



Multiple Datacenter (Primary/Secondary) Deployment for Enterprise

Secure SD-WAN



DEFINE / DESIGN / **DEPLOY** / DEMO



Table of Contents

Change Log	4
Introduction	5
Audience	6
About this guide	6
Deployment objectives	6
Solution overview	7
Design overview	8
Use case and topology	8
Product prerequisites	8
Deployment procedures	9
Prerequisites	9
Planning	9
Assumptions	10
Configuration steps	10
Create Branches device group and add two FortiGates to the group	10
Creating an SD-WAN Overlay template	11
Configuring SD-WAN rules	17
Creating policy packages and firewall policies	27
Installing policy packages	33
Verifying the SD-WAN configuration	36
Extensions	39
ADVPN	39
Enabling ADVPN	39
Editing branch SD-WAN template	40
Editing branch policy package	40
Install the policy packages to both Branches and Hub	40
Verifying the ADVPN configuration	41
Adaptive FEC	42
Defining a custom service	42
Defining FEC mappings	42

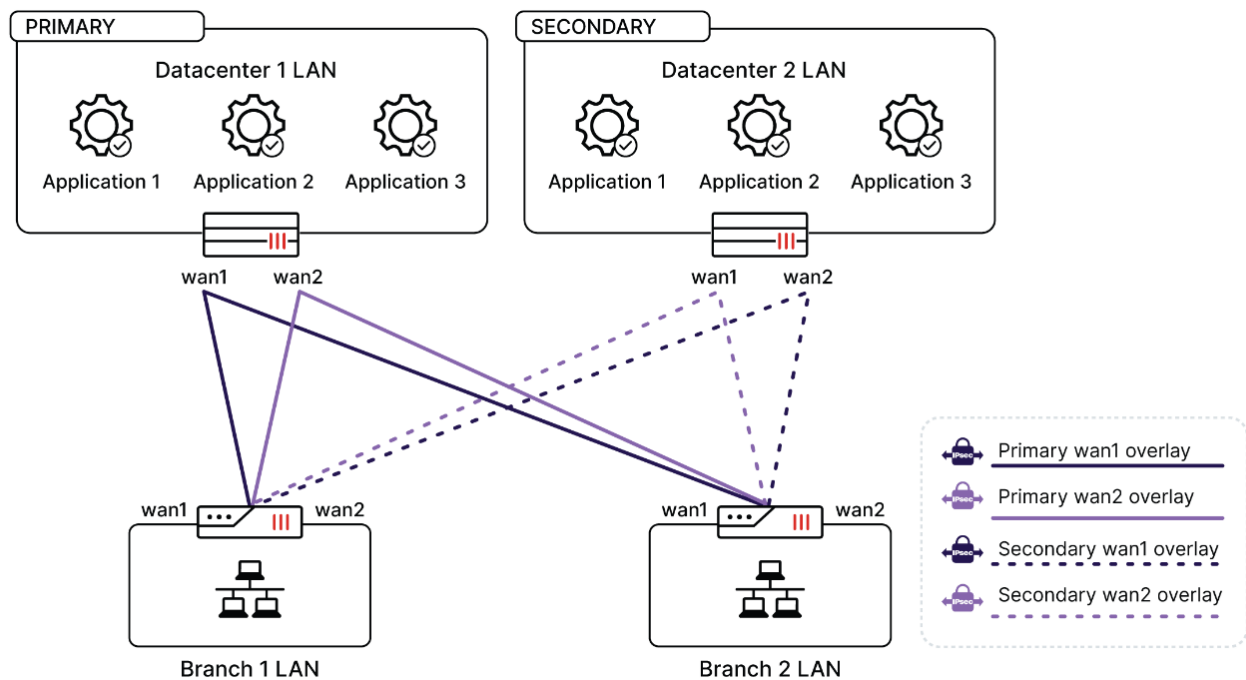
Enabling FEC for hub devices	43
Enabling FEC on branch devices	44
Creating policies and installing policy packages	44
Appendix A - Products used	46
Appendix B - Documentation references	47
Appendix C - Troubleshooting	48

Change Log

Date	Change Description
2025-04-25	Initial release.

Introduction

This deployment example utilizes the [multiple datacenter \(primary-secondary gateway\) architecture](#) discussed in the [SD-WAN Architecture for Enterprise](#) guide to provide a deployment example of SD-WAN for a dual hub topology.



The steps included in this guide provide a working configuration comprised of the following components:

- SD-WAN dual hub - primary & secondary
 - BGP configuration
 - IPSec overlay
 - SD-WAN rules, Performance SLAs, SD-WAN zones
 - Firewall Policies
- Extensions
 - ADVPN
 - FEC

This section contains the following topics:

- Audience on page 6
- About this guide on page 6
- Deployment objectives on page 6

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

The architecture, components and technology referenced in this document is covered in the [Multiple datacenter \(primary/secondary gateway\)](#) 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 guide utilizes FortiManager 7.4.6 and FortiOS 7.4.7 for all configuration examples. When selecting a firmware to use in your deployment, it is important to reference the FortiManager and FortiOS Release Notes.

Furthermore, both the FortiManager and FortiGates are KVM virtual machines. This is reflected in some of the steps, particularly when normalizing interfaces within FortiManager. This must be adjusted to reflect your given hardware or software platforms.

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.

Deployment objectives

- Greenfield deployment of new Fortinet Secure SD-WAN devices.
- The hub FortiGates are located in a private locations (such as an HQ location, datacenter, or cloud).
- The hubs will provide secure access to remote branch locations that require connectivity to local application and services.
- Each branch WAN interface has a VPN connection to each of the HUB WAN interfaces (SD-WAN Overlay, 4 connections per branch).
- SD-WAN rules steer traffic across links.
- Performance SLAs are used to evaluate links for specific application performance requirements.
- BGP routing is used to facilitate communication.

Solution overview

This guide is separated into the following parts:

SD-WAN overlay template creates the following templates:

- BGP templates
- SD-WAN template
- IPsec Tunnel templates
- Template Groups

Policy Packages:

- Firewall policies for HUB and Branch devices

Deploy the configuration to the FortiGates:

- Install both the policy package and template configurations

Review and verify the configuration:

- Generate traffic and utilize monitors to verify tunnels, traffic, review rules

Apply Extensions



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 39](#), 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.

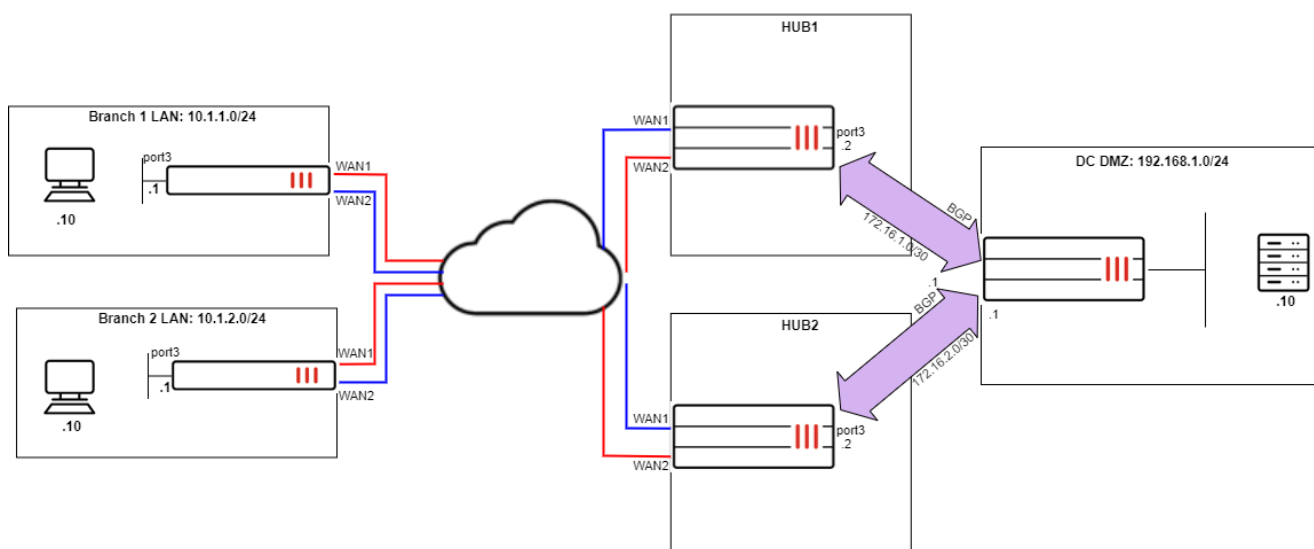
The following sections help describe the solution design:

- [Use case and topology on page 8](#)
- [Product prerequisites on page 8](#)

Use case and topology

This topology is used to demonstrate the deployment of SD-WAN dual hub (Primary/Secondary). As there are several ways to deploy SD-WAN dual hub, the goal of this topology is to provide context to some of the configuration that follows. Specifically, address objects (LAN, Branch, DataCenter) and port usage.

