



# Multiple Datacenter (Primary/Primary) Deployment for Enterprise

Secure SD-WAN



DEFINE / DESIGN / **DEPLOY** / DEMO



## Table of Contents

<b>Change Log</b>	<b>3</b>
<b>Deployment procedures</b>	<b>4</b>
Prerequisites	4
Recommendations	4
Planning	5
Assumptions	5
Configuration steps	6
Creating an overlay template	6
Assigning meta data values to branch devices	10
Configuring SD-WAN rules	11
Creating normalized interfaces	15
Creating policy packages and firewall policies	17
Installing policy packages	22
Verifying the SD-WAN configuration	25

# Change Log

Date	Change Description
2022-05-10	Initial release.
2022-11-03	Updated <a href="#">Branch BGP signaling</a> .

# Deployment procedures

FortiManager is used to configure SD-WAN for a topology that includes multiple datacenter devices (hubs) and multiple branch devices.

In this example, both HUB devices are configured as *primary* HUB devices instead of *primary/secondary* HUB devices. This use case is common where HUB devices provide remote access to different resources.

- Example 1: HUB1 in HQ, HUB2 in Datacenter
- Example 2: HUB1 in Datacenter, HUB2 in AWS
- Example 3: HUB1 in AWS, HUB2 in Azure

The deployment instructions include the following topics:

- [Prerequisites on page 4](#)
- [Recommendations on page 4](#)
- [Planning on page 5](#)
- [Assumptions on page 5](#)
- [Configuration steps on page 6](#)

## Prerequisites

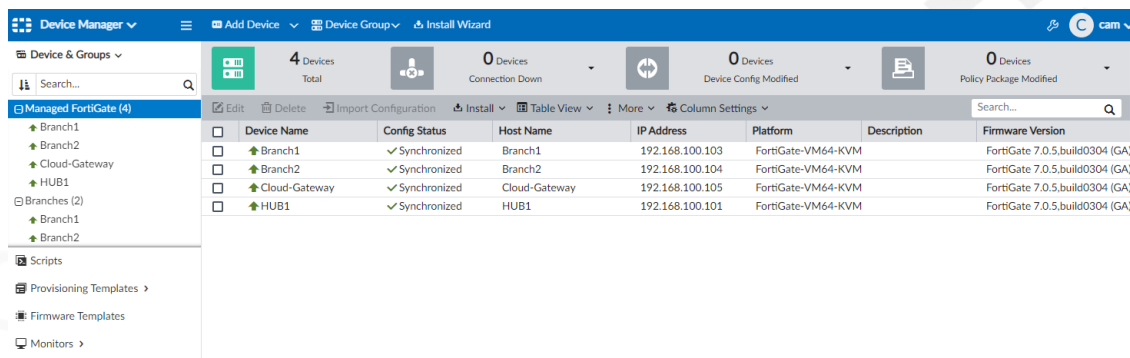
This guide presumes the following prerequisites have been met:

- 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.



## 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:

- HUB1 is located at a private or public corporate location (for example, HQ, datacenter, colo, and so on).
  - This hub provides access to one or more applications or services.
- The second hub, Cloud-Gateway, is located in a public cloud.
  - The Cloud-Gateway provides access to one or more cloud applications or services.
  - This gateway has only 1 WAN connection.
- 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 subnet is 192.168.1.0/24 and is learned through a BGP peer.
- The Cloud services are directly connected on port3 with the subnet 172.20.1.0/24.

## 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 6](#).
2. Assign metadata values to branch devices. See [Assigning meta data values to branch devices on page 10](#).
3. Configure SD-WAN rules. See [Configuring SD-WAN rules on page 11](#).
4. Create normalized interfaces. See [Creating normalized interfaces on page 15](#).
5. Create policy packages and firewall policies for hub and branch devices. See [Creating policy packages and firewall policies on page 17](#).
6. Install policy packages to devices. See [Installing policy packages on page 22](#).
7. Verify the SD-WAN configuration. See [Verifying the SD-WAN configuration on page 25](#).

