Deployment procedures

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

Prerequisites

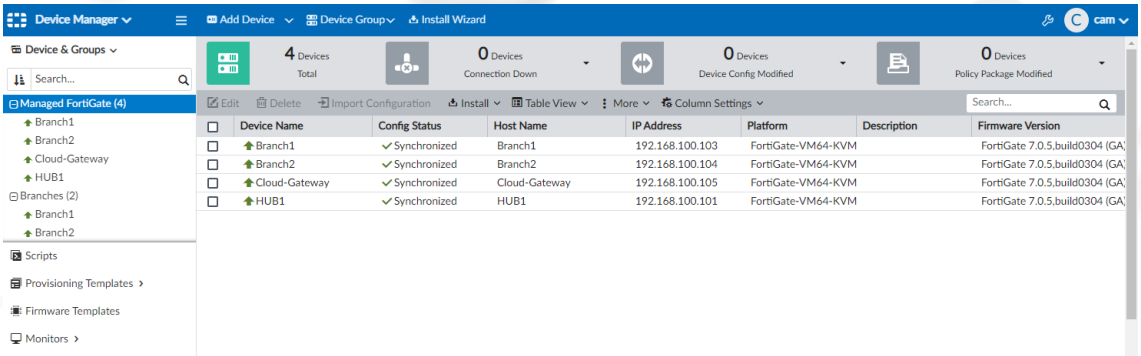
This guide presumes the following prerequisites have been met:

- 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:

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

Configuration steps

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

1. Configure the overlay using the SD-WAN overlay template. See Creating an overlay template on page 3.
2. Assign metadata values to branch devices. See Assigning meta data values to branch devices on page 7.
3. Configure SD-WAN rules. See Configuring SD-WAN rules on page 7.
4. Create normalized interfaces. See Creating normalized interfaces on page 10.

5. Create policy packages and firewall policies for hub and branch devices. See Creating policy packages and firewall policies on page 11.
6. Install policy packages to devices. See Installing policy packages on page 16.
7. Verify the SD-WAN configuration. See Verifying the SD-WAN configuration on page 19.

Creating an overlay template

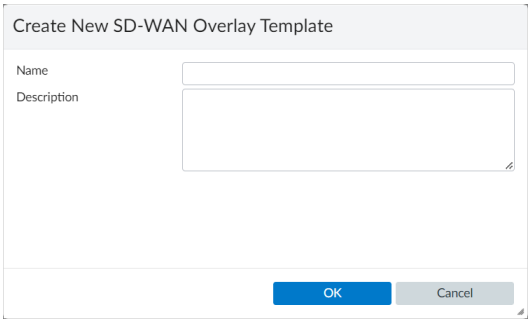
This section describes how to use the SD-WAN overlay template to configure the overlay network.

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

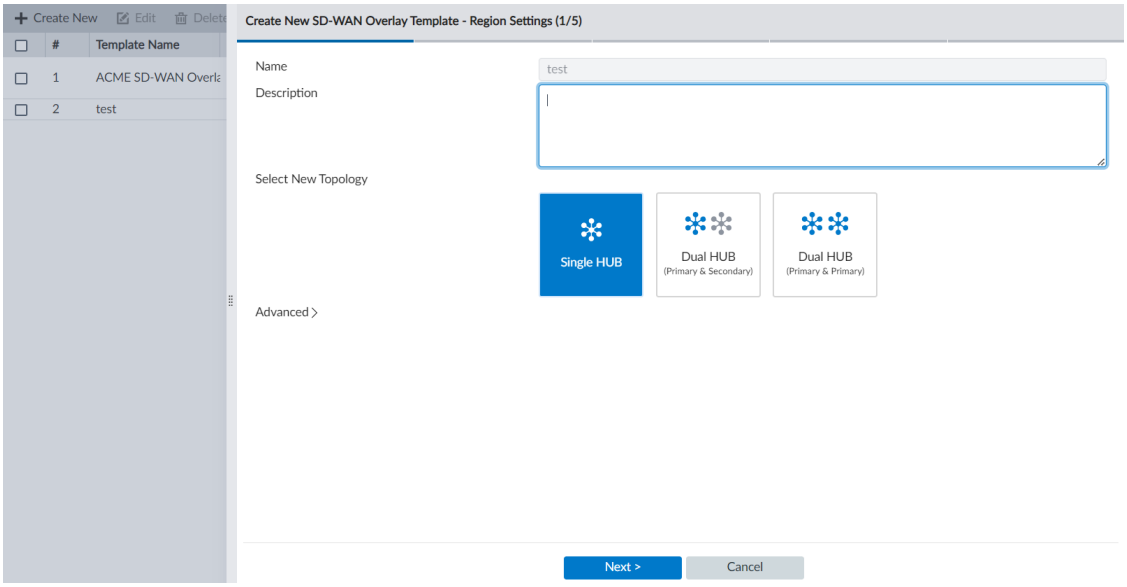
For more information, see the *FortiManager 7.2 Administration Guide*.

To create an overlay template:

