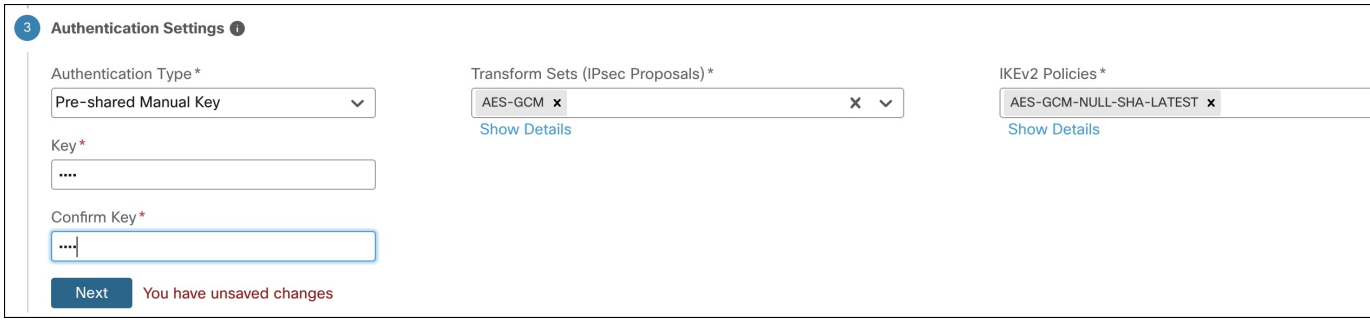
a) From the **Authentication Type** drop-down list, choose a manual pre-shared key, an auto-generated pre-shared key, or a certificate for device authentication.

You can use the default settings in this step and proceed to the next step. If required, you can edit the settings later on. In this example, we use Pre-shared Manual Key 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.

a) 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).

b) 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.

c) 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 the spokes are configured with **64512** as the AS number, and the secondary hub is configured with a different AS number.

d) In the **Community Tag for Local Routes** field, enter the BGP community attribute to tag connected and redistributed local routes. This attribute enables easy route filtering. Note this community string, you must use the same community string for the second SD-WAN VPN topology.

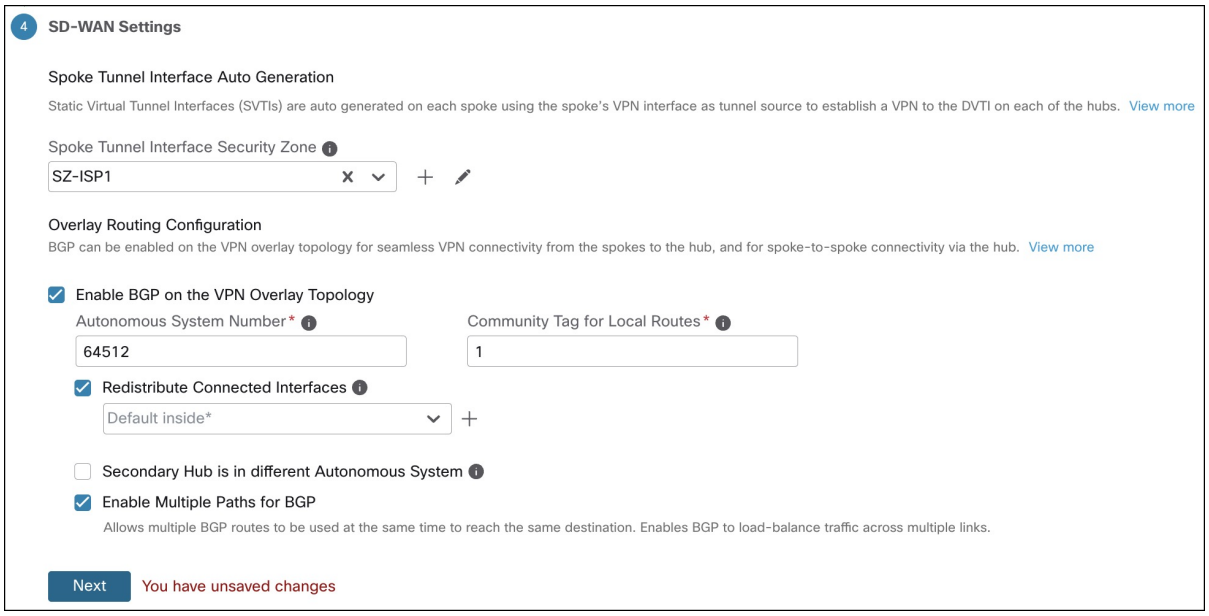
e) Check the **Redistribute Connected Interfaces** check box and choose an interface group from the drop-down list or click **+** to create an interface group with connected inside or LAN interfaces for BGP route redistribution in the overlay topology.

f) 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.

g) (Optional) Check the **Secondary Hub is in Different Autonomous System** check box. This check box appears only if you have a secondary hub in this topology.

h) In the **Autonomous System Number** field, enter the AS number for the secondary hub. In our example, both the hubs are in the same region and have the same AS number.

i) In the **Community Tag for Learned Routes** field, enter the BGP community attribute to tag 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. In our example, we do not have to configure this value because all the devices are in the same region.



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.

What to do next

1. Repeat Step 1 to Step 8 to configure the SDWAN-VPN2 topology with the VPN interface for ISP2: outside-isp2.
2. 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.

Create a Device Template

Before you begin

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

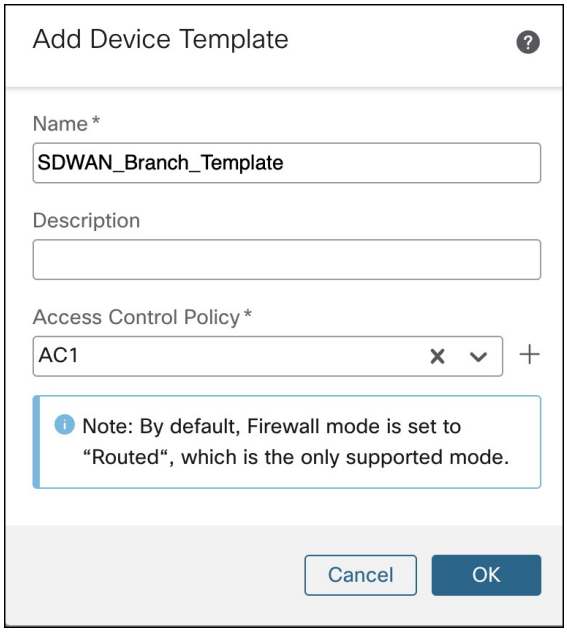
Procedure

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

Step 2 Click **Add Device Template**.

