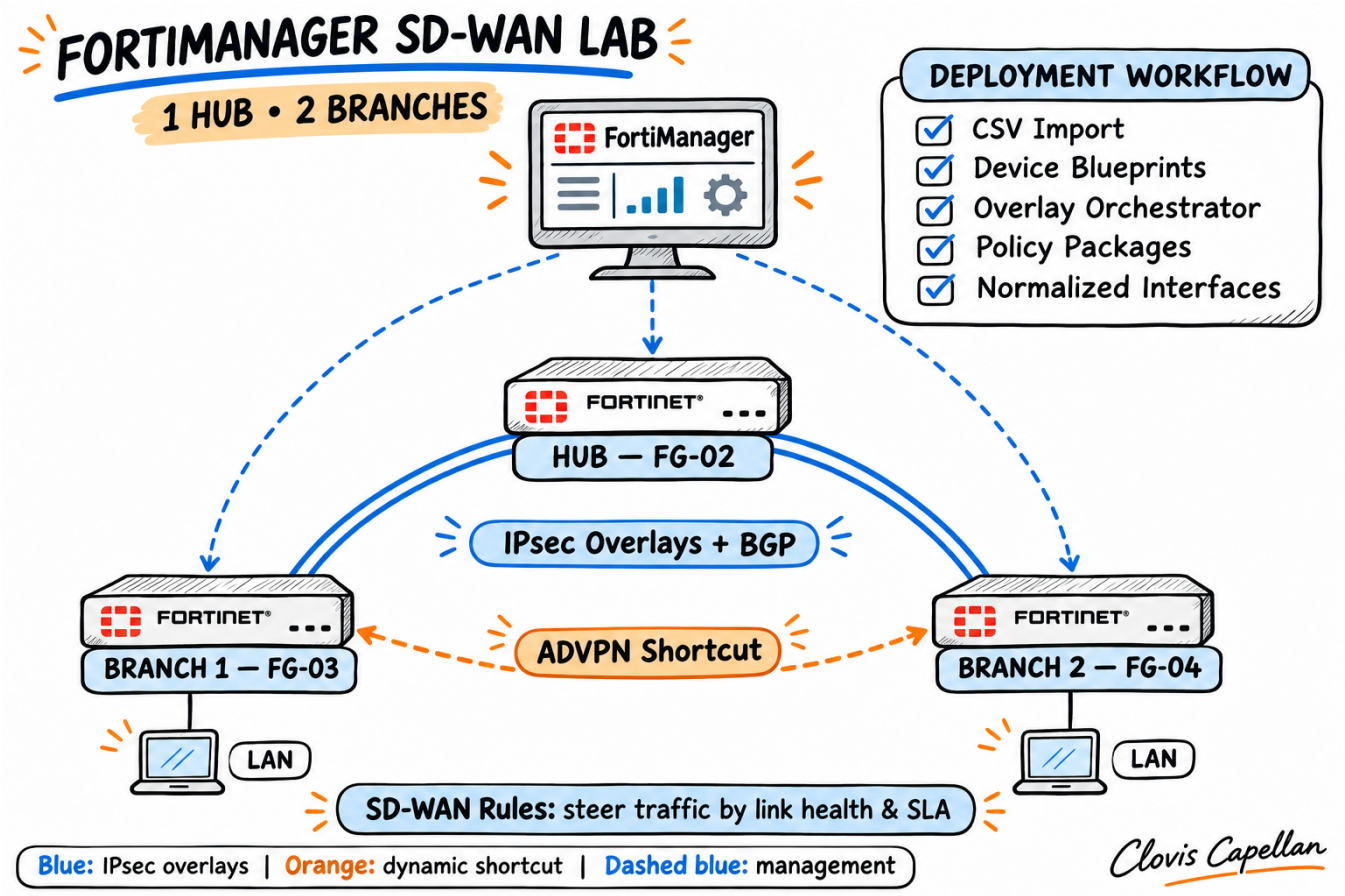
FortiManager SD-WAN Lab

ADVPN 2.0 with BGP on loopbacks • Clovis Capellan



Configuration walkthrough

One FortiGate hub and two branches, with two WAN underlays per site. This walkthrough follows the lab from model-device provisioning through policy installation and shortcut verification.

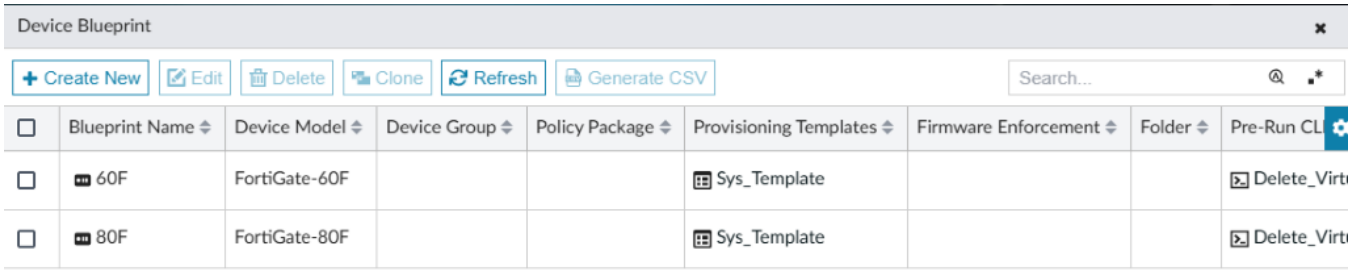
Device	Role	LAN	BGP loopback
FG-02 · 80F	Hub	10.10.2.0/24	172.16.255.252
FG-03 · 60F	Branch 1	10.10.3.0/24	172.16.0.1
FG-04 · 60F	Branch 2	10.10.4.0/24	172.16.0.2

Device Blueprints

FortiManager lab configuration and verification

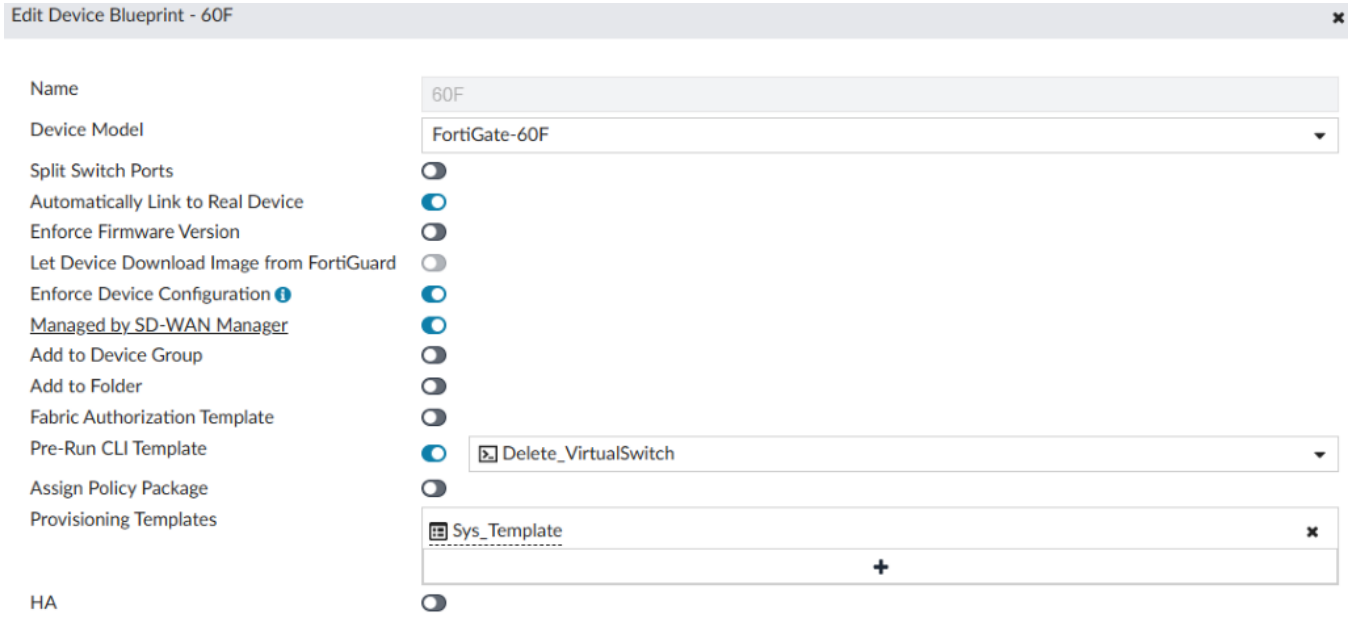
01.01

Create separate 60F and 80F Device Blueprints. Both reference the Sys_Template provisioning template.



01.02

Enable Automatically Link to Real Device, Enforce Device Configuration and Managed by SD-WAN Manager. Attach Delete_VirtualSwitch as the Pre-Run CLI Template. Repeat for the 80F blueprint with its matching device model.

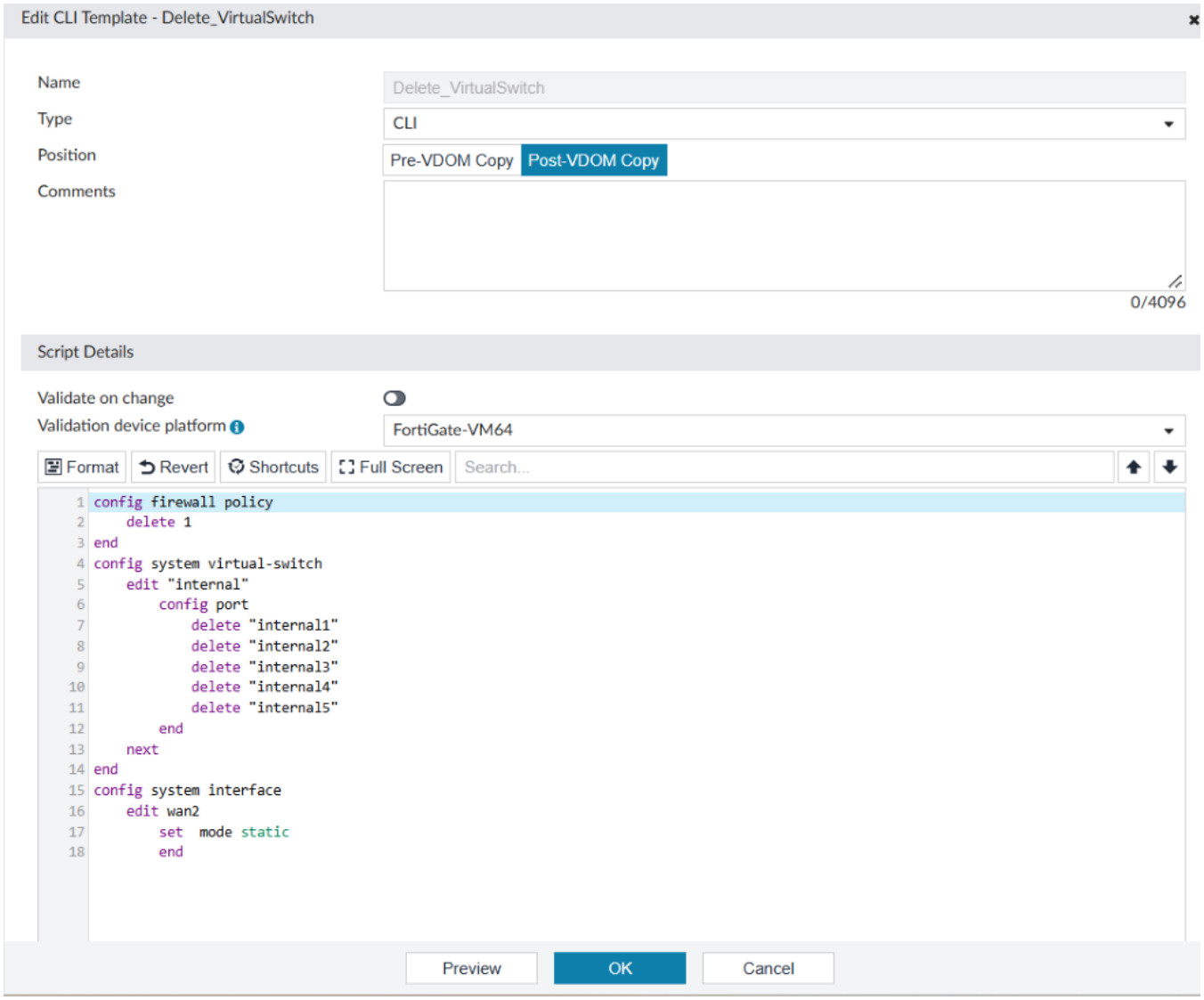


Device Blueprints

FortiManager lab configuration and verification

01.03

Create the pre-run CLI template. Set WAN1 to DHCP for bootstrap and WAN2 to static. Remove internal1 through internal5 from the internal switch so the system template can configure the ports individually.

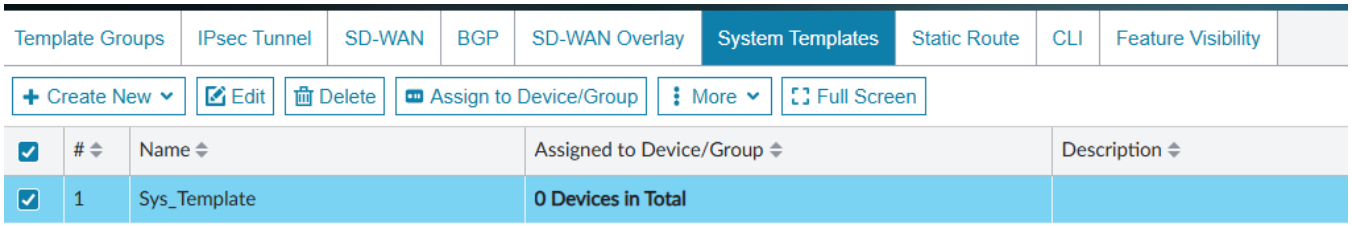


System template and metadata

FortiManager lab configuration and verification

02.01

Open the System Templates tab and create Sys_Template.

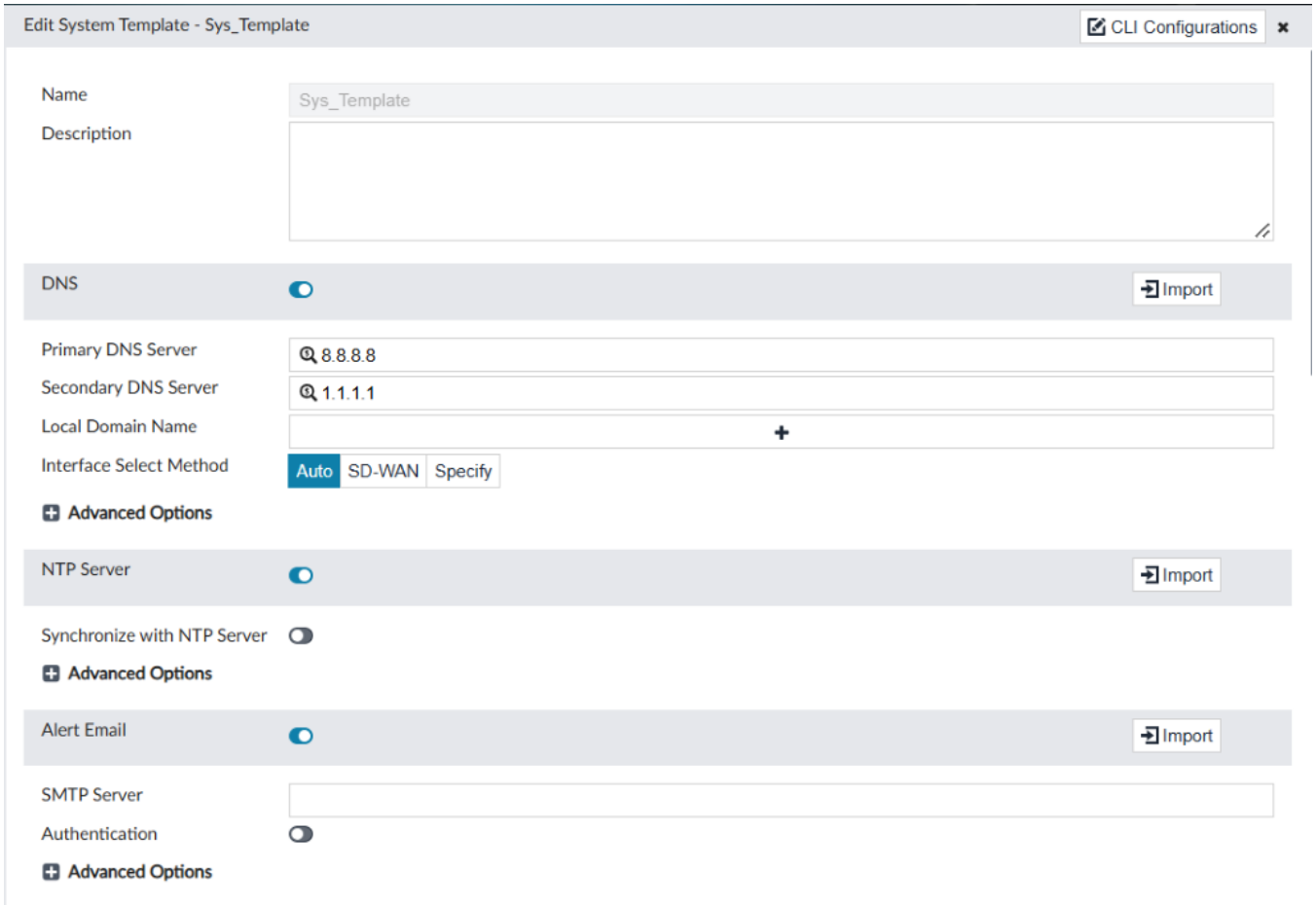


System template and metadata

FortiManager lab configuration and verification

02.02

Configure DNS in the system template using the values shown in the lab.