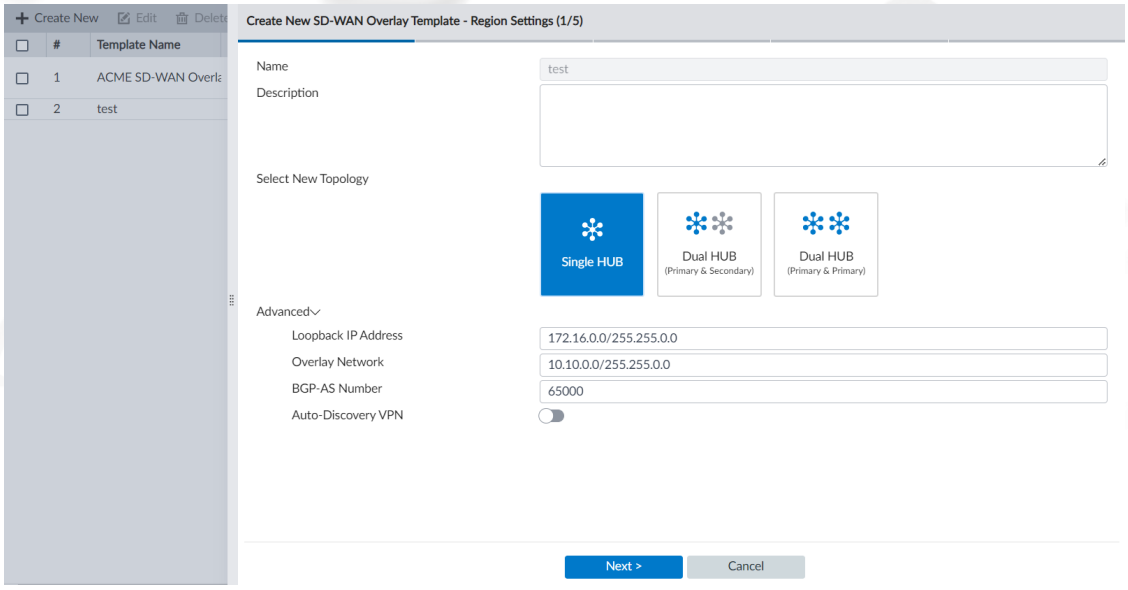
1. In FortiManager, go to *Device Manager* > *Provisioning Templates* > *SD-WAN Overlay Templates*.
2. Click *Create New*. The *Create New SD-WAN Overlay Template* dialog box is displayed.



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

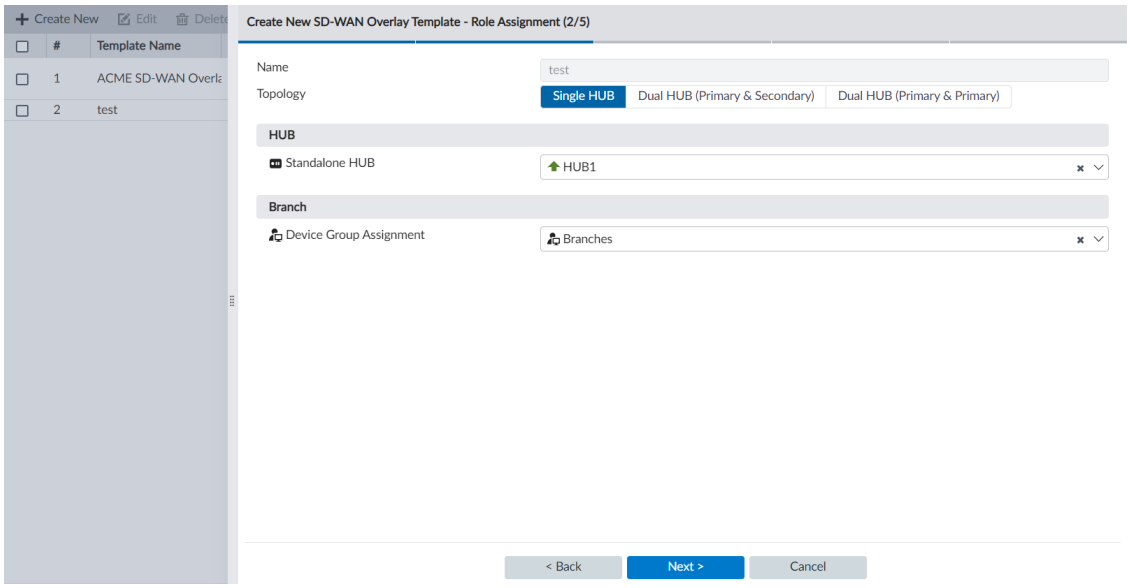


c. Click *Next*.The *Role Assignment* pane is displayed.

5. Set the role assignment:

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

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



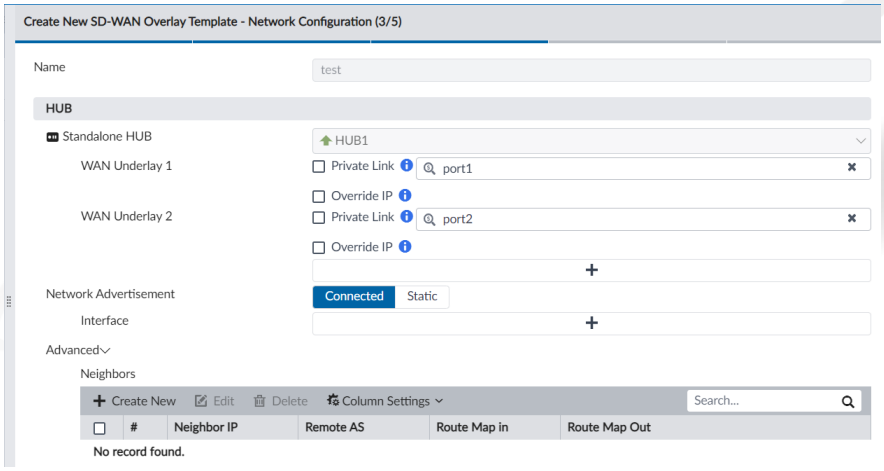
c. Click *Next*. The *Network Configuration* pane is displayed.

6. Set the network configuration for the HUB:

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

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

c. Expand *Advanced*.



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

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

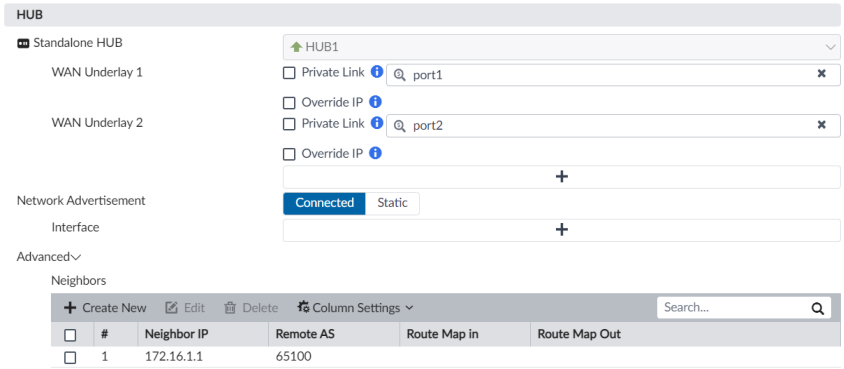
f. Set *Remote AS* to *65100*.