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

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



Step 3 Click **OK**.

Add a Physical Interface in the Template

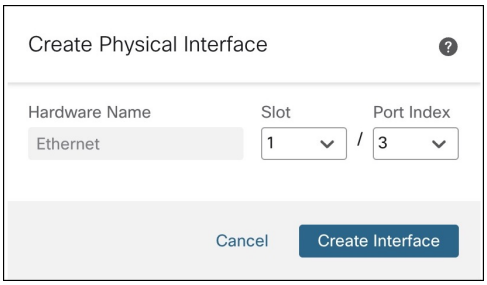
By default, a device template enables the device to come up with the following physical interfaces:

- 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**.



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, on page 81 and Guidelines and Limitations, on page 81.

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:

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

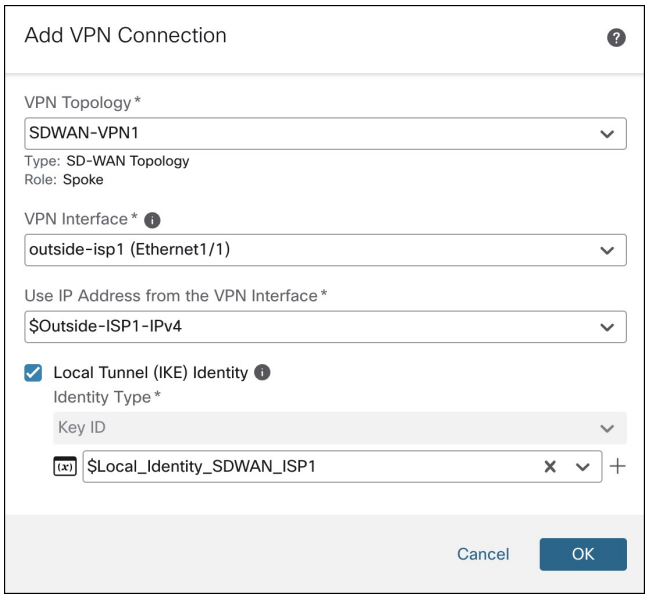
This list contains all the interfaces configured on the device template. In this example, the VPN interface is outside-isp1.

b) **Use IP Address from the VPN Interface**—This drop-down list is auto populated with the IP address variable. For IPv6 addresses, choose an IPv6 address from the drop-down list.

c) 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.

d) **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**.



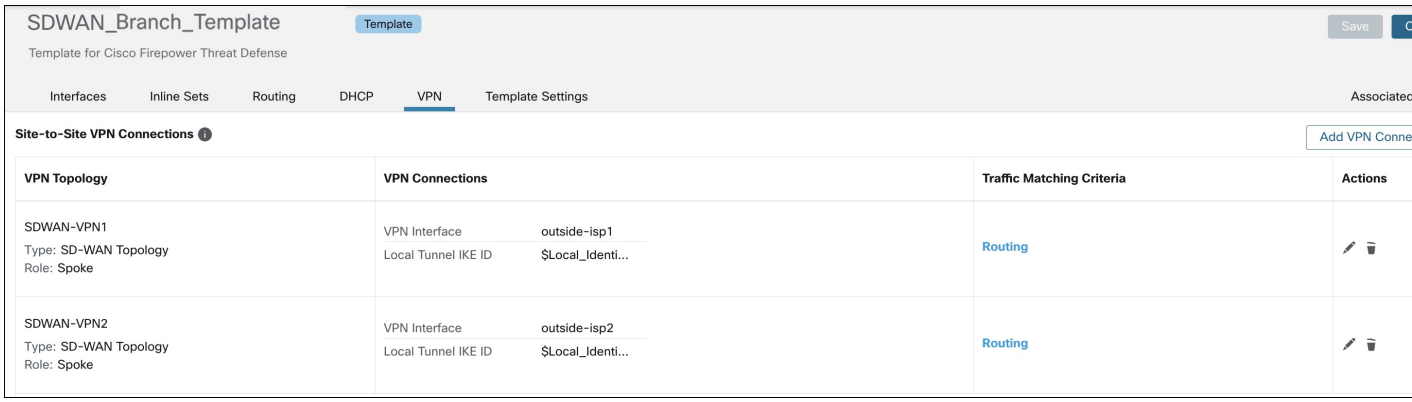
You can view the VPN connection in the **Site-to-Site VPN Connections** table.

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



Map Template Interfaces to Device Model Interfaces

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

Step 3 Click the **Template Settings** tab.

Step 4 In the left pane, choose **Model Mapping**

Step 5 Click **Add Model Mapping**.

Step 6 Choose the **Device Model** from the drop-down list.

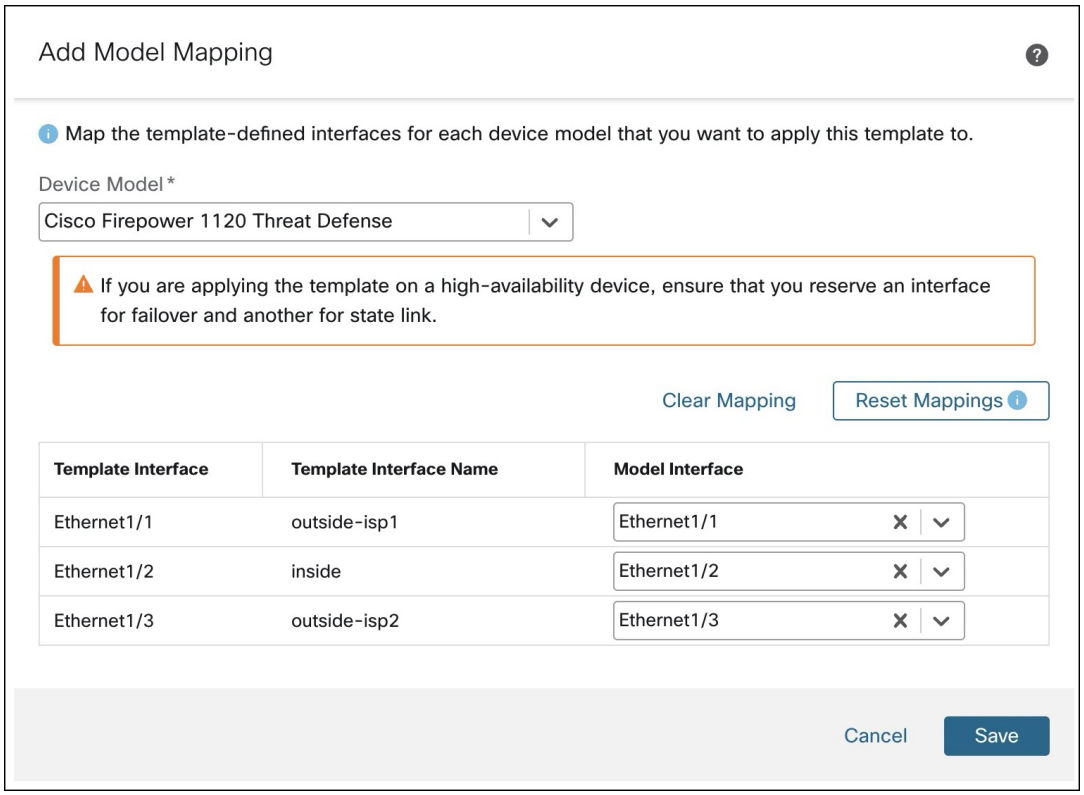
In this example, we choose a Cisco Firepower 1120 Threat Defense.

