FORTINET

# Single Datacenter Deployment for Enterprise

Secure SD-WAN

4D

DEFINE / DESIGN / DEPLOY / DEMO

# Table of Contents

# Change Log

| Date | Change Description |
|---|---|
| 2022-05-10 | Initial release. |
| 2022-11-03 | Updated Branch BGP signaling on page 35. |

# Introduction

Fortinet Secure SD-WAN documentation is categorized into four distinct documents (called 4-D documents): Define, Design, Deploy, and Demo. Each document is designed for a specific purpose and builds on the other documents by providing you a complete path from beginning to end.

The 4-D documentation series includes the following components:

- **Define**: Conceptual guide meant to introduce the reader to common SD-WAN use cases and the Fortinet Secure SD-WAN solution
- **Design**: Reference architecture guide that provides an overview of the components and architectures to satisfy common uses
- **Deploy**: Deployment guides that provide step-by-step procedures for deploying the desired architecture
- **Demo**: Github repository of the configuration and examples provided by documents

This document will cover the step-by-step procedures required to deploy the Fortinet Secure SD-WAN solution in single hub regions.

The architecture, components and technology referenced in this document is covered in the Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide.

For additional information and documentation about the topics covered in this document, please see the Fortinet Document Library at https://docs.fortinet.com.

This section contains the following topics:

## Audience

This guide is primarily created for a technical audience, including system architects and design engineers who want to deploy Fortinet Secure SD-WAN in greenfield scenarios. It is assumed that the reader has read the SD-WAN Architecture for Enterprise guide and has identified the architecture that satisfies their use case and goals. Solution overviews and descriptive explanations of the technologies and components will not be covered in this document.

For implementation, a working knowledge of FortiOS networking and policy configuration is ideal.

# About this guide

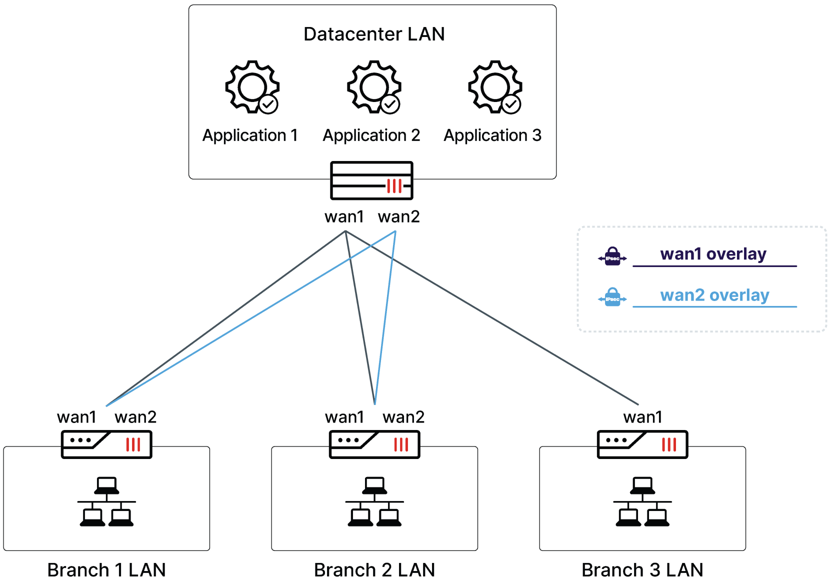
This guide utilizes FortiManager 7.2.0 and FortiOS 7.2.0 for all configuration examples. FortiOS 7.0 is also supported for FortiGate devices using the same steps and procedures covered in this document. When selecting a firmware to use in your deployment, it is important to reference the FortiManager and FortiOS Release Notes.

Release notes will cover supported FortiGate and FortiManager models, special notices, upgrade information, known issues, and other critical information that should be evaluated for your scenario.

For comments and feedback about this document, visit Single Datacenter Enterprise SD-WAN on community.fortinet.com.

# Deployment objectives

This deployment guide is the supporting document to the Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide.



# Deployment assumptions

- Greenfield deployment of new Fortinet Secure SD-WAN devices.
- Single hub FortiGate is located in a private location (such as an HQ location, datacenter, or cloud).
- Single hub will provide secure access to remote branch locations that require connectivity to local application and services.
- Single hub has two, redundant WAN connections.
- Each Branch location has two, redundant WAN connections
- WAN connections are public links that can reach all other devices in the region.

## DEPLOYMENT OBJECTIVES

- All WAN interfaces have already been configured and have default gateways configured across both links.

# Solution overview

This guide is separated into the following parts:

1. In FortiManager, configure the overlay network using the SD-WAN Overlay Provisioning Template.
   **One-to-one overlay mapping per underlay**: in this design, each branch underlay terminates a new IPsec tunnel to one—and only one—gateway underlay. This is the most common overlay design, and simplifies our configuration, but also provides less redundancy than the subsequent full mesh. Full mesh overlay mapping is generally not recommended for multi-datacenter deployments, unless there is a specific use case by which this may be required.
2. Assign Meta fields to Branch devices.
3. Configure SD-WAN rules for Corporate and Internet traffic
   **Direct Internet Access (DIA)**: used when local internet breakout at a branch location is required. This is typically SaaS applications or websites, located on the internet, which the branches will access directly. SD-WAN applies intelligence to select the best WAN link for this access.

   **Branch to Corporate LAN**: Preference is given to the primary DC connections when accessing corporate resources. If the primary DC is unable to meet SLA requirements, the secondary DC is selected.
4. Create a Policy Package for the Branches and Hub.
   - Branches
     i. Branch to DC
     ii. Branch to internet.
   - Hub
     i. Branch to DC
     ii. SLA-healthcheck
5. Deploy the configuration to the devices.

Basic policies are provided to facilitate communication. Additional features discussed in the architecture guide, such as ADVPN and forward error correction, are discussed in Extensions on page 31, and you can add them to the configuration later. If you plan to implement one of these features as part of your design, be sure to review the relevant section prior to beginning so that you may incorporate the steps inline.

FortiManager provides continued value post deployment through SD-WAN monitoring, IPsec monitoring, and change management.

# Design overview

In this design, the SD-WAN gateway (or sometimes referred to as the hub) acts as a head-end into the business application or private workload. SD-WAN gateways can be located in a single datacenter or central office, and typically provide connectivity for remote locations.

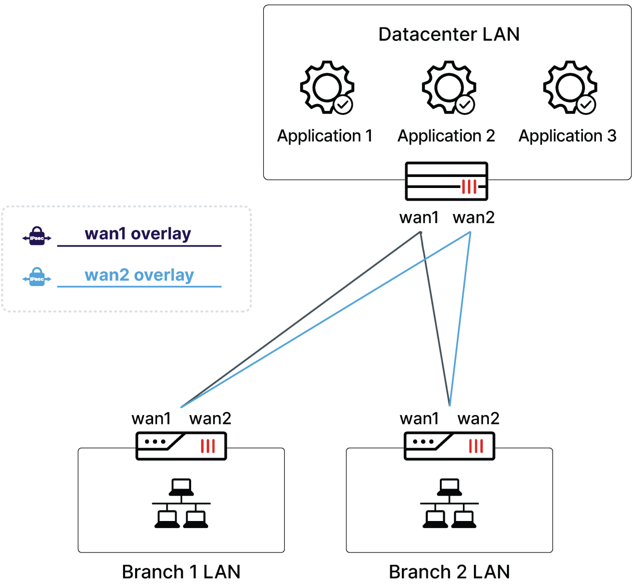
The following sections help describe the solution design:

- Use cases and topologies on page 9
- Product prerequisites on page 10

## Use cases and topologies

The most common use case for a single SD-WAN gateway is for private workloads and applications where stability is preferred.

This topology may be expanded to include other design features such as cloud on-ramp, direct internet access and AD-VPN to name a few. See Extensions on page 31 for details.



# Product prerequisites

- Hub FortiGate with dual WAN connections
- Branch FortiGate with dual WAN connections
- FortiManager 7.2.0 or later to leverage SD-WAN overlay provisioning template

# Deployment procedures

FortiManager is used to configure SD-WAN for a topology that includes a single datacenter (hub) and multiple branch devices. The deployment instructions include the following topics:

- Prerequisites on page 11
- Recommendations on page 11
- Planning on page 12
- Assumptions on page 12
- Configuration steps on page 12

## Prerequisites

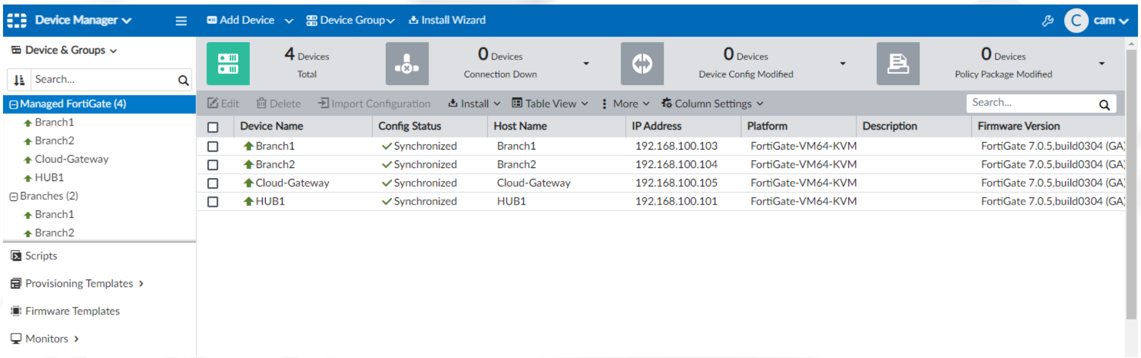
This guide presumes the following prerequisites have been met:

- Hub and branch FortiGates have been imported into FortiManager.
  - The hub and branch devices have active connections to FortiManager.
- ISP links and other interfaces have been configured on all devices.
  - ISP routing is configured where branches have proper routes to reach the Hub.
  - LAN and other directly connected networks have been assigned.

## Recommendations

It is recommended to create a device group in FortiManager for the branch devices before utilizing the SD-WAN Overlay template. With device groups, you can add additional branch devices to the group, and the newly added devices will automatically inherit the configuration for SD-WAN.

In *Device Manager*, use the *Device Group* menu in the banner to create a new device group.



| ☐ | Device Name | Config Status | Host Name | IP Address | Platform | Description | Firmware Version |
|---|---|---|---|---|---|---|---|
| ☐ | Branch1 | ✓ Synchronized | Branch1 | 192.168.100.103 | FortiGate-VM64-KVM | | FortiGate 7.0.5,build0304 (GA) |
| ☐ | Branch2 | ✓ Synchronized | Branch2 | 192.168.100.104 | FortiGate-VM64-KVM | | FortiGate 7.0.5,build0304 (GA) |
| ☐ | Cloud-Gateway | ✓ Synchronized | Cloud-Gateway | 192.168.100.105 | FortiGate-VM64-KVM | | FortiGate 7.0.5,build0304 (GA) |
| ☐ | HUB1 | ✓ Synchronized | HUB1 | 192.168.100.101 | FortiGate-VM64-KVM | | FortiGate 7.0.5,build0304 (GA) |

# Planning

The deployment example in this guide uses the following settings, including IP networks, BGP AS number, performance SLA criteria, and so on:

1. Overlay network address space:
   a. This address space is used for the IP addressing of all Hub and Branch devices.
   b. The default 10.10.0.0/16 is used.
2. Loopback IP address space:
   a. These addresses are used for Performance SLAs, Router IDs and other admin operations.
   b. The default 172.16.0.0/16 is used.
3. Autonomous System number for BGP:
   a. A private number is used and must remain exclusively for this SD-WAN BGP configuration.
   b. The default of 65000 is used.

# Assumptions

The deployment example in this guide uses the following ports and IP addresses:

- ISP1 is connected to port1 on all FortiGates.
- ISP2 is connected to port2 on all FortiGates.
- LAN is connected to port3 on all FortiGates.
- Corporate datacenter LAN is 192.168.1.0/24.

# Configuration steps

Following is a summary of the steps required to configure SD-WAN using FortiManager:

1. Configure the overlay using the SD-WAN overlay template. See Creating an overlay template on page 13.
2. Assign metadata values to branch devices. See Assigning meta data values to branch devices on page 17.
3. Configure SD-WAN rules. See Configuring SD-WAN rules on page 17.
4. Create normalized interfaces. See Creating normalized interfaces on page 20.

5. Create policy packages and firewall policies for hub and branch devices. See Creating policy packages and firewall policies on page 21.
6. Install policy packages to devices. See Installing policy packages on page 26.
7. Verify the SD-WAN configuration. See Verifying the SD-WAN configuration on page 29.

## Creating an overlay template

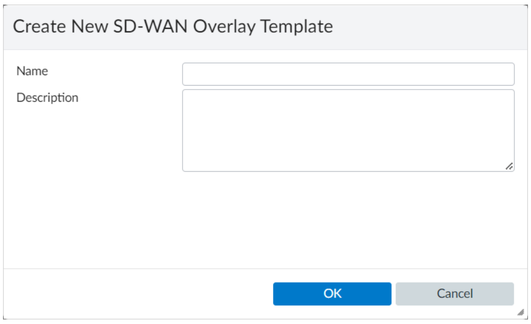
This section describes how to use the SD-WAN overlay template to configure the overlay network.

