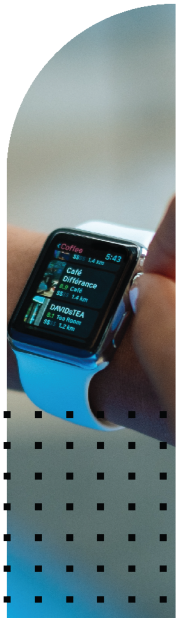
New Features Guide

SD-WAN with FortiOS, FortiManager, and FortiAnalyzer 7.0.x



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 4, 2022
SD-WAN with FortiOS, FortiManager, and FortiAnalyzer 7.0.x New Features Guide
01-700-NNNNNN-20220304

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-02-04	Initial release.
2022-02-16	Added BGP and IPsec recommended templates for SD-WAN overlays FMG 7.0.3 on page 84.
2022-03-04	Added SD-WAN application performance monitoring FAZ 7.0.3 on page 52.

Overview

This guide provides details of new features for SD-WAN introduced in FortiOS 7.0, FortiManager 7.0, and FortiAnalyzer 7.0:

- What's new in 7.0.0 on page 6
- What's new in 7.0.1 on page 7
- What's new in 7.0.2 on page 7
- What's new in 7.0.3 on page 8

For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable. For features introduced in FortiManager or FortiAnalyzer, the short product name is appended to the end of the topic heading, for example FMG or FAZ.

For features introduced in 7.0.1 and later versions, the version number is appended to the end of the topic heading. For example, Display ADVPN shortcut information in the GUI 7.0.1 on page 37 was introduced in 7.0.1. If a topic heading has no version number at the end, the feature was introduced in 7.0.0.

For features introduced in FortiManager or FortiAnalyzer 7.0.1 and later versions, the short product name and version number are appended to the end of the topic heading. For example, IPsec template enhanced support for tunnel interface configuration FMG 7.0.1 on page 66 was introduced in FortiManager 7.0.1.

What's new in 7.0.0

Feature	Details
Application performance	• Usability enhancements to SD-WAN Network Monitor service on page 9 • Hold down time to support SD-WAN service strategies on page 11 • Passive WAN health measurement on page 12
Monitoring	• SD-WAN monitoring improvements FMG on page 31 • Improved secure SD-WAN monitor FAZ on page 35
Provisioning	• New SD-WAN template FMG on page 55
Routing	• ECMP routes for recursive BGP next hop resolution on page 99 • BGP next hop recursive resolution using other BGP routes on page 100 • GUI advanced routing options for BGP on page 101 • GUI page for OSPF settings on page 104 • GUI routing monitor for BGP and OSPF on page 106
WAN remediation	• Packet duplication for dial-up IPsec tunnels on page 119

What's new in 7.0.1

Feature	Details
Application performance	• SD-WAN passive health check configurable on GUI 7.0.1 on page 13 • Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 15 • Interface based QoS on individual child tunnels based on speed test results 7.0.1 on page 22
Cloud	• SD-WAN transit routing with Google Network Connectivity Center 7.0.1 on page 30
Monitoring	• Display ADVPN shortcut information in the GUI 7.0.1 on page 37 • SD-WAN Summary Report FAZ 7.0.1 on page 38 • SD-WAN monitoring improvement FAZ 7.0.1 on page 42
Provisioning	• IPsec template enhanced support for tunnel interface configuration FMG 7.0.1 on page 66 • Templates support assignment to device groups FMG 7.0.1 on page 68 • CLI Template improvements FMG 7.0.1 on page 70
Reporting	• Additional charts for SD-WAN reporting FAZ 7.0.1 on page 93
SD-WAN steering	• ECMP support for the longest match in SD-WAN rule matching 7.0.1 on page 109 • Override quality comparisons in SD-WAN longest match rule matching 7.0.1 on page 111 • Specify an SD-WAN zone in static routes and SD-WAN rules 7.0.1 on page 114

What's new in 7.0.2

Feature	Details
Application performance	• Passive health-check measurement by internet service and application 7.0.2 on page 25
Monitoring	• SD-WAN monitoring shows the SD-WAN rule and its status, active selected member for a given SLA FMG 7.0.2 on page 44 • QoS monitoring support added for dialup VPN interfaces FMG 7.0.2 on page 46 • SD-WAN application bandwidth per interface widget FAZ 7.0.2 on page 47
Provisioning	• BGP template to manage all BGP routing configurations FMG 7.0.2 on page 74 • Import IPSec VPN configuration from a managed FortiGate into a IPSec template FMG 7.0.2 on page 81

Feature	Details
WAN remediation	• Adaptive Forward Error Correction 7.0.2 on page 123

What's new in 7.0.3

Feature	Details
Monitoring	• SD-WAN real-time monitoring (30 seconds) supported per-device FMG 7.0.3 on page 51 • SD-WAN application performance monitoring FAZ 7.0.3 on page 52
Provisioning	• Import BGP routing configuration from a managed FortiGate into a template FMG 7.0.3 on page 83 • BGP and IPsec recommended templates for SD-WAN overlays FMG 7.0.3 on page 84

Application performance

7.0.0

7.0.1

7.0.2

Usability enhancements to SD-WAN Network Monitor service

The SD-WAN Network Monitor service now supports running a speed test based on a schedule. The test results are automatically updated in the interface `measured-upstream-bandwidth` and `measured-downstream-bandwidth` fields. These fields do not impact the interface inbound bandwidth, outbound bandwidth, estimated upstream bandwidth, or estimated downstream bandwidth settings.

When the scheduled speed tests run, it is possible to temporarily bypass the bandwidth limits set on the interface and configure custom maximum or minimum bandwidth limits. These configurations are optional.

```
config system speed-test-schedule
    edit <interface>
        set schedules <schedule> ...
        set update-inbandwidth enable {enable | disable}
        set update-outbandwidth enable {enable | disable}
        set update-inbandwidth-maximum <integer>
        set update-inbandwidth-minimum <integer>
        set update-outbandwidth-maximum <integer>
        set update-outbandwidth-minimum <integer>
    next
end
```

`update-inbandwidth enable {enable | disable}`	Enable/disable bypassing the interface's inbound bandwidth setting.
`update-outbandwidth enable {enable | disable}`	Enable/disable bypassing the interface's outbound bandwidth setting.
`update-inbandwidth-maximum <integer>`	Maximum downloading bandwidth to be used in a speed test, in Kbps (0 - 16776000).

`update-inbandwidth-minimum <integer>`	Minimum downloading bandwidth to be considered effective, in Kbps (0 - 16776000).
`update-outbandwidth-maximum <integer>`	Maximum uploading bandwidth to be used in a speed test, in Kbps (0 - 16776000).
`update-outbandwidth-minimum <integer>`	Minimum uploading bandwidth to be considered effective, in Kbps (0 - 16776000).

In the following example, a speed test is scheduled on port1 at 10:00 AM, and another one at 14:00 PM.

To run a speed test based on a schedule:

1. Configure the recurring schedules:

```
config firewall schedule recurring
    edit "10"
        set start 10:00
        set end 12:00
        set day monday tuesday wednesday thursday friday
    next
    edit "14"
        set start 14:00
        set end 16:00
        set day monday tuesday wednesday thursday friday
    next
end
```

2. Configure the speed test schedule:

```
config system speed-test-schedule
    edit "port1"
        set schedules "10" "14"
        set update-inbandwidth enable
        set update-outbandwidth enable
        set update-inbandwidth-maximum 60000
        set update-inbandwidth-minimum 10000
        set update-outbandwidth-maximum 50000
        set update-outbandwidth-minimum 10000
    next
end
```

3. View the speed test results:

```
config system interface
    edit port1
        get | grep measure
            measured-upstream-bandwidth: 23691
            measured-downstream-bandwidth: 48862
            bandwidth-measure-time:  Wed Jan 27 14:00:39 2021
    next
end
```

Hold down time to support SD-WAN service strategies

In a hub and spoke SD-WAN topology with shortcuts created over ADVPN, a downed or recovered shortcut can affect which member is selected by an SD-WAN service strategy. When a downed shortcut tunnel recovers and the shortcut is added back into the service strategy, the shortcut is held at a low priority until the hold down time has elapsed.

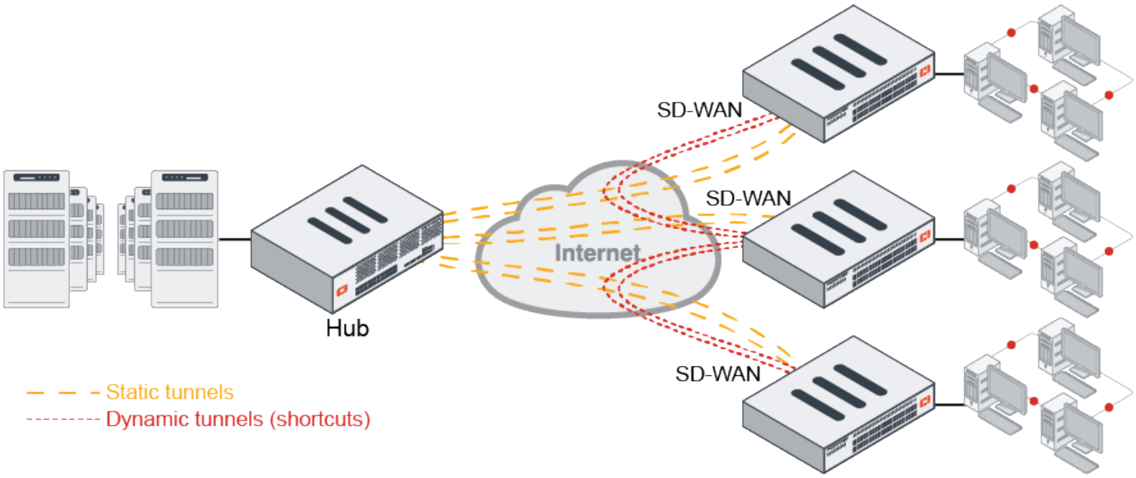
By default, the hold down time is zero seconds. It can be set to 0 - 10000000 seconds.

To configure the hold down time:

```
config system sdwan
    config service
        edit 1
            set hold-down-time <integer>
        next
    end
end
```

Example

In this example, the hold down time is set to 15 seconds, and then the SD-WAN service is looked at before and after the hold down elapses after a downed shortcut recovers.



To configure the hold down time:

```
config system sdwan
    config service
        edit 1
            set hold-down-time 15
        next
    end
end
```

To view which SD-WAN member is selected before and after the hold down time elapses:

Before the hold down time has elapsed:

```
# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(34), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(ping)
Hold down time(15) seconds, Hold start at 2003 second, now 2010
  Member sub interface(4):
    1: seq_num(1), interface(vd2-1):
       1: vd2-1_0(86)
    3: seq_num(2), interface(vd2-2):
       1: vd2-2_0(88)

  Members(4):
    1: Seq_num(1 vd2-1), alive, packet loss: 27.000%, selected
    2: Seq_num(2 vd2-2_0), alive, packet loss: 0.000%, selected
    3: Seq_num(2 vd2-2), alive, packet loss: 0.000%, selected
    4: Seq_num(1 vd2-1_0), alive, packet loss: 61.000%, selected
  Dst address(1):
        33.1.1.101-33.1.1.200
```

After the hold down time has elapsed:

```
# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(35), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(ping)
Hold down time(15) seconds, Hold start at 2018 second, now 2019
  Member sub interface(4):

    2: seq_num(2), interface(vd2-2):
       1: vd2-2_0(88)
    3: seq_num(1), interface(vd2-1):
       1: vd2-1_0(86)
  Members(4):
    1: Seq_num(2 vd2-2_0), alive, packet loss: 0.000%, selected
    2: Seq_num(2 vd2-2), alive, packet loss: 0.000%, selected
    3: Seq_num(1 vd2-1), alive, packet loss: 24.000%, selected
    4: Seq_num(1 vd2-1_0), alive, packet loss: 44.000%, selected
  Dst address(1):
        33.1.1.101-33.1.1.200\
```

Passive WAN health measurement

SD-WAN passive WAN health measurement determines the health check measurements using session information that is captured on firewall policies that have `passive-wan-health-measurement` enabled.

Using passive WAN health measurement reduces the amount of configuration required and decreases the traffic that is produced by health check monitor probes doing active measurements. Active WAN health measurement using a detection server might not reflect the real-life traffic.

By default, active WAN health measurement is enabled.

To configure passive WAN health check:

```
config system sdwan
    config health-check
        edit "1"
            set server <ip_address>
            set detect-mode {passive | prefer-passive}
            set members <members>
        next
    end
end
```

`passive`	Health is measured using traffic, without probes. No link health monitor needs to be configured.
`prefer-passive`	Health is measured using traffic when there is traffic, and using probes when there is no traffic. A link health monitor must be configured, see Link health monitor for details.

To enable passive WAN health measurement in a policy:

```
config firewall policy
    edit 1
        set passive-wan-health-measurement enable
    next
end
```

When `passive-wan-health-measurement` is enabled, `auto-asic-offload` will be disabled.

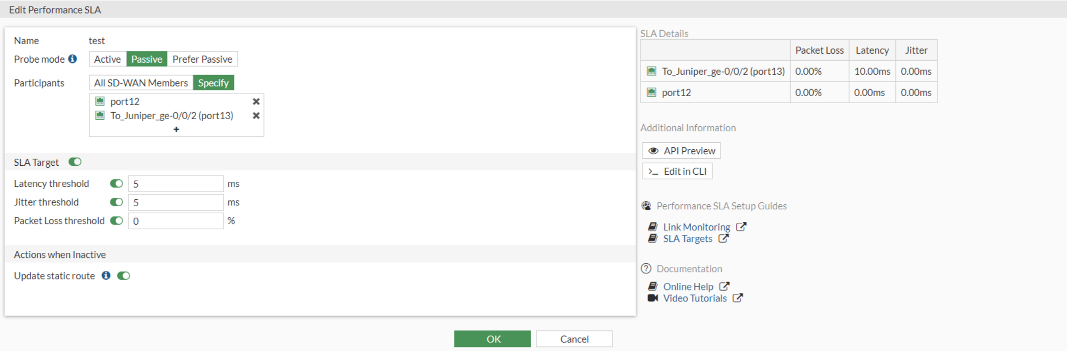
SD-WAN passive health check configurable on GUI - 7.0.1

SD-WAN passive WAN health can be configured in the GUI.

By enabling passive health check in a policy, TCP traffic on that policy will be used in health check measurements.

To configure passive WAN health check in the GUI:

1. Go to *Network* > *SD-WAN* and select the *Performance SLAs* tab.
2. Edit an existing health check, or create a new one.
3. Set *Probe mode* to *Passive* or *Prefer Passive*.



Edit Performance SLA

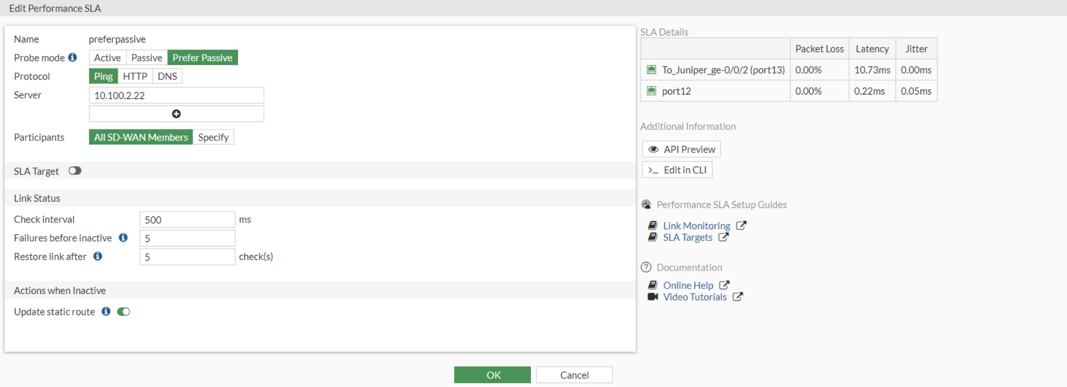
Name: test
Probe mode: Active | **Passive** | Prefer Passive
Participants: All SD-WAN Members | **Specify**
- port12
- To_Juniper_ge-0/0/2 (port13)

SLA Target: on
Latency threshold: 5 ms
Jitter threshold: 5 ms
Packet Loss threshold: 0 %

Actions when Inactive
Update static route: on

SLA Details

	Packet Loss	Latency	Jitter
To_Juniper_ge-0/0/2 (port13)	0.00%	10.00ms	0.00ms
port12	0.00%	0.00ms	0.00ms



Edit Performance SLA

Name: preferpassive
Probe mode: Active | Passive | **Prefer Passive**
Protocol: **Ping** | HTTP | DNS
Server: 10.100.2.22
Participants: **All SD-WAN Members** | Specify

SLA Target: off

Link Status
Check interval: 500 ms
Failures before inactive: 5
Restore link after: 5 check(s)

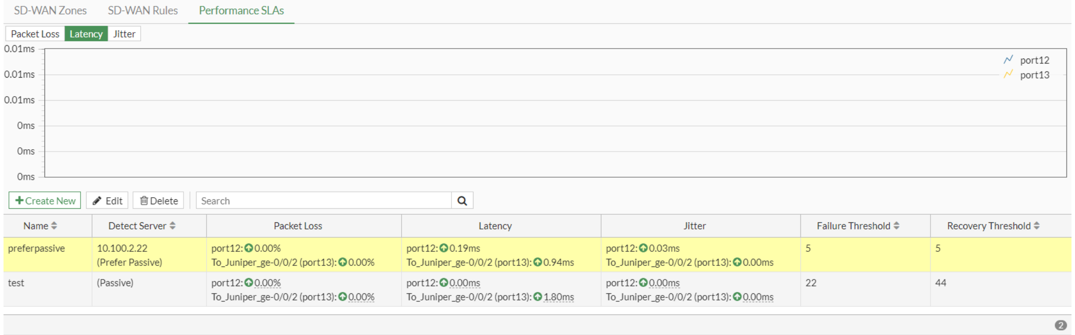
Actions when Inactive
Update static route: on

SLA Details

	Packet Loss	Latency	Jitter
To_Juniper_ge-0/0/2 (port13)	0.00%	10.73ms	0.00ms
port12	0.00%	0.22ms	0.05ms

4. Configure the remaining settings as needed.
5. Click *OK*.

   The SLA list shows the probe mode in the *Detect Server* column, if the probe mode is passive or prefer passive.

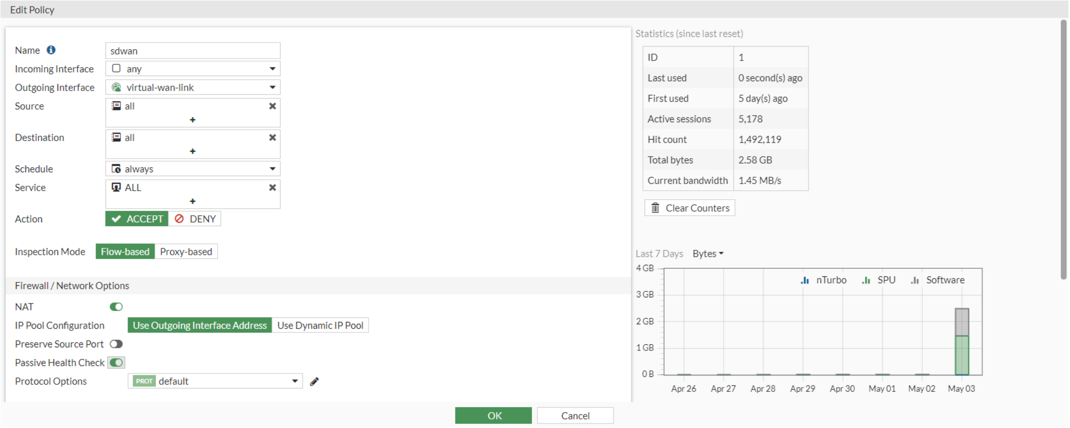


Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
preferpassive	10.100.2.22 (Prefer Passive)	port12: 0.00% To_Juniper_ge-0/0/2 (port13): 0.00%	port12: 0.19ms To_Juniper_ge-0/0/2 (port13): 0.94ms	port12: 0.03ms To_Juniper_ge-0/0/2 (port13): 0.00ms	5	5
test	(Passive)	port12: 0.00% To_Juniper_ge-0/0/2 (port13): 0.00%	port12: 0.00ms To_Juniper_ge-0/0/2 (port13): 1.80ms	port12: 0.00ms To_Juniper_ge-0/0/2 (port13): 0.00ms	22	44

Probe packets can only be disabled in the CLI and when the probe mode is not passive.

To enable passive WAN health measurement in a policy in the GUI:

1. Go to *Policy & Objects > Firewall Policy*.
2. Edit an existing policy, or create a new one.
3. Set *Outgoing Interface* to an SD-WAN zone. Passive health check can only be enabled in a policy when the outgoing interface is an SD-WAN zone.
4. Enable *Passive Health Check*.



Edit Policy

Name: sdwan
Incoming Interface: any
Outgoing Interface: virtual-wan-link
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ACCEPT | DENY
Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options

NAT: enabled
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: disabled
Passive Health Check: enabled
Protocol Options: PROT default

Statistics (since last reset)

ID	1
Last used	0 second(s) ago
First used	5 day(s) ago
Active sessions	5,178
Hit count	1,492,119
Total bytes	2.58 GB
Current bandwidth	1.45 MB/s

5. Configure the remaining settings as needed.
6. Click *OK*.

Speed tests run from the hub to the spokes in dial-up IPsec tunnels - 7.0.1

In a hub and spoke SD-WAN topology that uses dial-up VPN overlays, QoS can be applied on individual tunnels based on the measured bandwidth between the hub and spokes. The FortiGate can use the built in speed test to dynamically populate the egress bandwidth to individual dial-up tunnels from the hub.

SD-WAN members on a spoke can switch routes when the speed test is running from the hub to the spoke. The speed test results can be cached for reuse when a tunnel comes back after going down.

CLI commands

Allow upload speed tests to be run from the hub to spokes on demand for dial-up IPsec tunnel:

```
config system speed-test-schedule
    edit <interface>
        set dynamic-server {enable | disable}
    next
end
```

`<interface>`	The dial-up IPsec tunnel interface on the hub.
`dynamic-server {enable	disable}`	Enable/disable the dynamic speed test server (default = disable).

To limit the maximum and minimum bandwidth used in the speed test, enable `set update-inbandwidth` and `set update-outbandwidth`. See Scheduled interface speedtest for more information.

```
config system global
   set speed-test-server {enable | disable}
end
```

`speed-test-server {enable	disable}`	Enable/disable the speed test server on the spoke (default = disable). This setting must be enabled on spoke FortiGates. This enables iPerf in server mode, which listens on the default iPerf TCP port 5201.

Allow an SD-WAN member on the spoke to switch routes when it is on speed test from the hub to spokes:

```
config system sdwan
    set speedtest-bypass-route {enable | disable}
    config neighbor
        edit <bgp neighbor>
            set mode speedtest
        next
    end
end
```

`speedtest-bypass-route {enable	disable}`	Enable/disable bypass routing when doing a speed test on an SD-WAN member (default = disable).
`set mode speedtest`	Use the speed test to select the neighbor.

Manually run uploading speed test on the physical interfaces of each tunnel of an dial-up IPsec interface:

```
execute speed-test-dynamic <interface> <tunnel_name> <'y'/'n'> <max-out> <min-out>
```

`<interface>`	IPsec phase1 interface name.
`<tunnel_name>`	The tunnel name, or `all` for all tunnels.
`<'y'/'n'>`	Apply the result to the tunnels' shaper or not.
`<max-out>`	The maximum speed used in a speed test, in kbps.
`<min-out>`	The minimum speed used in a speed test, in kbps.

Manually run a non-blocking uploading speed test:

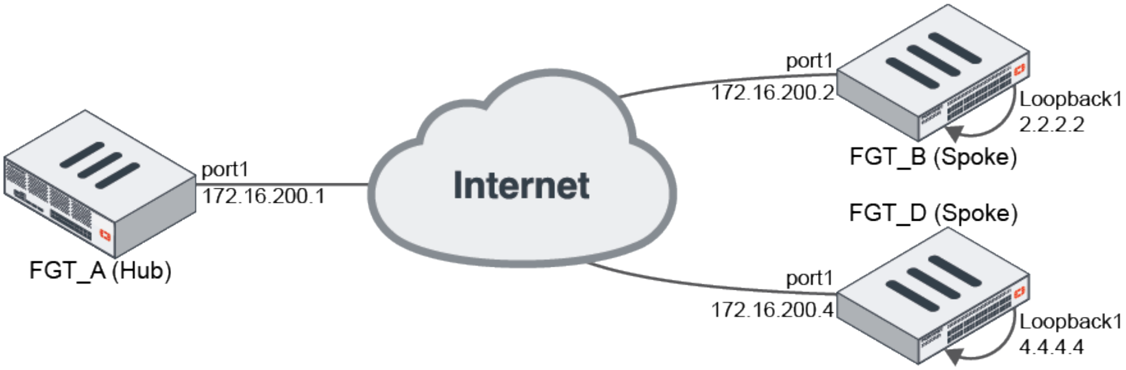
```
diagnose netlink interface speed-test-tunnel <interface> <tunnel_name>
```

Debug and test commands:

`diagnose debug application speedtest <int>`	Enable debug of the speed test module in the forticron daemon.
`diagnose debug application speedtestd <int>`	Enable debug of the speed test server daemon.
`diagnose test application forticron 9`	List the scheduled speed tests.

`diagnose test application forticron 10`	Show the cached speed test results.
`diagnose test application forticron 11`	Write the cached speed test results to disk.
`diagnose test application forticron 12`	Load the speed test results from disk.
`diagnose test application forticron 99`	Cancel all pending speed tests.

Example



In this example, the hub is configured as a VPN dial-up server and both of the spokes are connected to the hub. It is assumed that the VPN configuration is already done, with a dynamic gateway type and kernel device creation (`net-device`) disabled. Only one SD-WAN interface is used, so there is only one VPN overlay member in the SD-WAN zone. Multiple WAN interfaces and VPN overlays could be used.

The VPN interfaces and IP addresses are:

FortiGate	Interface	IP Address
FGT_A (Hub)	hub-phase1	10.10.100.254
FGT_B (Spoke)	spoke11-p1	10.10.100.2
FGT_D (Spoke)	spoke21-p1	10.10.100.3

A recurring speed test is configured that runs on the hub over the dial-up interfaces. The speed tests are performed over the underlay interface from the hub to the spoke. Each spoke is configured to operate as a speed test server and to allow the speed test to run on its underlay interface. The spokes establish BGP peering with the hub over the VPN interface, and advertises its loopback network to the hub. The specific configuration is only shown for FGT_B.

When the speed test is running, routing through the VPN overlay can be bypassed, and route maps are used to filter the routes that are advertised to peers. The spoke's route map does not advertise any routes to the peer, forcing the hub to use others paths to reach the spoke's network.

When no speed tests are running, the spoke's route map allows its network to be advertised on the hub.

When the speed test is complete, the measured egress bandwidth is dynamically applied to the VPN tunnel on the hub, and the result is cached for future use, in case the tunnel is disconnected and reconnected again.

To configure the hub FortiGate (FGT_A):

1. Configure a shaping profile:

   ```
   config firewall shaping-profile
       edit "profile_1"
           config shaping-entries
               edit 1
                   set class-id 2
                   set priority low
                   set guaranteed-bandwidth-percentage 10
                   set maximum-bandwidth-percentage 10
               next
           end
           set default-class-id 2
       next
   end
   ```

   Three classes are used in the profile for low, medium, and high priority traffic. Each class is assigned a guaranteed and maximum bandwidth as a percentage of the measured bandwidth from the speed test.

2. Use the shaping profile in the interface:

   ```
   config system interface
       edit "hub-phase1"
           set egress-shaping-profile "profile_1"
       next
   end
   ```

3. Configure a schedule to use for the speed tests:

   ```
   config firewall schedule recurring
       edit "speedtest_recurring"
           set start 01:00
           set end 23:00
           set day monday tuesday wednesday thursday friday saturday
       next
   end
   ```

4. Configure the speed test schedule:

   ```
   config system speed-test-schedule
       edit "hub-phase1"
           set schedules "speedtest_recurring"
           set dynamic-server enable
       next
   end
   ```

To configure the spoke FortiGates (FGT_B and FGT_D):

1. Enable the speed test daemon:

   ```
   config system global
       set speedtest-server enable
   end
   ```

2. Allow speed tests on the interface:

   ```
   config system interface
       edit "port1"
   ```

```
        append allowaccess speed-test
    next
end
```

3. Configure SD-WAN with bypass routing enabled for speed tests on member *spoke11-p1*:

```
config system sdwan
    set speedtest-bypass-routing enable
    config members
        edit 1
            set interface "spoke11-p1"
        next
    end
    config neighbor
        edit "10.10.100.254"
            set member 1
            set mode speedtest
        next
    end
end
```

4. Configure BGP routing:

```
config router route-map
    edit "No_Speed-Test"
        config rule
            edit 1
                set action permit
            next
        end
    next
    edit "Start_Speed-Test"
        config rule
            edit 1
                set action deny
            next
        end
    next
end
```

```
config router bgp
    set as 65412
    config neighbor
        edit "10.10.100.254"
            set remote-as 65412
            set route-map-out "Start_Speed-Test"
            set route-map-out-preferable "No_Speed-Test"
        next
    end
    config network
        edit 1
            set prefix 2.2.2.2 255.255.255.255
        next
        edit 2
            set prefix 10.1.100.0 255.255.255.0
        next
    end
end
```

To manually run the speed test:

```
# execute speed-test-dynamic hub-phase1 all y 1000 100
Start testing the speed of each tunnel of hub-phase1
[6400d9] hub-phase1_0: physical_intf=port1, local_ip=172.16.200.1, server_ip=172.16.200.2
Wait for test 6400d9 to finish...
Speed-test result for test ID 6400d9:
    Completed
    measured upload bandwidth is 1002 kbps
    measured time Sun Jun 20 15:56:34 2021

The tested out-bandwidth is more than the set maximum accepted value 1000. Will update the
tunnel's shaper by the set update-outbandwidth-maximum.
Apply shaping profile 'profile_1' with bandwidth 1000 to tunnel hub-phase1_0 of interface
hub-phase1
[6400e0] hub-phase1_1: physical_intf=port1, local_ip=172.16.200.1, server_ip=172.16.200.4
Wait for test 6400e0 to finish...
Speed-test result for test ID 6400e0:
    Completed
    measured upload bandwidth is 1002 kbps
    measured time Sun Jun 20 15:56:39 2021

The tested out-bandwidth is more than the set maximum accepted value 1000. Will update the
tunnel's shaper by the set update-outbandwidth-maximum.
Apply shaping profile 'profile_1' with bandwidth 1000 to tunnel hub-phase1_1 of interface
hub-phase1
```

```
# diagnose netlink interface speed-test-tunnel hub-phase1 all
send speed test request for tunnel 'hub-phase1_0' of 'hub-phase1': 172.16.200.1 ->
172.16.200.2
send speed test request for tunnel 'hub-phase1_1' of 'hub-phase1': 172.16.200.1 ->
172.16.200.4
```

Results

1. Before the speed test starts, FGT_A can receive the route from FGT_B by BGP:

   ```
   # get router info routing-table bgp
   Routing table for VRF=0
   B       2.2.2.2/32 [200/0] via 10.10.100.2 (recursive via 172.16.200.2, hub-phase1),
   00:00:10
   B       10.1.100.0/24 [200/0] via 10.10.100.2 (recursive via 172.16.200.2, hub-phase1),
   00:00:10
   ```

2. At the scheduled time, the speed test starts for the hub-phase1 interface from hub to spoke:

   ```
   # diagnose test application forticron 9
   Speed test schedules:
       Interface     Server     Update    Up/Down-limit (kbps)                Days
   H:M     TOS     Schedule
   ------------------------------------------------------------------------------------
   -----------------------------------
       hub-phase1    dynamic                                                  1111111
   14:41    0x00    speedtest_recurring
   Active schedules:
   ```

```
        64002f: hub-phase1(port1) 172.16.200.2     hub-phase1_1
        64002e: hub-phase1(port1) 172.16.200.4     hub-phase1_0
```

The `diagnose debug application speedtest -1` command can be used on both the hub and spokes to check the speed test execution.

3. While the speed test is running, FGT_A does not receive the route from FGT_B by BGP:

```
#  get router info routing-table bgp
Routing table for VRF=0
```

4. Speed tests results can be dynamically applied to the dial-up tunnel for egress traffic shaping:

```
# diagnose vpn tunnel list
------------------------------------------------------
name=hub-phase1_0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 tun_id=172.16.200.4 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
        bandwidth=737210(kbps) lock_hit=0 default_class=2 n_active_class=3
        class-id=2      allocated-bandwidth=73720(kbps)         guaranteed-
bandwidth=73720(kbps)
                        max-bandwidth=73720(kbps)       current-bandwidth=0(kbps)
                        priority=low    forwarded_bytes=52
                        dropped_packets=0       dropped_bytes=0
        class-id=3      allocated-bandwidth=221163(kbps)        guaranteed-
bandwidth=221162(kbps)
                        max-bandwidth=294883(kbps)      current-bandwidth=0(kbps)
                        priority=medium         forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
        class-id=4      allocated-bandwidth=442325(kbps)        guaranteed-
bandwidth=147441(kbps)
                        max-bandwidth=442325(kbps)      current-bandwidth=0(kbps)
                        priority=high   forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
------------------------------------------------------
name=hub-phase1_1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 tun_id=172.16.200.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
        bandwidth=726813(kbps) lock_hit=0 default_class=2 n_active_class=3
        class-id=2      allocated-bandwidth=72681(kbps)         guaranteed-
bandwidth=72681(kbps)
                        max-bandwidth=72681(kbps)       current-bandwidth=0(kbps)
                        priority=low    forwarded_bytes=123
                        dropped_packets=0       dropped_bytes=0
        class-id=3      allocated-bandwidth=218044(kbps)        guaranteed-
bandwidth=218043(kbps)
                        max-bandwidth=290725(kbps)      current-bandwidth=0(kbps)
                        priority=medium         forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
        class-id=4      allocated-bandwidth=436087(kbps)        guaranteed-
bandwidth=145362(kbps)
                        max-bandwidth=436087(kbps)      current-bandwidth=0(kbps)
                        priority=high   forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
```

5. Speed test results can be cached, indexed, and written to disk:

```
# diagnose test application forticron 10
Speed test results:
1: vdom=root, phase1intf=hub-phase1, peer-id='spoke11-p1', bandwidth=737210, last_
log=1624226603
2: vdom=root, phase1intf=hub-phase1, peer-id='spoke21-p1', bandwidth=726813, last_
log=1624226614
```

```
# diagnose test application forticron 11
Write 2 logs to disk.
```

```
# diagnose test application forticron 12
load 2 results.
```

Disable then reenable the IPsec VPN tunnel and the cached speed test results can be applied to the tunnel again:

```
# diagnose vpn tunnel  list
------------------------------------------------------
name=hub-phase1_0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 tun_id=172.16.200.4 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
        bandwidth=737210(kbps) lock_hit=0 default_class=2 n_active_class=3
------------------------------------------------------
name=hub-phase1_1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 tun_id=172.16.200.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
        bandwidth=726813(kbps) lock_hit=0 default_class=2 n_active_class=3
```

Interface based QoS on individual child tunnels based on speed test results - 7.0.1

In a hub and spoke SD-WAN topology that uses dial-up VPN overlays, QoS can be applied on individual tunnels based on the measured bandwidth between the hub and spokes. The FortiGate can use the built in speed test to dynamically populate the egress bandwidth to individual dial-up tunnels from the hub.

A bandwidth limit, derived from the speed test, and a traffic shaping profile can be applied on the dial-up IPsec tunnel interface on the hub. A class ID and percentage based QoS settings can be applied to individual child tunnels using a traffic shaping policy and profile.

CLI commands

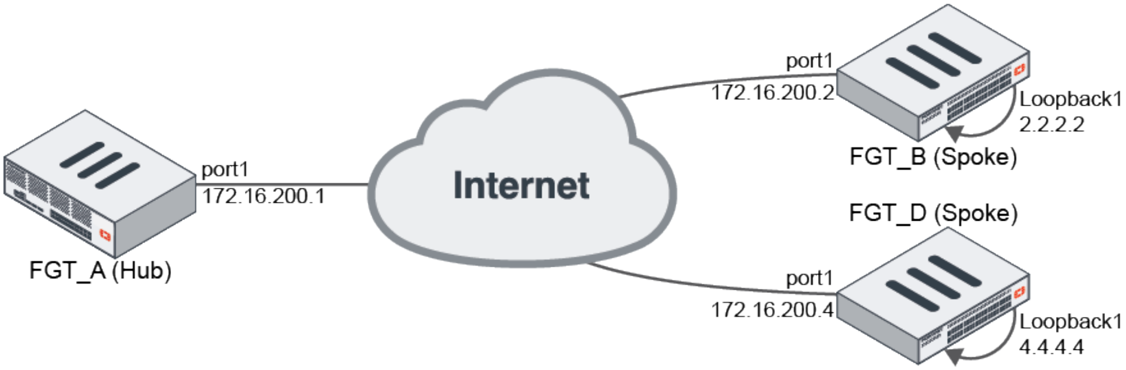
If the interface is an IPsec dial-up server, then egress shaping profile type can only be set to `policing`; it cannot be set to `queuing`:

```
config firewall shaping-profile
    edit <profile-name>
        set type policing
    next
end
```

The outbandwidth value is dynamically obtained from the speed test results for each individual child tunnel, and should not be set manually:

```
config system interface
    edit <dialup-server-phase1-name>
        set egress-shaping-profile <profile-name>
        set outbandwidth <bandwidth>
    next
end
```

Example



In this example, the hub is configured as a VPN dial-up server and both of the spokes are connected to the hub. It is assumed that the VPN configuration is already done, with a dynamic gateway type and kernel device creation (`net-device`) disabled. Only one SD-WAN interface is used, so there is only one VPN overlay member in the SD-WAN zone. Multiple WAN interfaces and VPN overlays could be used.

