cisco.



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

	Full Cisco Trademarks with Software License ?				
CHAPTER 1	Getting Started 1				
	About This Publication 1				
	Cisco Secure Firewall 1				
	Overview of SD-WAN Capabilities 2				
	Features 3				
CHAPTER 2	Simplify Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI) 5				
	Route-based VPN in a Hub and Spoke Topology 5				
	Benefits 6				
	Is This Use Case For You? 6				
	Scenario 7				
	Network Topology 7				
	Best Practices 8				
	Prerequisites 8				
	End-to-End Procedure for Configuring a Route-based VPN (Hub and Spoke Topology) 9				
	Create a Route-based Site-to-Site VPN 10				
	Configure the Endpoint for the Hub Node 11				
	Configure the Endpoint for the Spoke Node 12				
	Configure OSPF on the Hub Node 14				
	Configure OSPF on the Spoke Node 16				
	Configure the Access Control Policy 17				
	Deploy Configuration 20				
	Verify Traffic Flow Over the VPN Tunnel 20				
	Configure the Backup VTI Interface on the Spoke Node 24				

Configure an ECMP Zone for the Primary and Secondary VTI Interfaces 26 Verify the Primary and Secondary Tunnels 26 Troubleshoot Route-based VPN Tunnels 30 Additional Resources 30

CHAPTER 3

Route Application Traffic from the Branch to the Internet Using Direct Internet Access (DIA) 31

Direct Internet Access 31 Benefits 33 Is This Use Case For You? 33 Components for Direct Internet Access 33 **Best Practices** 34 Prerequisites 34 Scenario 1: Direct Internet Access 34 Network Topology for DIA 35 End-to-End Procedure for Configuring DIA 36 Scenario 2: Direct Internet Access With Path Monitoring 37 Network Topology-DIA With Path Monitoring 37 End-to-End Procedure for Configuring DIA With Path Monitoring 38 Configure a Trusted DNS Server 40 Configure Interface Priority 41 Create an ECMP Zone 41 Configure an Equal Cost Static Route 42 Configure Path Monitoring Settings 42 Configure an Extended ACL Object for YouTube 43 Configure an Extended ACL Object for WebEx 43 Configure a Policy Based Routing Policy for YouTube 44 Configure a Policy Based Routing Policy for WebEx 45 Configure a Policy Based Routing Policy With Path Monitoring for Webex 46 Deploy Configuration 47 Verify Application Traffic Flow 47 Monitor and Troubleshoot Policy Based Routing 49 Additional Resources 52

CHAPTER 4 Secure Internet Traffic Using Umbrella Auto Tunnel 55

Cisco Umbrella Auto Tunnel 55
Benefits 56
Is This Use Case For You? 57
Scenario 57
Network Topology 57
Best Practices for SASE Umbrella Tunnels 58
Prerequisites for Configuring Umbrella SASE Tunnels 58
Best Practices for SASE Umbrella Tunnels 59
Prerequisites for Configuring Umbrella SASE Tunnels 59
End-to-end Procedure for Configuring Umbrella Auto Tunnel 60
Configure a SASE Tunnel for Umbrella 61
Configure a Static Route 65
Configure an Extended ACL for DNS and Web Traffic 65
Configure a PBR Policy for DNS and Web Traffic 66
Deploy Configuration 67
Verify SASE Umbrella Tunnel Deployment 67
Troubleshoot Umbrella Auto Tunnels 72
Additional Resources 73

CHAPTER 5	Empower Remote Workers with Secure Connectivity: DIA, Umbrella Auto Tunnel, and DVTI in Action 75						
	Enhancing Connectivity and Security for Remote Workers with DIA, Umbrella SASE Auto Tunnel and DVTI 75						
	Is This Use Case For You? 75						
	Scenario 76						
	Topology 76						
	End-to-end Procedure for Configuring DIA, Umbrella Auto Tunnel, and DVTI 77						
	Additional Resources 77						
CHAPTER 6	Set Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates 79						
	Introduction 79						
	Is this Guide for You 80						
	Scenario 80						
	System Requirements 80						

Prerequisites 81
Guidelines and Limitations 81
Network Topology 81
End-to-End Procedure for Setting Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates 83
Configure SD-WAN Topologies Using the SD-WAN Wizard 84
Create a Device Template 89
Add a Physical Interface in the Template 90
Configure an SD-WAN VPN Connection in a Device Template 91
Map Template Interfaces to Device Model Interfaces 92
Onboard a Device to the Management Center Using a Registration Key and Device Template 94
Verify Tunnel Statuses and Configurations of Route-Based VPN 97
Troubleshoot Device Templates and Route-Based VPN Tunnels 102



UNAFIE

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, on page 1
- Cisco Secure Firewall, on page 1
- Overview of SD-WAN Capabilities, on page 2
- Features, on page 3

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

I

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



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, on page 5
- Benefits, on page 6
- Is This Use Case For You?, on page 6
- Scenario, on page 7
- Network Topology, on page 7
- Best Practices, on page 8
- Prerequisites, on page 8
- End-to-End Procedure for Configuring a Route-based VPN (Hub and Spoke Topology), on page 9
- Create a Route-based Site-to-Site VPN, on page 10
- Configure the Endpoint for the Hub Node, on page 11
- Configure the Endpoint for the Spoke Node, on page 12
- Configure OSPF on the Hub Node, on page 14
- Configure OSPF on the Spoke Node, on page 16
- Configure the Access Control Policy, on page 17
- Deploy Configuration, on page 20
- Verify Traffic Flow Over the VPN Tunnel, on page 20
- Configure the Backup VTI Interface on the Spoke Node, on page 24
- Configure an ECMP Zone for the Primary and Secondary VTI Interfaces, on page 26
- Verify the Primary and Secondary Tunnels, on page 26
- Troubleshoot Route-based VPN Tunnels, on page 30
- Additional Resources, on page 30

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.
- 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
	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.

Firew Site To	vall Management o Site	Center	Overview	Analysis	Policies	Devices	Objects	s Integration	Deploy	Q	C	¢ 0	admin \checkmark
					Last Upo	dated: 01:2	1 AM	Refresh	+ Site to Si	te VPN		+ SASE	Topology
▼ Se	elect											×	Refresh
	Topology Name	VPN Ty	pe	N	letwork Topo	logy	Tu	nnel Status Distri	bution		IKEv1	IKEv2	
~	Corporate-VPN	Route E	Based (VTI)	F	lub & Spoke		De	eployment Pendir	ng			\checkmark	1
			Hub						Spoke				
De	vice	VPN Interfa	ce	VTI Interface			Device		VPN Interfac	е	V	TI Interfa	ce
FT	D NGFW1	out (198	3.18.133.81)	out (198.4	48.133.81)		FTD N	GFWBR1	outsi (19	8.19.30	0.4) o	uts (1	69.254.20.1)

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.

0

Create New VPN Topology

Topology Name:*							
Corporate-VPN							
O Policy Based (Crypto Map) Route Based (VTI)							
Network Topology:							
Point to Point Hub and Spoke Full M	esh						
IKE Version:* 🗌 IKEv1 🗹 IKEv2							
Endpoints IKE IPsec Advanced							
Hub Nodes:			+				
Device Name	VPN Interface	Traffic Match Criteria					
FTD NGFW1 outside_dynamic_vti_1 (198.48.133.81) Routing Policy			11				
Spoke Nodes:			+				
Device Name	VPN Interface	Traffic Match Criteria					
FTD NGFWBR1	outside_static_vti_1 (169.254.20.1)	Routing Policy	/ 1				

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

Ston 1	To edit the hub node, choose Davices > Davice Management and click the Edit (\mathcal{A}) icon for the NGEW1 node
	To cut the hub hole, choose Device Management and check the Eurit (*) from for the NOT without.
Step 2	In the Interfaces tab, verify the Loopback1 interface that was created earlier and serves as the IP address for the DVII 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.

NOTINA

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

Cisco Firepo	wer Threat Defense fo	r VMWare						
Device	Routing Interfac	es Inline Sets	DHCP	VTEP				
Manage V	irtual Routers	Process 1		ID:	1			
		OSPF Role:						
Global	•	Internal Router		•	Enter Description	here	Advanced	
Virtual Rout	ter Properties			ID:				
ECMP		Process 2		ID.				
BFD		OSPF Role:						
OSPF		Internal Router		v	Enter Description	here	Advanced	
OSPFv3								
FIGDD		Area Redi	stribution	InterArea	Filter Rule	Summary Address	Interface	
RIP								
Policy Base	ed Routing	OSPE Process	Are: Area	Type	Networks	Ontions	Authentication	
V RGP		our Ploces:	Ale Alea	i i î be	Networks	opuons	Automitication	
IPv4		1	1 norm	nal	HUB_Tunnel_IP	false	none	

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

Configure OSPF on the Spoke Node

Procedure

Step 1 Step 2	To edit the spoke node, choose Devices > Device Management and click the Edit () icon for the NGFWBR1 node. 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.