The SD-WAN overlay provisioning template supports metafields for each input box that displays a magnifying glass.

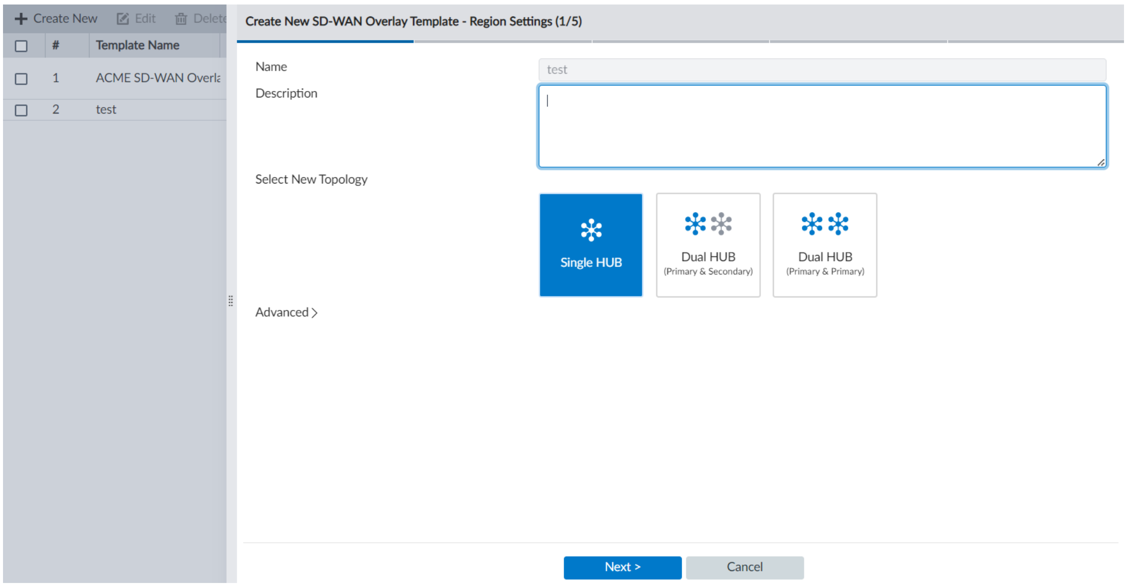
For more information, see the *FortiManager 7.2 Administration Guide*.

To create an overlay template:

1. In FortiManager, go to *Device Manager > Provisioning Templates > SD-WAN Overlay Templates*.
2. Click *Create New*. The *Create New SD-WAN Overlay Template* dialog box is displayed.



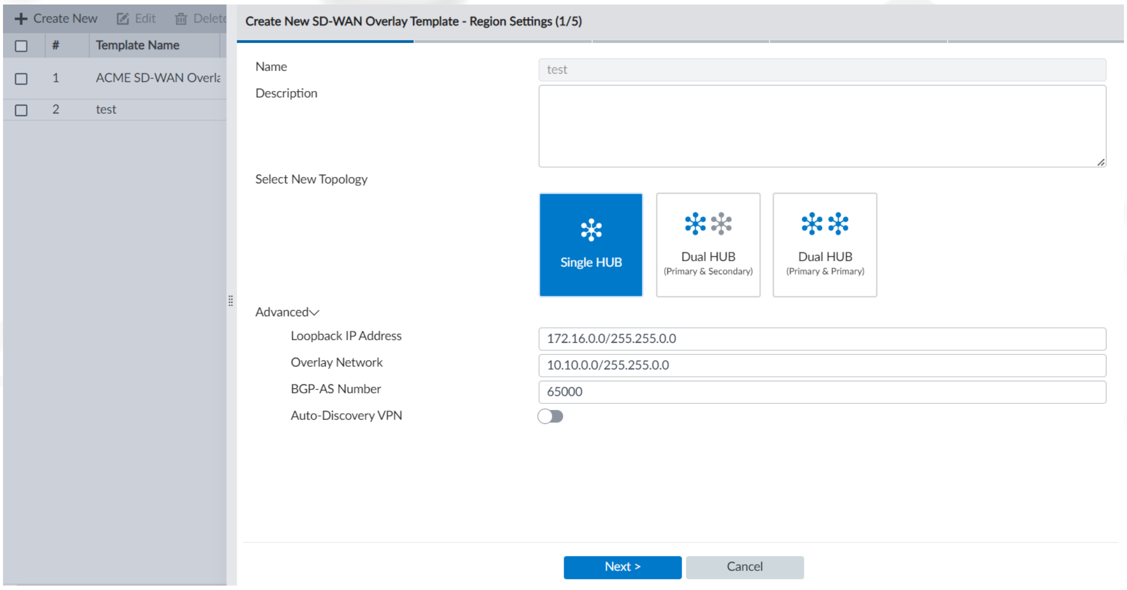
3. Enter a name and description for the template, and click *OK*. The *Region Settings* pane is displayed.



| # | Template Name |
|---|---|
| 1 | ACME SD-WAN Overla |
| 2 | test |

Name: test

4. Set the region settings:
   a. Select *Single Hub*.
   b. Expand *Advanced*, and modify the default IP address scheme for loopback and overlay networks, BGP-AS number, and to enable AD-VPN as desired.



Create New SD-WAN Overlay Template - Region Settings (1/5)

| | # | Template Name |
|---|---|---|
| □ | 1 | ACME SD-WAN Overla |
| □ | 2 | test |

Name: test

Description:

Select New Topology: Single HUB | Dual HUB (Primary & Secondary) | Dual HUB (Primary & Primary)

Advanced

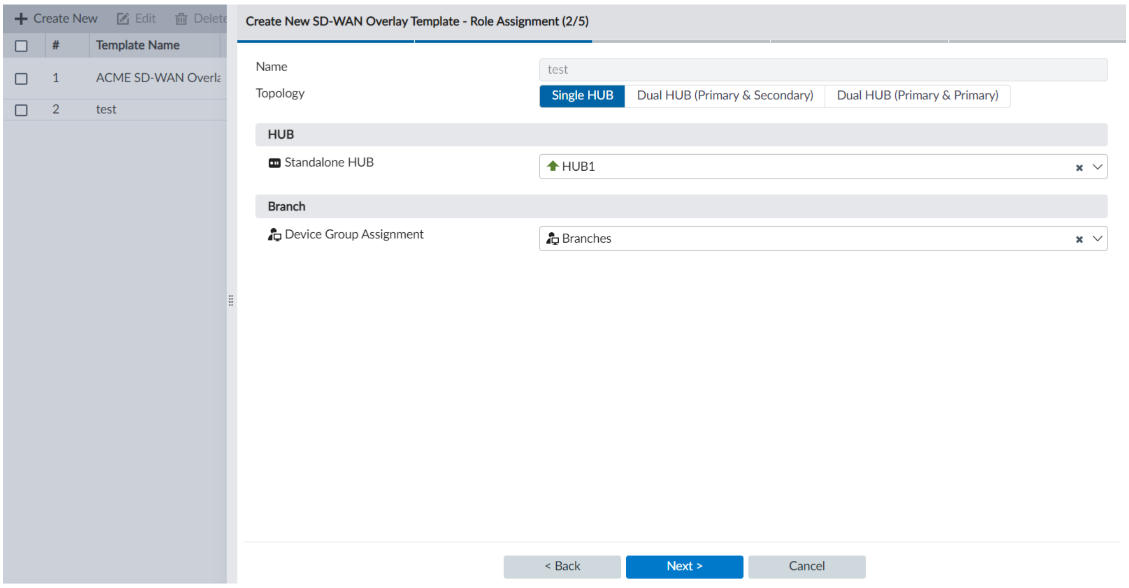
- Loopback IP Address: 172.16.0.0/255.255.0.0
- Overlay Network: 10.10.0.0/255.255.0.0
- BGP-AS Number: 65000
- Auto-Discovery VPN

c. Click *Next*.The *Role Assignment* pane is displayed.

5. Set the role assignment:

   a. Set *Standalone HUB* to *HUB1*.

   b. Set *Device Group Assignment* to *Branches*.



Create New SD-WAN Overlay Template - Role Assignment (2/5)

| | # | Template Name |
|---|---|---|
| □ | 1 | ACME SD-WAN Overla |
| □ | 2 | test |

Name: test

Topology: Single HUB | Dual HUB (Primary & Secondary) | Dual HUB (Primary & Primary)

HUB

- Standalone HUB: HUB1

Branch

- Device Group Assignment: Branches

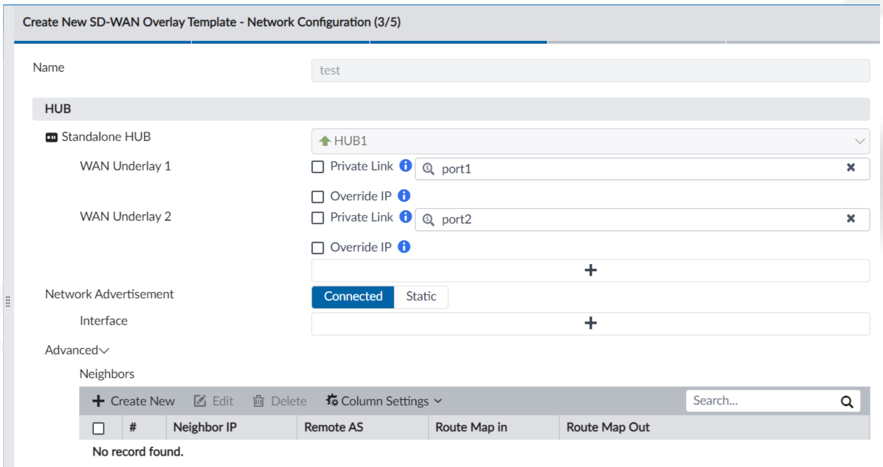
c. Click *Next*. The *Network Configuration* pane is displayed.

6. Set the network configuration for the HUB:

   a. Under *Standalone HUB*, set *WAN Underlay 1* to *port1*.

   b. Set *WAN Underlay 2* to *port2*.

c. Expand *Advanced*.



Create New SD-WAN Overlay Template - Network Configuration (3/5)

Name: test

HUB

Standalone HUB: HUB1

WAN Underlay 1: □ Private Link | port1 | □ Override IP

WAN Underlay 2: □ Private Link | port2 | □ Override IP

Network Advertisement: Connected | Static

Interface

Advanced

Neighbors

| □ | # | Neighbor IP | Remote AS | Route Map in | Route Map Out |
|---|---|---|---|---|---|

No record found.

d. Click *Create New*. The *Create New Neighbor* pane is displayed.

e. Set *Neighbor IP* to *172.16.1.1*.

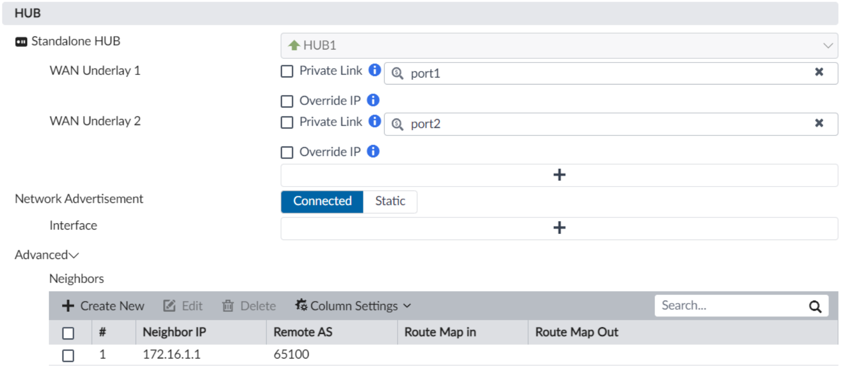
f. Set *Remote AS* to *65100*.

g. Click *OK*. The BGP neighbor is created.

A neighbor is configured for the HUB to learn the route to the Corporate Datacenter LAN (192.168.1.0/24) over BGP. This is also why there is no need to specify a Network Advertisement. Routes learned from an eBGP peer are re-advertised to all iBGP and eBGP peers by default.

Select *Private Link* if the port is on a private circuit, and you do not want to create an overlay network utilizing this link.

Select *Override IP* if you want to manually input an IP address that remote branches will connect to. This is commonly used in public cloud providers where interfaces have private IP address or other NAT'd environments.



HUB

Standalone HUB: HUB1

WAN Underlay 1: □ Private Link | port1 | □ Override IP

WAN Underlay 2: □ Private Link | port2 | □ Override IP

Network Advertisement: Connected | Static

Interface

Advanced

Neighbors

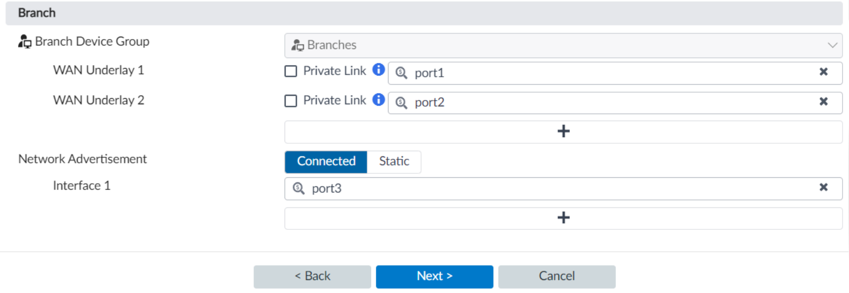
| □ | # | Neighbor IP | Remote AS | Route Map in | Route Map Out |
|---|---|---|---|---|---|
| □ | 1 | 172.16.1.1 | 65100 | | |

7. Set the network configuration for the branch device group:

a. Scroll down to *Branch Device Group*, and set *WAN Underlay 1* to *port1*.

b. Set *WAN Underlay 2* to *port2*.

c. Set *Network Advertisement* to *Connected* and *port3*.