This topology may be expanded to include other design features, such as ADVPN. See [Extensions on page 39](#) for details.



Product prerequisites

- Hub 1 FortiGate 7.4.7 with dual WAN connections
- Hub 2 FortiGate 7.4.7 with dual WAN connections
- Branch FortiGate 7.4.7 with dual WAN connections
- FortiManager 7.4.6

Deployment procedures

The following deployment procedures provide assumptions, prerequisites, and steps to configure SD-WAN for a dual hub (Primary / Secondary) topology. The deployment procedures include the following topics:

- [Prerequisites on page 9](#)
- [Planning on page 9](#)
- [Assumptions on page 10](#)
- [Configuration steps on page 10](#)

Prerequisites

This guide presumes the following prerequisites have been met:

- Two Hub and two branch FortiGates have been imported into FortiManager.
- The Hub and branch devices have active connections to FortiManager.

Device Name	Config Status	Host Name	IP Address	Platform	Firmware Version	Policy Package Status	Firmware Template	Provisioning Templates
Br1	✓ Auto-update	Br1	192.168.100.103	FortiGate-VM64-KVM	FortiGate 7.4.7, build 2731 (GA) (Mature)	▲ Never Installed		
Br2	✓ Auto-update	Br2	192.168.100.104	FortiGate-VM64-KVM	FortiGate 7.4.7, build 2731 (GA) (Mature)	▲ Never Installed		
HUB1	✓ Auto-update	HUB1	192.168.100.101	FortiGate-VM64-KVM	FortiGate 7.4.7, build 2731 (GA) (Mature)	▲ Never Installed		
HUB2	✓ Auto-update	HUB2	192.168.100.102	FortiGate-VM64-KVM	FortiGate 7.4.7, build 2731 (GA) (Mature)	▲ Never Installed		

- Each 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.
- 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.

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:

1. Corporate datacenter LAN is 192.168.1.0/24.
2. Branch LAN is 10.1.<branch#>.0/24.
3. HUB1 is located at the primary corporate location.
4. HUB2 is located at the backup corporate location.
5. ISP1 is connected to port1 on all FortiGates.
6. ISP2 is connected to port2 on all FortiGates.
7. LAN is connected to port3 on all FortiGates.
8. SD-WAN rules should use the link with the best quality for traffic.

Configuration steps

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

1. Create a Branches device group and add two FortiGates to the group.
2. Create an SD-WAN Overlay template. See [Creating an SD-WAN Overlay template on page 11](#).



It is no longer required to assign and configure metadata values to branch devices.

-
3. Configure SD-WAN rules. See [Configuring SD-WAN rules on page 17](#).



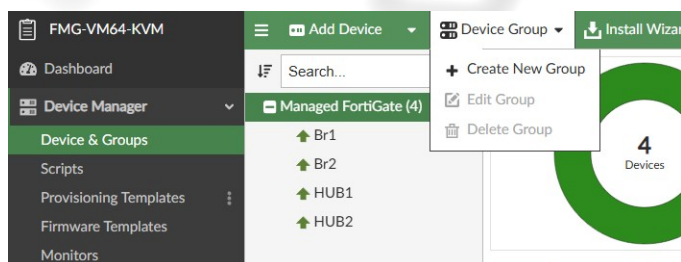
The overlay template now has the capability to create normalized interfaces for branch and HUB devices.

-
4. Create policy packages and firewall policies. See [Creating policy packages and firewall policies on page 27](#).
 5. Install policy packages to devices. See [Installing policy packages on page 33](#).
 6. Verify the SD-WAN configuration. See [Verifying the SD-WAN configuration on page 36](#).
 7. Review and apply Extensions as desired. See [Extensions on page 39](#).

Create Branches device group and add two FortiGates to the group

Create device groups to apply SD-WAN configuration to several devices at once.

1. On FortiManager, select *Device & Groups*, then select *Device Group* from the top menu bar to see a dropdown. From this dropdown, select *Create New Group*.



- In the *Create New Device Group* popup menu, provide the name *Branches*, then use the *Add Member* button to select *Br1* and *Br2*.

Device Name	Type	Platform	IP	Firmware Version
Br1	Device	FortiGate-VM64-...	192.168.100.103	FortiGate 7.4.7,build2731 (GA)
Br2	Device	FortiGate-VM64-...	192.168.100.104	FortiGate 7.4.7,build2731 (GA)

- Click *OK* to save.

Creating an SD-WAN Overlay template

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

To create an SD-WAN Overlay template:

- In FortiManager, go to *Device Manager > Provisioning Templates > SD-WAN Overlay*.



You may have to enable SD-WAN Overlay visibility. Select Feature Visibility in the top menu bar to enable this.

- Click *Create New*. The *Create New SD-WAN Overlay Template - Region Settings (1/5)* dialog box is displayed.
- Set the region settings:

- a. Enter a name and description for the template.
- b. Select *Dual Hub (Primary & Secondary)*.

- c. Click *Next*. The *Role Assignment* pane is displayed.
4. Set the role assignment:
 - a. Set *Primary HUB* to *HUB1*.
 - b. Set *Secondary HUB* to *HUB2*.
 - c. Set *Device Group Assignment* to *Branches*.
 - d. Enable *Automatic Branch ID Assignment*.



Enabling automatic branch ID assignment assigns each device in the Branches group a unique *branch_id* value. Previously this value was manually configured and is used by several provisioning templates that the SD-WAN overlay template generates.

Review the branches BGP template, branches CLI template, and branches IPsec templates to see the *branch_id* variable in use.

- e. Click *Next*. The *Network Configuration* pane is displayed.
5. Set the network configuration for the HUBs:
 - a. In the HUB section under Primary HUB, set:
 - i. *WAN Underlay 1* to *port1*.
 - ii. *WAN Underlay 2* to *port2*.
 - iii. Expand *Advanced* to configure the BGP peering between HUB1 and the Datacenter.

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

Name: Primary_secondary_dual_hub

HUB

Primary HUB

Underlay

#	Private Link	Override IP	Action
WAN Underlay 1	<input type="radio"/> port1	<input type="radio"/>	<input type="button" value="x"/> <input type="button" value="+"/>
WAN Underlay 2	<input type="radio"/> port2	<input type="radio"/>	<input type="button" value="x"/> <input type="button" value="+"/>

Network Advertisement

☒ Connected ☐ Static

#	Interface	Action
<input type="button" value="+"/>		

Advanced ▾

Neighbors

Search...

<input type="checkbox"/>	#	Neighbor IP	Remote AS	Route Map in	Route Map Out	<input type="button" value="Settings"/>
No record found.						

0

- iv. Under *Neighbors*, click *Create New*. The *Create New Neighbor* pane is displayed.
- v. Set *Neighbor IP* to 172.16.1.1.
- vi. Set *Remote AS* to 65100.
- vii. Click *OK*. The BGP neighbor is created.

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

Name: Primary_secondary_dual_hub

HUB

Primary HUB

Underlay

#	Private Link	Override IP	Action
WAN Underlay 1	<input checked="" type="radio"/> port1	<input type="radio"/>	<input type="button" value="x"/> <input type="button" value="+"/>
WAN Underlay 2	<input type="radio"/> port2	<input type="radio"/>	<input type="button" value="x"/> <input type="button" value="+"/>

Network Advertisement

☒ Connected ☐ Static

#	Interface	Action
<input type="button" value="+"/>		

Advanced ▾

Neighbors

Search...

<input type="checkbox"/>	#	Neighbor IP	Remote AS	Route Map in	Route Map Out	<input type="button" value="Settings"/>
<input type="checkbox"/>		172.16.1.1	65100			

1

- b. In the HUB section under Secondary HUB, set:
 - i. WAN Underlay 1 to port1.
 - ii. WAN Underlay 2 to port2.

- iii. Expand *Advanced* to configure the BGP peering between HUB2 and the Datacenter.

The screenshot shows the configuration page for a device named 'HUB2'. The 'Advanced' section is expanded, and the 'Neighbors' tab is selected. The 'Neighbors' table is currently empty, with a message 'No record found.' and a '0' at the bottom right. The 'Create New' button is visible in the top left of the 'Neighbors' section.

- iv. Under *Neighbors*, click *Create New*. The *Create New Neighbor* pane is displayed.
v. Set *Neighbor IP* to 172.16.2.1.
vi. Set *Remote AS* to 65100.
vii. Click *OK*. The BGP neighbor is created.