NGFWBR1 Cisco Firepower Threat Defense for	VMWare				
Device Routing Interface	es Inline Sets DHCP	VTEP			
Manage Virtual Routers	✓ Process 1	ID:	1		
Global 🔻	OSPF Role: Internal Router	•	Enter Description here		Advanced
Virtual Router Properties ECMP	Process 2	ID:			
BFD OSPF	OSPF Role: Internal Router	Ŧ	Enter Description here		Advanced
OSPFv3	Area Redistribution	InterArea	Filter Rule Sum	mary Address	Interface
RIP					
Policy Based Routing	OSPF Proces Area ID	Area Type	Networks	Options	Authentication
∽ BGP IPv4	1 1	normal	Spoke_Tunnel	false	none

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

L

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

10 Citing Rule Allow-To-Branch-Ove	er-Tunnel		NGFW1 Default 🖉
Name Allow-To-Branch-Over-Tunnel	1 Action	🗢 Allow	Logging ON 🐻 Time Range None
	Intr	usion Policy None	Select Variable Set
Q Zones (2) Networks (2) Ports	Applications	Users URLs Dynamic Attrib	utes VLAN Tags
Q Tunnel X	Showing 1 out of 11	Selected Sources: 2	Selected Destinations and Applicati 2
<u>A</u> Tunnel_Zone (Routed Security Zone)		Collapse All Remove All	Collapse All Remove All
		ZONE v 1 object InZone1	ZONE ~ 1 object
		NET v 1 object Corporate-LAN	NET v 1 object Branch-LAN
+ Create Security Zone Object		Add Source Zone	Add Destination Zone
Comments A			Cancel Apply

- c. Click Apply to save the rule.
- **d.** To edit the **Allow-To-Corp-Over-Tunnel** policy, click the **Edit** (\mathscr{I}) icon.
- e. In the Zones tab, search for Tunnel_Zone, select it, and click Add Source Zone.

11 Citing Rule Allow-To-Corp-Over-Tunnel	NGFW1 Default
Name Allow Action Allow	Image: Select Variable Set Image: Select Variable Set
Q Zones (2) Networks (2) Ports Applications Users	URLs Dynamic Attributes VLAN Tags
C Tunnel X Showing 1 out of 11	Selected Sources: 2 Selected Destinations and Applications: 2
Tunnel_Zone (Routed Security Zone)	Collapse All Remove All Collapse All Remove All ZONE 1 object Branch-LAN Comporter LAN Collapse All Colapse All Colapse All Colla
+ Create Security Zone Object	Add Source Zone Add Destination Zone
	Cancel Apply

- 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.

4 Citing Rule Allow-To-Branch-Over-T	Tunnel		
Name Allow-To-Branch-Over-Tunnel	1 Action O Allow	Sector Logging ON	Time Range None
	Intrusion Policy	ne 🔍 Select Vari	able Set V File Policy None
Q Zones (2) Networks (2) Ports	Applications Users	URLs Dynamic Attributes VLAN Ta	gs
Q. Tunnel	× Showing 1 out of 11	Selected Sources: 2	Selected Destinations and Applications: 2
Tunnel_Zone (Routed Security Zone)		Collapse All Remove All ZONE 1 object Tunnel_Zone NET 1 object Corporate-LAN 	Collapse All Remove All ZONE • 1 object InZone NET • 1 object Branch-LAN
+ Create Security Zone Object		Add Source Zone	Add Destination Zone
Comments A			Cancel Apply

- **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.

3	Citing Rule Allow-To-Corp-Over-Tun	nel						Branch Access Control	Default)
Nai	Me Allow-To-Corp-Over-Tunnel	î,	Action	Allow			ogging	ON 🐻 Time Range	None	Î
			Intrus	sion Policy	None			Select Variable Set	~	l
(C Zones (2) Networks (2) Ports	Applicati	ions	Users	URLs	Dynamic Attrib	utes	VLAN Tags		l
	R Tunnel X Show	wing 1 out o	of 11	Selecte	d Sources: 2		Select	ed Destinations and Appl	icati 2	1
E	Tunnel_Zone (Routed Security Zone)			Collaps	e All	Remove All	Collap	se All Ren	nove All	1
				ZONE	✓ 1 object InZone		ZONE	 ✓ 1 object ∴ Tunnel_Zone 		l
				NET	✓ 1 object Branch-LA	AN	NET	✓ 1 object Corporate-LAN		l
	+ Create Security Zone Object				Add Source	Zone	[Add Destination Zone		Ŧ
c	Comments ~							Cancel	Apply	

- 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

On the management center menu bar, click Deploy . This displays the list of devices that are Ready for Deployment.
Check the checkboxes adjacent to NGFWBR1 and NGFW1 on which you want to deploy configuration changes.
Click Deploy . Wait till the deployment is marked Completed on the Deploy dialog box.
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**.

Firewall Manager Overview / Dashboards	Ment Center / Site to Site VPN	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 💰	₽ \$ 0
Device NGFW1 × × S	elect						×	Apply Cancel	Refresh ever
Tunnel Summary			Node A			Node B		Topology	Status
			NGFW1	(VPN IP: 198.1	8.133.81)	NGFWBR1	(VPN IP: 198.19.30.4)	Corporate-VPN	Active
0	100% Active 1 connection								
Topology									
Name	e e	0							
Corporate-VPN	0 0	1							

- 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.

Firewall Management Center Overview Overview / Dashboards / Site to Site VPN Overview	ew Analysis Policies Devices Objects	Integration Deploy Q	admin ~ dudu SECU
Pevice NGFW1 × × Select		X Apply Cancel	Refresh every 5 minutes 🗸
Node & Node 8 NGFW1 (VPW IP: 198.18.133.87) NGFWBR1 (VPW IP: 198	Topology Status Last Updated + 19.30.4) Corporate-VPN O Active 2023-07-05 02:0	A: NGFW1 ←→→ B: NGFWBR1 Topology: Corporate-VPN Status: @ General CLI Details Packet) Active t Tracer
Summary		C Refresh C Maximize view) Hard - D (400 40 70 4/500) (7)
Node A (198.18.133.81/500) Transmitted: 4.69 KB (4804 B) Received: 6.07 KB (6212 B)	Image: Work of Control (1) Image: Work of Control (1) Transmitted: 4.86 KB (4972 B) Received: 5.94 KB (6084 B)	Node A (198.18.13.81/500)	Transmitted: 4.86 KB (4972 B) Received: 5.94 KB (6084 B)
Settings: L2L,Tunnel,IKEV2,VTI Encaps/Encrypt: 59 / 59 pkts Dcaps/Decrypt: 52 / 62 pkts	Associations (1) Settings: L2L,Tunnel (KEv2,VTI Encaps/Encrypt: 62 / 62 pkts Dcaps/Docrypt: 60 / 60 pkts	IPsec Security / Sattings: L2L,Tunnel,IKEv Encaps/Encrypt: 59 / 59 pkts Dcaps/Decrypt: 62 / 62 pkts	Associations (1) Settings: L2L,Tunnel,IKEv2,VTI Encaps/Encrypt: 62 / 62 pkts Dcaps/Decrypt: 60 / 60 pkts
Remaining Lifetim Outbound: 3.82 GB (4101115000 B) 02:51:27 (28287 sec) Remaining Lifetim	a for SPI ID: 0xF96273E3 Inbound: 3.91 GB (4193275000 B) 02:51:26 (28286 sec) a for SPI ID: 0x201775BF	Remaining Lifetime Outbound: 3.82 GB (4101115000 B) 02:51:27 (28287 sec) Remaining Lifetime	
Inbound: 3.78 GB (4055035000 B) 02:51:27 (28287 sec)	Outbound: 3.78 GB (4055035000 B) 02:51:26 (28286 sec)	Inbound: 3.78 GB (4055035000 B) 02:51:27 (28287 sec)	Outbound: 3.78 GB (4055035000 B) 02:51:26 (28286 sec) 33.81)
Show crypto ipsec sa peer 198.19.30.4 peer address: 198.19.30.4 interface: butside_dynamic_vti_1_val Crypto map tag: outside_dynamic_vti_1_vtempla	show crypto ipsec sa peer 198.18.133.81 peer address: 198.18.133.81 interface: putside_static_vti_1 Crypto map tag:vti-crypto-map-Tunnel1-0-1	 show crypto ipsec sa peer 198. show vpn-sessiondb detail 121 	19.30.4 📲 filter ipaddress 198.19.30.4 📲

- 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.

>_ Command: show route ⇒ Execute
PC-respective PC
> show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IX - OSPF inter area NI - OSPF NS5A external type 1, N2 - OSPF external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - OOR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is 198.18.128.1 to network 0.0.0
<pre>S* 0.0.0 0.0.0 [1/0] via 198.18.128.1, outside S 11.11.60.0 255.255.255.0 [1/0] via 198.18.133.60, outside V 160.254.20.1 255.255.255.255 connected by VPN (advertised), outside dynamic vti 1 val C 198.18.133.81 255.255.255.255 is directly connected, outside 1 198.18.133.81 255.255.255.255 is directly connected, outside C 198.19.10.0 255.255.255.255 is directly connected, in10 0 198.19.10.1 255.255.255.255.0 is directly connected, in12 C 198.19.20.1 255.255.255.0 is directly connected, in20 C 198.19.20.1 255.255.255.0 is directly connected, in20 0 198.19.20.1 255.255.255.0 is directly connected, in20 C 198.19.20.1 255.255.255.0 is directly connected, in20 C 198.19.20.1 255.255.255.0 is directly connected, in20 C 198.19.30.0 255.255.255.0 is directly connected, in20 C 198.19.30.0 255.255.255.0 is directly connected, in20 C 198.19.30.0 255.255.255.0 if /0] via 198.18.133.64, outside C 198.48.133.81 255.255.255.255 is directly connected, Hub_Tunnel_IP</pre>

- 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.