Branch

Branch Device Group — Branches

WAN Underlay 1 — □ Private Link — port1

WAN Underlay 2 — □ Private Link — port2

Network Advertisement — Connected | Static

Interface 1 — port3

< Back | Next > | Cancel

This interface will be advertised to the rest of the SD-WAN region. In this example, port3 is our LAN interface for each branch, and so will advertise the branch's LAN subnet..

d. Click *Next*. The *SD-WAN Template Options* pane is displayed.

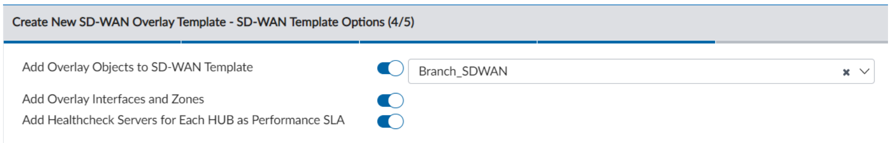
8. Set the SD-WAN template options:

a. Enable *Add Overlay Objects to SD-WAN Template*.

b. In the list, click *Create New* to create a new SD-WAN template named *Branch_SDWAN*. No configuration of the template is needed at this time.

c. Enable *Add Overlay Interfaces and Zones*.

d. Enable *Add Healthcheck Servers for Each Hub as Performance SLA*.



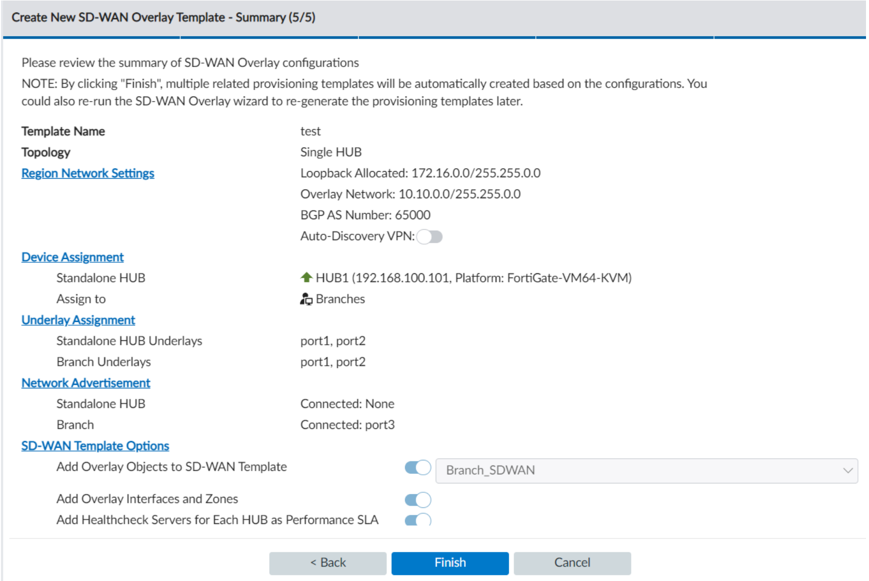
Create New SD-WAN Overlay Template - SD-WAN Template Options (4/5)

Add Overlay Objects to SD-WAN Template — ● Branch_SDWAN

Add Overlay Interfaces and Zones — ●

Add Healthcheck Servers for Each HUB as Performance SLA — ●

e. Click *Next*.The *Summary* pane is displayed.



Create New SD-WAN Overlay Template - Summary (5/5)

Please review the summary of SD-WAN Overlay configurations
NOTE: By clicking "Finish", multiple related provisioning templates will be automatically created based on the configurations. You could also re-run the SD-WAN Overlay wizard to re-generate the provisioning templates later.

| | |
|---|---|
| **Template Name** | test |
| **Topology** | Single HUB |
| Region Network Settings | Loopback Allocated: 172.16.0.0/255.255.0.0 |
| | Overlay Network: 10.10.0.0/255.255.0.0 |
| | BGP AS Number: 65000 |
| | Auto-Discovery VPN: ○ |
| Device Assignment | |
| Standalone HUB | HUB1 (192.168.100.101, Platform: FortiGate-VM64-KVM) |
| Assign to | Branches |
| Underlay Assignment | |
| Standalone HUB Underlays | port1, port2 |
| Branch Underlays | port1, port2 |
| Network Advertisement | |
| Standalone HUB | Connected: None |
| Branch | Connected: port3 |
| SD-WAN Template Options | |
| Add Overlay Objects to SD-WAN Template | ● Branch_SDWAN |
| Add Overlay Interfaces and Zones | ● |
| Add Healthcheck Servers for Each HUB as Performance SLA | ● |

< Back | Finish | Cancel

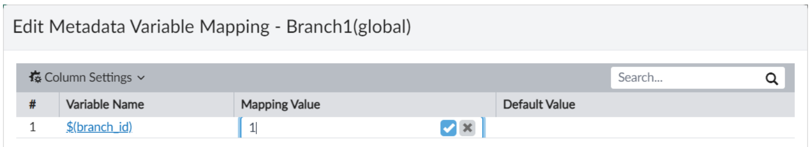
9. Click *Finish* to save the template.

## Assigning meta data values to branch devices

Each branch must have a unique *branch_id* mapping value in order to successfully utilize the SD-WAN overlay provisioning template.

To assign meta data values to branch devices:

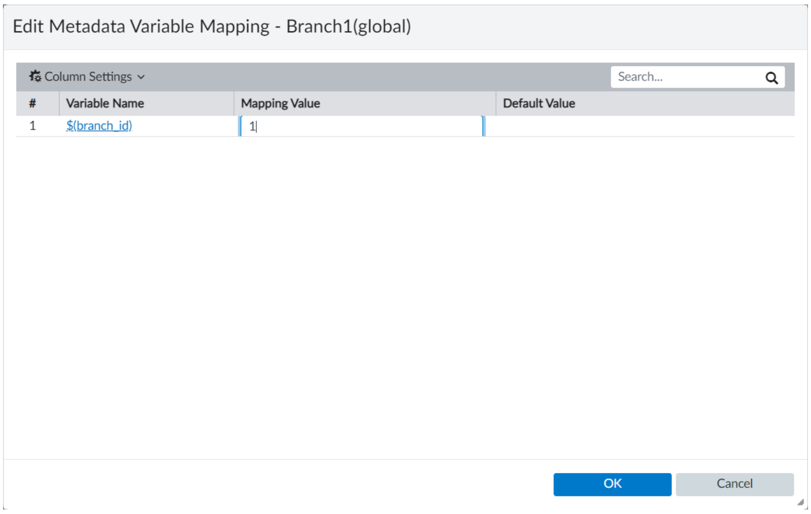
1. In FortiManager, go to *Device Manager > Device & Groups*, and expand *Managed FortiGates*.
2. Set the variable for Branch1:
   - a. In the content pane, right-click *Branch1* and select *Edit Variable Mapping*. The *Edit Metadata Variable Mapping* dialog box is displayed.
   - b. Click the *Mapping Value* cell, type *1*, and select the checkmark to set the value.



Edit Metadata Variable Mapping - Branch1(global)

| # | Variable Name | Mapping Value | Default Value |
|---|---|---|---|
| 1 | $(branch_id) | 1 | |

The value is set.



Edit Metadata Variable Mapping - Branch1(global)

| # | Variable Name | Mapping Value | Default Value |
|---|---|---|---|
| 1 | $(branch_id) | 1 | |

   - c. Click *OK* to save the changes.
3. Repeat to set *Branch2* to *2*.

## Configuring SD-WAN rules

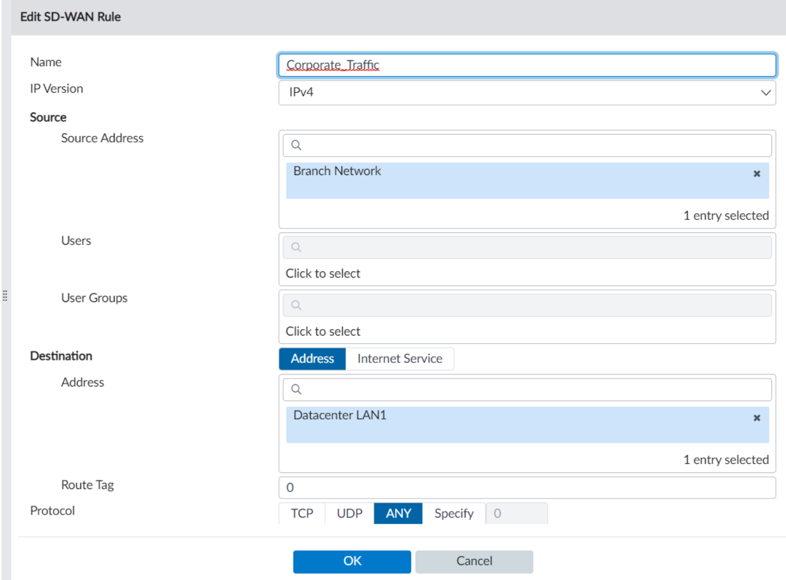
In this section we are going to edit the SD-WAN template to create a new performance SLA target as well as new SD-WAN rules.

To configure SD-WAN rules:

1. In FortiManager, go to *Provisioning Templates > SD-WAN Templates*.
2. Double-click the *Branch_SDWAN* template to open it for editing.

3. Create a rule named *Corporate_Traffic*:
    a. Under *SD-WAN Rules*, and click *Create New*. The *Create New SD-WAN Rule* pane opens.
    b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Corporate_Traffic |
| Source | Branch Network, 10.1.0.0/16 (Create new Address Object) |
| Destination | Datacenter LAN1, 192.168.100.0/24 (Create new Address Object) |
| Strategy | Lowest Cost SLA |
| Interface Preference | HUB1-VPN1, HUB1-VPN2 |
| Required SLA Target | HUB1_HC#1 |



Edit SD-WAN Rule

Name: Corporate_Traffic

IP Version: IPv4

Source

Source Address: Branch Network ×
1 entry selected

Users: Click to select

User Groups: Click to select

Destination: Address | Internet Service

Address: Datacenter LAN1 ×
1 entry selected

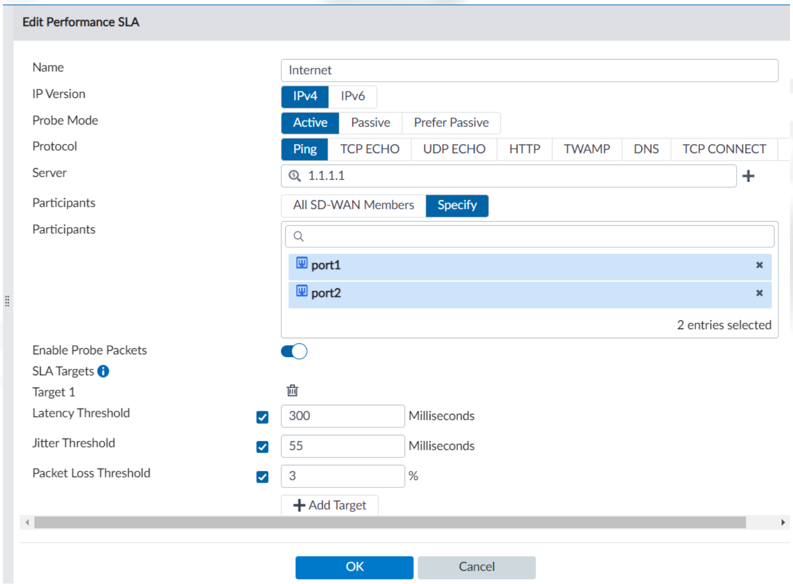
Route Tag: 0

Protocol: TCP | UDP | ANY | Specify | 0

The SD-WAN rule is created.