## 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.
4. Set the region settings:
  - a. Select *Dual Hub (Primary & Primary)*.
  - 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)**

Name	ACME SD-WAN Overlay
Description	Overlay for ACME corp.
Select New Topology	<div>Single HUB</div> <div>Dual HUB (Primary &amp; Secondary)</div> <div><b>Dual HUB (Primary &amp; Primary)</b></div>
Advanced	<div>Loopback IP Address: 172.16.0.0/255.255.0.0</div> <div>Overlay Network: 10.10.0.0/255.255.0.0</div> <div>BGP-AS Number: 65000</div> <div>Auto-Discovery VPN: <input type="checkbox"/></div>

Next > Cancel

- c. Click *Next*. The *Role Assignment* pane is displayed.
5. Set the role assignment:
  - a. Set *Primary HUB* to *HUB1*.
  - b. Set *Secondary HUB* to *Cloud-Gateway*.
  - c. Set *Device Group Assignment* to *Branches*.

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

Name	ACME SD-WAN Overlay	
Topology	<div>Single HUB</div> <div>Dual HUB (Primary &amp; Secondary)</div> <div><b>Dual HUB (Primary &amp; Primary)</b></div>	
<b>HUB</b>		
Primary HUB	HUB1	
Primary HUB	Cloud-Gateway	
<b>Branch</b>		
Device Group Assignment	Branches	

< Back Next > Cancel

- d. Click *Next*. The *Network Configuration* pane is displayed.
6. Set the network configuration for the primary HUB:
  - a. Under *Primary HUB*, set *WAN Underlay 1* to *port1*.
  - b. Set *WAN Underlay 2* to *port2*.

## c. Expand *Advanced*.

The screenshot shows the 'Edit SD-WAN Overlay Template - Network Configuration (3/5)' window. The 'Advanced' section is expanded, revealing the 'Neighbors' table. The table has columns: #, Neighbor IP, Remote AS, Route Map in, and Route Map Out. It contains one row with #1, Neighbor IP 172.16.1.1, and Remote AS 65100. Below the table, the 'Network Advertisement' section shows 'Connected' selected for the interface. The 'Private Link' and 'Override IP' options are also visible for WAN Underlay 1 and 2.

- 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.



When entering the port name, it is case sensitive and must match the port as written on the FortiGate exactly.

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.

7. Set the network configuration for the secondary HUB:
  - a. Under *Secondary HUB*, set *WAN Underlay 1* to *port1*.
  - b. Under *Secondary HUB*, click the x for *WAN Underlay 2* to remove it.
  - c. Set *Network Advertisement* to *Connected*.

The screenshot shows the 'Edit SD-WAN Overlay Template - Network Configuration (3/5)' window. The 'Secondary HUB' section is visible. Under 'WAN Underlay 1', 'port1' is selected. Under 'Network Advertisement', 'Connected' is selected. Under 'Interface 1', 'port2' is selected. The 'Advanced' section is collapsed.



A neighbor is configured for HUB1 to learn the route to the Corporate Datacenter LAN (192.168.1.0/24) and the Cloud resource network (172.20.1.0/24) 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.

8. Set the network configuration for the branches 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*.



The Network Advertisement 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.
9. 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*.

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

**Edit 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.

<b>Template Name</b>	ACME SD-WAN Overlay
<b>Topology</b>	Dual HUB (Primary & Primary)
<b>Region Network Settings</b>	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: <input type="checkbox"/>
<b>Device Assignment</b>	Primary HUB:  HUB1 (192.168.100.101, Platform: FortiGate-VM64-KVM) Primary HUB:  Cloud-Gateway (192.168.100.105, Platform: FortiGate-VM64-KVM) Assign to:  Branches
<b>Underlay Assignment</b>	Primary HUB Underlays: port1, port2 Primary HUB Underlays: port1 Branch Underlays: port1, port2
<b>Network Advertisement</b>	Primary HUB: Connected: None Primary HUB: Connected: None Branch: Connected: port3
<b>SD-WAN Template Options</b>	Add Overlay Objects to SD-WAN Template: <input checked="" type="checkbox"/> Branch_SDWAN Add Overlay Interfaces and Zones: <input type="checkbox"/> Add Healthcheck Servers for Each HUB as Performance SLA: <input type="checkbox"/>

< Back Finish Cancel

10. 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)**

Column Settings Search...

#	Variable Name	Mapping Value	Default Value
1	\$(branch_id)	1	<input checked="" type="checkbox"/>

The value is set.