Step 7 Map the template interfaces to the device model interfaces by choosing the interface from the **Model Interface** drop-down list.

Note
You can 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 8 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.



Onboard a Device to the Management Center Using a Registration Key and Device Template

You can use the device template to add a device, register the device with the Management Center, and bring up the device with the given template configurations.

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.

A sample checklist is given below.

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

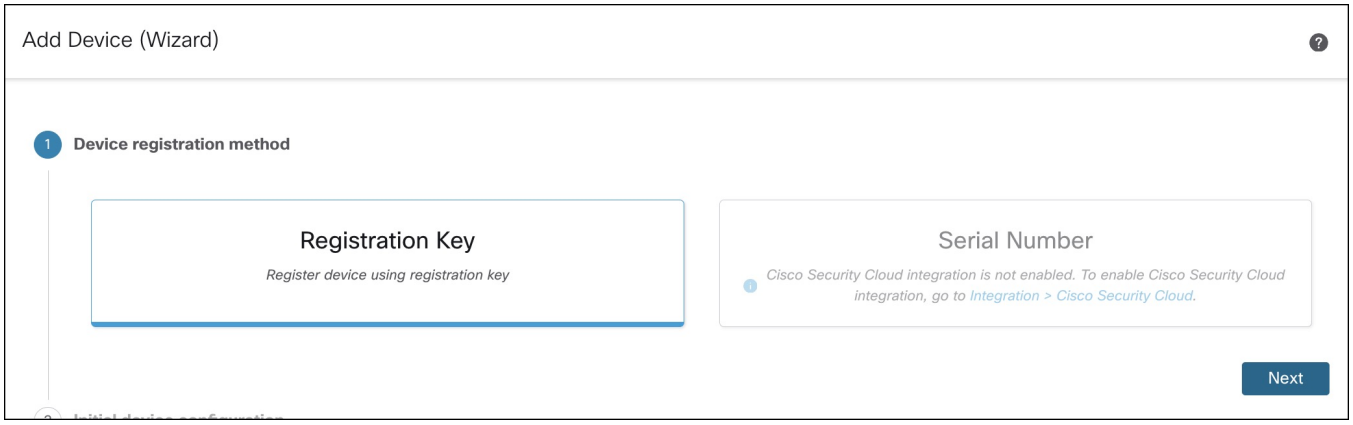
Note If you add a Threat Defense device that will be managed by a data interface for Management Center connectivity, ensure that you configure the template to be compatible with the connectivity parameters of the device. For more information, see Configure a Template for Threat Defense Devices Managed Through the Data Interface.

Procedure

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

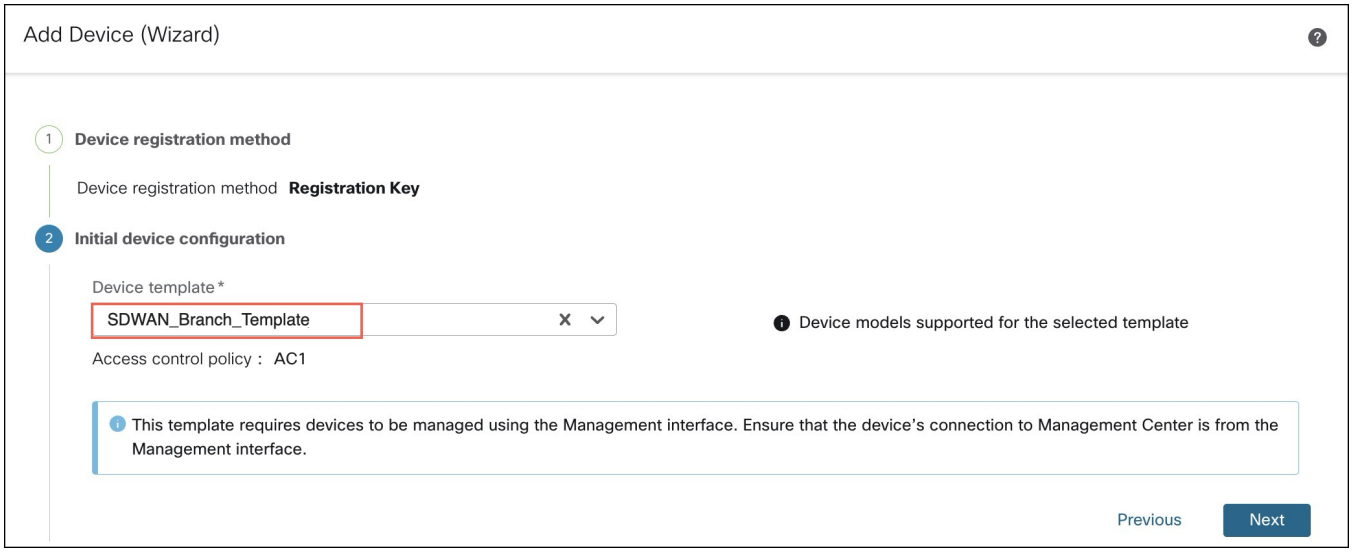
Step 2 Click **Add** > **Device (Wizard)**.

Step 3 On the **Add Device (Wizard)** window, choose **Registration Key** to register a device using registration key.



Step 4 Click **Next**.

Step 5 Choose a template from the **Device template** drop-down list.