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

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

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

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

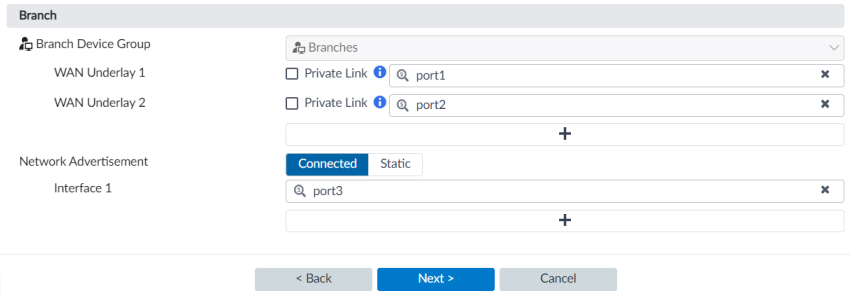


7. Set the network configuration for the branch device group:

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

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

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



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

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

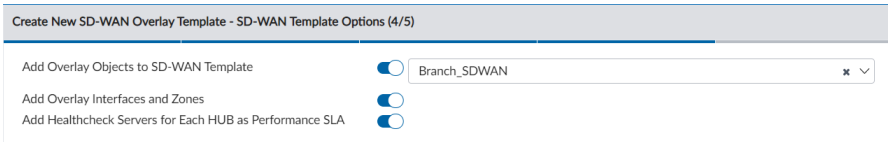
8. Set the SD-WAN template options:

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

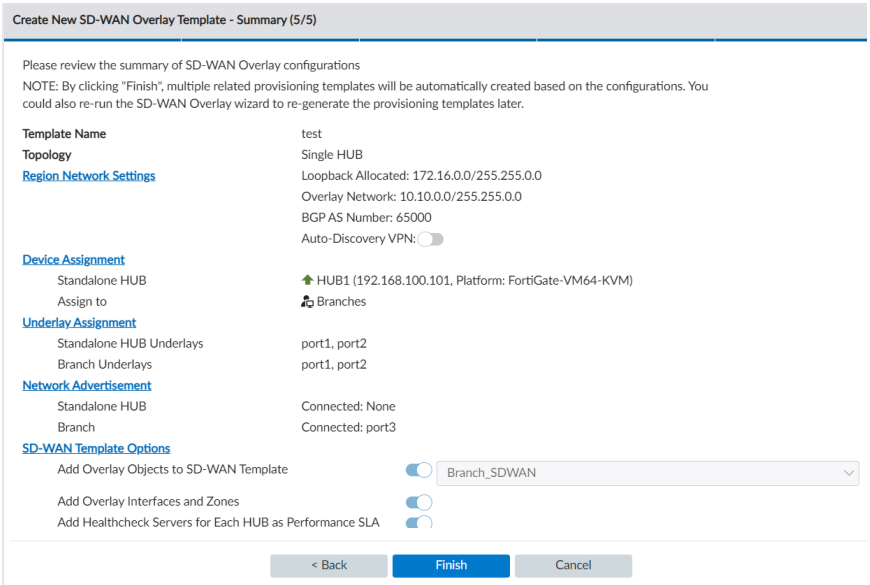
b. In the list, click *Create New* to create a new SD-WAN template named *Branch_SDWAN*. No configuration of the template is needed at this time.

c. Enable *Add Overlay Interfaces and Zones*.

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



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



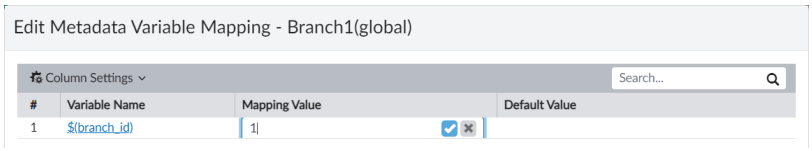
9. Click *Finish* to save the template.

Assigning meta data values to branch devices

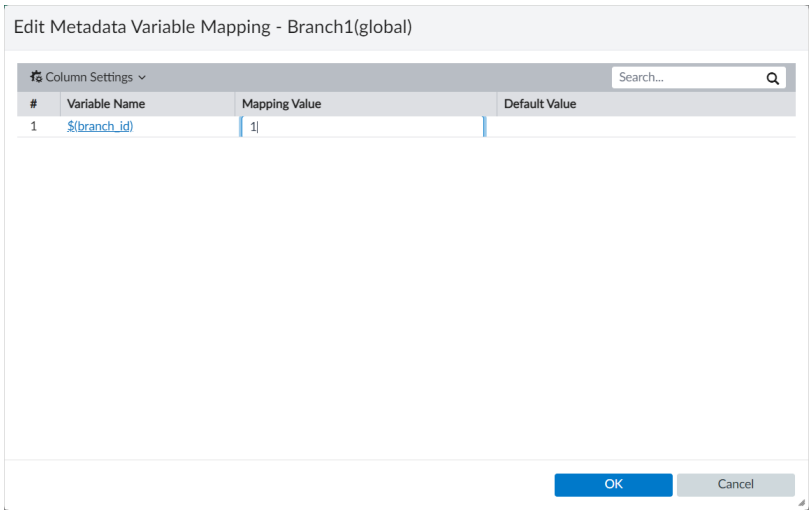
Each branch must have a unique *branch_id* mapping value in order to successfully utilize the SD-WAN overlay provisioning template.

To assign meta data values to branch devices:

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



   The value is set.