The screenshot shows the configuration page for a device named 'HUB2'. The 'Advanced' section is expanded, and the 'Neighbors' tab is selected. The 'Neighbors' table now contains one record with the following details:

#	Neighbor IP	Remote AS	Route Map in	Route Map Out
	172.16.2.1	65100		

The 'Create New' button is still visible in the top left of the 'Neighbors' section.

6. Set the network configuration for the branches device group:
a. Scroll down to the *Branch* section, and set *WAN Underlay 1* to *port1*.
b. Set *WAN Underlay 2* to *port2*.
c. Set *Network Advertisement* on *Connected* and click the + icon to specify *port3*.

CONFIGURATION STEPS



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.
7. 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. Click **OK** to save the empty SD-WAN template. Select the newly created SD-WAN template from the dropdown.
 - d. Enable *Add Overlay Interfaces and Zones*.
 - e. Enable *Add Healthcheck Servers for Each Hub as Performance SLA*.
 - f. Enable *Normalize Interfaces*.
 - g. Enable the newly displayed *Add Health Check Firewall Policy to Hub Policy Package*.
 - h. In the list, click the **+** icon to create a new hub policy package named *Hub*.

- i. Click **OK** to save the empty policy package, and select the new policy package in the dropdown.
- j. Enable *Add Health Check Firewall Policy to Branch Policy Package*.
- k. In the list, click the **+** icon to create a new branches policy package named *Branches*.
- l. Click **OK** to save the empty policy package, and select the new policy package in the dropdown.

m. 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

Primary_secondary_dual_hub

Topology

Dual HUB (Primary & Secondary)

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

Primary HUB

↑ HUB1 [root] (192.168.100.101, Platform: Forti...)

Secondary HUB

↑ HUB2 [root] (192.168.100.102, Platform: Forti...)

Branch

🏠 Branches

Underlay Assignment

Primary HUB Underlays

Underlay 1: port1
Underlay 2: port2

Secondary HUB Underlays

Underlay 1: port1
Underlay 2: port2

Branch Underlays

Underlay 1: port1
Underlay 2: port2

Network Advertisement

Primary HUB

Connected
Interface: None

Secondary HUB

Connected
Interface: None

Branch

Connected
Interface 1: port3

SD-WAN Template Options

Add Overlay Objects to SD-WAN Template

☒ Branch_SDWAN

Add Overlay Interfaces and Zones

☒

Add Health Check Servers for Each HUB as Performance SLA

☐

Normalize Interfaces

☒

Add Health Check Firewall Policy to Hub Policy Package

☒ Hub

Add Health Check Firewall Policy to Branch Policy Package

☒ Branches

8. Click *Finish* to save the template.

The SD-WAN Overlay template generates four other templates which can be seen using the top menu bar from *Device Manager > Provisioning Templates*. These templates are collected into Template Groups for HUB1, HUB2, and Branch devices.

- IPsec Tunnel template
 - Primary_secondary_dual_hub_BRANCH_IPsec
 - Primary_secondary_dual_hub_HUB1_IPsec
 - Primary_secondary_dual_hub_HUB2_IPsec
- SD-WAN template
 - Branch_SDWAN
- CLI template (and CLI template groups)
 - Primary_secondary_dual_hub_BRANCH_CLI(GRP)
 - Primary_secondary_dual_hub_HUB1_CLI(GRP)

CONFIGURATION STEPS

- Primary_secondary_dual_hub_HUB2_CLI(GRP)
- BGP template*
 - Primary_secondary_dual_hub_BRANCH_BGP
 - Primary_secondary_dual_hub_HUB1_BGP
 - Primary_secondary_dual_hub_HUB2_BGP



You may have to enable visibility of this template by selecting *Feature Visibility* and enabling *BGP*.

Configuring SD-WAN rules

In this section we are going to edit the Branch_SDWAN SD-WAN template that was created in the previous section to create performance SLA targets and SD-WAN rules. In this example, WAN1 is the faster and preferred link. WAN2 is the less expensive broadband link. The business requirements are to steer business critical applications through the best connection, and all other public traffic through WAN2.

Rule #	Traffic Type	Steering Strategy	Expected Interface/Zone
1	SalesForce, Microsoft.Teams, Dropbox	Best Quality (Latency)	WAN1, WAN2
2	Zoom, GoToMeeting, YouTube	Best Quality (Latency)	WAN1, WAN2
3	Corporate Traffic	Lowest cost (SLA)	HUB1-VPN1 HUB1-VPN2 HUB2_VPN1 HUB2_VPN2
4	All other public internet traffic	Manual	WAN2

To begin configuring the above rules, navigate to *Device Manager > Provisioning Templates > SD-WAN* from the top menu bar. Then edit the *Branch_SDWAN* template.

Following is a summary of how to configure the performance SLA targets and SD-WAN rules:

1. [Create rule: Corporate_Traffic on page 18](#)
2. [Define two performance SLAs for further rules on page 19](#)
3. [Create rule: Internet_Traffic on page 22](#)
4. [Create rule: Critical_Video on page 23](#)
5. [Create rule: Critical_DIA on page 25](#)
6. [Adjust SD-WAN rule order on page 26](#)

Create rule: Corporate_Traffic

To create rule: Corporate_Traffic

1. Under *SD-WAN Rules*, click *Create New*. The *Create New SD-WAN Rule* pane opens.
2. Set the following options:

Name	Corporate_Traffic
Source	Branch-LAN, 10.1.0.0/16 (Create new Address Object)*
Destination	Datacenter-LAN1, 192.168.1.0/24 (Create new Address Object)*
Strategy	Lowest cost (SLA)
Interface Preference	HUB1_VPN1, HUB1_VPN2, HUB2_VPN1, HUB2_VPN2
Required SLA target	HUB1_HC, HUB2_HC

* These address objects are created inline by selecting the address bar dropdown, then the + icon in the *top right > Firewall Address*. Set the *Name* and *IP/Netmask*, then click *OK* to save.

Create New SD-WAN Rule

Click to select

1 entry selected

User Group

Click to select

Destination

Address

Q

Datacenter-LAN1

IP/Netmask: 192.168.1.0/255.255.255.0

Click to select

1 entry selected

Protocol

TCP UDP Any Specify

0

Internet Service

Click to select

Application

Click to select

Outgoing Interfaces

Strategy

Lowest Cost (SLA)

Interface Preference

+

HUB1-VPN1

HUB1-VPN2

HUB2-VPN1

HUB2-VPN2

Zone Preference

+

Measured SLA

Click to select

Required SLA Target

+

HUB1_HC#1

Ping: 172.16.255.253 ; Latency: 255ms, Jitter: 55ms, Packet Loss: 1%

HUB2_HC#1

Ping: 172.16.255.252 ; Latency: 255ms, Jitter: 55ms, Packet Loss: 1%

Quality Criteria

Latency

Forward DSCP

Reverse DSCP

Agent Exclusive

Advanced Options

OK

Cancel

3. Click OK to save the rule.



The *Corporate_Traffic* rule was created first because it uses a performance SLA that was defined in the SD-WAN Overlay template.

Define two performance SLAs for further rules

To define two performance SLAs for further rules:

1. Under *Performance SLA*, use the checkbox to select and then delete the following default performance SLAs:
 - a. Default_AWS
 - b. Default_DNS
 - c. Default_FortiGuard
 - d. Default_Gmail

CONFIGURATION STEPS

- e. Default_Google Search
- f. Default Office_365
2. Under *Performance SLA*, click *Create New*. The *Create New Performance SLA* pane opens.
3. Set the following options:

Name	Internet
Server	1.1.1.1
Participants	Specify: port1, port2
SLA Targets	<i>Latency threshold: 300</i> <i>Jitter Threshold: 55</i> <i>Packet Loss Threshold: 3%</i>
Update Static Route	Disable
Cascade Interfaces	Disable

Create New Performance SLA

Name

Internet

IP Version

IPv4 IPv6

Probe Mode

Active

Enable Probe Packets

☒

Protocol

Ping

Server

1.1.1.1

Participants

All SD-WAN Members Specify

port1

port2

2 entries selected

Embedded Measure Health

☐

Redistribute SLA ID

0 (0 - 32)

Installation Target

Click to select

SLA Target

Link Cost Fac...	Latency Thre...	Jitter Thresh...	Packet Loss ...	Mos Threshold	Priority IN-S...	Priority OUT...	Action
<input checked="" type="checkbox"/> Auto	<input checked="" type="checkbox"/> 300 ms	<input checked="" type="checkbox"/> 55 ms	<input checked="" type="checkbox"/> 3 %	<input type="checkbox"/>	0	0	<input checked="" type="checkbox"/> <input type="checkbox"/>

4. Click *OK* to save the performance SLA.
5. Under *Performance SLA*, click *Create New*. The *Create New Performance SLA* pane opens.
6. Set the following options to define a second performance SLA:

Name	Prefer_Passive
Probe Mode	Prefer Passive
Server	8.8.8.8
Participants	Specify: port1, port2
SLA Targets	<i>Latency threshold: 180</i> <i>Jitter Threshold: 45</i> <i>Packet Loss Threshold: 1%</i>

CONFIGURATION STEPS

Update Static Route

Disable

Cascade Interfaces

Disable



Prefer passive is used to demonstrate an additional option for SD-WAN performance SLAs. When probe mode is set to passive, health is measured using live traffic passing through an SD-WAN link to determine link metrics (jitter, latency, and packet loss) of participating SD-WAN links. Prefer passive allows the FortiGate to send probes when there is no live traffic to measure. See [Passive WAN health measurement](#) for more details.