Step 6 Click **Next**.

Step 7 In the **Host** field, enter the IP address or the hostname of the device you want to add.

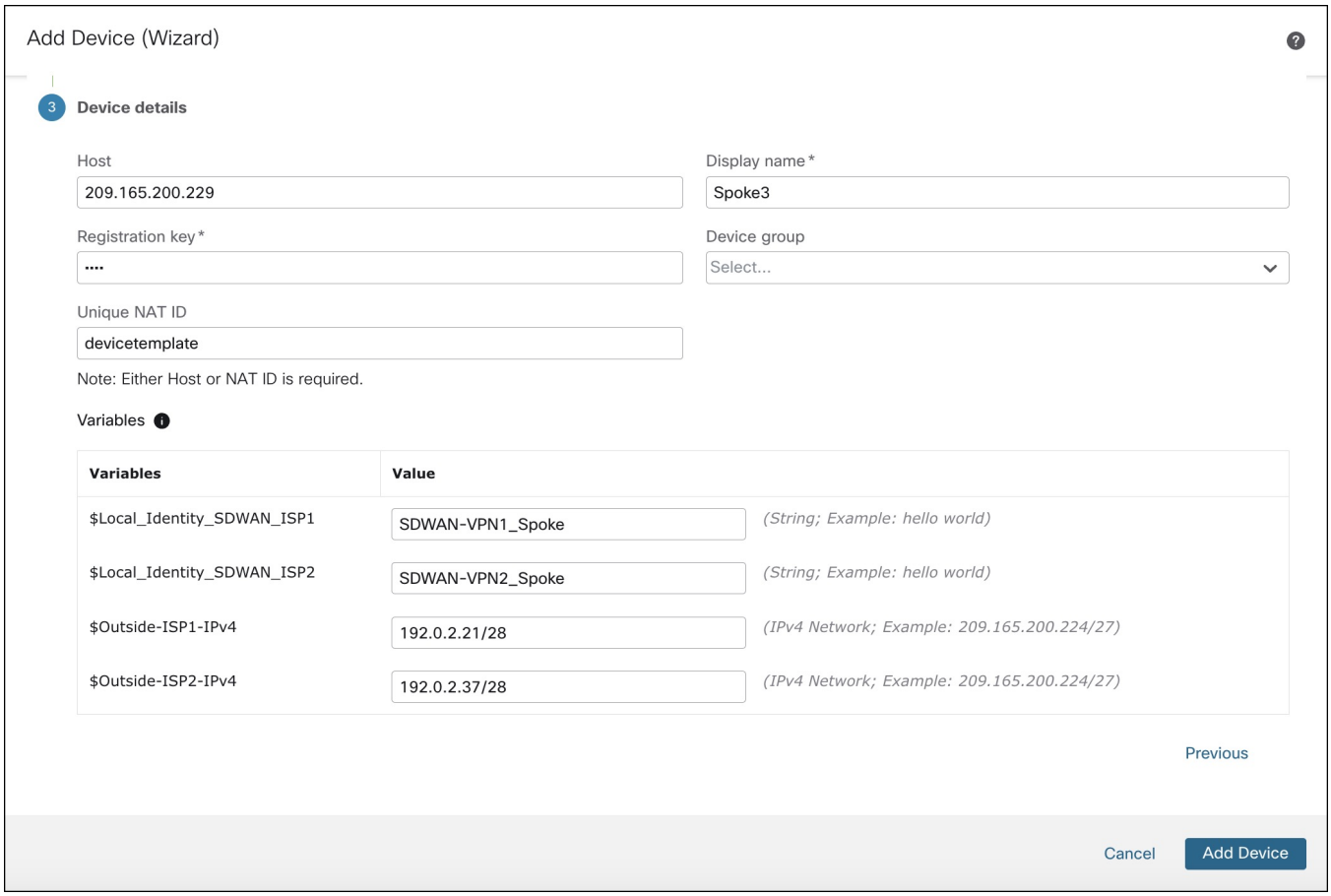
The hostname of the device is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address. Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

Step 8 In the **Display name** field, enter a name for the device as you want it to display in the management center.

Step 9 In the **Registration key** field, enter the same registration key that you used when you configured the device to be managed by the management center. The registration key is a one-time-use shared secret. The key can include alphanumeric characters and hyphens (-).

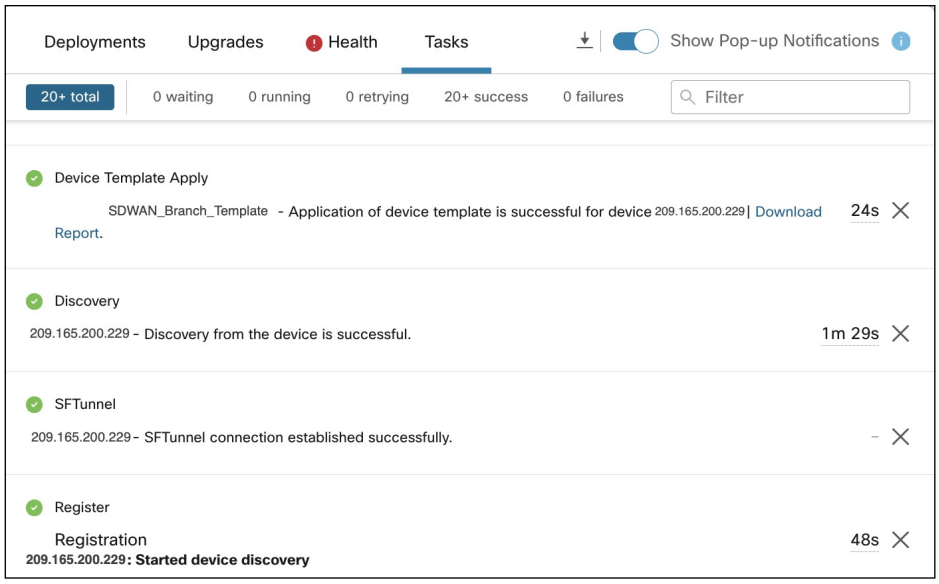
Step 10 (Optional) From the **Device group** drop-down list, choose a device group in which the device is added.

Step 11 Enter values for the **Variables** and **Network object overrides**.



Step 12 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.