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

Configuring SD-WAN rules

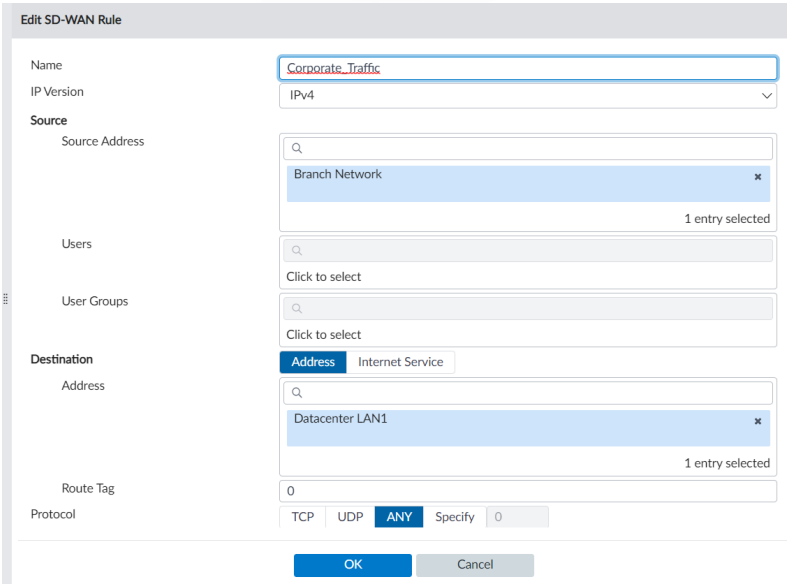
In this section we are going to edit the SD-WAN template to create a new performance SLA target as well as new SD-WAN rules.

To configure SD-WAN rules:

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

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

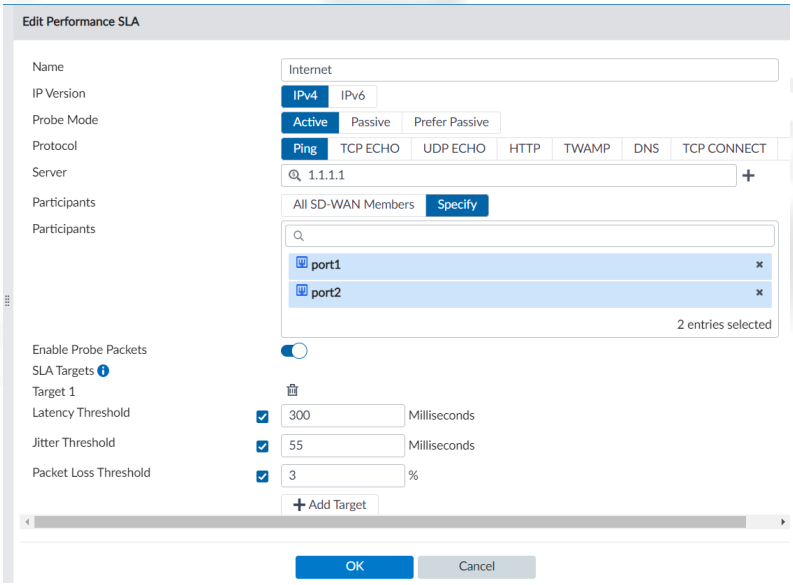
Name	Corporate_Traffic
Source	Branch Network, 10.1.0.0/16 (Create new Address Object)
Destination	Datacenter LAN1, 192.168.100.0/24 (Create new Address Object)
Strategy	Lowest Cost SLA
Interface Preference	HUB1-VPN1, HUB1-VPN2
Required SLA Target	HUB1_HC#1



   The SD-WAN rule is created.

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

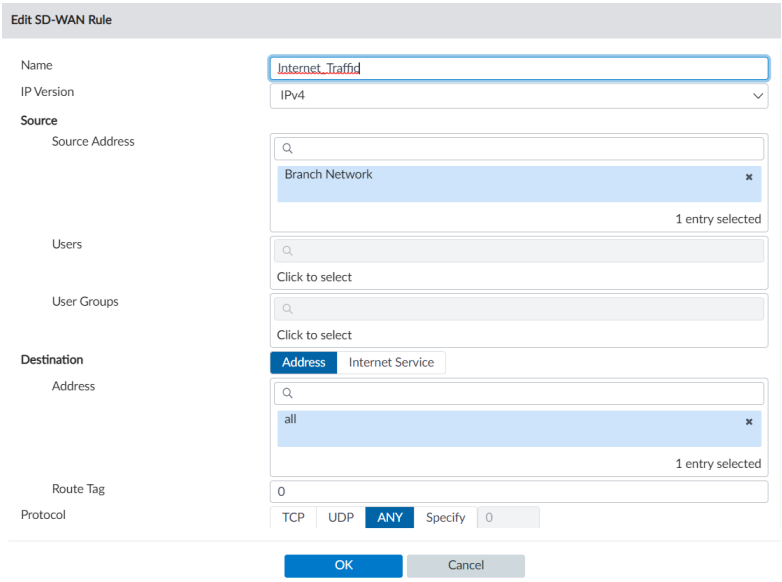
Name	Internet
Server	1.1.1.1
Participants	port1, port2
SLA Targets	• Latency threshold: 300 • Jitter Threshold: 55 • Packet Loss Threshold: 3%



The SLA target is created.

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

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



The SD-WAN rule is created.

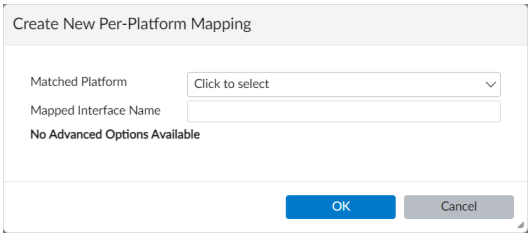
6. Click *OK* to save the SD-WAN template.