>_ Co	ommand: show route	⇒ Execute Copy	Device: NGFWBR1	~
> sho	w route			
Codes	<pre>: L - local, C - connected, S - st D - ELGRP, EX - ELGRP external, ' N1 - OSPF NSSA external type 1, E2 - i - IS-IS, su - IS-IS summary, L ia - IS-IS inter area, * - candi o - OOR, P - periodic downloaded SI - Static InterVRF, BI - BGP I ay of last resort is 198.19.40.64</pre>	atic, R - RIP, M - mobile, B - BGP O - OSPF, IA - OSPF inter area NZ - OSPF NSSA external type 2 OSPF external type 2, V - VPN 1 - IS-IS level-1, L2 - IS-IS level-2 date default, U - per-user static route static route, + - replicated route nterVRF to network 0.0.0.0		
s*	0.0.0.0 0.0.0.0 [1/0] via 198.	19.40.64. outside2		
5*	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198.	19.40.64, outside2 19.30.63, outside3		
s* c	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255 i	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP		
5* C	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255.255 i 198.18.128.0 255.255.192.0 is	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside		
5* C C L	0.0.0.0 0.0.0 [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255 i 198.18.128.0 255.255.192.0 is 198.18.128.81 255.255.255.255	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside		
5* C L	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255.255 i 198.18.128.0 255.255.192.0 is 198.18.128.11 255.255.255.255 198.19.10.0 255.255.255.0	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside		
5* C L D	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255 i 198.18.128.0 255.255.255 i 198.18.128.0 255.255.255 i 198.19.10.0 255.255.255.255 i 198.19.10.0 255.255.255.0 [110/1572] via 198.48.133.81	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside , 00:22:52, outside_static_vti1 [1/0] uis 10.40.64 outside3		
5* - - -	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255.255.191.0 is 198.18.128.0 255.255.255.255.255 198.19.10.0 255.255.255.255 198.19.10.0 255.255.255.255 [10](11)(1572) via 198.48.133.81 198.19.10.100 255.255.255.255	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside , 00:22:52, outside_static_vti_1 [1/0] via 198.19.40.64, outside2 [1/0] via 198.19.40.64, outside3		
	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. [1/0] via 198. 109.254.20.1 255.255.255.155 198.18.128.0 255.255.255.102.0 is 198.18.128.0 255.255.255.255 198.19.10.0 255.255.255.255 198.19.10.00 255.255.255.255 198.19.10.100 255.255.255.0 is d	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside s directly connected, outside ,00:22:52, outside_static_vti_1 [/0] via 198.19.40.64, outside2 [/0] via 198.19.40.64, outside3 [/0] via 198.19.40.64, outside3		
;* - -	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255 i 198.18.128.81 255.255.255 i 198.19.10.0 255.255.255.05 [110/1572] via 198.48.133.81 198.19.10.100 255.255.255.255 198.19.11.0 255.255.255.05 is d 198.19.11.4 255.255.255.255.05 is d	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside , 00:22:52, outside_static_vti_1 [1/0] via 198.19.40.64, outside2 [1/0] via 198.19.30.63, outside3 irectly connected, inside directly connected, inside		
5* 	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255.255.255 198.18.128.0 255.255.255.255 198.19.10.0 255.255.255.255 198.19.10.0 255.255.255.255 [110/1572] via 198.48.133.81 198.19.10.100 255.255.255.0 is d 198.19.11.4 255.255.255.0 is d 198.19.11.4 255.255.255.0 is d	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside , 00:22:52, outside_static_vti_1 [1/0] via 198.19.30.63, outside3 irectly connected, inside directly connected, inside irectly connected, sinside		
	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. [1/0] via 198. 169.254.20.1 255.255.255.155. 198.18.128.0 255.255.255.192.0 is 198.18.128.0 255.255.255.255 198.19.10.0 255.255.255.255 198.19.10.100 255.255.255.255 198.19.11.4 255.255.255.0 is d 198.19.11.4 255.255.255.255 is 198.19.30.0 255.255.255.255 is 198.19.30.4 255.255.255.255 is	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside .00:22:52, outside_static_vti_1 [1/0] via 198.19.40.64, outside2 [1/0] via 198.19.40.64, outside3 directly connected, inside directly connected, outside3 directly connected, outside3		
	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. [1/0] via 198. 199.254.20.1 255.255.255 i 198.18.128.0 255.255.255 i 198.19.10.0 255.255.255.05 [110/1572] via 198.48.133.81 198.19.10.100 255.255.255.255 198.19.11.4 255.255.255.255 is 198.19.11.4 255.255.255.0 is d 198.19.30.0 255.255.255.0 is d 198.19.30.4 255.255.255.0 is d 198.19.30.4 0.255.255.255.0 is d	19.40.64, outside2 19.30.63, outside3 s directly connected, Spoke_tunnel_IP directly connected, outside is directly connected, outside , 00:22:52, outside_static_vti_1 [1/0] via 198.19.40.64, outside2 [1/0] via 198.19.30.63, outside3 irectly connected, inside directly connected, outside3 directly connected, outside3 directly connected, outside3 irectly connected, outside3		
5* 	0.0.0.0 0.0.0.0 [1/0] via 198. [1/0] via 198. [1/0] via 198. 109.254.20.1 255.255.255.25 198.18.128.0 255.255.255.192.0 is 198.18.128.0 255.255.255.255 198.19.10.0 255.255.255.255 198.19.10.100 255.255.255.255 198.19.11.4 255.255.255.255 is 198.19.11.4 255.255.255.255 is 198.19.30.4 255.255.255.255 is 198.19.40.4 255.255.255.255 is 198.19.40.4 255.255.255.255 is	19.40.64, outside2 19.30.63, outside3 s directly connected, spoke_tunnel_IP directly connected, outside (00.2252, outside_static_vti_1 (1/0] via 198.19.40.64, outside2 (1/0] via 198.19.40.64, outside3 directly connected, inside directly connected, inside directly connected, outside3 directly connected, outside3		

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.

So wkstbr - 198.19.11.225 - Remote Desktop Connection
administrator@inside: ~
ThiMicrosoft Windows [Version 10.0.19042.789] (c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\Administrator> <mark>ssh_administrator@198.19.10.200</mark> administrator@198.19.10.200's password: Linux inside 5.4.0-kali2-amd64 #1 SMP Debian 5.4.8-1kali1 (2020-01-06) x86_64
Pu (64The programs included with the Kali GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent MTFpermitted by applicable law. Last login: Thu May 11 16:15:40 2023 from 198.19.10.50 Administrator@inside:-\$

- · 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.

Ę	Firewall Manage Analysis / Unified Even	ement Center	Overview Anal	ysis Policie	s Devices	Objects	Integration	Deploy	९ 🗳 ;	🗘 🕜 adm	in ~ diala	SECUR	1
Q	Search										☆×	Refresh	
\odot	Showing all 31 events (\$	24 🗅 7) 🛓					Po	2023-07-05 03:3	0:44 EDT → 2023	-07-05 03:32:45	EDT 2m 1s	Go Live	
	Time	Event Type	Destination Port	/ Web Application	Access Control Rule	Access Control Policy	Device	VPN Action	Decrypt Peer	Encrypt Peer	Egress Interface	m	
>	2023-07-05 03:31:43	D File	57406 / tcp	Microsoft			NGFWBR1					-	
>	2023-07-05 03:31:40	t Connection	22 (ssh) / tcp	1	Allow-To-Co	NGFW1	NGFW1	Decrypt	198.19.30.4		in10	1	
>	2023-07-05 03:31:40	S Connection	22 (ssh) / tcp		Allow-To-Co	Branch Access	NGFWBR1	Encrypt		198.18.133	outside_sta		
>	2023-07-05 03:31:38	Sconnection	80 (http) / tcp	Microsoft	Allow Outbou	Branch Access	NGFWBR1				outside2	-	

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.

Edit Endpoint	0
Device:*	
NGFWBR1 -	
Static Virtual Tunnel Interface	
outside_static_vti_1 (IP: 169.254 -+	
Tunnel Source: outside3 (IP: 198.19.30.4) Tunnel Source IP is Private	Edit VTI
Send Local Identity to Peers	
Backup VTI:	Remove
Virtual Tunnel Interface:*	
· +	
Tunnel Source IP is Private	Edit VTI
Send Local Identity to Peers	
Additional 0	
Configuration Poute traffic to the VTI Pouting Policy	
Permit VPN traffic : <u>AC Policy</u>	
 Advanced Settings 	
	-
Cance	ОК

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 hox_and then click Add

ECIVIF-VII			
Available Interfaces		Selected Interfaces	
outside		outside_static_vti_1	•
inside		outside_static_vti_2	-
outside?			-
outsidez		1	
outside3	Add	J	

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**.

Firewall Management Center Overview / Dashboards / Site to Site VPN	verview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q 🌖	👂 🗘 🕼 🤤	dmin ~ diale SECURE
Y Select							× Refre	sh	Refresh every	5 minutes 🗸 🗸
Tunnel Summary		Node A			Node B		Topology		Status	Last Updated 🔺
		NGFW1	(VPN IP: 198.1	8.133.81)	NGFWBR1	(VPN IP: 198.19.30.4)	Corporate	-VPN	🥝 Active	2023-07-05 02:07:58
		NGFW1	(VPN IP: 198.1	8.133.81)	NGFWBR1	(VPN IP: 198.19.40.4)	Corporate	-VPN	Active	2023-07-05 11:32:11
100% Active 2 connections										
Topology										
Name 🗢 🥝	0									
Corporate-VPN 0 0	2									

- 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.

CLI Troubleshoot			
>_ Command: show interfac	e ip brief	⇒ Execute Copy Device: NGFW1	
> show interface in brief			
Interface	IP-Address	OK? Method Status Protocol	
GigabitEthernet0/0	198.18.133.81	YES CONFIG UP UP	
GigabitEthernet0/1	198.19.10.1	YES CONFIG up up	
GigabitEthernet0/2	198.19.20.1	YES CONFIG up up	
GigabitEthernet0/3	unassigned	YES unset administratively down up	
GigabitEthernet0/3.100	unassigned	YES unset down down	
GigabitEthernet0/3.110	unassigned	YES unset down down	
GigabitEthernet0/4	unassigned	YES unset administratively down up	
GigabitEthernet0/4.200	unassigned	YES unset down down	
GigabitEthernet0/4.220	unassigned	YES unset down down	
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	unassigned	YES unset up up	
Loopback1	198.48.133.81	YES manual up up	
Virtual-Access1	198.48.133.81	YES CONFIG up up	
Virtual-Access2	198.48.133.81	YES CONFIG up up	
Virtual-Template1	198.48.133.81	YES CONFIG up up	
Virtual-Template2	198.48.133.81	YES CONFIG up up	

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.