4. Define an SLA target for internet traffic:
    a. Under *Performance SLA*, and click *Create New*. The *Create New Performance SLA* pane opens.
    b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Internet |
| Server | 1.1.1.1 |
| Participants | port1, port2 |
| SLA Targets | • Latency threshold: 300<br>• Jitter Threshold: 55<br>• Packet Loss Threshold: 3% |



Edit Performance SLA

Name: Internet

IP Version: IPv4 | IPv6

Probe Mode: Active | Passive | Prefer Passive

Protocol: Ping | TCP ECHO | UDP ECHO | HTTP | TWAMP | DNS | TCP CONNECT

Server: 1.1.1.1

Participants: All SD-WAN Members | Specify

Participants: port1, port2 — 2 entries selected

Enable Probe Packets: ●

SLA Targets

Target 1

Latency Threshold: ☑ 300 Milliseconds

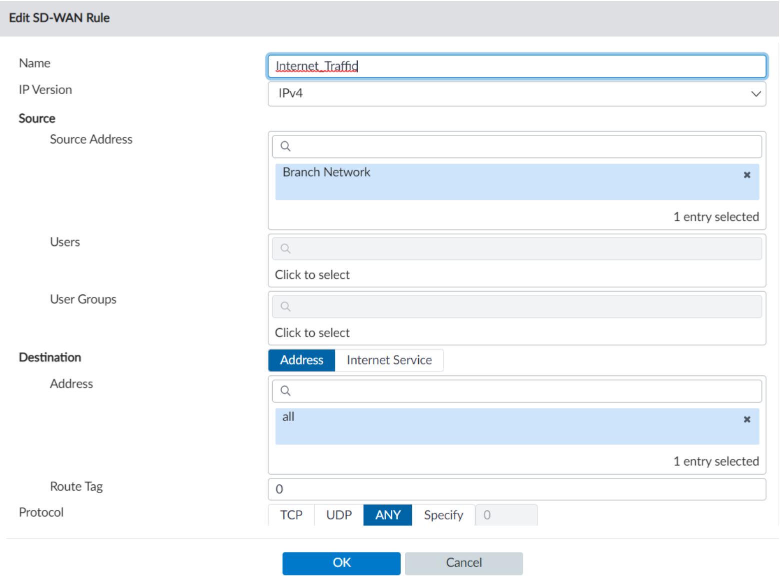
Jitter Threshold: ☑ 55 Milliseconds

Packet Loss Threshold: ☑ 3 %

The SLA target is created.

5. Create a rule named *Internet Traffic*:
   a. Under *SD-WAN Rules*, and click *Create New*. The *Create New SD-WAN Rule* pane opens.
   b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Internet_Traffic |
| Source | Branch Network |
| Destination | all |
| Strategy | Lowest Cost SLA |
| Interface Preference | port1, port2 |
| Required SLA Target | Internet |



Edit SD-WAN Rule

Name: Internet_Traffic

IP Version: IPv4

Source

Source Address: Branch Network — 1 entry selected

Users: Click to select

User Groups: Click to select

Destination: Address | Internet Service

Address: all — 1 entry selected

Route Tag: 0

Protocol: TCP | UDP | ANY | Specify 0

The SD-WAN rule is created.

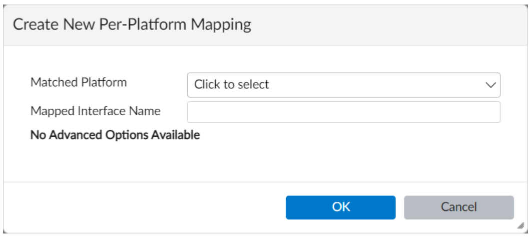
6. Click *OK* to save the SD-WAN template.

## Creating normalized interfaces

Because the policy package uses interface objects instead of directly referring to the interface, we must link the interface objects with the actual interfaces on any/all devices. We do this by creating normalized interfaces with per-platform mappings.

To create normalized interfaces:

1. In FortiManager, go to *Policy & Objects* > *Object Configurations* > *Normalized Interface*.
2. In the content pane, click *Create New*.
   The *Create New Normalized Interface* pane opens.
3. Set *Name* to *HUB1*.
4. Under *Per-Platform Mapping*, click *Create New*.
   The *Create New Per-Platform Mapping* dialog box is displayed.



Create New Per-Platform Mapping

Matched Platform: Click to select

Mapped Interface Name:

No Advanced Options Available

5. Set the following options, and click *OK*:

| | |
|---|---|
| Matched Platform | Select *all*. |
| Mapped Interface Name | Type *HUB1*. |

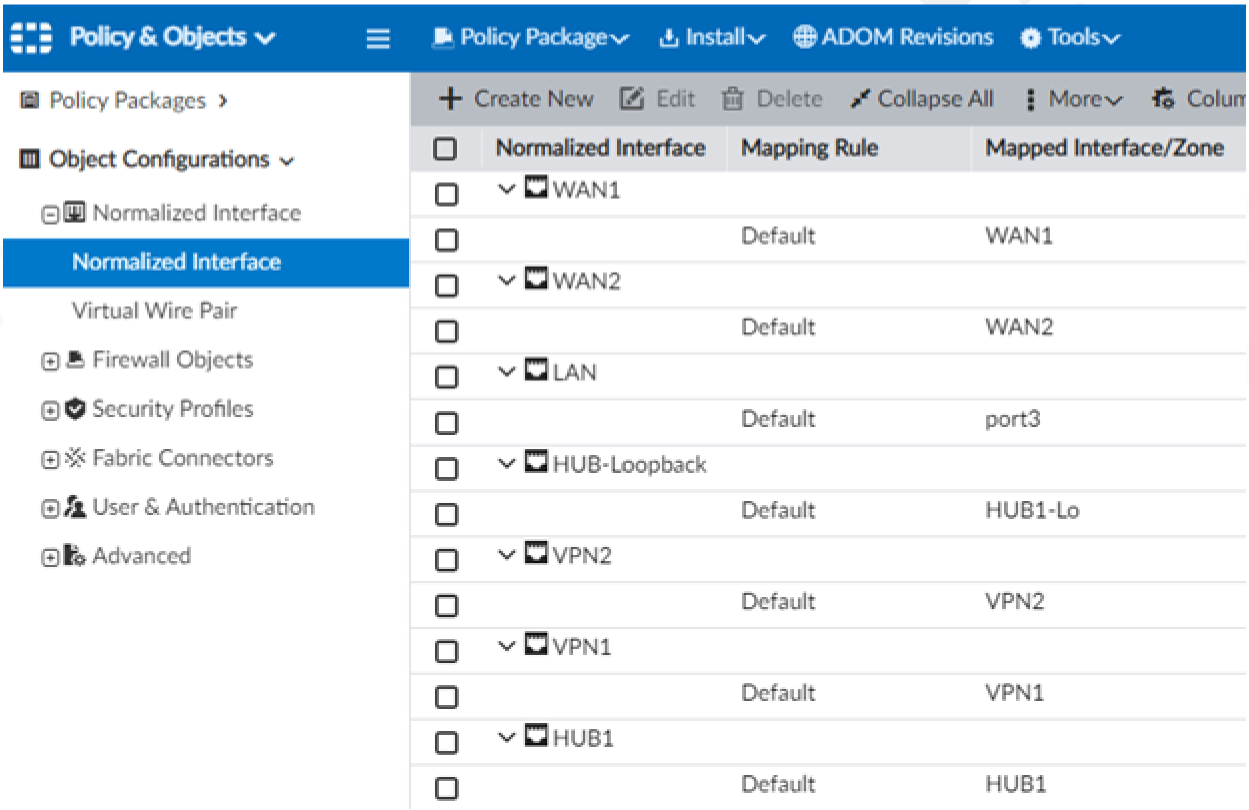
The mapped interface is case sensitive. It must exactly match the interface on the target FortiGate.

The per-platform mapping is created.

6. Repeat this procedure to the following per-platform mappings:

| Interface | Option | Setting |
|---|---|---|
| VPN1 | Matched Platform | all |
| | Mapped Interface Name | VPN1 |
| VPN2 | Matched Platform | all |
| | Mapped Interface Name | VPN2 |
| WAN1 | Matched Platform | all |
| | Mapped Interface Name | WAN1 |
| WAN2 | Matched Platform | all |
| | Mapped Interface Name | WAN2 |
| HUB-Loopback | Matched Platform | all |
| | Mapped Interface Name | HUB-Lo |
| LAN | Matched Platform | all |
| | Mapped Interface Name | port3 |

All the per-platform mappings are created:



| □ | Normalized Interface | Mapping Rule | Mapped Interface/Zone |
|---|---|---|---|
| □ | WAN1 | | |
| □ | | Default | WAN1 |
| □ | WAN2 | | |
| □ | | Default | WAN2 |
| □ | LAN | | |
| □ | | Default | port3 |
| □ | HUB-Loopback | | |
| □ | | Default | HUB1-Lo |
| □ | VPN2 | | |
| □ | | Default | VPN2 |
| □ | VPN1 | | |
| □ | | Default | VPN1 |
| □ | HUB1 | | |
| □ | | Default | HUB1 |

If you are using different ports for LAN between branches, you can leverage per-device mapping to override the matched platform: all.

## Creating policy packages and firewall policies

The following policies are provided to allow traffic to flow between branches and hub. They require further security configuration to secure the communication.

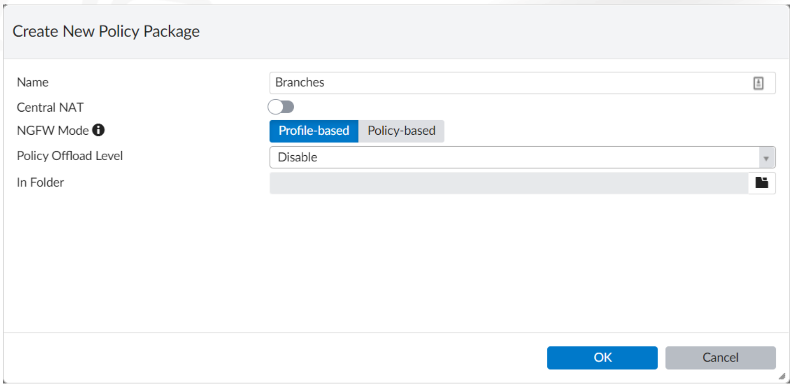
Following is a summary of how to create the policy package:

1. Create a policy package for branch devices. See Creating the branch policy package and policies on page 22.
   These firewall policies leverage the SD-WAN zones and interfaces.
2. Create a policy package for the hub device. See Creating the hub policy package and policies on page 24.

## Creating the branch policy package and policies

To create the branch policy package and policies:

1. In FortiManager, go to *Policy & Objects*.
2. Create a policy package named *Branches*:
   a. From the *Policy Package* menu, select *New*.
   The *Create New Policy Package* dialog box is displayed.
   b. Set name to *Branches*, and click *OK*.



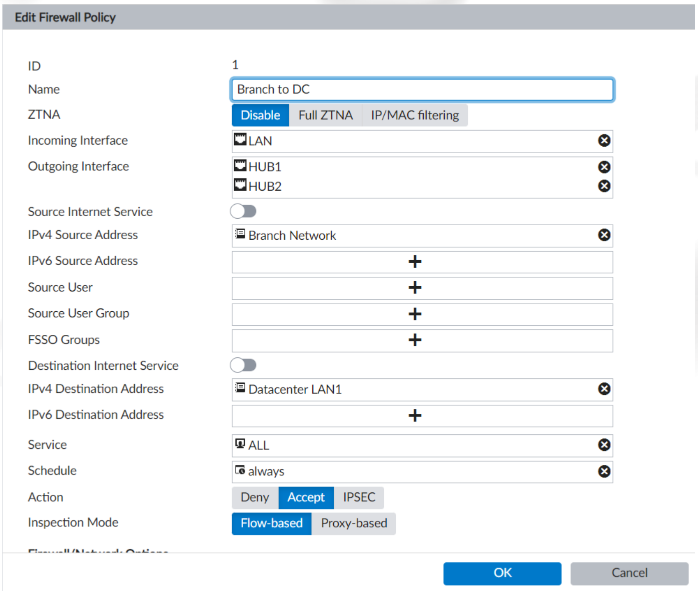
Create New Policy Package

Name: Branches
Central NAT: ○
NGFW Mode: Profile-based | Policy-based
Policy Offload Level: Disable
In Folder:

The policy package named *Branches* is created.

3. In the branches policy package, create a firewall policy named *Branch to DC* :
   a. Select the *Branches* policy package, and click *Create New*. The *Create New Firewall Policy* pane opens.
   b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Branch to DC |
| Incoming Interface | LAN |
| Outgoing Interface | HUB1 |
| IPv4 Source Address | Branch network |
| IPv4 Destination Address | Datacenter LAN1 |
| Action | Accept |



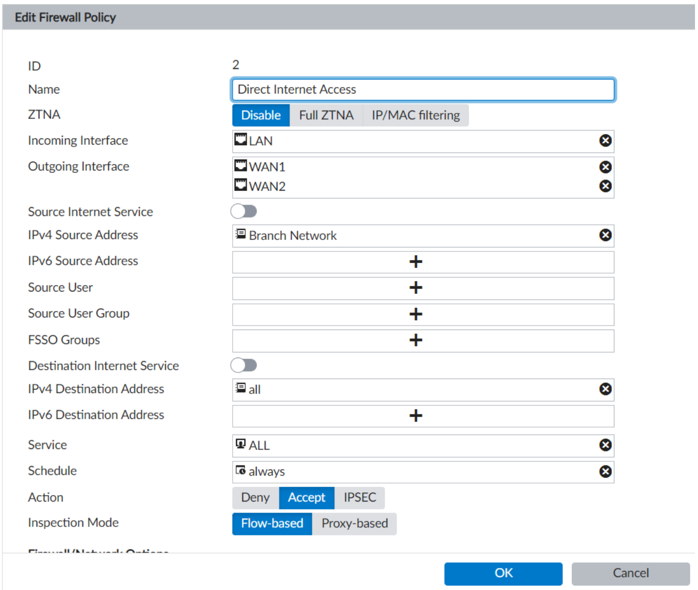
Edit Firewall Policy

|  |  |
|---|---|
| ID | 1 |
| Name | Branch to DC |
| ZTNA | [✓ Disable] Full ZTNA IP/MAC filtering |
| Incoming Interface | LAN |
| Outgoing Interface | HUB1<br>HUB2 |
| Source Internet Service | ○ |
| IPv4 Source Address | Branch Network |
| IPv6 Source Address | + |
| Source User | + |
| Source User Group | + |
| FSSO Groups | + |
| Destination Internet Service | ○ |
| IPv4 Destination Address | Datacenter LAN1 |
| IPv6 Destination Address | + |
| Service | ALL |
| Schedule | always |
| Action | Deny [✓ Accept] IPSEC |
| Inspection Mode | [✓ Flow-based] Proxy-based |
| Firewall/Network Options |  |

The firewall policy is created.