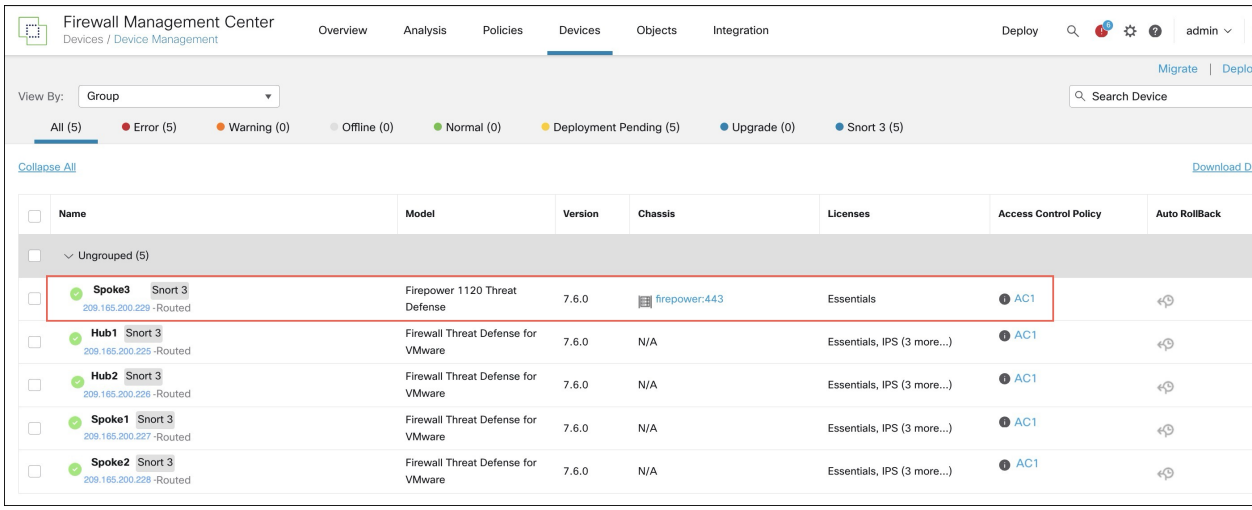


A **Device Template Apply** report is generated after the apply template task is completed. This report is generated on both successful and unsuccessful application of the template on the device. You will see a link to this report in the **Notifications** > **Tasks** window.

Verify Tunnel Statuses and Configurations of Route-Based VPN

View the Onboarded Device in the Device Management Page

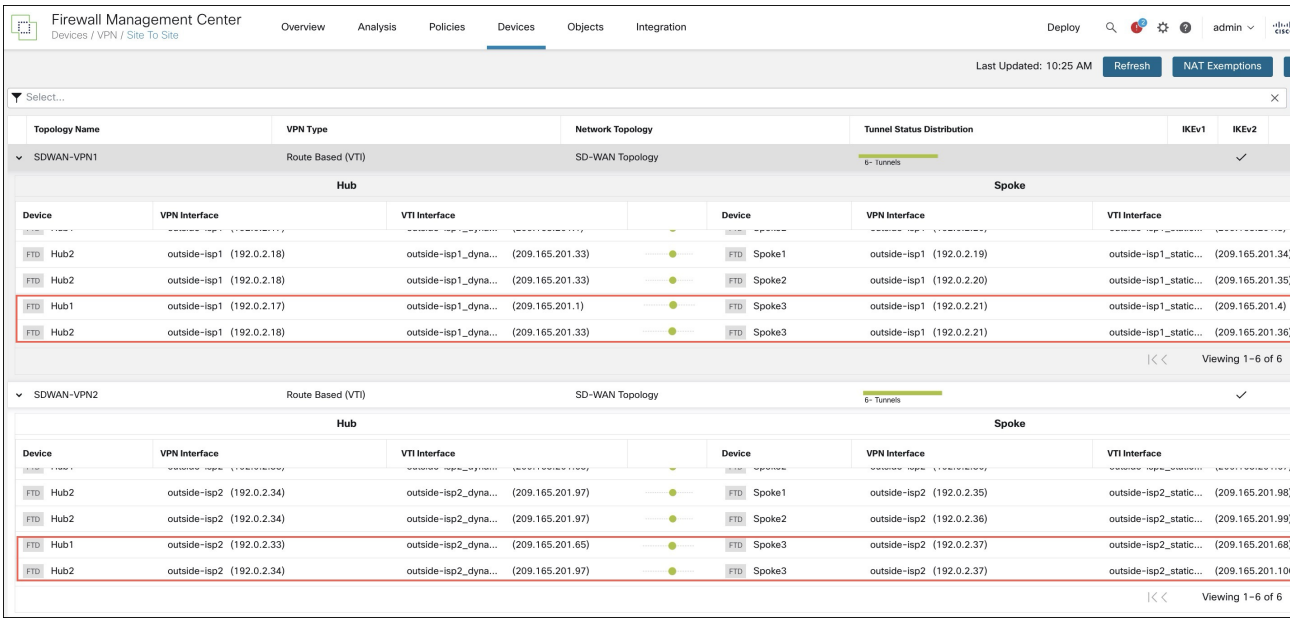
After the device template is successfully applied on the device, you can view the device in the **Device Management** page.



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**.

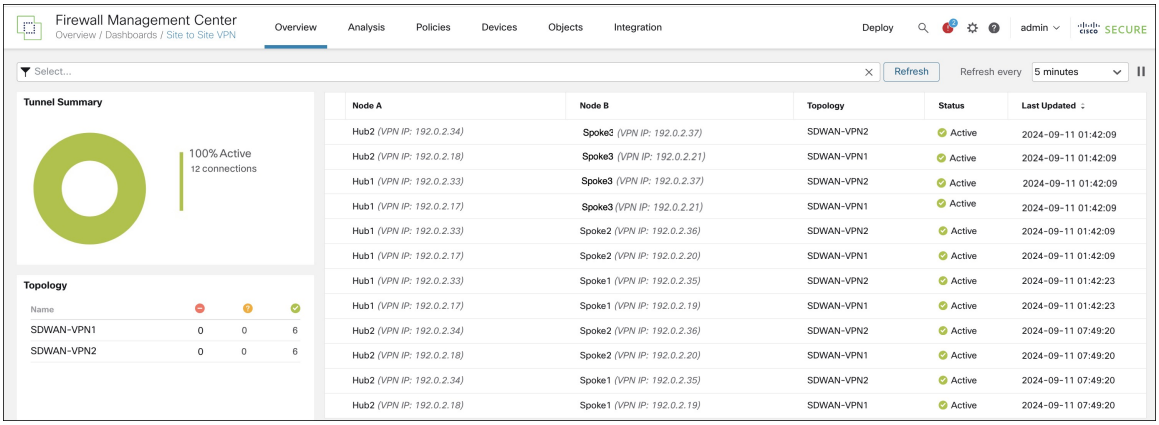
After the device template is successfully applied on the device, the device (Spoke3) gets added to the SD-WAN topologies.You can view the VPN tunnels between the hubs and the spokes, and also the VPN tunnels between the hubs and the onboarded device, Spoke3.