#	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, 192.168.1.0/24 (Create new Address Object)
Strategy	Lowest Cost SLA
Interface Preference	HUB1 zone
Required SLA Target	HUB1_HC#1

The SD-WAN rule is created.

4. Create a rule named *Cloud\_Traffic*:

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

Name	Cloud_Traffic
Source	Branch Network
Destination	Cloud LAN1, 172.20.1.0/24 (Create new Address Object)
Strategy	Lowest Cost SLA
Interface Preference	HUB2 zone
Required SLA Target	HUB2_HC#1

## CONFIGURATION STEPS

The screenshot shows the 'Create New SD-WAN Rule' dialog in the Fortinet SD-WAN configuration interface. The rule is named 'Cloud\_Traffic' and is configured for IPv4. The source is 'Branch Network' and the destination is 'Cloud LAN1'. The protocol is set to 'ANY' and the outgoing interface preference is 'Lowest Cost (SLA)'. The required SLA target is 'HUB2\_HC#1'.

The SD-WAN rule is created.

### 5. Define an SLA target for internet traffic:

- Under *Performance SLA*, and click *Create New*. The *Create New Performance SLA* pane opens.
- Set the following options, and click *OK*:

Name	Internet
Server	1.1.1.1
Participants	port1, port2
SLA Targets	<ul style="list-style-type: none"> <li>Latency threshold: 300</li> <li>Jitter Threshold: 55</li> <li>Packet Loss Threshold: 3%</li> </ul>

## CONFIGURATION STEPS

**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 %

+ Add Target

OK Cancel

The SLA target is created.

### 6. Create a rule named *Internet Traffic*:

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

Name	Internet_Traffic
Source	Branch Network
Destination	all
Strategy	Lowest Cost SLA
Interface Preference	WAN1, WAN2
Required SLA Target	Internet

The SD-WAN rule is created.

7. 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.

## CONFIGURATION STEPS

Create New Per-Platform Mapping

Matched Platform

Click to select

Mapped Interface Name

No Advanced Options Available

OK

Cancel

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

Matched Platform	Select <i>all</i> .
Mapped Interface Name	Type <i>HUB1</i> .



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

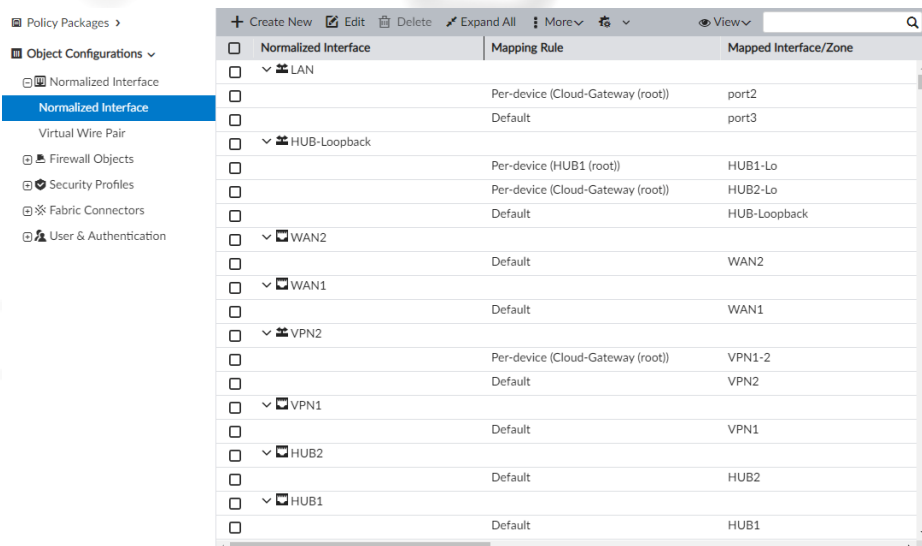
The per-platform mapping is created.