4. In the branches policy package, create a firewall policy named *Direct Internet Access*:
   a. Select the *Branches* policy package, and click *Create New*. The *Create New Firewall Policy* pane opens.
   b. Set the following options, and click *OK*:

|  |  |
|---|---|
| Name | Direct Internet Access |
| Incoming Interface | LAN |
| Outgoing Interface | wan1, wan2 |
| IPv4 Source Address | Branch network |
| IPv4 Destination Address | all |
| Action | Accept |
| NAT | Enable |

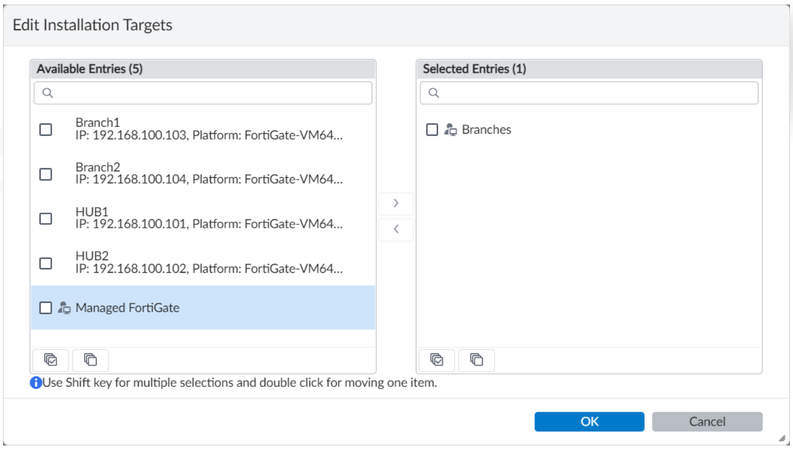


Edit Firewall Policy

|  |  |
|---|---|
| ID | 2 |
| Name | Direct Internet Access |
| ZTNA | [✓ Disable] Full ZTNA IP/MAC filtering |
| Incoming Interface | LAN |
| Outgoing Interface | WAN1<br>WAN2 |
| Source Internet Service | ○ |
| IPv4 Source Address | Branch Network |
| IPv6 Source Address | + |
| Source User | + |
| Source User Group | + |
| FSSO Groups | + |
| Destination Internet Service | ○ |
| IPv4 Destination Address | all |
| IPv6 Destination Address | + |
| Service | ALL |
| Schedule | always |
| Action | Deny [✓ Accept] IPSEC |
| Inspection Mode | [✓ Flow-based] Proxy-based |
| Firewall/Network Options |  |

The firewall policy is created.

5. Assign the branches policy package to the branch device group:
   a. On the *Policy & Objects* pane, expand the *Branches* policy package, and select *Installation Targets*.
   b. In the toolbar, click *Edit*. The *Edit Installation Targets* dialog box opens.
   c. In the *Available Entries* list, select the *Branches* group, and click the right arrow (>) to move it to the *Selected Entries* list.



Edit Installation Targets

Available Entries (5)

- ☐ Branch1 IP: 192.168.100.103, Platform: FortiGate-VM64...
- ☐ Branch2 IP: 192.168.100.104, Platform: FortiGate-VM64...
- ☐ HUB1 IP: 192.168.100.101, Platform: FortiGate-VM64...
- ☐ HUB2 IP: 192.168.100.102, Platform: FortiGate-VM64...
- ☐ Managed FortiGate

Selected Entries (1)

- ☐ Branches

Use Shift key for multiple selections and double click for moving one item.

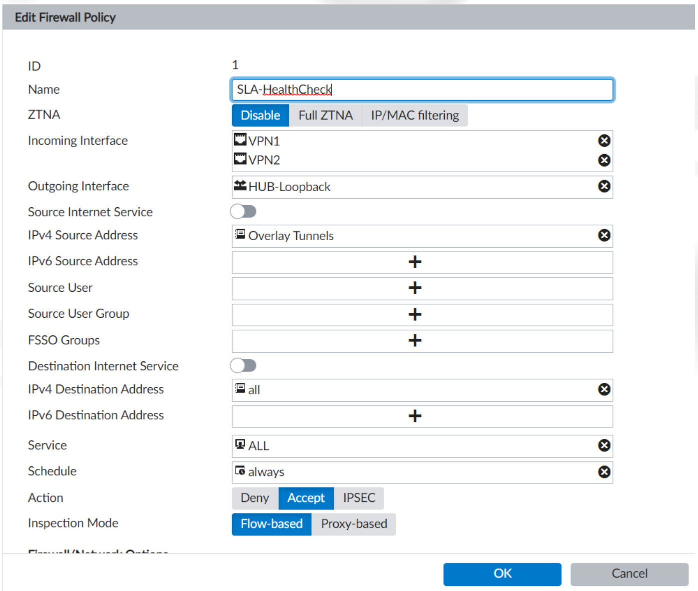
   d. Click OK.
      The installation target for the branches policy package is the *Branches* device group.

## Creating the hub policy package and policies

To create the hub policy package and policies:

1. In FortiManager, go to *Policy & Objects*.
2. Create a policy package named *HUB*:
   a. From the *Policy Package* menu, select *New*.
      The *Create New Policy Package* dialog box is displayed.
   b. Set name to *HUB*, and click *OK*.
      The policy package named *HUB* is created.
3. In the HUB policy package, create a firewall policy named *SLA-HealthCheck* :
   a. Select the *HUB* policy package, and click *Create New*. The *Create New Firewall Policy* pane opens.
   b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | SLA-HealthCheck |
| Incoming Interface | VPN1, VPN2 |
| Outgoing Interface | HUB-Lo |
| IPv4 Source Address | Overlay Tunnels, 10.10.0.0/16 (create new address object) |
| IPv4 Destination Address | all |
| Action | Accept |



Edit Firewall Policy

| | |
|---|---|
| ID | 1 |
| Name | SLA-HealthCheck |
| ZTNA | [✓ Disable] Full ZTNA IP/MAC filtering |
| Incoming Interface | VPN1<br>VPN2 |
| Outgoing Interface | HUB-Loopback |
| Source Internet Service | ○ |
| IPv4 Source Address | Overlay Tunnels |
| IPv6 Source Address | + |
| Source User | + |
| Source User Group | + |
| FSSO Groups | + |
| Destination Internet Service | ○ |
| IPv4 Destination Address | all |
| IPv6 Destination Address | + |
| Service | ALL |
| Schedule | always |
| Action | Deny [✓ Accept] IPSEC |
| Inspection Mode | [✓ Flow-based] Proxy-based |

Firewall/Network Options

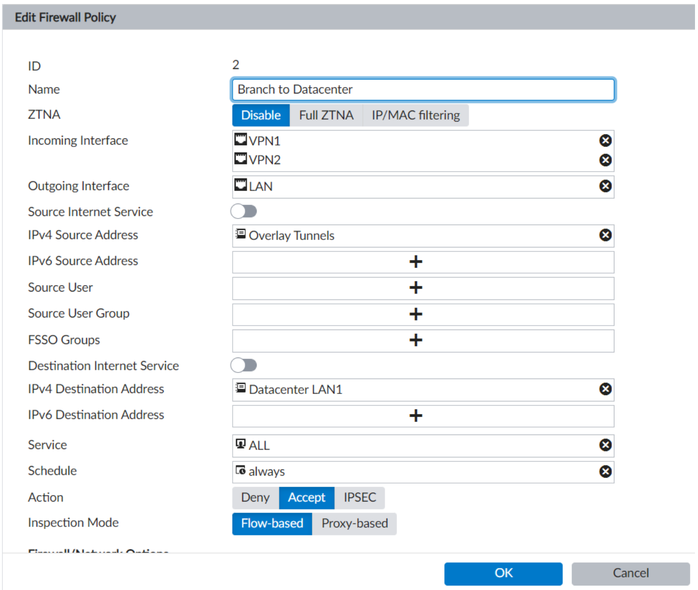
The firewall policy is created.

4. In the HUB policy package, create a firewall policy named *Branch to Datacenter*:

   a. Select the *HUB* policy package, and click *Create New*. The *Create New Firewall Policy* pane opens.

   b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Branch to Datacenter |
| Incoming Interface | VPN1, VPN2 |
| Outgoing Interface | LAN |
| IPv4 Source Address | Overlay tunnels |
| IPv4 Destination Address | Datacenter LAN1 |
| Action | Accept |



Edit Firewall Policy

| | |
|---|---|
| ID | 2 |
| Name | Branch to Datacenter |
| ZTNA | [✓ Disable] Full ZTNA IP/MAC filtering |
| Incoming Interface | VPN1<br>VPN2 |
| Outgoing Interface | LAN |
| Source Internet Service | ○ |
| IPv4 Source Address | Overlay Tunnels |
| IPv6 Source Address | + |
| Source User | + |
| Source User Group | + |
| FSSO Groups | + |
| Destination Internet Service | ○ |
| IPv4 Destination Address | Datacenter LAN1 |
| IPv6 Destination Address | + |
| Service | ALL |
| Schedule | always |
| Action | Deny [✓ Accept] IPSEC |
| Inspection Mode | [✓ Flow-based] Proxy-based |

Firewall/Network Options

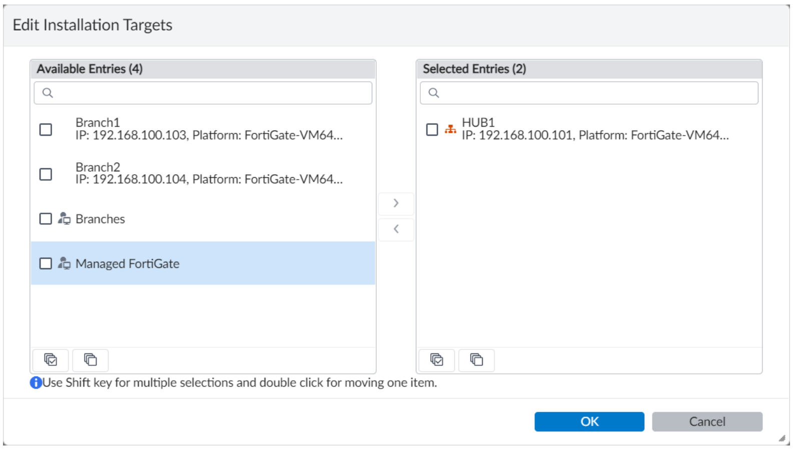
The firewall policy is created.

5. In the HUB policy package, create a firewall policy named *Datacenter to Branch*:
   - a. Select the *HUB* policy package, and click *Create New*. The *Create New Firewall Policy* pane opens.
   - b. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Datacenter to Branch |
| Incoming Interface | LAN |
| Outgoing Interface | VPN1, VPN2 |
| IPv4 Source Address | Datacenter LAN1 |
| IPv4 Destination Address | Branch network |
| Action | Accept |

   The firewall policy is created.

6. Assign the HUB policy package to the HUB1 device:
   - a. On the *Policy & Objects* pane, expand the *HUB* policy package, and select *Installation Targets*.
   - b. In the toolbar, click *Edit*. The *Edit Installation Targets* dialog box opens.
   - c. In the *Available Entries* list, select the *HUB1* device, and click the right arrow (>) to move it to the *Selected Entries* list.



Edit Installation Targets

Available Entries (4)

□ Branch1 IP: 192.168.100.103, Platform: FortiGate-VM64...

□ Branch2 IP: 192.168.100.104, Platform: FortiGate-VM64...

□ Branches

□ Managed FortiGate

Selected Entries (2)

□ HUB1 IP: 192.168.100.101, Platform: FortiGate-VM64...

Use Shift key for multiple selections and double click for moving one item.

   - d. Click *OK*.

   The installation target for the HUB policy package is the *HUB1* device.

## Installing policy packages

Because the HUB and branches use separate policy packages, we will install each policy package one one at a time:

1. Install the HUB policy package to the HUB1 device. See Installing the HUB policy package on page 26.
2. Install the branch policy package to branch device group. See Installing the branch policy package on page 28.

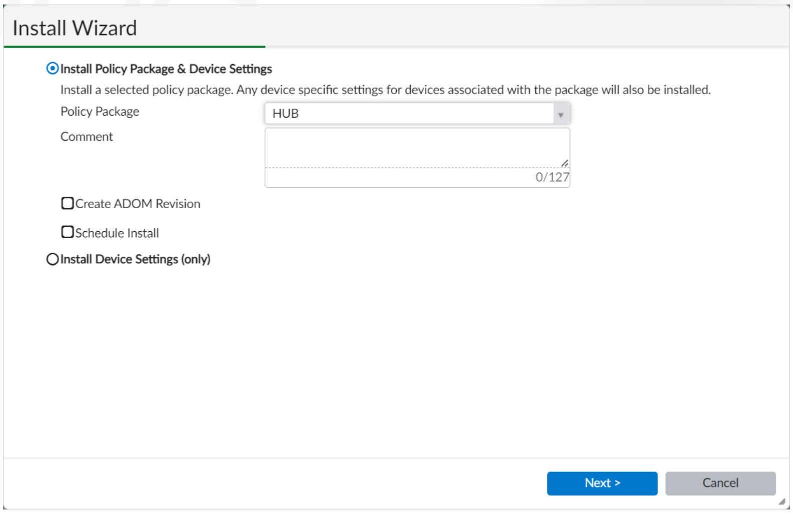
## Installing the HUB policy package

In this step, we install the HUB policy package to the HUB1 device.