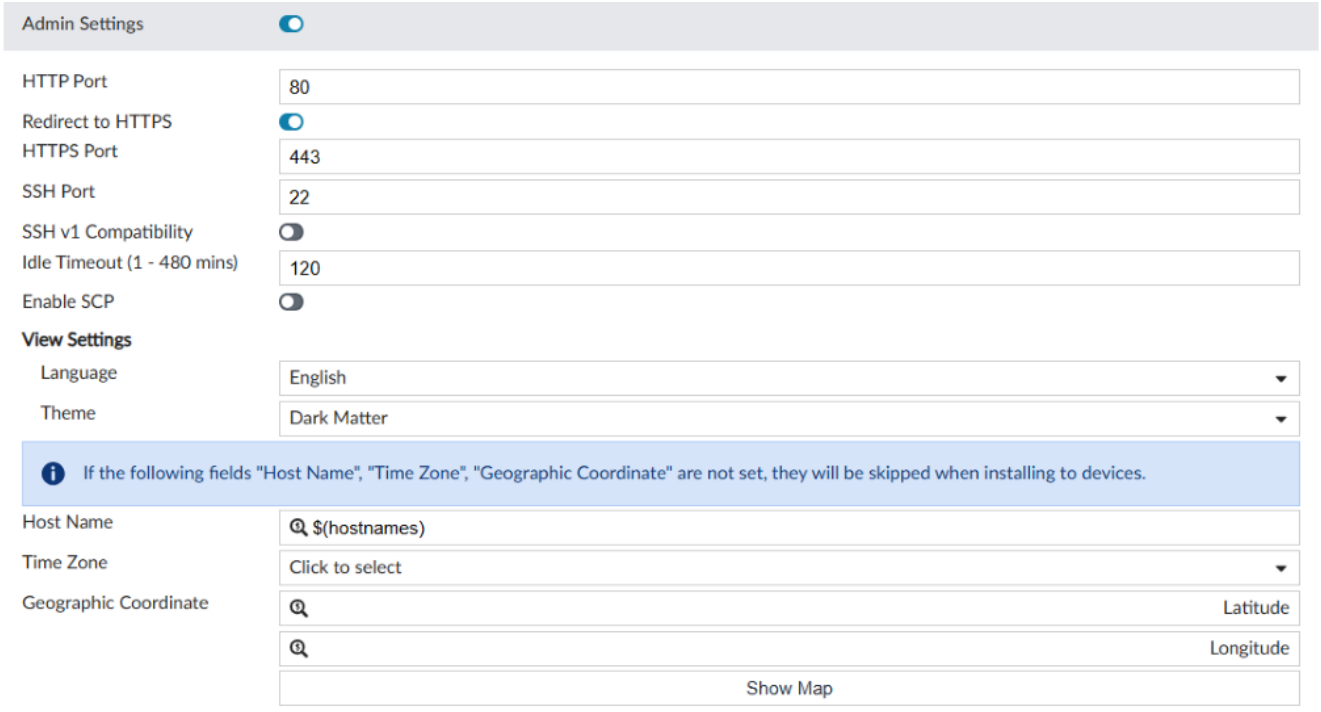


System template and metadata

FortiManager lab configuration and verification

02.03

Configure the hostname metadata reference and administrative idle timeout.

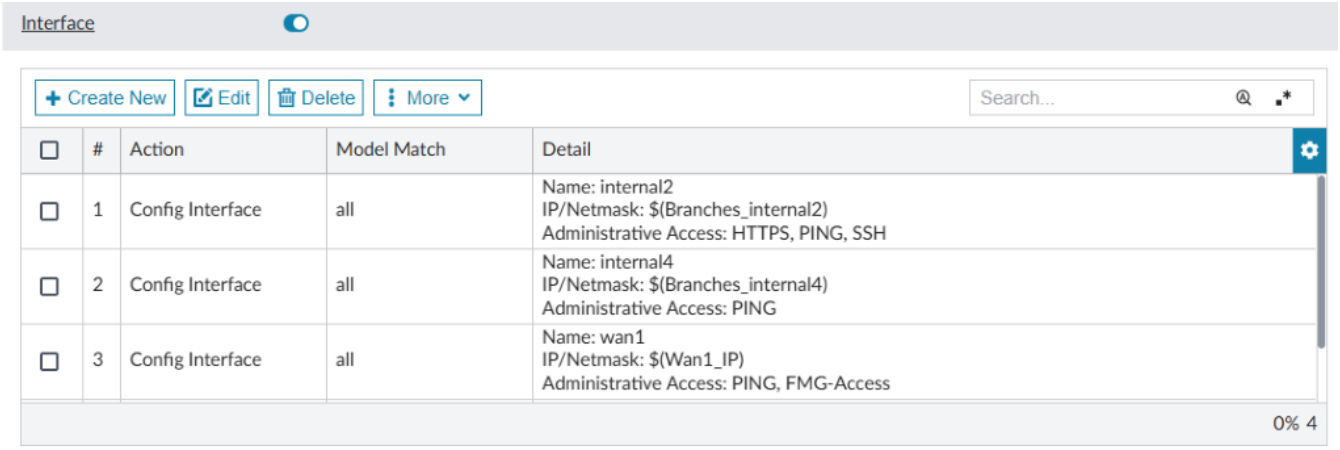


System template and metadata

FortiManager lab configuration and verification

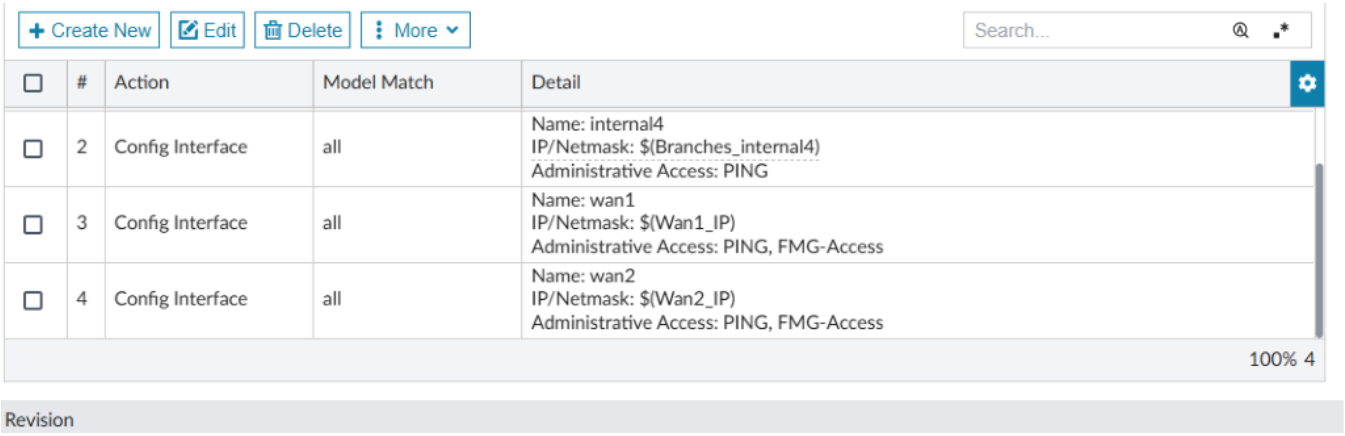
02.04

Configure internal2 and internal4 using the case-sensitive Branches_internal2 and Branches_internal4 variables. Set wan1 using Wan1_IP.



02.05

Set wan2 using Wan2_IP. The lab enables PING and FMG-Access on the WAN interfaces.



CSV import

FortiManager lab configuration and verification

03.01

Populate one CSV row per model device. Include the required Serial Number column and match the remaining fields to the exported headers. The serial number values are masked in this screenshot.

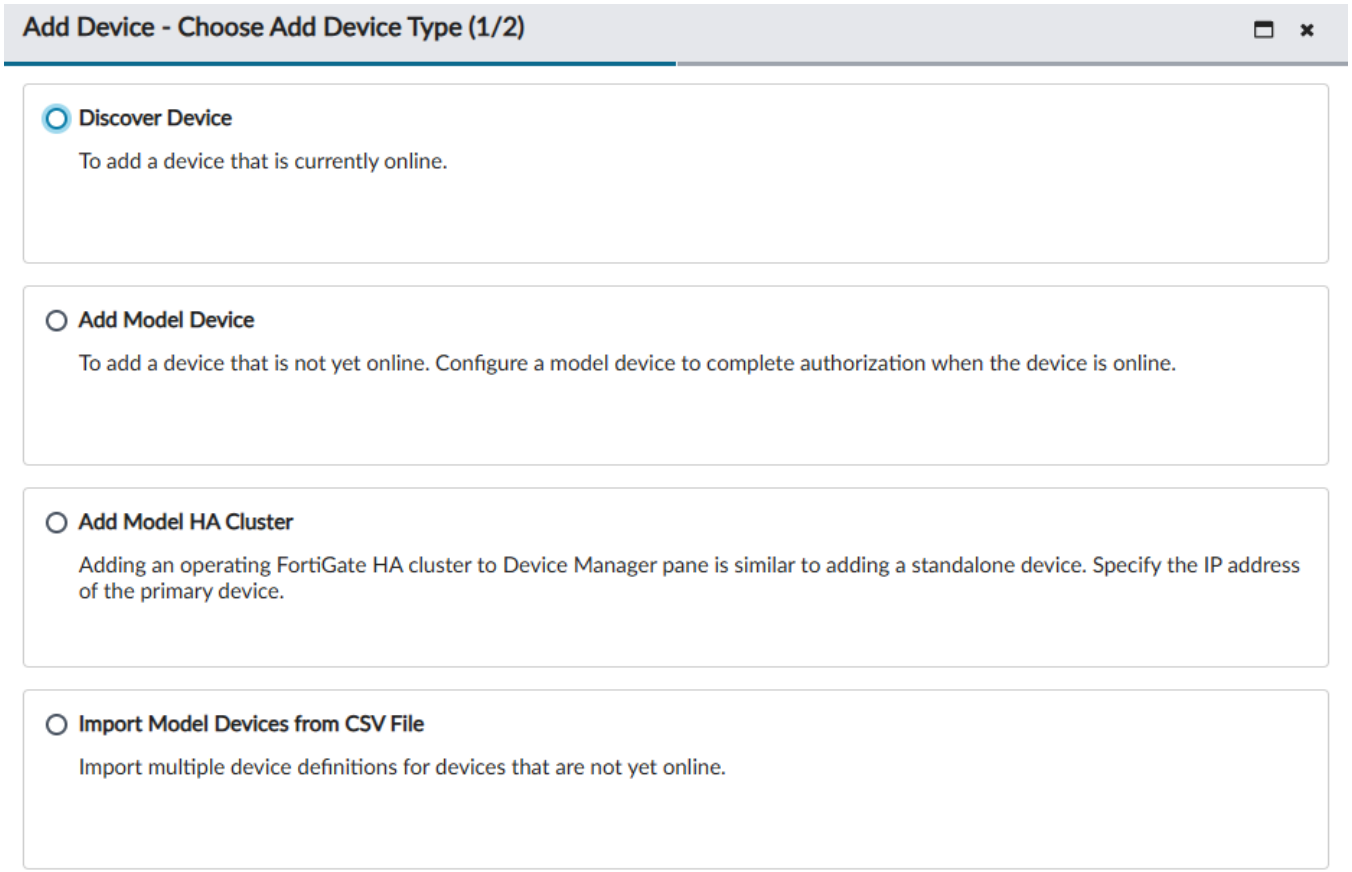
	A	B	C	D	E	F	G	H	I	J	K
1	serial number	device blueprint	name	Branches_Internal4	Wan1_IP	Wan2_IP	Branches_internal2	Branches_internal4	Wan1_GW	Wan2_GW	hostnames
2	[redacted]	80F	FG-02	internal4	35.1.2.2/30	40.1.2.2/30	192.168.99.2/24	10.10.2.1/24	35.1.2.1	40.1.2.1	FG-02
3		60F	FG-03	internal4	45.32.54.2/30	55.64.1.2/30	192.168.99.3/24	10.10.3.1/24	45.32.54.1	55.64.1.1	FG-03
4		60F	FG-04	internal4	66.31.1.2/30	43.64.1.2/30	192.168.99.4/24	10.10.4.1/24	66.31.1.1	43.64.1.1	FG-04
5											
6											

CSV import

FortiManager lab configuration and verification

03.02

Go to Device Manager → Device & Groups → Add Device. Select Import Model Devices from CSV File.

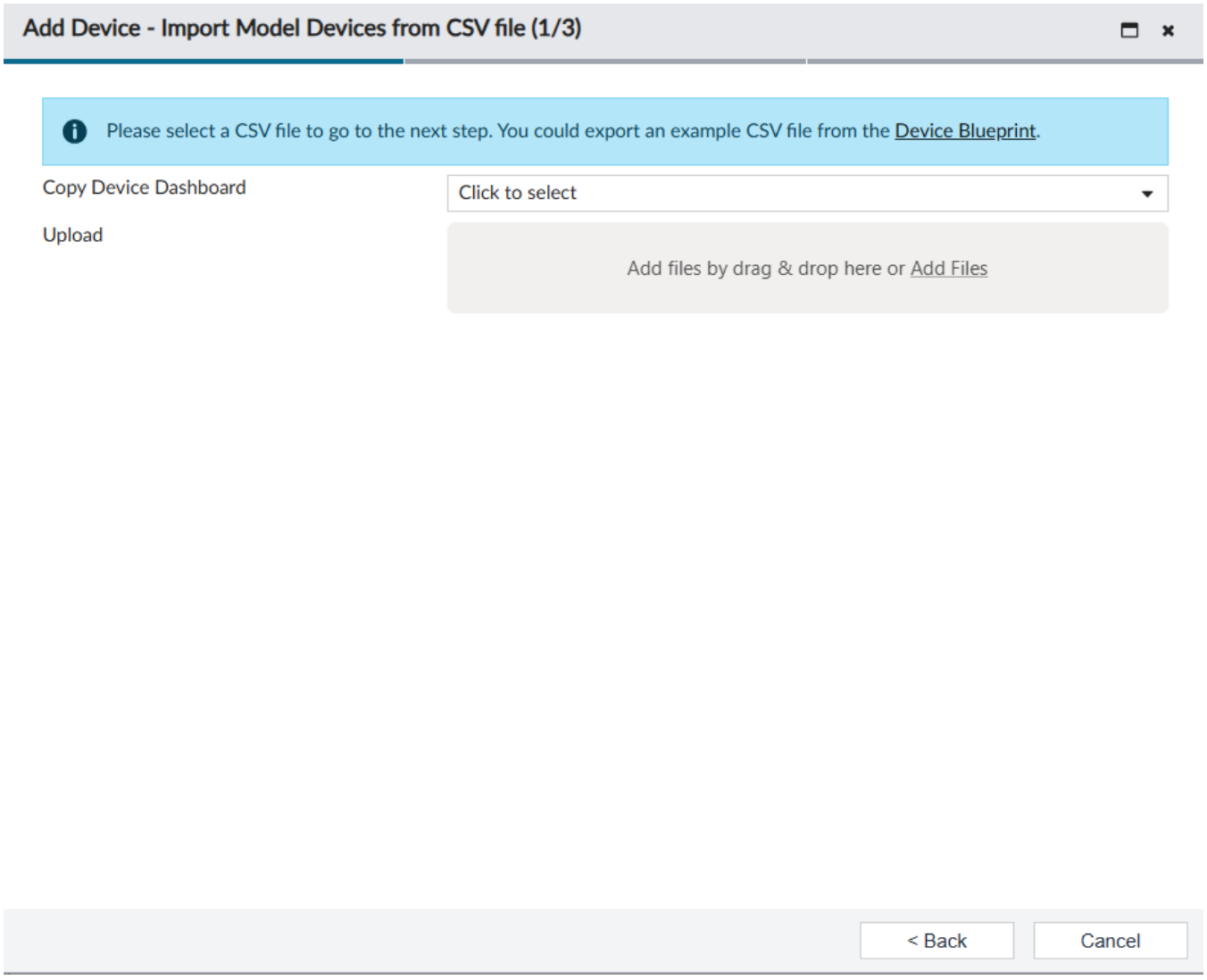


CSV import

FortiManager lab configuration and verification

03.03

Upload your populated CSV and complete the wizard. Check the device names and blueprint assignments. Model devices appear offline until the physical units link.

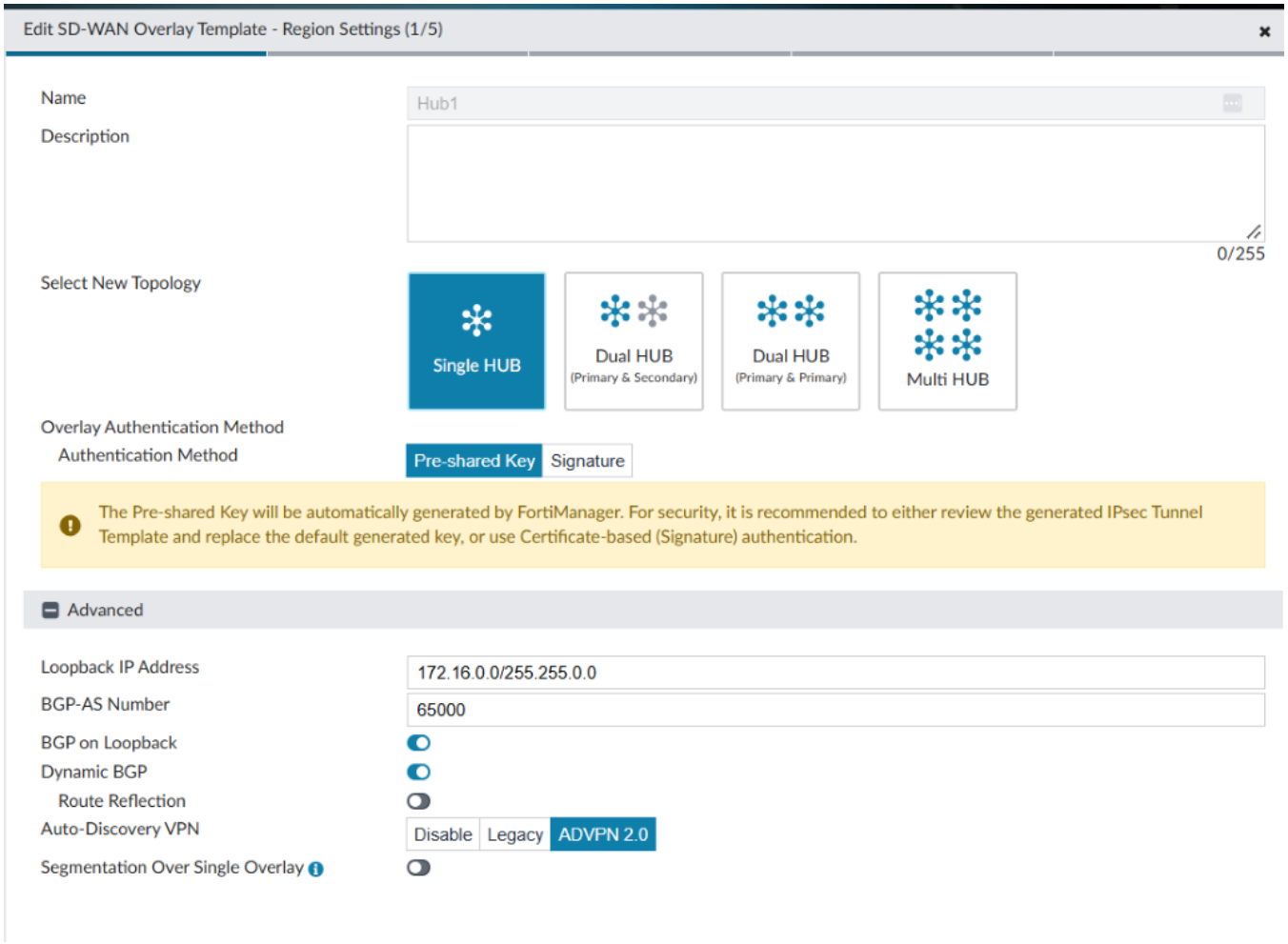


Overlay Orchestration

FortiManager lab configuration and verification

04.01

Create an overlay template and select Single HUB. Review the advanced settings for ADVPN and loopback BGP.