The VPN interfaces and IP addresses are:

FortiGate	Interface	IP Address
FGT_A (Hub)	hub-phase1	10.10.100.254
FGT_B (Spoke)	spoke11-p1	10.10.100.2
FGT_D (Spoke)	spoke21-p1	10.10.100.3

The hub VPN has two child tunnels, one to each spoke.

The speed test configuration is shown in Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 15. This example shows applying a shaping profile to the hub's tunnel interface in order to apply interface based traffic shaping to the child tunnels.

A traffic shaping policy is used to match and assign traffic to the classes in the shaping profile.

To configure the hub FortiGate (FGT_A) and check the results:

1. Configure the hub FortiGate (FGT_A) as in Speed tests run from the hub to the spokes in dial-up IPsec tunnels 7.0.1 on page 15.
2. Configure the shaping profile:

```
config firewall shaping-profile
    edit "profile_1"
        config shaping-entries
            edit 1
                set class-id 2
                set priority low
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 10
            next
            edit 2
                set class-id 3
                set priority medium
                set guaranteed-bandwidth-percentage 30
                set maximum-bandwidth-percentage 40
            next
            edit 3
                set class-id 4
                set priority high
                set guaranteed-bandwidth-percentage 20
                set maximum-bandwidth-percentage 60
            next
        end
        set default-class-id 2
    next
end
```

3. Configure a traffic shaping policy:

```
config firewall shaping-policy
    edit 2
        set service "ALL"
        set schedule "always"
        set dstintf "hub-phase1"
        set class-id 3
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

   In this example, all traffic through the hub-phase1 interface is put into class ID 3. Class IDs an be assigned based on your traffic requirements.

4. At the schedules time, the speed test will start for the hub-phase1 interface from the hub to the spokes. The speed test results can then be dynamically applied on individual child tunnels as egress traffic shaping, and the class ID percentage based QoS settings is applicable on them as templates.

```
# diagnose vpn tunnel  list
------------------------------------------------------
name=hub-phase1_0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 tun_id=172.16.200.4 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
        bandwidth=737210(kbps) lock_hit=0 default_class=2 n_active_class=3
        class-id=2      allocated-bandwidth=73720(kbps)         guaranteed-
bandwidth=73720(kbps)
                        max-bandwidth=73720(kbps)       current-bandwidth=0(kbps)
                        priority=low    forwarded_bytes=52
                        dropped_packets=0       dropped_bytes=0
        class-id=3      allocated-bandwidth=221163(kbps)        guaranteed-
bandwidth=221162(kbps)
                        max-bandwidth=294883(kbps)      current-bandwidth=0(kbps)
                        priority=medium         forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
        class-id=4      allocated-bandwidth=442325(kbps)        guaranteed-
bandwidth=147441(kbps)
                        max-bandwidth=442325(kbps)      current-bandwidth=0(kbps)
                        priority=high   forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
------------------------------------------------------
name=hub-phase1_1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 tun_id=172.16.200.2 dst_
mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
...
egress traffic control:
        bandwidth=726813(kbps) lock_hit=0 default_class=2 n_active_class=3
        class-id=2      allocated-bandwidth=72681(kbps)         guaranteed-
bandwidth=72681(kbps)
                        max-bandwidth=72681(kbps)       current-bandwidth=0(kbps)
                        priority=low    forwarded_bytes=123
                        dropped_packets=0       dropped_bytes=0
        class-id=3      allocated-bandwidth=218044(kbps)        guaranteed-
bandwidth=218043(kbps)
                        max-bandwidth=290725(kbps)      current-bandwidth=0(kbps)
                        priority=medium         forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
        class-id=4      allocated-bandwidth=436087(kbps)        guaranteed-
bandwidth=145362(kbps)
                        max-bandwidth=436087(kbps)      current-bandwidth=0(kbps)
                        priority=high   forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
```

The guaranteed and maximum bandwidths equal 10% of the speed test result, as expected.

Passive health-check measurement by internet service and application - 7.0.2

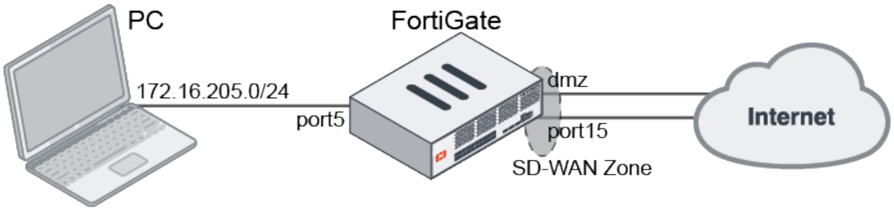
Passive health measurement supports passive detection for each internet service and application.

If internet services or applications are defined in an SD-WAN rule with passive health check, SLA information for each service or application will be differentiated and collected. SLA metrics (latency, jitter, and packet loss) on each SD-WAN member in the rule are then calculated based on the relevant internet service's or application's SLA information.

In this example, three SD-WAN rules are created:

- Rule 1: Best quality (latency) using passive SLA for the internet services Alibaba and Amazon.
- Rule 2: Best quality (latency) using passive SLA for the applications Netflix and YouTube.
- Rule 3: Best quality (latency) using passive SLA for all other traffic.

After passive application measurement is enabled for rules one and two, the SLA metric of rule one is the average latency of the internet services Alibaba and Amazon, and the SLA metric of rule two is the average latency of the applications Netflix and YouTube.



To configure the SD-WAN:

1. Configure the SD-WAN members:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 2
            set interface "port15"
            set gateway 172.16.209.2
        next
    end
end
```

2. Configure the passive mode health check:

```
config health-check
    edit "Passive_HC"
        set detect-mode passive
        set members 1 2
    next
end
```

3. Configure SD-WAN service rules:

```
config service
    edit 1
        set name "1"
        set mode priority
        set src "172.16.205.0"
        set internet-service enable
        set internet-service-name "Alibaba-Web" "Amazon-Web"
        set health-check "Passive_HC"
        set priority-members 1 2
        set passive-measurement enable    //Enable "passive application measurement", it
is a new command which is introduced in this project.
    next
    edit 2
        set name "2"
        set mode priority
        set src "172.16.205.0"
        set internet-service enable
        set internet-service-app-ctrl 18155 31077
        set health-check "Passive_HC"
        set priority-members 1 2
        set passive-measurement enable    ////Enable "passive application measurement"
    next
    edit 3
        set name "3"
        set mode priority
        set dst "all"
        set src "172.16.205.0"
        set health-check "Passive_HC"
        set priority-members 1 2
    next
end
```

4. Configure SD-WAN routes:

```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

5. Configure the firewall policy with passive WAN health measurement enabled:

```
config firewall policy
    edit 1
        set uuid 972345c6-1595-51ec-66c5-d705d266f712
        set srcintf "port5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "172.16.205.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "g-default"
        set auto-asic-offload disable
    next
end
```

To verify the results:

1. On the PC, open the browser and visit the internet services and applications.
2. On the FortiGate, check the collected SLA information to confirm that each server or application on the SD-WAN members was measured individually:

```
# diagnose sys link-monitor-passive interface

Interface dmz (5):
       Default(0x00000000): latency=3080.0  11:57:54, jitter=5.0     11:58:08, 
pktloss=0.0  % NA
   Alibaba-Web(0x00690001): latency=30.0    11:30:06, jitter=25.0    11:29:13, 
pktloss=0.0  % NA
       YouTube(0x00007965): latency=100.0   12:00:35, jitter=2.5     12:00:30,
pktloss=0.0  % NA
       Netflix(0x000046eb): latency=10.0    11:31:24, jitter=10.0    11:30:30,
pktloss=0.0  % NA
    Amazon-Web(0x00060001): latency=80.0    11:31:52, jitter=35.0    11:32:07,
pktloss=0.0  % NA

Interface port15 (27):
       Default(0x00000000): latency=100.0   12:00:42, jitter=0.0     12:00:42,
pktloss=0.0  % NA
    Amazon-Web(0x00060001): latency=30.0    11:56:05, jitter=0.0     11:55:21,
pktloss=0.0  % NA
   Alibaba-Web(0x00690001): latency=0.0     11:26:08, jitter=35.0    11:27:08,
pktloss=0.0  % NA
       YouTube(0x00007965): latency=100.0   11:33:34, jitter=0.0     11:33:50,
pktloss=0.0  % NA
       Netflix(0x000046eb): latency=0.0     11:26:29, jitter=0.0     11:29:03,
pktloss=0.0  % NA
```

3. Verify that the SLA metrics on the members are calculated as expected:

```
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x600 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), heath-check(Passive_HC)
  Members(2):
    1: Seq_num(2 port15), alive, latency: 15.000, selected           // Average latency
of "Alibaba-Web" and "Amazon-Web" on port15:     15.000 = (0.0+30.0)/2
    2: Seq_num(1 dmz), alive, latency: 55.000, selected              // Average latency
of "Alibaba-Web" and "Amazon-Web" on dmz:         55.000 = (30.0+80.0)/2
  Internet Service(2): Alibaba-Web(6881281,0,0,0) Amazon-Web(393217,0,0,0)
  Src address(1):
        172.16.205.0-172.16.205.255

Service(2): Address Mode(IPV4) flags=0x600 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), heath-check(Passive_HC)
  Members(2):
    1: Seq_num(1 dmz), alive, latency: 55.000, selected               // Average latency
of "Netflix" and "YouTube" on dmz:        55.000 = (10.0+100.0)/2
    2: Seq_num(2 port15), alive, latency: 50.000, selected           // Average latency
of "Netflix" and "YouTube" on port15:     50.000 = (0.0+100.0)/2
  Internet Service(2): Netflix(4294837427,0,0,0 18155) YouTube(4294838283,0,0,0 31077)
  Src address(1):
        172.16.205.0-172.16.205.255

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(9), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), heath-check(Passive_HC)
  Members(2):
    1: Seq_num(2 port15), alive, latency: 46.000, selected          // Average latency
of all TCP traffic on port15:       46   = (100.0+30.0+0.0+100.0+0.0)/5
    2: Seq_num(1 dmz), alive, latency: 660.000, selected           // Average latency of
all TCP traffic on dmz:           660 = (3080.0+30.0+100.0+10.0+80.0)/5
  Src address(1):
          172.16.205.0-172.16.205.255

    Dst address(1):
          0.0.0.0-255.255.255.255
```

Cloud

7.0.1

SD-WAN transit routing with Google Network Connectivity Center - 7.0.1

With an SD-WAN transit routing setup with Google Network Connectivity Center (NCC), you can route data and exchange border gateway protocol (BGP) routing information between two or more remote sites via GCP.

You can do this by configuring the NCC hub and an endpoint (spoke) for each remote site. To reduce network latency, deploy a spoke in the GCP region that is located geographically closest to the remote site that you are creating the spoke for. The NCC hub itself is VPC-specific.

For a detailed example, see SD-WAN transit routing with Google Network Connectivity Center.

Monitoring

7.0.0

7.0.1

7.0.2

7.0.3

SD-WAN monitoring improvements - FMG

SD-WAN Monitor now includes information about ADVPN shortcut interfaces for monitoring SD-WAN networks. When device history monitoring is enabled for *SD-WAN Monitor*, the device history also includes information about ADVPN shortcut interfaces.

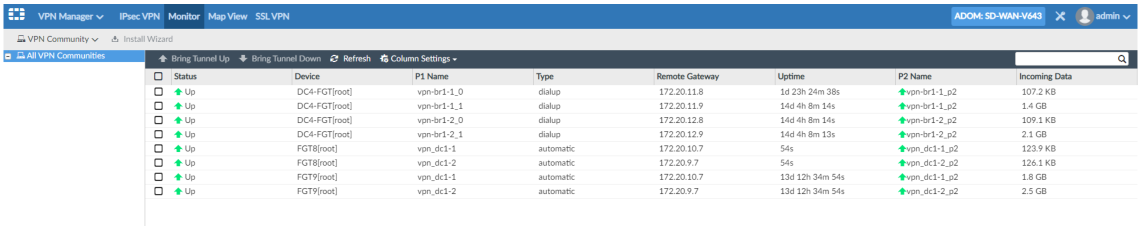
Monitoring SD-WAN interfaces (without shortcuts)

When an SD-WAN network is configured without ADVPN shortcuts, no shortcut information is displayed on *VPN Monitor* and on the graphs on *SD-WAN Monitor*.

In this example, device history monitoring is disabled for *SD-WAN Monitor*.

To view VPN monitor:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*.
   The *VPN Monitor* is displayed. No shortcuts are configured.



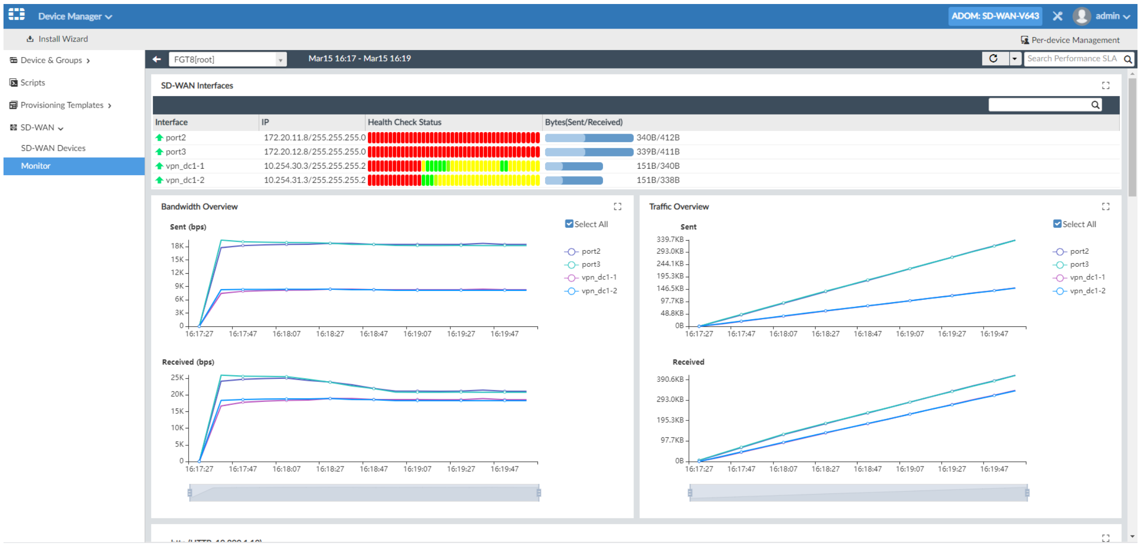
☐	Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
☐	Up	DC4-FGT[root]	vpn-br1-1_0	dialup	172.20.11.8	1d 23h 24m 38s	vpn-br1-1_p2	107.2 KB
☐	Up	DC4-FGT[root]	vpn-br1-1_1	dialup	172.20.11.9	14d 4h 8m 14s	vpn-br1-1_p2	1.4 GB
☐	Up	DC4-FGT[root]	vpn-br1-2_0	dialup	172.20.12.8	14d 4h 8m 14s	vpn-br1-2_p2	109.1 KB
☐	Up	DC4-FGT[root]	vpn-br1-2_1	dialup	172.20.12.9	14d 4h 8m 13s	vpn-br1-2_p2	2.1 GB
☐	Up	FGT8[root]	vpn_dc1-1	automatic	172.20.10.7	54s	vpn_dc1-1_p2	123.9 KB
☐	Up	FGT8[root]	vpn_dc1-2	automatic	172.20.9.7	54s	vpn_dc1-2_p2	126.1 KB
☐	Up	FGT9[root]	vpn_dc1-1	automatic	172.20.10.7	13d 12h 34m 54s	vpn_dc1-1_p2	1.8 GB
☐	Up	FGT9[root]	vpn_dc1-2	automatic	172.20.9.7	13d 12h 34m 54s	vpn_dc1-2_p2	2.5 GB

To view SD-WAN monitor:

1. Disable device history monitoring by using the following command:

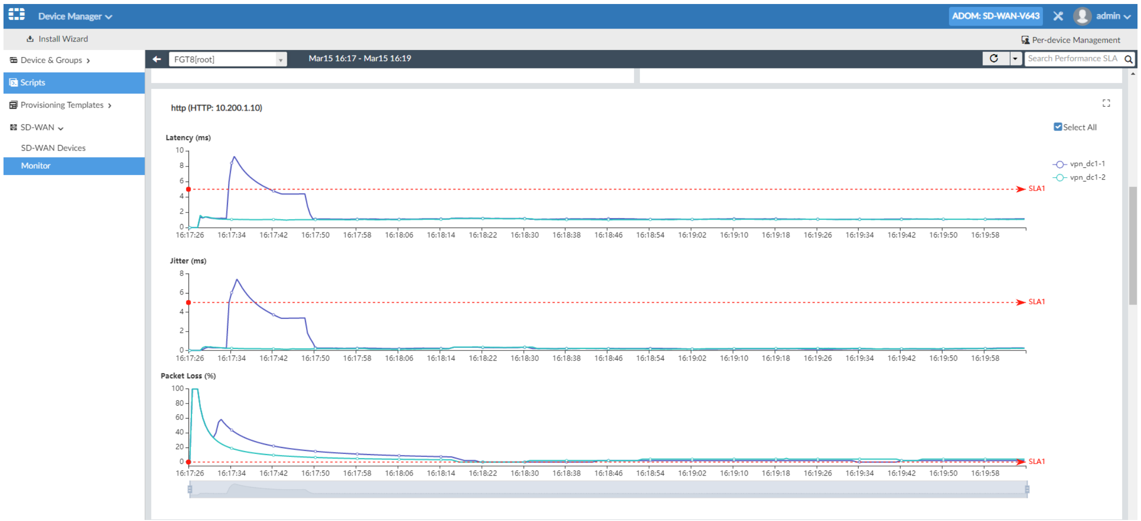
```
config system admin setting
   set sdwan-monitor-history disable
end
```

2. Go to *Device Manager > Monitors > SD-WAN Monitor*.
   The *SD-WAN Monitor* is displayed.
3. In the toolbar, click *Table View*.
   Table View is displayed.
4. In the *Device* column, click a device.
   SD-WAN monitoring information for the last 10 minutes for the device is displayed. In the *SD-WAN Interfaces* section, you can view interfaces.



Interface	IP	Health Check Status	Bytes(Sent/Received)
port2	172.20.11.8/255.255.255.0		340B/412B
port3	172.20.12.8/255.255.255.0		339B/411B
vpn_dc1-1	10.254.30.3/255.255.255.2		151B/340B
vpn_dc1-2	10.254.31.3/255.255.255.2		151B/338B

Scroll down to view SLA information, such as latency, jitter, and packet loss.



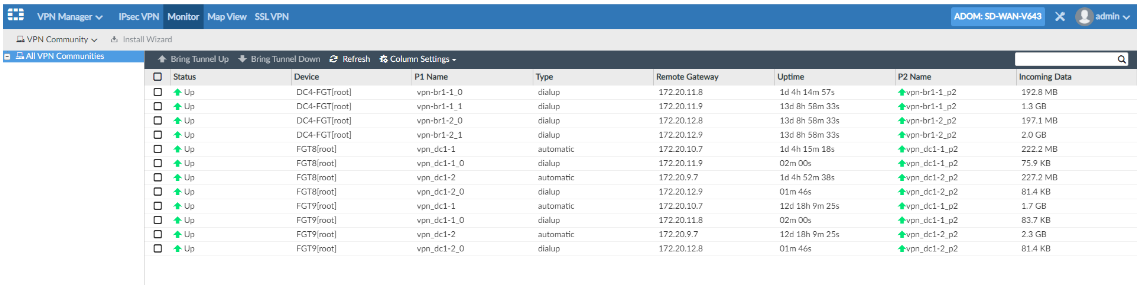
Monitoring SD-WAN interfaces (with shortcuts)

When an SD-WAN network is configured to use ADVPN shortcuts, you can view information about the shortcuts on *VPN Monitor* and in graphs on *SD-WAN Monitor*.

In this example, device history monitoring is enabled for *SD-WAN Monitor*.

To view shortcut information on VPN monitor:

1. Go to *Device Manager* > *Monitors* > *VPN Monitor*.
   The *VPN Monitor* is displayed. Shortcuts are configured.

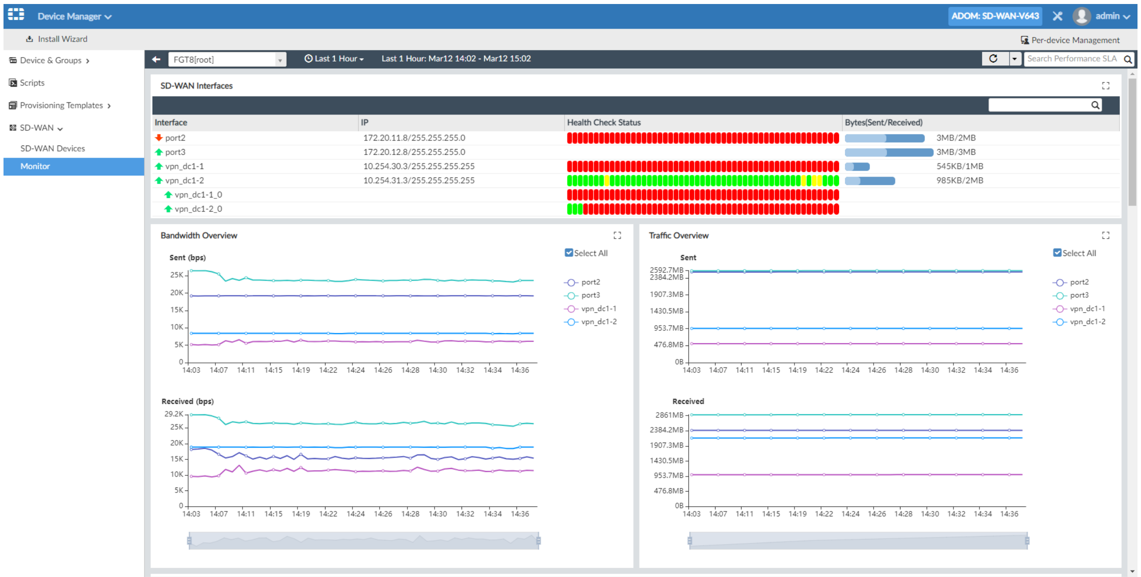


□	Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
□	↑ Up	DC4-FGT[root]	vpn-br1-1_0	dialup	172.20.11.8	1d 4h 14m 57s	↑vpn-br1-1_p2	192.8 MB
□	↑ Up	DC4-FGT[root]	vpn-br1-1_1	dialup	172.20.11.9	13d 8h 58m 33s	↑vpn-br1-1_p2	1.3 GB
□	↑ Up	DC4-FGT[root]	vpn-br1-2_0	dialup	172.20.12.8	13d 8h 58m 33s	↑vpn-br1-2_p2	197.1 MB
□	↑ Up	DC4-FGT[root]	vpn-br1-2_1	dialup	172.20.12.9	13d 8h 58m 33s	↑vpn-br1-2_p2	2.0 GB
□	↑ Up	FGT8[root]	vpn_dc1-1	automatic	172.20.10.7	1d 4h 15m 18s	↑vpn_dc1-1_p2	222.2 MB
□	↑ Up	FGT8[root]	vpn_dc1-1_0	dialup	172.20.11.9	02m 00s	↑vpn_dc1-1_p2	75.9 KB
□	↑ Up	FGT8[root]	vpn_dc1-2	automatic	172.20.9.7	1d 4h 52m 38s	↑vpn_dc1-2_p2	227.2 MB
□	↑ Up	FGT8[root]	vpn_dc1-2_0	dialup	172.20.12.9	01m 46s	↑vpn_dc1-2_p2	81.4 KB
□	↑ Up	FGT9[root]	vpn_dc1-1	automatic	172.20.10.7	12d 18h 9m 25s	↑vpn_dc1-1_p2	1.7 GB
□	↑ Up	FGT9[root]	vpn_dc1-1_0	dialup	172.20.11.8	02m 00s	↑vpn_dc1-1_p2	83.7 KB
□	↑ Up	FGT9[root]	vpn_dc1-2	automatic	172.20.9.7	12d 18h 9m 25s	↑vpn_dc1-2_p2	2.3 GB
□	↑ Up	FGT9[root]	vpn_dc1-2_0	dialup	172.20.12.8	01m 46s	↑vpn_dc1-2_p2	81.4 KB

To view shortcut information on SD-WAN monitor:

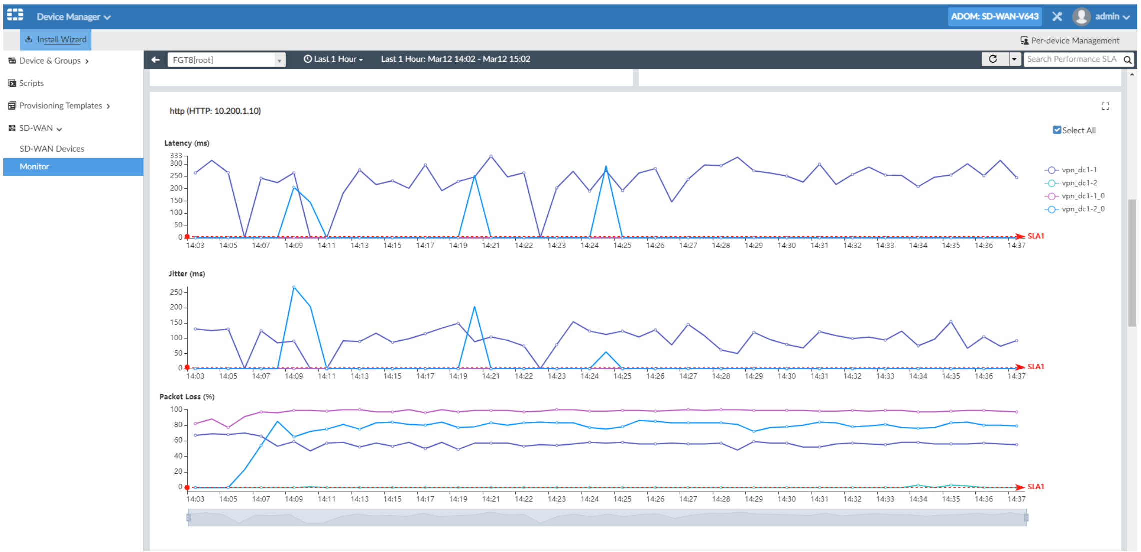
1. Enable device history monitoring by using the following command:
   ```
   config system admin setting
      set sdwan-monitor-history enable
   end
   ```
2. Go to *Device Manager* > *Monitors* > *SD-WAN Monitor*.
   The *SD-WAN Monitor* is displayed.
3. In the toolbar, click *Table View*.
   Table View is displayed.

4. In the *Device* column, click a device.
   SD-WAN monitoring information for the device is displayed. You can choose the length of history to display. In the *SD-WAN Interfaces* section, you can view interfaces, including ADVPN shortcuts.

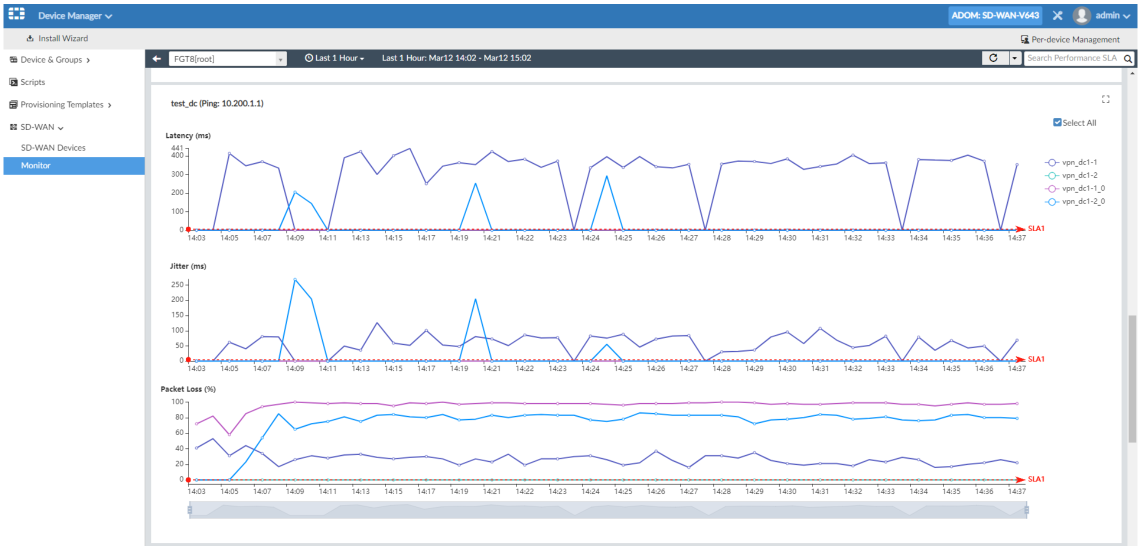


Interface	IP	Health Check Status	Bytes(Sent/Received)
port2	172.20.11.8/255.255.255.0	🟥	3MB/2MB
port3	172.20.12.8/255.255.255.0		3MB/3MB
vpn_dc1-1	10.254.30.3/255.255.255.255	🟥	545KB/1MB
vpn_dc1-2	10.254.31.3/255.255.255.255	🟩	985KB/2MB
vpn_dc1-1_0		🟥	
vpn_dc1-2_0		🟥	

Scroll down to view SLA information, such as latency, jitter, and packet loss, for each interface. The SLA graphs include information for dynamic interfaces.



Scroll down to view more interfaces.

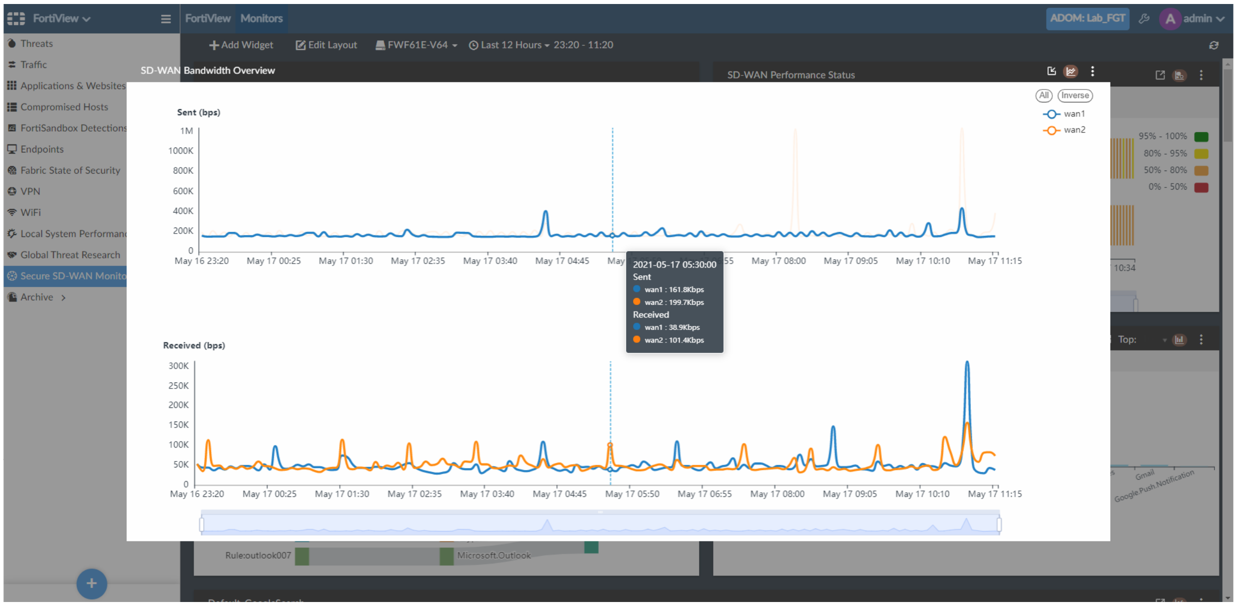


Improved secure SD-WAN monitor - FAZ

This is an enhancement to the existing Secure SD-WAN Monitor dashboard by providing more widgets and detailed information.

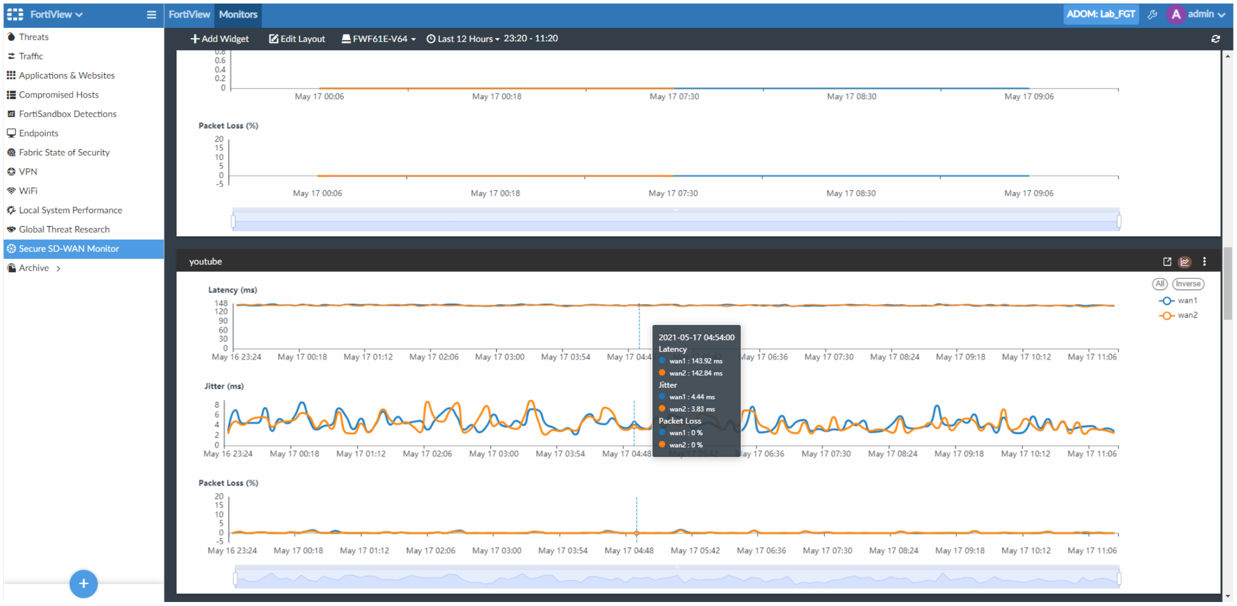
To view the secure SD-WAN monitor enhancements:

1. Go to *FortiView > Monitors > Secure SD-WAN Monitor*.
A new widget called *SD-WAN Bandwidth Overview* has been added which displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces. In this widget, users can select or deselect member interfaces and mouse over the line chart to view the sent/received rate in a tooltip for the selected interfaces.

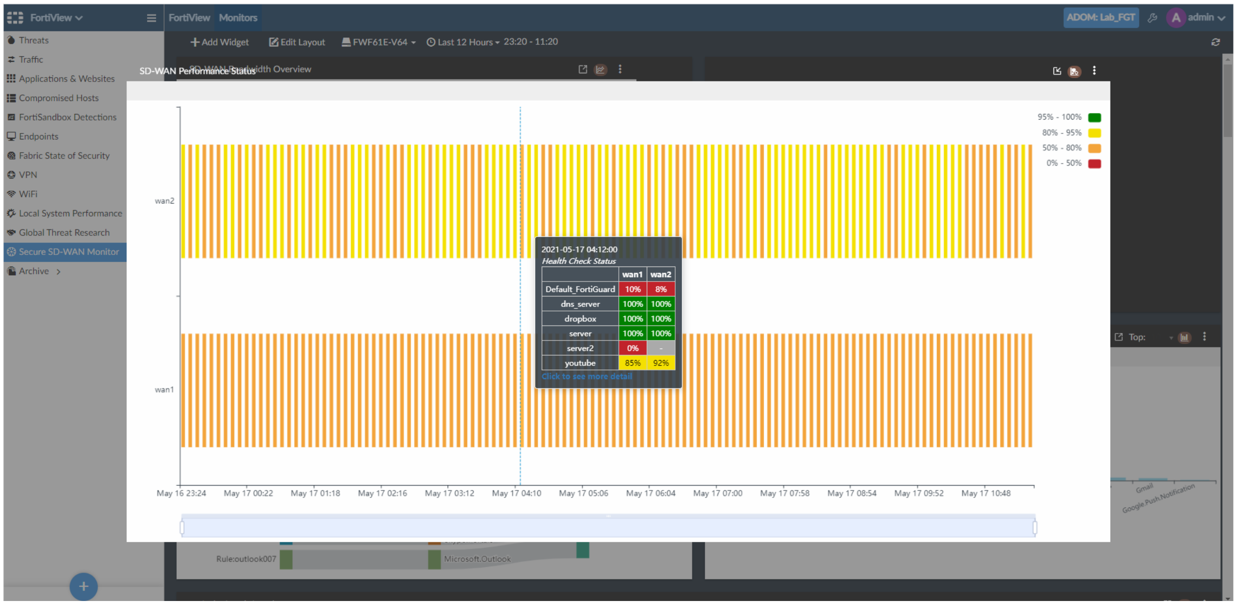


The *Latency*, *Jitter*, and *Packet Loss* widgets have been replaced with the new *Health Check Status* widget. This

widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.
In each *Health Check Status* widget, users can select/deselect member interfaces and mouse over line charts to view the latency, jitter, and packet loss in a tooltip for the selected interface.



In the *SD-WAN Performance Status* widget, mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check.

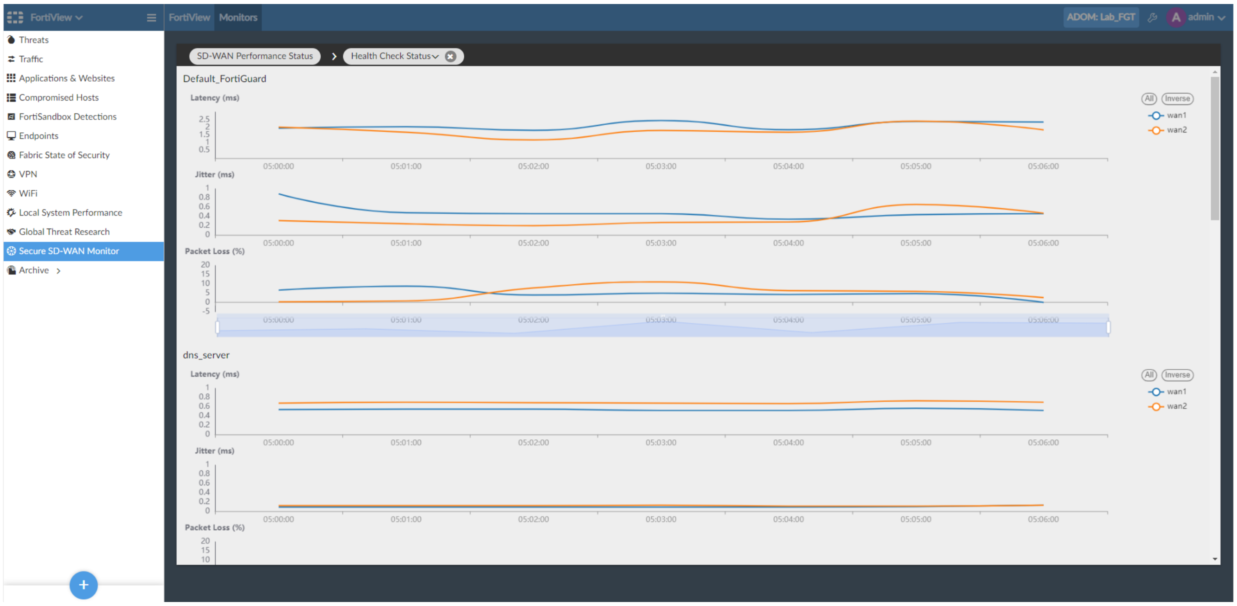


2021-05-17 04:12:00
Health Check Status

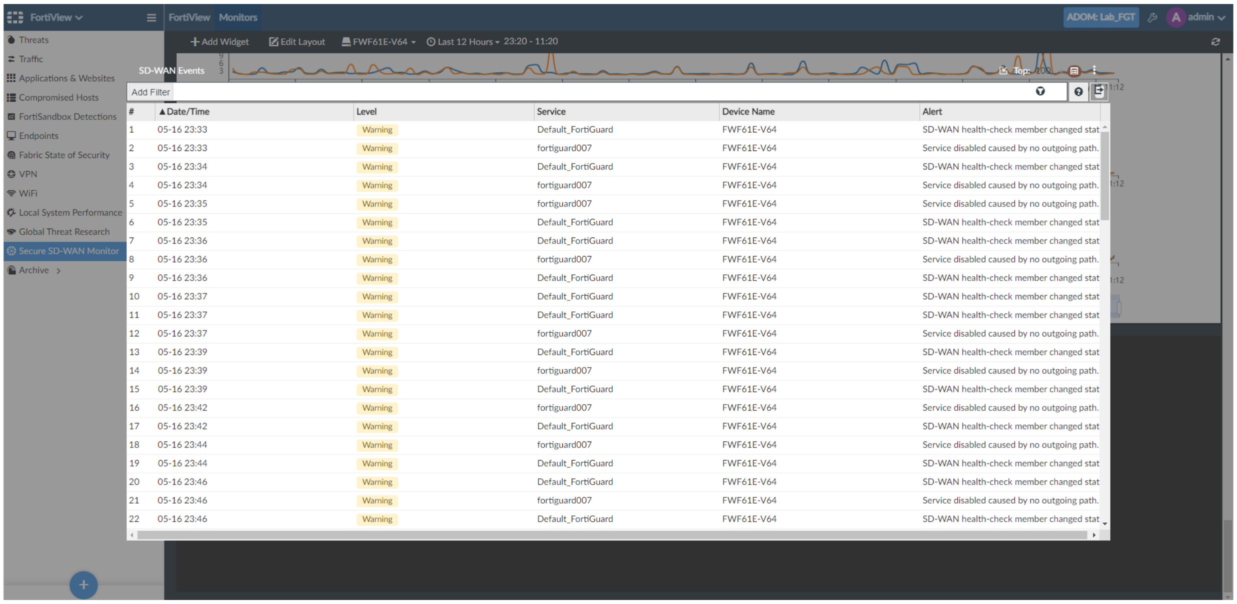
	wan1	wan2
Default_FortiGuard	10%	8%
dns_server	100%	100%
dropbox	100%	100%
server	100%	100%
server2	0%	-
youtube	85%	92%

Click to see more detail

In the *SD-WAN Performance Status* widget, click on a scatter chart to view additional details.



The *SD-WAN High and Critical Events* widget has been replaced with the new *SD-WAN Events* widget. This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.



#	▲Date/Time	Level	Service	Device Name	Alert
1	05-16 23:33	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
2	05-16 23:33	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
3	05-16 23:34	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
4	05-16 23:34	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
5	05-16 23:35	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
6	05-16 23:35	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
7	05-16 23:36	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
8	05-16 23:36	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
9	05-16 23:36	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
10	05-16 23:37	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
11	05-16 23:37	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
12	05-16 23:37	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
13	05-16 23:39	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
14	05-16 23:39	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
15	05-16 23:39	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
16	05-16 23:42	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
17	05-16 23:42	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
18	05-16 23:44	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
19	05-16 23:44	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
20	05-16 23:46	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat
21	05-16 23:46	Warning	fortiguard007	FWF61E-V64	Service disabled caused by no outgoing path.
22	05-16 23:46	Warning	Default_FortiGuard	FWF61E-V64	SD-WAN health-check member changed stat

Display ADVPN shortcut information in the GUI - 7.0.1

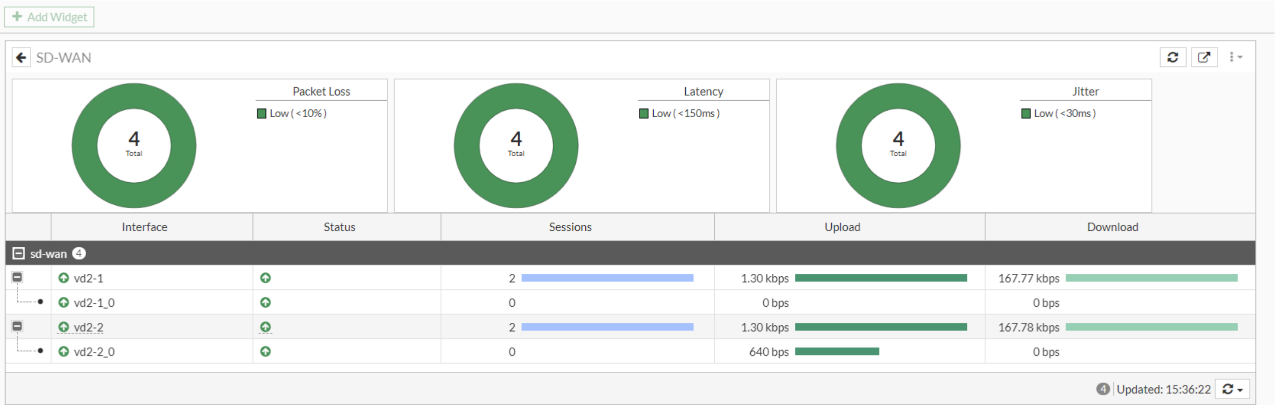
ADVPN shortcut tunnel information is displayed in the *SD-WAN* and *IPsec* dashboard widgets.

The following command has been added to check the dynamic tunnel status:

```
diagnose sys link-monitor interface <name> <name>_0
```

To view the SD-WAN widget:

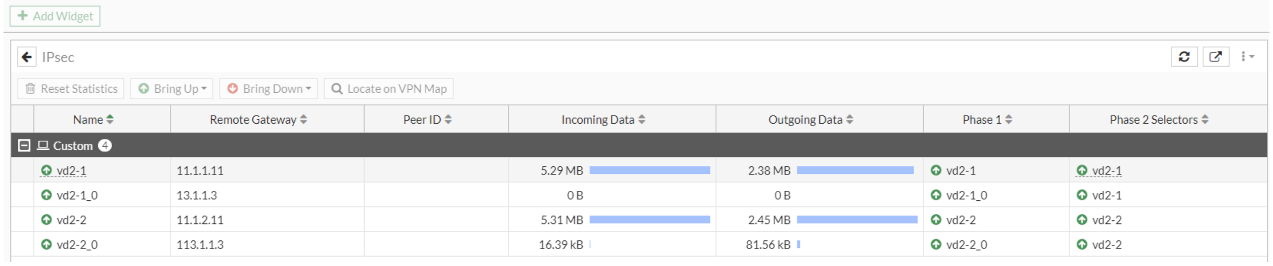
1. Go to *Dashboard* > *Network*.
2. Hover over the *SD-WAN* widget and click *Expand to full screen*.
3. Click the + to expand the SD-WAN members and view the child ADVPN shortcuts.



Interface	Status	Sessions	Upload	Download
sd-wan 4				
vd2-1		2	1.30 kbps	167.77 kbps
vd2-1_0		0	0 bps	0 bps
vd2-2		2	1.30 kbps	167.78 kbps
vd2-2_0		0	640 bps	0 bps

To view the IPsec widget:

1. Go to *Dashboard* > *Network*.
2. Hover over the *IPsec* widget and click *Expand to full screen*.



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 4						
vd2-1	11.1.1.11		5.29 MB	2.38 MB	vd2-1	vd2-1
vd2-1_0	13.1.1.3		0 B	0 B	vd2-1_0	vd2-1
vd2-2	11.1.2.11		5.31 MB	2.45 MB	vd2-2	vd2-2
vd2-2_0	113.1.1.3		16.39 kB	81.56 kB	vd2-2_0	vd2-2

To verify the dynamic tunnel status:

```
# diagnose sys link-monitor interface vd2-2
Interface(vd2-2): state(up, since Tue Jun 15 12:31:28 2021), bandwidth(up:1299bps,
down:0bps), session count(IPv4:2, IPv6:0), tx(2409919 bytes), rx(5292290 bytes), latency
(0.03), jitter(0.00), packet-loss(0.00).
```

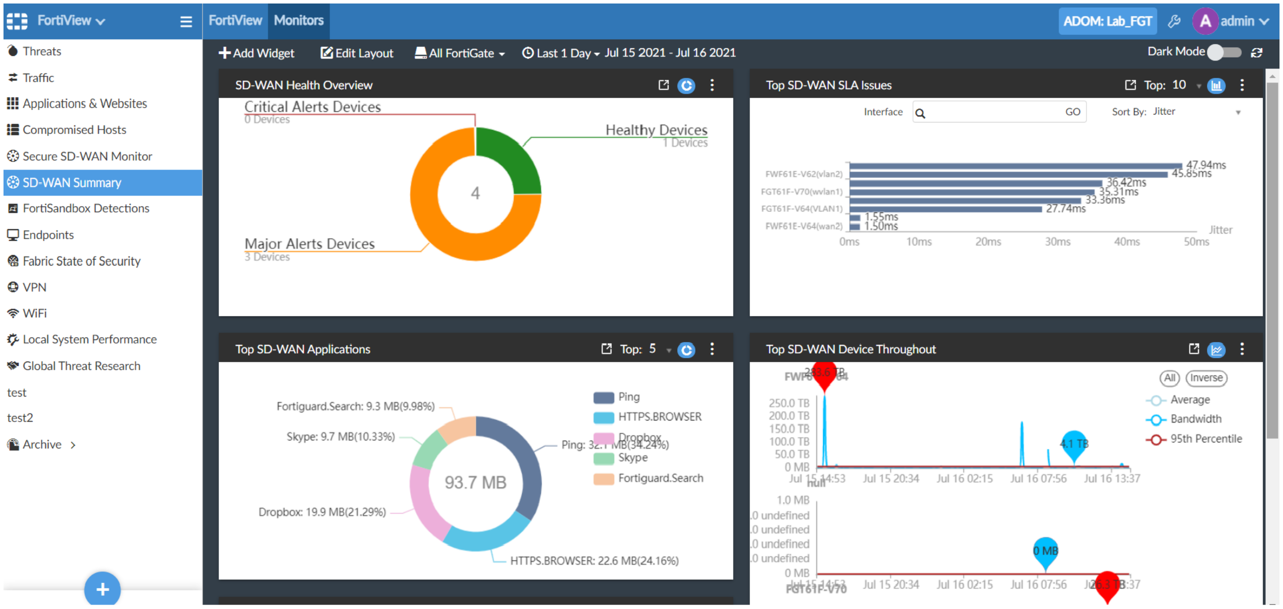
```
# diagnose sys link-monitor interface vd2-2 vd2-2_0
Interface(vd2-2_0): state(up, since Tue Jun 15 15:21:52 2021), bandwidth(up:640bps,
down:0bps), session count(IPv4:0, IPv6:0), tx(102242 bytes), rx(16388 bytes), latency(0.03),
jitter(0.00), packet-loss(0.00).
```

SD-WAN Summary Report - FAZ 7.0.1

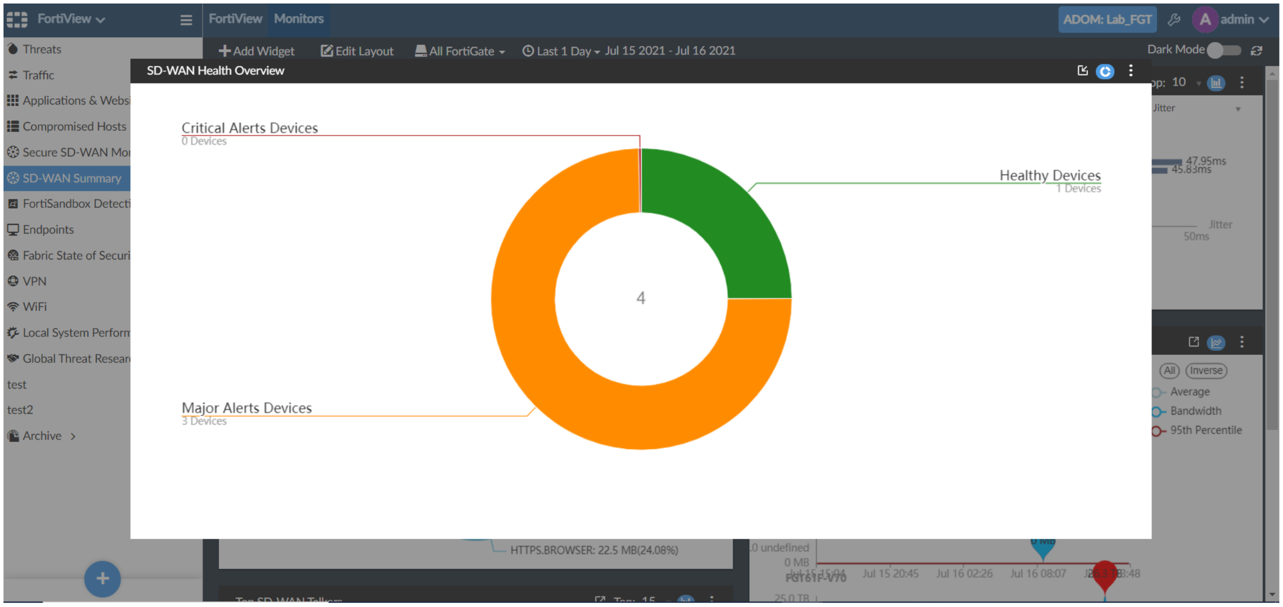
A new summary dashboard for SD-WAN is available in FortiView under the *Monitors* tab to provide more visibility for NOC to monitor SD-WAN performance and identify SLA issues.

To view the SD-WAN Summary dashboard:

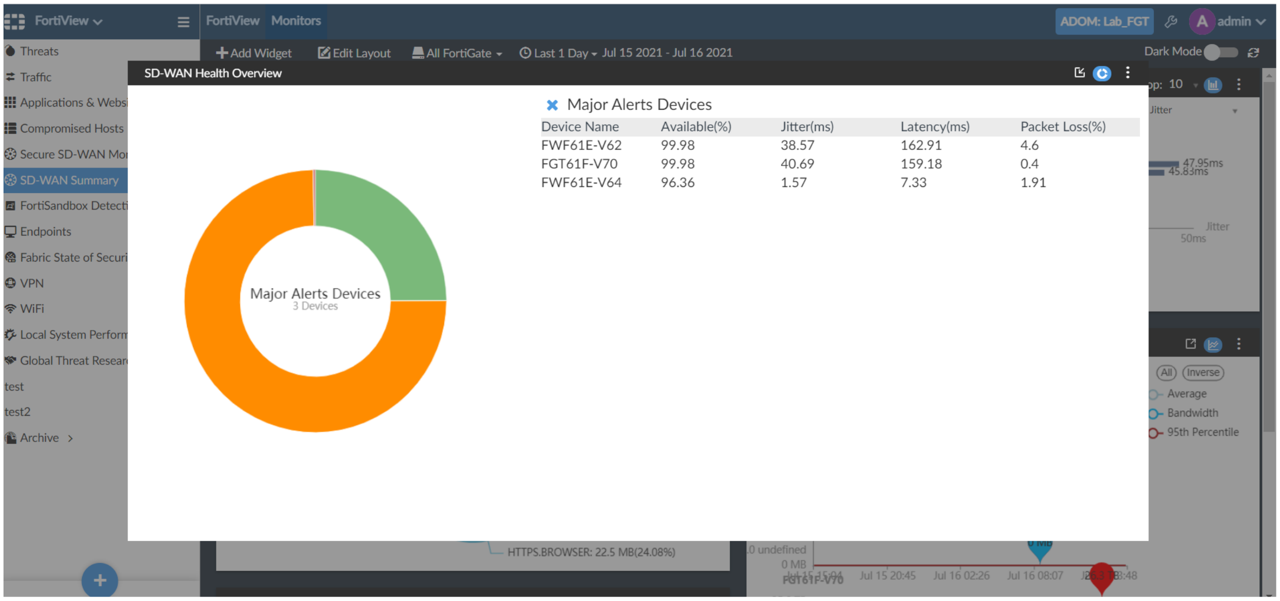
1. Go to *FortiView* > *Monitors* > *SD-WAN Summary*.
   The SD-WAN Summary dashboard is displayed.



2. In the *SD-WAN Health Overview* widget, a donut chart displays the number of devices that have critical alerts, major alerts, or are healthy. The total number of devices is displayed at the center of the donut chart.



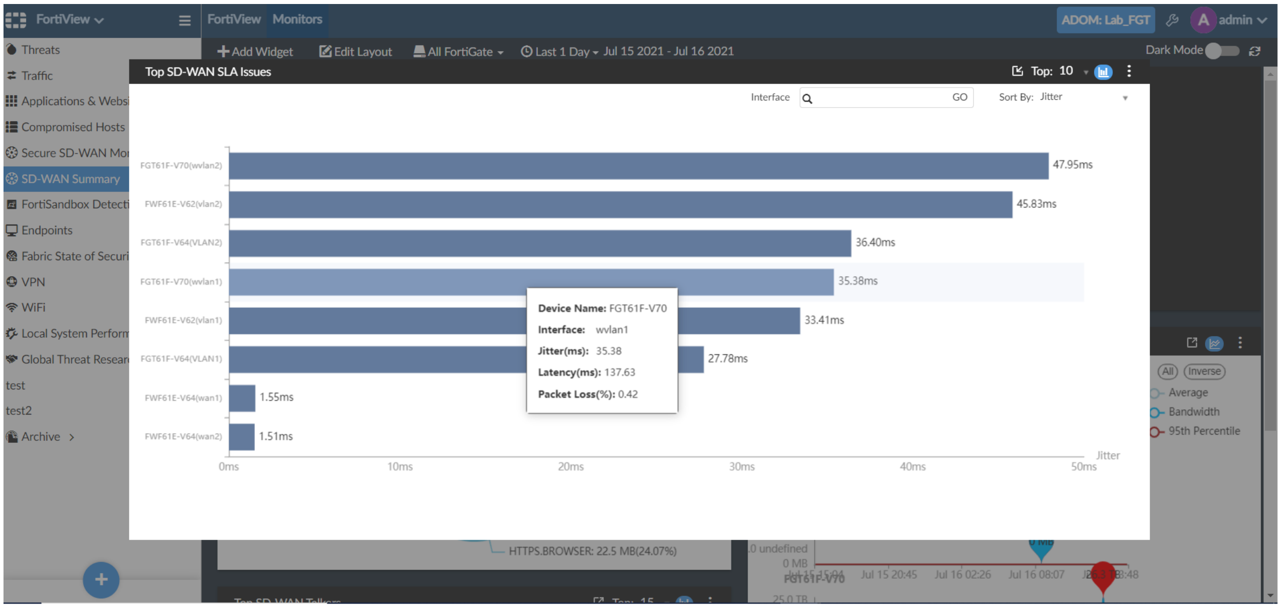
Click on the donut chart to display details for related devices including the device names, available(%), jitter(ms), latency(ms), and packet loss (%).



Major Alerts Devices

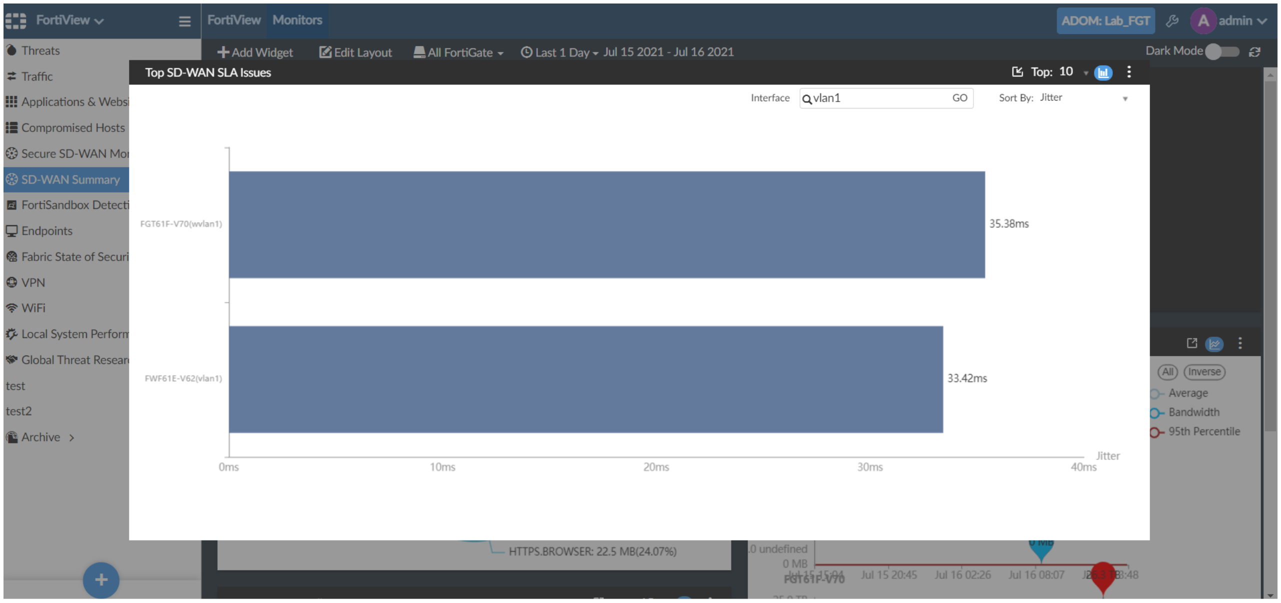
Device Name	Available(%)	Jitter(ms)	Latency(ms)	Packet Loss(%)
FWF61E-V62	99.98	38.57	162.91	4.6
FGT61F-V70	99.98	40.69	159.18	0.4
FWF61E-V64	96.36	1.57	7.33	1.91

3. In the *Top SD-WAN SLA Issues* widget, the top 10/15/20 worst SD-WAN performance values are displayed for selected devices in the specified time period. Mouse over the bar chart to show details in a tooltip.

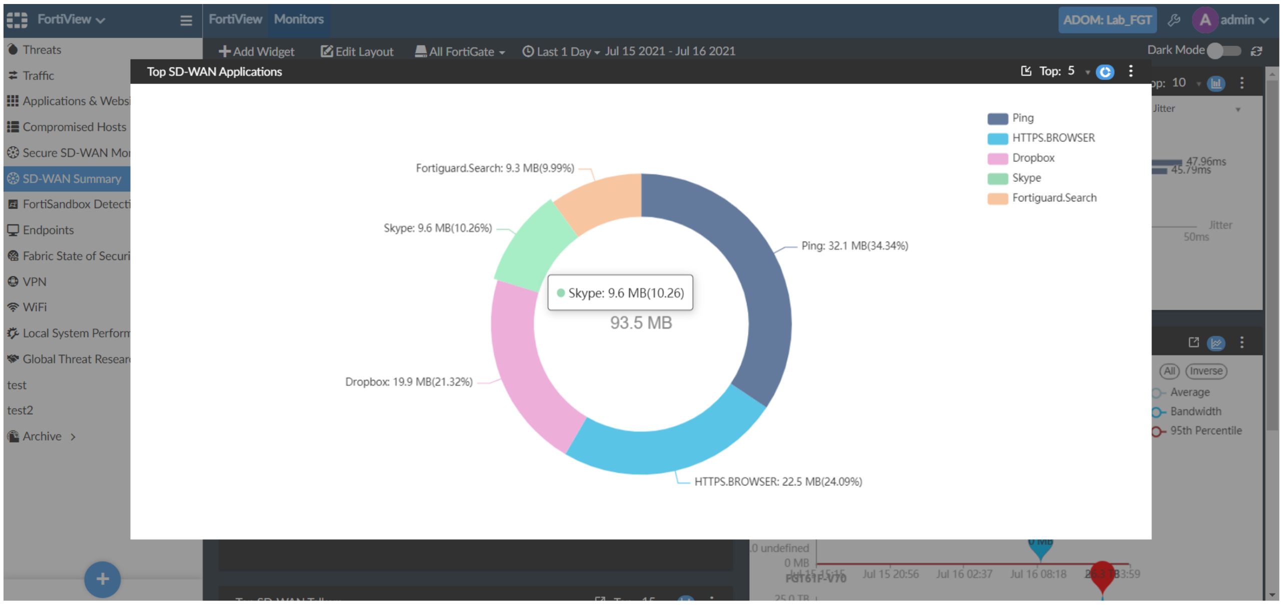


Device Name: FGT61F-V70
Interface: wvlan1
Jitter(ms): 35.38
Latency(ms): 137.63
Packet Loss(%): 0.42

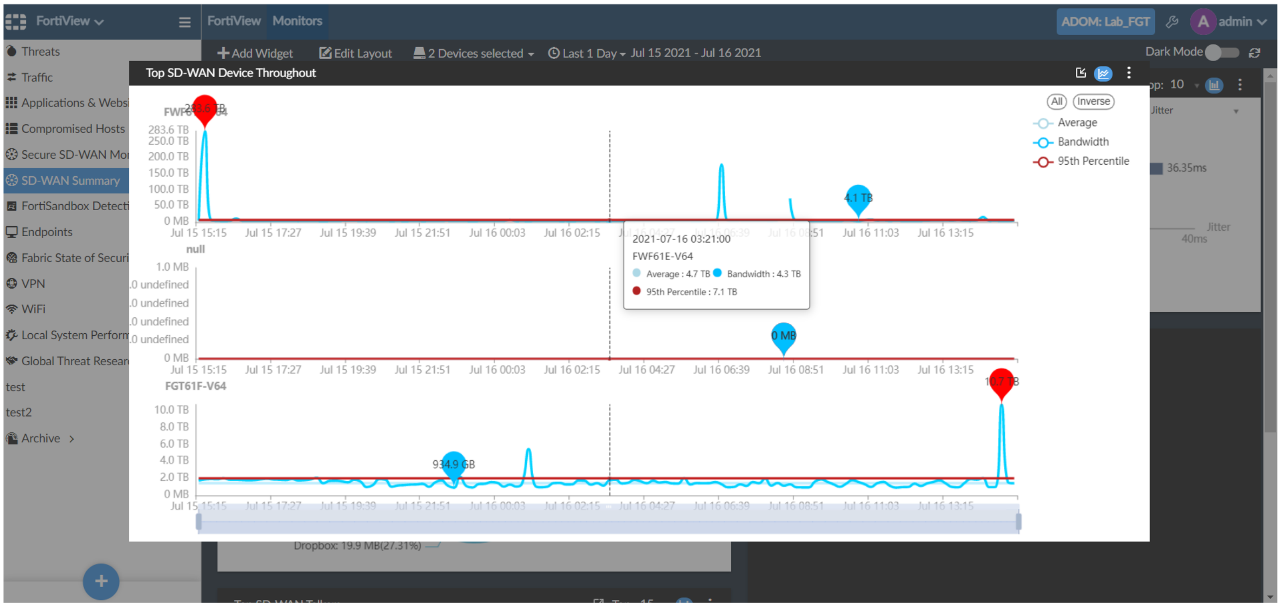
Use the search option to filter all SD-WAN interfaces with names including the entered search text, and display the top 10/15/20 values for jitter, latency, and packet loss.



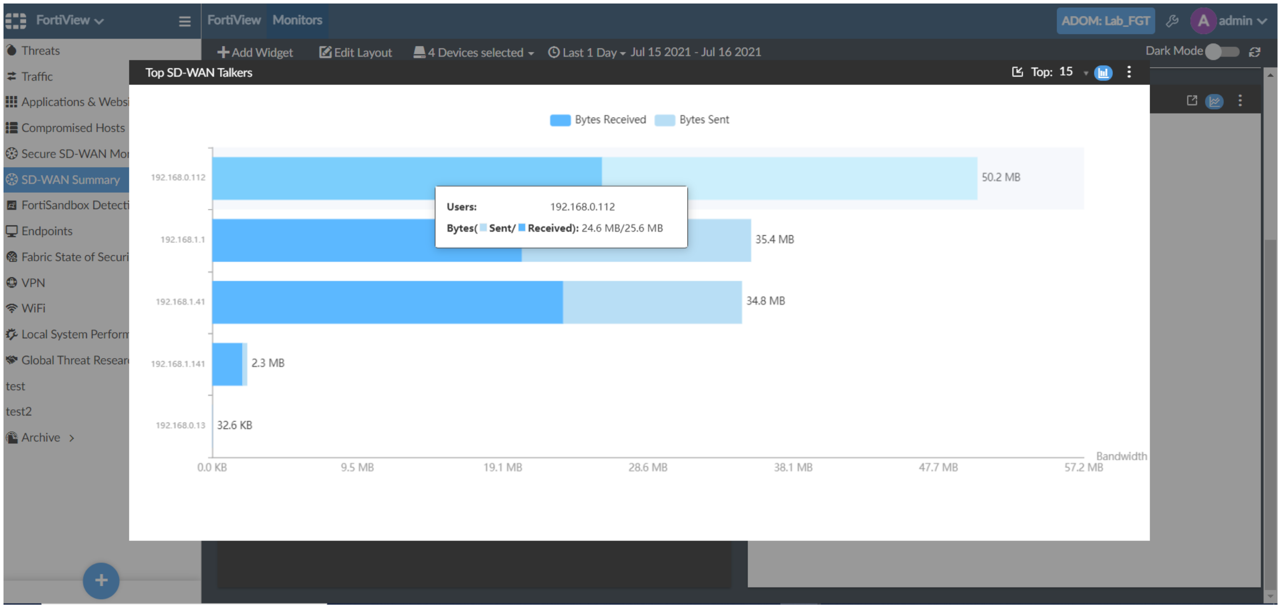
4. In the *Top Applications* widget, the top 5/10/20 applications which use SD-WAN interfaces are displayed in a donut chart. Mouse over the donut chart to view details in a tooltip.



5. In the *SD-WAN Top Device Throughput* widget, for each selected devices, line charts of the average, bandwidth, and 95th percentile in the specified time period are displayed. Mouse over the line charts to view details in a tooltip.



6. In the Top SD-WAN Talkers widget, sources which have the top 10/15/20 bandwidth (byes received and bytes sent) are displayed in a horizontal bar chart. Hover your mouse over the bar chart to view details in a tooltip.

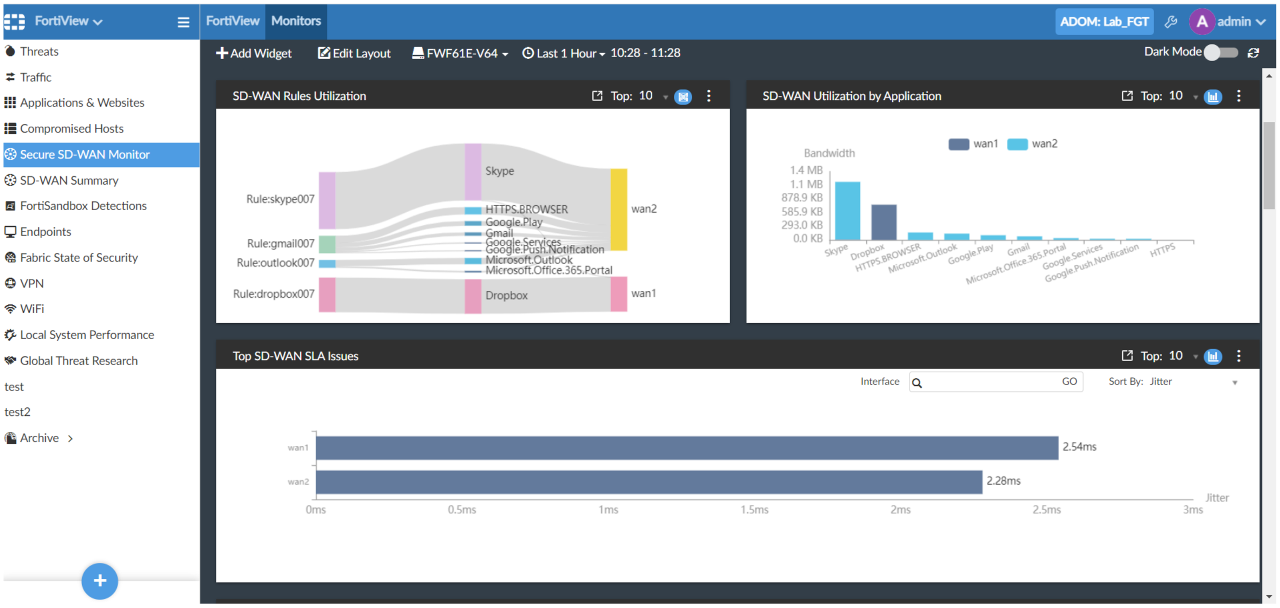


SD-WAN monitoring improvement - FAZ 7.0.1

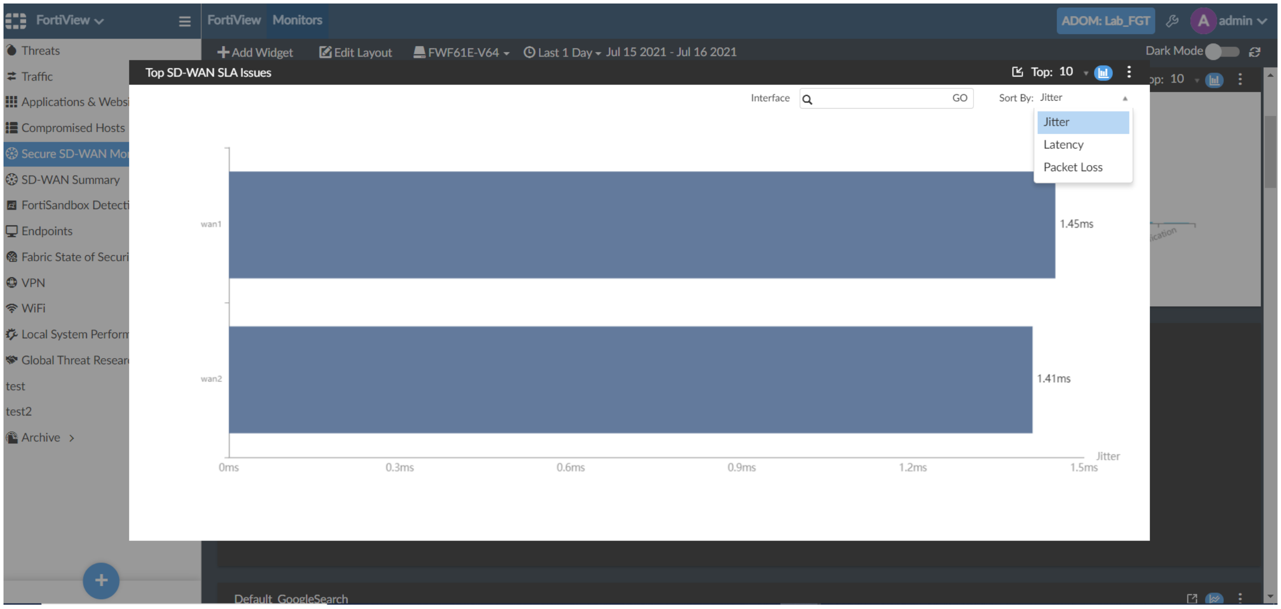
A new widget is added to *Secure SD-WAN Monitor* for IT admins to monitor and identify the SD-WAN links that have the worst performance issues

To view the new SD-WAN Monitor dashboard:

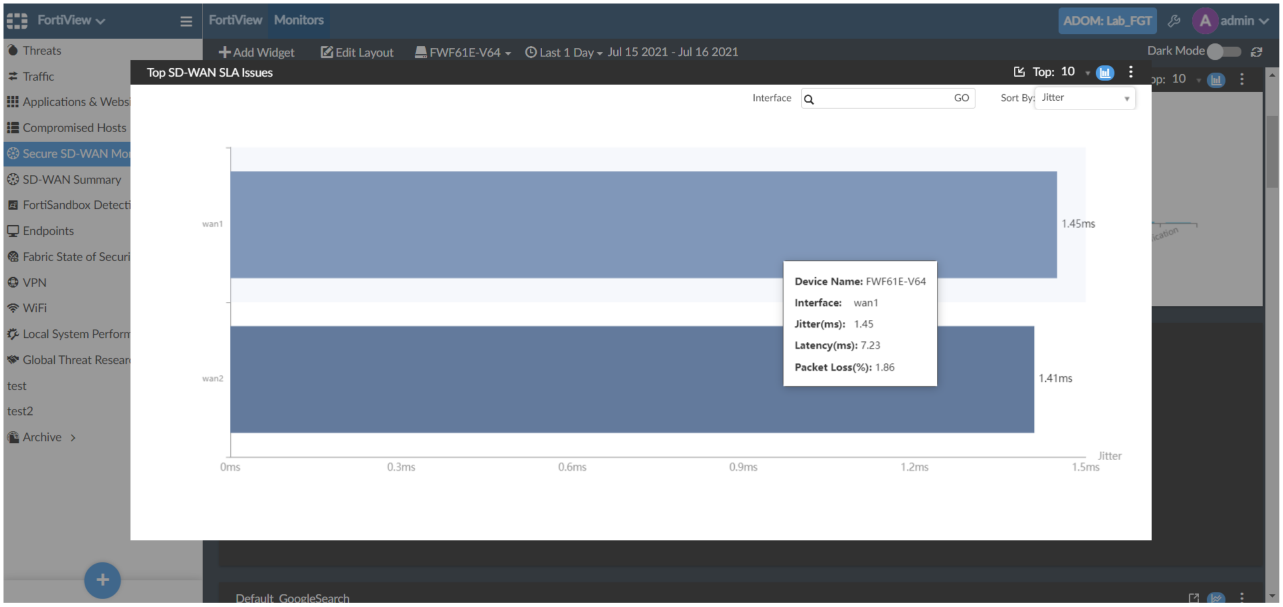
1. Go to *FortiView >Monitors > Secure SD-WAN Monitor.*
   A new *Top SD-WAN SLA Issues* widget has been added to the existing dashboard. This widget displays the top 10/15/20 worst SD-WAN performance values for the selected device in the specified time period.



2. Use the *Sort By* field to sort the *Top SD-WAN SLA Issues widget* by *Jitter*, *Latency*, or *Packet Loss*, and then show the graph for the selected SLA type.

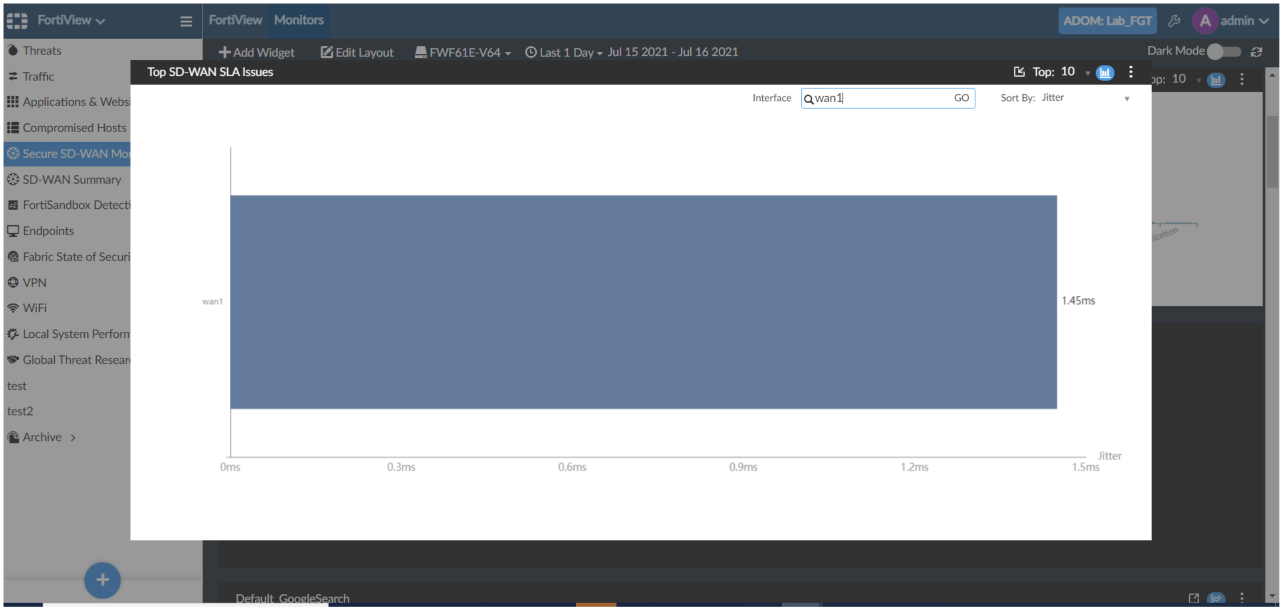


3. Mousing over the graph of an interface will display the worst *Jitter*, *Latency*, or *Packet Loss* values for that interface.



Device Name: FWF61E-V64
Interface: wan1
Jitter(ms): 1.45
Latency(ms): 7.23
Packet Loss(%): 1.86

4. Use the search field within the widget to filter all SD-WAN interfaces by name.



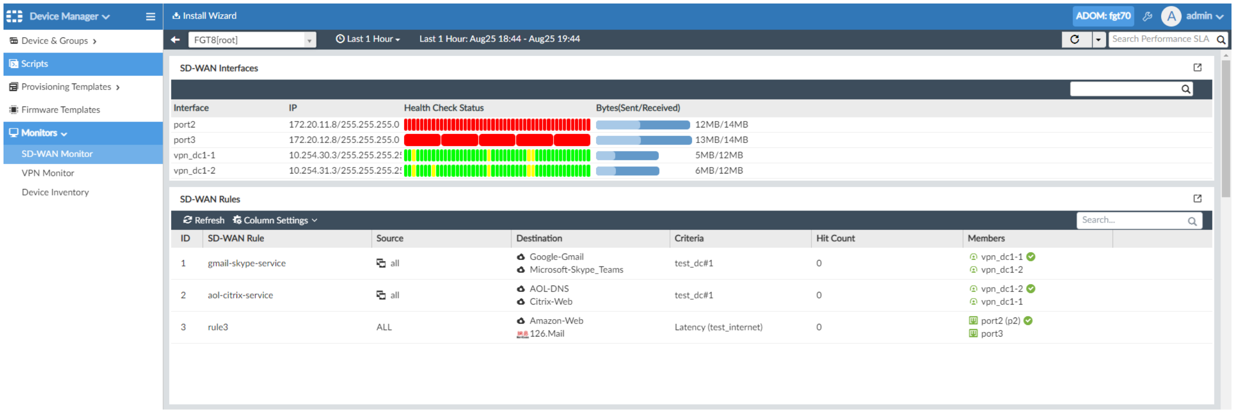
Interface: wan1

SD-WAN monitoring shows the SD-WAN rule and its status, active selected member for a given SLA - FMG 7.0.2

In FortiManager 7.0.2, SD-WAN monitoring shows the SD-WAN rule and its status, and the active selected member for a given SLA.

To view the SD-WAN Rules widget:

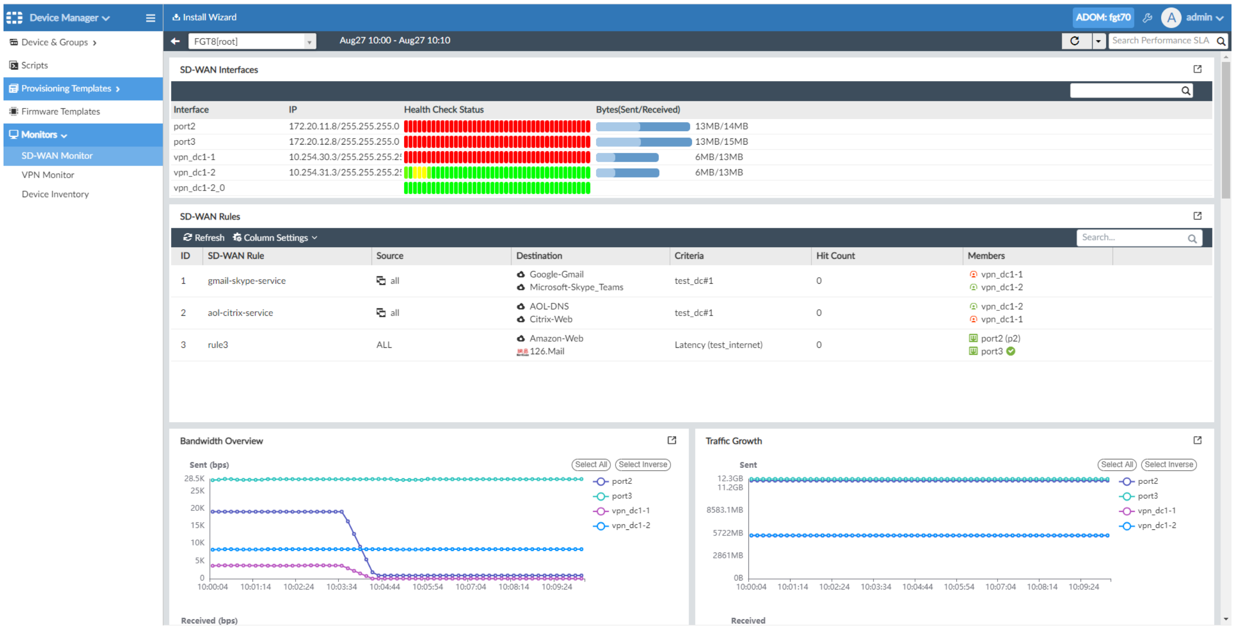
1. Go to *Device Manager > Monitors > SD-WAN Monitor*.
   The SD-WAN Rules widget is displayed.



Interface	IP	Health Check Status	Bytes(Sent/Received)
port2	172.20.11.8/255.255.255.0		12MB/14MB
port3	172.20.12.8/255.255.255.0		13MB/14MB
vpn_dc1-1	10.254.30.3/255.255.255.2!		5MB/12MB
vpn_dc1-2	10.254.31.3/255.255.255.2!		6MB/12MB

ID	SD-WAN Rule	Source	Destination	Criteria	Hit Count	Members
1	gmail-skype-service	all	Google-Gmail Microsoft-Skype_Teams	test_dc#1	0	vpn_dc1-1 ✓ vpn_dc1-2
2	aol-citrix-service	all	AOL-DNS Citrix-Web	test_dc#1	0	vpn_dc1-2 ✓ vpn_dc1-1
3	rule3	ALL	Amazon-Web 126.Mail	Latency (test_internet)	0	port2 (p2) ✓ port3

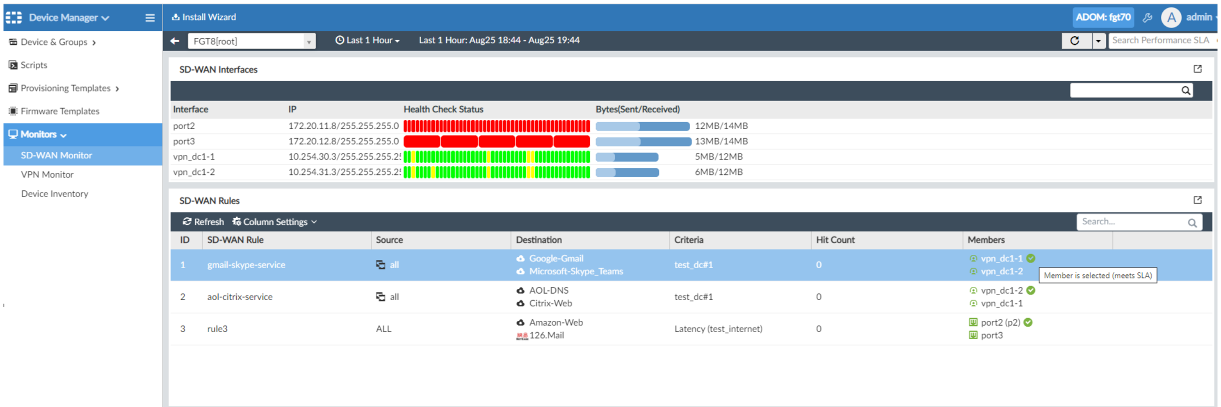
2. The SD-WAN Rules widget indicates rule statuses by color. Red statuses indicate that the interface is down and the rule is inactive.



Interface	IP	Health Check Status	Bytes(Sent/Received)
port2	172.20.11.8/255.255.255.0		13MB/14MB
port3	172.20.12.8/255.255.255.0		13MB/15MB
vpn_dc1-1	10.254.30.3/255.255.255.2!		6MB/13MB
vpn_dc1-2	10.254.31.3/255.255.255.2!		6MB/13MB
vpn_dc1-2_0			

ID	SD-WAN Rule	Source	Destination	Criteria	Hit Count	Members
1	gmail-skype-service	all	Google-Gmail Microsoft-Skype_Teams	test_dc#1	0	vpn_dc1-1 vpn_dc1-2
2	aol-citrix-service	all	AOL-DNS Citrix-Web	test_dc#1	0	vpn_dc1-2 vpn_dc1-1
3	rule3	ALL	Amazon-Web 126.Mail	Latency (test_internet)	0	port2 (p2) port3 ✓

3. Selected (active) interfaces are indicated with a check mark icon.
   You can hover over a selected interface to see the reason that the interface is selected.



SD-WAN Interfaces

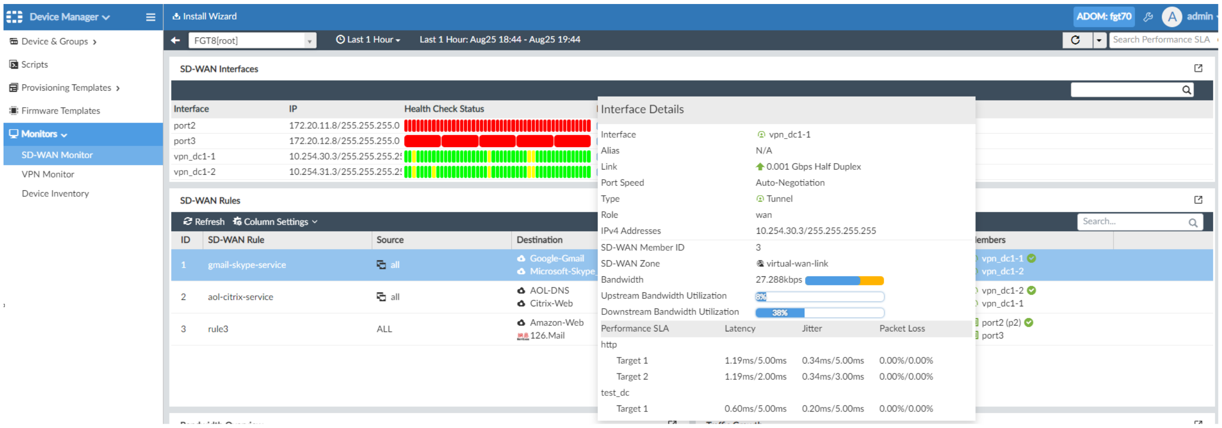
Interface	IP	Health Check Status	Bytes(Sent/Received)
port2	172.20.11.8/255.255.255.0		12MB/14MB
port3	172.20.12.8/255.255.255.0		13MB/14MB
vpn_dc1-1	10.254.30.3/255.255.255.2!		5MB/12MB
vpn_dc1-2	10.254.31.3/255.255.255.2!		6MB/12MB

SD-WAN Rules

ID	SD-WAN Rule	Source	Destination	Criteria	Hit Count	Members
1	gmail-skype-service	all	Google-Gmail Microsoft-Skype_Teams	test_dc#1	0	vpn_dc1-1 ✓ vpn_dc1-2
2	aol-citrix-service	all	AOL-DNS Citrix-Web	test_dc#1	0	vpn_dc1-2 ✓ vpn_dc1-1
3	rule3	ALL	Amazon-Web 126.Mail	Latency (test_internet)	0	port2 (p2) ✓ port3

Member is selected (meets SLA)

4. Interface statistics display SLAs tied to that interface, including upstream bandwidth, downstream bandwidth, IP address, link speed, and more.



Interface Details

Interface	vpn_dc1-1
Alias	N/A
Link	0.001 Gbps Half Duplex
Port Speed	Auto-Negotiation
Type	Tunnel
Role	wan
IPv4 Addresses	10.254.30.3/255.255.255.255
SD-WAN Member ID	3
SD-WAN Zone	virtual-wan-link
Bandwidth	27.288kbps
Upstream Bandwidth Utilization	8%
Downstream Bandwidth Utilization	38%

Performance SLA	Latency	Jitter	Packet Loss
http			
Target 1	1.19ms/5.00ms	0.34ms/5.00ms	0.00%/0.00%
Target 2	1.19ms/2.00ms	0.34ms/3.00ms	0.00%/0.00%
test_dc			
Target 1	0.60ms/5.00ms	0.20ms/5.00ms	0.00%/0.00%

QoS monitoring support added for dialup VPN interfaces - FMG 7.0.2

QoS monitoring support added for dialup VPN interfaces

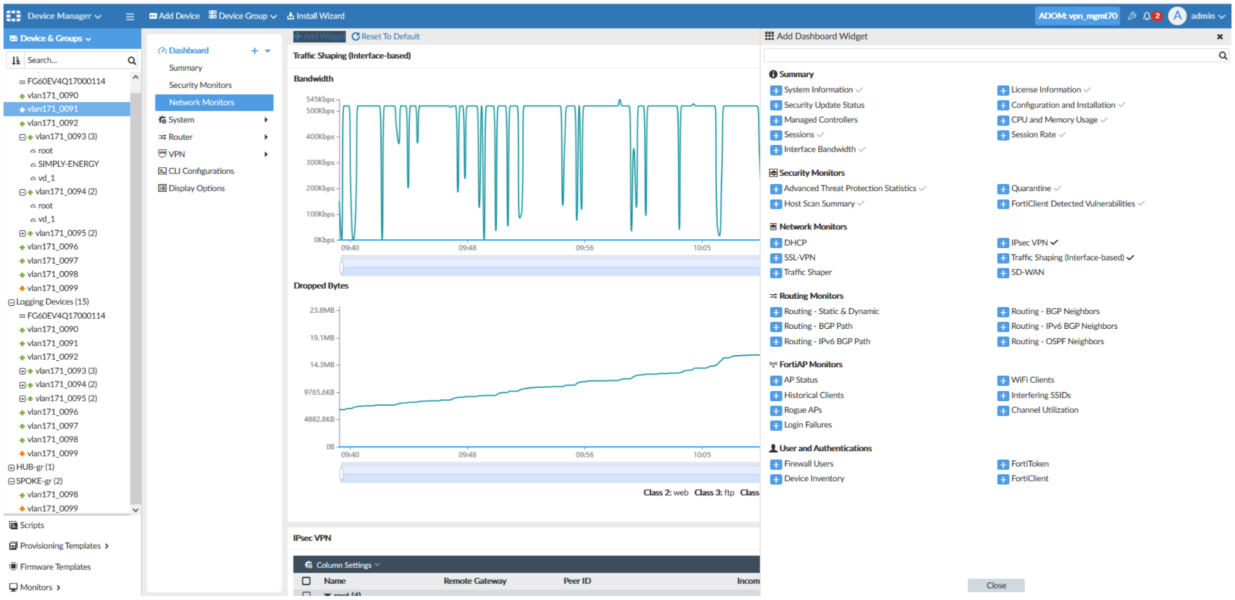
To view QoS monitoring for dialup VPN interfaces:

1. In the FortiManager CLI, enter the following commands to enable traffic shaping history.

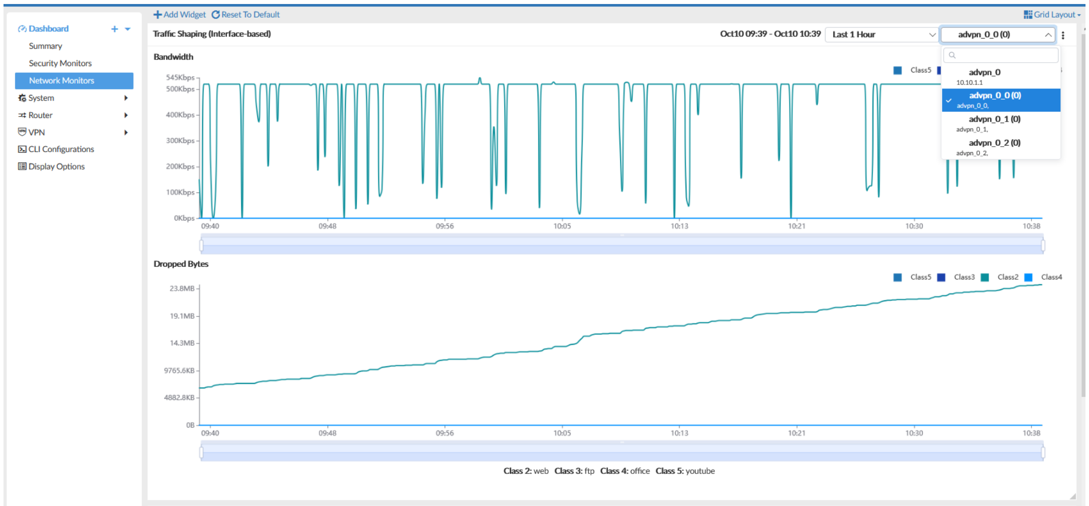
```
config system admin setting
   set traffic-shaping-history enable
end
```

2. In the FortiManager GUI, go to *Device Manager*.
3. Select a dialup HUP VPN FortiGate device from the device list, and go to *Dashboard* > *Network Monitors* and click *Add Widget*.
   A list of available widgets is displayed.

4. Select the plus icon next to *Traffic Shaping (Interface-based)* to add the widget to the device's dashboard.



5. Select a VPN tunnel interface from the dropdown menu to view the QoS information.



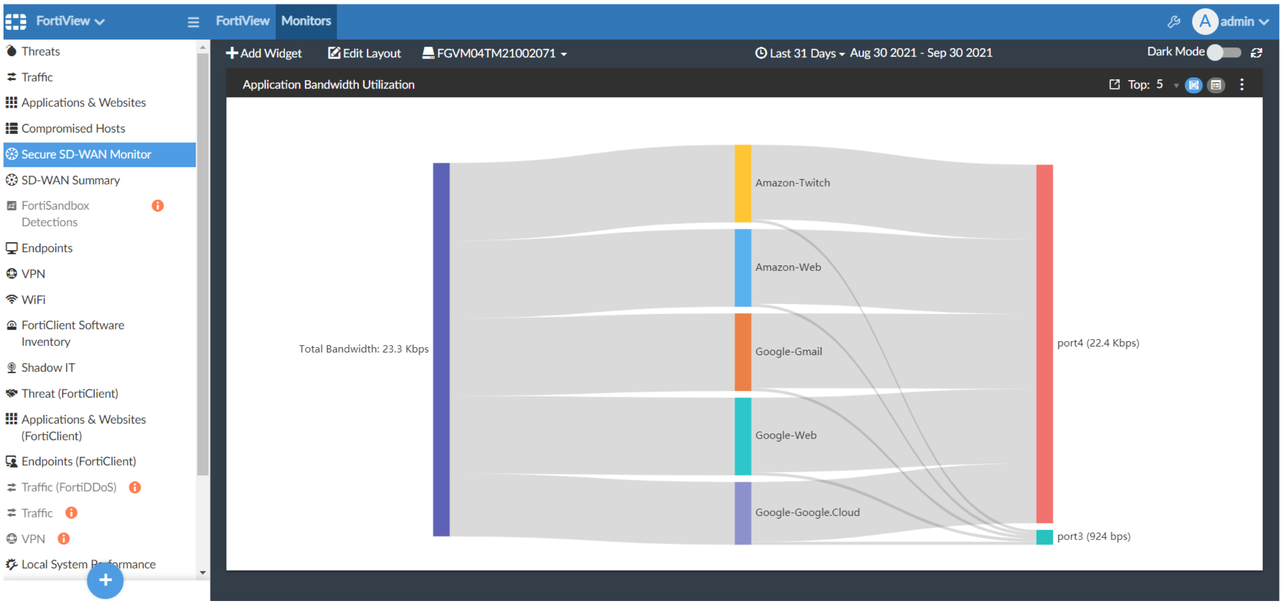
SD-WAN application bandwidth per interface widget - FAZ 7.0.2

A new application bandwidth chart is added to the *Secure SD-WAN Monitor* to show total bandwidth usage from all applications, bandwidth usage per application, as well as bandwidth usage per SD-WAN interface.

To view the application bandwidth chart:

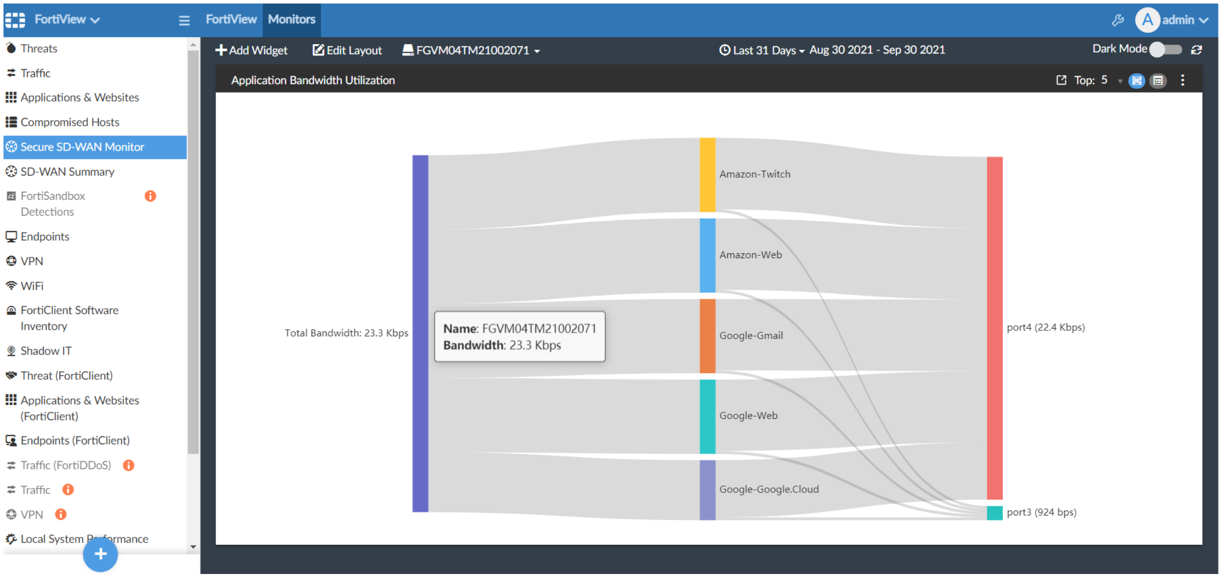
1. Go to *FortiView > Monitors > Secure SD-WAN Monitor*.

2. In the *Application Bandwidth Utilization* widget, a Sanky chart displays the total bandwidth from all applications, bandwidth by application, as well as bandwidth by SD-WAN interface.



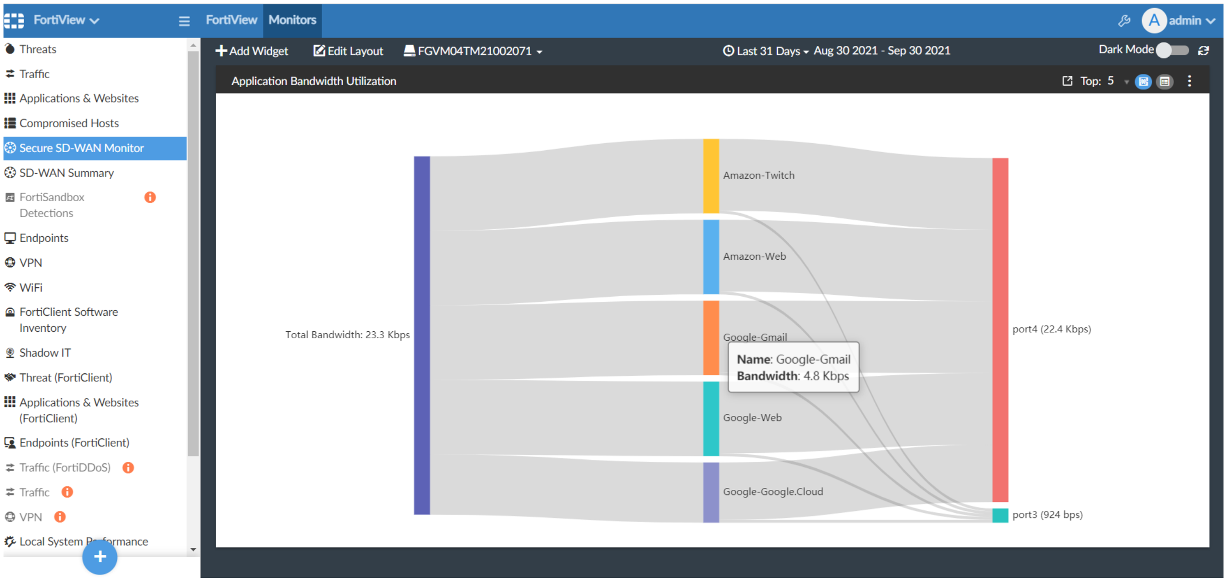
3. You can mouse over bars to see additional information:

- Mousing over a bar on the left of the chart displays the total bandwidth from all applications on a device.



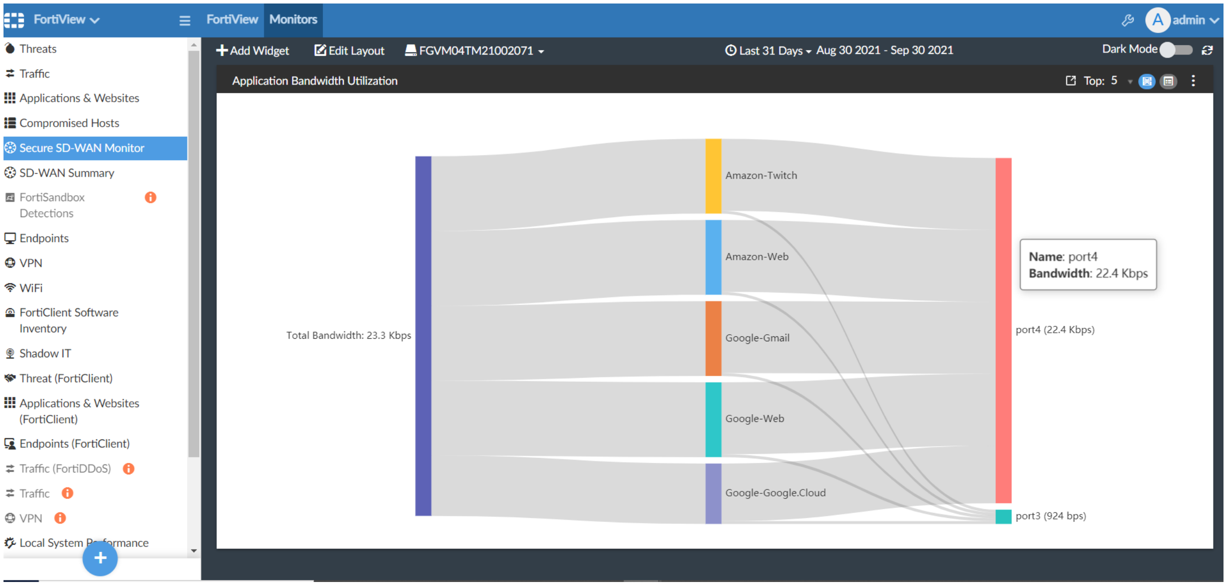
Name: FGVM04TM21002071
Bandwidth: 23.3 Kbps

- Mousing over a bar in the middle of the chart displays bandwidth for an application.



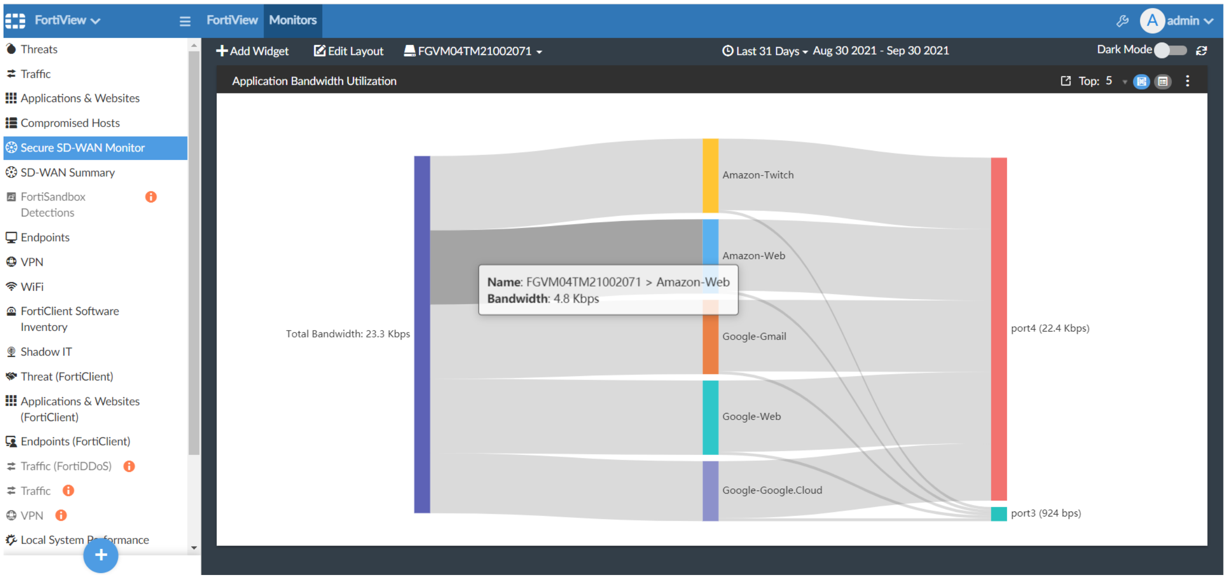
Name: Google-Gmail
Bandwidth: 4.8 Kbps

- Mousing over a bar on the right of the chart displays bandwidth for an interface.