To install the HUB policy package:

1. Go to *Device Manager*, and click *Install Wizard* in the toolbar.
   The *Install Wizard* dialog box opens.
2. Set the following options, and click *Next*:

| | |
|---|---|
| Install Policy Package & Device Settings | Select |
| Policy Package | HUB |



Install Wizard

● Install Policy Package & Device Settings

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: HUB

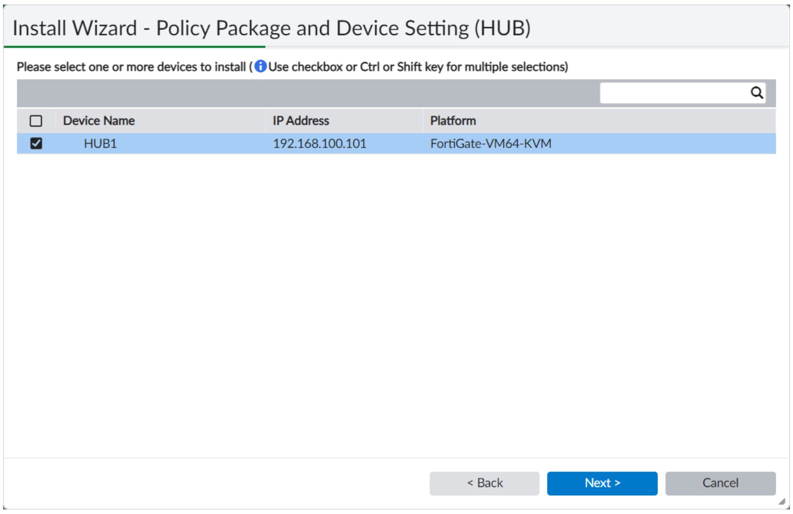
Comment: 0/127

□ Create ADOM Revision

□ Schedule Install

○ Install Device Settings (only)

The wizard moves to the next screen:

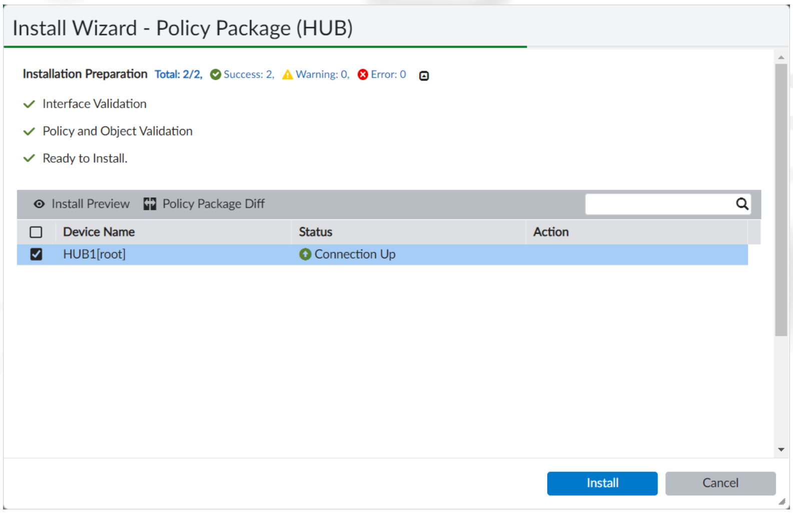


Install Wizard - Policy Package and Device Setting (HUB)

Please select one or more devices to install ( Use checkbox or Ctrl or Shift key for multiple selections)

| □ | Device Name | IP Address | Platform |
|---|---|---|---|
| ☑ | HUB1 | 192.168.100.101 | FortiGate-VM64-KVM |

3. Verify that *HUB1* is selected, and click *Next*.
   The wizard moves to the installation preparation page. When the installation preparation completes, you should see three, green checkmarks that indicate the policy package is ready to install.



Install Wizard - Policy Package (HUB)

Installation Preparation Total: 2/2, Success: 2, Warning: 0, Error: 0

✓ Interface Validation

✓ Policy and Object Validation

✓ Ready to Install.

| □ | Device Name | Status | Action |
|---|---|---|---|
| ☑ | HUB1[root] | Connection Up | |

4. Review the page, and click *Install*.
   You can click *Install Preview* to view more details before installing the policy package.
   Installation is complete when the status indicates *install and save finished status=OK*.

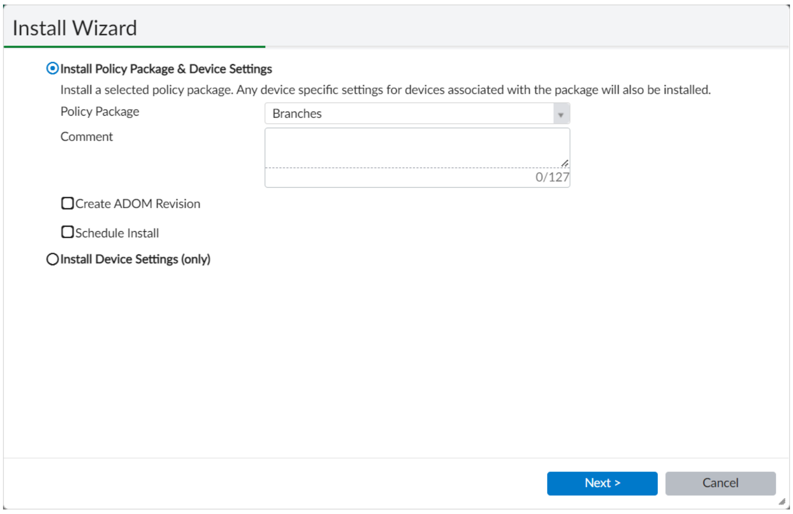
## Installing the branch policy package

In this step, we install the branch policy package to the branch device group.

To install the branch policy package:

1. Go to *Device Manager*, and click *Install Wizard* in the toolbar.
   The *Install Wizard* dialog box opens.
2. Set the following options, and click *Next*:

| | |
|---|---|
| Install Policy Package & Device Settings | Select |
| Policy Package | Branches |



Install Wizard

● Install Policy Package & Device Settings

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: Branches

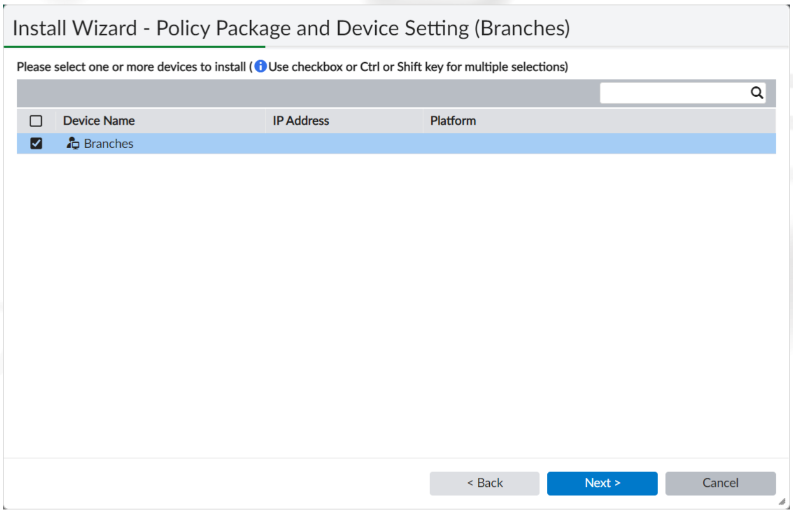
Comment: 0/127

□ Create ADOM Revision

□ Schedule Install

○ Install Device Settings (only)

The wizard moves to the next screen:



Install Wizard - Policy Package and Device Setting (Branches)

Please select one or more devices to install (ⓘ Use checkbox or Ctrl or Shift key for multiple selections)

| □ | Device Name | IP Address | Platform |
|---|---|---|---|
| ☑ | Branches | | |

3. Verify that *Branches* is selected, and click *Next*.
   The wizard moves to the installation preparation page. When the installation preparation completes, you should see three, green checkmarks that indicate the policy package is ready to install.
4. Review the page, and click *Install*.
   You can click *Install Preview* to view more details before installing the policy package.

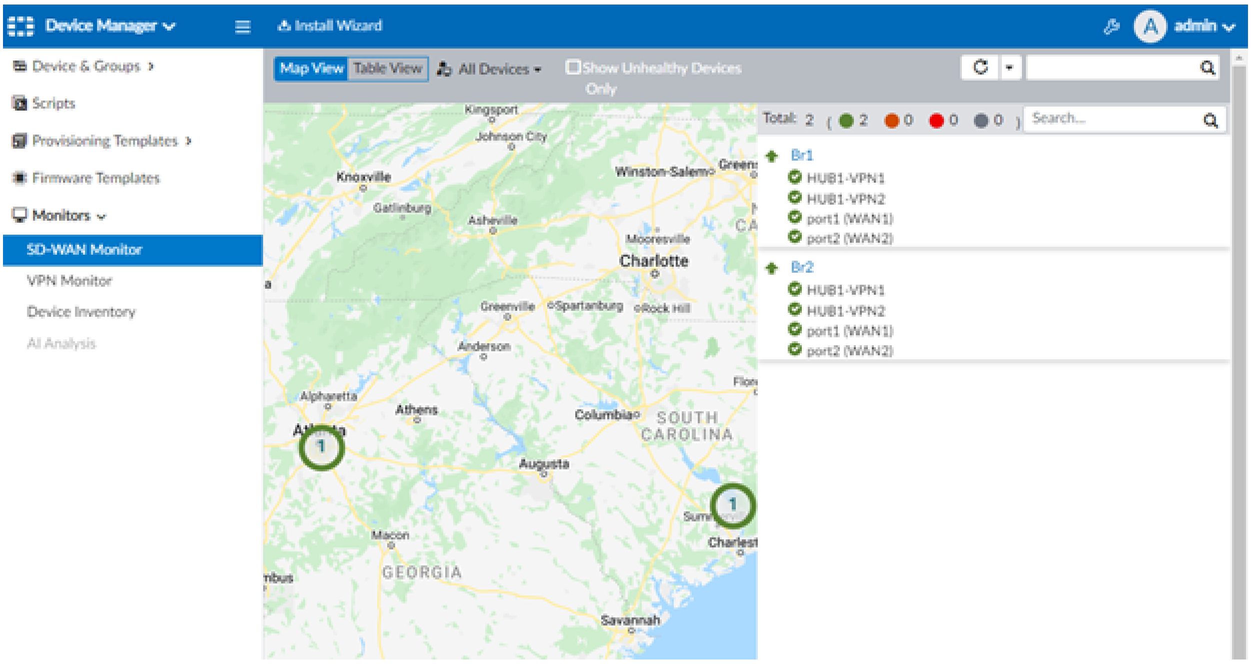
   Installation is complete when the status indicates *install and save finished status=OK*.

## Verifying the SD-WAN configuration

You can verify the SD-WAN and overlay configuration in the Device Manager > Monitor > SD-WAN Monitor pane.

To verify:

1. Go to *Device Manager > Monitors > SD-WAN Monitor*.
   A list of FortiGates are displayed in the map and on the right-hand side.



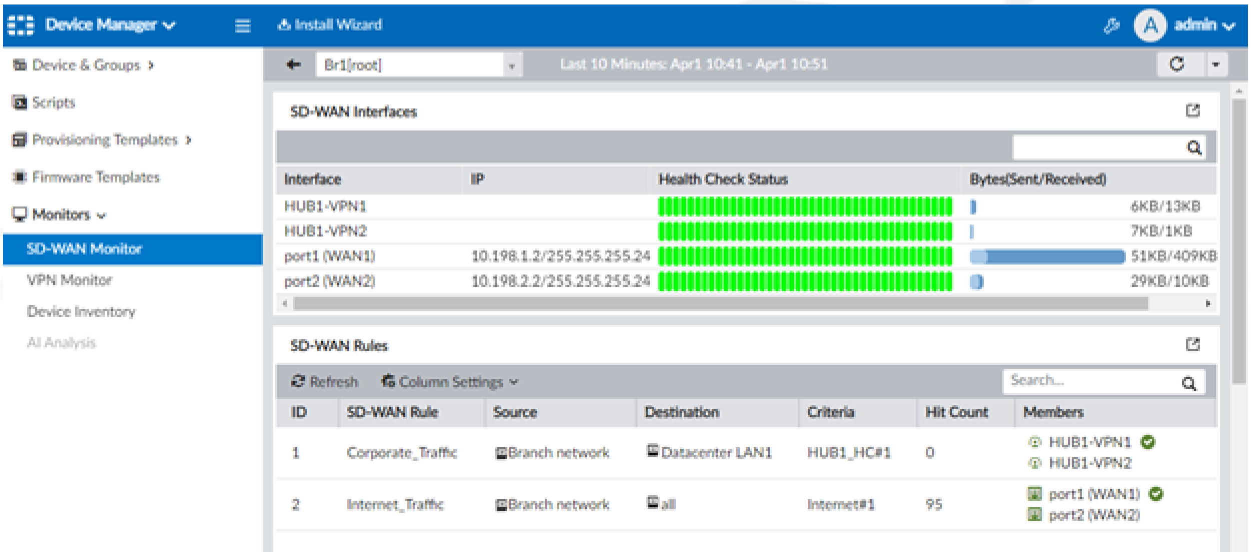
Total: 2 ( ● 2 ● 0 ● 0 ● 0 )

Br1
- ✓ HUB1-VPN1
- ✓ HUB1-VPN2
- ✓ port1 (WAN1)
- ✓ port2 (WAN2)

Br2
- ✓ HUB1-VPN1
- ✓ HUB1-VPN2
- ✓ port1 (WAN1)
- ✓ port2 (WAN2)

2. Select a FortiGate to view its SD-WAN status.

In addition to the current SD-WAN selection and status, the monitor section provides a historical view of the link health and SLA server health.