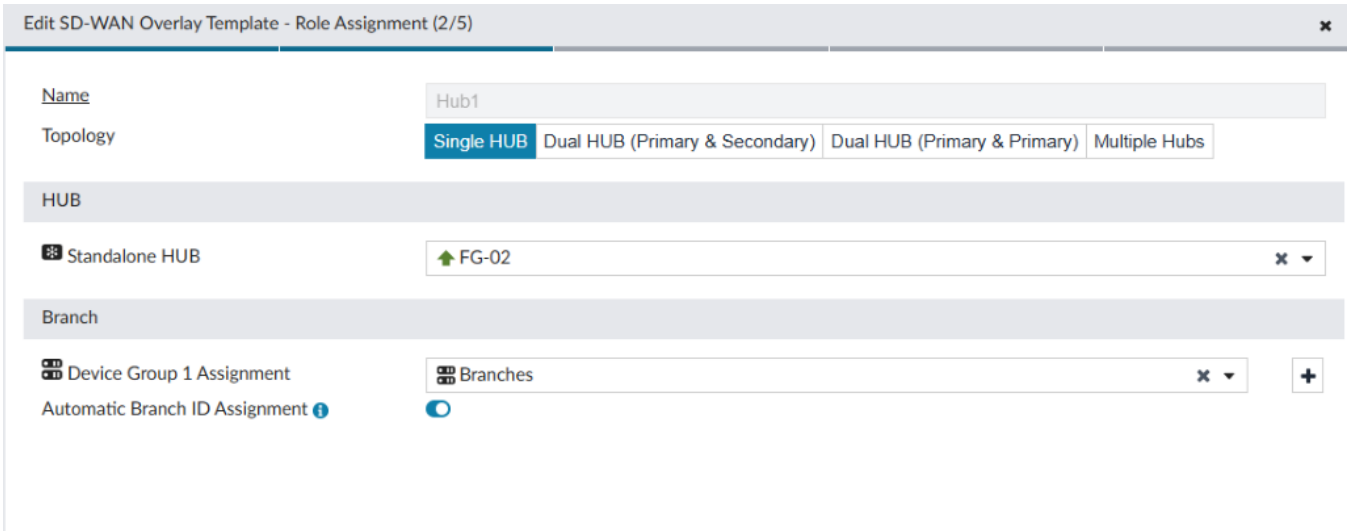


Overlay Orchestration

FortiManager lab configuration and verification

04.02

Assign FG-02 as the hub and the Branches device group as the spokes.

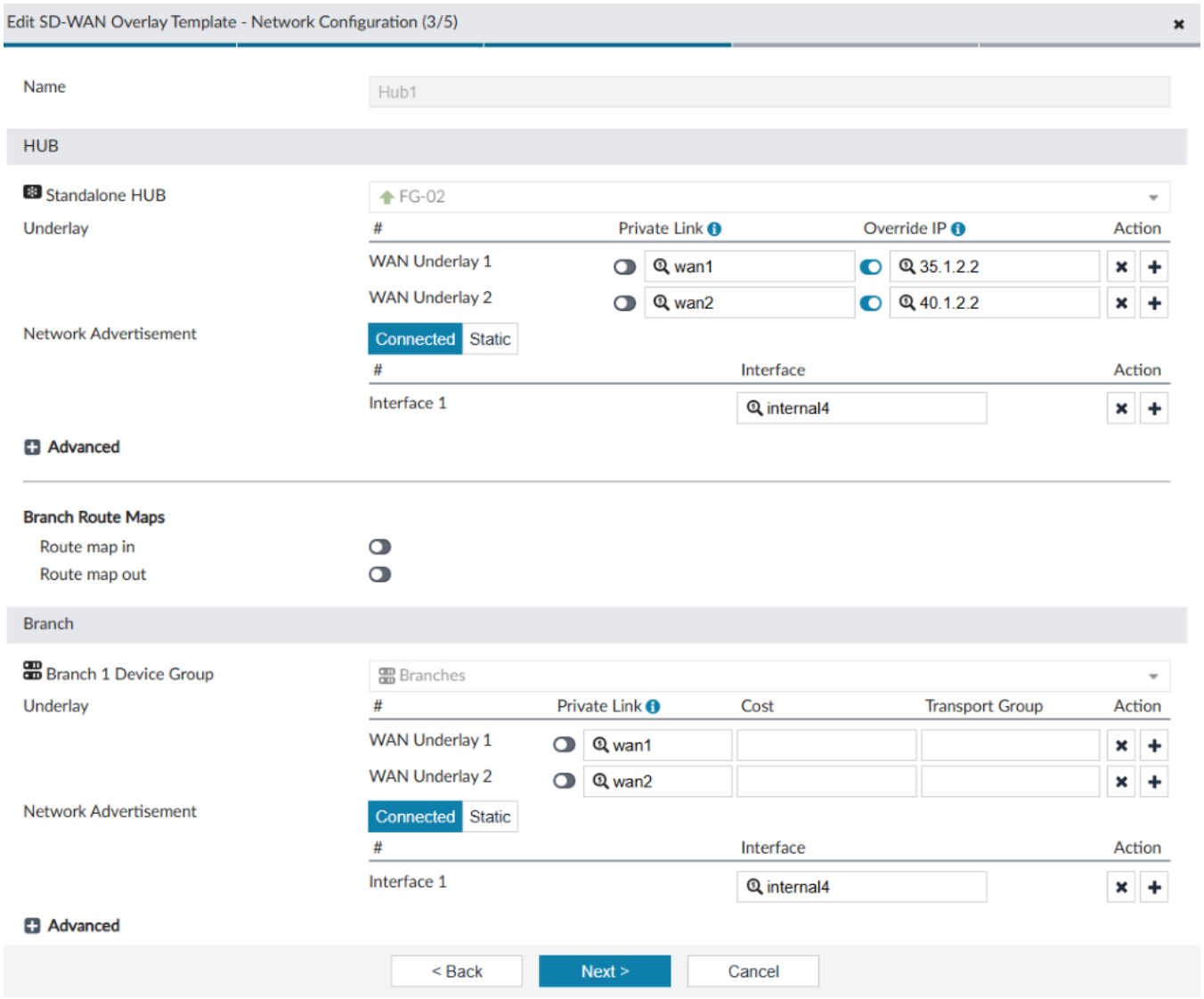


Overlay Orchestration

FortiManager lab configuration and verification

04.03

Map wan1 and wan2 as underlays. Enable Override IP for the hub WAN endpoints and enter the branch-reachable addresses. Add internal4 to branch network advertisements.

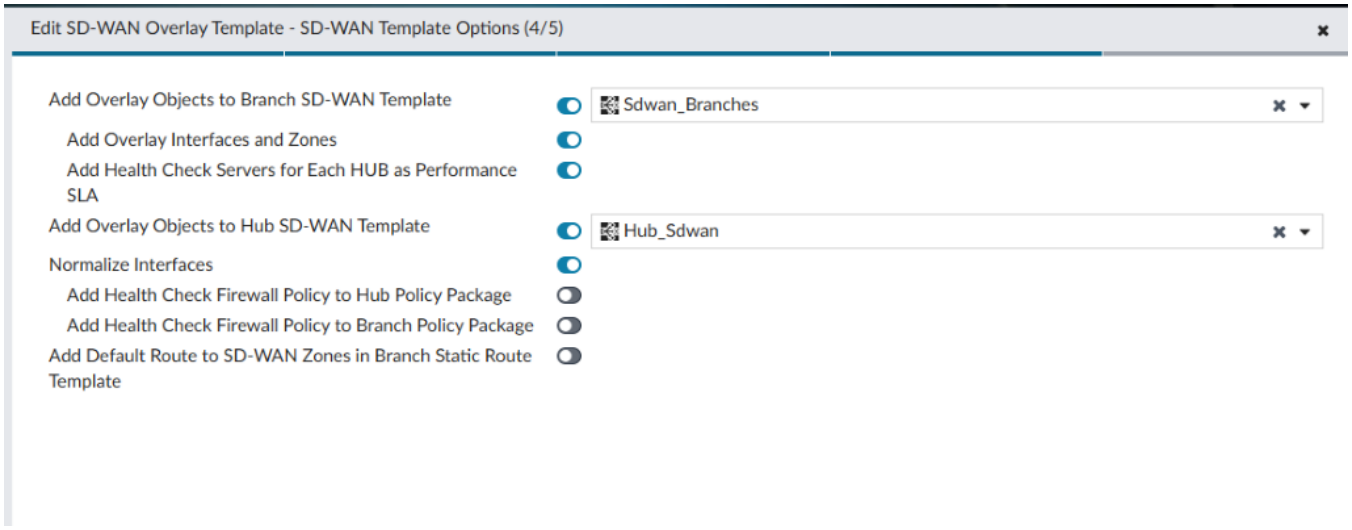


Overlay Orchestration

FortiManager lab configuration and verification

04.04

Select the branch and hub SD-WAN templates and review the overlay and normalization options. The hub SD-WAN template is part of this lab design.

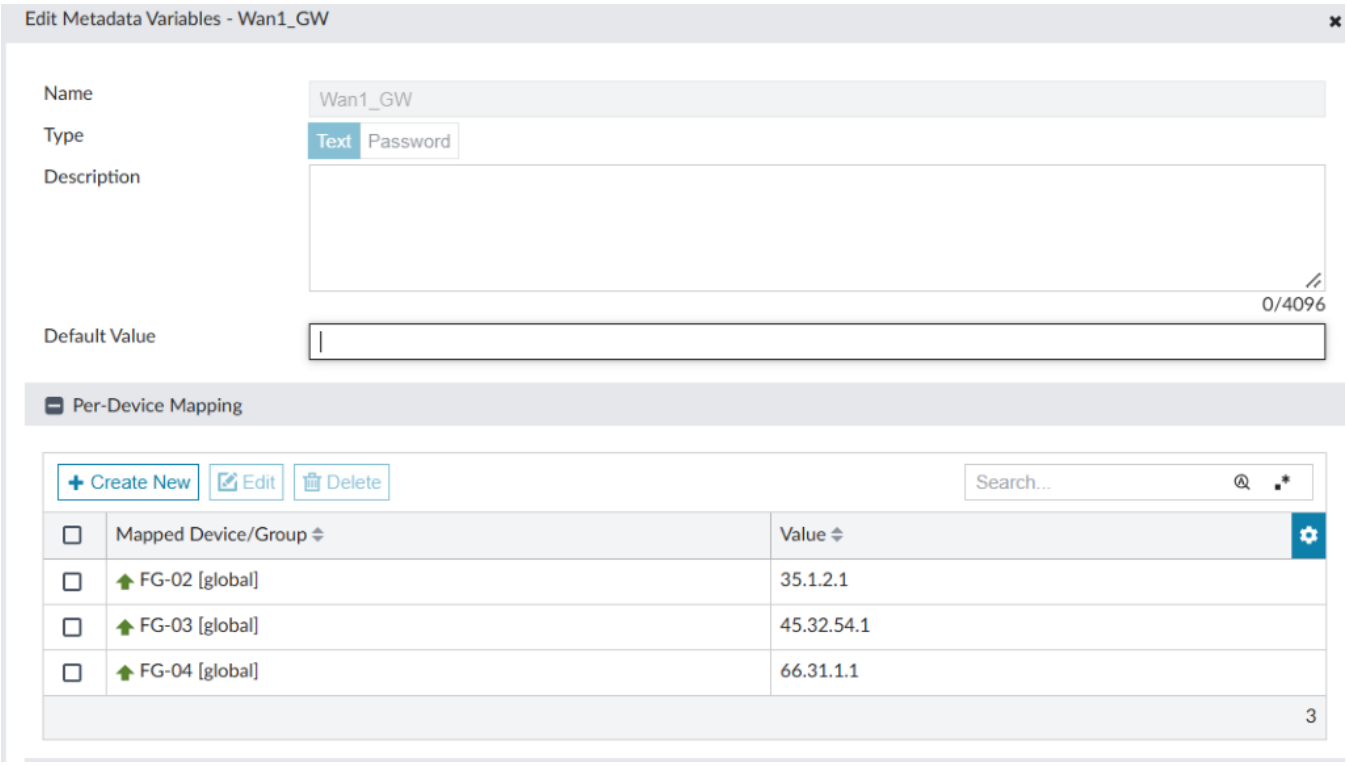


Branch SD-WAN

FortiManager lab configuration and verification

05.01

Create the Internet zone and add wan1. Use the site metadata variable for its gateway.

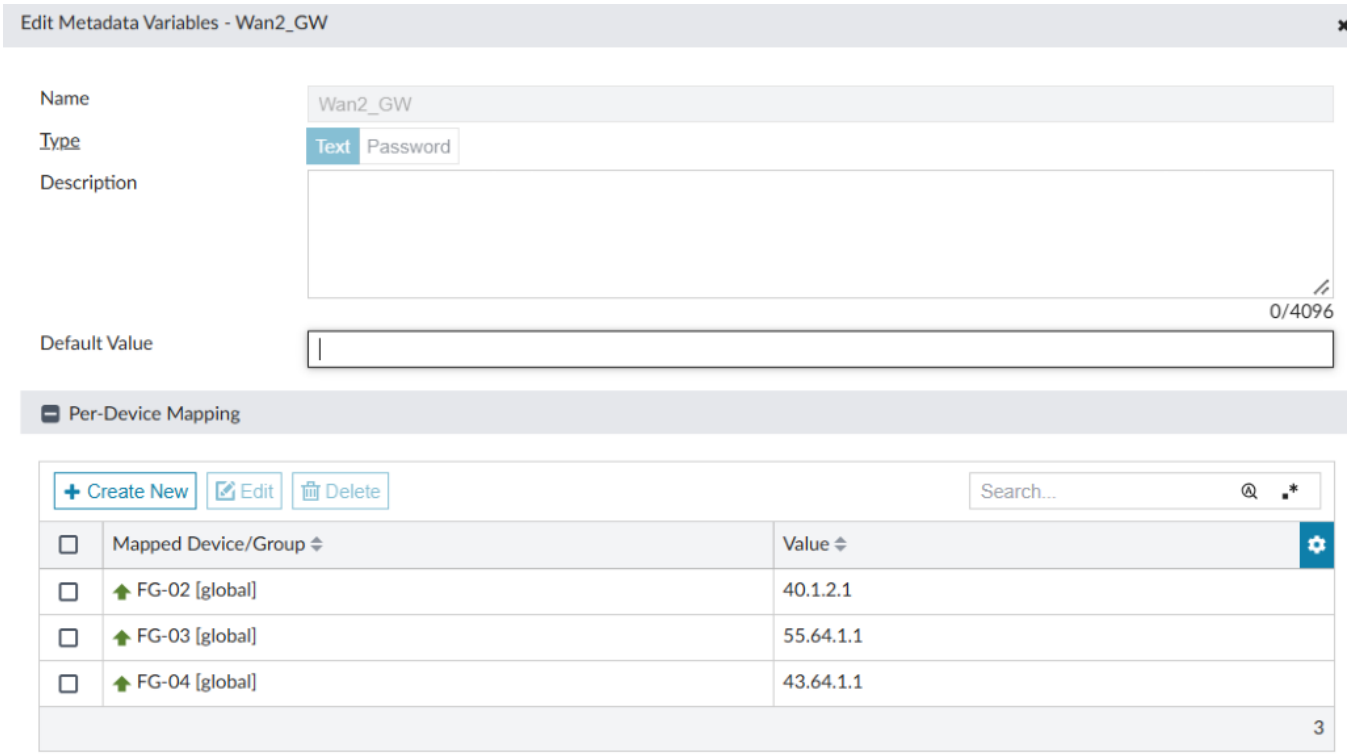


Branch SD-WAN

FortiManager lab configuration and verification

05.02

Add wan2 to Internet and bind its gateway to the second WAN metadata variable.