CLI	Troubleshoot
	Houbiconool

>_ Command: show interfac	e ip brief		⇒ Execu	ite 🧲 Refresh 🛅 Cop	У	Device:	NGFWBR1
> show interface ip brief							
Interface	IP-Address	OK?	Method	Status	Protocol		
GigabitEthernet0/0	198.18.128.81	YES	CONFIG	up	up		
GigabitEthernet0/1	198.19.11.4	YES	CONFIG	up	up		
GigabitEthernet0/2	unassigned	YES	unset	administratively down	up		
GigabitEthernet0/3	198.19.40.4	YES	CONFIG	up	up		
GigabitEthernet0/4	198.19.30.4	YES	CONFIG	up	up		
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	unassigned	YES	unset	up	up		
Loopback1	169.254.20.1	YES	manual	up	up		
Tunnel1	169.254.20.1	YES	CONFIG	up	up		
Tunnel2	169.254.20.1	YES	CONFIG	up	up		

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

CLI Troubleshoot

> show route	
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF	
Galeway of last resort is 198.19.40.04 to network 0.0.0.0	
<pre>S* 0.0.0.0 0.0.0 [1/0] via 198.19.40.64, outside2</pre>	

- 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.

Firewall Management Center Overview / Dashboards / Site to Site VPN	Analysis Policies Devices	Objects Integration	Deploy Q 💕	🔅 🕜 adı	min ~
Y Select			× Refresh	Refresh every	5 minutes 🗸 📕
Tunnel Summary	Node A	Node B	Topology	Status	Last Updated 🔺
	NGFW1 (VPN IP: 198.18.133.81)	NGFWBR1 (VPN IP: 198.19.40.4)	Corporate-VPN	Active	2023-07-05 11:32:11
50% Active 1 connection 50% Inactive 1 connection	NGPW1 (VPN IP: 198.18.133.81)	NGFWBR1 (VPN IP: 198.19.30.4)	Corporate-VPN	Inactive	2023-07-05 11:48:00
Topology					
Name Image: Original content of the second sec					

- **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.

Q	Search									合 :
0	Showing all 102 events (\$	101 🗅 1) 🛨						10 2023-07-05 1	0:52:50 EDT → 2	023-07-05 11:52:50 EDT 1
	Time	Event Type	Destination Port / ICMP Code	Access Control Rule	Access Control Policy	Device	VPN Action	Encrypt Peer	Decrypt Peer	Egress Interface
>	2023-07-05 11:52:34	⇔ Connection	3 (Port unreach	Allow Outbou	Branch Access	NGFWBR1				outside2
>	2023-07-05 11:52:12	S Connection	. 443 (https) / tcp	Allow Outbou	Branch Access	NGFWBR1				outside2
>	2023-07-05 11:51:46	D File	. 58273 / tcp			NGFW1				
>	2023-07-05 11:51:44	S Connection	443 (https) / tcp	Allow Outbou	NGFW1	NGFW1				outside
>	2023-07-05 11:51:27	⇔ Connection	443 (https) / tcp	Allow Outbou	NGFW1	NGFW1				outside
>	2023-07-05 11:51:16	S Connection	22 (ssh) / tcp	Allow-To-Co	Branch Access .	NGFWBR1	Encrypt	198.18.133		outside_static_vti_2
>	2023-07-05 11:51:15	S Connection	22 (ssh) / tcp	Allow-To-Co	NGFW1	NGFW1	Decrypt		198.19.40.4	in10
>	2023-07-05 11:51:05	S Connection	80 (http) / tcp	Allow Outbou	Branch Access	NGFWBR1				outside3
>	2023-07-05 11:50:43	S Connection	443 (https) / tcp	Allow Outbou	NGFW1	NGFW1				outside

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></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 J

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, on page 31
- Benefits, on page 33
- Is This Use Case For You?, on page 33
- Components for Direct Internet Access, on page 33
- Best Practices, on page 34
- Prerequisites, on page 34
- Scenario 1: Direct Internet Access, on page 34
- Scenario 2: Direct Internet Access With Path Monitoring, on page 37
- Configure a Trusted DNS Server, on page 40
- Configure Interface Priority, on page 41
- Create an ECMP Zone, on page 41
- Configure an Equal Cost Static Route, on page 42
- Configure Path Monitoring Settings, on page 42
- Configure an Extended ACL Object for YouTube, on page 43
- Configure an Extended ACL Object for WebEx, on page 43
- Configure a Policy Based Routing Policy for YouTube, on page 44
- Configure a Policy Based Routing Policy for WebEx, on page 45
- Configure a Policy Based Routing Policy With Path Monitoring for Webex, on page 46
- Deploy Configuration, on page 47
- Verify Application Traffic Flow, on page 47
- Monitor and Troubleshoot Policy Based Routing, on page 49
- Additional Resources, on page 52

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	(<i>Prerequisite</i>) Configure a Trusted DNS server. See Configure a Trusted DNS Server, on page 40.
2	(<i>Prerequisite</i>) Configure interface priority. See Configure Interface Priority, on page 41.
3	(<i>Prerequisite</i>) Create an ECMP zone. See Create an ECMP Zone, on page 41.
4	(<i>Prerequisite</i>) 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	(<i>Prerequisite</i>) Configure a Trusted DNS server. See Configure a Trusted DNS Server, on page 40.
2	[<i>Prerequisite (Optional)</i>] 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

L

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

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 (<i>I</i>) 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.

Step 1	Select Devices > Device	Management and click E	dit (🖉) for the threat	t defense device (NG	FWBR1).

- **Step 2** Click **Edit** (*I*) 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

L

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.

Step 1 Select Objects > Object Management and choose Access Lists > Extended from the table	f 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 with priority 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** (\checkmark) 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 (T)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.

I

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

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.

	Firewall Managemen Unified Events	nt Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	⇔
٩	Web Application WebEx	× × Select										×
\odot	Showing all 9 events (\lneq 9)	<u>+</u>					2023-03	3-29 11:57:54 EDT	→ 2023-03-3	29 12:5	7:54 E	DT 1h
	Time	Event Type		Web Applic	ation	Ingress Inte	erface	Egress Interf	асе	De	evice	
>	2023-03-29 12:54:18	Sconnection	ı	WebEx	1	inside		outside3		N	GFWE	3R1
>	2023-03-29 12:54:18	Sconnection	ı	WebEx		inside		outside3		N	GFWE	3R1
>	2023-03-29 12:54:18	🕏 Connection	ı	WebEx		inside		outside3		N	GFWE	3R1
>	2023-03-29 12:54:18	S Connection	ı	WebEx		inside		outside3		N	GFWE	3R1
>	2023-03-29 12:54:18	Sonnection	ı	WebEx		inside		outside3		N	GFWE	3R1

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

	Firewall Manager Analysis / Unified Events	ment Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	o 🜣	🕜 a	dmin 🔻 👘
٩	Web Application Youtube	× × Select										×	Apply
\oslash	Showing all 2,285 events (\u00e9	; 1,832 🗅 453) 🛨						2023	-03-15 05:29	:35 EDT -	→ 2023-0	3-29 05:	29:35 EDT 2w
	Time	Event Type		W	eb Application	In	gress Interface	Egres	s Interface		Devi	се	
>	2023-03-29 03:43:50	S Connection		Yo	JuTube	in	side	outsi	de2		NGF	WBR1	
>	2023-03-29 03:43:30	Sconnection ≤ Connection		Yo	JuTube	in	side	outsi	de2		NGF	WBR1	
>	2023-03-29 03:43:10	S Connection		Yo	JuTube	in	side	outsi	de		NGF	WBR1	
>	2023-03-29 03:42:50	\Leftrightarrow Connection		Yo	JuTube	in	side	outsi	de		NGF	WBR1	
>	2023-03-29 03:42:50	\Leftrightarrow Connection		Yo	JuTube	in	side	outsi	de2		NGF	WBR1	
>	2023-03-29 03:42:40	rightarrow Connection		Yo	JuTube	in	side	outsi	de		NGF	WBR1	

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.

	Firewall Management	t Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	¢	🕜 ad	lmin 🔻
٩	Web Application WebEx	× × Select										×	Refr	resh
0	Showing all 2 events (🖕 2)	+					10 2023-0	3-29 11:31:45 EDT	→ 2023-03-	29 12:3 1	1:45 EC)⊤ 1h	• Go	Live
OTT	Time	Event Type	Event Type			ation	Ingress Inte	rface	Egress Inter	face		1	Device	*
>	2023-03-29 12:29:08	S Connection	ı		WebEx		inside		outside2			1	NGFWB	R1
>	2023-03-29 12:28:30	S Connection	ı		WebEx		inside		outside2			1	NGFWB	R1

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
1
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
1
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 Branch (es) Address Idle(sec) Timeout(sec) Hit-count 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

Use Cases for SD-WAN Capabilities in Cisco 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, on page 55
- Benefits, on page 56
- Is This Use Case For You?, on page 57
- Scenario, on page 57
- Network Topology, on page 57
- Best Practices for SASE Umbrella Tunnels, on page 59
- Prerequisites for Configuring Umbrella SASE Tunnels, on page 59
- End-to-end Procedure for Configuring Umbrella Auto Tunnel, on page 60
- Configure a SASE Tunnel for Umbrella, on page 61
- Configure a Static Route, on page 65
- Configure an Extended ACL for DNS and Web Traffic, on page 65
- Configure a PBR Policy for DNS and Web Traffic, on page 66
- Deploy Configuration, on page 67
- Verify SASE Umbrella Tunnel Deployment, on page 67
- Troubleshoot Umbrella Auto Tunnels , on page 72
- Additional Resources, on page 73

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	(<i>Prerequisite</i>) Generate and copy the API keys in Cisco Umbrella. See Map Management Center Umbrella Parameters and Cisco Umbrella API Keys.
2	(<i>Prerequisite</i>) 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.