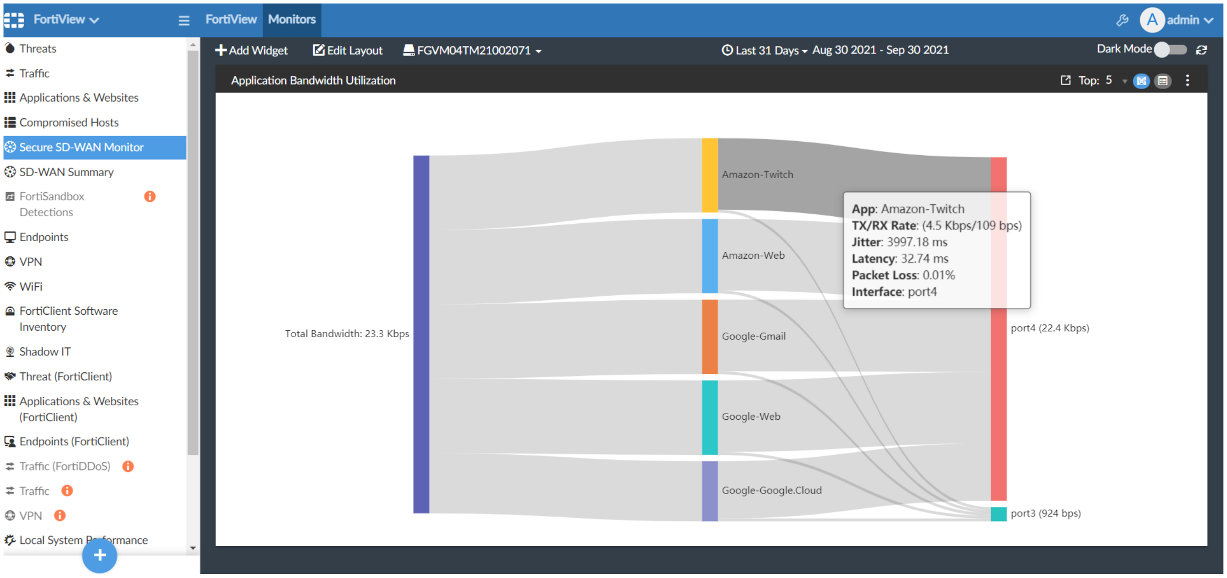
Name: port4
Bandwidth: 22.4 Kbps

4. You can mouse over chords to see additional information:
   - Mousing over a chord on the left side displays bandwidth from the device to an application.



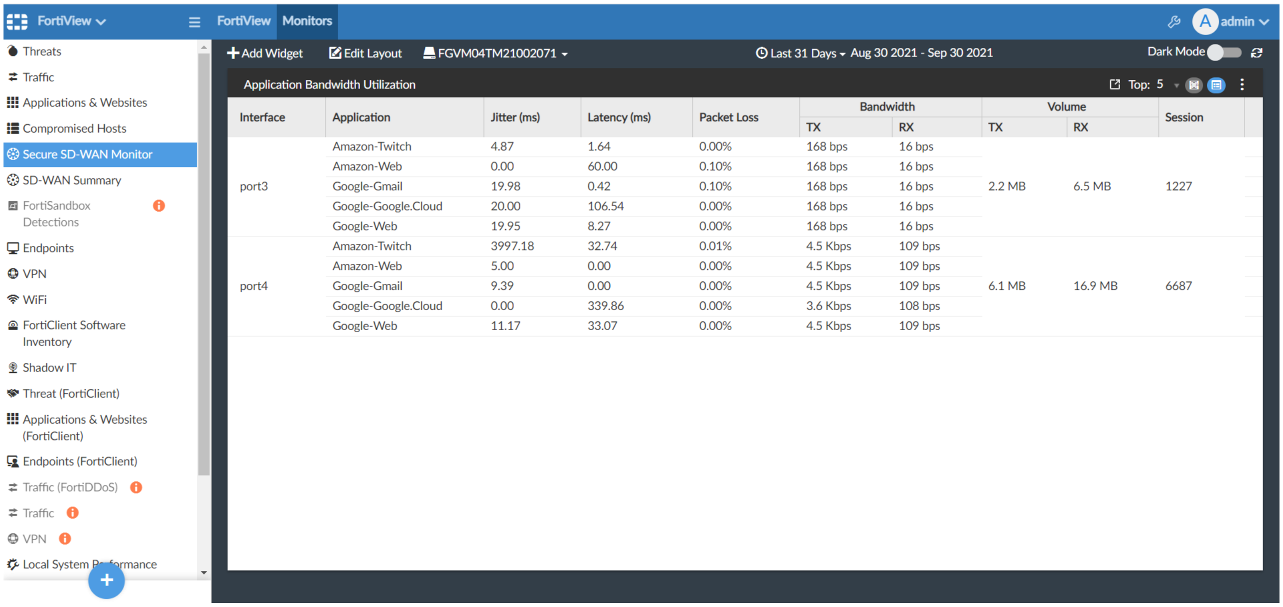
Name: FGVM04TM21002071 > Amazon-Web
Bandwidth: 4.8 Kbps

   - Mousing over a chord on the right side displays bandwidth from an application to an interface, as well as the jitter, latency, and packet loss.



App: Amazon-Twitch
TX/RX Rate: (4.5 Kbps/109 bps)
Jitter: 3997.18 ms
Latency: 32.74 ms
Packet Loss: 0.01%
Interface: port4

5. In the Application Bandwidth Utilization widget, the table chart shows interface, application, jitter, latency, packet loss, bandwidth (TX/RX), volume (TX/RC), and session.



Application Bandwidth Utilization

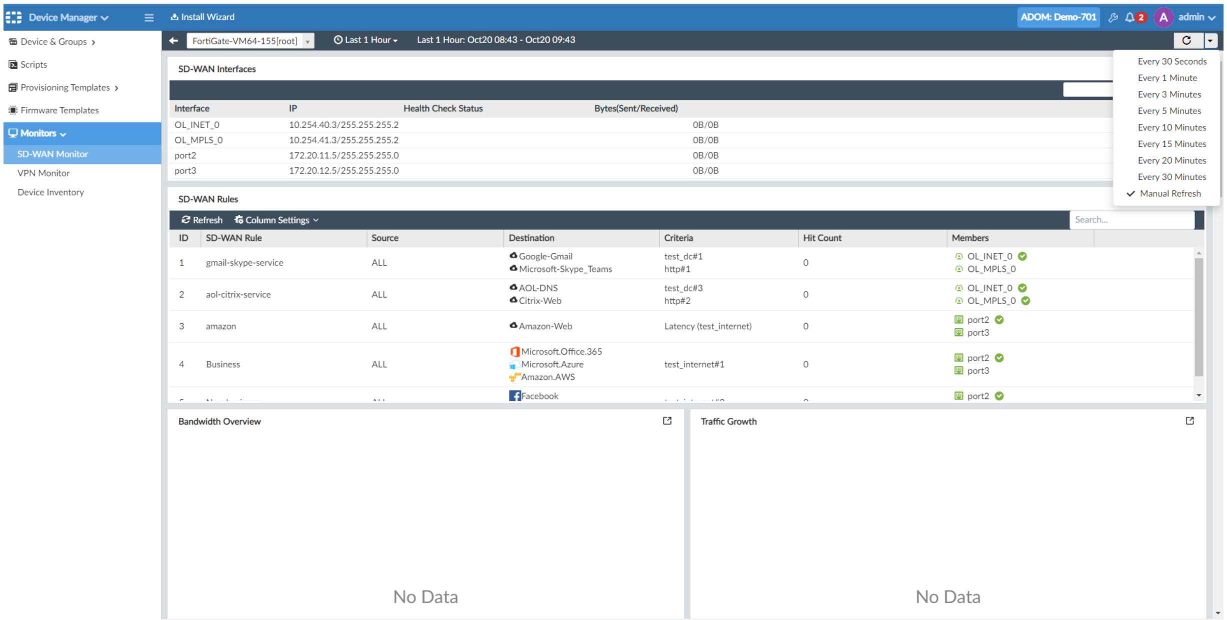
Interface	Application	Jitter (ms)	Latency (ms)	Packet Loss	Bandwidth		Volume		Session
					TX	RX	TX	RX	
port3	Amazon-Twitch	4.87	1.64	0.00%	168 bps	16 bps	2.2 MB	6.5 MB	1227
	Amazon-Web	0.00	60.00	0.10%	168 bps	16 bps			
	Google-Gmail	19.98	0.42	0.10%	168 bps	16 bps			
	Google-Google.Cloud	20.00	106.54	0.00%	168 bps	16 bps			
	Google-Web	19.95	8.27	0.00%	168 bps	16 bps			
port4	Amazon-Twitch	3997.18	32.74	0.01%	4.5 Kbps	109 bps	6.1 MB	16.9 MB	6687
	Amazon-Web	5.00	0.00	0.00%	4.5 Kbps	109 bps			
	Google-Gmail	9.39	0.00	0.00%	4.5 Kbps	109 bps			
	Google-Google.Cloud	0.00	339.86	0.00%	3.6 Kbps	108 bps			
	Google-Web	11.17	33.07	0.00%	4.5 Kbps	109 bps			

SD-WAN real-time monitoring (30 seconds) supported per-device - FMG 7.0.3

SD-WAN real-time monitoring (30 seconds) supported per-device.

To configure real-time monitoring in the SD-WAN Monitor:

1. In a 7.0 ADOM, go to *Device Manager* > *Monitors* > *SD-WAN Monitor*.
2. Select *Table View* from the toolbar.
3. Select a device from the *Devices* dropdown menu.
4. Open the *Refresh* dropdown menu. The menu now includes real-time monitoring options including *Every 30 Seconds*, *Every 1 Minute*, and *Every 3 Minutes* in addition to the previously available refresh options.
5. In the FortiManager CLI, enable SD-WAN monitor history:
   ```
   config system admin setting
      set sdwan-monitor-history enable
   end
   ```
   The GUI works in mixed modes when SD-WAN history is enabled so that administrators do not need to switch the CLI back and forth to view realtime data.
   - When you drilldown per-device on the SD-WAN Monitor page, the default refresh interval is one hour with manual refresh.



Last 1 Hour: Oct20 08:43 - Oct20 09:43

SD-WAN Interfaces

Interface	IP	Health Check Status	Bytes(Sent/Received)
OL_INET_0	10.254.40.3/255.255.255.2		0B/0B
OL_MPLS_0	10.254.41.3/255.255.255.2		0B/0B
port2	172.20.11.5/255.255.255.0		0B/0B
port3	172.20.12.5/255.255.255.0		0B/0B

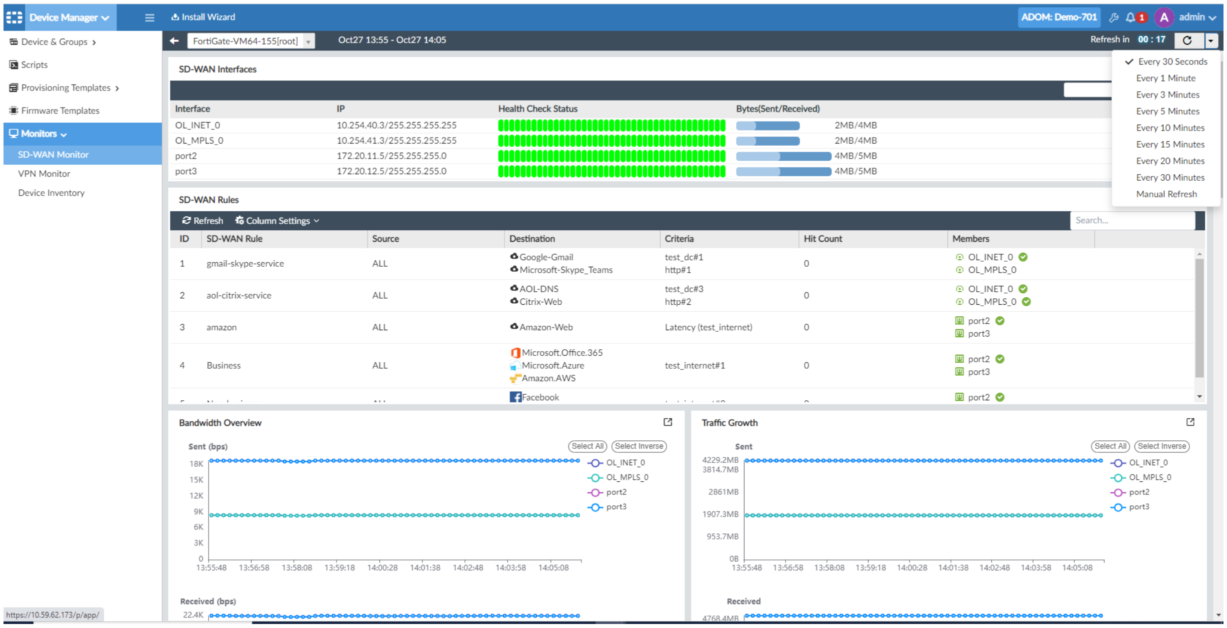
SD-WAN Rules

ID	SD-WAN Rule	Source	Destination	Criteria	Hit Count	Members
1	gmail-skype-service	ALL	Google-Gmail Microsoft-Skype_Teams	test_dc#1 http#1	0	OL_INET_0 ✓ OL_MPLS_0
2	aol-citrix-service	ALL	AOL-DNS Citrix-Web	test_dc#3 http#2	0	OL_INET_0 ✓ OL_MPLS_0 ✓
3	amazon	ALL	Amazon-Web	Latency (test_internet)	0	port2 ✓ port3
4	Business	ALL	Microsoft.Office.365 Microsoft.Azure Amazon.AWS	test_internet#1	0	port2 ✓ port3
			Facebook			port2 ✓

Bandwidth Overview

Traffic Growth

- If you choose to set the refresh interval to every 30 seconds, 1 minute, or three minutes, the timespan range is fixed to the last 10 minutes and cannot be changed. The FortiManager GUI will retrieve data from FortiGate.



Oct27 13:55 - Oct27 14:05

SD-WAN Interfaces

Interface	IP	Health Check Status	Bytes(Sent/Received)
OL_INET_0	10.254.40.3/255.255.255.255		2MB/4MB
OL_MPLS_0	10.254.41.3/255.255.255.255		2MB/4MB
port2	172.20.11.5/255.255.255.0		4MB/5MB
port3	172.20.12.5/255.255.255.0		4MB/5MB

SD-WAN Rules

ID	SD-WAN Rule	Source	Destination	Criteria	Hit Count	Members
1	gmail-skype-service	ALL	Google-Gmail Microsoft-Skype_Teams	test_dc#1 http#1	0	OL_INET_0 ✓ OL_MPLS_0
2	aol-citrix-service	ALL	AOL-DNS Citrix-Web	test_dc#3 http#2	0	OL_INET_0 ✓ OL_MPLS_0 ✓
3	amazon	ALL	Amazon-Web	Latency (test_internet)	0	port2 ✓ port3
4	Business	ALL	Microsoft.Office.365 Microsoft.Azure Amazon.AWS	test_internet#1	0	port2 ✓ port3
			Facebook			port2 ✓

Bandwidth Overview

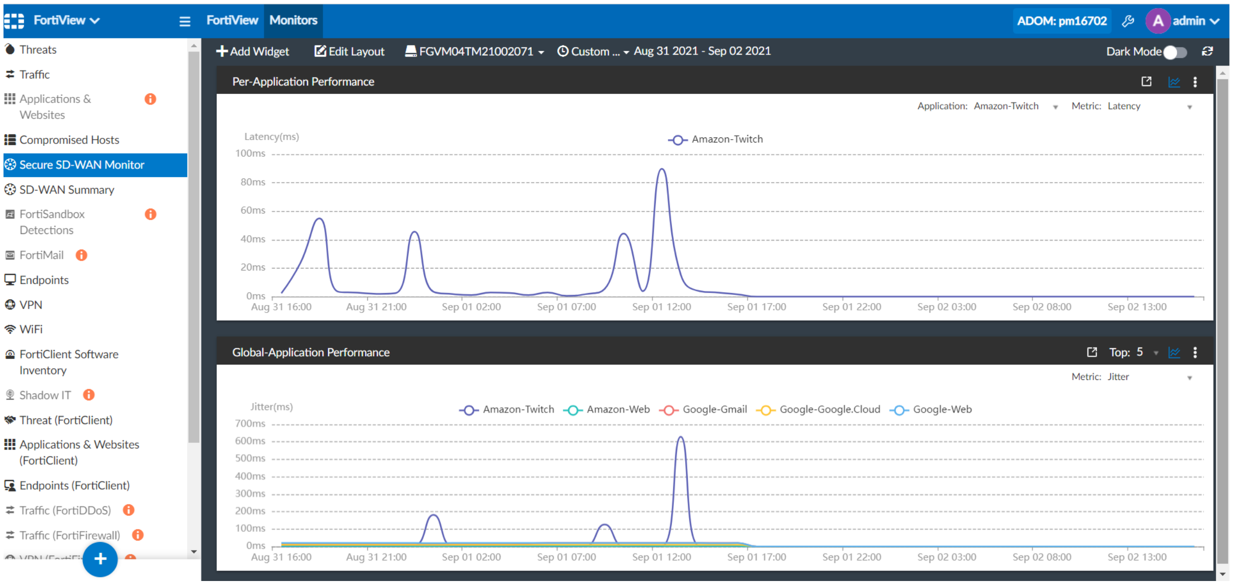
Traffic Growth

SD-WAN application performance monitoring - FAZ 7.0.3

In FortiAnalyzer, the following new widgets have been added to *Secure SD-WAN Monitor*:

- Per-Application Performance
- Global-Application Performance

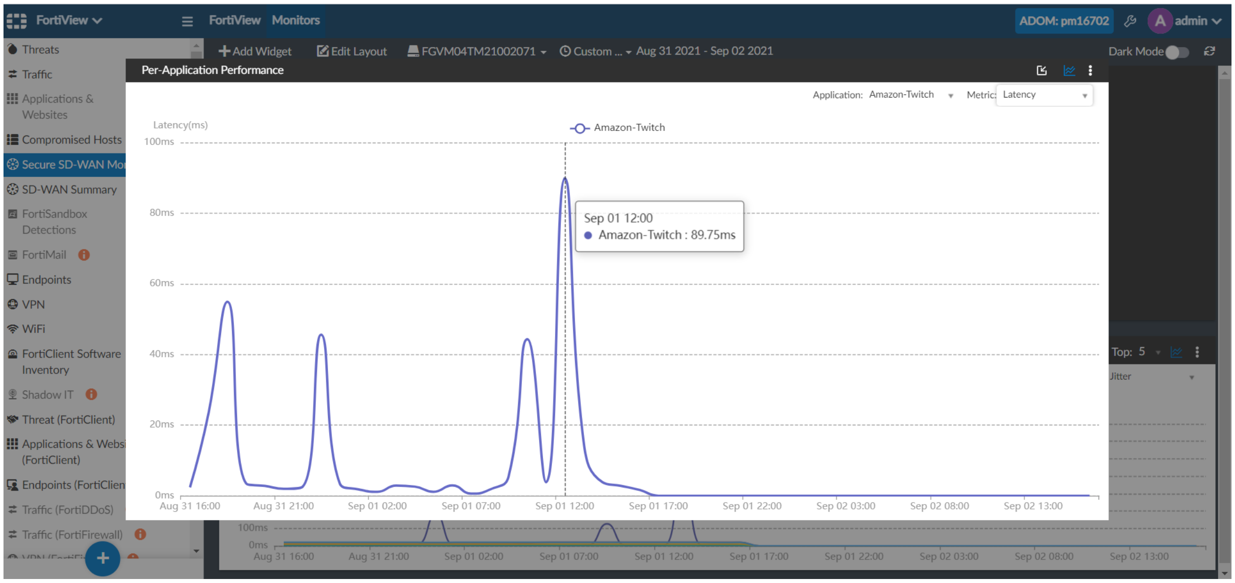
These widgets provide additional visibility for user application experience on the SD-WAN network.



These widgets allow for individual application logging of SD-WAN health information, including latency, jitter, packet loss, and bandwidth. This information is received as SD-WAN event logs with LogID 0113022936.

To view the *Per-Application Performance* widget:

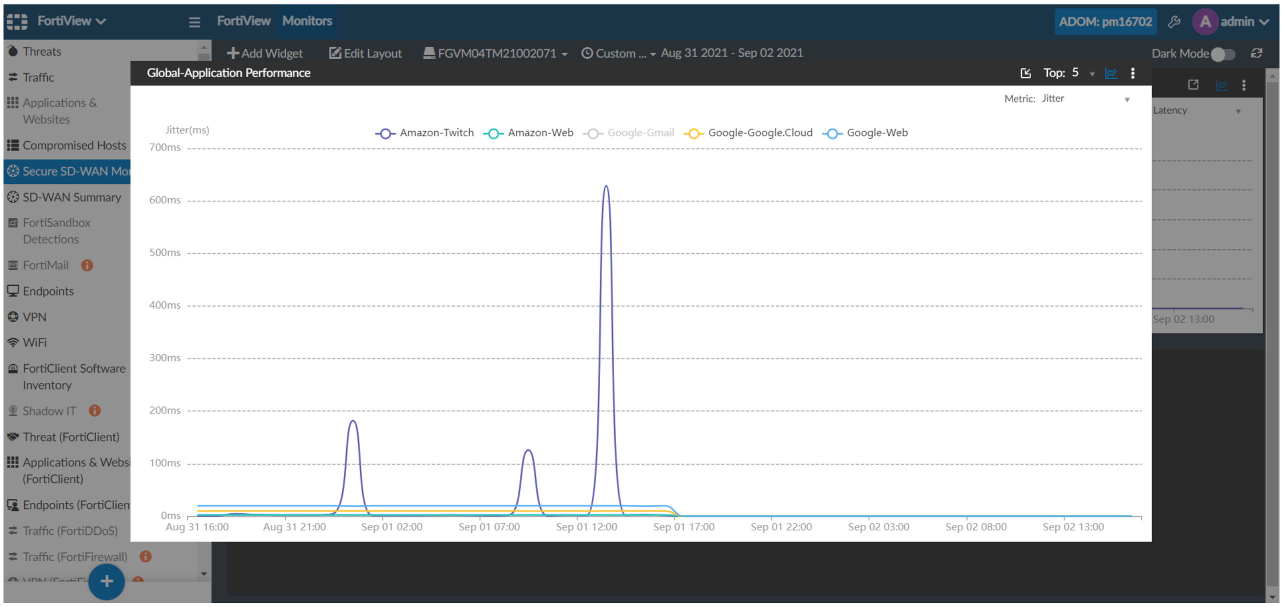
1. Go to *FortiView* > *Monitors* > *Secure SD-WAN Monitor* to see the *Per-Application Performance* widget. If you do not see this widget, you can add it to the dashboard from the *Add Widget* button in the toolbar.
2. From the *Application* dropdown in the widget, select an application to view its performance in a line chart.
3. From the *Metric* dropdown in the widget, select a metric to view in the line chart.
4. Hover your cursor over the line chart to view performance at that time.



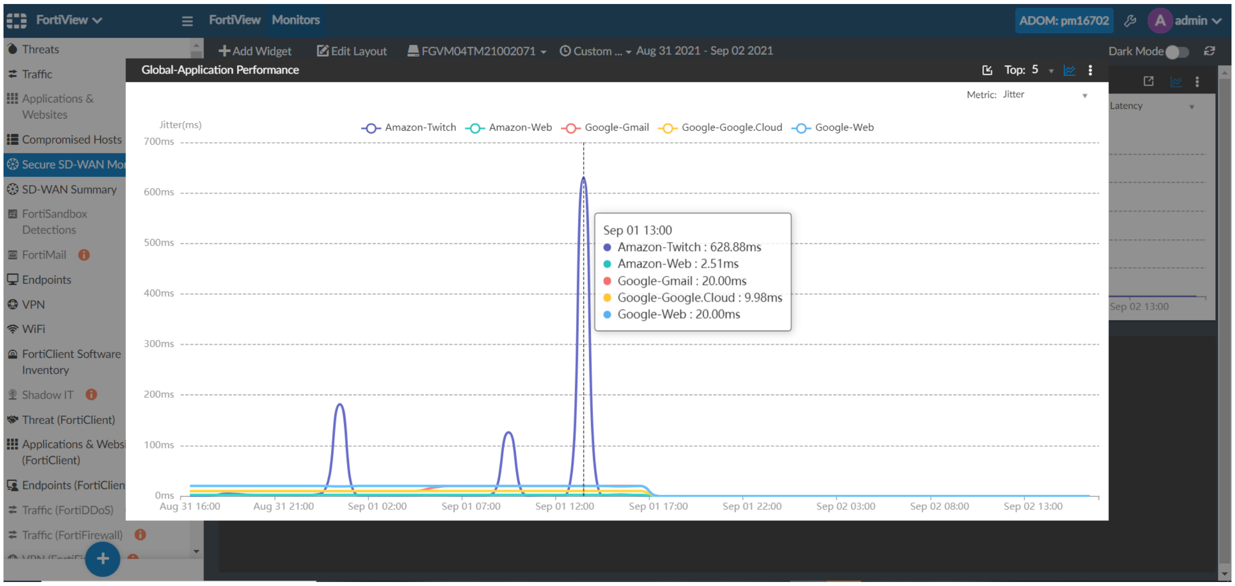
To view the *Global-Application Performance* widget:

1. Go to *FortiView* > *Monitors* > *Secure SD-WAN Monitor* to see the *Global-Application Performance* widget. If you do not see this widget, you can add it to the dashboard from the *Add Widget* button in the toolbar.

2. From the *Top* dropdown in the widget, select how many of the top applications to view in the line chart.
3. From the *Metric* dropdown in the widget, select a performance metric in the line chart.
4. To hide/show an application in the line chart, click the application title in the chart legend.
   Grayed-out applications in the legend are hidden in the line chart.



5. Hover your cursor over the line chart to view performance at that time.



Sep 01 13:00
- Amazon-Twitch : 628.88ms
- Amazon-Web : 2.51ms
- Google-Gmail : 20.00ms
- Google-Google.Cloud : 9.98ms
- Google-Web : 20.00ms

Provisioning

7.0.0

- New SD-WAN template FMG on page 55

7.0.1

- IPsec template enhanced support for tunnel interface configuration FMG 7.0.1 on page 66
- Templates support assignment to device groups FMG 7.0.1 on page 68
- CLI Template improvements FMG 7.0.1 on page 70

7.0.2

- BGP template to manage all BGP routing configurations FMG 7.0.2 on page 74
- Import IPSec VPN configuration from a managed FortiGate into a IPSec template FMG 7.0.2 on page 81

7.0.3

- Import BGP routing configuration from a managed FortiGate into a template FMG 7.0.3 on page 83
- BGP and IPsec recommended templates for SD-WAN overlays FMG 7.0.3 on page 84

New SD-WAN template - FMG

With the new SD-WAN template, you can use Device VDOM meta fields in the member interface/ interface gateway, neighbor IP, and health-check server definitions.

In addition, how you enable and configure SD-WAN per-device management and central management has changed. You now use the following methods to enable and configure each:

- For per-device management, use the device database to configure SD-WAN settings on each device.
- For central management, use SD-WAN templates to configure SD-WAN settings on one or more devices. SD-WAN templates have moved in *Device Manager* to *Provisioning Templates*.
  When you assign an SD-WAN template to a device, you have enabled SD-WAN central management for the device.

  Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.

When using SD-WAN templates with other types of provisioning templates, such as interface templates and IPsec templates, you should execute the templates in the following order:

- Interface template
- IPsec template
- SD-WAN template

This topic contains the following sections:

- SD-WAN per-device management on page 56
- SD-WAN central management on page 57

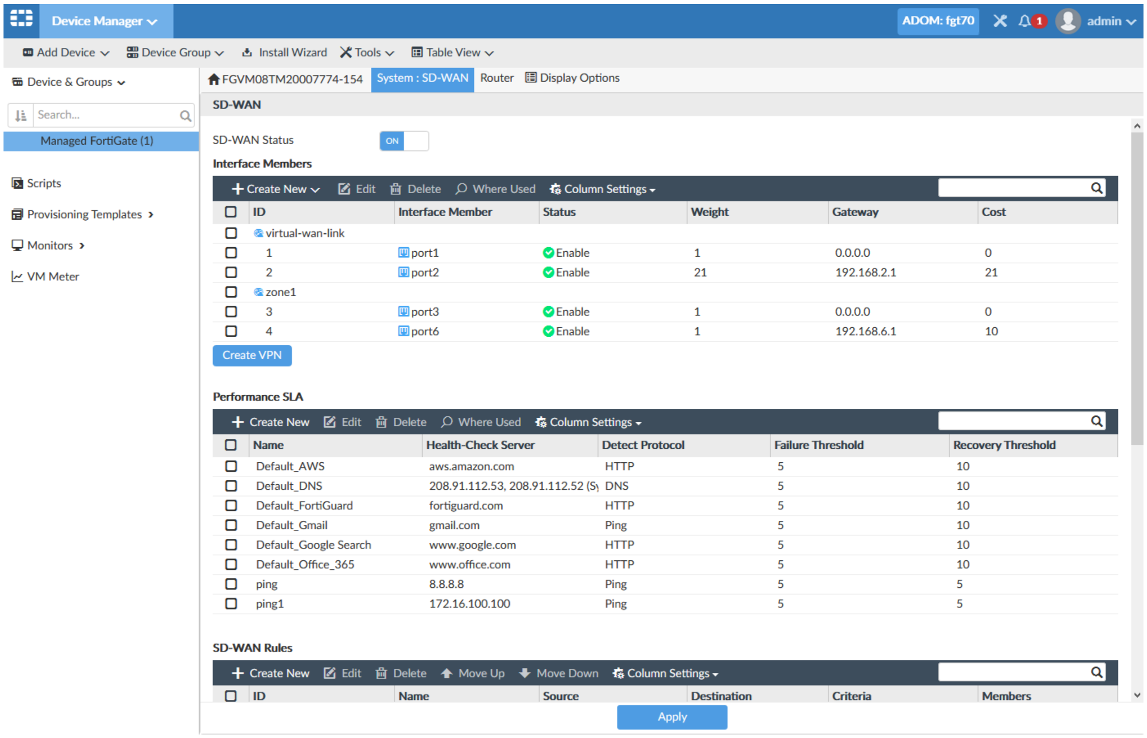
- SD-WAN template support for meta fields on page 63

SD-WAN per-device management

For SD-WAN per-device management, you can create, edit, and delete interface members, performance SLA, SD-WAN rules, Neighbor, and duplication. After configuring SD-WAN settings, install the configuration to the device.

To access SD-WAN per-device management:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Open the device database for the device:
   a. Go to *Device Manager > Device & Groups*.
   b. From the toolbar, select *Table View*.
   c. In the tree menu, select a device group.
      The devices in the group are displayed in the content pane.
   d. In the content pane, double-click a device.
      Alternately, select a device, and select *Configuration* from the *More* menu.
      The device database is displayed in the content pane.
3. In the toolbar, click the *System* menu, and select *SD-WAN*.
   The *SD-WAN* pane opens.



SD-WAN

SD-WAN Status: ON

Interface Members

ID	Interface Member	Status	Weight	Gateway	Cost
virtual-wan-link					