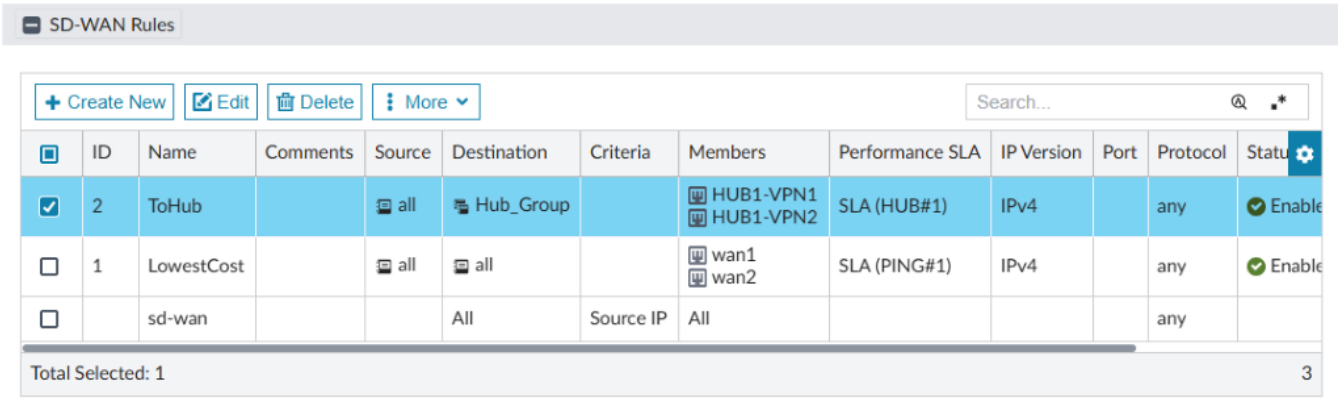


Branch SD-WAN

FortiManager lab configuration and verification

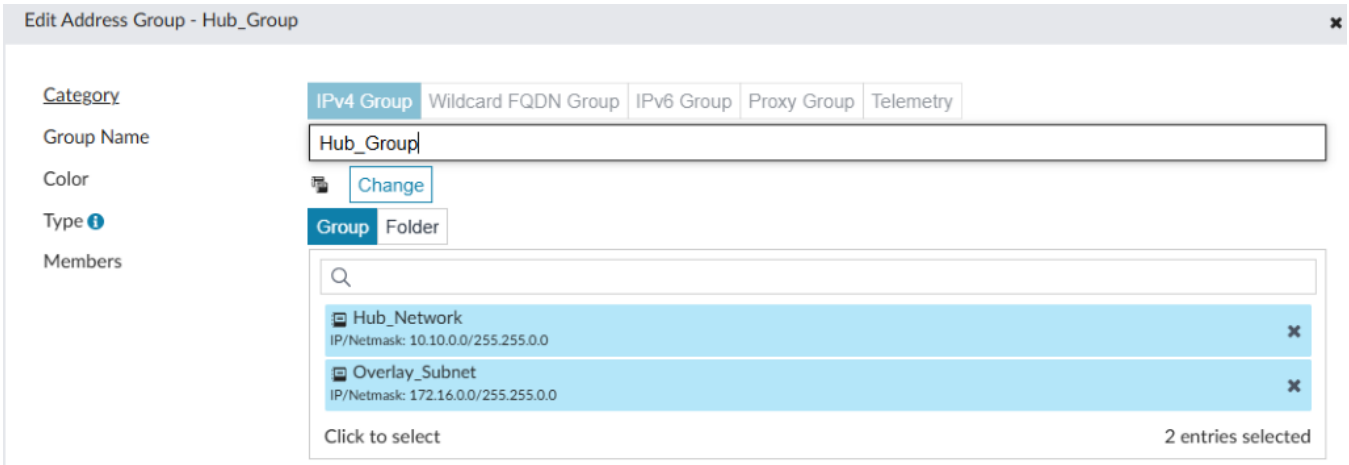
05.03

Review the rule list and place ToHub above the catch-all LowestCost internet rule.



05.04

Define the traffic match for the overlay rule using Hub_Network, which covers 10.10.0.0/16.

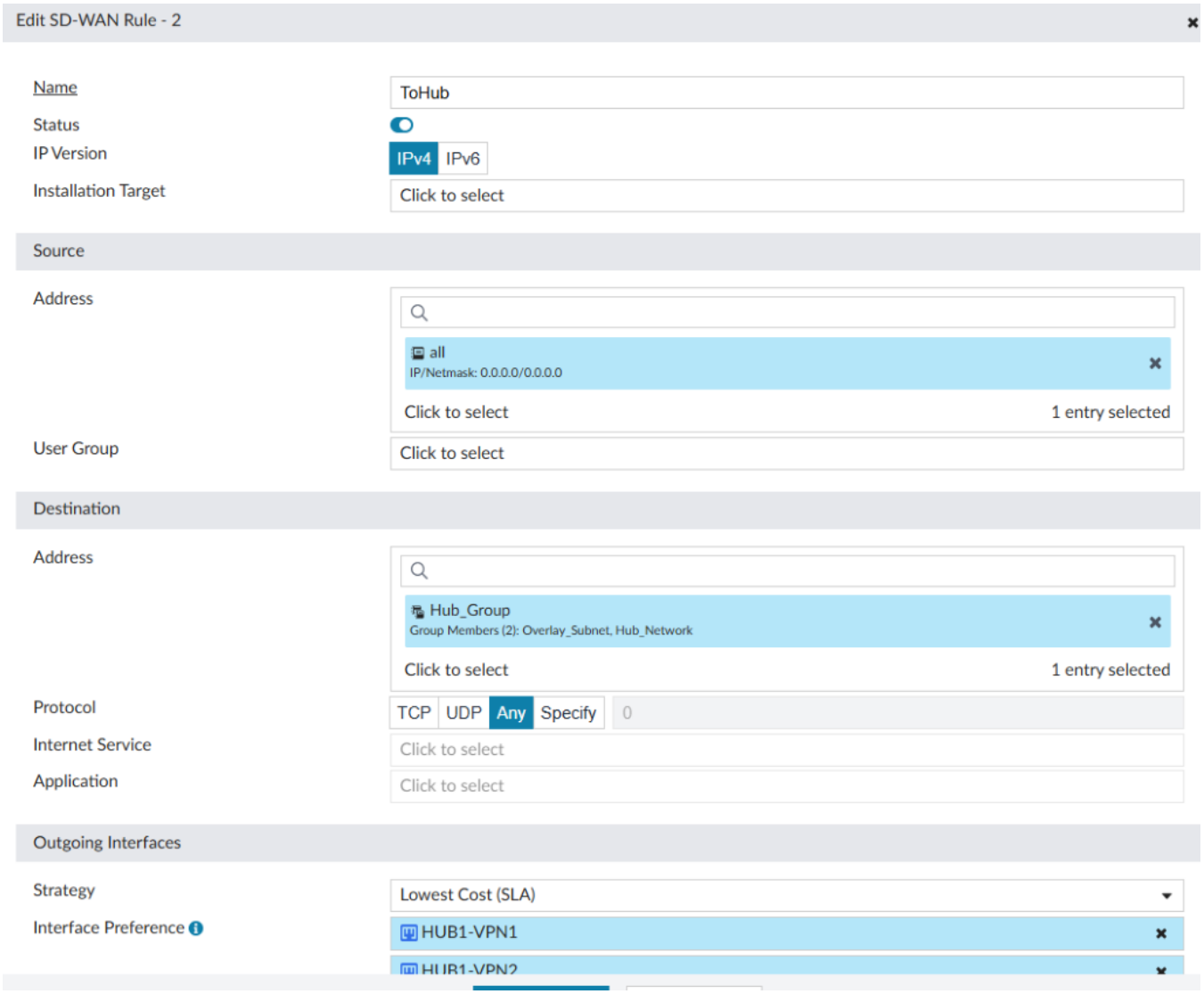


Branch SD-WAN

FortiManager lab configuration and verification

05.05

Set the overlay rule to Lowest Cost (SLA) and use the HUB SLA for the VPN members.

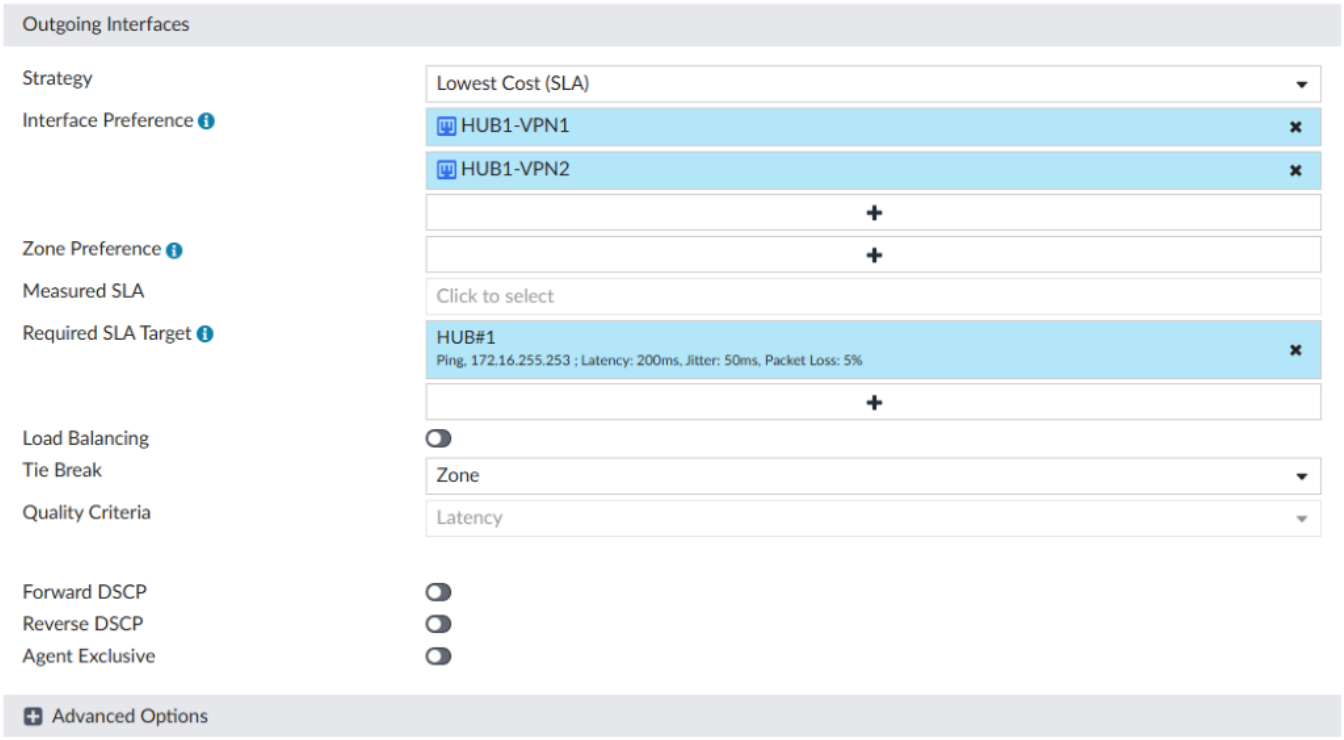


Branch SD-WAN

FortiManager lab configuration and verification

05.06

Configure the internet rule to use the two WAN members and the PING SLA.



Branch SD-WAN

FortiManager lab configuration and verification

05.07

Review Performance SLAs. HUB probes 172.16.255.253 through both VPN members. PING uses the public DNS endpoints shown in the capture.

Performance SLA

+ Create New | Edit | Delete | Where Used | Search...

Name	Detect Server	Protocol	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold	Installation Targe
HUB	172.16.255.253	Ping	5	200	50	5	5	
PING	1.1.1.1, 8.8.8.8	Ping	2	200	75	4	4	

Total Selected: 1 2

Neighbor

+ Create New | Edit | Delete | Search...

Neighbor	Role	Interface Member	Performance SLA	SLA	Installation Target
172.16.255.252	Standalone	HUB1-VPN1 HUB1-VPN2	HUB	1	

1

05.08

Review the SD-WAN neighbor entry for 172.16.255.252. Associate both overlay members with HUB, SLA ID 1.

Edit SD-WAN Overlay Template - SD-WAN Template Options (4/5)

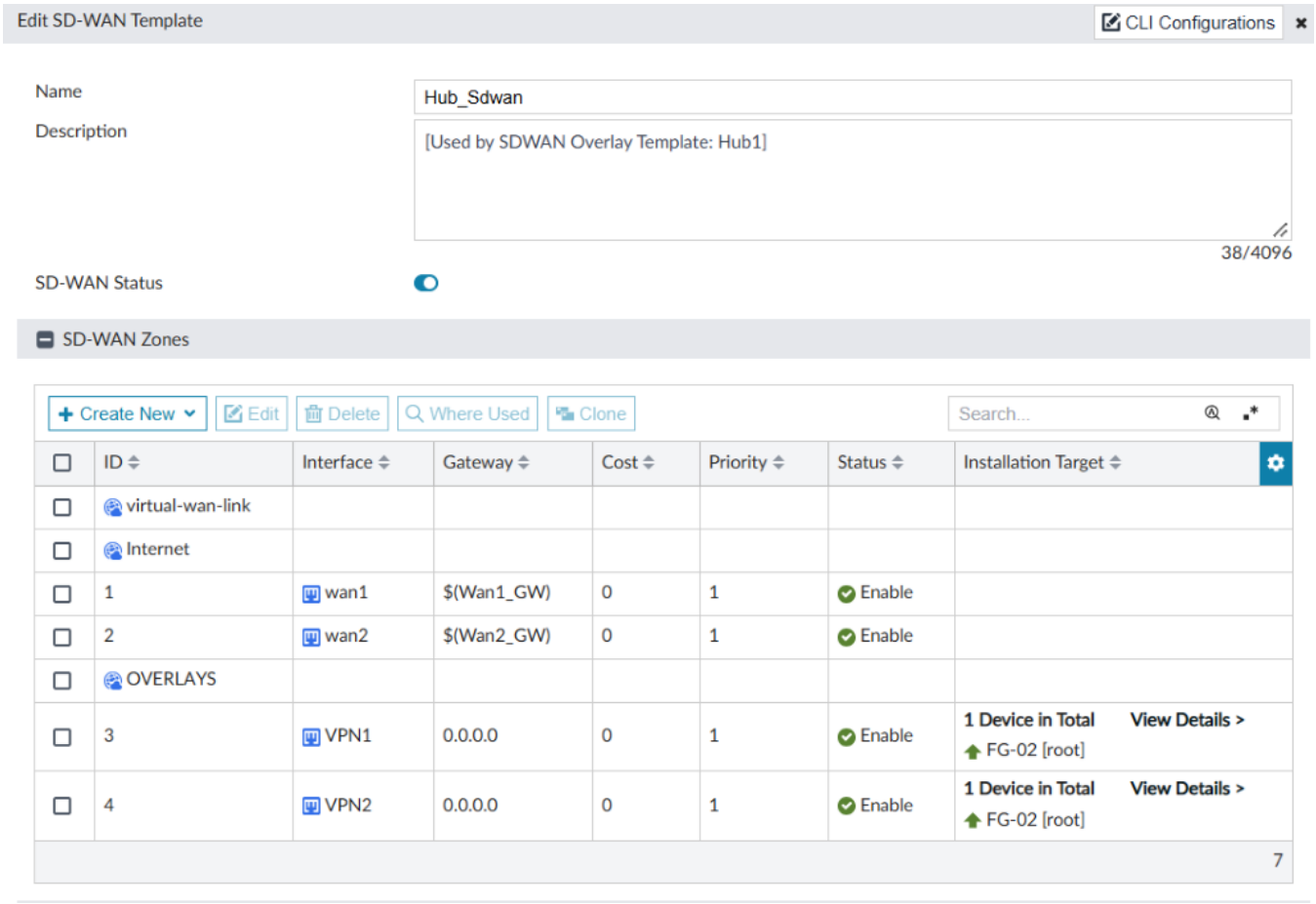
Add Overlay Objects to Branch SD-WAN Template	Sdwan_Branches
Add Overlay Interfaces and Zones	
Add Health Check Servers for Each HUB as Performance SLA	
Add Overlay Objects to Hub SD-WAN Template	Hub_Sdwan
Normalize Interfaces	
Add Health Check Firewall Policy to Hub Policy Package	
Add Health Check Firewall Policy to Branch Policy Package	
Add Default Route to SD-WAN Zones in Branch Static Route Template	

Hub SD-WAN and BGP

FortiManager lab configuration and verification

06.01

Review the hub SD-WAN template, including the zone and member assignments.



Hub SD-WAN and BGP

FortiManager lab configuration and verification

06.02

Open the generated branch BGP template. Review the local AS, router ID and hub neighbor settings for loopback peering.

Neighbor Range

+ Create New | Edit | Delete | More | Search...

Prefix	Neighbor Group	Maximum Neighbor Number
172.16.0.0/255.255.0.0	DYN_EDGE	0

1

IPv6 Neighbor Range

+ Create New | Edit | Delete | More | Search...

IPv6 Prefix	Neighbor Group	Maximum Neighbor Number
No record found.		

0

Networks

+ Create New | Edit | Delete | More | Search...

Prefix	Backdoor	Network Import Check	Route Map
$(Branches_Network_Prefixes_BGP)	Disabled	Global	

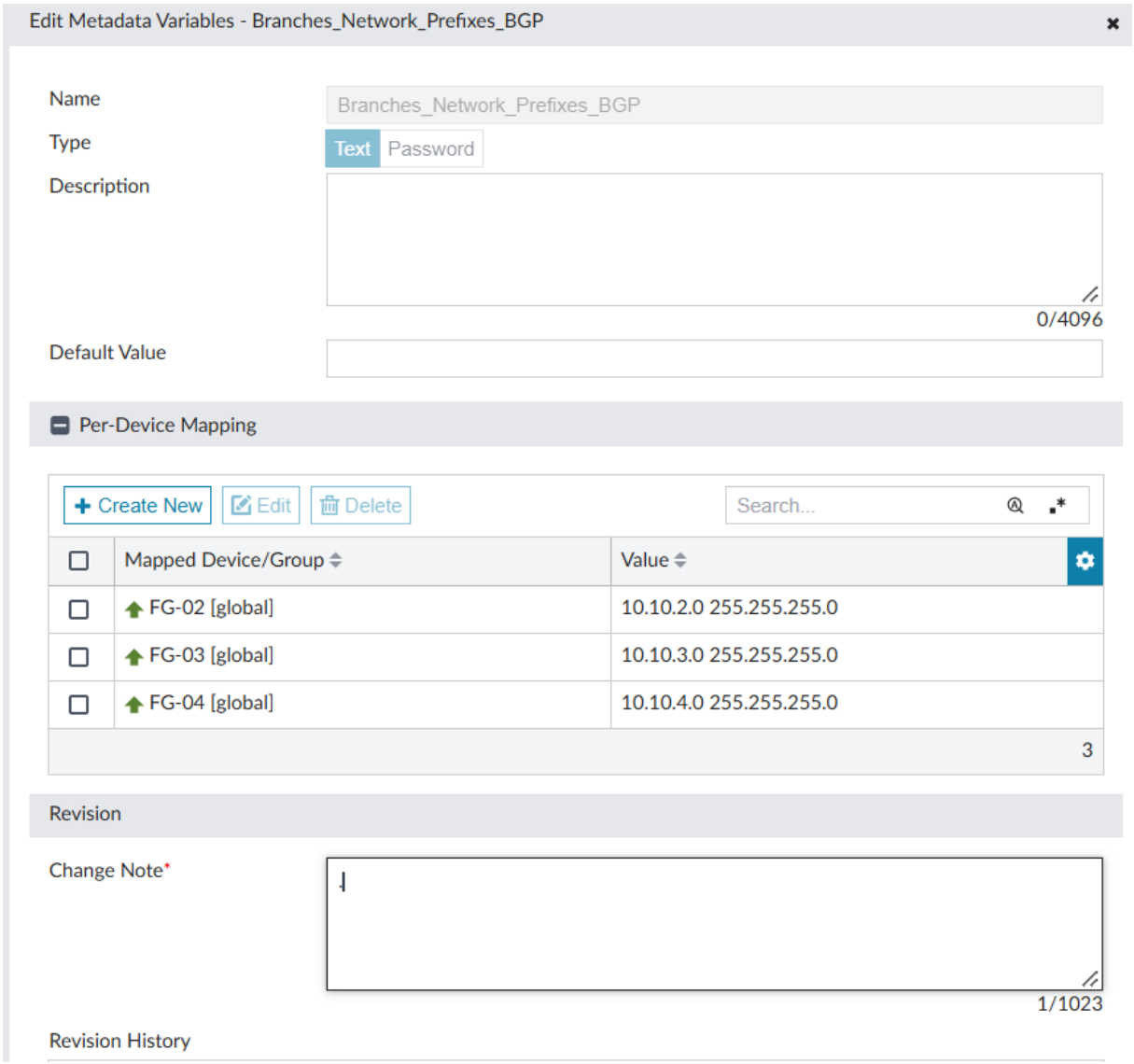
1

Hub SD-WAN and BGP

FortiManager lab configuration and verification

06.03

Use the branch LAN metadata variable for the locally advertised branch network.