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

Normalized Interface	Matching Type	Mapped Interface/Zone
HUB1	Matched Platform: all	HUB1
HUB2	Matched Platform: all	HUB2
VPN1	Matched Platform: all	VPN1
VPN2	Matched Platform: all Device: Cloud-Gateway	VPN2 VPN1-2
WAN1	Matched Platform: all	WAN1
WAN2	Matched Platform: all	WAN2
HUB-Loopback	Matched Device: HUB1 Device: Cloud-Gateway	HUB1-Lo HUB2-Lo
LAN	Matched Platform: all Device: Cloud-Gateway	port3 port2

All the per-platform mappings are created:

## CONFIGURATION STEPS



The screenshot shows the FortiManager interface with the 'Normalized Interface' configuration table. The table has three columns: 'Normalized Interface', 'Mapping Rule', and 'Mapped Interface/Zone'. The 'Normalized Interface' column is expanded, showing a list of interfaces including LAN, HUB-Loopback, WAN2, WAN1, VPN2, VPN1, HUB2, and HUB1. The 'Mapping Rule' column shows the rule applied to each interface, and the 'Mapped Interface/Zone' column shows the mapped interface or zone.

Normalized Interface	Mapping Rule	Mapped Interface/Zone
LAN	Per-device (Cloud-Gateway (root))	port2
	Default	port3
HUB-Loopback	Per-device (HUB1 (root))	HUB1-Lo
	Per-device (Cloud-Gateway (root))	HUB2-Lo
	Default	HUB-Loopback
WAN2	Default	WAN2
WAN1	Default	WAN1
VPN2	Per-device (Cloud-Gateway (root))	VPN1-2
	Default	VPN2
VPN1	Default	VPN1
HUB2	Default	HUB2
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 17](#).  
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 20](#).

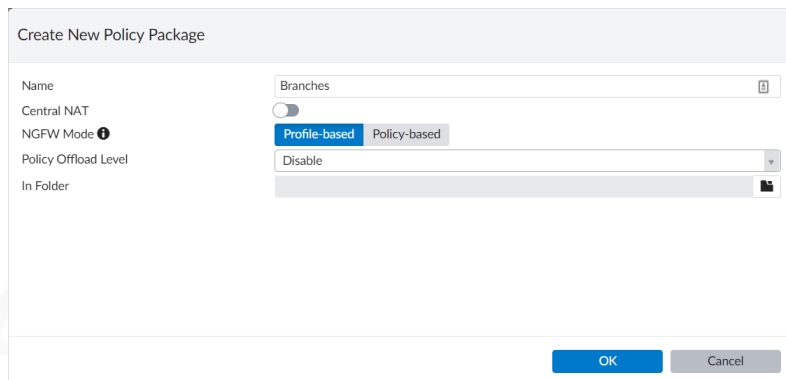
### Creating the branch policy package and policies

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.

## CONFIGURATION STEPS

- b. Set name to *Branches*, and click *OK*.



The 'Create New Policy Package' dialog box is shown. The 'Name' field is set to 'Branches'. The 'Central NAT' toggle is off. The 'NGFW Mode' is set to 'Profile-based'. The 'Policy Offload Level' is set to 'Disable'. The 'In Folder' field is empty. The 'OK' button is highlighted in blue.

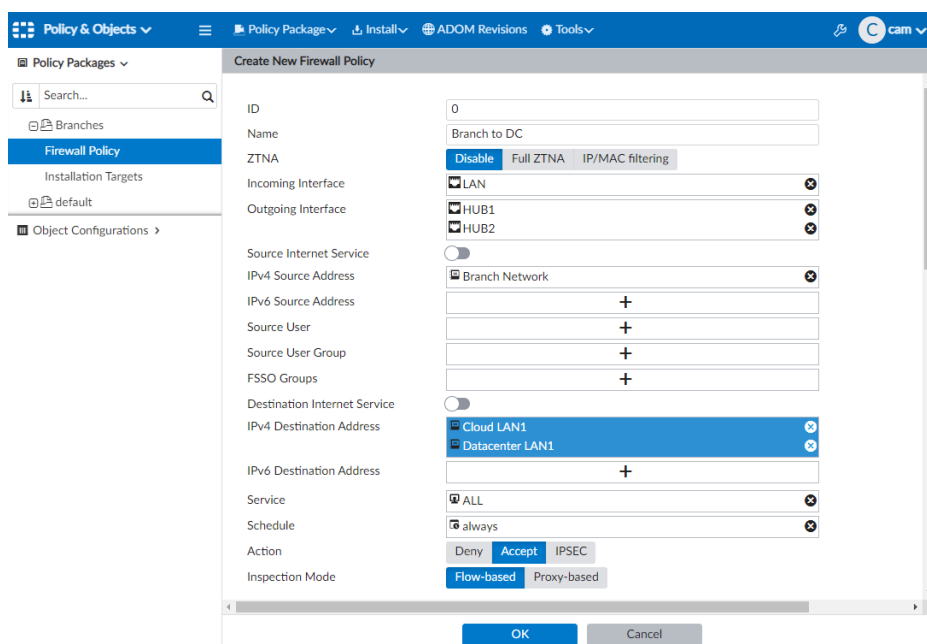
The policy package named *Branches* is created.