Verify Tunnel Statuses in the Site-to-Site VPN Dashboard

To view details of the SD-WAN VPN tunnels, choose **Overview > Dashboards > Site-to-site VPN**.

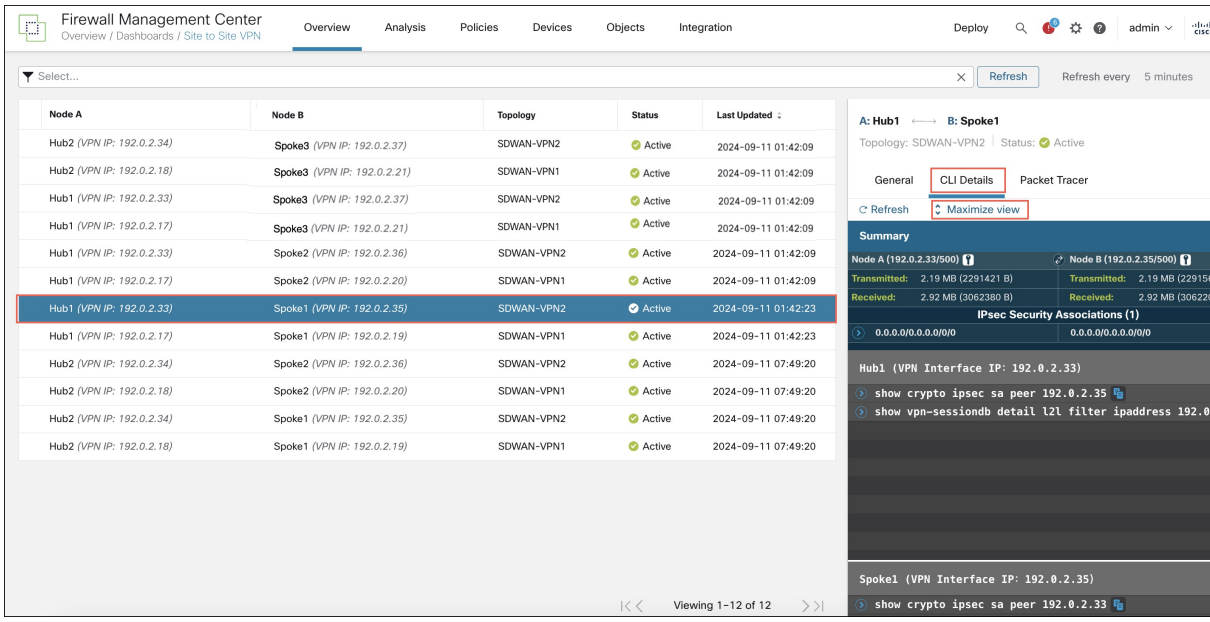
Following are the VPN tunnels of the two SD-WAN topologies: SDWAN-VPN1 and SDWAN-VPN2:



You can also see the VPN tunnels between Spoke3 and the two hubs.

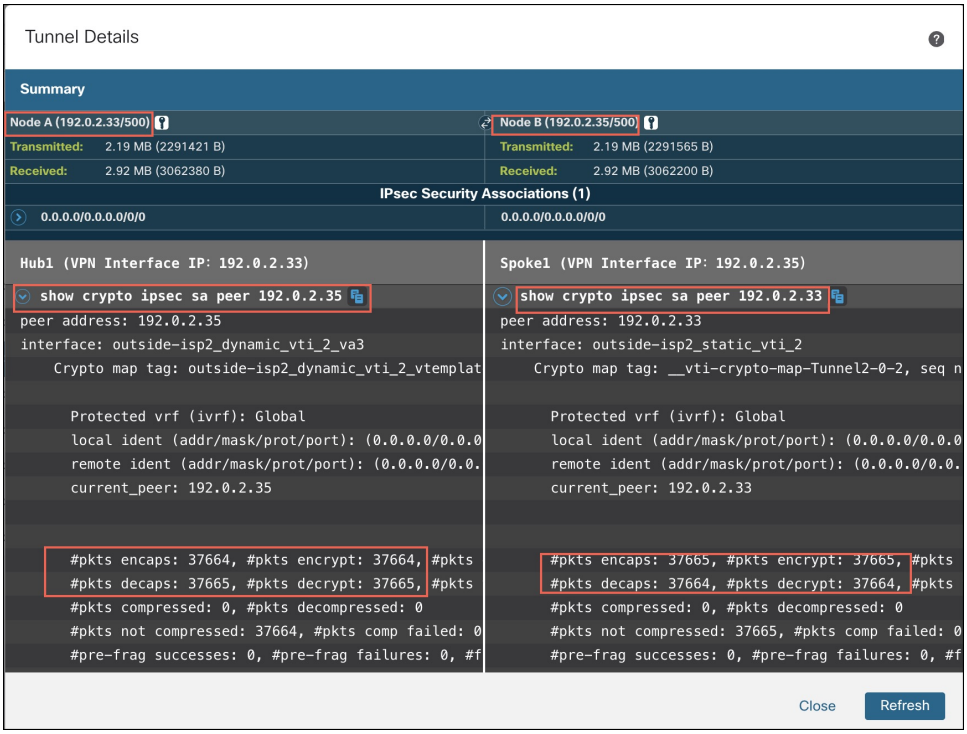
To see more details about each tunnel:

1. For each tunnel, hover your cursor over a topology and click the **View** icon to view more information about the tunnels.
2. Click the **CLI Details** tab.