Cisco Umbrella C	onfiguration	0
Topology Name:	VPN-MumbaiUmbrella	
Primary Data Center:	Asia-Mumbai	
DC IP Address:	146.112.117.8	
Start Time:	Apr 27, 2023 7:02 PM	
Completion Time:	Apr 27, 2023 7:02 PM	
100%	0.40mmland 0.45%	
Tunnel Configuratio	n Status	Umbrella Dashboard
Device	Status	Transcript
NGFWBR1	SUCCESS	8.
		Close

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.

Active Tunnels Inactive Tunnels 1 1		Unestablished Tunnels <mark>0</mark>		Unknown Tunnel Status O	Data Center Locations 1	
FILTERS Q Search	n tunnels by name					
Tunnel Name VPN-CLPOD8-U Secure Internet Access	Site Default Site	Data Center Location Los Angeles, California - US	Device Public IP 1	Tunnel Status	Last Status Update Jun 07, 2023 - 6:31 PM	 ~
Tunnel Name VPN-MumbaiUmb Secure Internet Access	Site Default Site	Data Center Location Mumbai, Maharashtra - India	Device Public IP 1	Tunnel Status	Last Status Update Jul 21, 2023 - 12:51 PM	 ~

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.

NGFWBR1 Cisco Firepower Threat Defense for	VMWare					
Device Routing Interface	s Inline Sets DI	HCP VTEP				
Manage Virtual Routers						
Global 🔻	Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
Virtual Router Properties	▼ IPv4 Routes					
ECMP BFD	any-ipv4	outside_static_vti_1	Global	Host_169.254.2.2	false	2

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.

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.

Edit Extended Access List Object

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

Name LAN_to_Internet									
Entries (1)									
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	O Allow	Branch-LAN	Any	Any	DNS_over_TCP HTTP HTTPS DNS_over_UDP	Any	Any	Any	

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.

- 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.

Policy Based Routing

0								1. 1	T 00 1		F	1	1° 1	
~	DOCITV	Ingraci	C INTOTTOCOC	match	critoria and	Adrace Intertacae	to route trattic	accordinally	Irotte con bo	routed acr	ace Larace int	CONTRACOS SOCO	ardinally	
	JECHV	IIIUICS.		Inducin			to toute traint			TUDIEU AUT		CHALES ALL		
	,					- 3								

			Configure Interface Priority	Add
Ingress Interfaces	Match criteria and forward action			
inside	If traffic matches the Access List LAN_to_Internet	Send through [#0] outside_static_vti_1		/1

Deploy Configuration

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

Procedure

On the management center menu bar, click Deploy . This displays the list of devices that are Ready for Deployment.
Check the checkboxes adjacent to NGFWBR1 and NGFW1 on which you want to deploy configuration changes.
Click Deploy . Wait till the deployment is marked Completed on the Deploy dialog box.
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).

Deploymer	nts Upgra	ides 🌗	Health	Tasks	
20+ total	0 waiting	0 running	0 retrying	20+ success	0 failures
Policy Dep Policy De	loyment ployment to N	IGFWBR1. A	pplied success	sfully	
Policy Pre- Pre-deple success	Deployment	figuration fo	or NGFWBR1		
 Policy Pre- Pre-deple success 	Deployment oy Global Cor	figuration G	eneration		
Umbrella Tunn Umbrella Tunn	el Deployment el deployment for S	ite to Site VPN VI	PN-MumbaiUmbre	ella has succeeded	

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

	Firewall Managen Devices / VPN / Site To S	nent Center ^{Site}	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	6 9 .	¢ 0		admin	~ .	1.1 1. 15CO	SEC	URE
							Last Updat	ed: 04:10 PM	Refresh		⊦ Site t	o Site	VPN		+ SASE	Тор	ology	
▼ Se	lect														×		Refre	sh
	Topology Name	VPN Type			Network Topo	logy		Tunnel Status	Distribution				1	IKEv1	IKEv2			
>	VPN-CLPOD8-Umbrella	Route Based (VTI)		SASE			1- Tunnels							\checkmark	4	/ 1	
~	VPN-MumbaiUmbrella	Route Based (VTI)		SASE			1- Tunnels							\checkmark	•	/ 1	
		Node /	4						N	ode B								
Dev	ice	VPN Interface	VTI Int	terface			Device		VPN Inter	face			VTI	Interfac	e			
UM	BRELLA Asia-Mumbai	146.112.1 (146.11	2.117.8)			•••	FTD NGFW	BR1	Outside	(172.16	5.2.10)		Out	side_st	ati (169.2	254.2.	1)

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.

Firewall Management Center Devices / VPN / Site To Site	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	¢	¢ 0	admin ~	-ilia ciso	b' SECURE
Edit SASE Topology													
1 Endpoints — 2 Summary													
Topology Name* VPN-MumbaiUmbrella													
Pre-shared Key*													
Umbrella Data Center* Asia - Mumbai(146.112.117.8)													
Threat Defense Nodes												,	Add
Device	VPN	Interface				Local Tunnel ID)						
NGFWBR1	Outs	ide_static_vti_	1			FTDvChandiga	arh@4	-	704	-umbrell	a.com		i

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

Firewall Management Center Overview / Dashboards / Site to Site VPN	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	, Q	6 3	≱ 0	admir	n ∽ dua ciso	SECURE
Y Select							×	Refresh	Re	fresh ev	ery 5	minutes	~ II
Tunnel Summary		Node A	λ.		Node B			Topology		Stat	tus	Last Upda	ated 🔺
		Asia-N	/lumbai (VPN IP	: 146.112.11	NGFWBR1	(VPN IP: 172.16.	2.10)	VPN-Mu	nbaiUml	or 📀 /	Active	2023-04	-27 15:1
		North_	America-Los_	Angeles (VPN	NGFWBR1	(VPN IP: 172.16.	2.10)	VPN-CLF	POD8-U	n 📀 /	Active	2023-05-	-11 11:1
100% Act 2 connection	ive ons												
Topology													
Name	0 0												
VPN-CLPOD8-Umbrella 0	0 1												
VPN-MumbaiUmbrella 0	0 1												

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-xxxxxxx-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:

```
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
```

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

• 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)
     remote ident (addr/mask/prot/port): (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:
         0x0000000 0x0000001
   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.

Active Tunnels	Inactive Tunnels	Unestablis Tunnels <mark>0</mark>	shed	Unknown Tunnel Status O	Data Center Locations 1
C Searc	h tunnels by name				
Tunnel Name VPN-CLPOD8-U Secure Internet Access	Site Default Site	Data Center Location Los Angeles, California - US	Device Public IP 1	Tunnel Status	Last Status Update Jun 07, 2023 - 6:31 PM
Tunnel Name VPN-MumbaiUmb	Site Default Site	Data Center Location Mumbai,	Device Public IP	Tunnel Status	Last Status Update Jul 21, 2023 -
Secure Internet Access		Maharashtra - India			12:51 PM

Expand the section to view the details of the tunnel.

Tunnel ID			Dev	vice Type	Data Center IP	
FTDvChandigar	h@4		- oth	ner	146.112.117.8	
umprelia.com						
Total Network Tr	affic					
Traffic Data Initializ	ed		Packets In	n Bytes In	Idle Time In	
Jul 20, 2023 - 8	3:52 PM		2.63 K	85.73 K	B 0 sec	
Packets Out	Bytes Out	Idle Tim	ne Out			
69.37 K	185.26 KB	0 sec				
IPsec						
State	Age		Integrity	Algorithm	Encryption Alg	gorithm Key Size
Installed	727	sec	-		AES_GCM_	.16 256
SPI In	SPI (Dut				
c76f91b4	649	07273				
IKE						
Key Exchange Stat	us Age		PRF Algo	prithm	Encryption Alg	gorithm DH Group
Established	385	6 sec	PRF_HM	MAC_SHA2_256	AES_GCM_	.16 ECP_384
Initiator SPI	Resp	onder SPI				
53285f5df73e0	c22 204	e90910aca	4243			

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.