Last 10 Minutes: Apr1 10:41 - Apr1 10:51

SD-WAN Interfaces

| Interface | IP | Health Check Status | Bytes(Sent/Received) |
|---|---|---|---|
| HUB1-VPN1 | | 🟩 | 6KB/13KB |
| HUB1-VPN2 | | 🟩 | 7KB/1KB |
| port1 (WAN1) | 10.198.1.2/255.255.255.24 | 🟩 | 51KB/409KB |
| port2 (WAN2) | 10.198.2.2/255.255.255.24 | 🟩 | 29KB/10KB |

SD-WAN Rules

| ID | SD-WAN Rule | Source | Destination | Criteria | Hit Count | Members |
|---|---|---|---|---|---|---|
| 1 | Corporate_Traffic | Branch network | Datacenter LAN1 | HUB1_HC#1 | 0 | HUB1-VPN1 ✓<br>HUB1-VPN2 |
| 2 | Internet_Traffic | Branch network | all | Internet#1 | 95 | port1 (WAN1) ✓<br>port2 (WAN2) |

# Extensions

Extensions are optional enhancements to the SD-WAN solution. The extensions include:

- Auto-Discovery VPN is used to dynamically build overlay tunnels between devices in an SD-WAN region. The SD-WAN hub is the ADVPN sender that provides branch devices with the necessary details to establish their own tunnels as necessary.
- Adaptive Forward Error Correction (FEC) is a WAN remediation technique that dynamically corrects packet loss based on the detected packet loss on the link.
- SD-WAN self-healing with BGP is used to signal the optimal interface to use for traffic destined back to the spoke. Interfaces that do not meet our pre-defined SLA will be marked as *out-of-sla* to other devices in the SD-WAN network.
- SaaS remote internet breakout is used when branch traffic needs to route a SaaS application (for example, a VoIP solution) through the HUB.

This section contains the following topics:

- ADVPN on page 31
- Adaptive FEC on page 32
- SD-WAN self-healing with BGP on page 35
- SaaS remote internet breakout on page 40

## ADVPN

Following is a summary of enabling ADVPN:

1. Enable ADVPN. See ADVPN on page 31.
2. Edit the branch template to add *Branch_NET* as a destination address. See Editing branch templates on page 32.
3. Make policy routes visible in the GUI for HUB1. See Display policy routes on page 32.

### Enabling ADVPN

Edit an SD-WAN overlay template to enable ADVPN, which automatically adds the required settings to the IPsec template and the BGP template.

To enable ADVPN:

1. Go to *Device Manager > Provisioning templates > SD-WAN Overlay Template*, and double-click the *ACME SD-WAN Overlay* template to open it for editing.
2. Expand the *Advanced* menu, and enable the *Auto-Discovery VPN* toggle.
3. Click *Next* five (5) times to complete the wizard.
   The required settings are added to the IPsec template and BGP template.

## Editing branch templates

Edit the branch template to add *Branch_NET* as a destination address.

To edit the branches template:

1. Go to *SD-WAN Templates*, and double-click the the *branches* template to open it for editing.
2. In the *SD-WAN Rules* section, double-click the *Corporate_Traffic* rule to open it for editing.
3. Under *Destination*, add *Branch_NET* as a destination address (in addition to the *Datacenter LAN1* subnet), and click *OK* to save the template.

## Display policy routes

Change the display options for HUB1 to make policy routes visible in the GUI.

To display policy routes:

1. In the tree menu under *Managed FortiGates*, select *HUB1*.
2. In the second-from-left pane, click *Display Options*. The *Display Options* dialog box is displayed.
3. Enable *Router > Policy Route*, and click *OK*.

# Adaptive FEC

Following is a summary of configuring adaptive FEC:

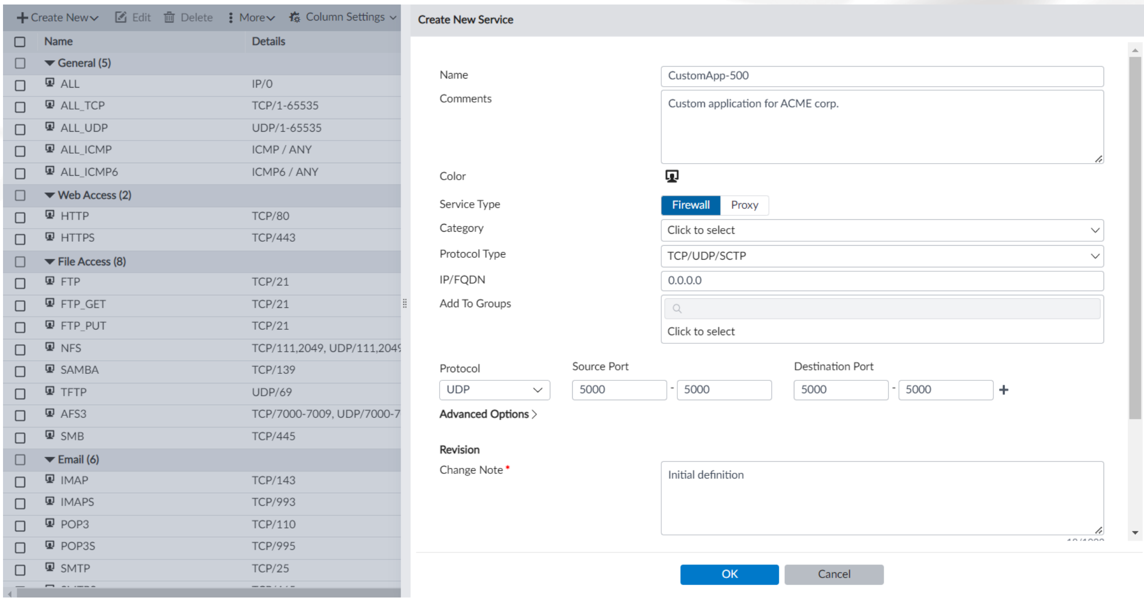
1. Define the service that FEC will protect. See Defining a custom service on page 32.
2. Define the FEC mapping to specify how many parity bits are sent based on different packet loss conditions. See Defining FEC mappings on page 33.
3. Enable FEC on both HUB VPN phase 1 interfaces. See Enabling FEC for hub devices on page 34.
4. Enable FEC on both branch VPN tunnels. See Enabling FEC on branch devices on page 34.
5. Create policies for hub and branch devices, and install the policy packages. See Creating policies and installing policy packages on page 34.

## Defining a custom service

Define the service that FEC will protect. In this example we will define a custom service.

To define a custom service:

1. Go to *Policy & Object* > *Object Configurations* > *Firewall Objects* > *Services*.
2. Click +*Create New* > *Service*.
3. Specify the name of the service, the protocol and the ports, and click *OK* to save the service.



| | Name | Details |
|---|---|---|
| □ | General (5) | |
| □ | ALL | IP/0 |
| □ | ALL_TCP | TCP/1-65535 |
| □ | ALL_UDP | UDP/1-65535 |
| □ | ALL_ICMP | ICMP / ANY |
| □ | ALL_ICMP6 | ICMP6 / ANY |
| □ | Web Access (2) | |
| □ | HTTP | TCP/80 |
| □ | HTTPS | TCP/443 |
| □ | File Access (8) | |
| □ | FTP | TCP/21 |
| □ | FTP_GET | TCP/21 |
| □ | FTP_PUT | TCP/21 |
| □ | NFS | TCP/111,2049, UDP/111,2049 |
| □ | SAMBA | TCP/139 |
| □ | TFTP | UDP/69 |
| □ | AFS3 | TCP/7000-7009, UDP/7000-7 |
| □ | SMB | TCP/445 |
| □ | Email (6) | |
| □ | IMAP | TCP/143 |
| □ | IMAPS | TCP/993 |
| □ | POP3 | TCP/110 |
| □ | POP3S | TCP/995 |
| □ | SMTP | TCP/25 |

Name: CustomApp-500
Comments: Custom application for ACME corp.
Color
Service Type: Firewall | Proxy
Category: Click to select
Protocol Type: TCP/UDP/SCTP
IP/FQDN: 0.0.0.0
Add To Groups: Click to select

| Protocol | Source Port | | Destination Port | |
|---|---|---|---|---|
| UDP | 5000 | 5000 | 5000 | 5000 |

Advanced Options

**Revision**
Change Note *: Initial definition

## Defining FEC mappings

Define the FEC mapping to specify how many parity bits are sent based on different packet loss conditions.

To define FEC mappings:

1. From the *Policy & Objects* page, use *Tools* in the banner to select *Display Options*.
2. Select *CLI Only Objects* at the bottom, and click *OK*.
3. Expand *Object Configurations* > *CLI Only Objects* > *CLI Only Objects*, and search for *FEC*.
4. c. Select *fec*, and click +*Create New*. The *create vpn ipsec fec* pane is displayed.
5. In the *Name* box, type *dc_fec*.
6. Under *mappings*, click *Create New*. The *create vpn ipsec fec* mapping pane is displayed.
7. Set the following options, and click *OK* to create the mapping:

| | |
|---|---|
| base | 8 |
| packet-loss-threshold | 5 |
| redundant | 2 |

The mapping is created.

8. Under mappings, click *Create New* again to create another mapping.
9. Set the following options, and click *OK* to create the mapping:

| | |
|---|---|
| base | 5 |
| packet-loss-threshold | 10 |
| redundant | 2 |

10. Click *OK* to save the object with two mappings.

## Enabling FEC for hub devices

Enable FEC on both HUB VPN phase 1 interfaces.

To enable FEC for hub devices:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
2. Double-click the *ACME SD-WAN Overlay_hub1_ipsec* template to open it for editing.
3. Select *VPN1*, and click *Edit*.
4. Scroll down to and expand *Advanced Options*.
5. Enable *fec-egress* and *fec-ingress*, and click *OK*.
6. Repeat for *HUB1-VPN2*.

## Enabling FEC on branch devices

Enable FEC on both branch VPN tunnels.

To enable FEC on branch devices:

1. From *IPsec Tunnel templates*, double-click the *ACME SD-WAN Overlay_branch_ipsec* template to open it for editing.
2. Double-click *HUB1-VPN1* to open it for editing.
3. For *FEC Health Check*, enter *HUB1_HC*.
4. Scroll down and expand *Advanced Options*.
5. Set the following options, and click *OK*.

| | |
|---|---|
| fec-mapping-profile | dc_fec |
| fec-egress | enable |
| rec-ingress | enable |

6. Repeat for *HUB1-VPN2*.

## Creating policies and installing policy packages

Create policies for the hub and branch devices for the custom application, and then install the policy packages to the devices.

To create policies and install policy packages:

1. Create a policy for the HUB policy package:
   a. Go to *Policy & Object* > *Policy Packages* > *HUB* > *Firewall Policy*, and click *+Create New*.
   b. Set the following options, and click *OK*.

| | |
|---|---|
| Name | Custom App Policy |
| Incoming Interface | LAN |
| Outgoing Interface | HUB1 |
| Pv4 Source Address | Branch network |

| | |
|---|---|
| Pv4 Destination Address | Datacenter LAN1 |
| Service | CustomApp-5000 |
| Action | Accept |
| Advanced Options | fec enabled |

c. Move this policy under the *SLA-HealthCheck* policy.

2. Create a policy for the branches policy package:
   a. Go to *Policy & Object* > *Policy Packages* > *Branches* > *Firewall Policy* and click +*Create New*.
   b. Set the following options, and click *OK*.

| | |
|---|---|
| Name | Custom App Policy |
| Incoming Interface | LAN |
| Outgoing Interface | HUB1 |
| Pv4 Source Address | Branch network |
| Pv4 Destination Address | Datacenter LAN1 |
| Service | CustomApp-5000 |
| Action | Accept |
| Advanced Options | fec enabled |

   c. Move this policy under the *Direct Internet Access* policy.
3. Install both HUB and Branch policy packages.

# SD-WAN self-healing with BGP

This example demonstrates a scalable configuration using options that help simplify head-end traffic-steering in an SD-WAN setup that uses a hub and spoke topology. In this example, the hub and branches have basic configurations, with one set of SD-WAN rules on the hub to cover all branch instances.