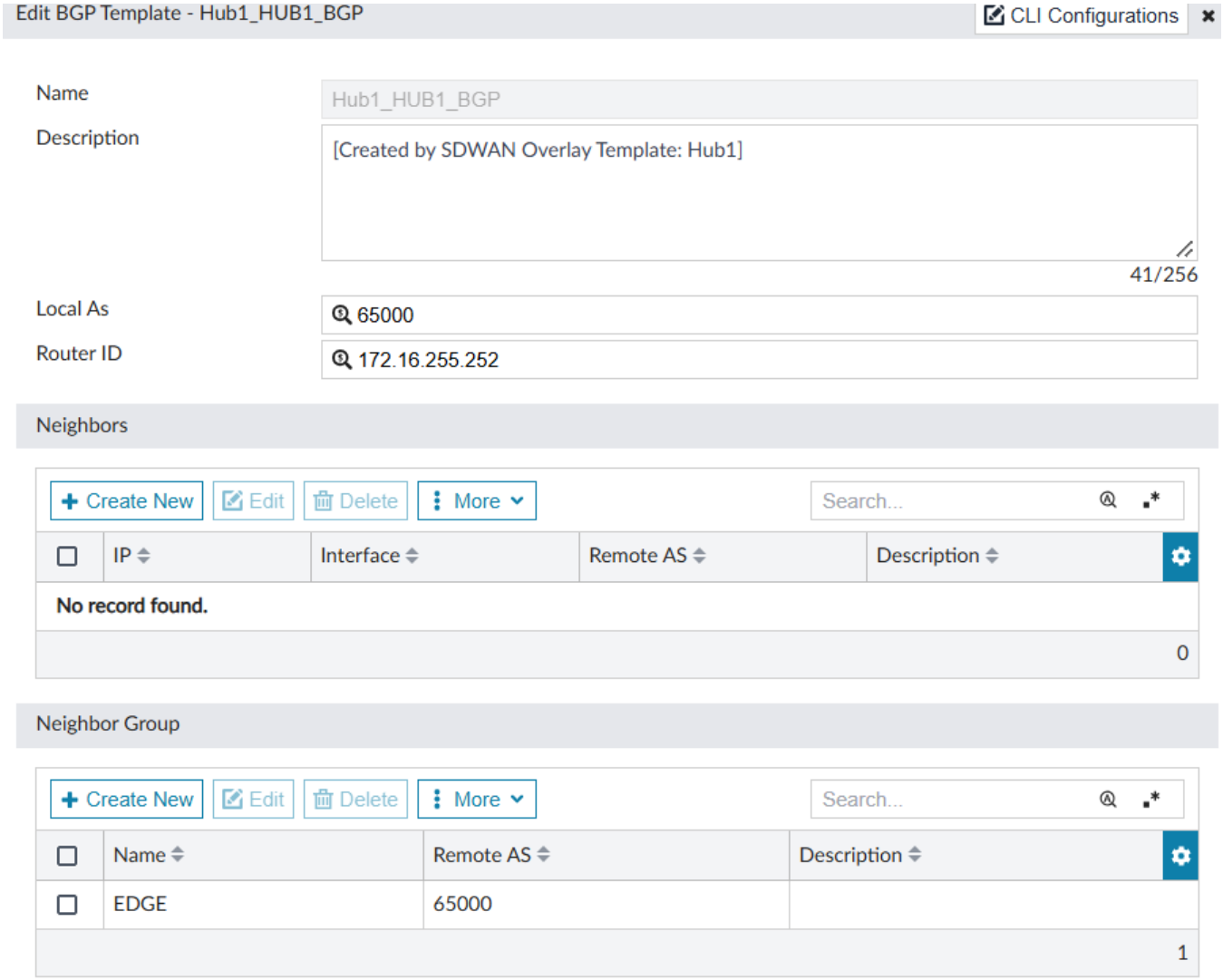


Hub SD-WAN and BGP

FortiManager lab configuration and verification

06.04

Open the generated hub BGP template. Review its hub router ID and local AS.



Hub SD-WAN and BGP

FortiManager lab configuration and verification

06.05

Review the branch neighbor settings in the hub BGP template.

Neighbor Range

+ Create New | Edit | Delete | More | Search...

	Prefix	Neighbor Group	Maximum Neighbor Number
☐	172.16.0.0/255.255.0.0	EDGE	0

1

IPv6 Neighbor Range

+ Create New | Edit | Delete | More | Search...

	IPv6 Prefix	Neighbor Group	Maximum Neighbor Number
No record found.			

0

Networks

+ Create New | Edit | Delete | More | Search...

	Prefix	Backdoor	Network Import Check	Route Map
☐	172.16.0.0/255.255.0.0	⊘ Disabled	Global	LOCAL_REGION

1

Hub SD-WAN and BGP

FortiManager lab configuration and verification

06.06

Configure the hub aggregate networks. This lab uses aggregation as a routing design choice with loopback BGP.

IPv6 Networks

+ Create New	Edit	Delete	More	Search...

	IPv6 Prefix	Backdoor	Network Import Check	Route Map
No record found.				

0

Aggregate Address

+ Create New	Edit	Delete	More	Search...

	Prefix	Generate AS Set Path	Filter More Specific Routes
	10.10.0.0/255.255.0.0	Disabled	Disabled

1

IPv6 Aggregate Address

+ Create New	Edit	Delete	More	Search...

	IPv6 Prefix	Generate AS Set Path	Filter More Specific Routes
No record found.			

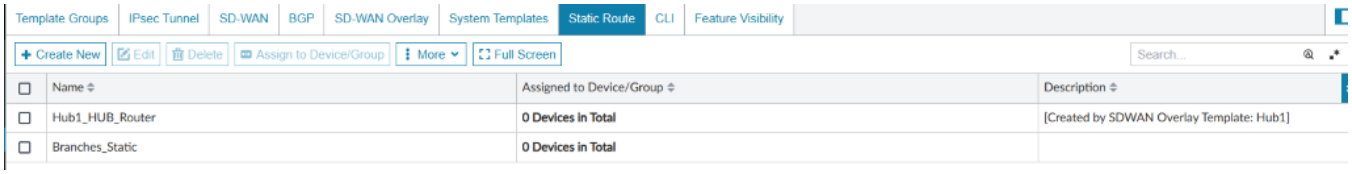
0

Static routes

FortiManager lab configuration and verification

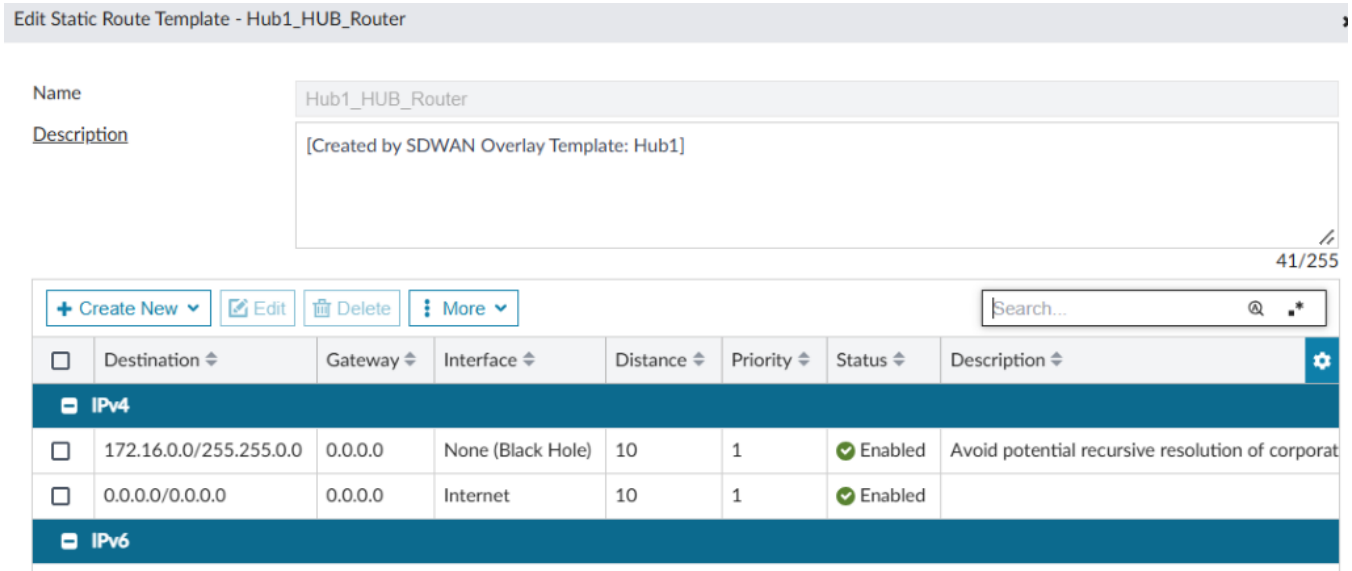
07.01

Review the generated hub and branch static route templates and their assignments.



07.02

Open the hub static route template. Verify that the loopback network uses the overlay path and the Internet default uses the Internet zone where configured.

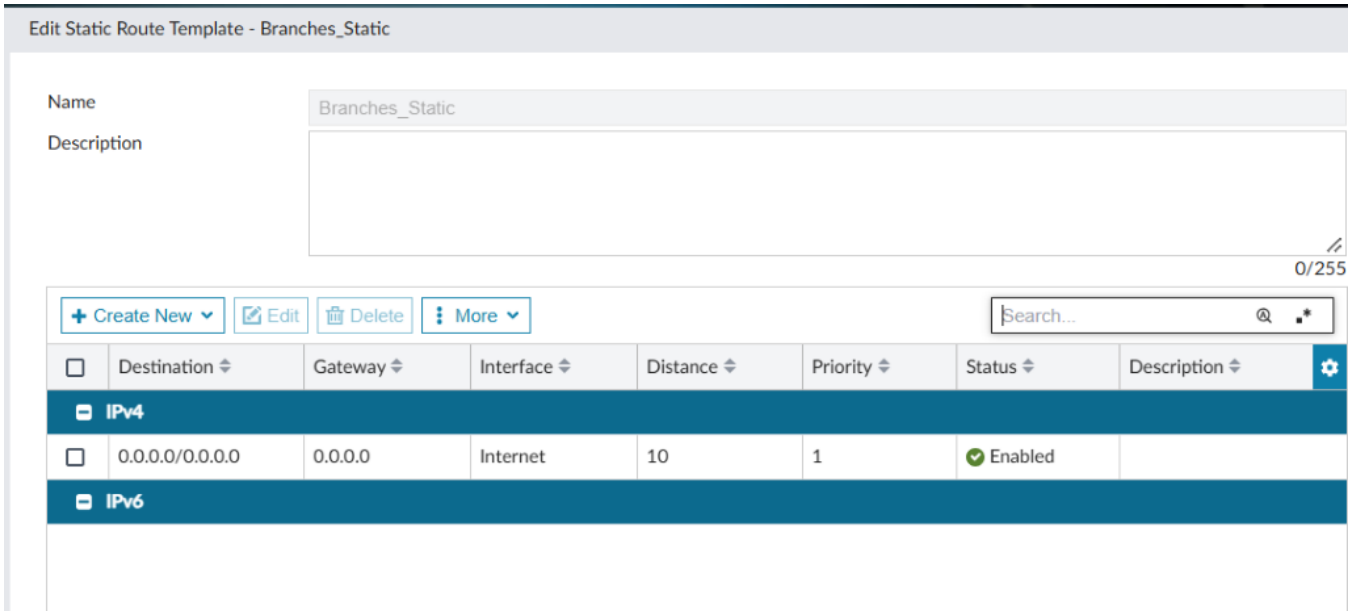


Static routes

FortiManager lab configuration and verification

07.03

Open the branch static route template. Verify the hub BGP peer has a /32 through the parent VPNs and review the separate Internet default route.

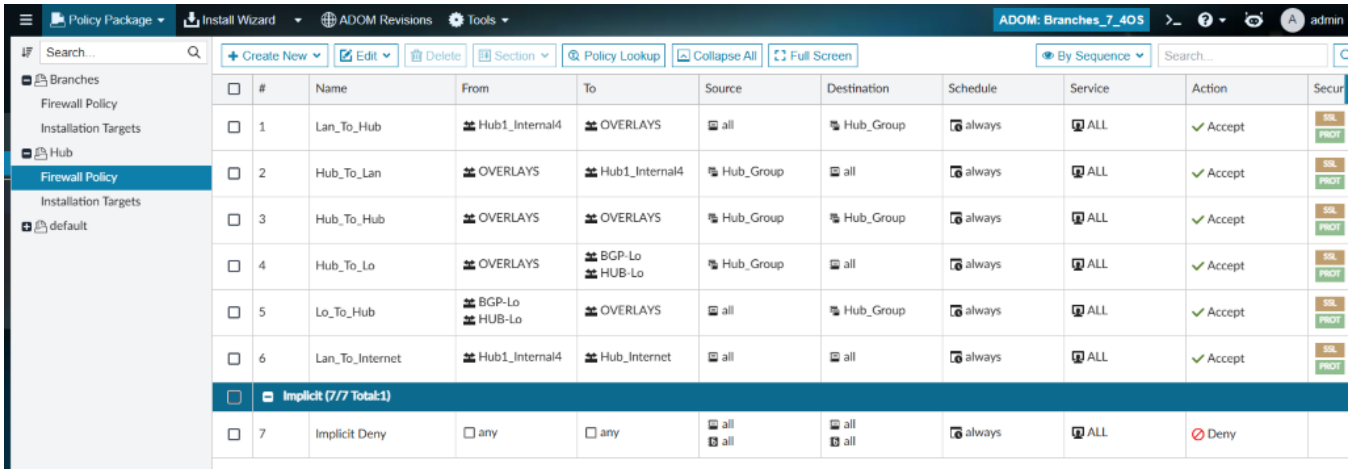


Hub policy package

FortiManager lab configuration and verification

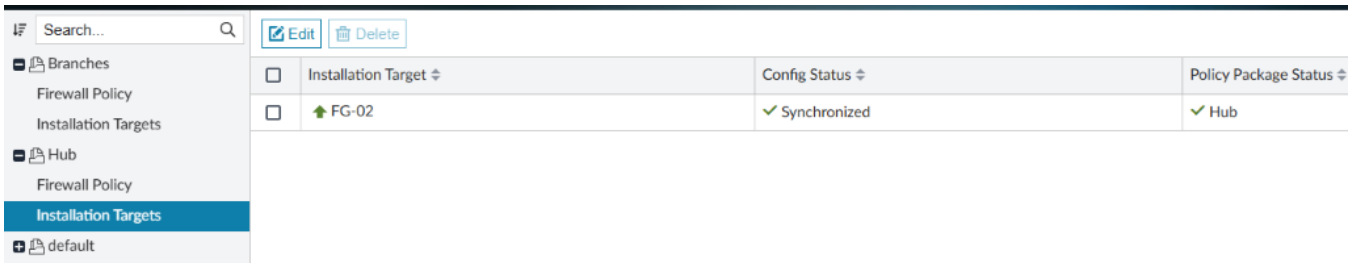
08.01

Review the hub policy package and confirm the overlay and Internet policies are in the intended order.



08.02

Inspect the overlay interface or zone mapping used by the hub policy.

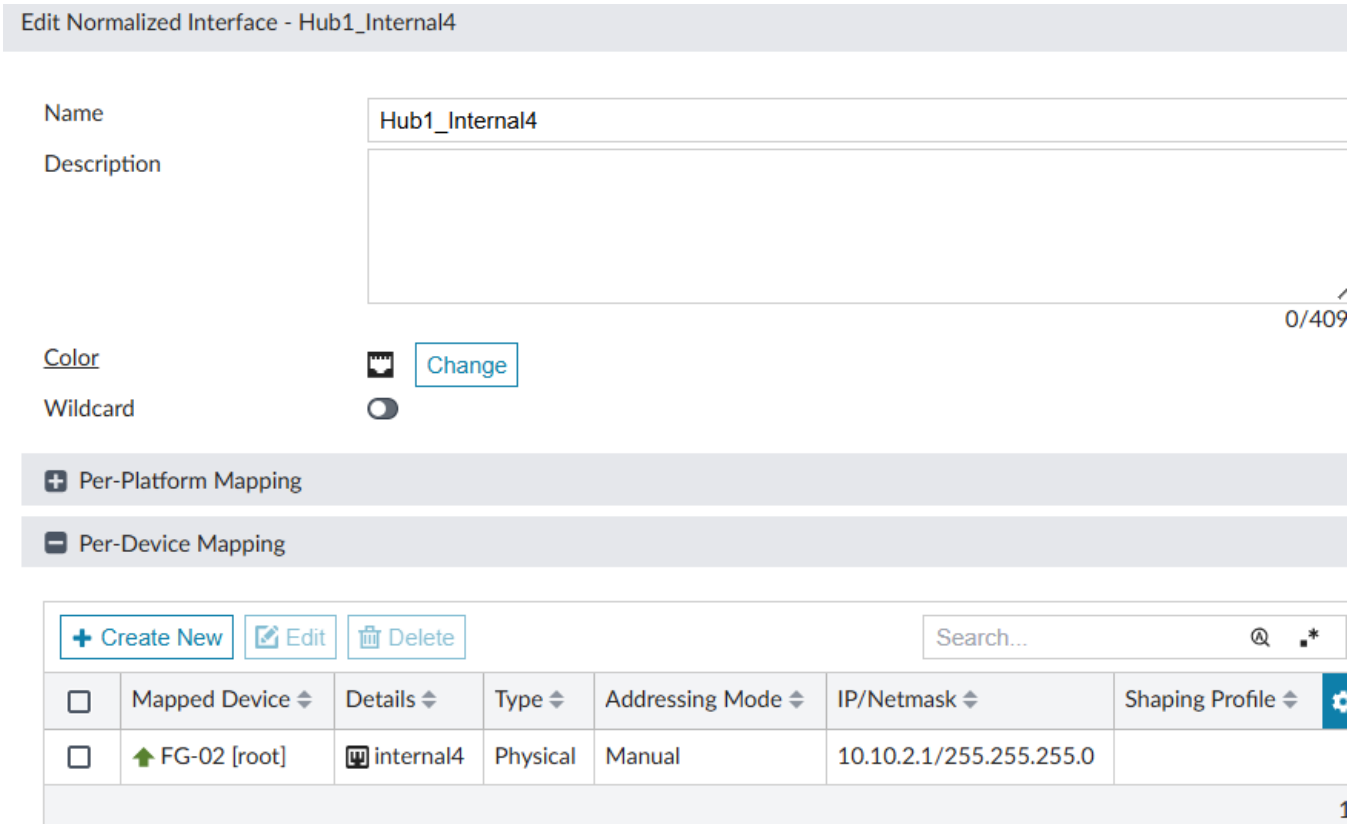


Hub policy package

FortiManager lab configuration and verification

08.03

Review the address objects and policy settings shown in the hub package.