CLI Command
debug crypto condition peer <peer-ip></peer-ip>
debug vti 255
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255
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 J

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, on page 75
- Is This Use Case For You?, on page 75
- Scenario, on page 76
- Topology, on page 76
- End-to-end Procedure for Configuring DIA, Umbrella Auto Tunnel, and DVTI, on page 77
- Additional Resources, on page 77

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

I

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



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, on page 79
- Is this Guide for You, on page 80
- Scenario, on page 80
- System Requirements, on page 80
- Prerequisites, on page 81
- Guidelines and Limitations, on page 81
- Network Topology, on page 81
- End-to-End Procedure for Setting Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates, on page 83
- Configure SD-WAN Topologies Using the SD-WAN Wizard, on page 84
- Create a Device Template, on page 89
- Add a Physical Interface in the Template, on page 90
- Configure an SD-WAN VPN Connection in a Device Template, on page 91
- Map Template Interfaces to Device Model Interfaces, on page 92
- Onboard a Device to the Management Center Using a Registration Key and Device Template, on page 94
- Verify Tunnel Statuses and Configurations of Route-Based VPN, on page 97
- Troubleshoot Device Templates and Route-Based VPN Tunnels, on page 102

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

Hub1	Loopback1: 209.165.201.1/255.255.255.224	• IP_pool1_hub1: 209.165.201.2-209.165.201.30 (Mask: 255.255.255.224)
•		(IVIdSK. 255.255.255.224)
	Loopback2: 209.165.201.65/255.255.255.224	• IP_pool2_hub1: 209.165.201.66-209.165.201.94
Hub2 •	Loopback1: 209.165.201.33/255.255.255.224	• IP_pool1_hub2: 209.165.201.34-209.165.201.62 (Mask: 255.255.255.224)
•	Loopback2: 209.165.201.97/255.255.255.224	• IP_pool2_hub2: 209.165.201.98-209.165.201.126

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

•

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 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.

dd Hub				?
Device* (1)				
Hub1		~		
Dynamic Virtual Tunnel Interf	ace (DVTI) * 🚹			
outside-isp1_dynamic_vti_1	1	~	+	-
Tunnel Source: outside-isp1 192.0.2.17)	(IP Address:			
Hub Gateway IP Address 🌒				
192.0.2.17				
Spoke Tunnel IP Address Po	ol* 🚺			
IP_pool1_hub1	×	~	+	
	Cancel		Add	

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

Device		Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
Hub1 Threat Defense	Priman	Virtual-Template1 (outside-isp1_dynamic_vti_1) Source:GigabitEthernet0/1 (outside-isp1)	192.0.2.17	IP_pool1_hub1 Range: 209.165.201.2-209.165.201.30
Hub2 Threat Defense		Virtual-Template2 (outside-isp1_dynamic_vti_1) Source:GigabitEthernet0/1 (outside-isp1)	192.0.2.18	IP_pool1_hub2 Range: 209.165.201.34-209.165.201.6

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.

Add Bulk Spokes			0
1 Add Devices	(2)	Validate Devices	
Available Devices*		Selected Devices*	
୍ Search		Spoke1	Ì
Hub2	Add	Spoke2	¥
Select VPN Interface Using*			
outside-isp1			
 Security Zone () 			
Select	~ +		
			Cancel Next

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.

Authentication Type *	Transform Sets (IPsec Proposals) *		IKEv2 Policies*
Pre-shared Manual Key 🗸 🗸	AES-GCM ×	x ~	AES-GCM-NULL-SHA-LATEST X
	Show Details		Show Details
(ey*			
Confirm Key*			

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.

Spoke Tunnel Interface Secu	urity Zone 🚯		
SZ-ISP1	× ~	+ /	/
Autonomous System Nu	mber* 🗊		Community Tag for Local Routes *
64512			1
	ted Interfaces 🕕		
Redistribute Connec			
 Redistribute Connec Default inside* 		~	+
Redistribute Connec Default inside*		~	+

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.

Add Device	Template 3
Name *	
SDWAN_Branc	h_Template
Description	
Access Control	I Policy*
Note: By a "Routed",	default, Firewall mode is set to which is the only supported mode.
	Cancel OK

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 1Choose 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**.

Add VPN Connection		0
VPN Topology*		
SDWAN-VPN1		~
Type: SD-WAN Topology Role: Spoke		
VPN Interface * 🕕		
outside-isp1 (Ethernet1/1)		~
Use IP Address from the VPN Interface *		
\$Outside-ISP1-IPv4		~
Local Tunnel (IKE) Identity Identity Type *		
Key ID		~
(x) \$Local_Identity_SDWAN_ISP1		x ~ +
	Cancel	ОК

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

Step 6 Click Save.

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

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

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

SDWAN_Branch_Template	emplate			Save
Interfaces Inline Sets Routing DHCF	VPN Temp	late Settings		Associate
Site-to-Site VPN Connections 👔				Add VPN Conne
VPN Topology	VPN Connections		Traffic Matching Criteria	Actions
SDWAN-VPN1 Type: SD-WAN Topology Role: Spoke	VPN Interface Local Tunnel IKE ID	outside-isp1 \$Local_Identi	Routing	/ 1
SDWAN-VPN2 Type: SD-WAN Topology Role: Spoke	VPN Interface Local Tunnel IKE ID	outside-isp2 \$Local_Identi	Routing	/ 1

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.

Map the template-de	efined interfaces for each device r	nodel that you want to apply	this template to.
evice Model* Disco Firepower 1120	Threat Defense	7	
for failover and a	nother for state link.	Clear Mapping	Reset Mappings
Template Interface	Template Interface Name	Model Interface	
Ethernet1/1	outside-isp1	Ethernet1/1	× ·
2010111011171			
Ethernet1/2	inside	Ethernet1/2	× v
Ethernet1/2 Ethernet1/3	inside outside-isp2	Ethernet1/2 Ethernet1/3	x ~ x ~

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 Step 2 Step 3	Choose Devices > Device Management . Click Add > Device (Wizard) . On the Add Device (Wizard) window, choose Registration Key to register a device using registration key.			
	Add Device (Wizard)	9		

Registration Key	Serial Number
Register device using registration key	Cisco Security Cloud integration is not enabled. To enable Cisco Security Cloud integration, go to Integration > Cisco Security Cloud.

Click Next. Step 4

S

Step 5	Choose a temp	plate from the	e Device tem	plate drop	p-down li	ist
	Choose a temp		Device tem	place all		1.

Add Device (Wizard)			?
Device registration method Device registration method	ion Key		
2 Initial device configuration Device template * SDWAN_Branch_Template	x ~	Device models supported for the selected template	
Access control policy : AC1 This template requires device Management interface.	s to be managed using the Management interface.	Ensure that the device's connection to Management Center is from the	
		Previous 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**.

Host		Display name*	
209.165.200.229		Spoke3	
Registration key*		Device group	
		Select	
Unique NAT ID			
devicetemplate			
Note: Either Host or NAT ID is require	d.		
Variables 🕕			
Variables	Value		
\$Local_Identity_SDWAN_ISP1	SDWAN-VPN1_Spoke	(String; Example: hello world)	
\$Local_Identity_SDWAN_ISP1 \$Local_Identity_SDWAN_ISP2	SDWAN-VPN1_Spoke	(String; Example: hello world) (String; Example: hello world)	
\$Local_Identity_SDWAN_ISP1 \$Local_Identity_SDWAN_ISP2 \$Outside-ISP1-IPv4	SDWAN-VPN1_Spoke SDWAN-VPN2_Spoke 192.0.2.21/28	(String; Example: hello world) (String; Example: hello world) (IPv4 Network; Example: 209.165.200.224/27)	
<pre>\$Local_Identity_SDWAN_ISP1 \$Local_Identity_SDWAN_ISP2 \$Outside-ISP1-IPv4 \$Outside-ISP2-IPv4</pre>	SDWAN-VPN1_Spoke SDWAN-VPN2_Spoke 192.0.2.21/28 192.0.2.37/28	(String; Example: hello world) (String; Example: hello world) (IPv4 Network; Example: 209.165.200.224/27) (IPv4 Network; Example: 209.165.200.224/27)	
<pre>\$Local_Identity_SDWAN_ISP1 \$Local_Identity_SDWAN_ISP2 \$Outside-ISP1-IPv4 \$Outside-ISP2-IPv4</pre>	SDWAN-VPN1_Spoke SDWAN-VPN2_Spoke 192.0.2.21/28 192.0.2.37/28	(String; Example: hello world) (String; Example: hello world) (IPv4 Network; Example: 209.165.200.224/27) (IPv4 Network; Example: 209.165.200.224/27)	

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.

Deployments	Upgrades	Health	Tasks	<u>↓</u>	Show Pop-up Notifica	ations 🧻
20+ total 0	waiting 0 runr	ning 0 retrying	20+ success	0 failures	Q Filter	
Device Template SDWAN_ Report.	e Apply Branch_Template -	Application of dev	rice template is suc	cessful for device 20	9.165.200.229 Download	24s ×
Discovery 209.165.200.229 - Dis	scovery from the de	evice is successful			1r	n 29s 🗙
SFTunnel 209.165.200.229 - SF	Tunnel connection	established succe	ssfully.			- X
Register Registration 209.165.200.229: Star	rted device discov	ery				48s ×

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.

Ę		irewall Manageme evices / Device Manageme	nt Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (P 🗘	admin ~]
														Migrate Dep	pl
Vi	ew By:	Group	¥									୍ୟ	earch De	evice	
	All (5) • Error (5)	 Warning (0) 	Offline (0)	Nor	rmal (0)	Deployment P	ending (5)	 Upgrade (0) 	• Snort 3 (5)					
C	ollapse A	Ш												Download	1
	Na	me			Model		Version	Chassis		Licenses	Access Cont	ol Policy		Auto RollBack	
		Ungrouped (5)													
		Spoke3 Snort 3 209.165.200.229 -Routed			Firepower 1 Defense	120 Threat	7.6.0	firepowe	r:443	Essentials	AC1			4P	
		209.165.200.225 -Routed			Firewall Thr VMware	eat Defense for	7.6.0	N/A		Essentials, IPS (3 more)	AC1			49	
		U09.165.200.226 -Routed			Firewall Thr VMware	eat Defense for	7.6.0	N/A		Essentials, IPS (3 more)	C1 AC1			4P	
		Spoke1 Snort 3 209.165.200.227 -Routed			Firewall Thr VMware	eat Defense for	7.6.0	N/A		Essentials, IPS (3 more)	CAC1			49	
		Spoke2 Snort 3 209.165.200.228 -Routed			Firewall Thr VMware	eat Defense for	7.6.0	N/A		Essentials, IPS (3 more)	AC1			« 9	

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.