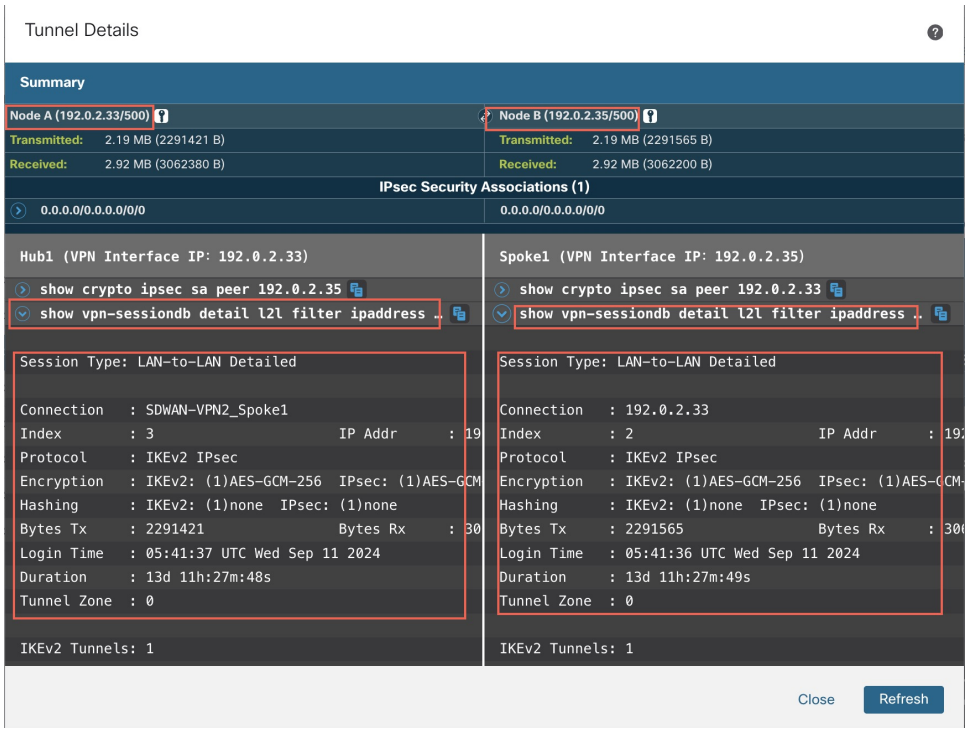


3. Click **Maximize View**. You can view the output of the following commands:

   - **show crypto ipsec sa peer**: Shows the number of packets that are transmitted through the tunnel.



   - **show vpn-sessiondb detail l2l filter ipaddress**: Shows more detailed data for the VPN connection.

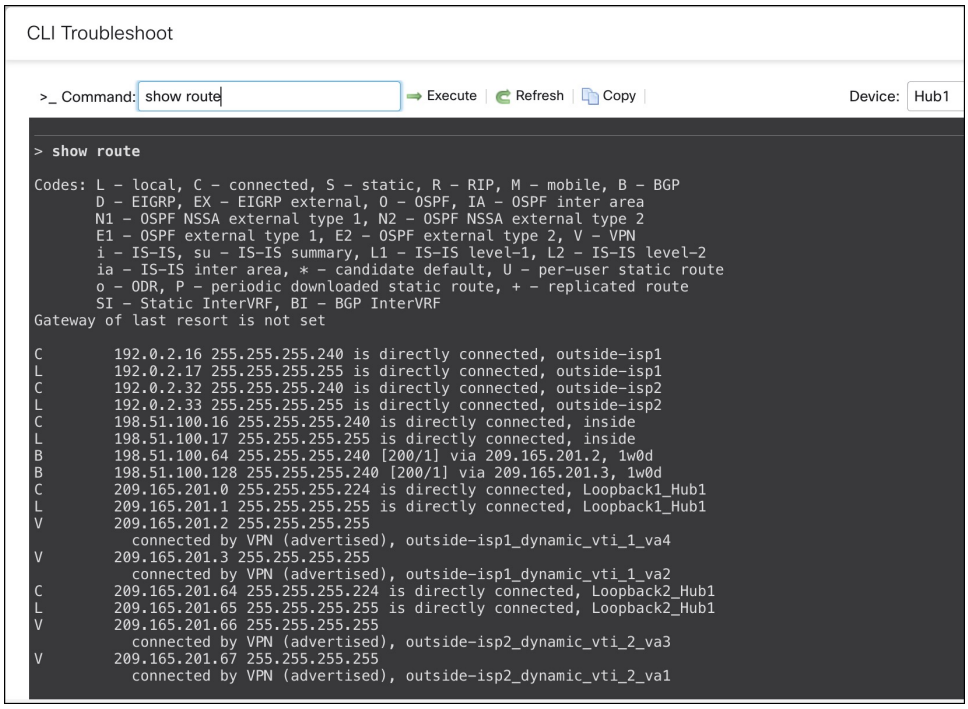


Verify Routing Information of the Threat Defense Device

To verify the routing information of the hub and the spokes, use the **show route** command on the device using the Management Center or the device CLI. You can also use the **show bgp** command.

1. In the Management Center, choose **Devices > Device Management**.
2. Click the edit icon adjacent to the device.
3. Click the **Device** tab.
4. Click **CLI** in the **General** card.

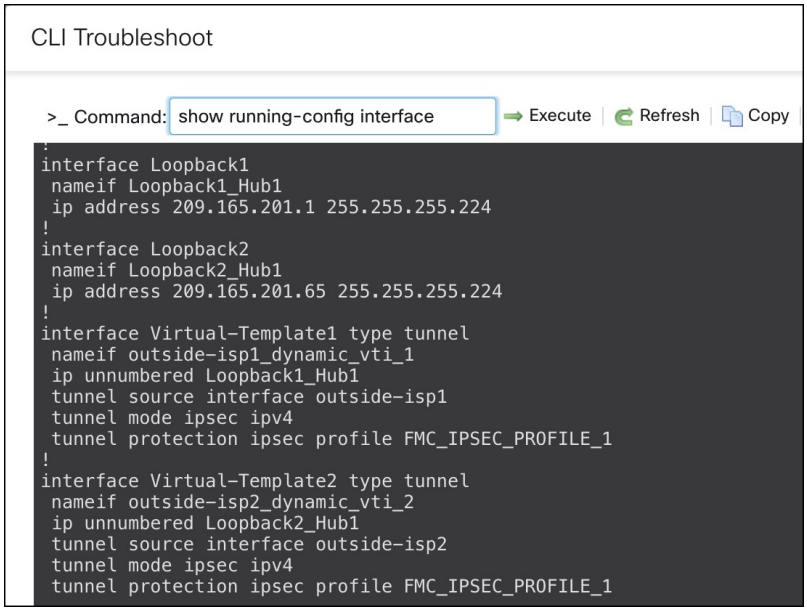
   In the **CLI Troubleshoot** window, enter **show route** in the **Command** field and click **Execute**.



You can also use the **show bgp** or **show bgp summary** commands.