1	port1	Enable	1	0.0.0.0	0
2	port2	Enable	21	192.168.2.1	21
zone1					
3	port3	Enable	1	0.0.0.0	0
4	port6	Enable	1	192.168.6.1	10

Performance SLA

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
Default_AWS	aws.amazon.com	HTTP	5	10
Default_DNS	208.91.112.53, 208.91.112.52 (Sy	DNS	5	10
Default_FortiGuard	fortiguard.com	HTTP	5	10
Default_Gmail	gmail.com	Ping	5	10
Default_Google Search	www.google.com	HTTP	5	10
Default_Office_365	www.office.com	HTTP	5	10
ping	8.8.8.8	Ping	5	5
ping1	172.16.100.100	Ping	5	5

SD-WAN Rules

ID	Name	Source	Destination	Criteria	Members

4. Configure the following sections for the device, and click *Apply*:
   - Interface Members
   - Performance SLA
   - SD-WAN Rules

- Neighbor
- Duplication

5. Install the configuration to the device.

SD-WAN central management

For SD-WAN central management, you can create an SD-WAN template, and assign the template to one or more devices.

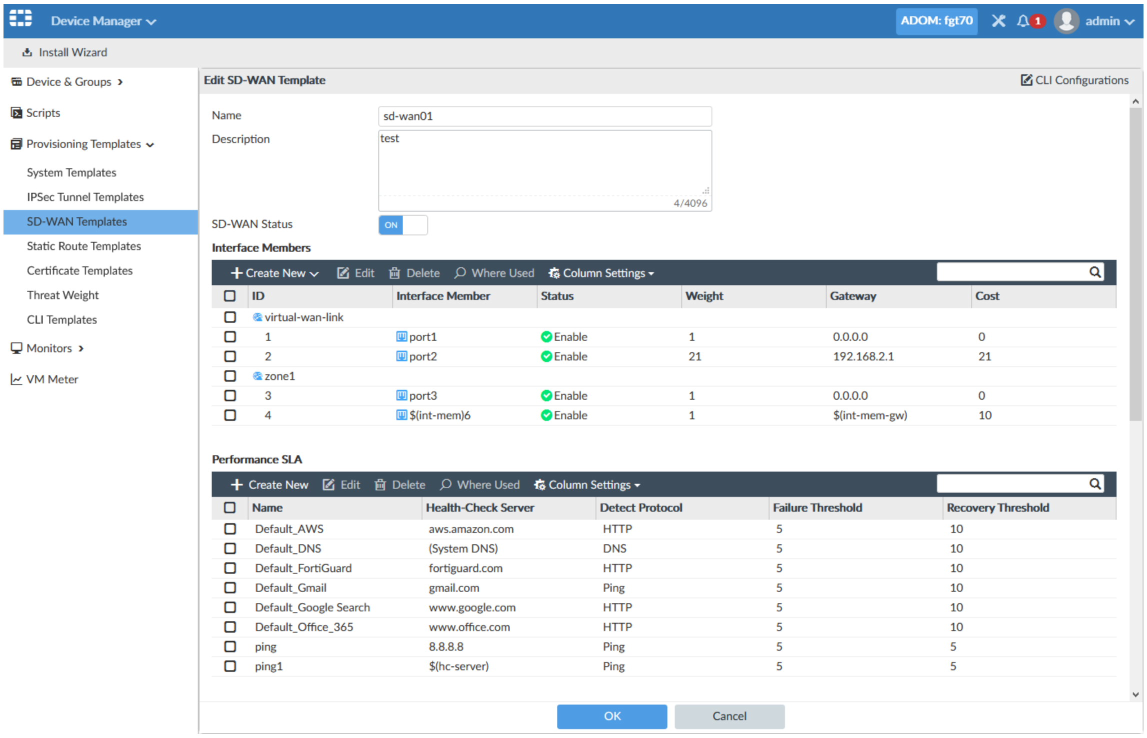
Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.

Create performance SLA and SD-WAN rules. You can also configure BGP neighbors and packet duplication. Advanced configuration options are also available.

After configuring an SD-WAN template, assign the template to one or more devices, and then install the configuration to the devices.

To access SD-WAN central management:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *Provisioning Templates* > *SD-WAN Templates*.
   The SD-WAN templates are displayed.
3. Click *Create New*, and select *Template*.
   The *SD-WAN Template* pane is displayed.



Edit SD-WAN Template

Name: sd-wan01

Description: test

4/4096

SD-WAN Status: ON

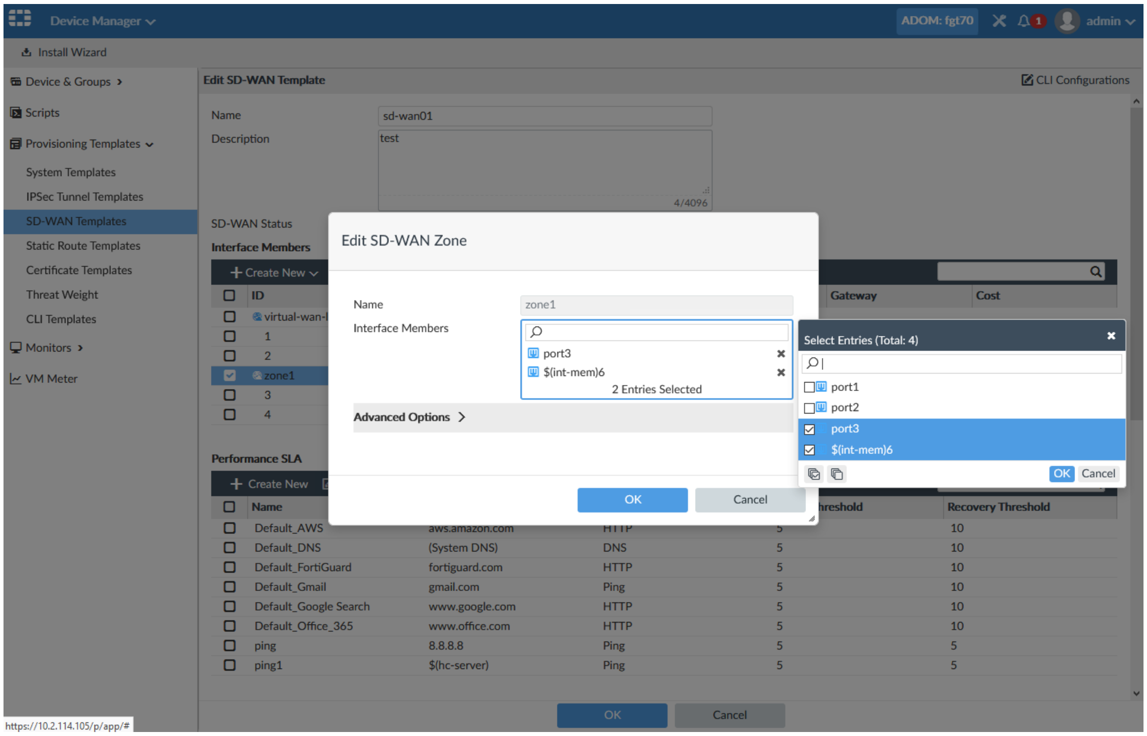
Interface Members

ID	Interface Member	Status	Weight	Gateway	Cost
virtual-wan-link					
1	port1	Enable	1	0.0.0.0	0
2	port2	Enable	21	192.168.2.1	21
zone1					
3	port3	Enable	1	0.0.0.0	0
4	$(int-mem)6	Enable	1	$(int-mem-gw)	10

Performance SLA

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
Default_AWS	aws.amazon.com	HTTP	5	10
Default_DNS	(System DNS)	DNS	5	10
Default_FortiGuard	fortiguard.com	HTTP	5	10
Default_Gmail	gmail.com	Ping	5	10
Default_Google Search	www.google.com	HTTP	5	10
Default_Office_365	www.office.com	HTTP	5	10
ping	8.8.8.8	Ping	5	5
ping1	$(hc-server)	Ping	5	5

4. In the *Interface Members* section, create one or more zones:
   - **a.** Click *Create New* > *SD-WAN Zone*.
     The *Create New SD-WAN Zone* dialog box is displayed.
   - **b.** In the *Name* box, type a name for the zone.
   - **c.** Beside *Interface Members*, click the box to select interface members.



Edit SD-WAN Template

Name: sd-wan01

Description: test

4/4096

SD-WAN Status

Interface Members

	ID	Gateway	Cost
□	virtual-wan-l		
□	1		
□	2		
☑	zone1		
□	3		
□	4		

Edit SD-WAN Zone

Name: zone1

Interface Members: port3, $(int-mem)6

2 Entries Selected

Select Entries (Total: 4)

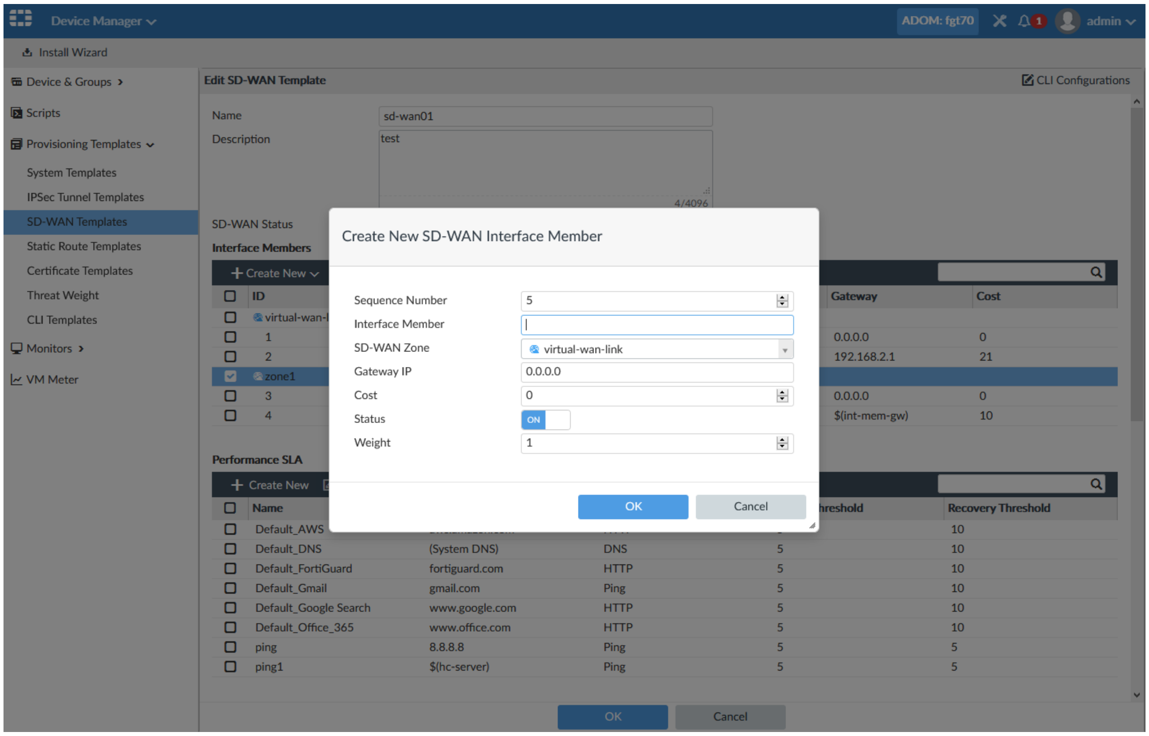
- □ port1
- □ port2
- ☑ port3
- ☑ $(int-mem)6

Performance SLA

	Name			hreshold	Recovery Threshold
□	Default_AWS	aws.amazon.com	HTTP	5	10
□	Default_DNS	(System DNS)	DNS	5	10
□	Default_FortiGuard	fortiguard.com	HTTP	5	10
□	Default_Gmail	gmail.com	Ping	5	10
□	Default_Google Search	www.google.com	HTTP	5	10
□	Default_Office_365	www.office.com	HTTP	5	10
□	ping	8.8.8.8	Ping	5	5
□	ping1	$(hc-server)	Ping	5	5

   - **d.** Click *OK*.
     The SD-WAN zone is created.

5. In the *Interface Members* section, create SD-WAN interface members:
   - **a.** Click *Create New* > *SD-WAN Member*.
     The *Create New SD-WAN Interface Member* dialog box is displayed.
   - **b.** In the *Interface Members* box, type the name of the interface.
     Bind the interfaces by name to physical or VPN interfaces.



Name sd-wan01

Description test

Create New SD-WAN Interface Member

Sequence Number	5
Interface Member	
SD-WAN Zone	virtual-wan-link
Gateway IP	0.0.0.0
Cost	0
Status	ON
Weight	1

OK Cancel

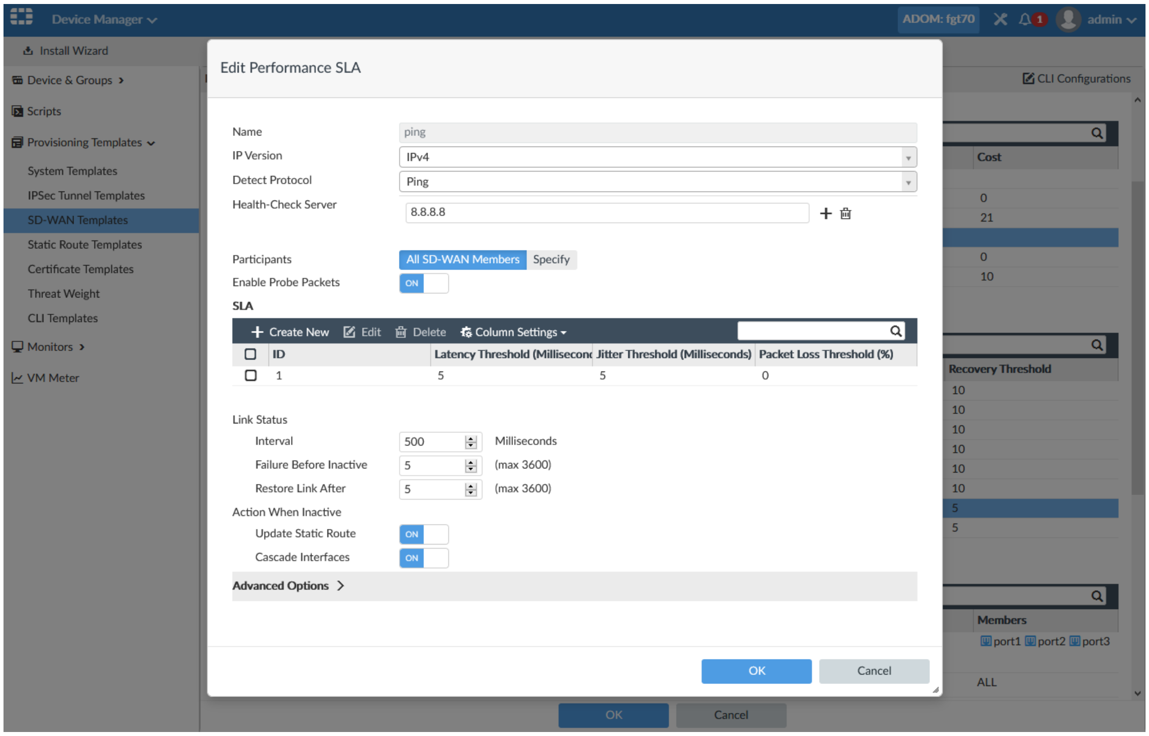
ID	Gateway	Cost
virtual-wan-l		
1	0.0.0.0	0
2	192.168.2.1	21
zone1		
3	0.0.0.0	0
4	$(int-mem-gw)	10

Name				hreshold	Recovery Threshold
Default_AWS					10
Default_DNS	(System DNS)	DNS	5		10
Default_FortiGuard	fortiguard.com	HTTP	5		10
Default_Gmail	gmail.com	Ping	5		10
Default_Google Search	www.google.com	HTTP	5		10
Default_Office_365	www.office.com	HTTP	5		10
ping	8.8.8.8	Ping	5		5
ping1	$(hc-server)	Ping	5		5

c. Click *OK*.
The SD-WAN interface member is created.

6. Create Performance SLA:

a. In the *Performance SLA* section, click *Create New*.
The *Performance SLA* dialog box is displayed.



Edit Performance SLA

Name	ping
IP Version	IPv4
Detect Protocol	Ping
Health-Check Server	8.8.8.8
Participants	All SD-WAN Members / Specify
Enable Probe Packets	ON

SLA

ID	Latency Threshold (Millisecond	Jitter Threshold (Milliseconds)	Packet Loss Threshold (%)
1	5	5	0

Link Status

Interval	500	Milliseconds
Failure Before Inactive	5	(max 3600)
Restore Link After	5	(max 3600)

Action When Inactive

Update Static Route	ON
Cascade Interfaces	ON

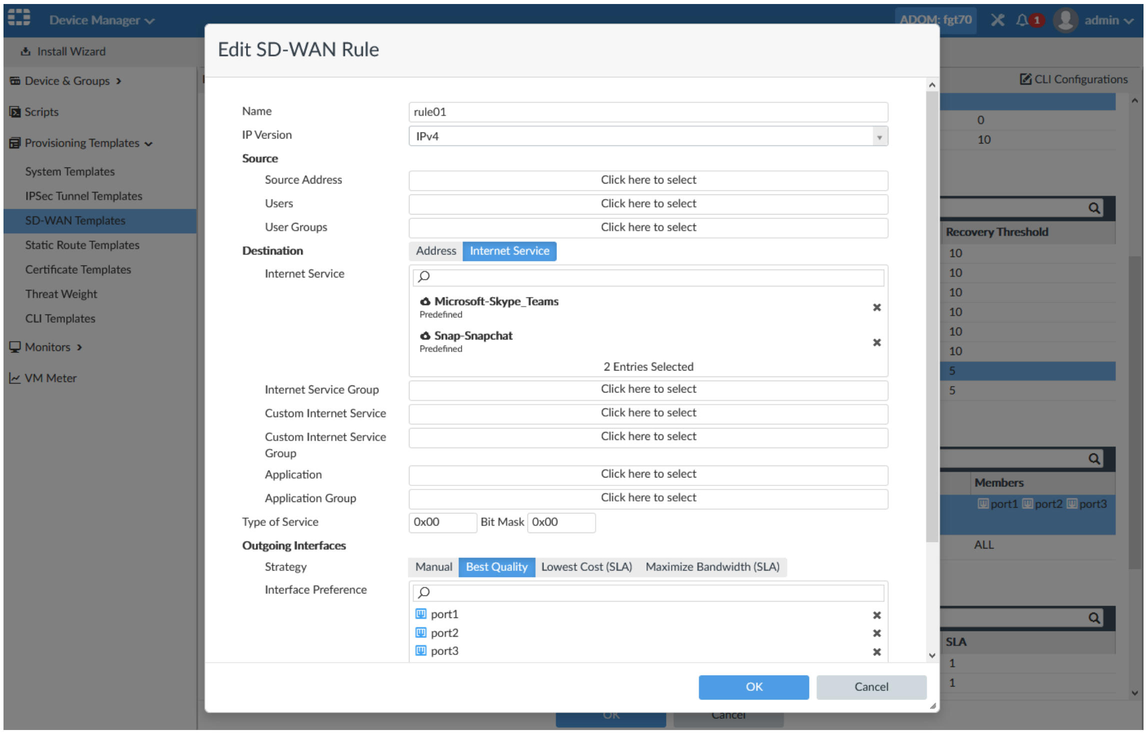
Advanced Options

OK Cancel

b. Complete the options, and click *OK*.
   The Performance SLA settings are saved.

7. Create SD-WAN rules.

   a. In the *SD-WAN Rules* section, click *Create New*.
      The *SD-WAN Rule* dialog box is displayed.



Edit SD-WAN Rule

Name: rule01

IP Version: IPv4

Source
- Source Address: Click here to select
- Users: Click here to select
- User Groups: Click here to select

Destination: Address | **Internet Service**
- Internet Service:
  - Microsoft-Skype_Teams (Predefined)
  - Snap-Snapchat (Predefined)
  - 2 Entries Selected
- Internet Service Group: Click here to select
- Custom Internet Service: Click here to select
- Custom Internet Service Group: Click here to select
- Application: Click here to select
- Application Group: Click here to select

Type of Service: 0x00 Bit Mask: 0x00

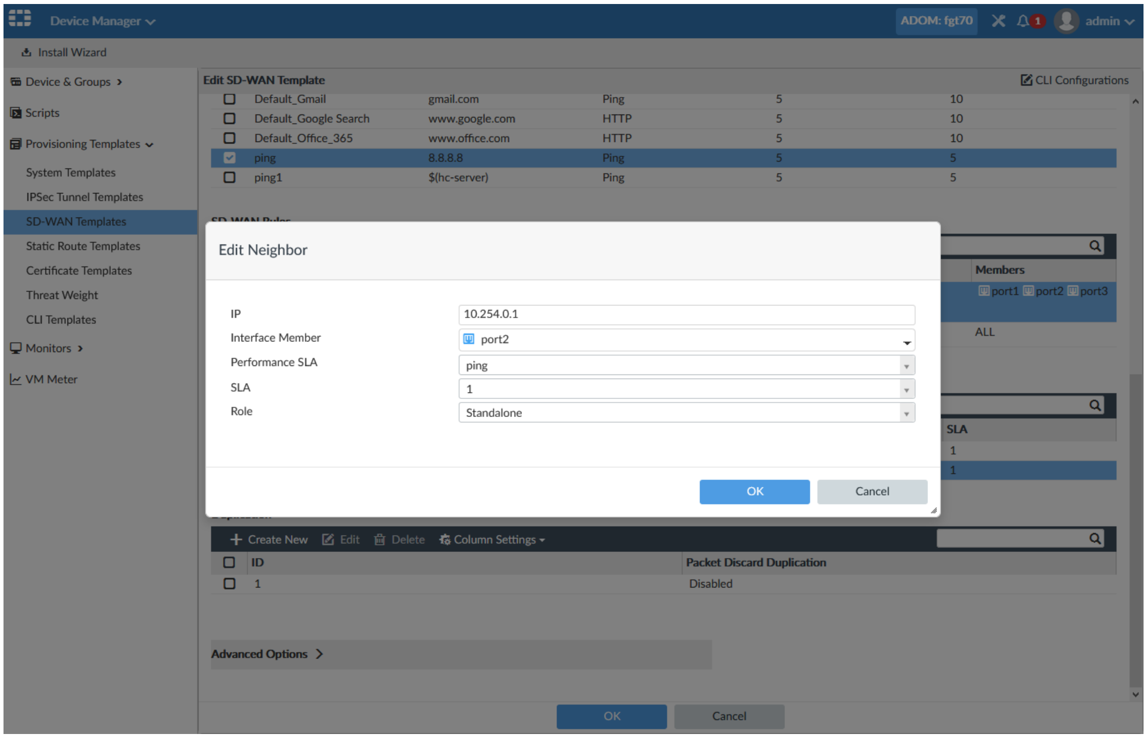
Outgoing Interfaces
- Strategy: Manual | **Best Quality** | Lowest Cost (SLA) | Maximize Bandwidth (SLA)
- Interface Preference:
  - port1
  - port2
  - port3

OK | Cancel

   b. Complete the options, and click *OK*.
      The SD-WAN rules are saved.

8. Configure BGP neighbors.

   a. In the *Neighbor* section, click *Create New*.
      The *Neighbor* dialog box is displayed.



Edit SD-WAN Template

□	Default_Gmail	gmail.com	Ping	5	10
□	Default_Google Search	www.google.com	HTTP	5	10
□	Default_Office_365	www.office.com	HTTP	5	10
☑	ping	8.8.8.8	Ping	5	5
□	ping1	$(hc-server)	Ping	5	5

Edit Neighbor

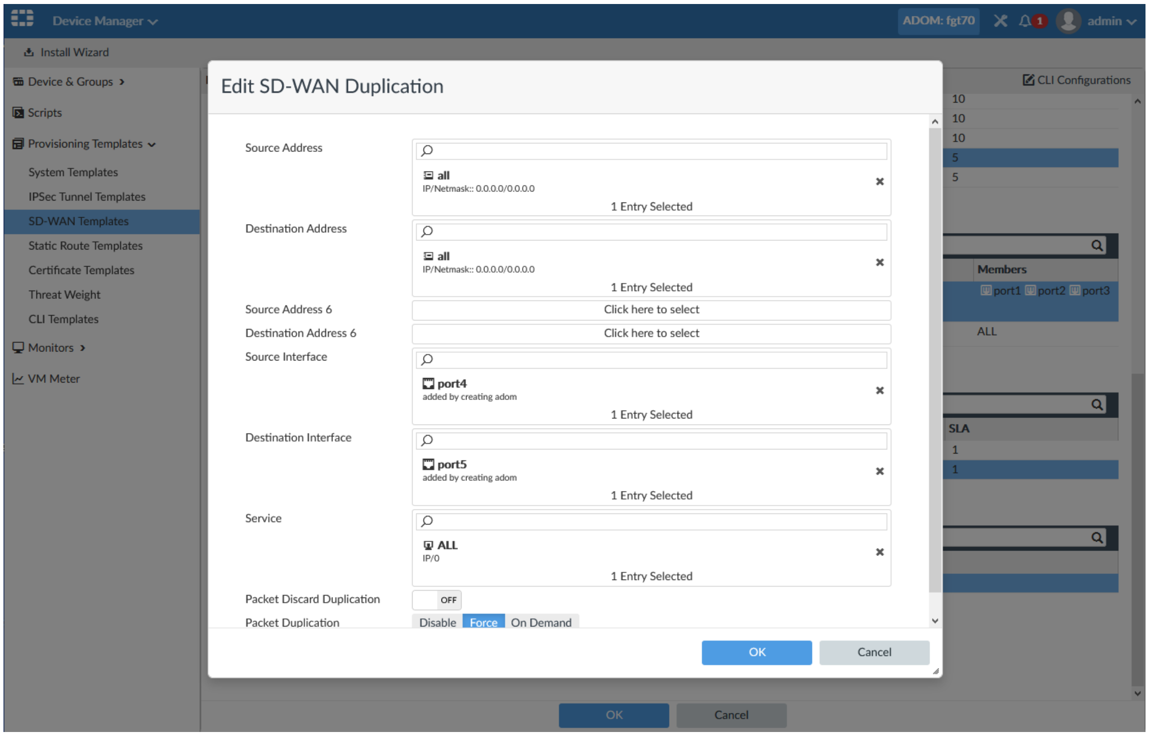
IP	10.254.0.1
Interface Member	port2
Performance SLA	ping
SLA	1
Role	Standalone

□	ID	Packet Discard Duplication
□	1	Disabled

b. Complete the options, and click *OK*.
The neighbor settings are saved.

9. Configure packet duplication.

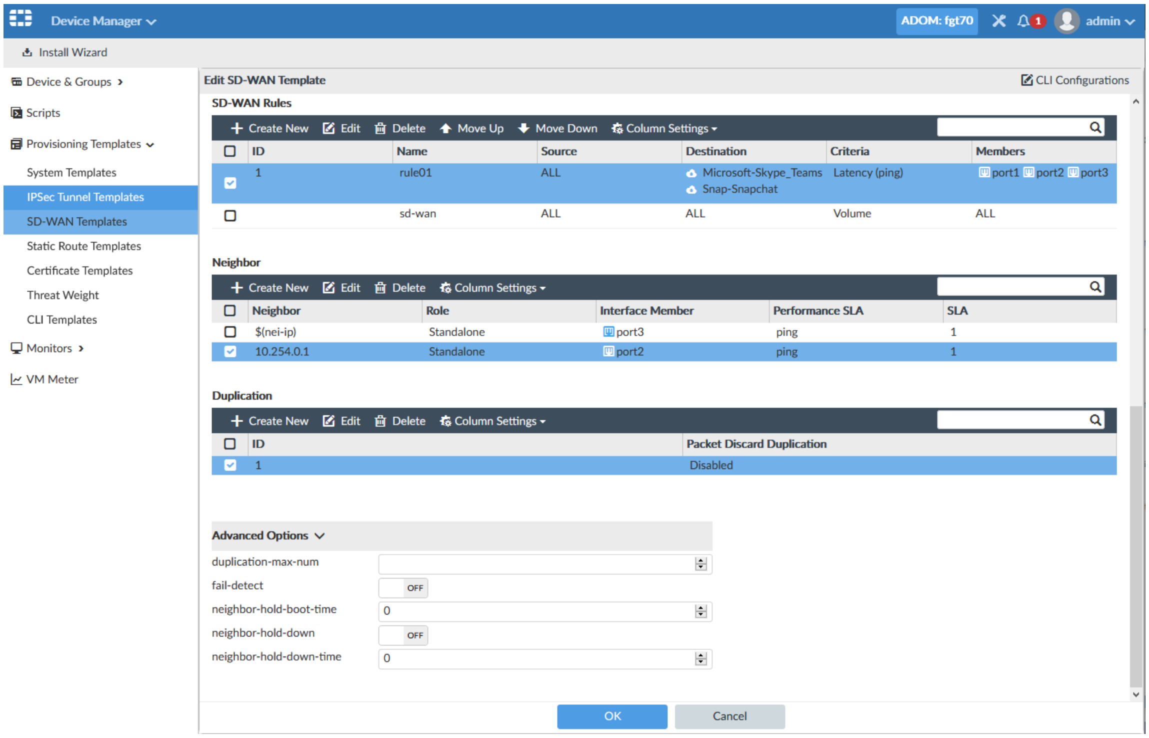
a. In the *Duplication* section, click *Create New*.
The *Duplication* dialog box is displayed.



Edit SD-WAN Duplication

Source Address	all IP/Netmask:: 0.0.0.0/0.0.0.0 1 Entry Selected
Destination Address	all IP/Netmask:: 0.0.0.0/0.0.0.0 1 Entry Selected
Source Address 6	Click here to select
Destination Address 6	Click here to select
Source Interface	port4 added by creating adom 1 Entry Selected
Destination Interface	port5 added by creating adom 1 Entry Selected
Service	ALL IP/0 1 Entry Selected
Packet Discard Duplication	OFF
Packet Duplication	Disable [✓ Force] On Demand

b. Complete the options, and click *OK*.
The packet duplication settings are saved.



Edit SD-WAN Template

SD-WAN Rules

□	ID	Name	Source	Destination	Criteria	Members
☑	1	rule01	ALL	Microsoft-Skype_Teams Snap-Snapchat	Latency (ping)	port1 port2 port3
□		sd-wan	ALL	ALL	Volume	ALL

Neighbor

□	Neighbor	Role	Interface Member	Performance SLA	SLA
□	$(nei-ip)	Standalone	port3	ping	1
☑	10.254.0.1	Standalone	port2	ping	1

Duplication

□	ID	Packet Discard Duplication
☑	1	Disabled

Advanced Options

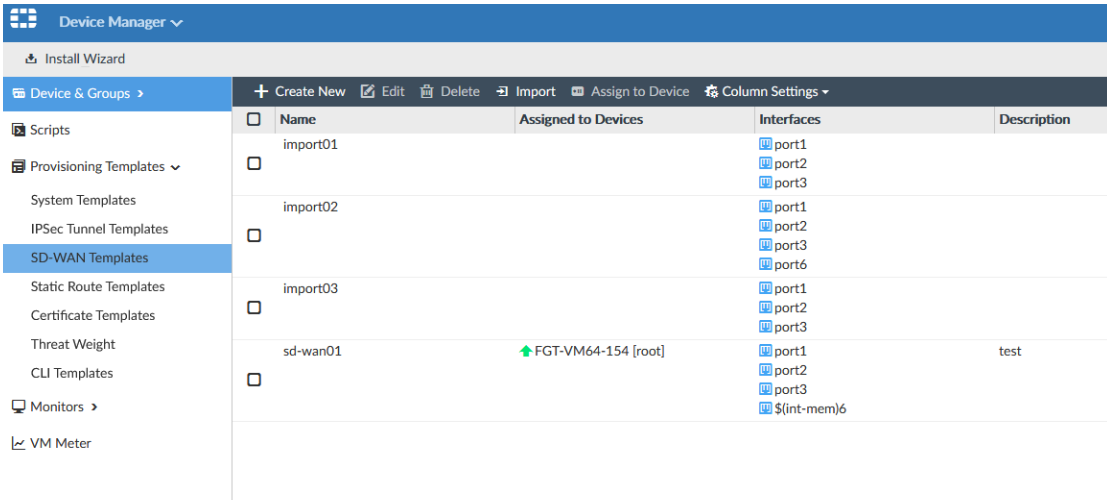
duplication-max-num	
fail-detect	OFF
neighbor-hold-boot-time	0
neighbor-hold-down	OFF
neighbor-hold-down-time	0

10. Click *OK*.
The SD-WAN template is saved.

11. Assign the SD-WAN template to one or more devices.

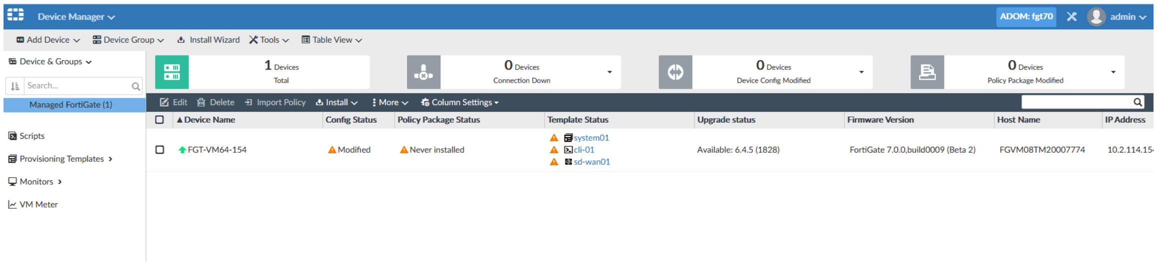
a. Select the SD-WAN template, and click *Assign to Device*.
The *Assign to Device* dialog box is displayed.

b. In the *Available Entries* list, select the device, and click the right arrow to move the device to the *Selected Entries* list, and click *OK*.
The SD-WAN template is assigned to the device.



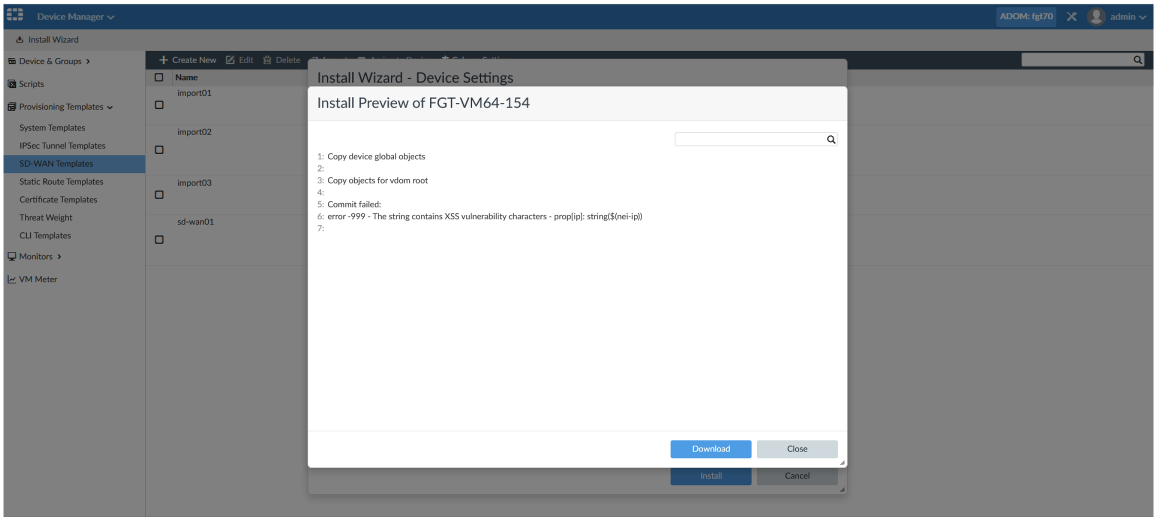
□	Name	Assigned to Devices	Interfaces	Description
□	import01		port1 port2 port3	
□	import02		port1 port2 port3 port6	
□	import03		port1 port2 port3	
□	sd-wan01	FGT-VM64-154 [root]	port1 port2 port3 $(int-mem)6	test

12. Go to *Device Manager* > *Device & Groups*, and view the assigned provisioning templates in the *Template Status* column.



Device Name	Config Status	Policy Package Status	Template Status	Upgrade status	Firmware Version	Host Name	IP Address
FGT-VM64-154	Modified	Never installed	system01 cli-01 sd-wan01	Available: 6.4.5 (1828)	FortiGate 7.0.0,build0009 (Beta 2)	FGVM08TM20007774	10.2.114.15

13. Click *Install Wizard* to install the device settings.
    You can preview the settings.



Install Wizard - Device Settings

Install Preview of FGT-VM64-154