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, HUB2
IPv4 Source Address	Branch network
IPv4 Destination Address	Datacenter LAN1, Cloud LAN1
Action	Accept



You may need to split the above rule into individual rules for each HUB, if their security needs differ, such as permitted services and security profiles.



The 'Create New Firewall Policy' dialog box is shown. The 'ID' field is set to '0'. The 'Name' field is set to 'Branch to DC'. The 'ZTNA' toggle is off, and the 'Full ZTNA' and 'IP/MAC filtering' tabs are selected. The 'Incoming Interface' is set to 'LAN'. The 'Outgoing Interface' is set to 'HUB1, HUB2'. The 'Source Internet Service' toggle is off. The 'IPv4 Source Address' is set to 'Branch Network'. The 'IPv6 Source Address' is empty. The 'Source User' is empty. The 'Source User Group' is empty. The 'FSSO Groups' are empty. The 'Destination Internet Service' toggle is off. The 'IPv4 Destination Address' is set to 'Cloud LAN1, Datacenter LAN1'. The 'IPv6 Destination Address' is empty. The 'Service' is set to 'ALL'. The 'Schedule' is set to 'always'. The 'Action' is set to 'Accept'. The 'Inspection Mode' is set to 'Flow-based'. The 'OK' button is highlighted in blue.

The firewall policy is created.

## CONFIGURATION STEPS

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

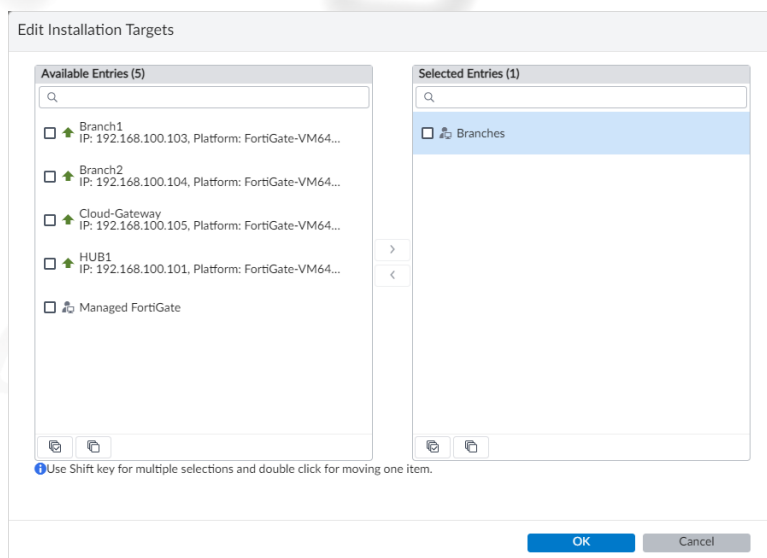
The screenshot shows the 'Create New Firewall Policy' dialog box. The left sidebar contains a tree view with 'Policy Packages' expanded, showing 'Branches' and 'Firewall Policy'. The main area is titled 'Create New Firewall Policy' and contains the following fields and options:

- ID:** 0
- Name:** Direct Internet Access
- ZTNA:** Disable (Full ZTNA, IP/MAC filtering)
- Incoming Interface:** LAN
- Outgoing Interface:** WAN1, WAN2
- Source Internet Service:** Off
- IPv4 Source Address:** Branch Network
- IPv6 Source Address:** +
- Source User:** +
- Source User Group:** +
- FSSO Groups:** +
- Destination Internet Service:** Off
- IPv4 Destination Address:** all
- IPv6 Destination Address:** +
- Service:** ALL
- Schedule:** always
- Action:** Deny, Accept (selected), IPSEC
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall/Network Options:**
  - NAT:** NAT (checked), NAT46, NAT64
  - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool
  - Preserve Source Port:** Off
  - Protocol Options:** default

At the bottom, there are 'OK' and 'Cancel' buttons.