View Tunnel Interface Configurations of the Threat Defense Device

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



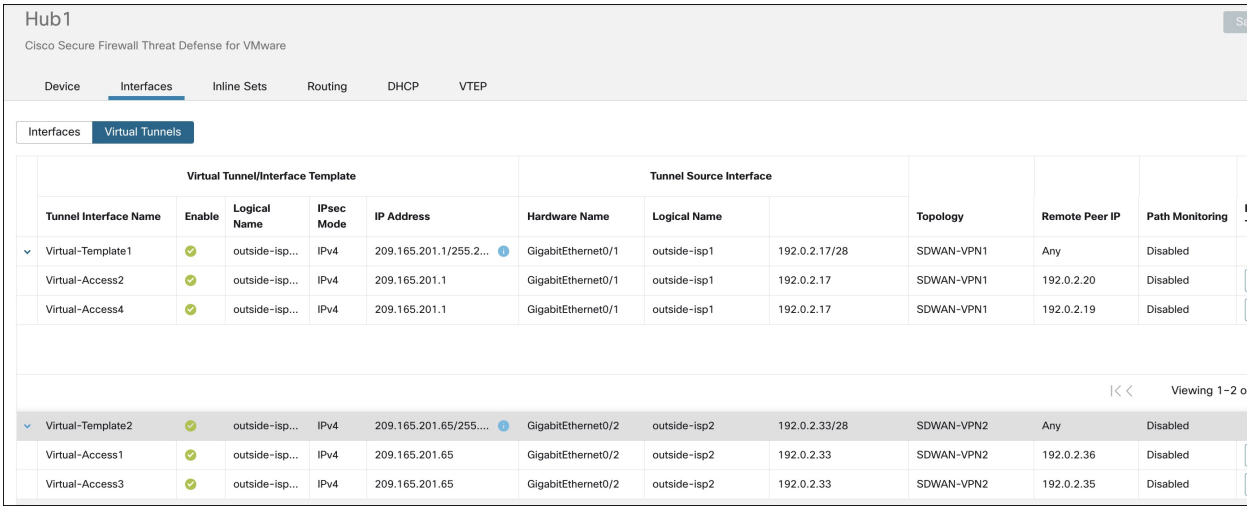
To view the dynamic VTIs of hubs and static VTIs of spokes:

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

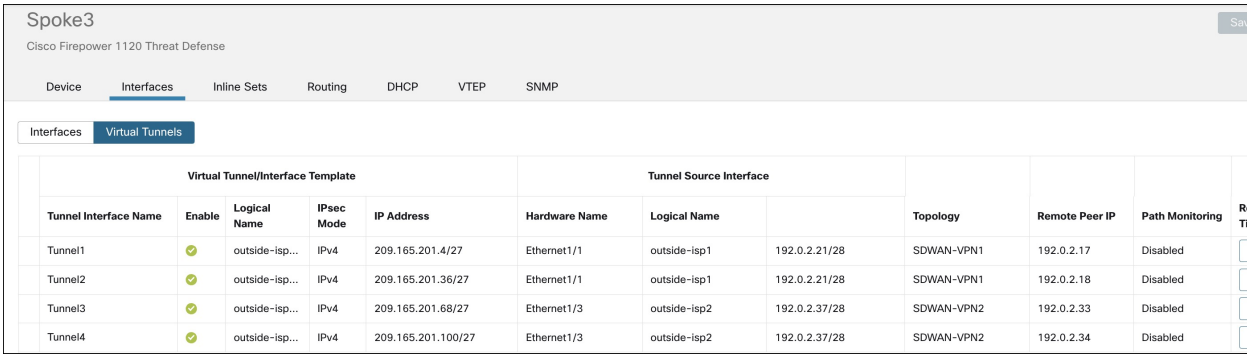
2. Click the edit icon adjacent to the device.
3. Click the **Interfaces** tab.
4. Click the **Virtual Tunnels** tab.

   For each VTI, you can view details such as name, IP address, IPsec mode, tunnel source interface details, topology, and remote peer IP.

   The dynamic VTI and the dynamically created virtual access interfaces of Hub1 are shown in the figure below:



   The static VTIs created on Spoke1 are shown in the figure below:



Troubleshoot Device Templates and Route-Based VPN Tunnels

Troubleshoot Device Templates

- Use the **Device Template Apply** report for initial troubleshooting:
  1. Check the errors mentioned in the report.
  2. Review variable values and network object overrides values. Check for overlaps and incompatibilities.

3. Check model mappings to ensure if the correct model mappings exist. Delete or add mappings accordingly.
4. Verify if the device or template is locked because of tasks such as application or modification of the template.
5. See the Management Center audit logs to find any other issues and resolve them.

- Use **Audit Logs**:

  Logs related to application of the device template, configuration updates, device template creation, and deletion, are logged under audit logs. The device template audit logs are added to the log both at the start and at the end of the task to apply the template on the device.

  An audit diff file is also generated that enables you to view configuration changes that have been done during application of the template on the device. To view the diff file:

  1. Choose **System > Monitoring > Audit**.

     The device template logs are logged under the subsystem **Devices > Template Management**.

  2. Click the diff icon to open a new window that displays the configuration changes that have been done during the application of the template on the device.

Troubleshoot Route-Based VPN Tunnels

After the deployment, use the following CLI commands and tools to debug issues related to route-based VPN tunnels on Threat Defense devices.

CLI and Debug Commands

Command	Description
ping	Ping the outside IP address of the peer to the check the connectivity between the devices.
show vpnsession db	Displays summary information about current VPN sessions.
debug crypto condition peer <peer-IP>	Enable conditional debugging for a particular peer
debug vti 255	Debug the Virtual Tunnel Interface information.

Packet Tracer

The Packet Tracer tool allows you to test policy configurations by modeling a packet with source and destination addresses, and protocol characteristics. Besides verifying your configuration, you can use this tool to debug unexpected behaviour, such as packets being denied access.

To use a packet tracer on Threat Defense devices, choose **Devices > Packet Tracer**. You must be an Admin or Maintenance user to use this tool.

You can also use the Packet Tracer in the **Site to Site VPN Dashboard** to troubleshoot VPN tunnels between two Threat Defense devices.

1. Choose **Overview > Dashboards**.

2. For each tunnel, hover your cursor over a topology and click the View icon to view more information about the tunnels.
3. Click the **Packet Tracer** tab.
4. Configure the parameters.
5. Click **Trace Now**.
6. After the trace completes, you can view the output of the trace with the results of each module.