Note: To utilize passive health measurement, one or more firewall policies must have Passive Health Check (`passive-wan-health-measurement`) enabled.

Create New Performance SLA

Name

Prefer_Passive

IP Version

IPv4 IPv6

Probe Mode

Prefer Passive

Enable Probe Packets

☒

Protocol

Ping

Server

8.8.8.8

Participants

All SD-WAN Members Specify

port1

port2

2 entries selected

Embedded Measure Health

☒

Redistribute SLA ID

0 (0 - 32)

Installation Target

Click to select

SLA Target

Link Cost Factor	Latency Threshold	Jitter Threshold	Packet Loss Thre...	Mos Threshold	Priority IN-SLA	Priority OUT-SLA	Action
<input checked="" type="checkbox"/> Auto	<input checked="" type="checkbox"/> 180 ms	<input checked="" type="checkbox"/> 45 ms	<input checked="" type="checkbox"/> 1 %	<input checked="" type="checkbox"/>	0	0	<input checked="" type="checkbox"/>

Link Status

Check Interval

500

Milliseconds (20 - 3600000)

Failure Before Inactive

5

(1 - 3600)

Restore Link After

5

Check(s) (1 - 3600)

Probe Timeout

500

Milliseconds (20 - 3600000)

Action When Inactive

Update Static Route

☒

Cascade Interfaces

☒

Advanced Options >

OK

Cancel

7. Click OK to save the performance SLA.

Create rule: Internet_Traffic

To create rule: Internet_Traffic

1. Under *SD-WAN Rules*, click *Create New*. The *Create New SD-WAN Rule* pane opens.
2. Set the following options:

Name	Internet_Traffic
Source	Branch-LAN
Destination	RFC-1918*

*This is an address group of the 3 subnets mentioned in RFC-1918. Create the empty address group "RFC-1918" first.

3. Next, create 3 firewall objects and add each to the newly created RFC-1918 group.

Name	Subnet
RFC-1918-10	10.0.0.0/8
RFC-1918-172	172.16.0.0/12
RFC-1918-192	192.168.0.0/16

4. Once the last RFC address object is defined and added to the group, select the group for *Destination > Address*.

Strategy	Manual
Interface Preference	port2
dst-negate	enable**

** This setting is found under *Advanced Options*.

Create New SD-WAN Rule

Source Address

Search:

Branch-LAN
IP/Netmask: 10.1.0.0/255.255.0.0

Click to select 1 entry selected

User Group

Click to select

Destination

Address

Search:

RFC-1918
Group Members (3): RFC1918-10, RFC1918-172, RFC1918-192

Click to select 1 entry selected

Protocol

TCP UDP **Any** Specify

Internet Service

Click to select

Application

Click to select

Outgoing Interfaces

Strategy

Manual

Interface Preference

+
port2

Zone Preference

+
Click to select

Measured SLA

Click to select

Required SLA Target

+
Click to select

Load Balancing

☐

Quality Criteria

Latency

Forward DSCP

☐

Reverse DSCP

☐

Agent Exclusive

☐

Advanced Options

addr-mode

ipv4

bandwidth-weight

default

☐

dst-negate

☒

OK **Cancel**

5. Click *OK* to save the rule.

Create rule: Critical_Video

To create rule: Critical_Video:

1. Under *SD-WAN Rules*, click *Create New*. The *Create New SD-WAN Rule* pane opens.
2. Set the following options:

Name	Critical_Video
Source	Branch-LAN
Destination	Application <ul style="list-style-type: none"> • GoToMeeting • YouTube

CONFIGURATION STEPS

- Zoom

Strategy	Best Quality
Interface Preference	port1, port2
Measured SLA	Prefer_Passive
Quality Criteria	Latency
passive-measurement*	Enable

* This setting is found under Advanced Options.



Recall the *Prefer_Passive* performance SLA defined earlier. The measurements taken from that health check will be used to steer traffic in this rule.

Create New SD-WAN Rule

Name

Critical_Video

Status

☒

IP Version

IPv4 IPv6

Installation Target

Click to select

Source

Source Address

Branch-LAN

IP/Netmask: 10.1.0.0/255.255.0.0

Click to select

1 entry selected

User Group

Click to select

Destination

Address

Click to select

Internet Service

Click to select

Application

GoToMeeting

id: 16354

YouTube

id: 31077

Zoom

id: 37065

Click to select

3 entries selected

Outgoing Interfaces

Strategy

Best Quality

Interface Preference

+

port1

port2

Zone Preference

+

Measured SLA

Prefer_Passive

Ping: 8.8.8.8

Click to select

1 entry selected

Required SLA Target

+

OK

Cancel

3. Click OK to save the rule.

Create rule: Critical_DIA

To create rule: Critical_DIA:

1. Under *SD-WAN Rules*, click *Create New*. The *Create New SD-WAN Rule* pane opens.
2. Set the following options:

Name	Critical_DIA
Source	Branch-LAN
Destination	Application <ul style="list-style-type: none">• Dropbox• Microsoft.Teams• Salesforce
Strategy	Best Quality
Interface Preference	port1, port2
Measured SLA	Internet
Quality Criteria	Latency

Create New SD-WAN Rule

Name

Critical_DIA

Status

☒

IP Version

☒ IPv4
 ☐ IPv6

Installation Target

Click to select

Source

Source Address

Branch-LAN

IP/Netmask: 10.1.0.0/255.255.0.0

×

Click to select

1 entry selected

User Group

Click to select

Destination

Address

Click to select

Internet Service

Click to select

Application

Dropbox

id: 17459

×

Microsoft.Teams

id: 43541

×

Salesforce

id: 16920

×

Click to select

3 entries selected

Outgoing Interfaces

Strategy

Best Quality

Interface Preference

+

port1

×

port2

×

Zone Preference

+

Measured SLA

Internet

Ping: 1.1.1.1

×

Click to select

1 entry selected

Required SLA Target

+

OK

Cancel

3. Click **OK** to save the rule.

Adjust SD-WAN rule order

Adjusting the rule order is necessary to ensure traffic is processed by the intended SD-WAN rule. As traffic is matched to rules in a top-down fashion, it is important to have the more narrow rules above the general ones to ensure they are given priority to matching traffic.

To adjust the SD-WAN rule order:

1. Hover over the *Critical_Video* rule within the SD-WAN Template. Use the group of dots on the left most side to reposition the rule above *Corporate Traffic*.

CONFIGURATION STEPS

SD-WAN Rules											
<div> + Create New Edit Delete More </div> <div>Search...</div>											
<input type="checkbox"/>	ID	Name	Source	Destination	Criteria	Members	Performance SLA	Port	Protocol	Status	
<input checked="" type="checkbox"/>	3	Critical_Video	Branch-LAN	YouTube Zoom GoToMeeting	Latency	port1 port2	Prefer_Passive		any	Enable	
<input type="checkbox"/>	1	Corporate_Traffic	Branch-LAN		Latency	HUB1-VPN1 HUB1-VPN2 HUB2-VPN1 HUB2-VPN2	HUB2_HC HUB1_HC		any	Enable	
<input type="checkbox"/>	2	Internet_Traffic	Branch-LAN			port2			any	Enable	
<input type="checkbox"/>	4	Critical_DIA	Branch-LAN	Salesforce Microsoft.Teams Dropbox	Latency	port1 port2	Internet		any	Enable	
<input type="checkbox"/>		sd-wan	All	All	Source IP	All			any		
											5

2. Drag the *Critical_DIA* rule to position 2.

SD-WAN Rules											
<div> + Create New Edit Delete More </div> <div>Search...</div>											
<input type="checkbox"/>	ID	Name	Source	Destination	Criteria	Members	Performance SLA	Port	Protocol	Status	
<input type="checkbox"/>	3	Critical_Video	Branch-LAN	YouTube Zoom GoToMeeting	Latency	port1 port2	Prefer_Passive		any	Enable	
<input type="checkbox"/>	4	Critical_DIA	Branch-LAN	Salesforce Microsoft.Teams Dropbox	Latency	port1 port2	Internet		any	Enable	
<input type="checkbox"/>	1	Corporate_Traffic	Branch-LAN		Latency	HUB1-VPN1 HUB1-VPN2 HUB2-VPN1 HUB2-VPN2	HUB2_HC HUB1_HC		any	Enable	
<input type="checkbox"/>	2	Internet_Traffic	Branch-LAN			port2			any	Enable	
<input type="checkbox"/>		sd-wan	All	All	Source IP	All			any		
											5

3. Click OK to save the SD-WAN template.



Question: Why is the SD-WAN template not assigned to the *Branches* group?