```
Copy device global objects

Copy objects for vdom root

Commit failed:
error -999 - The string contains XSS vulnerability characters - prop[ip]: string($(nei-ip))

```

SD-WAN template support for meta fields

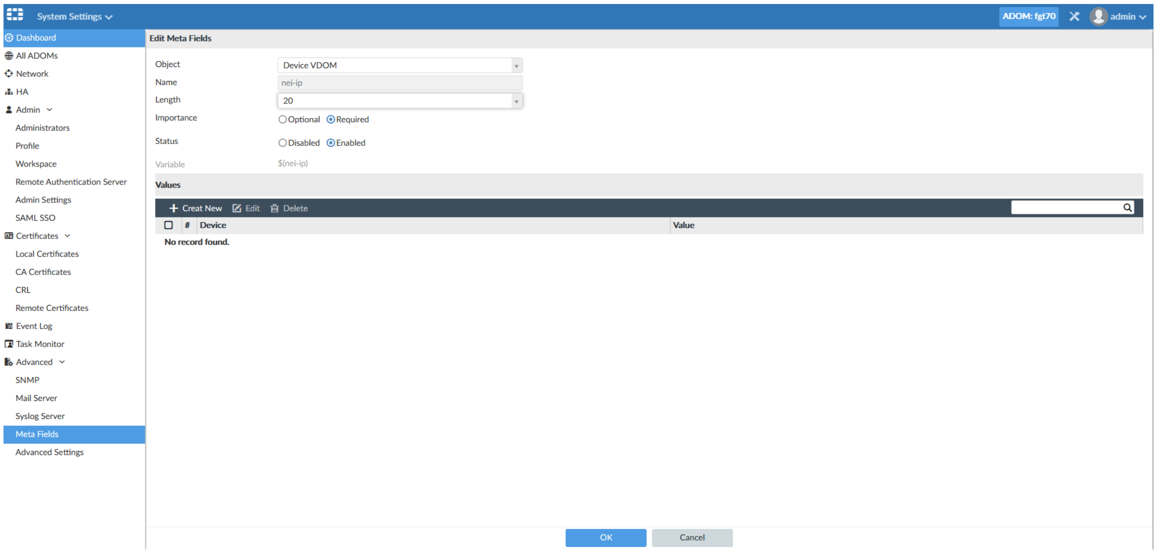
SD-WAN templates support Device VDOM meta fields. You can use meta fields in SD-WAN templates for the following options:

- SD-WAN interface member
  - Interface member option
  - Gateway IP option
- Neighbor
  - IP option
- Performance SLA
  - Health-Check Server option

To create meta fields:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Click *Create New*.
   The *Create New Meta Fields* pane is displayed.

3. In the *Object* box, select *Device VDOM*.



Edit Meta Fields

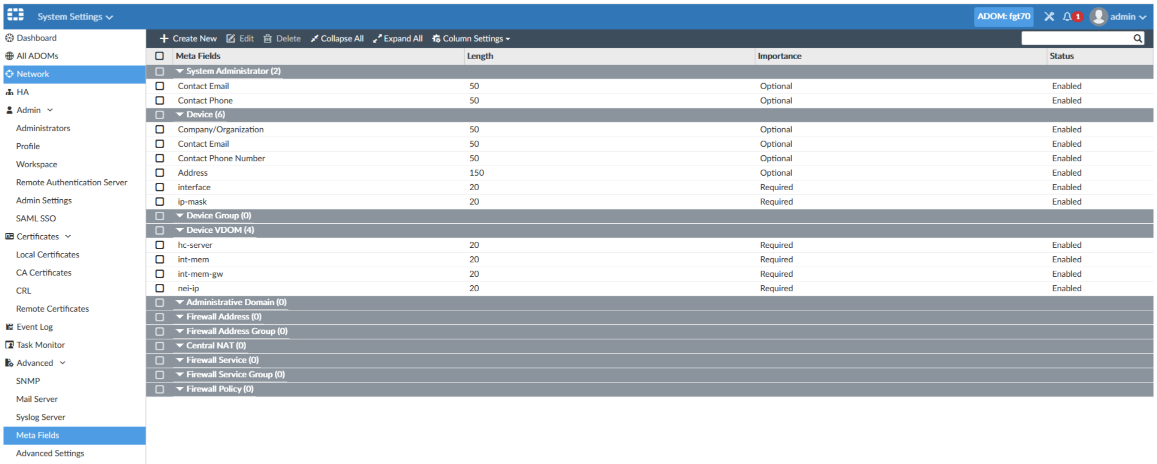
Object	Device VDOM
Name	nei-ip
Length	20
Importance	○ Optional ● Required
Status	○ Disabled ● Enabled
Variable	$(nei-ip)

Values

□	#	Device	Value

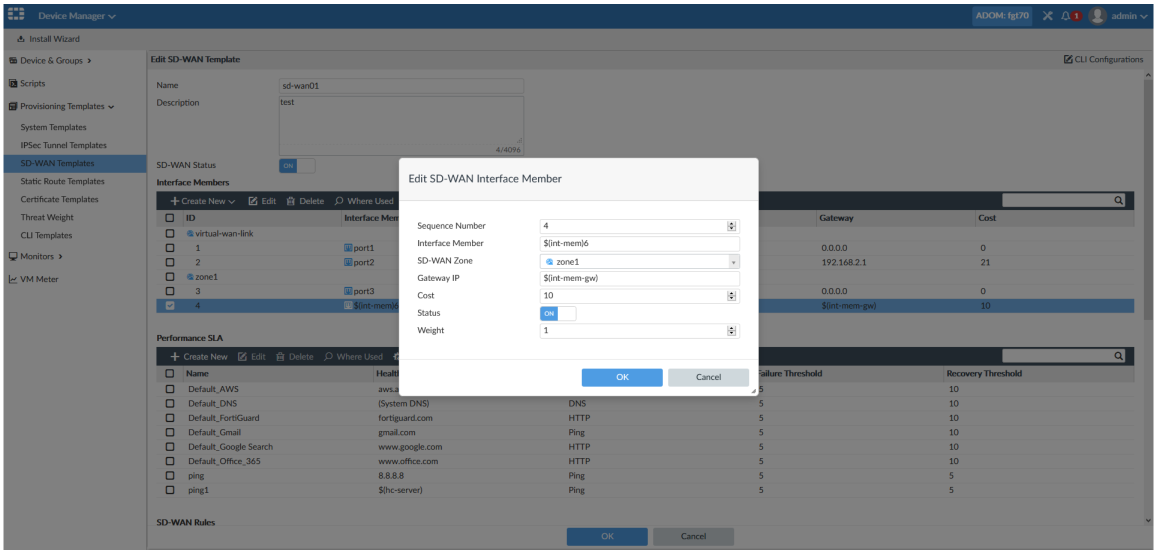
No record found.

4. In the *Name* box, type a name for the meta field.
   The name of the field becomes the variable name that you can use in SD-WAN templates.
5. In the *Values* area, click *Create New* to define a value for one or more devices.
6. Click *OK*.
   The meta field is created.



□	Meta Fields	Length	Importance	Status
□	System Administrator (2)			
□	Contact Email	50	Optional	Enabled
□	Contact Phone	50	Optional	Enabled
□	Device (6)			
□	Company/Organization	50	Optional	Enabled
□	Contact Email	50	Optional	Enabled
□	Contact Phone Number	50	Optional	Enabled
□	Address	150	Optional	Enabled
□	interface	20	Required	Enabled
□	ip-mask	20	Required	Enabled
□	Device Group (0)			
□	Device VDOM (4)			
□	hc-server	20	Required	Enabled
□	int-mem	20	Required	Enabled
□	int-mem-gw	20	Required	Enabled
□	nei-ip	20	Required	Enabled
□	Administrative Domain (0)			
□	Firewall Address (0)			
□	Firewall Address Group (0)			
□	Central NAT (0)			
□	Firewall Service (0)			
□	Firewall Service Group (0)			
□	Firewall Policy (0)			

In the following SD-WAN template example, meta fields are used for the following interface member options: *Interface Member* and *Gateway IP*:



Edit SD-WAN Template

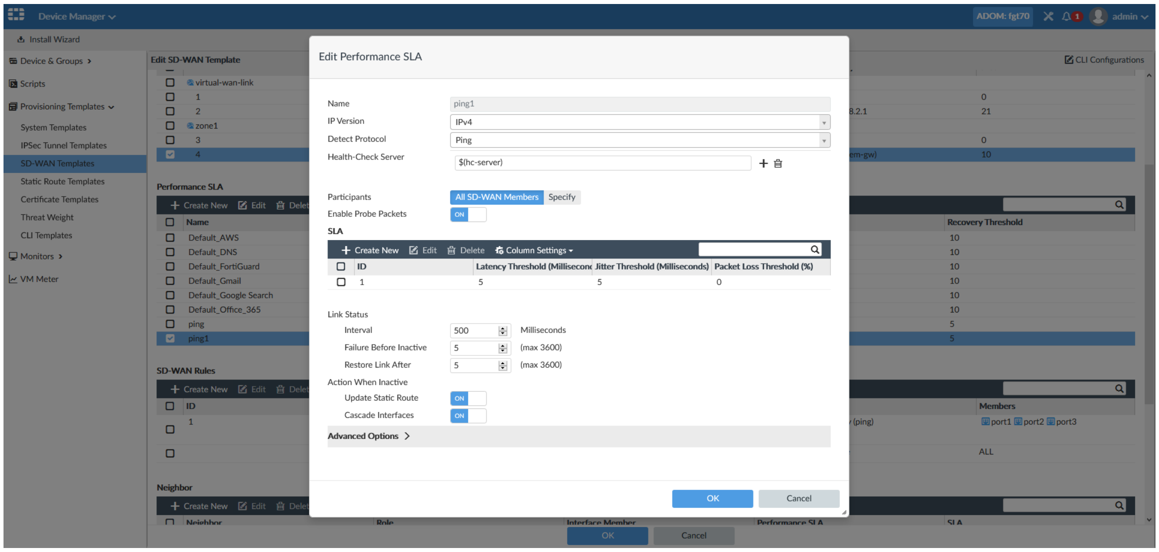
Name	sd-wan01
Description	test
SD-WAN Status	ON

Edit SD-WAN Interface Member

Sequence Number	4
Interface Member	$(int-mem)6
SD-WAN Zone	zone1
Gateway IP	$(int-mem-gw)
Cost	10
Status	ON
Weight	1

OK Cancel

In the following SD-WAN template example, a meta field is used for the *Health-Check Server* option in Performance SLA:



Edit Performance SLA

Name	ping1
IP Version	IPv4
Detect Protocol	Ping
Health-Check Server	$(hc-server)
Participants	All SD-WAN Members
Enable Probe Packets	ON

SLA

ID	Latency Threshold (Millisecond	Jitter Threshold (Milliseconds)	Packet Loss Threshold (%)
1	5	5	0

Link Status

Interval	500	Milliseconds
Failure Before Inactive	5	(max 3600)
Restore Link After	5	(max 3600)

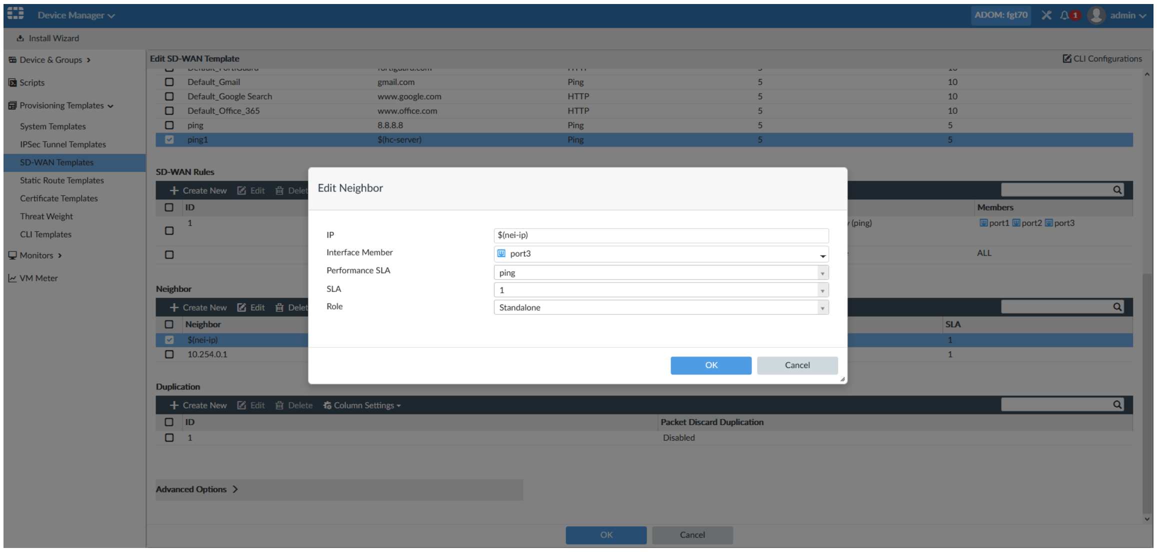
Action When Inactive

Update Static Route	ON
Cascade Interfaces	ON

Advanced Options

OK Cancel

In the following SD-WAN template example, a meta field is used for the *IP* option in Neighbor:



Edit SD-WAN Template

□	Default_Gmail	gmail.com	Ping	5	10
□	Default_Google Search	www.google.com	HTTP	5	10
□	Default_Office_365	www.office.com	HTTP	5	10
□	ping	8.8.8.8	Ping	5	5
☑	ping1	$(hc-server)	Ping	5	5

SD-WAN Rules

□	ID		Members
□	1	(ping)	port1 port2 port3
□			ALL

Neighbor

□	Neighbor	SLA
☑	$(nei-ip)	1
□	10.254.0.1	1

Duplication

□	ID	Packet Discard Duplication
□	1	Disabled

Edit Neighbor

IP	$(nei-ip)
Interface Member	port3
Performance SLA	ping
SLA	1
Role	Standalone

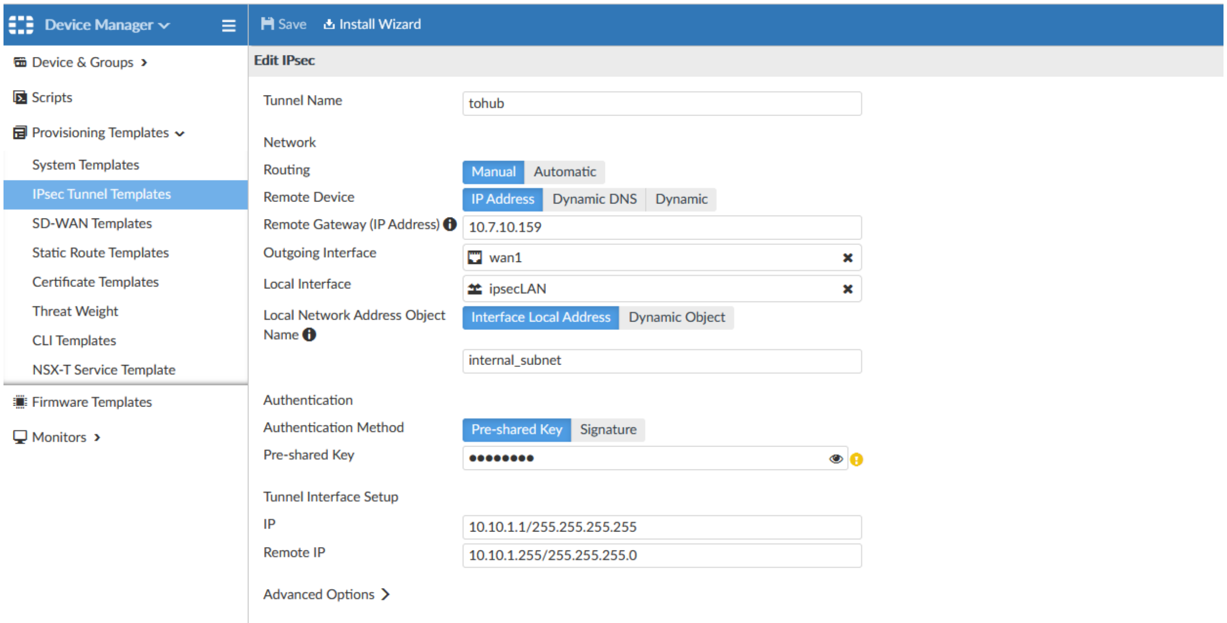
IPsec template enhanced support for tunnel interface configuration - FMG 7.0.1

IPSEC template enhanced support for tunnel interface configuration.

To configure an IPsec template:

1. Go to *Device Manager* > *Provisioning Template* > *IPsec Tunnel Templates*, and create or edit a template.
2. In the template, configure the IP address for an IPsec tunnel interface in Tunnel Interface Setup:
   - **IP**: Input the IP address, for example `10.10.1.1/32`. Meta fields are also supported, for example `10.10.$(side_id).1/32`.

- **Remote IP**: Input the IP address or meta field for the remote IP.



Edit IPsec

Tunnel Name: tohub

Network

Routing: [✓ Manual] Automatic

Remote Device: [✓ IP Address] Dynamic DNS Dynamic

Remote Gateway (IP Address): 10.7.10.159

Outgoing Interface: wan1

Local Interface: ipsecLAN

Local Network Address Object Name: [✓ Interface Local Address] Dynamic Object

internal_subnet

Authentication

Authentication Method: [✓ Pre-shared Key] Signature

Pre-shared Key: ••••••••

Tunnel Interface Setup

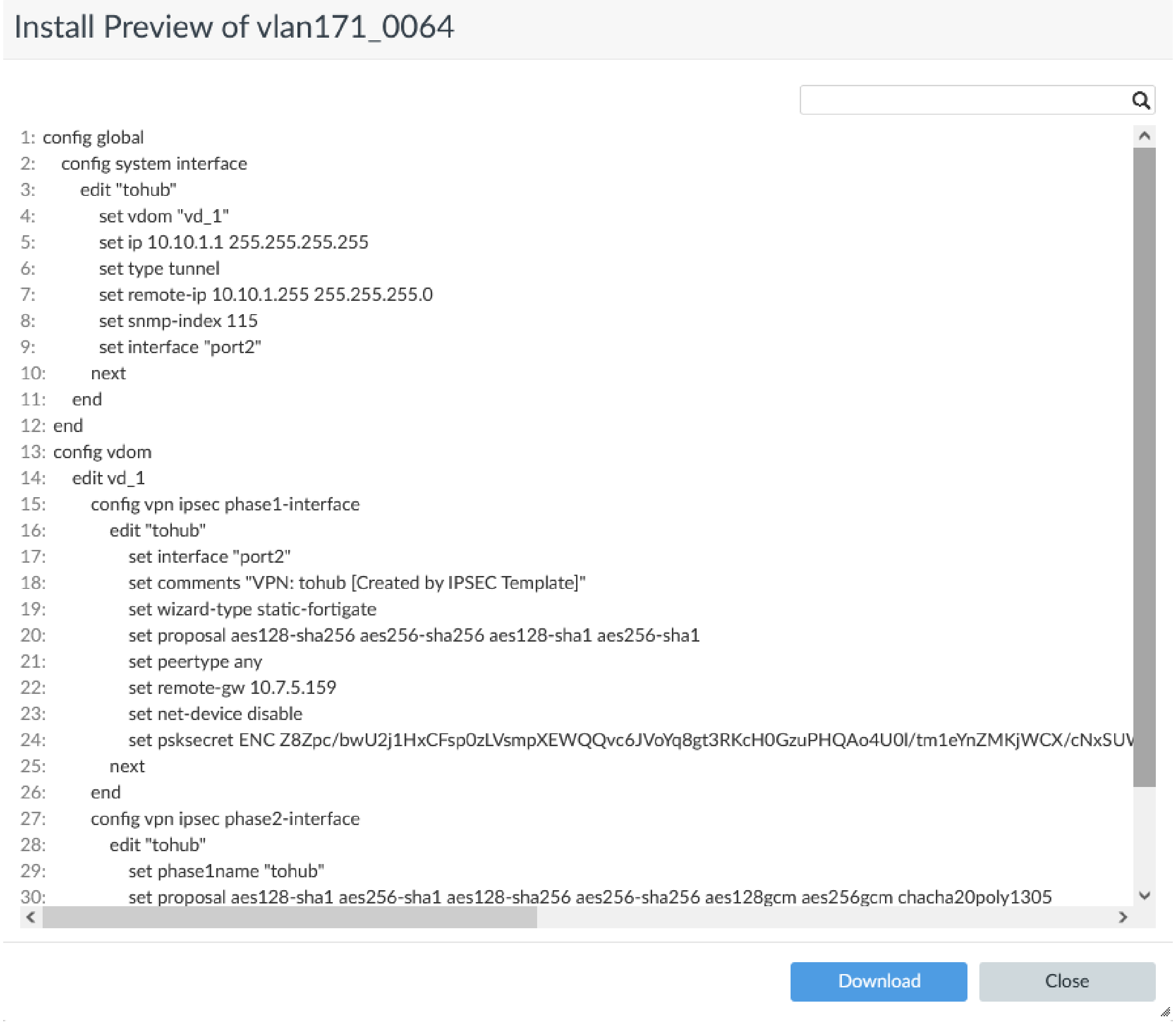
IP: 10.10.1.1/255.255.255.255

Remote IP: 10.10.1.255/255.255.255.0

Advanced Options >

3. Click *OK* to save the template.
4. Click *Install Wizard* at the top of the page to perform an installation.
   The *Install Preview* shows that FortiManager is pushing the IPsec VPN tunnel interface and its IP address to the

device.



Install Preview of vlan171_0064

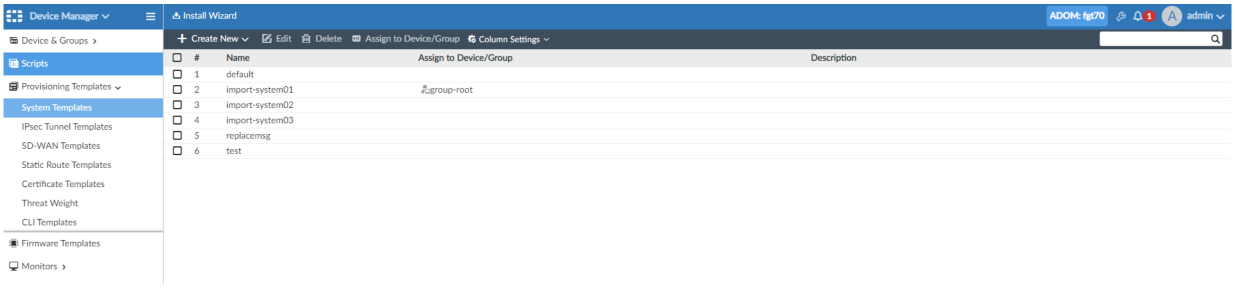
```
config global
    config system interface
        edit "tohub"
            set vdom "vd_1"
            set ip 10.10.1.1 255.255.255.255
            set type tunnel
            set remote-ip 10.10.1.255 255.255.255.0
            set snmp-index 115
            set interface "port2"
        next
    end
end
config vdom
    edit vd_1
        config vpn ipsec phase1-interface
            edit "tohub"
                set interface "port2"
                set comments "VPN: tohub [Created by IPSEC Template]"
                set wizard-type static-fortigate
                set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
                set peertype any
                set remote-gw 10.7.5.159
                set net-device disable
                set psksecret ENC Z8Zpc/bwU2j1HxCFsp0zLVsmpXEWQQvc6JVoYq8gt3RKcH0GzuPHQAo4U0I/tm1eYnZMKjWCX/cNxSUV
            next
        end
        config vpn ipsec phase2-interface
            edit "tohub"
                set phase1name "tohub"
                set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
```

Templates support assignment to device groups - FMG 7.0.1

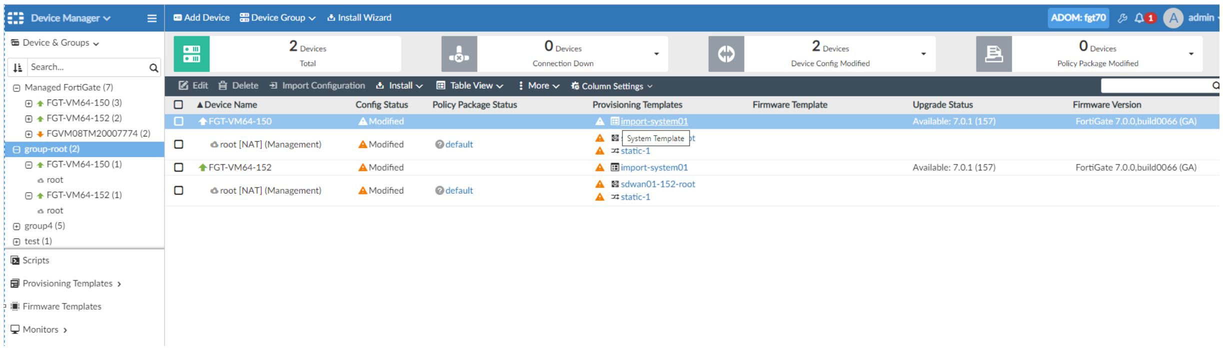
In FortiManager 7.0.1, templates support assignment to device groups.

To assign templates to a device group:

1. System Templates, SD-WAN Templates, Static Route Templates, and IPsec Templates can be assigned to a device or device group.



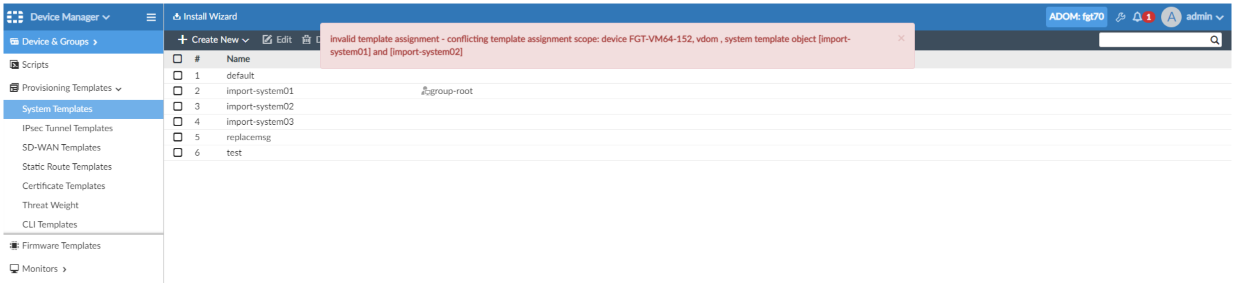
#	Name	Assign to Device/Group	Description
1	default		
2	import-system01	group-root	
3	import-system02		
4	import-system03		
5	replacemsg		
6	test		



2 Devices Total | 0 Devices Connection Down | 2 Devices Device Config Modified | 0 Devices Policy Package Modified

Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Template	Upgrade Status	Firmware Version
FGT-VM64-150	Modified		import-system01		Available: 7.0.1 (157)	FortiGate 7.0.0,build0066 (GA)
root [NAT] (Management)	Modified	default	System Template static-1			
FGT-VM64-152	Modified		import-system01		Available: 7.0.1 (157)	FortiGate 7.0.0,build0066 (GA)
root [NAT] (Management)	Modified	default	sdwan01-152-root static-1			

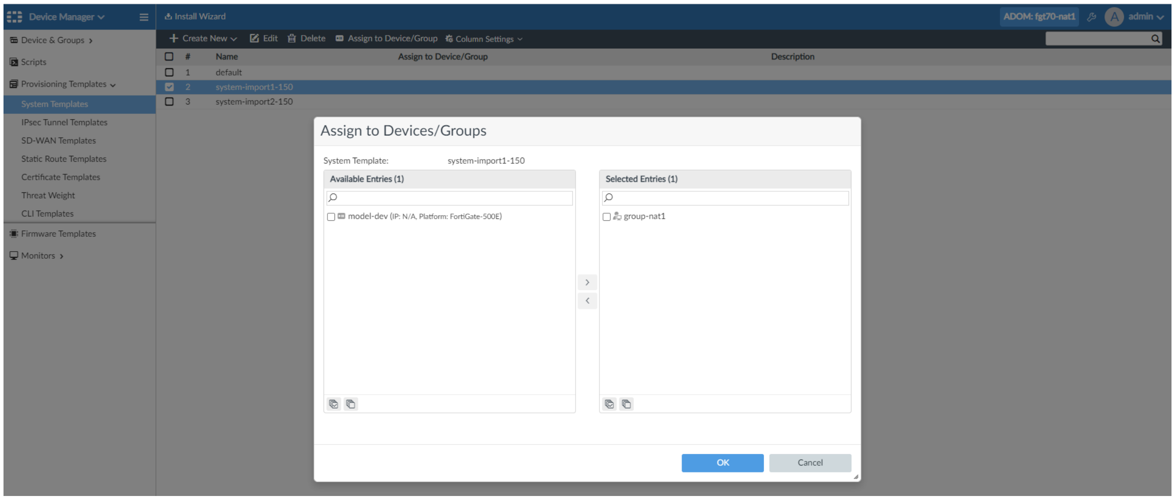
2. Device groups can only be assigned to one template, otherwise an error is reported indicating a conflict.



invalid template assignment - conflicting template assignment scope: device FGT-VM64-152, vdom , system template object [import-system01] and [import-system02]

#	Name	Assign to Device/Group
1	default	
2	import-system01	group-root
3	import-system02	
4	import-system03	
5	replacemsg	
6	test	

3. When assigning templates to device groups, the following applies:
   a. System Template:
      - For ADOMs with a management VDOM, templates can be assigned to the device group, then modified and installed.



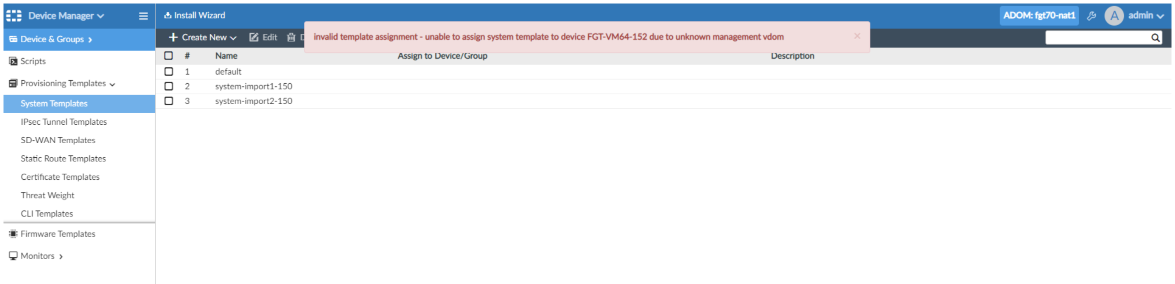
Assign to Devices/Groups

System Template: system-import1-150

Available Entries (1): model-dev (IP: N/A, Platform: FortiGate-500E)

Selected Entries (1): group-nat1

- For ADOMs with a non-management VDOM, the template cannot be assigned to the device group.

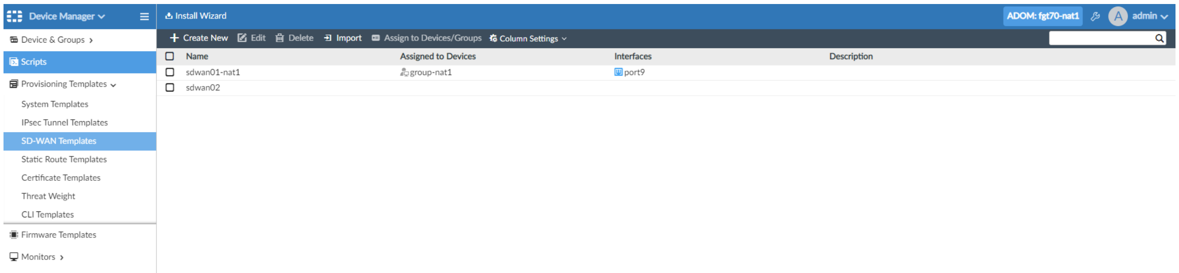


invalid template assignment - unable to assign system template to device FGT-VM64-152 due to unknown management vdom

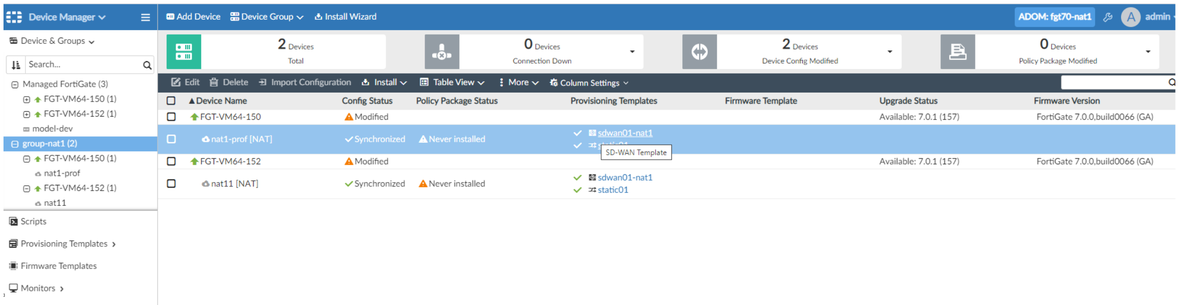
#	Name	Assign to Device/Group	Description
1	default		
2	system-import1-150		
3	system-import2-150		

b. SD-WAN Template and Static Route Templates:

- For ADOMs with a management or non-management VDOM, templates can be assigned to the device group, then modified and installed.



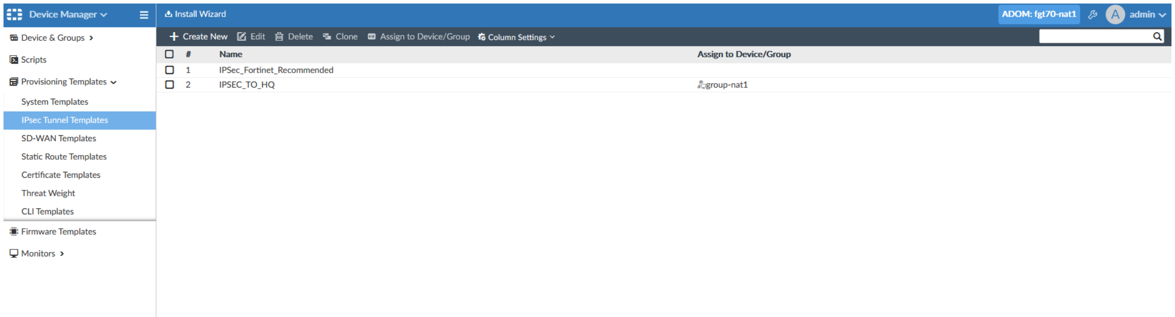
Name	Assigned to Devices	Interfaces	Description
sdwan01-nat1	group-nat1	port9	
sdwan02			



Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Template	Upgrade Status	Firmware Version
FGT-VM64-150	Modified				Available: 7.0.1 (157)	FortiGate 7.0.0,build0066 (GA)
nat1-prof [NAT]	Synchronized	Never installed	sdwan01-nat1			
FGT-VM64-152	Modified				Available: 7.0.1 (157)	FortiGate 7.0.0,build0066 (GA)
nat11 [NAT]	Synchronized	Never installed	sdwan01-nat1 static01			

c. IPsec Templates:

- IPsec Templates can be assigned to a device group. You can unassign an IPsec template from a device group member by going to *Device Manager* and editing the device group. When a deviceis removed from the device group, the IPsec Template will be unassigned from that device.



#	Name	Assign to Device/Group
1	IPSec_Fortinet_Recommended	
2	IPSEC_TO_HQ	group-nat1

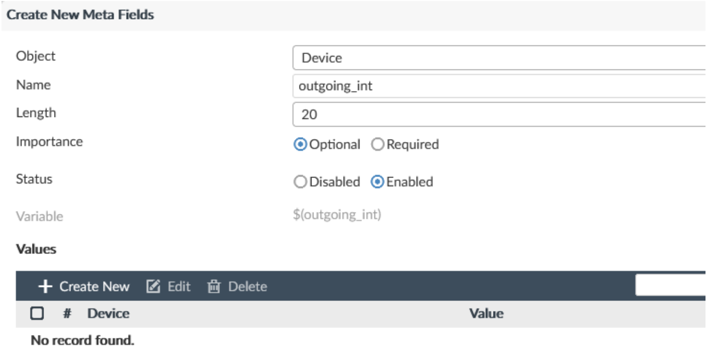
CLI Template improvements - FMG 7.0.1

In FortiManager 7.0.1, CLI templates include the following improvements:

- Jinja2 language support
- Validation check and preview
- Device and device-VDOM meta variables

To create an IPsec VPN using Jinja in the CLI Template:

1. Create a new meta field in FortiManager.
    a. Go to *System* > *Advanced* > *Meta Fields* and create a new meta field.
    b. Enter a name for the meta field, for example *outgoing_int*.
    c. Enter the meta field object. In this example, the *Object* can be *Device* or *DeviceVDOM*.
    d. Click *OK*.



Create New Meta Fields

Object: Device
Name: outgoing_int
Length: 20
Importance: ● Optional ○ Required
Status: ○ Disabled ● Enabled
Variable: $(outgoing_int)

Values

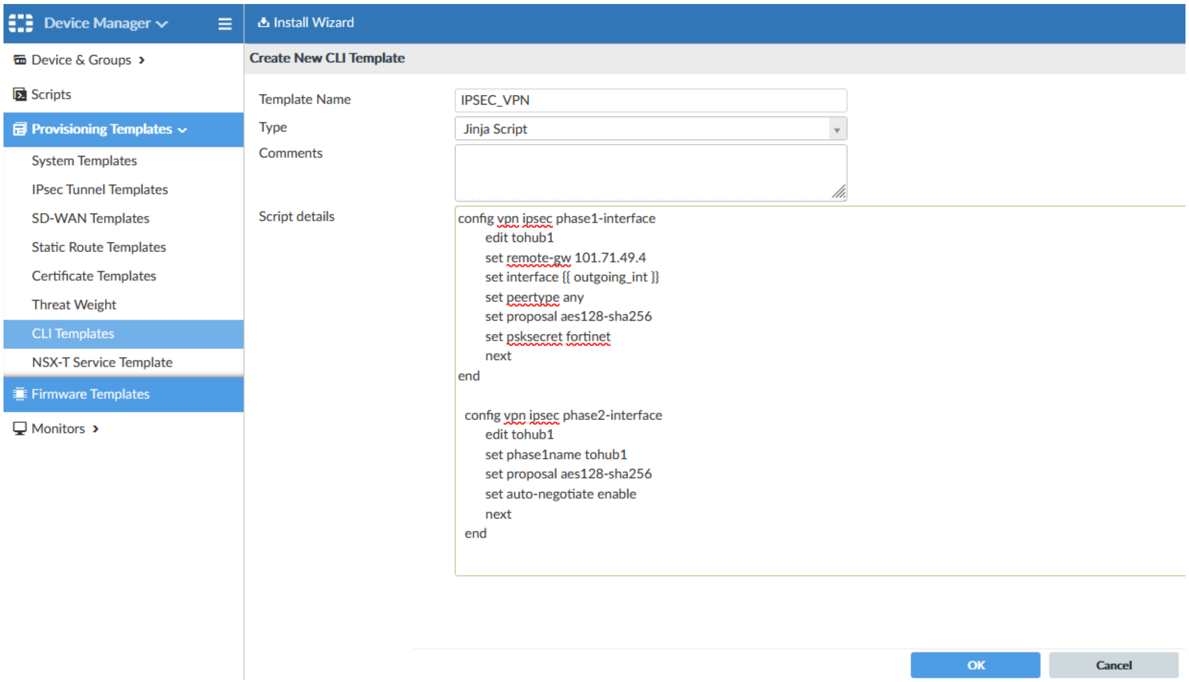
□	#	Device	Value

No record found.

2. Create the CLI Jinja Template:
    a. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*, and create a new *CLI Template*.
    b. Enter a name for the template, for example *IPSEC_VPN*.
    c. Select *Jinja Script* as the *Type*.
    d. Enter the *Script Details*. In this example, the following jinja script is used to create the IPsec phase1-interface and phase 2-interface. Jinja2 uses {{ ... }} for the expression of variables.

```
config vpn ipsec phase1-interface
   edit tohub1
      set remote-gw 101.71.49.4
      set interface {{ outgoing_int }}
      set peertype any
      set proposal aes128-sha256
      set psksecret fortinet
   next
end
config vpn ipsec phase2-interface
   edit tohub1
      set phase1name tohub1
      set proposal aes128-sha256
      set auto-negotiate enable
   next
end
```

e. Click *OK*.



Create New CLI Template

Template Name	IPSEC_VPN
Type	Jinja Script
Comments	

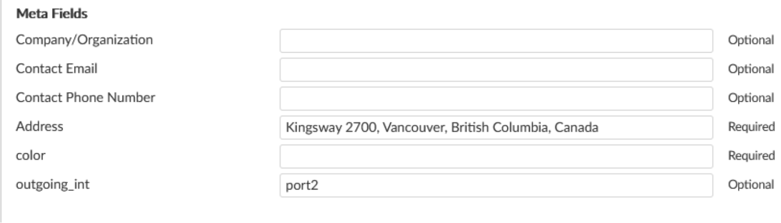
Script details

```
config vpn ipsec phase1-interface
    edit tohub1
    set remote-gw 101.71.49.4
    set interface {{ outgoing_int }}
    set peertype any
    set proposal aes128-sha256
    set psksecret fortinet
    next
end

 config vpn ipsec phase2-interface
    edit tohub1
    set phase1name tohub1
    set proposal aes128-sha256
    set auto-negotiate enable
    next
 end
```

3. Assign a port to the new meta field.

   a. Go to *Device Manager*and edit your device.

   b. In the previously created meta field, enter a port. In this example, *port2* is assigned to the *outgoing_int* field.



Meta Fields

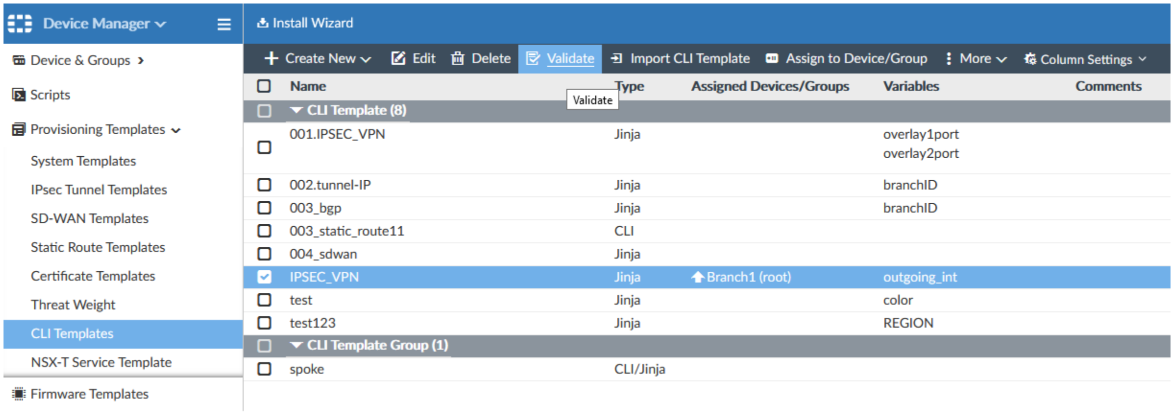
Company/Organization		Optional
Contact Email		Optional
Contact Phone Number		Optional
Address	Kingsway 2700, Vancouver, British Columbia, Canada	Required
color		Required
outgoing_int	port2	Optional

4. Assign the CLI Jinja template to a device and execute device installation. The following configuration is pushed to the FortiManager.

```
config vpn ipsec phase1-interface
   edit tohub1
      set remote-gw 101.71.49.4
      set interface port2
      set peertype any
      set proposal aes128-sha256
      set psksecret ENC
           Z8Zpc61yyxOe2K5QsJbYr7gRiykPe0EjU+e+TLSz12BucSSA6DfXPd23wnhkb560RSK92hqBpFH
           tC3/g1fopSKt80jn1G+I/0YMlNty6aoiyrDx5duo0g5cL4rB7UuT8TmmyeCDeUVy5wyT4afglm5
           P9Q8IzkY2P3D5/FG5DIuYHMZZg
   next
end
config vpn ipsec phase2-interface
   edit tohub1
      set phase1name tohub1
      set proposal aes128-sha256
      set auto-negotiate enable
   next
end
```

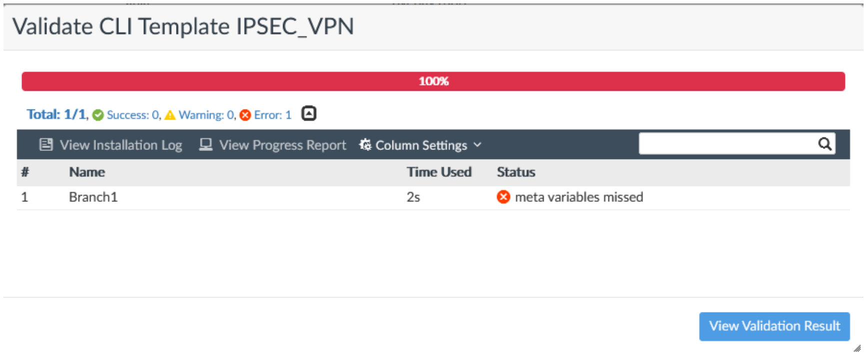
To validate a CLI Template:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Once the template is assigned to a device, click *Validate*.



	Name	Type	Assigned Devices/Groups	Variables	Comments
□	▾ CLI Template (8)				
□	001.IPSEC_VPN	Jinja		overlay1port overlay2port	
□	002.tunnel-IP	Jinja		branchID	
□	003_bgp	Jinja		branchID	
□	003_static_route11	CLI			
□	004_sdwan	Jinja			
☑	IPSEC_VPN	Jinja	Branch1 (root)	outgoing_int	
□	test	Jinja		color	
□	test123	Jinja		REGION	
□	▾ CLI Template Group (1)				
□	spoke	CLI/Jinja			

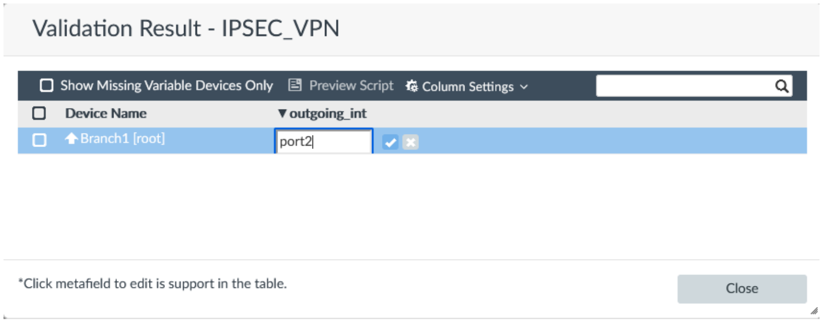
If there are any errors, for example missing values for meta fields, you can click *View Validation Result*.


Validate CLI Template IPSEC_VPN

Total: 1/1, Success: 0, Warning: 0, Error: 1

#	Name	Time Used	Status
1	Branch1	2s	meta variables missed

You will have the opportunity to input the value for the missing meta fields in the dialog box.

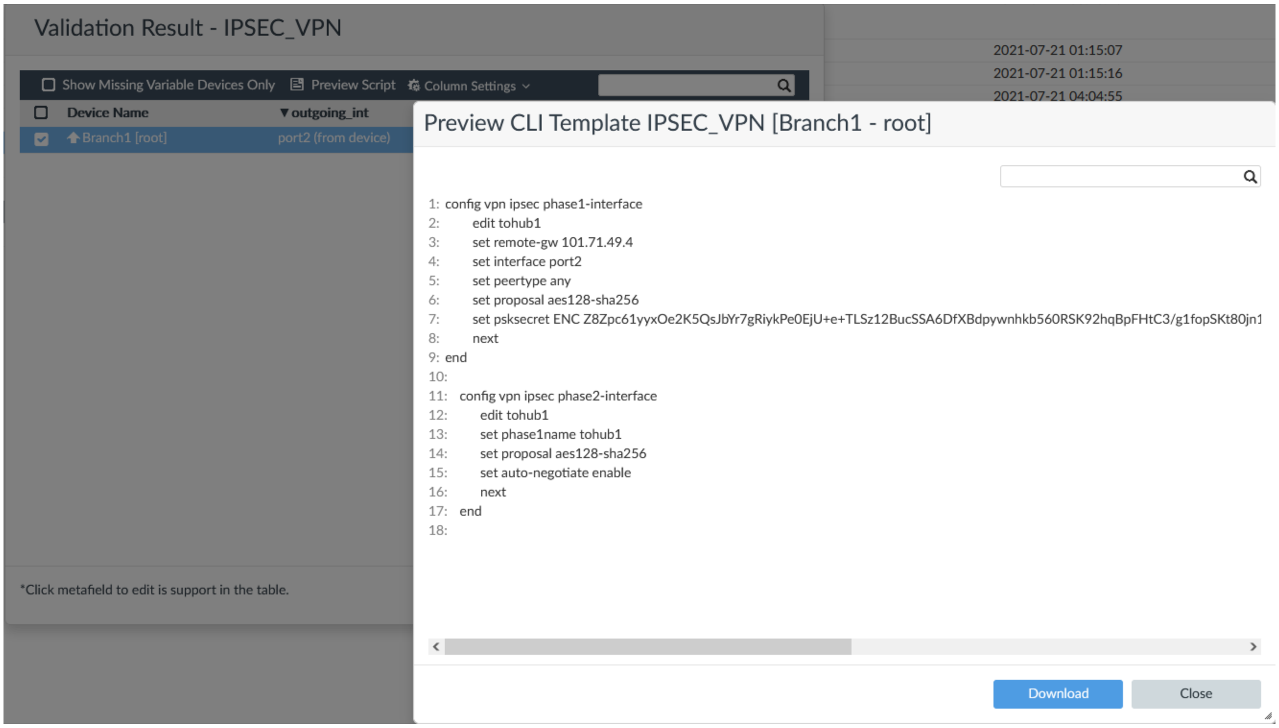

Validation Result - IPSEC_VPN

□	Device Name	outgoing_int
□	Branch1 [root]	port2

*Click metafield to edit is support in the table.

To preview a CLI Template script:

1. Go to *Device Manager* > *Provisioning Templates* > *CLI Template*.
2. Once the template is assigned, click *Validate*.
3. Click *View Validation Result* when the script validation is completed, and then click *Preview Result*.
   The CLI Template is replaced with the value or values seen by the end user. For example, in the example below the variable *{{outgoing_int}}* is replaced by *port2* in the script.



Validation Result - IPSEC_VPN

☐ Device Name	outgoing_int
☑ Branch1 [root]	port2 (from device)

2021-07-21 01:15:07
2021-07-21 01:15:16
2021-07-21 04:04:55

*Click metafield to edit is support in the table.

Preview CLI Template IPSEC_VPN [Branch1 - root]

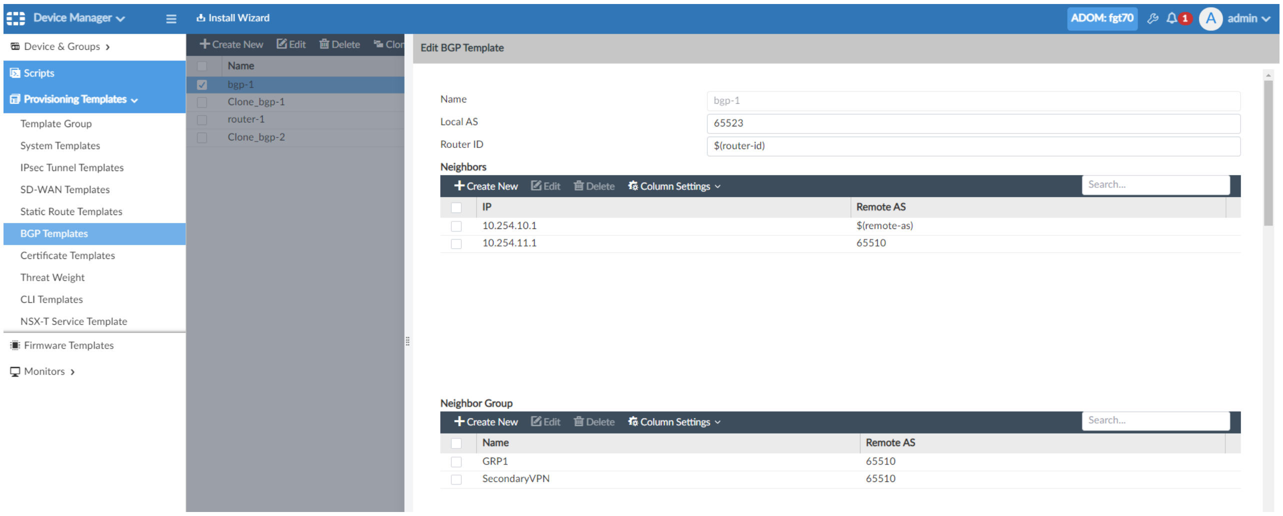
```
config vpn ipsec phase1-interface
      edit tohub1
      set remote-gw 101.71.49.4
      set interface port2
      set peertype any
      set proposal aes128-sha256
      set psksecret ENC Z8Zpc61yyxOe2K5QsJbYr7gRiykPe0EjU+e+TLSz12BucSSA6DfXBdpywnhkb560RSK92hqBpFHtC3/g1fopSKt80jn1
      next
end