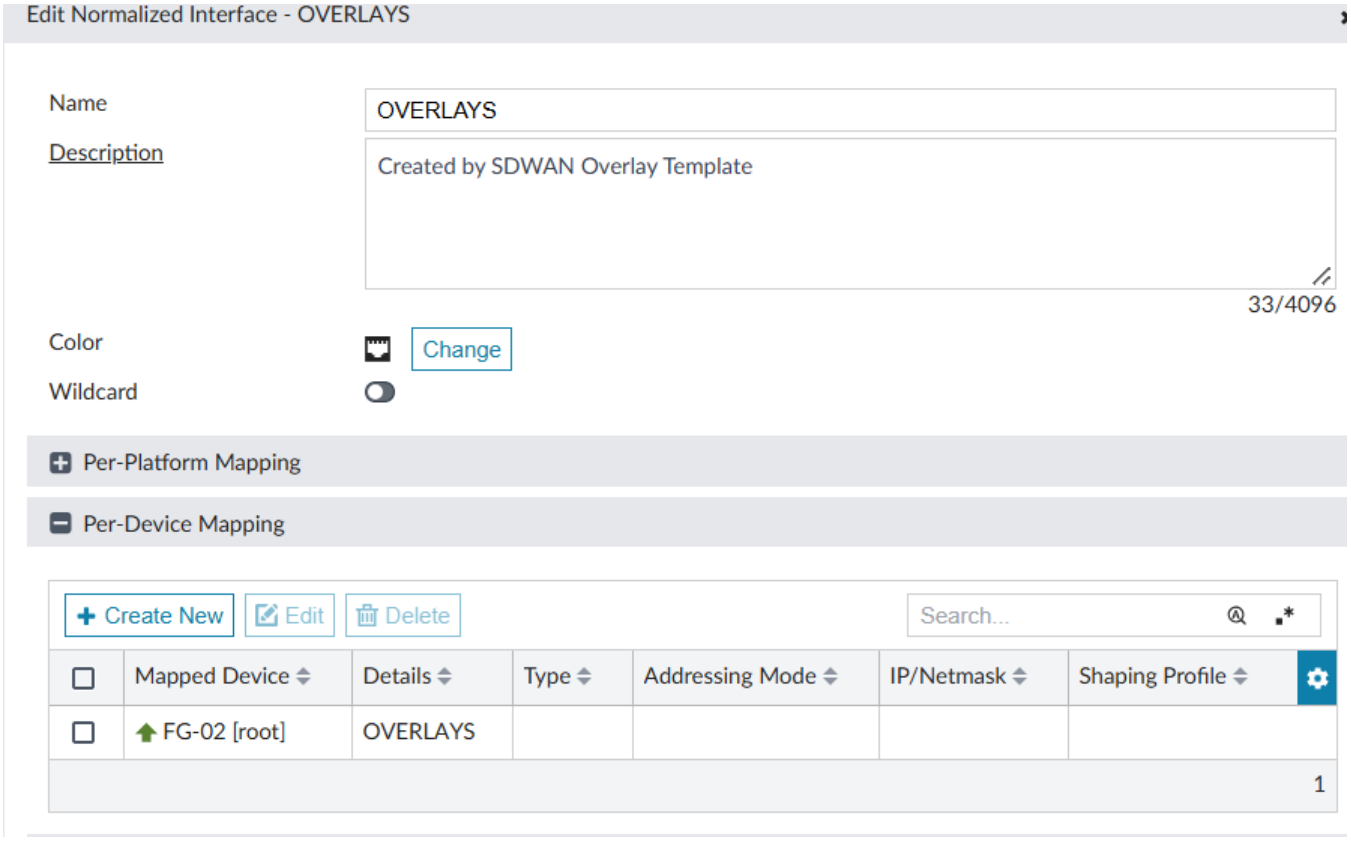


Hub policy package

FortiManager lab configuration and verification

08.04

Review the overlay-related settings before installing the hub package.

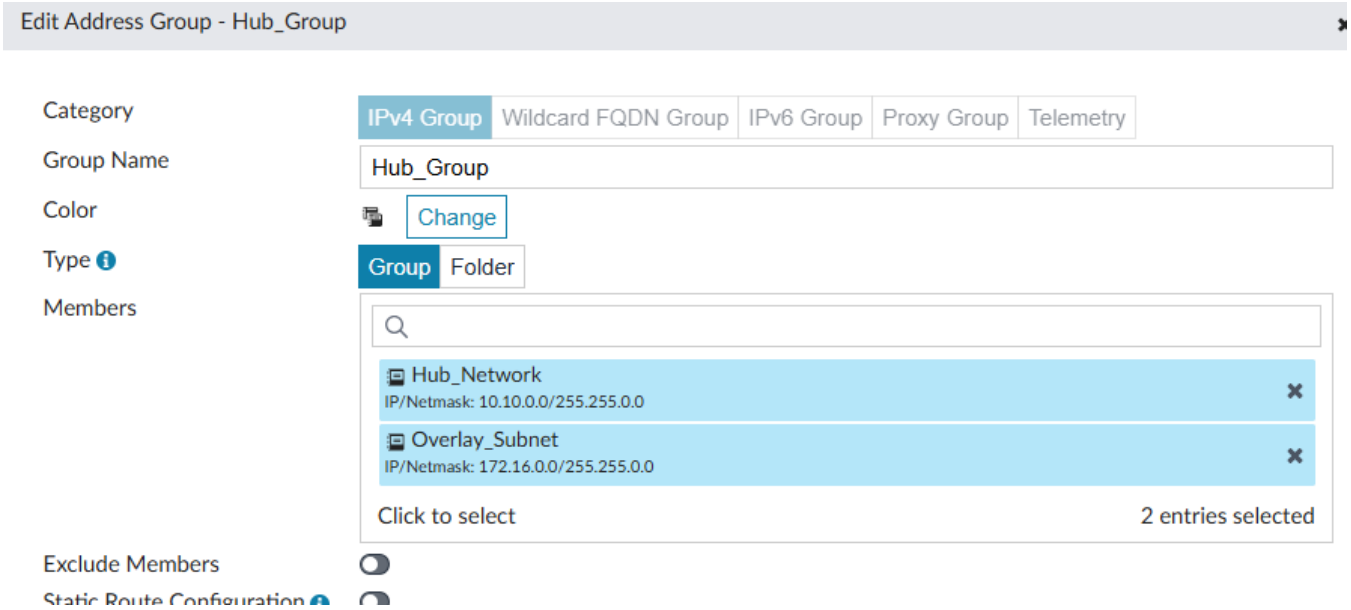


Hub policy package

FortiManager lab configuration and verification

08.05

Open Hub_Group and verify its member objects match the intended lab networks.

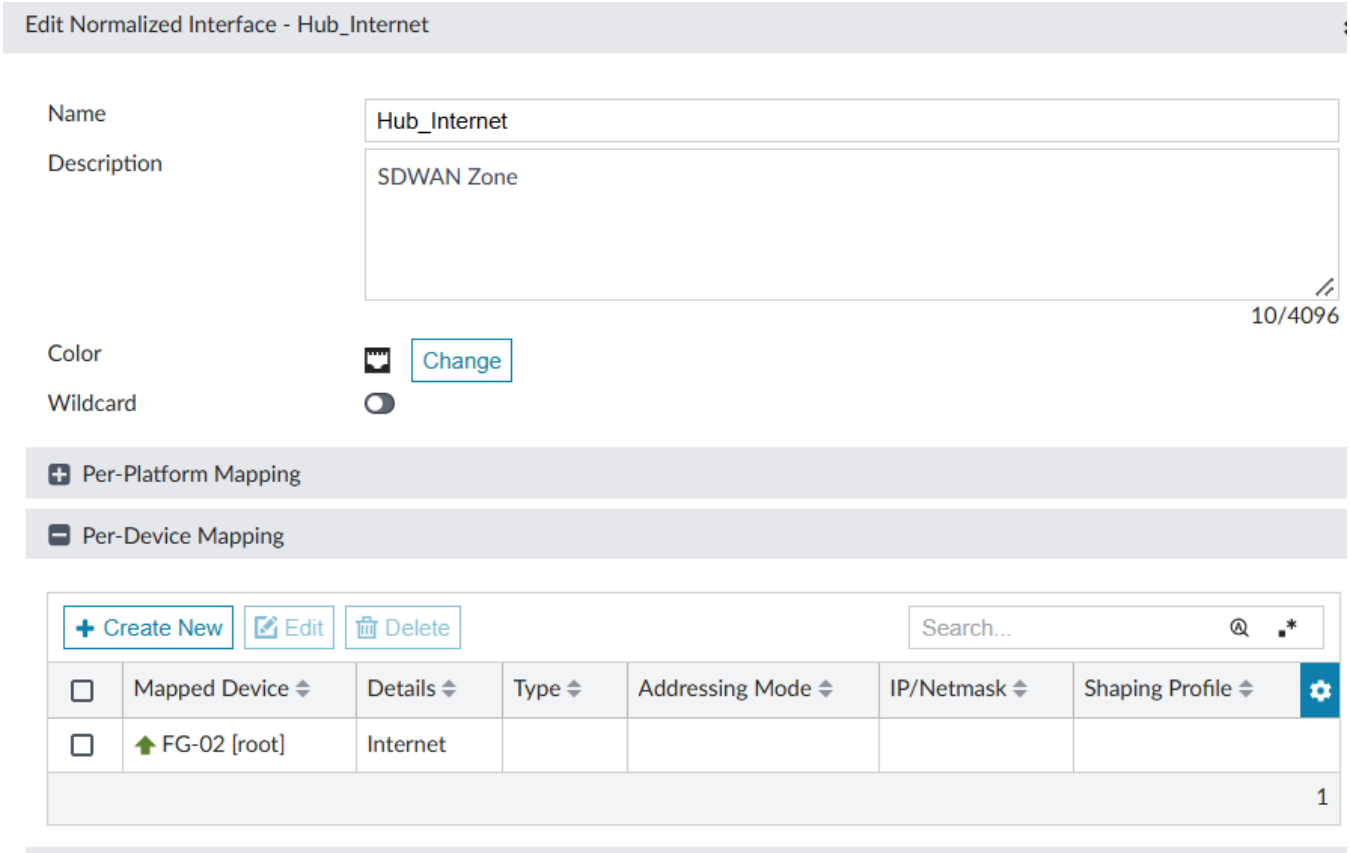


Hub policy package

FortiManager lab configuration and verification

08.06

Verify the hub Internet interface mapping references the Internet SD-WAN zone.

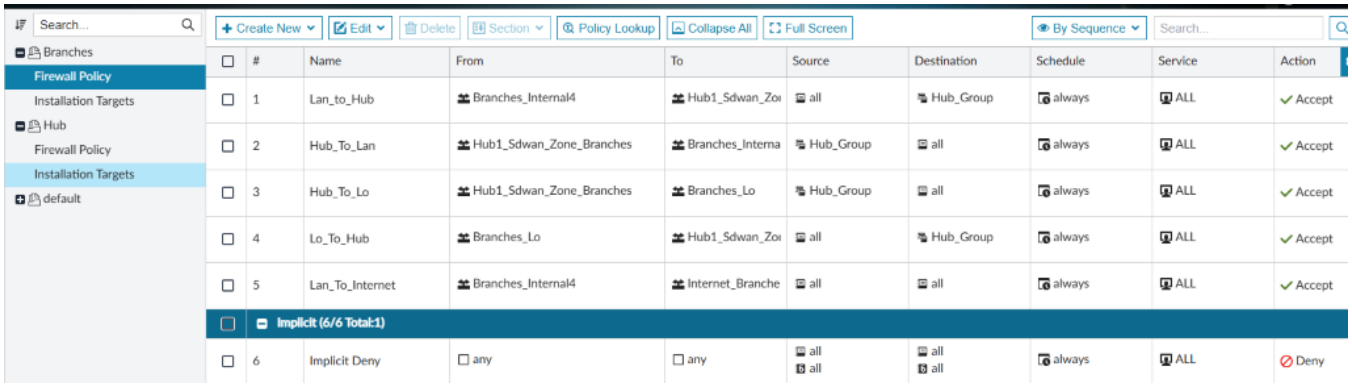


Branch policy package

FortiManager lab configuration and verification

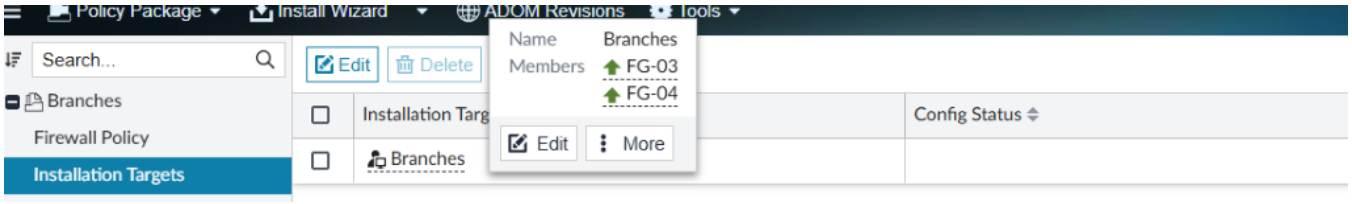
09.01

Review the branch rules for LAN-to-overlay, overlay-to-LAN, loopback access and LAN-to-Internet. Keep NAT disabled for internal overlay traffic.



09.02

Inspect the interface objects used in the branch package.

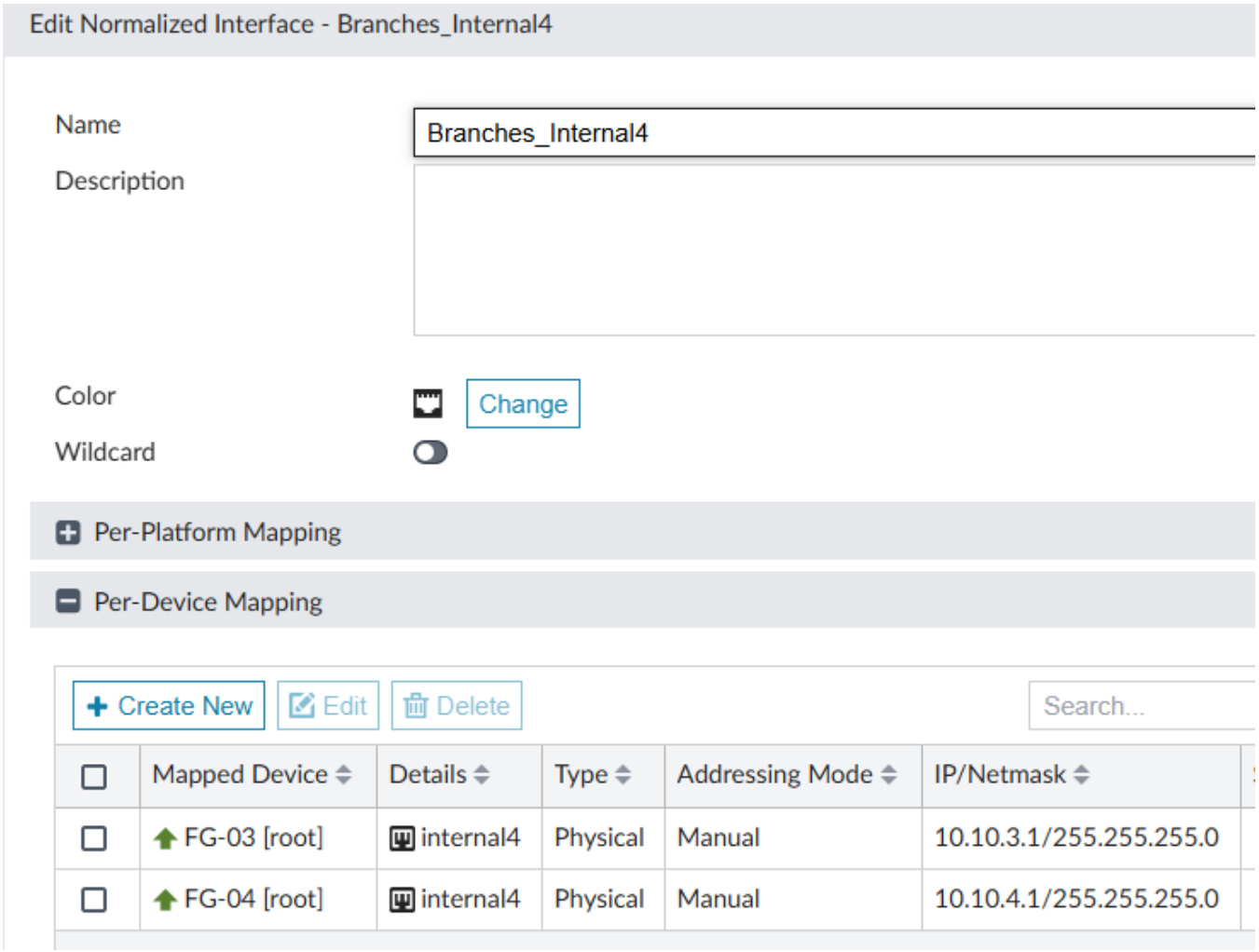


Branch policy package

FortiManager lab configuration and verification

09.03

Review the branch interface mapping in Policy & Objects.