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.



- 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-Loopback
IPv4 Source Address	Overlay Tunnels, 10.10.0.0/16 (create new address object)
IPv4 Destination Address	all
Action	Accept

## CONFIGURATION STEPS

**Edit Firewall Policy**

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

OK Cancel

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	Branch Network
IPv4 Destination Address	Datacenter LAN1
Action	Accept

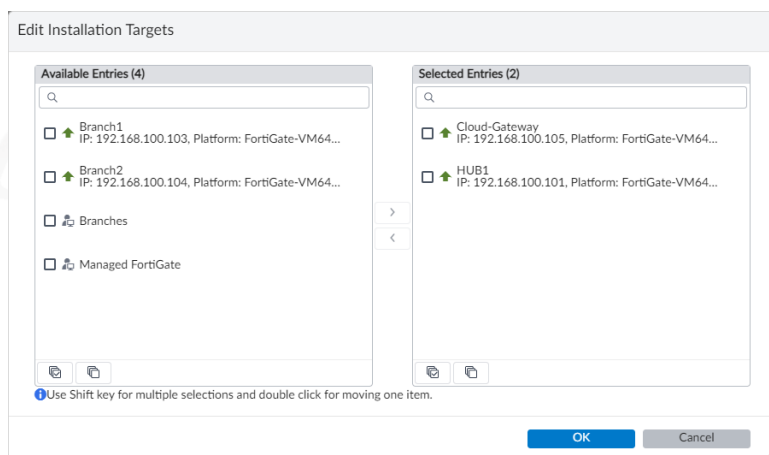
**Create New Firewall Policy**

ID	0
Name	Branch to Datacenter
ZTNA	Disable Full ZTNA IP/MAC filtering
Incoming Interface	VPN1 VPN2
Outgoing Interface	LAN
Source Internet Service	Off
IPv4 Source Address	Branch Network
IPv6 Source Address	+
Source User	+
Source User Group	+
FSSO Groups	+
Destination Internet Service	Off
IPv4 Destination Address	Datacenter LAN1 Cloud LAN1
IPv6 Destination Address	+
Service	ALL
Schedule	always
Action	Deny Accept IPSEC
Inspection Mode	Flow-based Proxy-based

OK Cancel

The firewall policy is created.

5. Assign the HUB policy package to the HUB1 and HUB2 devices:
  - 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* and *Cloud-Gateway* devices, and click the right arrow (>) to move it to the *Selected Entries* list.



- d. Click *OK*.

The installation target for the HUB policy package is the *HUB1* and *HUB2* devices.

## 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 22](#).
2. Install the branch policy package to branch device group. See [Installing the branch policy package on page 23](#).

### 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)

Next > Cancel

The wizard moves to the next screen:

**Install Wizard - Policy Package (HUB)**

Installation Preparation Total: 3/3, Success: 2, Warning: 1, Error: 0

View Installation Log View Progress Report Column Settings Search...

#	Name	Time Used	Status
1	Cloud-Gateway[copy]	<1s	Copy to device done
2	HUB1[copy]	<1s	Copy to device done
3	Write summary[preview]	4s	Write preview done

✓ Interface Validation

✓ Policy and Object Validation

✓ Ready to Install.

Install Preview Policy Package Diff Search...

Device Name	Status	Action
Cloud-Gateway[root]	Connection Up	
HUB1[root]	Connection Up	

Install Cancel

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.