Firewall Man Devices / VPN / S	agement Center Ov	verview Analysis	s Policies	Devices	Objects	Integration			Deploy	५ 🔮 ¢	£ 0	admin ~	cisc
								Last Updated	i: 10:25 AM	Refresh	NAT E	Exemptions	
Y Select													×
Topology Name	v	PN Type			Network T	opology		Tunnel Status Distribution			IKEv1	IKEv2	
 SDWAN-VPN1 	R	toute Based (VTI)			SD-WAN	Topology		8- Tunnels				~	
		Hub						Spoke					
Device	VPN Interface		VTI Interface				Device	VPN Interface		VTI Interface			
				- (200.105.2	,	-	con Constant			autolata land		(200.105.0	,
FID Hub2	outside-isp1 (192.0.2.18)		outside-ispit_dyn	a (209.165.2	01.33)		FID Spoke1	outside-isp1 (192.0.2.19)		outside-ispi	_static	(209.165.2	:01.34
FTD HUDZ	outside-isp1 (192.0.2.18)		outside-isp1_dyn	a (209.165.2)	01.33)		FTD Spoke2	outside-isp1 (192.0.2.20)		outside-isp1	_static	(209.165.2	201.35
FTD Hub1	outside-isp1 (192.0.2.17)		outside-isp1_dyn	a (209.165.2)	01.1)		FTD Spoke3	outside-isp1 (192.0.2.21)		outside-isp1	_static	(209.165.2	201.4)
FTD Hub2	outside-isp1 (192.0.2.18)		outside-isp1_dyn	a (209.165.2	01.33)		FTD Spoke3	outside-isp1 (192.0.2.21)		outside-isp1	_static	(209.165.2	201.36
										< <	< Vi	iewing 1-6	of 6
✓ SDWAN-VPN2	R	toute Based (VTI)			SD-WAN	Topology		6- Tunnels				~	
		Hub						Spoke					
Device	VPN Interface		VTI Interface				Device	VPN Interface		VTI Interface			
	outoido iope (rosioisioo)		outoido iopa_ajii		,	-	- opener	conner lobe (restricted)		outoido iopa,		(=========	
FTD Hub2	outside-isp2 (192.0.2.34)		outside-isp2_dyn	a (209.165.2	01.97)	•••••	FTD Spoke1	outside-isp2 (192.0.2.35)		outside-isp2	_static	(209.165.2	201.98
FTD Hub2	outside-isp2 (192.0.2.34)		outside-isp2_dyn	a (209.165.2	01.97)	••••••	FTD Spoke2	outside-isp2 (192.0.2.36)		outside-isp2	_static	(209.165.2	201.99
FTD Hub1	outside-isp2 (192.0.2.33)		outside-isp2_dyna	a (209.165.2)	01.65)		FTD Spoke3	outside-isp2 (192.0.2.37)		outside-isp2	_static	(209.165.2	201.68
FTD Hub2	outside-isp2 (192.0.2.34)		outside-isp2_dyn	a (209.165.2	01.97)		FTD Spoke3	outside-isp2 (192.0.2.37)		outside-isp2	static	(209.165.2	201.10
										< <	< Vi	iewing 1-6	of 6

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:

Firewall Manage Overview / Dashboards	ement Center s / Site to Site VPN	Analysis Policies Devices Ob	ojects Integration	Deploy	० 🔮 🌣 🙆	admin ~ dialo SECURE			
Y Select			X Refrest						
Tunnel Summary		Node A	Node B	Topology	Status	Last Updated 🗧			
		Hub2 (VPN IP: 192.0.2.34)	Spoke3 (VPN IP: 192.0.2.37)	SDWAN-VPN2	Active	2024-09-11 01:42:09			
100% Active		Hub2 (VPN IP: 192.0.2.18)	Spoke3 (VPN IP: 192.0.2.21)	SDWAN-VPN1	Active	2024-09-11 01:42:09			
	12 connections	Hub1 (VPN IP: 192.0.2.33)	Spoke3 (VPN IP: 192.0.2.37)	SDWAN-VPN2	Active	2024-09-11 01:42:09			
	1	Hub1 (VPN IP: 192.0.2.17)	Spoke3 (VPN IP: 192.0.2.21)	SDWAN-VPN1	Active	2024-09-11 01:42:09			
		Hub1 (VPN IP: 192.0.2.33)	Spoke2 (VPN IP: 192.0.2.36)	SDWAN-VPN2	Active	2024-09-11 01:42:09			
		Hub1 (VPN IP: 192.0.2.17)	Spoke2 (VPN IP: 192.0.2.20)	SDWAN-VPN1	Active	2024-09-11 01:42:09			
Topology		Hub1 (VPN IP: 192.0.2.33)	Spoke1 (VPN IP: 192.0.2.35)	SDWAN-VPN2	Active	2024-09-11 01:42:23			
Name	e e e	Hub1 (VPN IP: 192.0.2.17)	Spoke1 (VPN IP: 192.0.2.19)	SDWAN-VPN1	Active	2024-09-11 01:42:23			
SDWAN-VPN1	0 0 6	Hub2 (VPN IP: 192.0.2.34)	Spoke2 (VPN IP: 192.0.2.36)	SDWAN-VPN2	Active	2024-09-11 07:49:20			
SDWAN-VPN2	0 0 6	Hub2 (VPN IP: 192.0.2.18)	Spoke2 (VPN IP: 192.0.2.20)	SDWAN-VPN1	Active	2024-09-11 07:49:20			
		Hub2 (VPN IP: 192.0.2.34)	Spoke1 (VPN IP: 192.0.2.35)	SDWAN-VPN2	Active	2024-09-11 07:49:20			
		Hub2 (VPN IP: 192.0.2.18)	Spoke1 (VPN IP: 192.0.2.19)	SDWAN-VPN1	Active	2024-09-11 07:49:20			

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 **O** to view more information about the tunnels.
- 2. Click the CLI Details tab.

_	E 111						
	Overview / Dashboards / Site to Site VPN	Overview Analysis Polic	ies Devices O	bjects Integ	ration	Deploy 🔍 🐠	admin 🗸 👘
▼ S	elect					× Refresh	Refresh every 5 minutes
	Node A	Node B	Topology	Status	Last Updated 🗧	A: Hub1 ←→ B: Spoke1	
	Hub2 (VPN IP: 192.0.2.34)	Spoke3 (VPN IP: 192.0.2.37)	SDWAN-VPN2	Active	2024-09-11 01:42:09	Topology: SDWAN-VPN2 Status: 🥝	Active
	Hub2 (VPN IP: 192.0.2.18)	Spoke3 (VPN IP: 192.0.2.21)	SDWAN-VPN1	Active	2024-09-11 01:42:09	General CLI Details Packet	Tracer
	Hub1 (VPN IP: 192.0.2.33)	Spoke3 (VPN IP: 192.0.2.37)	SDWAN-VPN2	Active	2024-09-11 01:42:09	C Refresh Avimize view	
	Hub1 (VPN IP: 192.0.2.17)	Spoke3 (VPN IP: 192.0.2.21)	SDWAN-VPN1	Active	2024-09-11 01:42:09	Summary	
	Hub1 (VPN IP: 192.0.2.33)	Spoke2 (VPN IP: 192.0.2.36)	SDWAN-VPN2	Active	2024-09-11 01:42:09	Node A (192.0.2.33/500) 💡	🤄 Node B (192.0.2.35/500) 💡
	Hub1 (VPN IP: 192.0.2.17)	Spoke2 (VPN IP: 192.0.2.20)	SDWAN-VPN1	Active	2024-09-11 01:42:09	Transmitted: 2.19 MB (2291421 B)	Transmitted: 2.19 MB (22915
	Hub1 (VPN IP: 192.0.2.33)	Spoke1 (VPN IP: 192.0.2.35)	SDWAN-VPN2	Active	2024-09-11 01:42:23	Received: 2.92 MB (3062380 B) IPsec Security	Received: 2.92 MB (30622 Associations (1)
	Hub1 (VPN IP: 192.0.2.17)	Spoke1 (VPN IP: 192.0.2.19)	SDWAN-VPN1	Active	2024-09-11 01:42:23	0.0.0.0/0.0.0/0/0	0.0.0.0/0.0.0.0/0/0
	Hub2 (VPN IP: 192.0.2.34)	Spoke2 (VPN IP: 192.0.2.36)	SDWAN-VPN2	Active	2024-09-11 07:49:20	Hub1 (VPN Interface IP: 192.0.2	
	Hub2 (VPN IP: 192.0.2.18)	Spoke2 (VPN IP: 192.0.2.20)	SDWAN-VPN1	Active	2024-09-11 07:49:20	Show crypto ipsec sa peer 19	2.0.2.35 🖷
	Hub2 (VPN IP: 192.0.2.34)	Spoke1 (VPN IP: 192.0.2.35)	SDWAN-VPN2	Active	2024-09-11 07:49:20	Show vpn-sessiondb detail l2	l filter ipaddress 192.0
	Hub2 (VPN IP: 192.0.2.18)	Spoke1 (VPN IP: 192.0.2.19)	SDWAN-VPN1	Active	2024-09-11 07:49:20		
						Spokel (VPN Interface IP: 192.0	.2.35)
				I< < Viewin	ng 1-12 of 12 >>	Show crypto ipsec sa peer 19	2.0.2.33 📔

- 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.