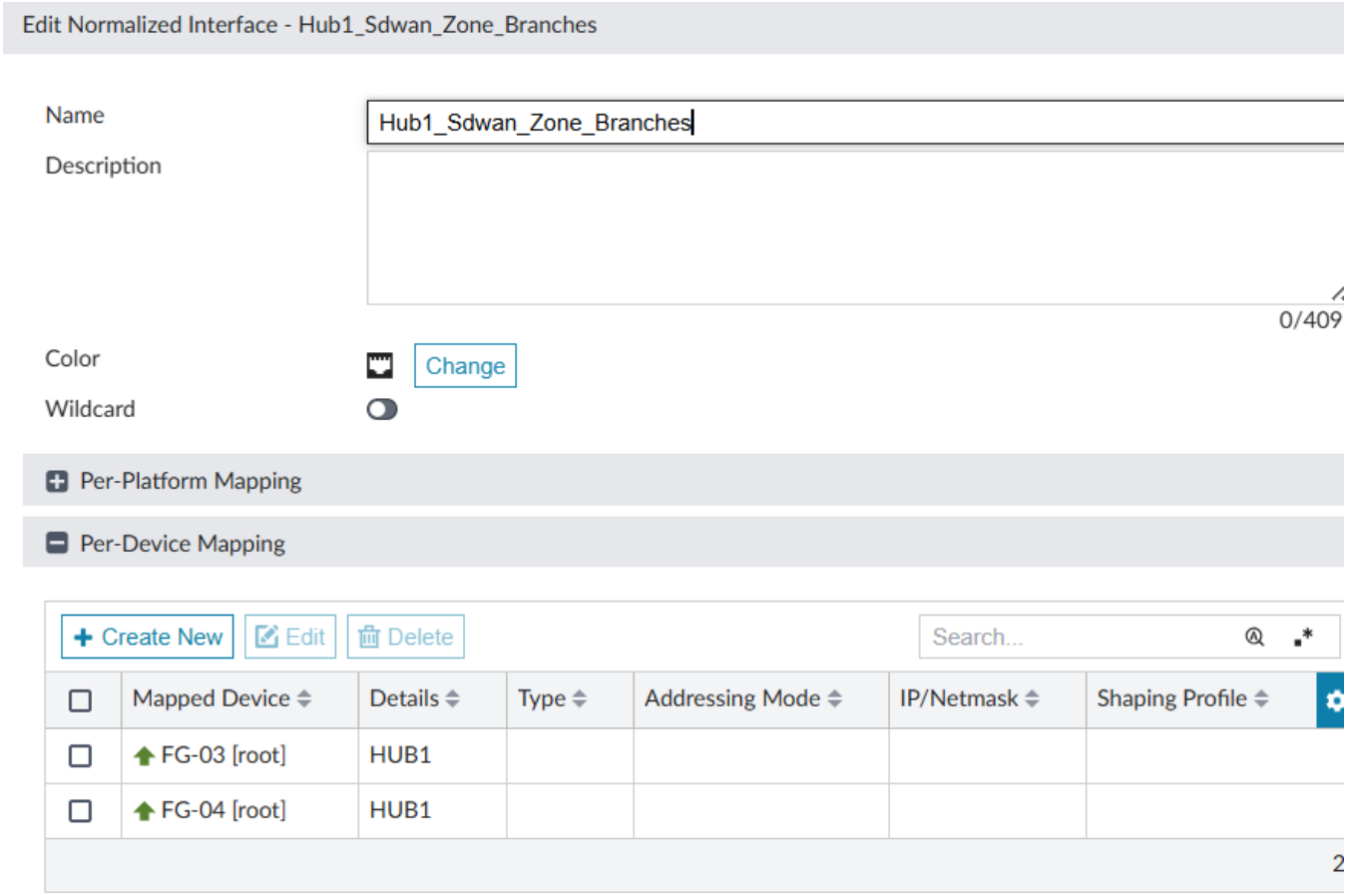


Branch policy package

FortiManager lab configuration and verification

09.04

Review the next branch interface mapping against its assigned target.

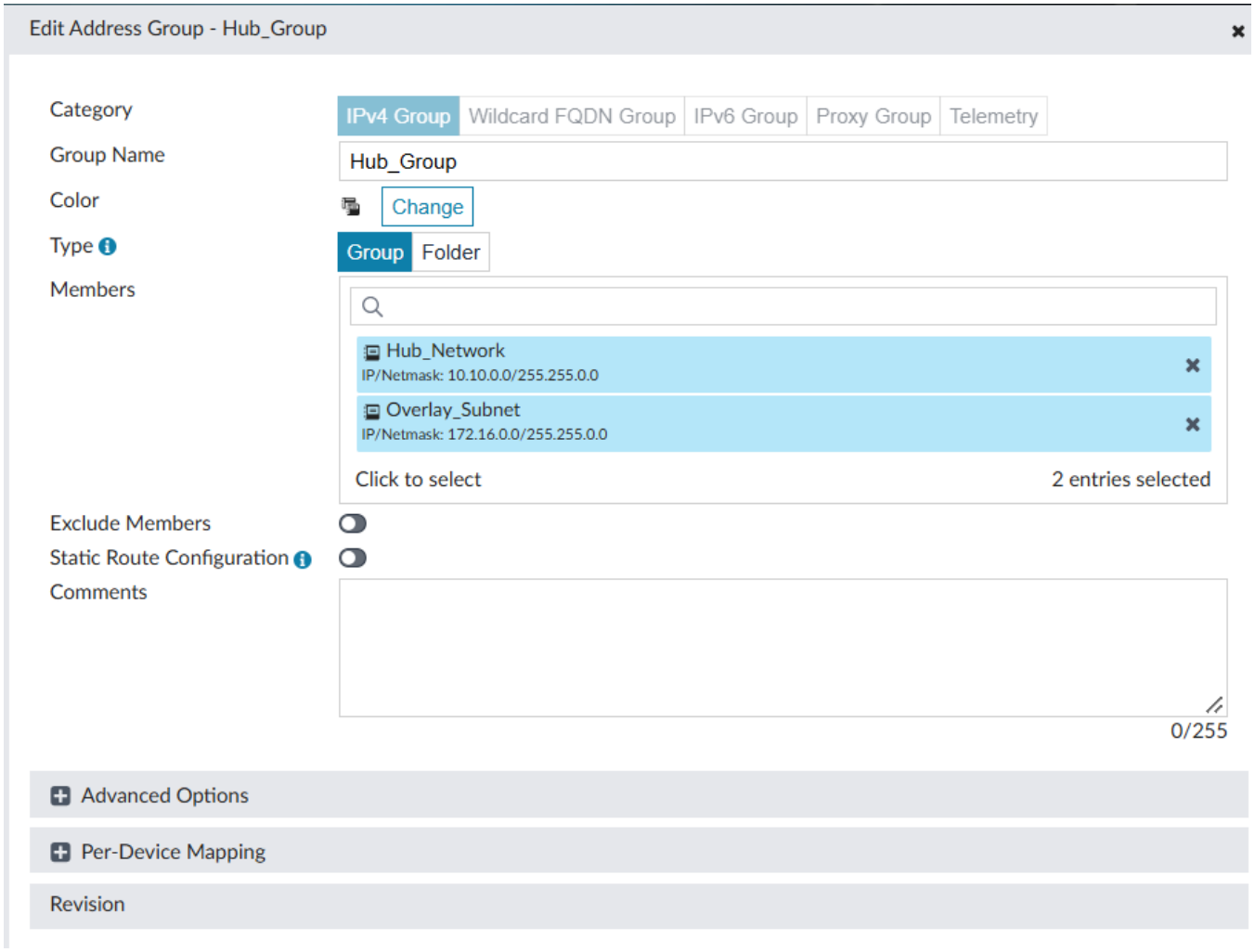


Branch policy package

FortiManager lab configuration and verification

09.05

Verify the branch address group and its intended members.

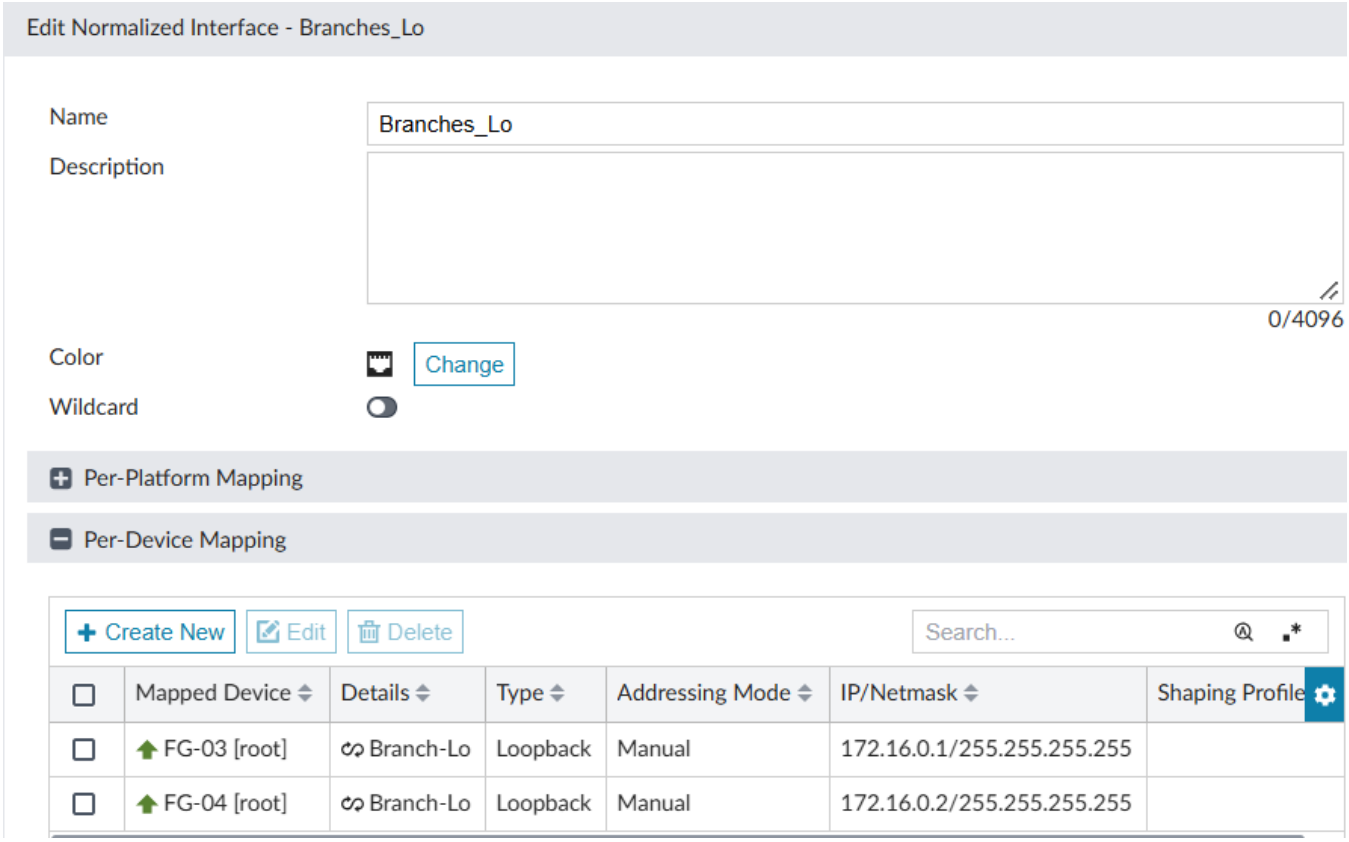


Branch policy package

FortiManager lab configuration and verification

09.06

Review the branch mapping and install target shown in the capture.

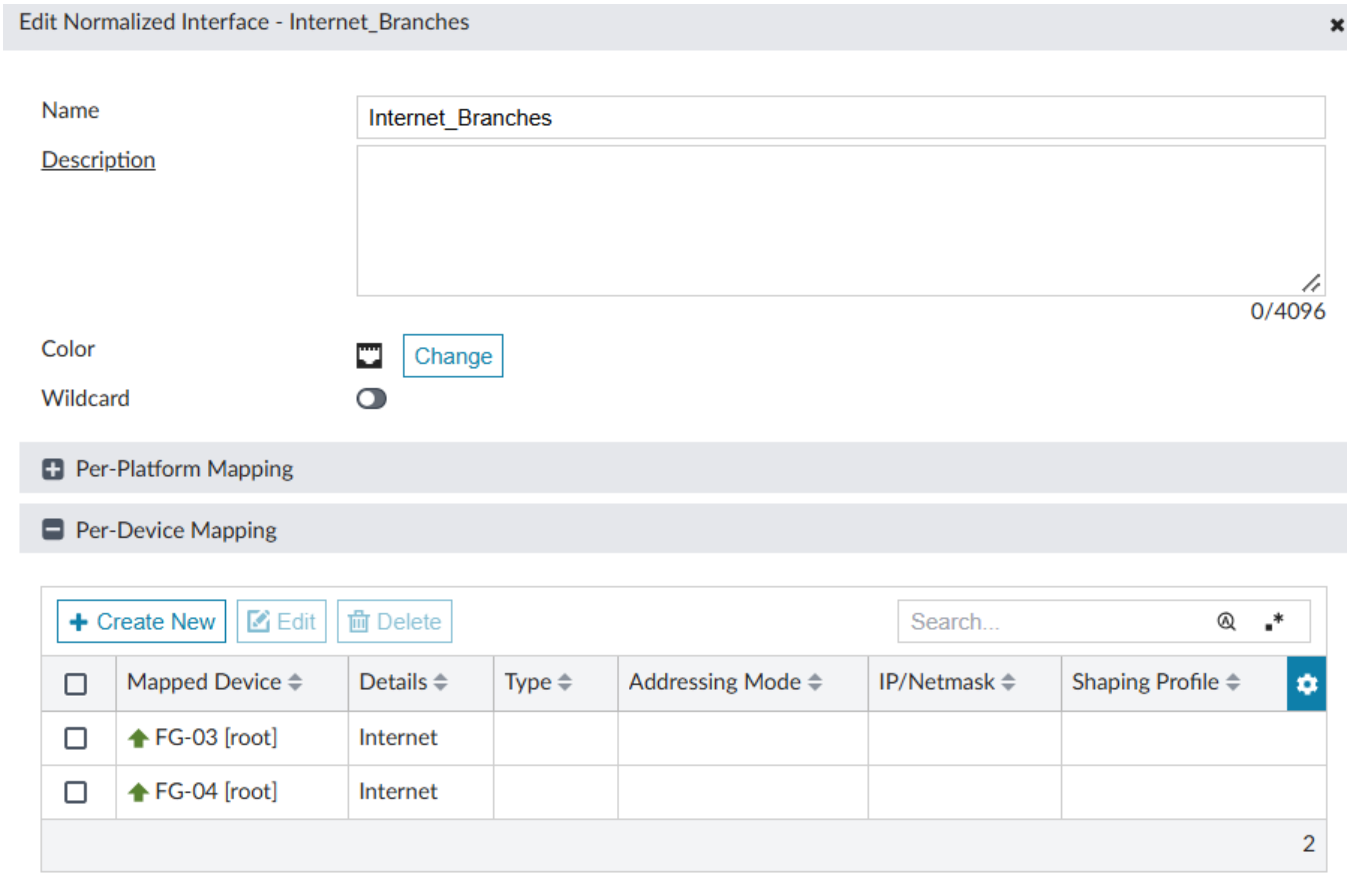


Branch policy package

FortiManager lab configuration and verification

09.07

Verify the remaining branch mapping before installing the package.

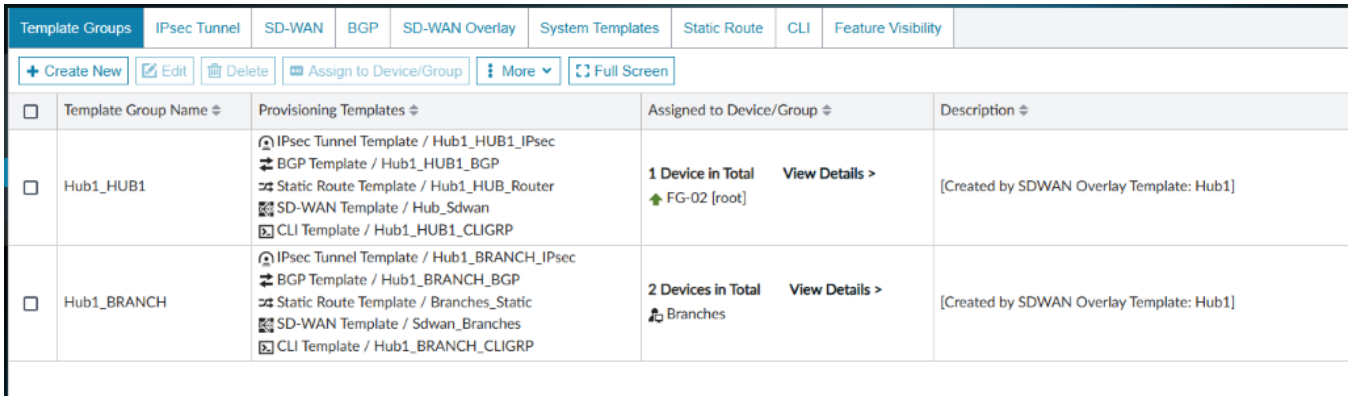


Branch policy package

FortiManager lab configuration and verification

09.08

Review both generated template groups. Hub1_HUB1 targets FG-02 and Hub1_BRANCH targets Branches. Each includes the intended IPsec, BGP, static route, SD-WAN and CLI configuration.