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)

**Next >** **Cancel**

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)

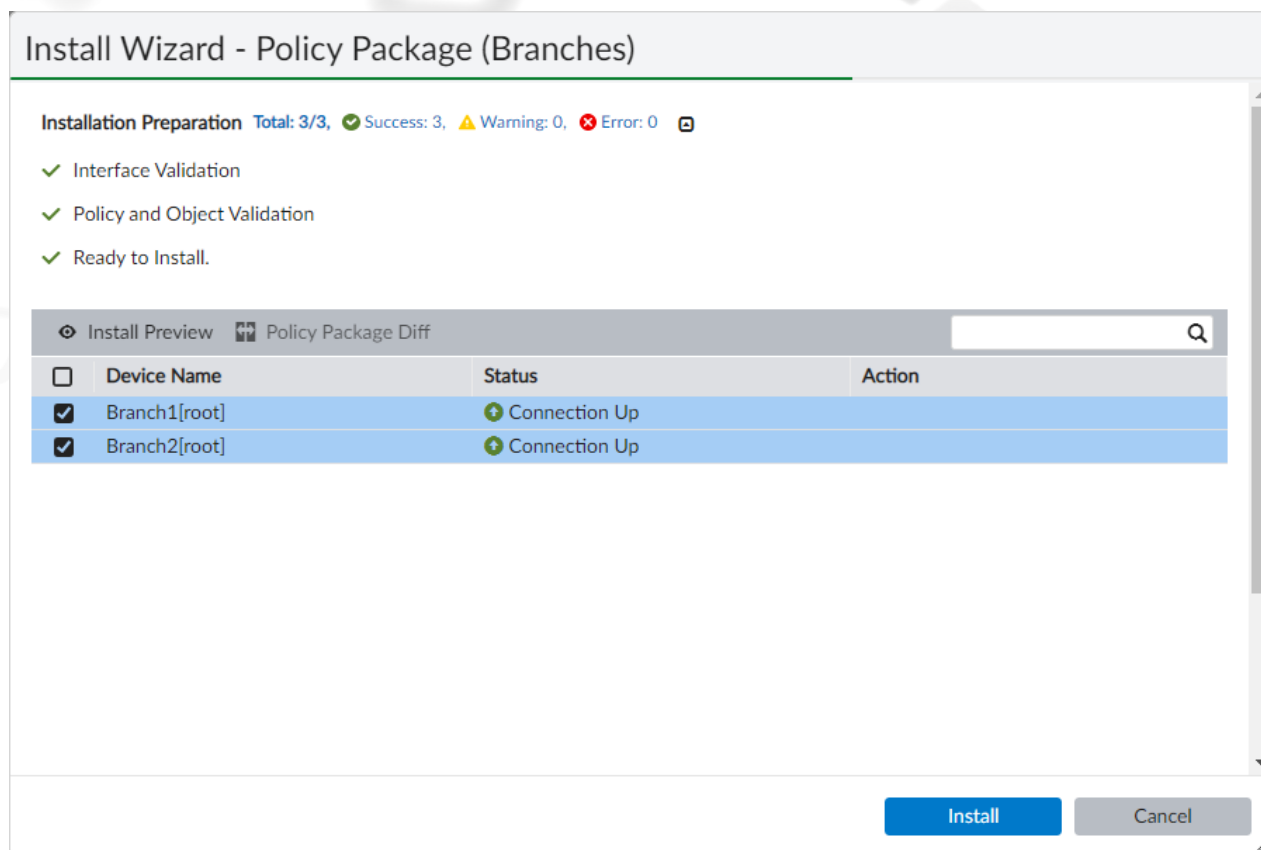
Search:

<input type="checkbox"/>	Device Name	IP Address	Platform
<input checked="" type="checkbox"/>	Branches		