Creating normalized interfaces

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

To create normalized interfaces:

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



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

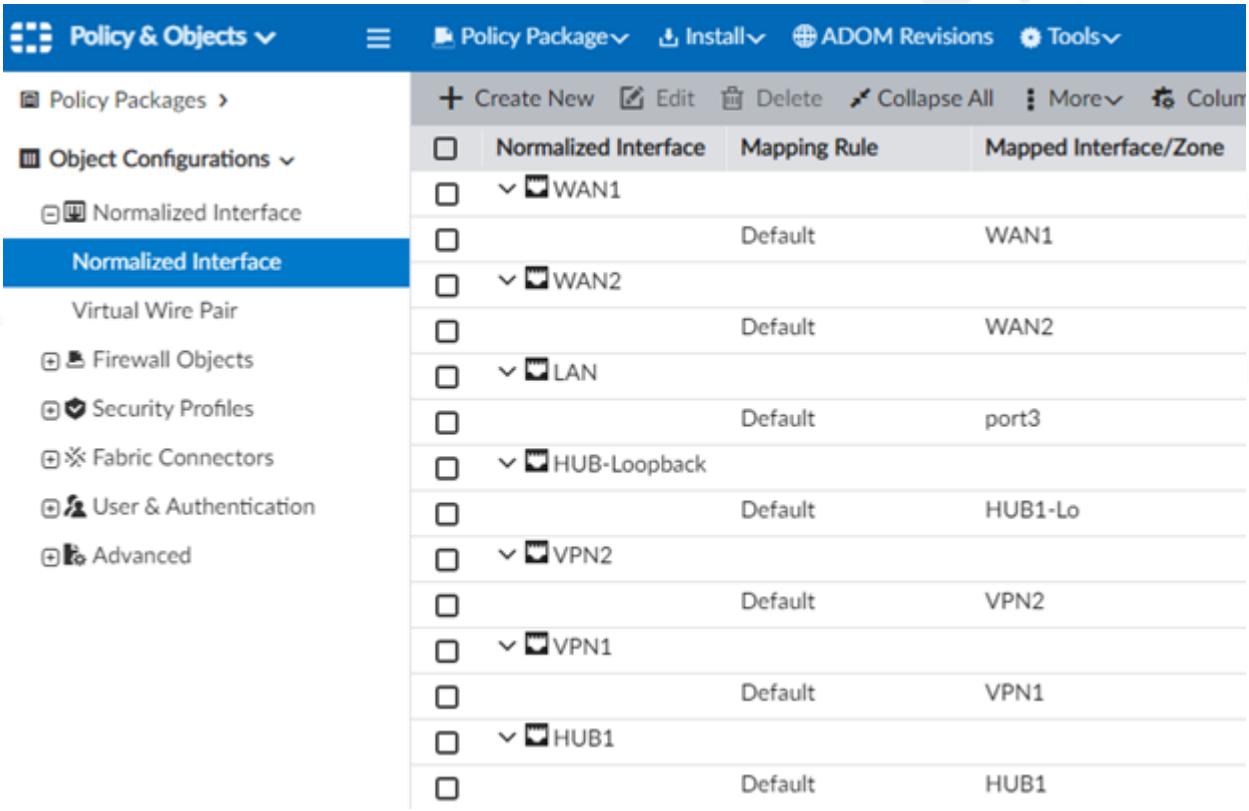
Matched Platform	Select *all*.
Mapped Interface Name	Type *HUB1*.

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

   The per-platform mapping is created.
6. Repeat this procedure to the following per-platform mappings:

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

All the per-platform mappings are created:



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.

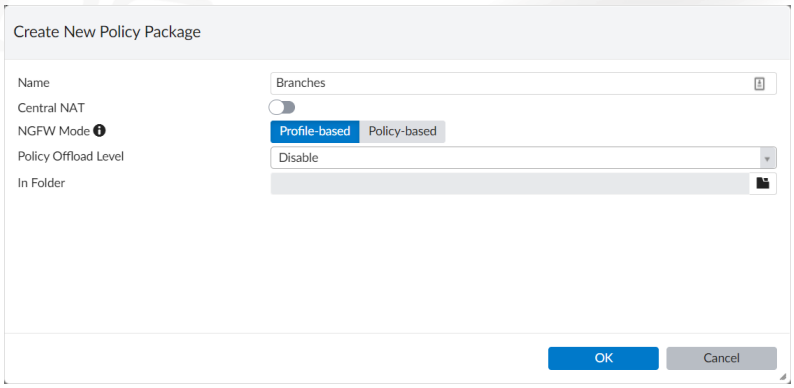
Following is a summary of how to create the policy package:

1. Create a policy package for branch devices. See Creating the branch policy package and policies on page 12.
   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 14.

Creating the branch policy package and policies

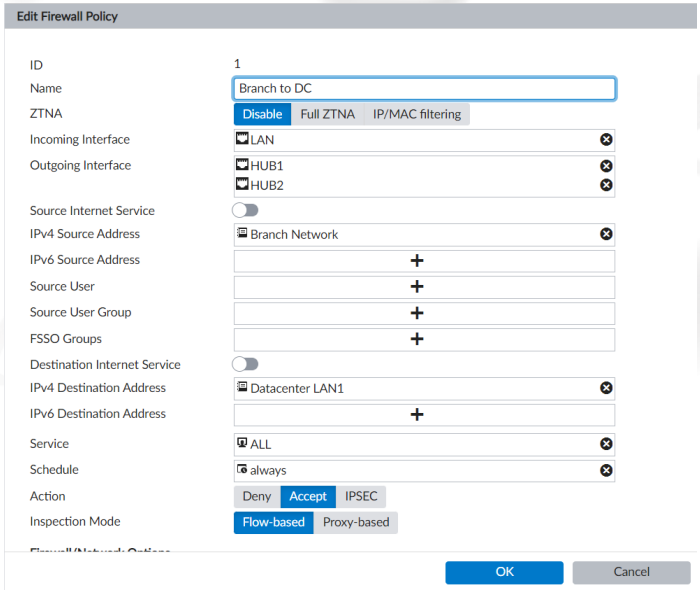
To create the branch policy package and policies:

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



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

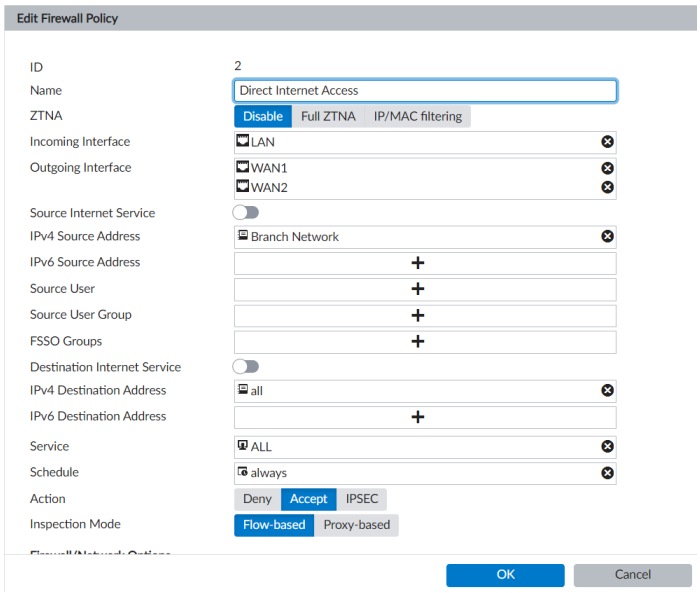
Name	Branch to DC
Incoming Interface	LAN
Outgoing Interface	HUB1
IPv4 Source Address	Branch network
IPv4 Destination Address	Datacenter LAN1
Action	Accept



The firewall policy is created.

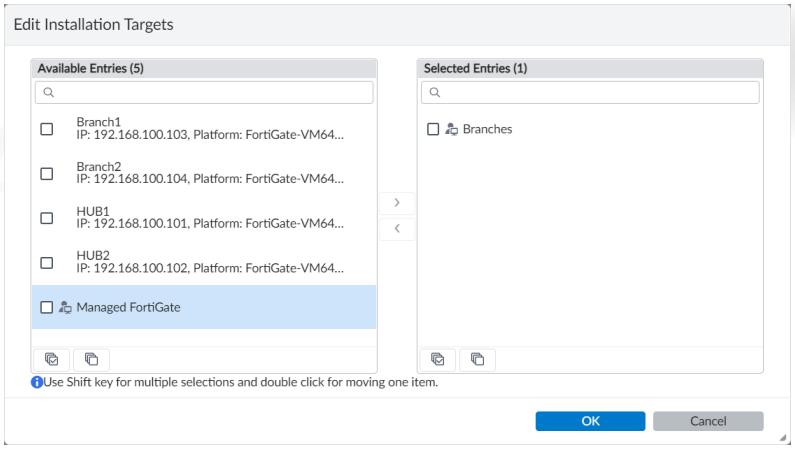
4. In the branches policy package, create a firewall policy named *Direct Internet Access*:
   a. Select the *Branches* policy package, and click *Create New*. The *Create New Firewall Policy* pane opens.
   b. Set the following options, and click *OK*:

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



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.



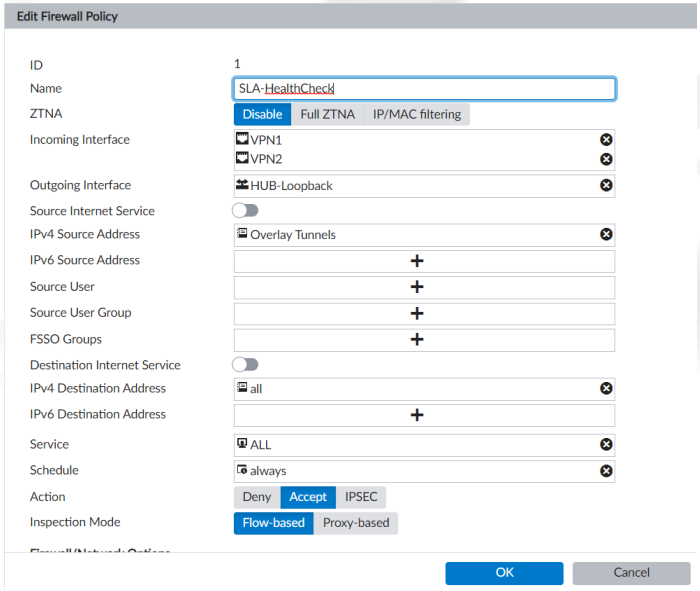
   d. Click OK.
      The installation target for the branches policy package is the *Branches* device group.

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*:

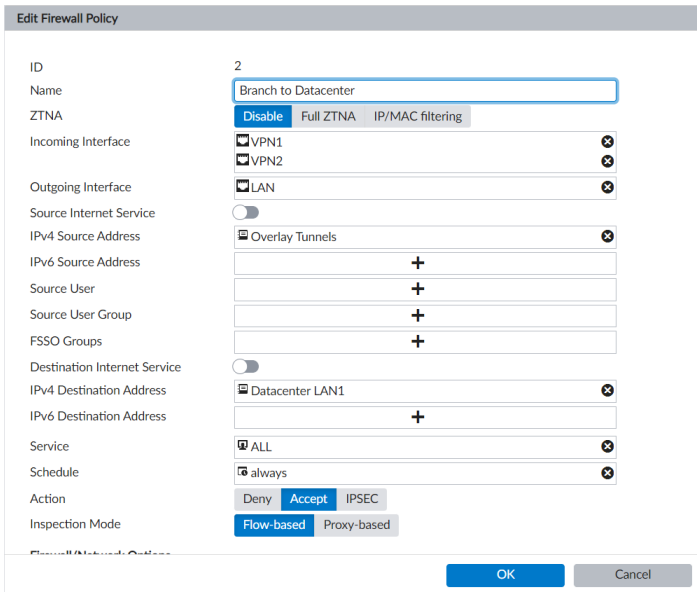
Name	SLA-HealthCheck
Incoming Interface	VPN1, VPN2
Outgoing Interface	HUB-Lo
IPv4 Source Address	Overlay Tunnels, 10.10.0.0/16 (create new address object)
IPv4 Destination Address	all
Action	Accept



The firewall policy is created.