The SD-WAN Overlay template utilizes a template group to assign an IPsec, BGP, SD-WAN template, and CLI template to the *Branches* group.

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. Configure interface mapping for LAN. See [Configure interface mapping for LAN on page 28](#).
2. Create a policy package for branch devices. See [Configure the branch policy package and policies on page](#)

29.

3. Create a policy package for the hub device. See [Configuring the Hub policy package and policies on page 31](#).

Configure interface mapping for LAN

Start by creating an interface mapping to map 'port3' to LAN. While you can use port3 in policies, creating this mapping makes the policy purpose more transparent. It also allows for different interfaces to be referenced as LAN. For example, maybe one branch location needs to use port5 as their LAN connection. This can be explicitly mapped for that branch and still utilize the branch policy package which references the LAN interface.

To configure interface mapping for LAN:

1. Navigate to *Policy & Objects > Normalized Interface*.
2. Use the search field in the top right to search for *port3*.
3. Edit the *port3* mapping by double-clicking on it.
4. Expand *Per-Platform Mapping*, and search within this menu for *FortiGate-VM64-KVM*.

5. Delete the entry and click *OK* to save.
6. Remaining in the *Normalized Interface* menu, select *Create New* in the top menu bar to create a new mapping as follows:

Name LAN

Per-Platform Mapping

Matched Platform: FortiGate-VM64-KVM
Mapped Interface Name: port3

Create New Normalized Interface

Name

LAN

Description

Color

Change

Wildcard

Per-Platform Mapping

Create New

Edit

Delete

Search...

	Name	Device Interface Name	Shaping Profile
<input type="checkbox"/>	FortiGate-VM64-KVM	port3	

1

Configure the branch policy package and policies

To create the branch policy package and policies:

1. Navigate to *Policy & Objects*, and expand the *Branches* folder, then select *Firewall Policy*.
The firewall policy already contains an entry for *Health Check Access*.
2. Use the *Create New* button in the top menu bar to create a firewall policy named *Branch to DC* as follows:

Name	Branch to DC
Incoming Interface	LAN
Outgoing Interface	HUB1, HUB2
IPv4 Source Address	Branch-LAN
IPv4 Destination Address	Datacenter LAN1
Action	Accept

Create New Firewall Policy

ID

0

Name

Branch to DC

Type

Standard ZTNA

Incoming Interface

LAN

Unmapped/Interface

+

Outgoing Interface

HUB1

Unmapped/Created by SDWAN Overlay Template

HUB2

Unmapped/Created by SDWAN Overlay Template

+

Source

Branch-LAN

IP/Netmask: 10.1.0.0/255.255.0.0

+

Negate Source

☐

IP/MAC Based Access Control

+

Logical And With Secondary Tags

Disabled

Specify

Destination

Datacenter-LAN1

IP/Netmask: 192.168.1.0/255.255.255.0

+

Negate Destination

☐

Service

ALL

+

Schedule

always

+

Action

Accept

Deny

IPSEC

Inspection Mode

Flow-based

Proxy-based

3. Click OK to create the firewall policy.

4. Create a second policy using the same method as above with the following details:

Name	Direct Internet Access
Incoming Interface	LAN
Outgoing Interface	WAN1, WAN2
IPv4 Source Address	Branch-LAN
IPv4 Destination Address	RFC-1918 address group
Negate Destination	Enable
Action	Accept
NAT	Enable
Security Profiles	Apply security profiles as needed to protect users from internet threats.

5. Click OK to create the firewall policy.

6. Create a third policy using the same method as above with the following details:

Name	DC to LAN
Incoming Interface	HUB1, HUB2
Outgoing Interface	LAN
IPv4 Source Address	Datacenter-LAN1, Branch-LAN
IPv4 Destination Address	Branch-LAN
Action	Accept

- Click *OK* to create the firewall policy.

Configuring the Hub policy package and policies

To create the hub policy package and policies:

- Remaining in *Policy & Objects*, expand the *Hub* folder and select *Firewall Policy* to review the Hub firewall policy.
- There will be one policy created from the SD-WAN Overlay template *Health Check Access*.
- Use the *Create New* button in the top menu bar to create a firewall policy named Branch to DC as follows:

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

Create New Firewall Policy

ID
Name
Type
Incoming Interface
Outgoing Interface
Source
Negate Source
IP/MAC Based Access Control
Logical And With Secondary Tags
Destination
Negate Destination
Service
Schedule
Action
Inspection Mode

0

Branch to DC

Standard ZTNA

VPN1

Unmapped/Created by SDWAN Overlay Template

VPN2

Unmapped/Created by SDWAN Overlay Template

+

LAN

Unmapped/Interface

+

all

+

+

Disabled Specify

Datacenter-LAN1

IP/Netmask: 192.168.1.0/255.255.255.0

+

+

ALL

+

always

+

Accept Deny IPSEC

Flow-based Proxy-based

- Click *OK* to create the firewall policy.
- Create a second Hub policy using the same method as above with the following details:

Name	DC to Branch
Incoming Interface	LAN
Outgoing Interface	VPN1, VPN2
IPv4 Source Address	Datacenter-LAN1

IPv4 Destination Address Branch-LAN

Action Accept

Create New Firewall Policy

ID	0
Name	DC to Branch
Type	Standard ZTNA
Incoming Interface	LAN Unmapped/Interface
Outgoing Interface	VPN1 Unmapped/Created by SDWAN Overlay Template VPN2 Unmapped/Created by SDWAN Overlay Template
Source	Datacenter-LAN1 IP/Netmask: 192.168.1.0/255.255.255.0
Negate Source	<input type="checkbox"/>
IP/MAC Based Access Control	<input type="checkbox"/>
Logical And With Secondary Tags	Disabled Specify
Destination	Branch-LAN IP/Netmask: 10.1.0.0/255.255.0.0
Negate Destination	<input type="checkbox"/>
Service	ALL
Schedule	always
Action	<input checked="" type="checkbox"/> Accept <input type="checkbox"/> Deny <input type="checkbox"/> IPSEC
Inspection Mode	Flow-based Proxy-based

- Click OK to create the firewall policy.
- Create a third Hub policy using the same method as above with the following details:

Name Branch to Branch

Incoming Interface VPN1, VPN2

Outgoing Interface VPN1, VPN2

IPv4 Source Address Branch-LAN

IPv4 Destination Address Branch-LAN

Action Accept

Create New Firewall Policy

ID: 0

Name: Branch to Branch

Type: Standard ZTNA

Incoming Interface: VPN1, VPN2

Outgoing Interface: VPN1, VPN2

Source: Branch-LAN, IP/Netmask: 10.1.0.0/255.255.0.0

Negate Source: Disabled

IP/MAC Based Access Control: Disabled

Logical And With Secondary Tags: Specify

Destination: Branch-LAN, IP/Netmask: 10.1.0.0/255.255.0.0

Negate Destination: Disabled

Service: ALL

Schedule: always

Action: Accept, Deny, IPSEC

Inspection Mode: Flow-based, Proxy-based

8. Click OK to create the firewall policy.

Installing policy packages

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

1. Install the HUB policy package to the HUB1 and HUB2 devices. See [Installing the HUB policy package on page 33](#).
2. Install the branch policy package to branch device group. See [Installing the branch policy package on page 35](#).

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 - Choose What to Install (1/4)

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

Install Comments

0/127

Create ADOM Revision

Revision Name

Hub_2025-03-07-05-51-45-PST

Revision Comments

0/127

Schedule Install

☒ Install Policy Package & Device Settings

☐ Install Device Settings (only)

< Back

Next >

Cancel

The wizard moves to the next screen:

Install Wizard - Select Devices to Install (Hub) (2/4)

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

Search...

<input checked="" type="checkbox"/>	Device Name ↕	IP Address ↕	Platform ↕	<div><div></div></div>
<input checked="" type="checkbox"/>	⬆️ HUB1	192.168.100.101	FortiGate-VM64-KVM	
<input checked="" type="checkbox"/>	⬆️ HUB2	192.168.100.102	FortiGate-VM64-KVM	

- 3.** Verify that *HUB1* and *HUB2* are 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 - Validate Devices (Hub) (3/4)

Installation Preparation

Total: 3/3

Success: 3

Warning: 0

Error: 0

Show Details

Interface Validation

Policy and Object Validation

Ready to Install

Install Preview

Policy Package Diff

Search...