The hub does not need to reference branch addresses in the SD-WAN rules to steer traffic to each branch over the healthy VPN overlay. It also does not need to run health checks to the branches to determine what paths are healthy. Instead, the branches configure health checks to monitor the links, and use BGP and BGP communities to satisfy both requirements by updating the hub with the status of the links over BGP. This avoids manual maintaining health checks from the head-end, allowing for better scalability.

This section contains the following topics:

- Branch BGP signaling on page 35
- Hub BGP signaling on page 38

## Branch BGP signaling

Following is a summary of enabling route steering on branch devices:

1. Edit BGP neighbors to define an access list for the branch LAN, define route maps that use the access list, and edit the BGP neighbors to send the route maps. See Editing BGP neighbors on page 36.

2. Edit SD-WAN templates to define the conditions for when each route map is sen. See Editing SD-WAN templates on page 37.
3. Install the device settings to the branch and hub devices.

## Editing BGP neighbors

Edit the BGP neighbors to:

- Define an access list for the branch LAN.
- Define two (2) route maps using this access list, which adjusts the BGP community sent.
- Edit the BGP neighbors to send these route maps.

To edit the BGP neighbor:

1. Go to *Device Manager > Provisioning Templates > BGP Templates*, and double-click the *ACME SD-WAN Overlay_branch_bgp* template to open it for editing.
2. Edit the neighbor that corresponds to the hub device's VPN1 interface:
   - **a.** Double-click the neighbor. The *Edit Neighbor* pane is displayed.
   - **b.** Beside *Route Map Out Preferable*, click the dropdown menu, and click +. The *Create New Route Map* pane is displayed.
   - **c.** Set the following options:

| Name | Primary |
|---|---|
| ID | 1 |
| Rules | 1. Click *Create New*. The *Create New Route Map Rule* pane is displayed.<br>2. Toggle on *Match IP address*.<br>3. Click the dropdown box, and click + > *Access List*. The *Create New Access List* pane is displayed.<br>4. Set *Name* to *LAN1*.<br>5. Under *Rules*, click *Create New*. The *Create New Access List Rule* pane is displayed.<br>6. Set *Type* to *Prefix*.<br>7. Set *Prefix* to *Specify*, and enter the desired subnet LAN, for example, *10.1.1.0/24*. Repeat this step for any additional LANs.<br>8. Click *OK* to save the access rule.<br>9. Click *OK* to save the access list. The *Create New Route Map Rule* pane is displayed.<br>10. In the *Match IP address* list, select the access list.<br>11. Click *OK* to save the route map rule. |

   - **d.** Click *OK* to save the route map.
   - **e.** In the *Route Map Out Preferable*, select the *Primary* route map.
   - **f.** Under *IPv4 Filtering*, enable *Route Map Out*.
   - **g.** Click the dropdown list, and click +. The *Create New Route Map* pane is displayed.
   - **h.** Set the following options:

| Name | Out-Of-SLA |
|---|---|
| Rules | 1. Click *Create New*. The *Create New Route Map Rule* pane is displayed. |

| | |
|---|---|
| | 2. Set ID to 1.<br>3. Toggle on *Match IP address*.<br>4. Click the dropdown box, select *LAN1*.<br>5. Enable *Set Community*, and enter *65000:1*.<br>6. Click *OK* to save the route map rule. |

   i. Click *OK* to save the route map.
   j. Set *Route Map Out* to *Out-of-SLA*.
   k. Click *OK* to save the HUB's VPN1 interface neighbor.

3. Edit the second neighbor that corresponds to HUB VPN2 interface:
   a. Double-click the neighbor. The *Edit Neighbor* pane is displayed.
   b. Beside *Route Map Out Preferable*, click the dropdown menu, and click +. The *Create New Route Map* pane is displayed.
   c. Set the following options:

| Name | Secondary |
|---|---|
| ID | 1 |
| Rules | 1. Click *Create New*. The *Create New Route Map Rule* pane is displayed.<br>2. Set *ID* to *1*.<br>3. Set *Match IP address* to *LAN1*.<br>4. Enable *Community*, and enter *65000:2*.<br>5. Click *OK* to save the route map rule. |

   d. Click *OK* to save the route map.
   e. Set *Route Map Out* to *Out-of-SLA*.
   f. Click *OK* to save the HUB's VPN2 interface neighbor.

4. Click *OK* to save the BGP template.

## Editing SD-WAN templates

Edit the SD-WAN neighbor to define the conditions for when each route map is sent.

To edit the SD-WAN template:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
2. Double-click the *Branches* template to open it for editing.
3. Under *Neighbor*, create a new neighbor for HUB’s VPN1:
   a. Click *+Create New*. The *Create New SD-WAN Neighbor* pane is displayed.
   b. Set the following options, and click *OK*:

| IP | Specify the IP address of the HUB’s VPN1 interface |
|---|---|
| Interface Member | HUB1-VPN1 |
| Performance SLA | HUB1_HC |
| SLA | 1 |
| Role | Standalone |

4. Under *Neighbor*, create a new neighbor for HUB's VPN2:
   a. Click *+Create New*. The *Create New SD-WAN Neighbor* pane is displayed.
   b. Set the following options, and click *OK*:

| | |
|---|---|
| IP | Specify the IP address of the HUB's VPN2 interface |
| Interface Member | HUB1-VPN1 |
| Performance SLA | HUB1_HC |
| SLA | 1 |
| Role | Standalone |

5. Click *OK* to save the template.
6. Install the device settings to the branch and hub devices.

## Hub BGP signaling

Enabling BGP route steering on the HUB is comprised of the following steps:

1. Edit the BGP template to edit neighbor groups *VPN1* and *VPN2* to create a new *Route Map In* with new rules for each neighbor group. See Editing the BGP template on page 38.
2. Edit the SD-WAN template to define which VPN is used based on the received tags. See Editing the SD-WAN template on page 40.
3. Install the device settings to the branch and hub devices.

### Editing the BGP template

Edit the BGP template to edit neighbor groups *VPN1* and *VPN2* to create a new *Route Map In* with new rules for each neighbor group. The process:

- Defines router community lists for each of the three (3) communities that may be sent.
- Defining a *Route Map In* for each VPN to set route tags.

To define router community lists:

1. Go to *Device Manager > Provisioning Templates > BGP Templates*.
2. Double-click the *ACME SD-WAN Overlay_hub1_bgp* template to open it for editing.
3. Edit the neighbor group named *VPN1* to create a new *Route Map In* with new rules:
   a. In the *Neighbor Group* section, double-click the *VPN1* group to open it for editing. The *Edit Neighbor Group* pane is displayed.
   b. Under *IPv4 Filtering*, enable *Route Map In*.
   c. Beside *Route Map In*, click the dropdown box, and click +. The *Create New Route Map* pane is displayed.
   d. In the *Name* box, type *VPN1-RouteMap_IN*.
   e. Create a new rule:
      i. Under *Rules*, click *Create New*. The *Create New Route Map Rule* pane is displayed
      ii. Set the following options:

| | |
|---|---|
| ID | 3 |
| Match Community | 1. Toggle on. |

| | |
|---|---|
| | **2.** Click the dropdown, and click +. The *Create New Community List* pane is displayed.<br>**3.** Set *Name* to *65000:1*.<br>**4.** Under *Rules*, click *Create New*. The *Community List Rule Edit* pane is displayed.<br>**5.** Set *ID* to *1*.<br>**6.** Set *Match* to *65000:1*, and click *OK* to save the rule.<br>**7.** Click *OK* to save the community list.<br>**8.** Select the newly created rule named *65000:1* for *Match Community*. |
| Set route tag | 1 |

**iii.** Click *OK* to save the route map rule.

**f.** Create another new rule:

**i.** Under *Rules*, click *Create New*. The *Create New Route Map Rule* pane is displayed

**ii.** Set the following options:

| | |
|---|---|
| ID | 4 |
| Match Community | **1.** Toggle on.<br>**2.** Click the dropdown, and click +. The *Create New Community List* pane is displayed.<br>**3.** Set *Name* to *65000:2*.<br>**4.** Under *Rules*, click *Create New*. The *Community List Rule Edit* pane is displayed.<br>**5.** Set *ID* to *1*.<br>**6.** Set *Match* to *65000:2*, and click *OK* to save the rule.<br>**7.** Click *OK* to save the community list.<br>**8.** Select the newly created rule named *65000:2* for *Match Community*. |
| Set route tag | 2 |

**iii.** Click *OK* to save the route map rule.

**g.** Create a third new rule:

**i.** Under *Rules*, click *Create New*. The *Create New Route Map Rule* pane is displayed

**ii.** Set the following options:

| | |
|---|---|
| ID | 5 |
| Match Community | **1.** Toggle on.<br>**2.** Click the dropdown, and click +. The *Create New Community List* pane is displayed.<br>**3.** Set *Name* to *65000:5*.<br>**4.** Under *Rules*, click *Create New*. The *Community List Rule Edit* pane is displayed.<br>**5.** Set *ID* to *1*.<br>**6.** Set *Match* to *65000:5*, and click *OK* to save the rule.<br>**7.** Click *OK* to save the community list.<br>**8.** Select the newly created rule named *65000:5* for *Match Community*. |
| Set route tag | 5 |

iii. Click *OK* to save the route map rule.

h. Click *OK* to save the route map. The *Edit Neighbor Group* pane is displayed.

4. For *Route Map In*, select the newly created *VPN1-RouteMap_IN*, and click *OK*.
5. Repeat this procedure for *VPN2*, replacing the *Route Map In* name with *VPN2-RouteMap_IN*.
   You can select the previously created communities when creating the three (3) rules for *VPN2*.
6. Click *OK* to save the BGP template.

### Editing the SD-WAN template

Edit the SD-WAN template to define which VPN is used based on the received tags.

To edit the SD-WAN template:

1. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
2. Double-click the *Hub_SDWAN* template to open it for editing.
3. Under *SD-WAN Rules*, define a new rule:
   a. Click *+Create New*. The *Create New SD-WAN Rule* pane is displayed.
   b. Set the following options, and click *OK*:

| Name | ToBranches_VPN1 |
|---|---|
| Source Address | all |
| Route Tag | 1 |
| Interface Preference | VPN1 |

4. Under *SD-WAN Rules*, define a second rule:
   a. Click *+Create New*. The *Create New SD-WAN Rule* pane is displayed.
   b. Set the following options, and click *OK*:

| Name | ToBranches_VPN2 |
|---|---|
| Source Address | all |
| Route Tag | 2 |
| Interface Preference | VPN2 |

5. Click *OK* to save the template.
6. Install the device settings to the branch and hub devices.

## SaaS remote internet breakout

You can use this configuration to enable SaaS remote internet breakout on the branch devices. This allows branch devices to access cloud applications through the hub device. The spoke device routes only Ringcentral VoIP traffic through hub overlays. The SD-WAN rule is set to *set gateway enable* to override the route table and send traffic that matches this application through the hub.

Following is a summary of configuring SaaS remote internet breakout:

1. Create an SD-WAN rule for cloud applications. See Creating an SD-WAN rule for cloud applications on page 41.

2. Create a policy to allow traffic on the hub. See Creating a policy to allow traffic on the hub on page 41.

## Creating an SD-WAN rule for cloud applications

To create an SD-WAN rule:

1. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
2. Double-click the *Branches* template to open it for editing.
3. Under *SD-WAN Rules*, click +*Create New*. The *Create New SD-WAN Rule* pane is displayed.
4. Complete the following options, and click *OK* to save the new rule:

| | |
|---|---|
| Name | Cloud Applications |
| Destination | 1. Select *Internet Service*.<br>2. Click the box beside *Application Group*, and click + to create a new application group.<br>3. Set *Name* to *Cloud_Applications*.<br>4. Set *Application* to *Ringcentral (ID: 42635)*.<br>5. Click OK to save the application group. |
| Strategy | Lowest Cost (SLA) |
| Interface Preference | HUB1-VPN1, HUB1-VPN2 |
| Required SLA Target | Hub1_HC |
| Advanced Options | Enable *gateway*. |

5. Move the rule to the position two (2) below *Corporate_Traffic*.
6. Click *OK* to save the SD-WAN template.

## Creating a policy to allow traffic on the hub

To create a policy to allow traffic on the hub device:

1. Go to *Policy & Objects*.
2. Select the *HUB* policy package, and click +*Create New* to define a new policy.
3. Set the following options, and click *OK*:

| | |
|---|---|
| Name | Remote Internet Breakout |
| Incoming Interface | Branches |
| Outgoing Interface | WAN1, WAN2 |
| IPv4 Source Address | Branch network |
| IPv4 Destination Address | all |
| Action | Accept |
| NAT | Enabled |

4. Install the branch and hub policy packages.

# Appendix A - Products used

The following product models and firmware were used in this guide:

| Product | Model | Firmware |
|---|---|---|
| FortiOS | All models supported by FortiManager | 7.2.0 and later |
| FortiManager | All models | 7.2.0 and later |

# Appendix B - Documentation references

Feature documentation:

- Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide

Solution hub:

- Secure SD-WAN

# Appendix C - Troubleshooting

The following debug commands can be used to troubleshoot SD-WAN issues:

| Command | Description |
|---|---|
| diag vpn ike gateway list | Confirm IPsec is up |
| get router info bpg summary | Confirm BGP is up and exchanging routes |
| diagnose sys sdwan health-check status HUB1_HC | Confirm hub device is reachable through SLA |

www.fortinet.com

01-720-802312-20221103