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

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

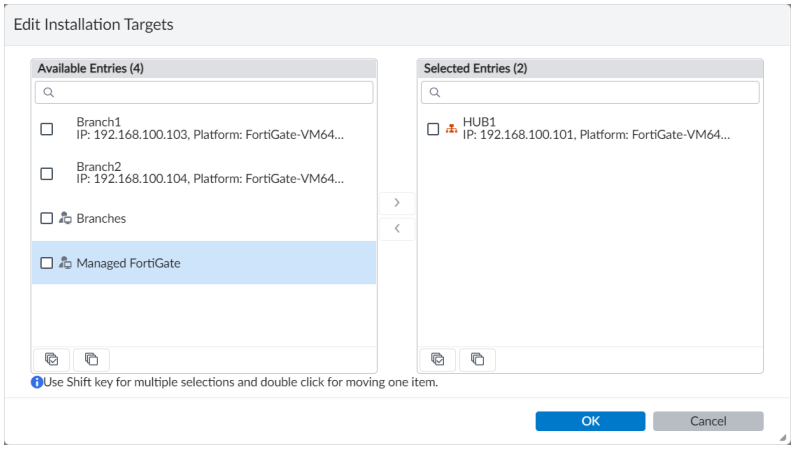


The firewall policy is created.

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

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

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



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

Installing policy packages

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

1. Install the HUB policy package to the HUB1 device. See Installing the HUB policy package on page 16.
2. Install the branch policy package to branch device group. See Installing the branch policy package on page 18.

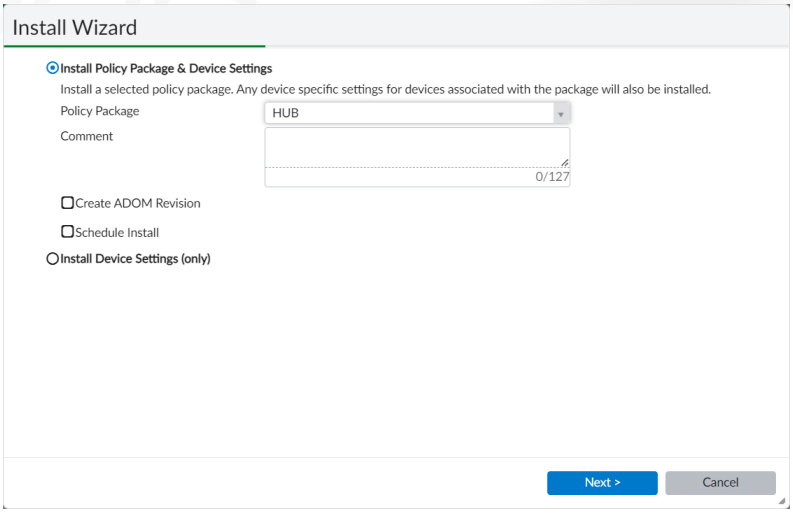
Installing the HUB policy package

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

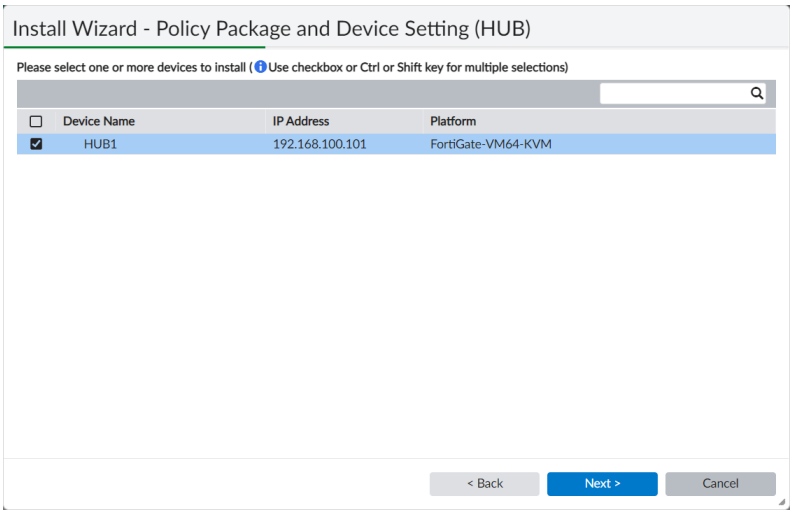
To install the HUB policy package:

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*:

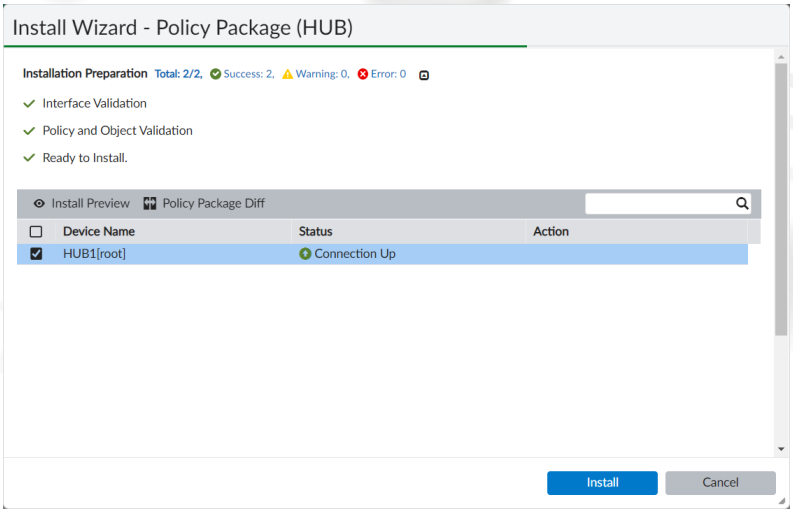
Install Policy Package & Device Settings	Select
Policy Package	HUB



The wizard moves to the next screen:



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



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*.