**< Back** **Next >** **Cancel**

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

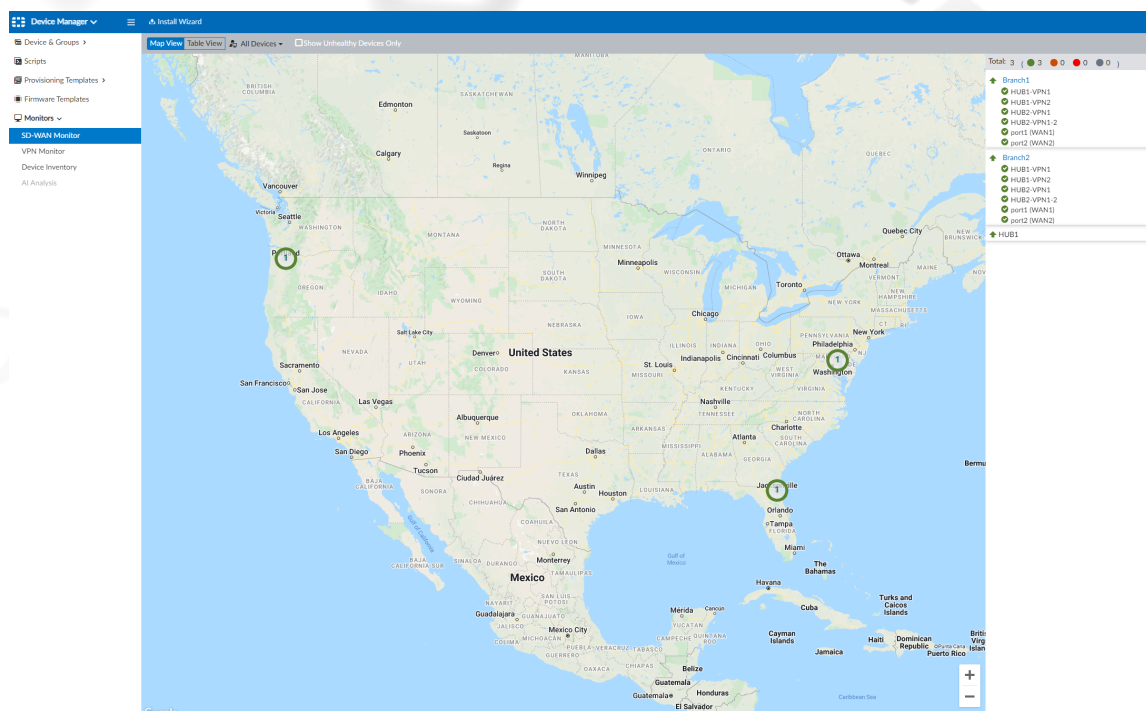
You can verify the SD-WAN and overlay configuration in the *Device Manager > Monitor > SD-WAN Monitor* pane.

To verify:

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

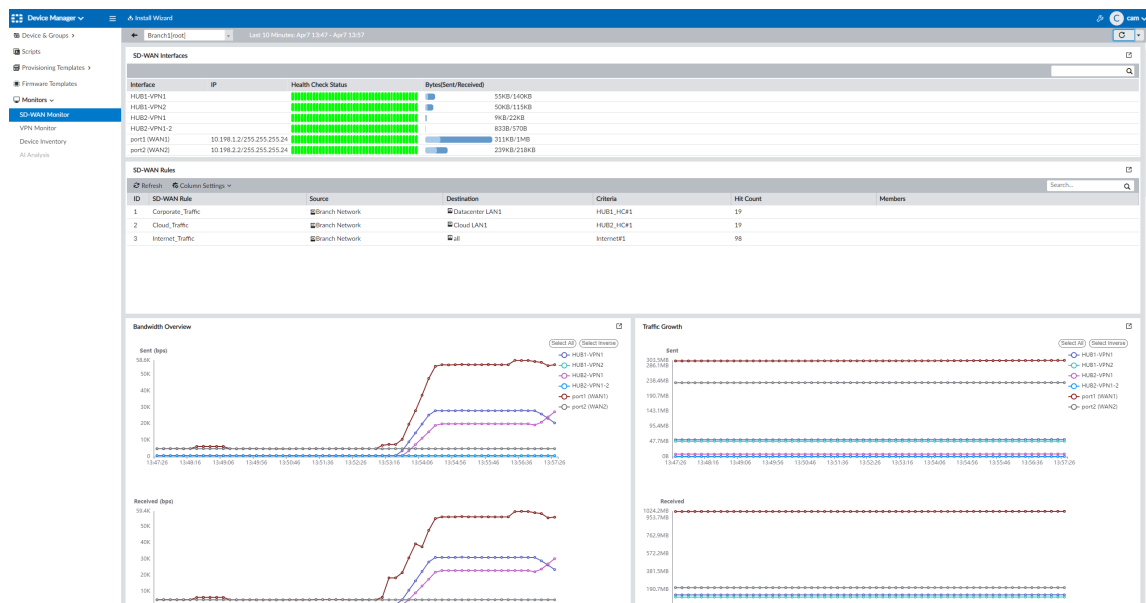
A list of FortiGates are displayed in the map and on the right-hand side.

## CONFIGURATION STEPS



## 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.





[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 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 Chief Legal Officer, 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.

01-720-802718-20220510