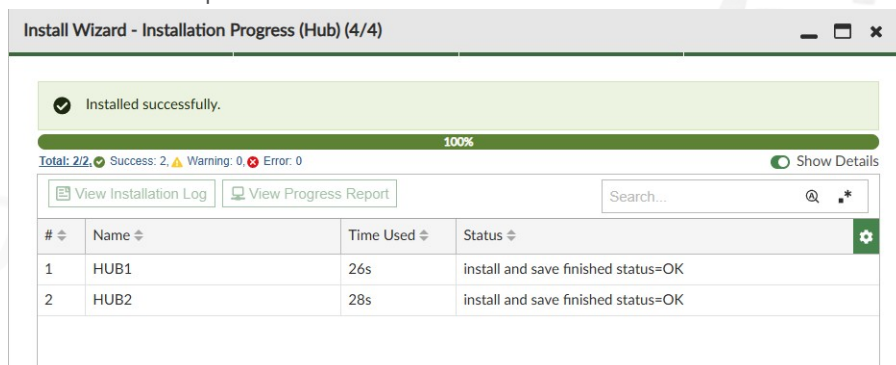
	Device Name	Status	Action
	HUB1	Connection Up	
	HUB2	Connection Up	

CONFIGURATION STEPS

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* for HUB1 and HUB2.



5. Click *Finish* to complete the install wizard.

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:

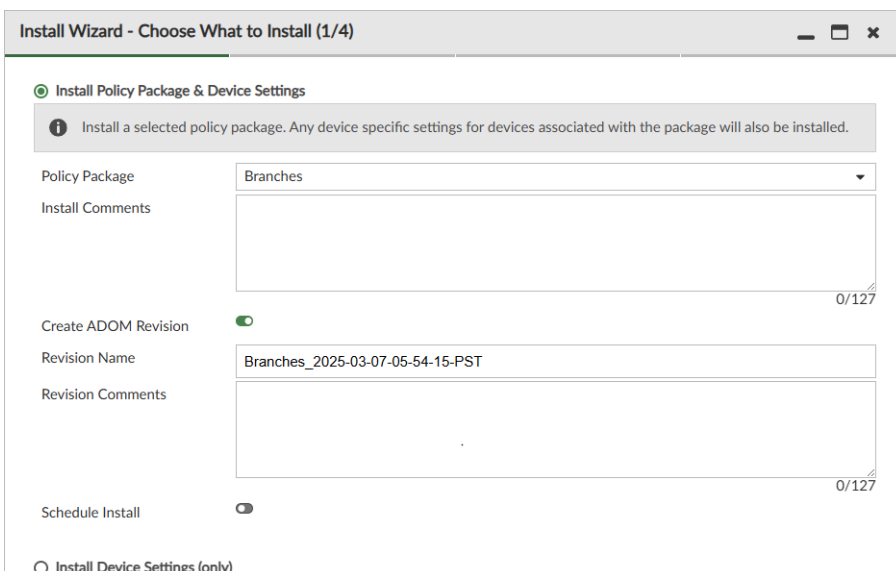
1. Go to *Device Manager*, and click *Install Wizard* in the toolbar.
The *Install Wizard* dialog box opens.
2. Set the following options, and click *Next*:

Install Policy Package & Device Settings

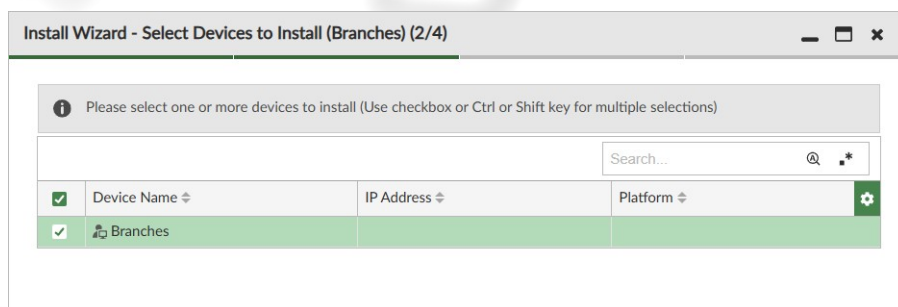
Select

Policy Package

Branches

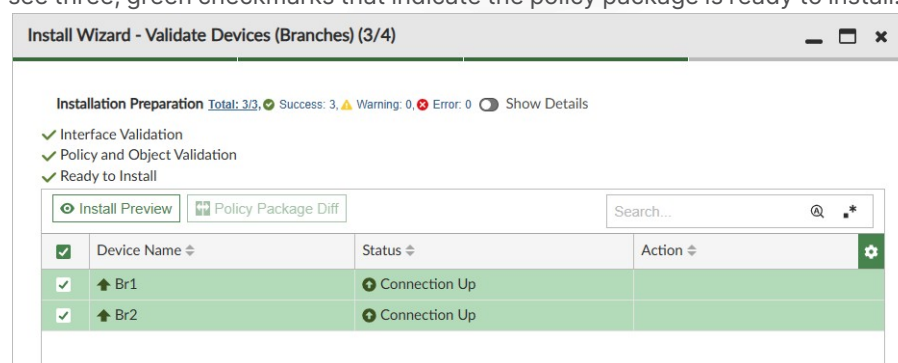


The wizard moves to the next screen:



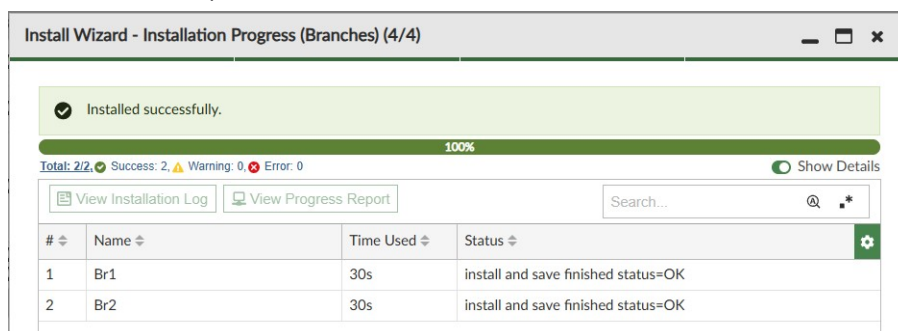
3. Verify that *Branches* is selected, and click *Next*.

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*.



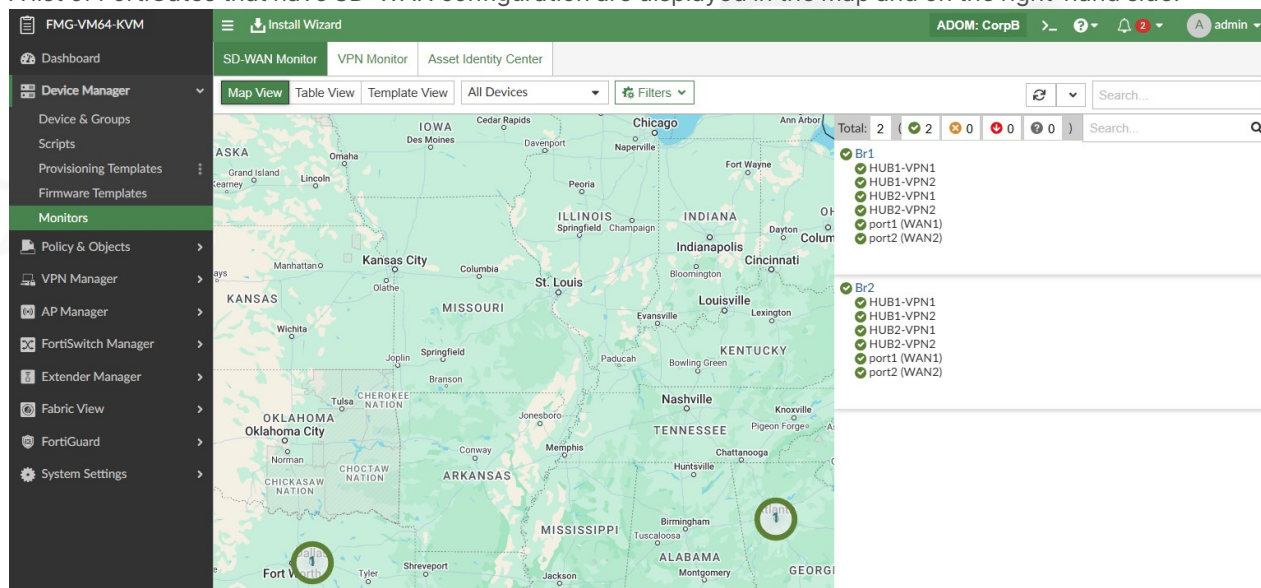
Verifying the SD-WAN configuration

You can verify the SD-WAN and overlay configuration in the *Device Manager > Monitor > SD-WAN Monitor* pane. The below examples show data based on application traffic being sent from the branch locations to public resources as well as corporate resources.