Tunnel Details	0
Summary	
Node A (192.0.2.33/500) 👔	2 Node B (192.0.2.35/500)
Transmitted: 2.19 MB (2291421 B)	Transmitted: 2.19 MB (2291565 B)
Received: 2.92 MB (3062380 B)	Received: 2.92 MB (3062200 B)
IPsec Security	Associations (1)
0.0.0.0/0.0.0/0/0	0.0.0/0.0.0/0/0
Hubl (VPN Interface IP: 192.0.2.33)	Spoke1 (VPN Interface IP: 192.0.2.35)
📀 show crypto ipsec sa peer 192.0.2.35 🖥	📀 show crypto ipsec sa peer 192.0.2.33 🖥
peer address: 192.0.2.35	peer address: 192.0.2.33
<pre>interface: outside-isp2_dynamic_vti_2_va3</pre>	<pre>interface: outside-isp2_static_vti_2</pre>
Crypto map tag: outside-isp2_dynamic_vti_2_vtemplat	Crypto map tag:vti-crypto-map-Tunnel2-0-2, seq n
Protected vrf (ivrf): Global	Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0	local ident (addr/mask/prot/port): (0.0.0.0/0.0.0
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.	remote ident (addr/mask/prot/port): (0.0.0.0/0.0.
current_peer: 192.0.2.35	current_peer: 192.0.2.33
<pre>#pkts encaps: 37664, #pkts encrypt: 37664, #pkts</pre>	<pre>#pkts encaps: 37665, #pkts encrypt: 37665, #pkts</pre>
<pre>#pkts decaps: 37665, #pkts decrypt: 37665, #pkts</pre>	<pre>#pkts decaps: 37664, #pkts decrypt: 37664, #pkts</pre>
#pkts compressed: 0, #pkts decompressed: 0	#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 3/664, #pkts comp failed: 0	#pkts not compressed: 3/665, #pkts comp failed: 0
<pre>#pre-frag successes: 0, #pre-frag failures: 0, #f</pre>	<pre>#pre-frag successes: 0, #pre-frag failures: 0, #f</pre>
	Close Refresh

• show vpn-sessiondb detail 121 filter ipaddress: Shows more detailed data for the VPN connection.

Tunnel Deta	ils						0
Summary							
Node A (192.0.2.33)	(500) 💡		¢	Node B (192.0.2.3	35/500) 📍		
Transmitted: 2.1	9 MB (2291421 B)			Transmitted: 2	2.19 MB (2291565 B)		
Received: 2.9	2 MB (3062380 B)			Received: 2	2.92 MB (3062200 B)		
		IPsec S	ecurity A	ssociations (1)			
> 0.0.0/0.0.0	/0/0			0.0.0.0/0.0.0.0/0/	/0		
Hubl (VPN In	terface IP: 192.0.2.33)			Spokel (VPN	Interface IP: 192.0.2.3	5)	
🔊 show crypt	o ipsec sa peer 192.0.2.3	35 🖷		Show cryp [™]	to ipsec sa peer 192.0.2	2.33 🖷	
😔 show vpn-s	essiondb detail l2l filte	er ipaddress	. 🖷	show vpn-	sessiondb detail l2l fil	lter ipaddress	. 6
Session Type Connection Index Protocol Encryption Hashing Bytes Tx Login Time Duration	: LAN-to-LAN Detailed : SDWAN-VPN2_Spoke1 : 3 : IKEv2 IPsec : IKEv2: (1)AES-GCM-256 : IKEv2: (1)none IPsec: : 2291421 : 05:41:37 UTC Wed Sep 1 : 13d 11h:27m:48s	IP Addr IPsec: (1)A (1)none Bytes Rx 1 2024	: 19 ES-GCM : 30	Session Type Connection Index Protocol Encryption Hashing Bytes Tx Login Time Duration	<pre>2: LAN-to-LAN Detailed : 192.0.2.33 : 2 : IKEv2 IPsec : IKEv2: (1)AES-GCM-25 : IKEv2: (1)none IPse : 2291565 : 05:41:36 UTC Wed Sep : 13d 11h:27m:49s</pre>	IP Addr 6 IPsec: (1)A c: (1)none Bytes Rx 11 2024	: 19 NES-C CM : 30
Tunnel Zone	: 0			Tunnel Zone	: 0		
IKEv2 Tunnel	s: 1			IKEv2 Tunnel	ls: 1	Close <u>Refr</u>	esh

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.

CLI Troubleshoot	
>_ Command: show route 🖂 A Execute 🛛 😋 Refresh 🛛 🔀 Copy	Device: Hub1
> show route	
<pre>Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF, BI - BGP InterVRF Gateway of last resort is not set</pre>	
<pre>C 192.0.2.16 255.255.255.250 is directly connected, outside-isp1 192.0.2.17 255.255.255.255 is directly connected, outside-isp2 192.0.2.33 255.255.255.255 is directly connected, outside-isp2 192.0.2.33 255.255.255.255 is directly connected, inside 198.51.100.16 255.255.255.256 is directly connected, inside 198.51.100.16 255.255.255.256 is directly connected, inside 198.51.100.16 255.255.255.256 is directly connected, inside 198.51.100.172 255.255.255.256 is directly connected, inside 209.165.201.0 255.255.255.240 [200/1] via 209.165.201.2, 1w0d B 198.51.100.128 255.255.255.240 is directly connected, Loopback1_Hub1 209.165.201.1 255.255.255.246 is directly connected, Loopback1_Hub1 209.165.201.2 255.255.255 is directly connected, Loopback1_Hub1 209.165.201.2 255.255.255 is directly connected, Loopback1_Hub1 209.165.201.2 255.255.255 is directly connected, Loopback1_Hub1 209.165.201.6 255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.6 255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.6 55.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.65 255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.66 255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.65 255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.66 295.255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.66 295.255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.66 295.255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.67 255.255.255.255 is directly connected, Loopback2_Hub1 209.165.201.67 295.255.255.255 is directly conn</pre>	

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.

CLI Troubleshoot
>_ Command: show running-config interface \Rightarrow Execute Certer Refresh Copy
: interface Loopback1 nameif Loopback1_Hub1 ip address 209.165.201.1 255.255.255.224 !
<pre>interface Loopback2 nameif Loopback2_Hub1 ip address 209.165.201.65 255.255.255.224 !</pre>
<pre>interface Virtual-Template1 type tunnel nameif outside-isp1_dynamic_vti_1 ip unnumbered Loopback1_Hub1 tunnel source interface outside-isp1</pre>
<pre>tunnel mode ipsec ipv4 tunnel protection ipsec profile FMC_IPSEC_PR0FILE_1 !</pre>
<pre>interface Virtual-Template2 type tunnel nameif outside-isp2_dynamic_vti_2 ip unnumbered Loopback2_Hub1 tunnel source interface outside-isp2</pre>
<pre>tunnel mode ipsec ipv4 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1</pre>

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:

												_
H	lub1											Sa
С	isco Secure Firewall Threa	t Defense	for VMware									
	Device Interfaces	In	line Sets	Routing	DHCP VTEP							
L Ir	terfaces Virtual Tunne	Is										
	Virtual Tunnel/Interface Template						Tunnel Source Interfac	e				
			Logical	IPsec								h
_	Tunnel Interface Name	Enable	Name	Mode	IP Address	Hardware Name	Logical Name		Topology	Remote Peer IP	Path Monitoring	
~	Virtual-Template1	0	outside-isp	IPv4	209.165.201.1/255.2 🕕	GigabitEthernet0/1	outside-isp1	192.0.2.17/28	SDWAN-VPN1	Any	Disabled	
	Virtual-Access2	0	outside-isp	IPv4	209.165.201.1	GigabitEthernet0/1	outside-isp1	192.0.2.17	SDWAN-VPN1	192.0.2.20	Disabled	
	Virtual-Access4	0	outside-isp	IPv4	209.165.201.1	GigabitEthernet0/1	outside-isp1	192.0.2.17	SDWAN-VPN1	192.0.2.19	Disabled	ſ
										< <	Viewing 1-2	2 0
~	Virtual-Template2	v	outside-isp	IPv4	209.165.201.65/255 🕤	GigabitEthernet0/2	outside-isp2	192.0.2.33/28	SDWAN-VPN2	Any	Disabled	
	Virtual-Access1	0	outside-isp	IPv4	209.165.201.65	GigabitEthernet0/2	outside-isp2	192.0.2.33	SDWAN-VPN2	192.0.2.36	Disabled	
	Virtual-Access3	0	outside-isp	IPv4	209.165.201.65	GigabitEthernet0/2	outside-isp2	192.0.2.33	SDWAN-VPN2	192.0.2.35	Disabled	

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

S	poke3												Sav
Cis	sco Firepower 1120 Threa	at Defense	9										
	Device Interfaces	i In	line Sets	Routing	DHCP \	VTEP	SNMP						
In	terfaces Virtual Tunne	ls											
	Virtual Tunnel/Interface Template						Tunnel Source Interface	9					
	Tunnel Interface Name	Enable	Logical Name	IPsec Mode	IP Address		Hardware Name	Logical Name		Topology	Remote Peer IP	Path Monitoring	R T
	Tunnel1	0	outside-isp	IPv4	209.165.201.4/27	7	Ethernet1/1	outside-isp1	192.0.2.21/28	SDWAN-VPN1	192.0.2.17	Disabled	
	Tunnel2	0	outside-isp	IPv4	209.165.201.36/2	27	Ethernet1/1	outside-isp1	192.0.2.21/28	SDWAN-VPN1	192.0.2.18	Disabled	
	Tunnel3	0	outside-isp	IPv4	209.165.201.68/2	27	Ethernet1/3	outside-isp2	192.0.2.37/28	SDWAN-VPN2	192.0.2.33	Disabled	
	Tunnel4	0	outside-isp	IPv4	209.165.201.100/	/27	Ethernet1/3	outside-isp2	192.0.2.37/28	SDWAN-VPN2	192.0.2.34	Disabled	

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.

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></peer-ip>	Enable conditional debugging for a particular peer
debug vti 255	Debug the Virtual Tunnel Interface information.

CLI and Debug Commands

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.

A: · → B: Topology: VPN101-P2Pv4 S	Status: 😑 Inactive	×
General CLI Details	Packet Tracer	
SELECT TRACE		
See Trace Config		
Node A Traces	🗙 Node B Traces	×
$\blacktriangleright \checkmark \rightarrow \text{Allow} \text{A: In} \rightarrow \text{Out}$	> \checkmark Allow B (Decrypted): Out –	→ In
> Allow A (Decrypted): I	In \leftarrow Out \rightarrow \checkmark \leftarrow Allow B: Out \leftarrow In	