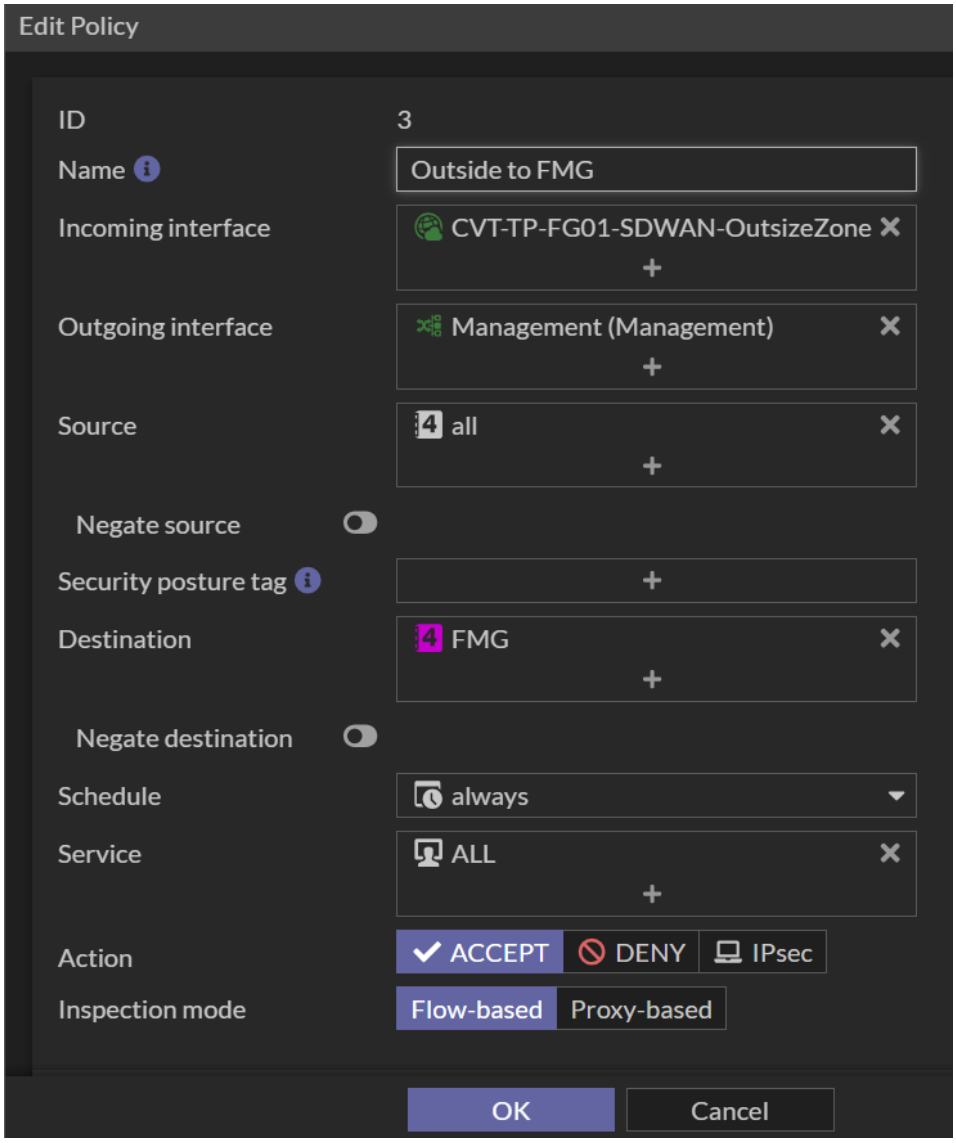


Bootstrap and installation

FortiManager lab configuration and verification

10.01

Review the management firewall policy for FortiManager behind NAT. Scope incoming FGFM to the expected device sources.

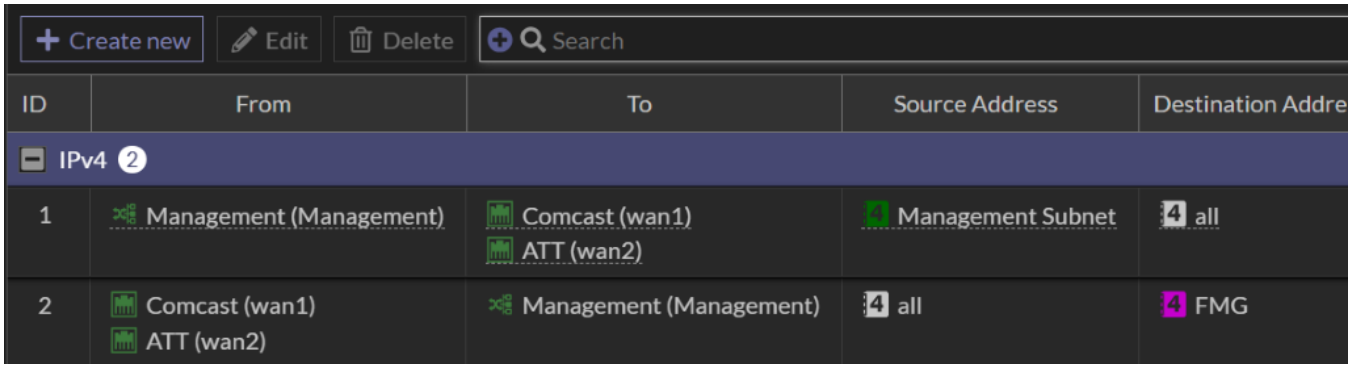


Bootstrap and installation

FortiManager lab configuration and verification

10.02

Review the Central NAT configuration used in the lab.

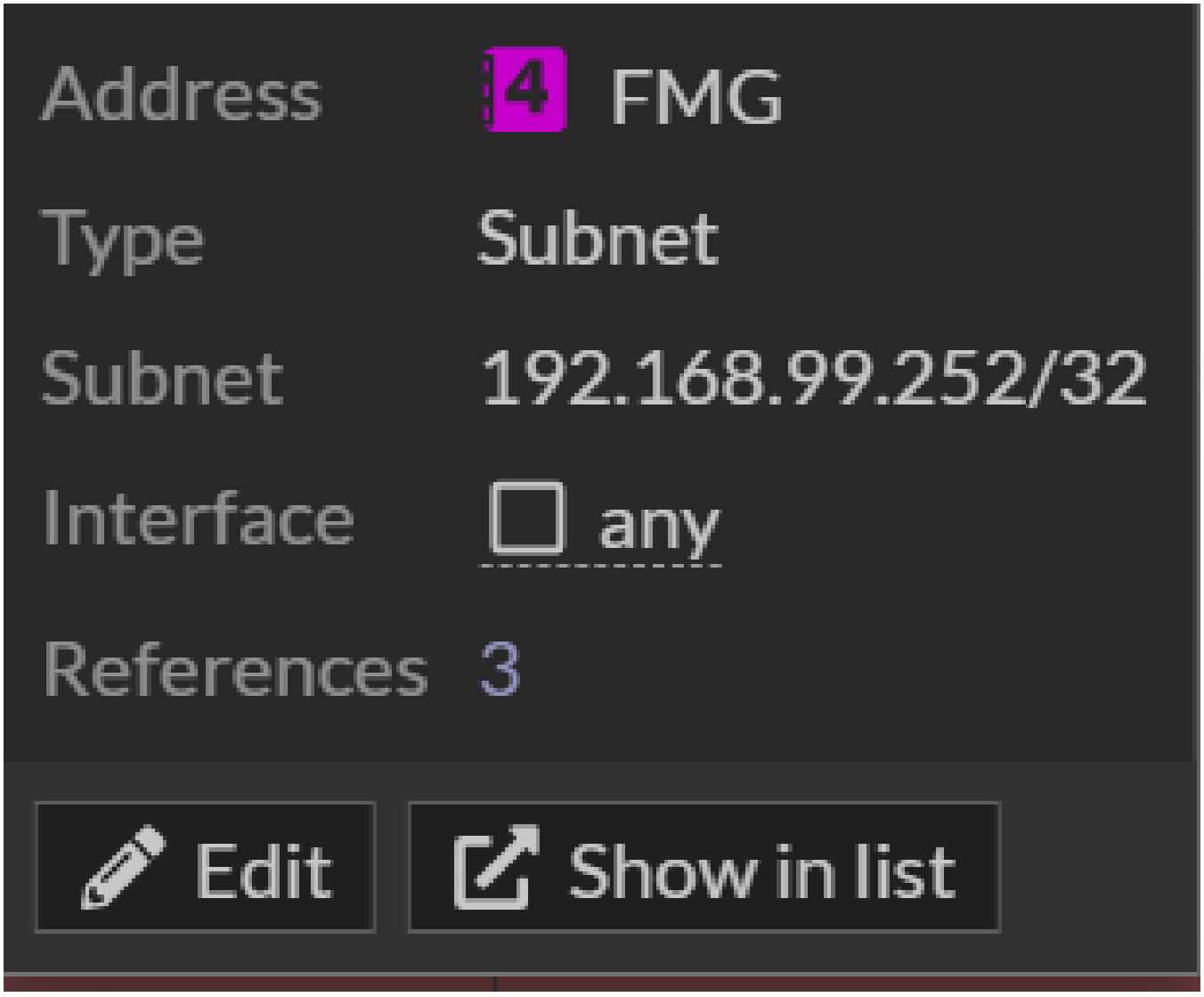


Bootstrap and installation

FortiManager lab configuration and verification

10.03

Verify the FortiManager destination address object used by the management policy.

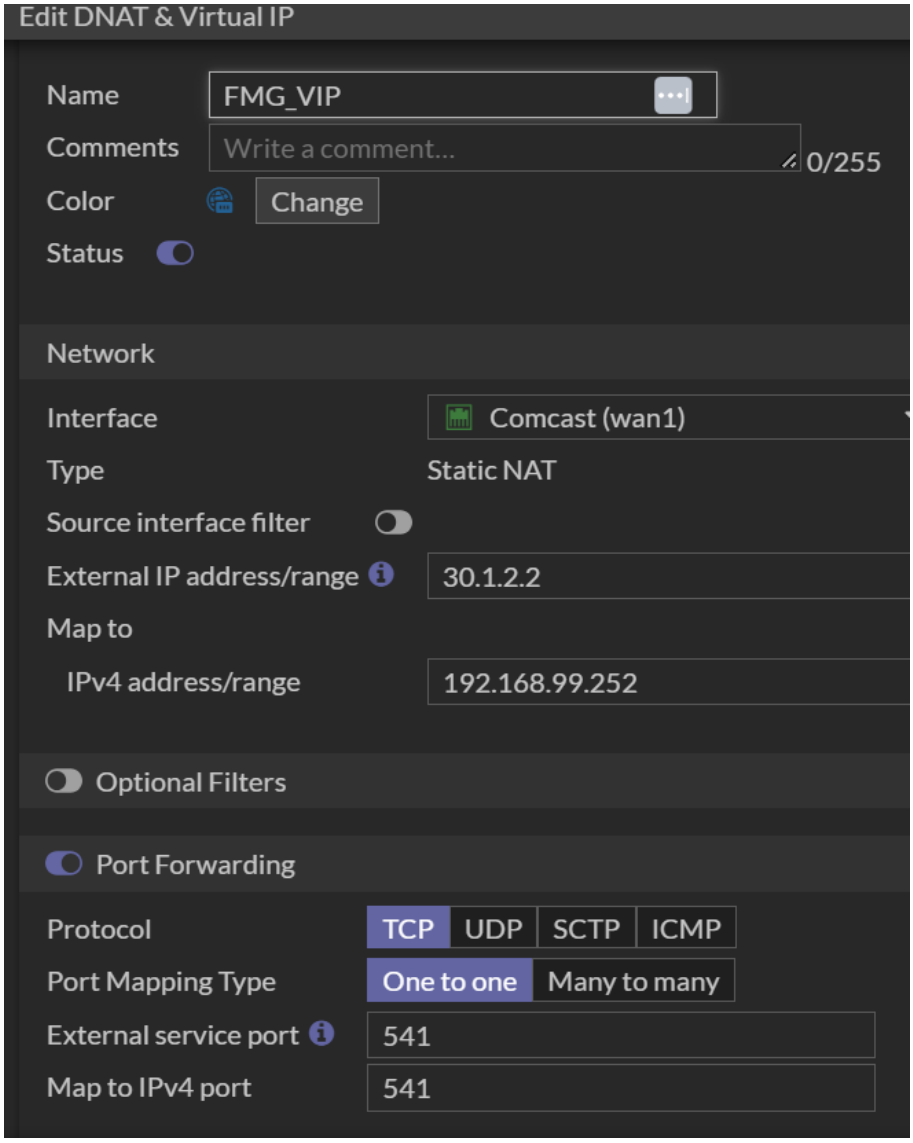


Bootstrap and installation

FortiManager lab configuration and verification

10.04

Verify the VIP forwards TCP/541 to FortiManager.



Bootstrap and installation

FortiManager lab configuration and verification

10.05

Verify basic reachability from the branch. Configure FortiManager central management, complete authorization or AutoLink, then preview and install device settings and policy packages.

```
FG-03 # execute ping 30.1.2.2
PING 30.1.2.2 (30.1.2.2): 56 data bytes
64 bytes from 30.1.2.2: icmp_seq=0 ttl=254 time=0.6 ms
64 bytes from 30.1.2.2: icmp_seq=1 ttl=254 time=0.4 ms
64 bytes from 30.1.2.2: icmp_seq=2 ttl=254 time=0.4 ms
64 bytes from 30.1.2.2: icmp_seq=3 ttl=254 time=0.4 ms
^C
--- 30.1.2.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.4/0.6 ms
```

Validate routing and shortcuts

FortiManager lab configuration and verification

11.01

Verify the branch routing table. The hub peer /32 resolves through both VPNs, and the BGP aggregates use the hub loopback as next hop.

```
FG-03 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 45.32.54.1, wan1, [1/0]
                  [1/0] via 55.64.1.1, wan2, [1/0]
B       10.10.0.0/16 [200/0] via 172.16.255.252 (recursive via HUB1-VPN1 tunnel 35.1.2.2), 00:57:12
                                                (recursive via HUB1-VPN2 tunnel 40.1.2.2), 00:57:12, [1/0]
C       10.10.3.0/24 is directly connected, internal4
C       45.32.54.0/30 is directly connected, wan1
C       55.64.1.0/30 is directly connected, wan2
B       172.16.0.0/16 [200/0] via 172.16.255.252 (recursive via HUB1-VPN1 tunnel 35.1.2.2), 00:57:12
                                                 (recursive via HUB1-VPN2 tunnel 40.1.2.2), 00:57:12, [1/0]
C       172.16.0.1/32 is directly connected, Branch-Lo
S       172.16.255.252/32 [15/0] via HUB1-VPN1 tunnel 35.1.2.2, [1/0]
                          [15/0] via HUB1-VPN2 tunnel 40.1.2.2, [1/0]
C       192.168.99.0/24 is directly connected, internal2
```

Validate routing and shortcuts

FortiManager lab configuration and verification

11.02

Verify reachability with ping and traceroute. This capture shows FG-03 reaching FG-04's LAN interface in one hop.

```
FG-03 # execute ping 10.10.4.1
PING 10.10.4.1 (10.10.4.1): 56 data bytes
64 bytes from 10.10.4.1: icmp_seq=0 ttl=255 time=1.2 ms
64 bytes from 10.10.4.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.10.4.1: icmp_seq=2 ttl=255 time=0.4 ms
^C
--- 10.10.4.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.6/1.2 ms

FG-03 # execute traceroute 10.10.4.1
traceroute to 10.10.4.1 (10.10.4.1), 32 hops max, 3 probe packets per hop, 84 byte packets
 1  10.10.4.1  0.564 ms  0.401 ms  0.372 ms

FG-03 #
```

11.03

Check diagnose sys sdwan advpn-session. A populated Selected path identifies the direct peer path chosen by SD-WAN.

```
FG-03 # diagnose sys sdwan advpn-session
Session head(FG-04-0-HUB1:1)
(1) Service ID(2), last access(8335964), remote health check info(2)
Selected path: local(HUB1-VPN1, wan1) gw: 45.32.54.2  remote IP: 66.31.1.2(172.16.0.2)
Remote information:
1: latency: 0.399567 jitter: 0.055233 pktloss: 0.000000 mos: 4.404142 sla: 0x1 cost: 0 remote gw: HUB1-VPN1 transport_group
: 0 bandwidth up: 999999 down: 999997 bidirection: 1999996
ipv4: 66.31.1.2(172.16.0.2) ipv6 b0a4:c8e:7f00:0:8a00::(827:4dd4:7f00:0:182a:4dd4:7f00:32)
2: latency: 0.343633 jitter: 0.038267 pktloss: 0.000000 mos: 4.404186 sla: 0x1 cost: 0 remote gw: HUB1-VPN2 transport_group
: 0 bandwidth up: 999999 down: 999997 bidirection: 1999996
ipv4: 43.64.1.2(172.16.0.2) ipv6 7f00:0:d8ff:ffff:80ff:ffff:3029:4dd4(7f00:0:180:adfb:80ff:ffff:182a:4dd4)
```

Validate routing and shortcuts

FortiManager lab configuration and verification

11.04

Check the IPsec tunnel summary for the dynamic, suffixed spoke-to-spoke tunnel. For a fresh LAN flow, compare shortcut counters before and after the test.

```
FG-03 # get vpn ipsec tunnel summary
'HUB1-VPN1_0' 66.31.1.2:0  selectors(total,up): 2/2  rx(pkt,err): 0/0  tx(pkt,err): 0/4
'HUB1-VPN1' 35.1.2.2:0  selectors(total,up): 1/1  rx(pkt,err): 42238/0  tx(pkt,err): 58327/611
'HUB1-VPN2' 40.1.2.2:0  selectors(total,up): 1/1  rx(pkt,err): 35822/0  tx(pkt,err): 48022/582
```

11.05

Verify BGP neighbor state and prefix counts. This capture shows FG-03 peering with FG-04 and the hub.

```
FG-03 # get router info bgp sum

VRF 0 BGP router identifier 172.16.0.1, local AS number 65000
BGP table version is 7
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.2      4      65000       9      10        7    0    0 00:05:15        1
172.16.255.252 4      65000     502     495        6    0    0 01:03:33        2

Total number of neighbors 2


FG-03 #
```

Restore shortcut selection

IPsec selectors were up while shortcut health checks failed.

Match the probe source on both branches

The existing Hub_To_Lo policy allowed 10.10.0.0/16 as its source. The arriving probe used the peer loopback instead, such as 172.16.0.1 → 172.16.0.2 on FG-04.

Field	Setting
Interfaces	HUB1 → Branch-Lo
Source and destination	Spoke loopback address group containing 172.16.0.1/32 and 172.16.0.2/32
Service and action	PING, Accept
NAT	Disabled

Install the policy on both spokes. Under the HUB SLA, check that shortcuts are alive. Start a fresh Windows flow to avoid reusing a session pinned to an older forwarding decision.

```
diagnose sys sdwan health-check
diagnose sys sdwan advpn-session
get vpn ipsec tunnel summary

Windows host: tracert -d 10.10.4.2
```