To verify:

1. Go to *Device Manager > Monitors > SD-WAN Monitor*.

A list of FortiGates that have SD-WAN configuration are displayed in the map and on the right-hand side.



Question: Why are the HUB devices not seen on the map?

This is the SD-WAN monitor map. The HUB devices are not configured to use SD-WAN and so they are not displayed here.

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.

CONFIGURATION STEPS

The screenshot displays the Fortinet FortiGate SD-WAN configuration interface. The left sidebar shows the navigation menu with 'Monitors' selected. The main content area is divided into two sections: 'SD-WAN Interfaces' and 'SD-WAN Rules'.

SD-WAN Interfaces:

Interface	IP	Health Check Status	Bytes (Sent/Received)	Link Mode	Error
HUB1-VPN1			161.95MB/161.70MB	N/A	6 / 0
HUB1-VPN2			320.41KB/320.36KB	N/A	2 / 0
HUB2-VPN1			320.48KB/320.41KB	N/A	2 / 0
HUB2-VPN2			320.46KB/320.43KB	N/A	2 / 0
port1 (WAN1)	10.198.1.2/255.255.2...		185.93MB/824.42MB	10 Gbps Full Duplex	0 / 0
port2 (WAN2)	10.198.2.2/255.255.2...		11.49MB/151.01MB	10 Gbps Full Duplex	0 / 0

SD-WAN Rules:

ID	SD-WAN Rule	Source	Destination	Criteria	Hit Count	Members
3	Critical_Video	Branch-LAN	YouTube, Zoom, GoToMeeting	Latency (Prefer_Passive)	3834	port1 (WAN1), port2 (WAN2)
4	Critical_DIA	Branch-LAN	Salesforce, Microsoft.Teams, Dropbox	Latency (Internet)	2210	port1 (WAN1), port2 (WAN2)
1	Corporate_Traffic	Branch-LAN	Datacenter-LAN1	Latency (HUB2_HC)	18	HUB1-VPN1, HUB1-VPN2, HUB2-VPN1, HUB2-VPN2
2	Internet_Traffic	Branch-LAN	all	Latency	10952	port2 (WAN2)

- Per the SD-WAN Rules widget, HUB1-VPN1 was selected for Corporate_Traffic. This is why the interface HUB1-VPN1 in the SD-WAN Interfaces widget is showing significantly more traffic than the other tunnels.

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.

This section contains the following topics:

- [ADVPN on page 39](#)
- [Adaptive FEC on page 42](#)

ADVPN

Following is a summary of enabling ADVPN:

1. Enable ADVPN in the SD-WAN Overlay template. See [ADVPN on page 39](#)
2. Edit the SD-WAN rules in the SD-WAN template. See [Editing branch SD-WAN template on page 40](#)
3. Edit the Branches policy package. See [Editing branch policy package on page 40](#)
4. Install the policy packages to both Branches and Hub. See [Install the policy packages to both Branches and Hub on page 40](#)

Enabling ADVPN

Edit an existing 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 SD-WAN Overlay template created earlier.
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 SD-WAN template

Edit the branch SD-WAN template to add *Branch_LAN* as a destination address for the *Corporate_Traffic* rule.

To edit the branches template:

1. Go to *Device Manager > Provisioning Templates > SD-WAN*, and double-click the branch SDWAN 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_LAN* as a destination address (in addition to the Datacenter LAN1 subnet).

4. Click *OK* to save the rule, then *OK* to save the template.

Editing branch policy package

Edit the branch policy package to add *Branch_LAN* as a destination address for the Branch to DC rule. Rename the rule to *Branch to Corporate*.

To edit the branches policy package:

1. Go to *Policy & Objects > Policy Packages*, and expand *Branches* to click on *Firewall Policy*.
2. Edit the *Branch to DC* rule.
3. Change the name from *Branch to DC* to *Branch to Corporate*.
4. Under *Destination*, add the *Branch-LAN* address object.
5. Click *OK* to save.

Install the policy packages to both Branches and Hub

To install the config to branch devices:

1. From the top menu bar, select *Install Wizard*.
2. Ensure *Branches* is selected for *Policy Package*, then click *Next*.

3. Once the validation passes, select *Install*.
4. Once install completes, select *Finish*.

To install the config to the hub:

1. From the top menu bar, select *Install Wizard*.
2. Ensure *HUB* is selected for *Policy Package*, then click *Next*.
3. Once the validation passes, select *Install*.
4. Once install completes, select *Finish*.

Verifying the ADVPN configuration

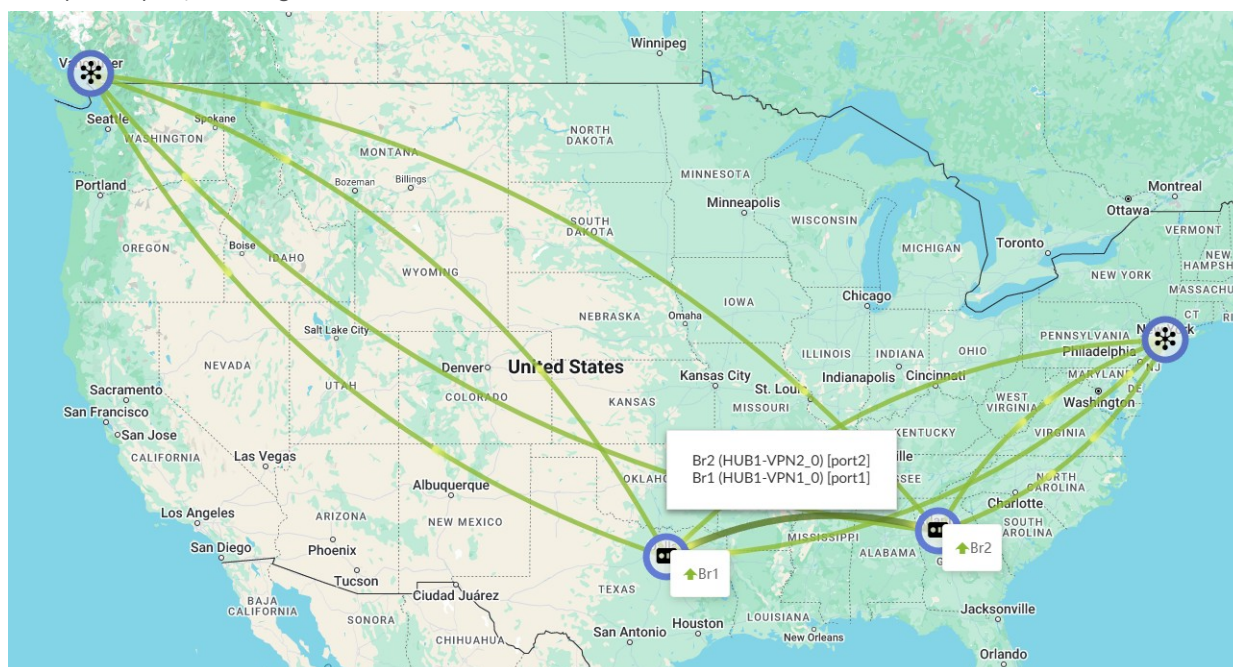
To verify the ADVPN configuration, initiate an ADVPN shortcut by sending traffic from one branch LAN to another.

```
10.1.1.10@Branch1:~$ ping 10.1.2.10
64 bytes from 10.1.2.10: icmp_seq=1 ttl 61 time 39.8 ms
64 bytes from 10.1.2.10: icmp_seq=2 ttl 62 time 23.8 ms
64 bytes from 10.1.2.10: icmp_seq=3 ttl 62 time 23.4 ms
64 bytes from 10.1.2.10: icmp_seq=4 ttl 62 time 23.3 ms
```

The first ping from 10.1.1.10 to 10.1.2.10 is routed through the HUB to branch2 with a latency of 40ms and a TTL of 61. After the initial ping, the shortcut is formed and the remaining pings are sent directly from branch1 to branch2.

This can be confirmed through the FortiManager VPN monitor as follows:

1. On FortiManager, navigate to *Device Manager > Monitors*.
2. From the top menu bar, select *VPN Monitor*.
3. A map will open, showing the branch and HUB device VPN tunnels.