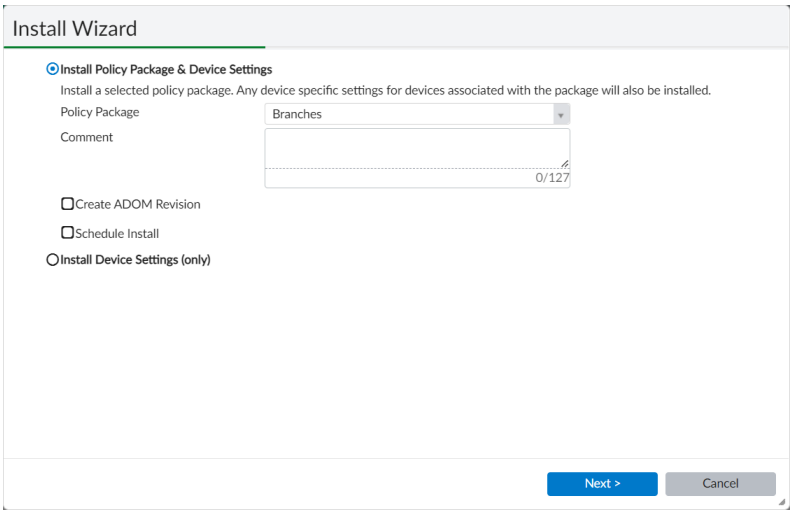
Installing the branch policy package

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

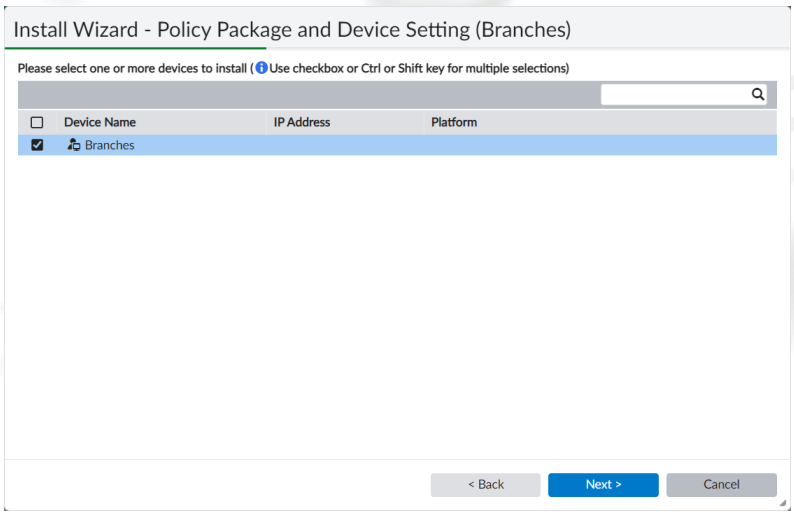
To install the branch policy package:

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



The wizard moves to the next screen:



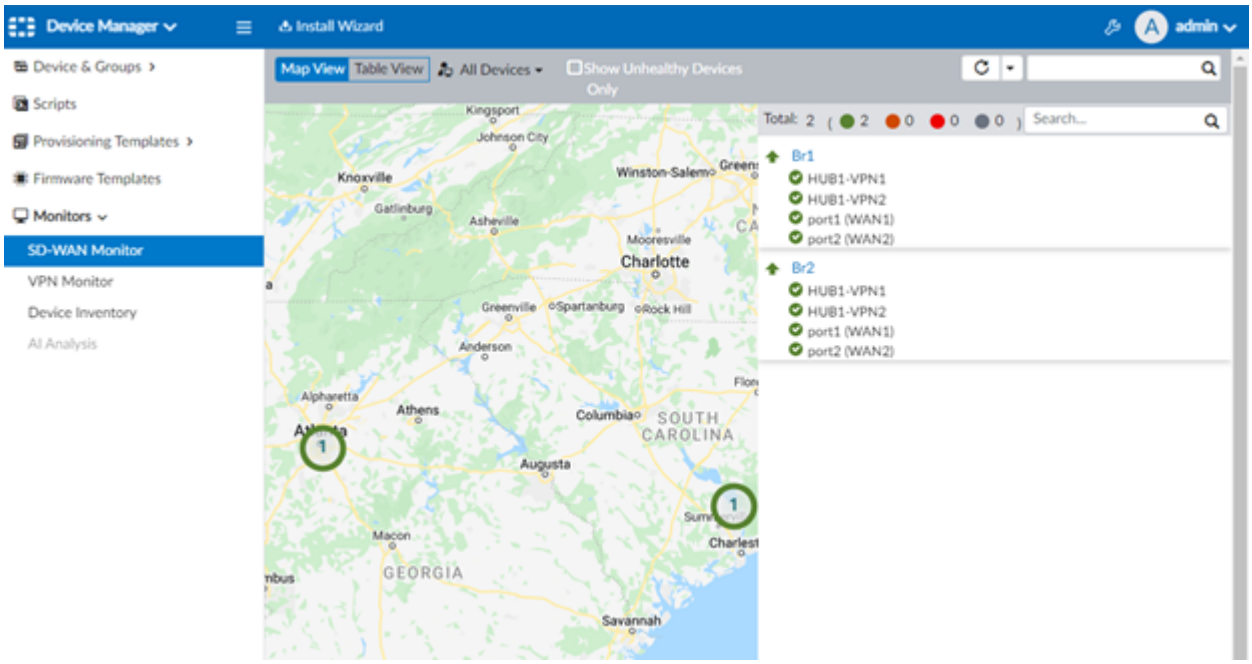
3. Verify that *Branches* is selected, and click *Next*.
   The wizard moves to the installation preparation page. When the installation preparation completes, you should see three, green checkmarks that indicate the policy package is ready to install.
4. Review the page, and click *Install*.
   You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

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.



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.