Notice how there is a VPN tunnel between the two branches at Fort Worth and Atlanta. This tunnel is significantly shorter than those going from Br1/2 to the HUB.

Enable the *Show Table* slider in the top left of the VPN monitor window to display a table showing the details for

each FortiGate's VPN tunnel. The ADVPN tunnel is highlighted.

Device	Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Br1[root]	HUB1-VPN1	automatic	10.198.5.2	10.198.5.2	10.75 KB	10.53 KB	HUB1-VPN1	HUB1-VPN1
Br1[root]	HUB1-VPN1_0	dialup	10.198.4.2	Branch1	3.44 KB	3.52 KB	HUB1-VPN1_0	HUB1-VPN1
Br1[root]	HUB1-VPN2	automatic	10.198.6.2	10.198.6.2	8.73 KB	8.52 KB	HUB1-VPN2	HUB1-VPN2
Br1[root]	HUB2-VPN1	automatic	10.198.7.2	10.198.7.2	8.73 KB	8.52 KB	HUB2-VPN1	HUB2-VPN1
Br1[root]	HUB2-VPN2	automatic	10.198.8.2	10.198.8.2	8.73 KB	8.52 KB	HUB2-VPN2	HUB2-VPN2
Br2[root]	HUB1-VPN1	automatic	10.198.5.2	10.198.5.2	5.27 KB	5.12 KB	HUB1-VPN1	HUB1-VPN1
Br2[root]	HUB1-VPN2	automatic	10.198.6.2	10.198.6.2	7.48 KB	7.31 KB	HUB1-VPN2	HUB1-VPN2
Br2[root]	HUB1-VPN2_0	dialup	10.198.1.2	Branch2	3.52 KB	3.44 KB	HUB1-VPN2_0	HUB1-VPN2
Br2[root]	HUB2-VPN1	automatic	10.198.7.2	10.198.7.2	5.44 KB	5.24 KB	HUB2-VPN1	HUB2-VPN1

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 42](#).
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 42](#).
3. Enable FEC on both HUB VPN phase 1 interfaces. See [Enabling FEC for hub devices on page 43](#).
4. Enable FEC on both branch VPN tunnels. See [Enabling FEC on branch devices on page 44](#).
5. Create policies for hub and branch devices, and install the policy packages. See [Creating policies and installing policy packages on page 44](#).

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.

Create New Service

Name

CustomApp-5000

Comments

Color

Change

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	Action
UDP	5000	5000	5000

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 left side menu, expand *Policy & Objects* and select *Advanced*.
2. Select *CLI Configurations* from the top menu.
3. In the *Search* box, type `fec`. The *vpn ipsec fec* menu will appear.
4. Click *Create New*. The *create vpn ipsec fec* mapping pane is displayed.
5. In the *Name* box, type `dc_fec`.
6. Under mappings, click *Create New*. The *Create New vpn ipsec fec mappings* 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

Create New vpn ipsec fec

name (maximum 35 characters)

mappings

	seqno	bandwidth-bi-threshold	bandwidth-down-threshold	bandwidth-up-threshold	base	latency
<input type="checkbox"/>	1	0	0	0	8	0
<input type="checkbox"/>	2	0	0	0	5	10

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*.
2. Double-click the *Primary_secondary_dual_hub_HUB1_IPsec* template to open it for editing.
3. Select *VPN1*, and click *Edit*.
4. Scroll down to and expand *Advanced Options*.
5. Set the following options:

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

6. Click *OK* to save the changes.
7. Repeat the same steps for VPN2.
8. Repeat steps 2 through 7 for the *Primary_secondary_dual_hub_HUB2_IPsec* template.

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 *Primary_secondary_dual_hub_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*.
7. Double-click *HUB2-VPN1* to open it for editing.
8. For *FEC Health Check*, enter *HUB2_HC*.
9. Scroll down and expand *Advanced Options*.
10. Set the following options and click *OK*:

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

11. Repeat for *HUB2-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	VPN1, VPN2
Outgoing Interface	LAN
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*.

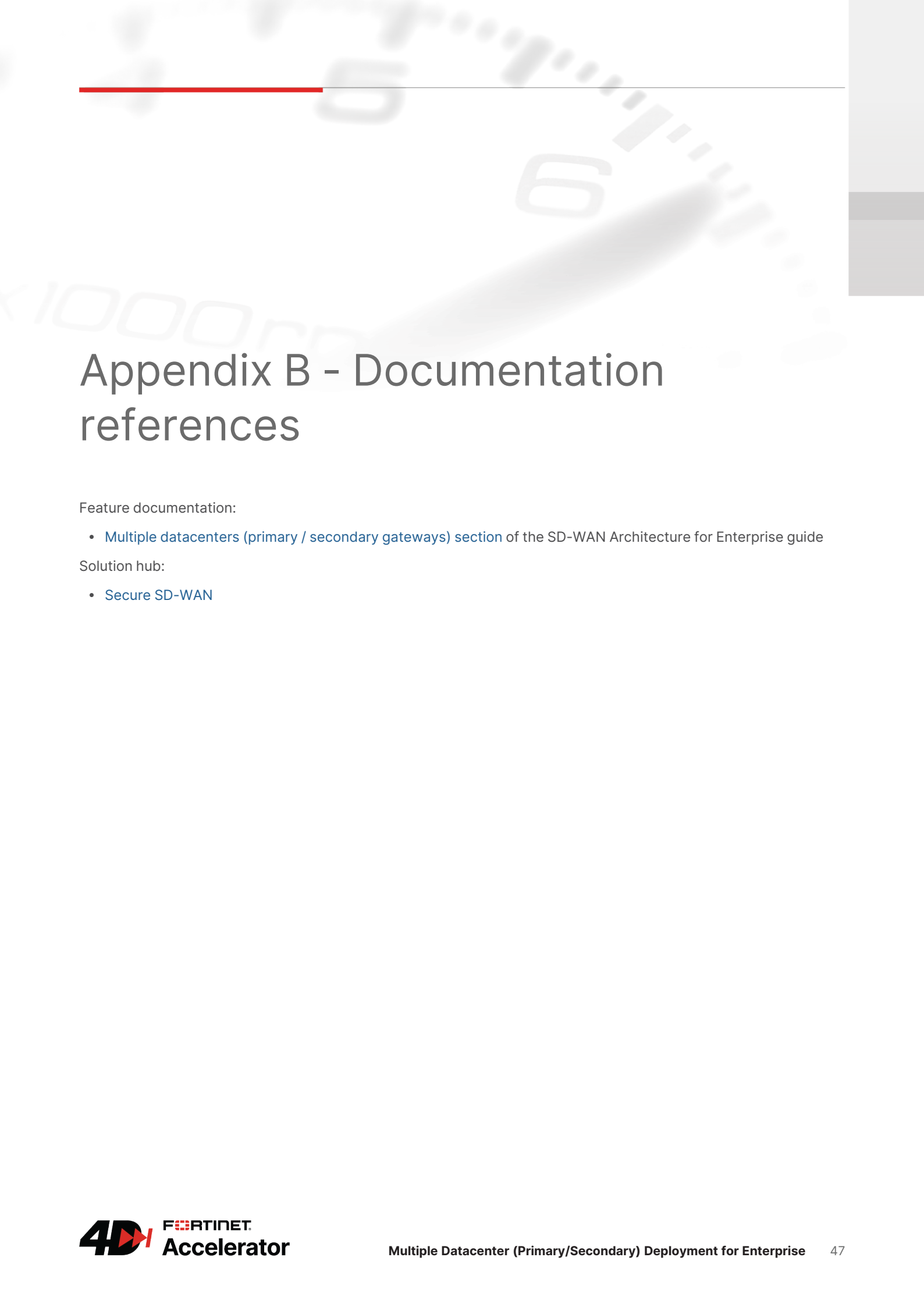
Name	Custom App Policy
Incoming Interface	LAN
Outgoing Interface	HUB1, HUB2
Pv4 Source Address	Branch network
Pv4 Destination Address	Datacenter LAN1
Service	CustomApp-5000
Action	Accept
Advanced Options	fec enabled

- c. Move this policy under the *Health Check Access* policy.
3. Install both HUB and Branch policy packages.

Appendix A - Products used

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

Product	Model	Firmware
FortiOS	KVM Virtual Machine	7.4.7
FortiManager	KVM Virtual Machine	7.4.6



Appendix B - Documentation references

Feature documentation:

- [Multiple datacenters \(primary / secondary gateways\)](#) 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
<code>diag vpn ike gateway list</code>	Confirm IPsec is up
<code>get router info bpg summary</code>	Confirm BGP is up and exchanging routes
<code>diagnose sys sdwan health-check status HUB1_HC</code>	Confirm hub device is reachable through SLA



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

01-740-802316-20250425