   config vpn ipsec phase2-interface
       edit tohub1
       set phase1name tohub1
       set proposal aes128-sha256
       set auto-negotiate enable
       next
   end

```

BGP template to manage all BGP routing configurations - FMG 7.0.2

FortiManager 7.0.2 includes a BGP template to manage all the BGP routing configurations.

To create a BGP template:

1. Go to *Device Manager > Provisioning Templates > BGP Templates*, and click *Create New*. The *Create BGP Template* wizard opens.



☐	Name
☑	bgp-1
☐	Clone_bgp-1
☐	router-1
☐	Clone_bgp-2

Edit BGP Template

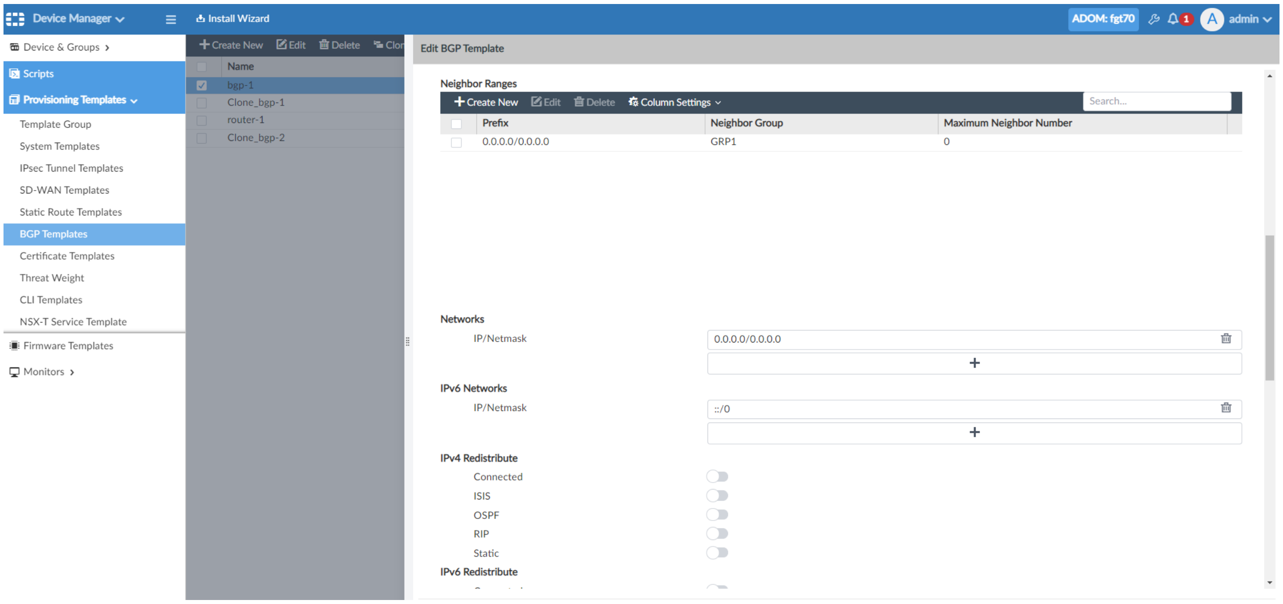
Name	bgp-1
Local AS	65523
Router ID	$(router-id)

Neighbors

☐	IP	Remote AS
☐	10.254.10.1	$(remote-as)
☐	10.254.11.1	65510

Neighbor Group

☐	Name	Remote AS
☐	GRP1	65510
☐	SecondaryVPN	65510



Name
bgp-1
Clone_bgp-1
router-1
Clone_bgp-2

Edit BGP Template

Neighbor Ranges

Prefix	Neighbor Group	Maximum Neighbor Number
0.0.0.0/0.0.0.0	GRP1	0

Networks

IP/Netmask 0.0.0.0/0.0.0.0

IPv6 Networks

IP/Netmask ::/0

IPv4 Redistribute

Connected

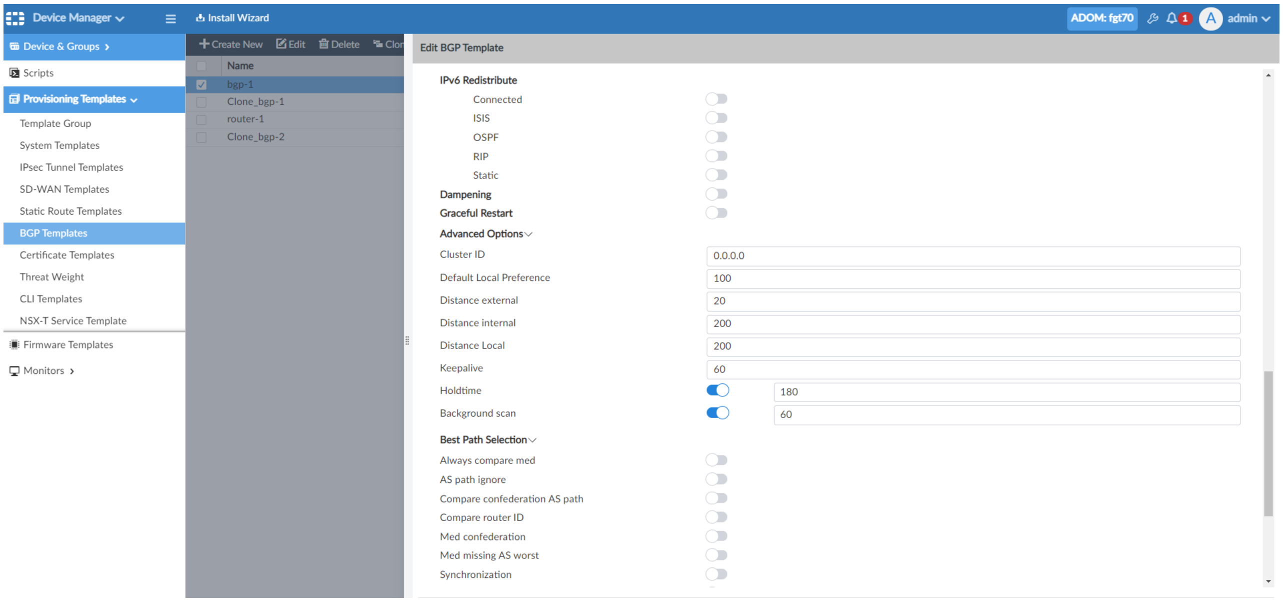
ISIS

OSPF

RIP

Static

IPv6 Redistribute



Name
bgp-1
Clone_bgp-1
router-1
Clone_bgp-2

Edit BGP Template

IPv6 Redistribute

Connected

ISIS

OSPF

RIP

Static

Dampening

Graceful Restart

Advanced Options

Cluster ID	0.0.0.0
Default Local Preference	100
Distance external	20
Distance internal	200
Distance Local	200
Keepalive	60
Holdtime	180
Background scan	60

Best Path Selection

Always compare med

AS path ignore

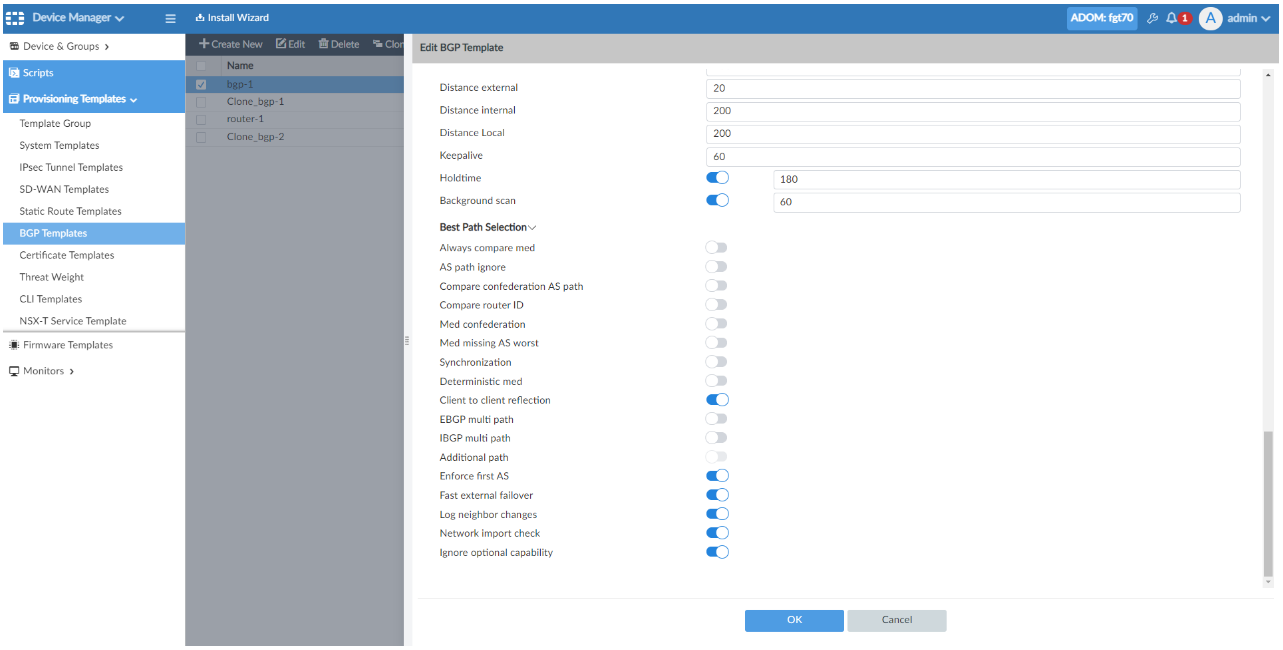
Compare confederation AS path

Compare router ID

Med confederation

Med missing AS worst

Synchronization



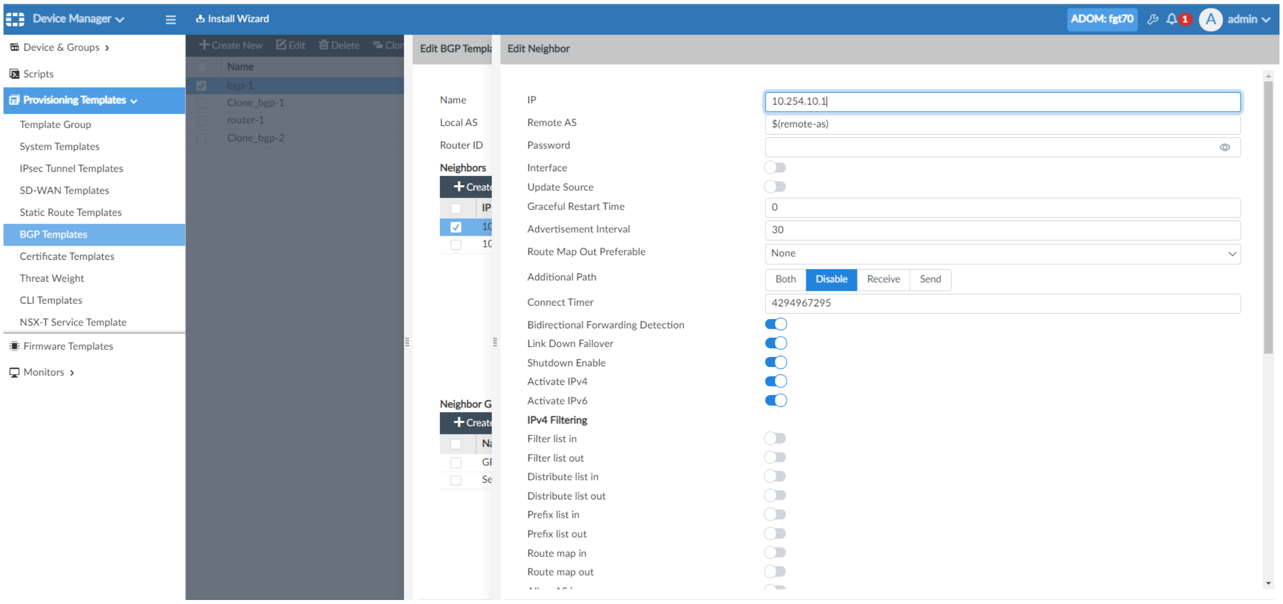
Edit BGP Template

Distance external	20	
Distance internal	200	
Distance Local	200	
Keepalive	60	
Holdtime	●	180
Background scan	●	60

Best Path Selection

Always compare med	○
AS path ignore	○
Compare confederation AS path	○
Compare router ID	○
Med confederation	○
Med missing AS worst	○
Synchronization	○
Deterministic med	○
Client to client reflection	●
EBGP multi path	○
IBGP multi path	○
Additional path	○
Enforce first AS	●
Fast external failover	●
Log neighbor changes	●
Network import check	●
Ignore optional capability	●

2. Add a Neighbor.

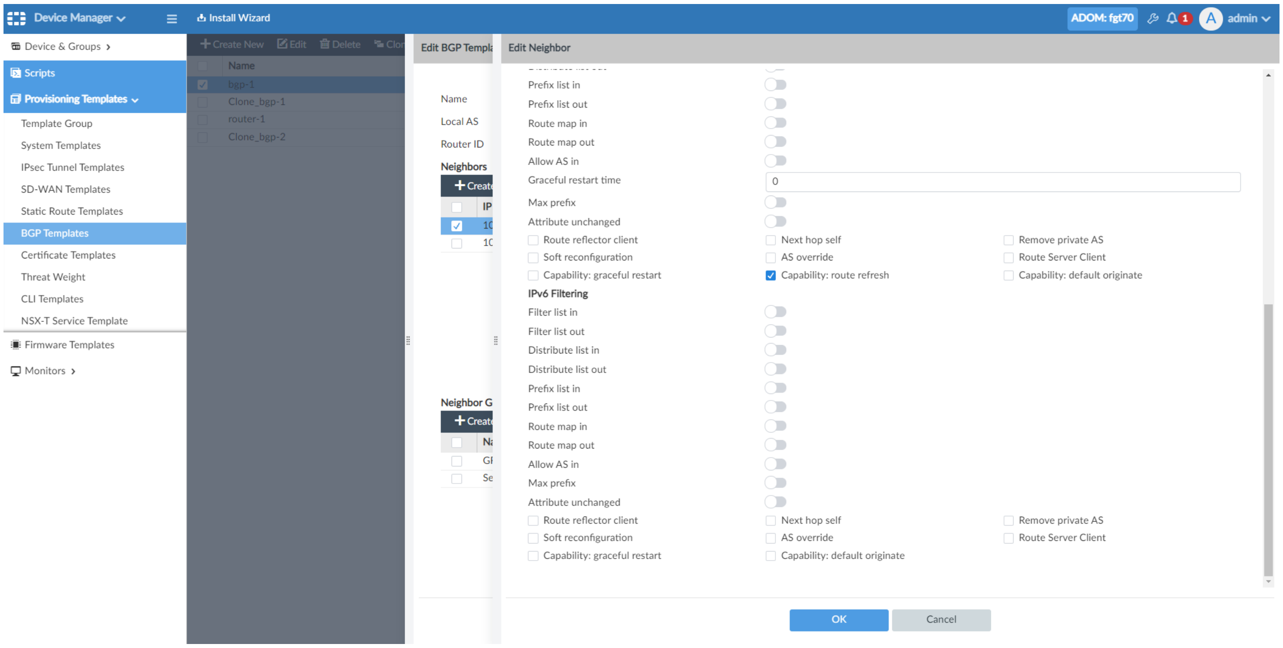


Edit Neighbor

- IP: 10.254.10.1
- Remote AS: $(remote-as)
- Password:
- Interface: off
- Update Source: off
- Graceful Restart Time: 0
- Advertisement Interval: 30
- Route Map Out Preferable: None
- Additional Path: Both [✓ Disable] Receive Send
- Connect Timer: 4294967295
- Bidirectional Forwarding Detection: on
- Link Down Failover: on
- Shutdown Enable: on
- Activate IPv4: on
- Activate IPv6: on

IPv4 Filtering

- Filter list in: off
- Filter list out: off
- Distribute list in: off
- Distribute list out: off
- Prefix list in: off
- Prefix list out: off
- Route map in: off
- Route map out: off



- Prefix list in: off
- Prefix list out: off
- Route map in: off
- Route map out: off
- Allow AS in: off
- Graceful restart time: 0
- Max prefix: off
- Attribute unchanged: off

□ Route reflector client □ Next hop self □ Remove private AS
□ Soft reconfiguration □ AS override □ Route Server Client
□ Capability: graceful restart ☑ Capability: route refresh □ Capability: default originate

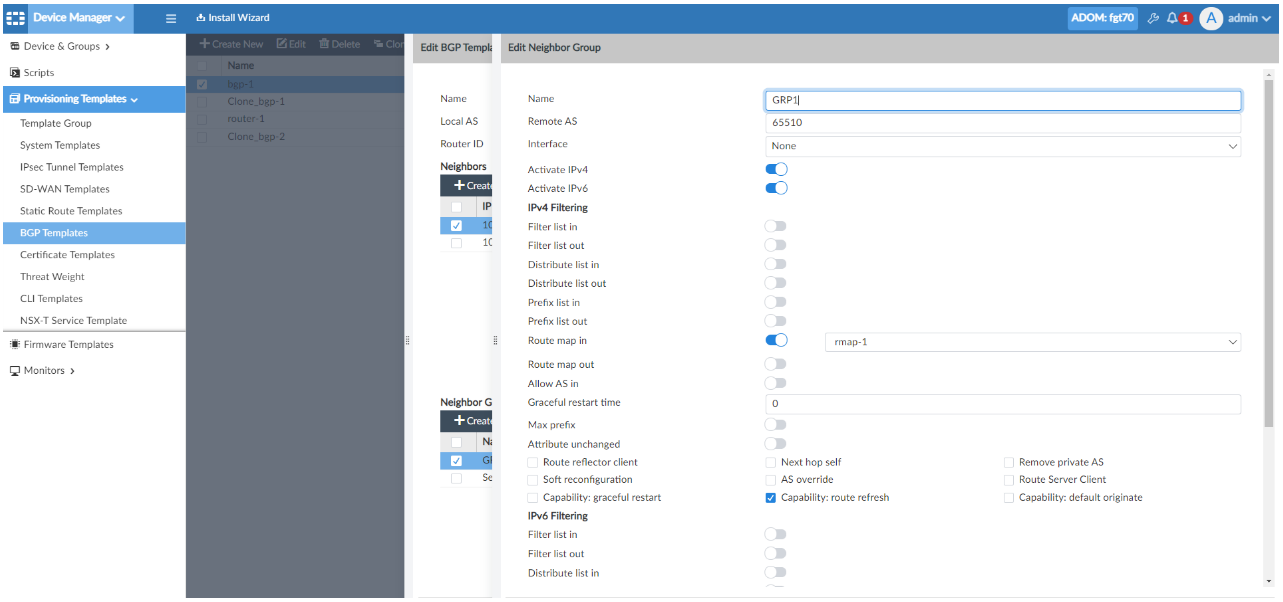
IPv6 Filtering

- Filter list in: off
- Filter list out: off
- Distribute list in: off
- Distribute list out: off
- Prefix list in: off
- Prefix list out: off
- Route map in: off
- Route map out: off
- Allow AS in: off
- Max prefix: off
- Attribute unchanged: off

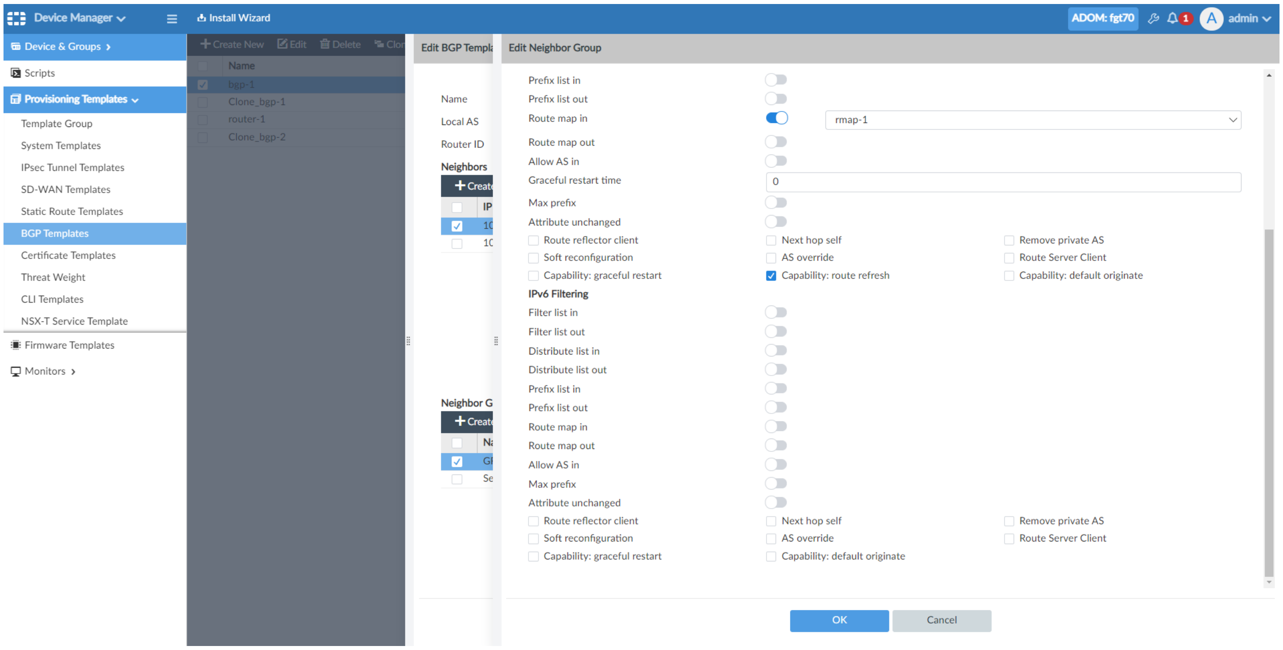
□ Route reflector client □ Next hop self □ Remove private AS
□ Soft reconfiguration □ AS override □ Route Server Client
□ Capability: graceful restart □ Capability: default originate

OK Cancel

3. Add a Neighbor Group.

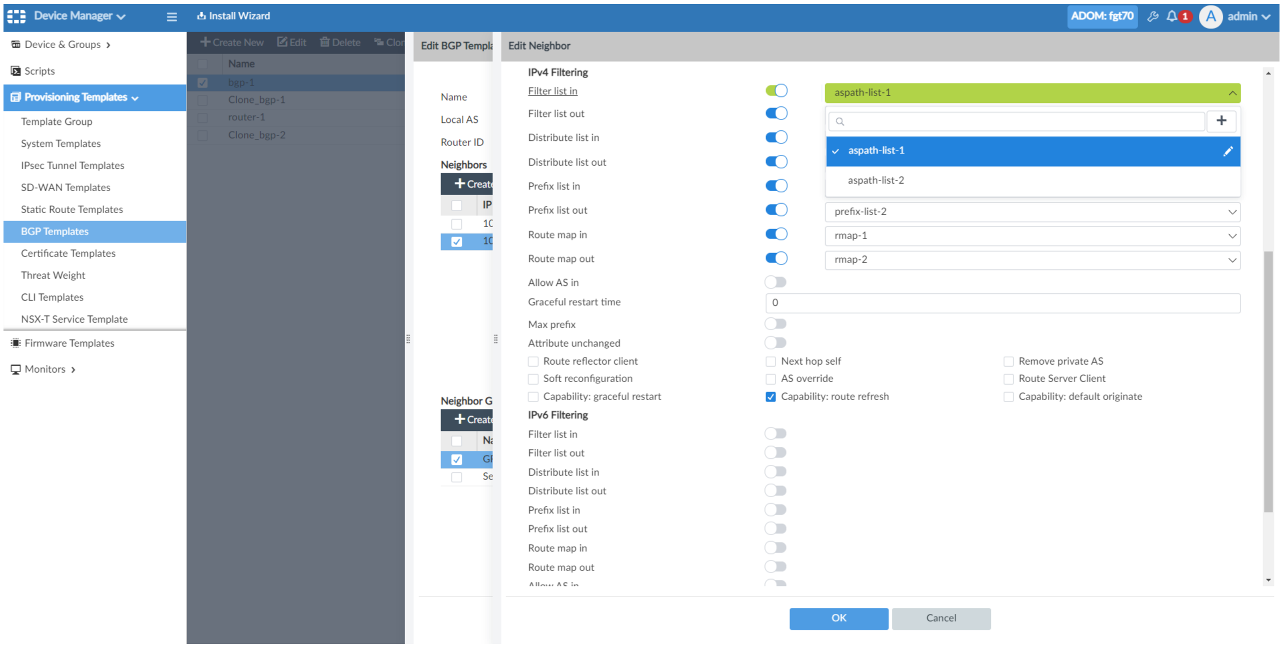


Name	GRP1		
Remote AS	65510		
Interface	None		
Activate IPv4	●		
Activate IPv6	●		
IPv4 Filtering			
Filter list in	○		
Filter list out	○		
Distribute list in	○		
Distribute list out	○		
Prefix list in	○		
Prefix list out	○		
Route map in	●	rmap-1	
Route map out	○		
Allow AS in	○		
Graceful restart time	0		
Max prefix	○		
Attribute unchanged	○		
□ Route reflector client	□ Next hop self	□ Remove private AS	
□ Soft reconfiguration	□ AS override	□ Route Server Client	
□ Capability: graceful restart	☑ Capability: route refresh	□ Capability: default originate	
IPv6 Filtering			
Filter list in	○		
Filter list out	○		
Distribute list in	○		



Prefix list in	○		
Prefix list out	○		
Route map in	●	rmap-1	
Route map out	○		
Allow AS in	○		
Graceful restart time	0		
Max prefix	○		
Attribute unchanged	○		
□ Route reflector client	□ Next hop self	□ Remove private AS	
□ Soft reconfiguration	□ AS override	□ Route Server Client	
□ Capability: graceful restart	☑ Capability: route refresh	□ Capability: default originate	
IPv6 Filtering			
Filter list in	○		
Filter list out	○		
Distribute list in	○		
Distribute list out	○		
Prefix list in	○		
Prefix list out	○		
Route map in	○		
Route map out	○		
Allow AS in	○		
Max prefix	○		
Attribute unchanged	○		
□ Route reflector client	□ Next hop self	□ Remove private AS	
□ Soft reconfiguration	□ AS override	□ Route Server Client	
□ Capability: graceful restart	□ Capability: default originate		

4. Create or edit a neighbor or neighbor group to create new routing objects. The following routing objects are available: Route Map, Access List, IPv6 Access List, Prefix List, IPv6 Prefix List, AS Path List, and Community List.



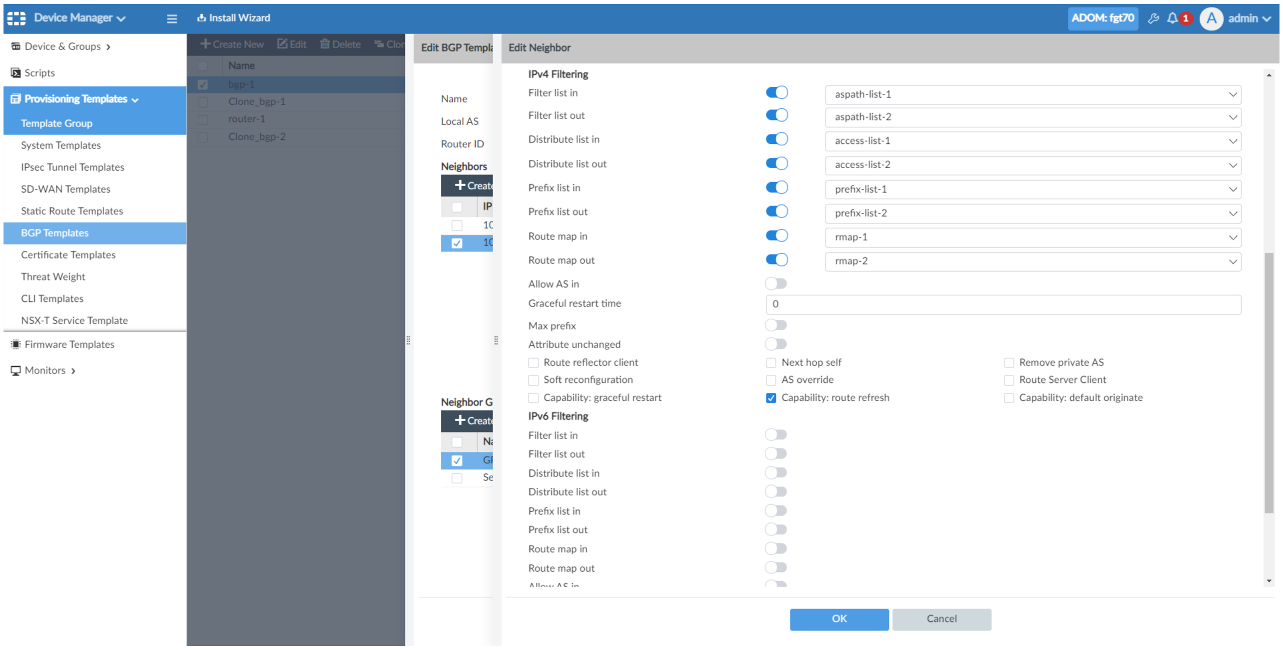
IPv4 Filtering

Filter list in	●	aspath-list-1
		✓ aspath-list-1 aspath-list-2
Filter list out	●	
Distribute list in	●	
Distribute list out	●	
Prefix list in	●	
Prefix list out	●	prefix-list-2
Route map in	●	rmap-1
Route map out	●	rmap-2
Allow AS in	○	
Graceful restart time		0
Max prefix	○	
Attribute unchanged	○	

☐ Route reflector client ☐ Next hop self ☐ Remove private AS
☐ Soft reconfiguration ☐ AS override ☐ Route Server Client
☐ Capability: graceful restart ☑ Capability: route refresh ☐ Capability: default originate

IPv6 Filtering

Filter list in	○
Filter list out	○
Distribute list in	○
Distribute list out	○
Prefix list in	○
Prefix list out	○
Route map in	○
Route map out	○



IPv4 Filtering

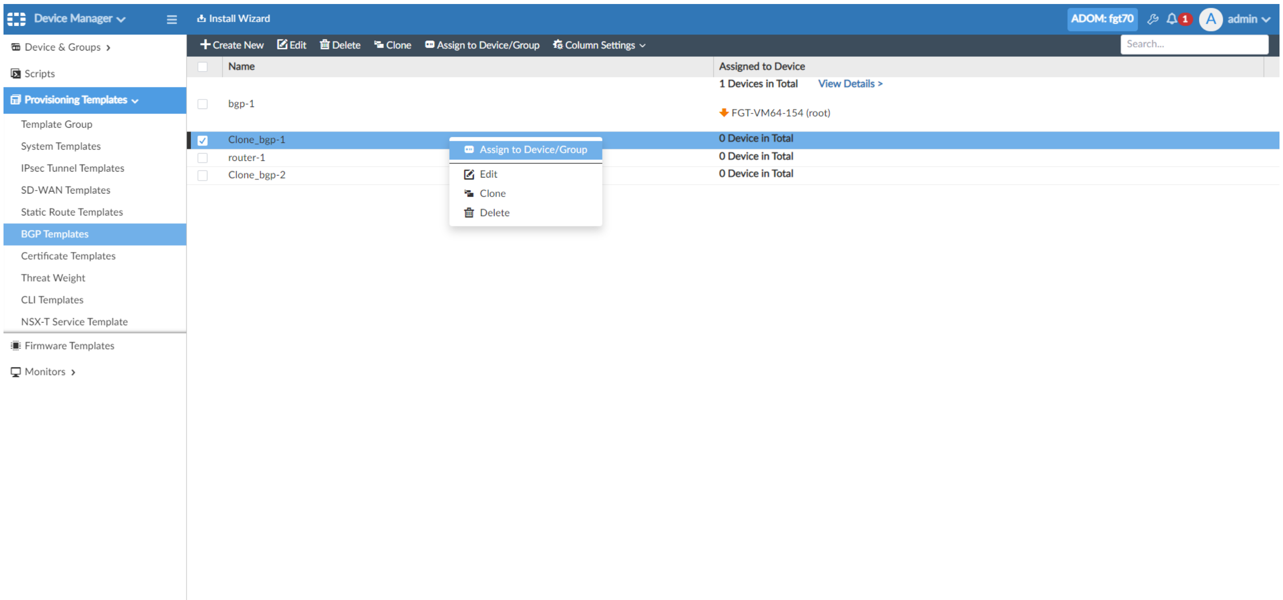
Filter list in	●	aspath-list-1
Filter list out	●	aspath-list-2
Distribute list in	●	access-list-1
Distribute list out	●	access-list-2
Prefix list in	●	prefix-list-1
Prefix list out	●	prefix-list-2
Route map in	●	rmap-1
Route map out	●	rmap-2
Allow AS in	○	
Graceful restart time		0
Max prefix	○	
Attribute unchanged	○	

☐ Route reflector client ☐ Next hop self ☐ Remove private AS
☐ Soft reconfiguration ☐ AS override ☐ Route Server Client
☐ Capability: graceful restart ☑ Capability: route refresh ☐ Capability: default originate

IPv6 Filtering

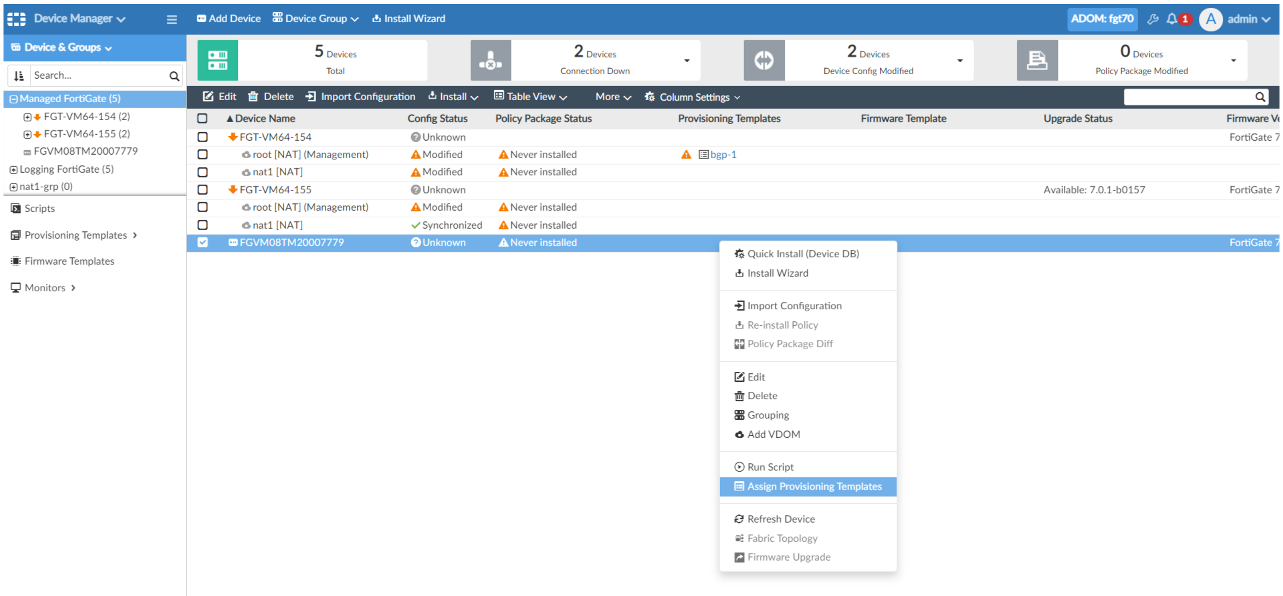
Filter list in	○
Filter list out	○
Distribute list in	○
Distribute list out	○
Prefix list in	○
Prefix list out	○
Route map in	○
Route map out	○

5. Click *OK* to save the BGP template.
6. In the BGP Templates pane, right-click a template and click *Assign to Device/Group* to assign the template to a device or device group.

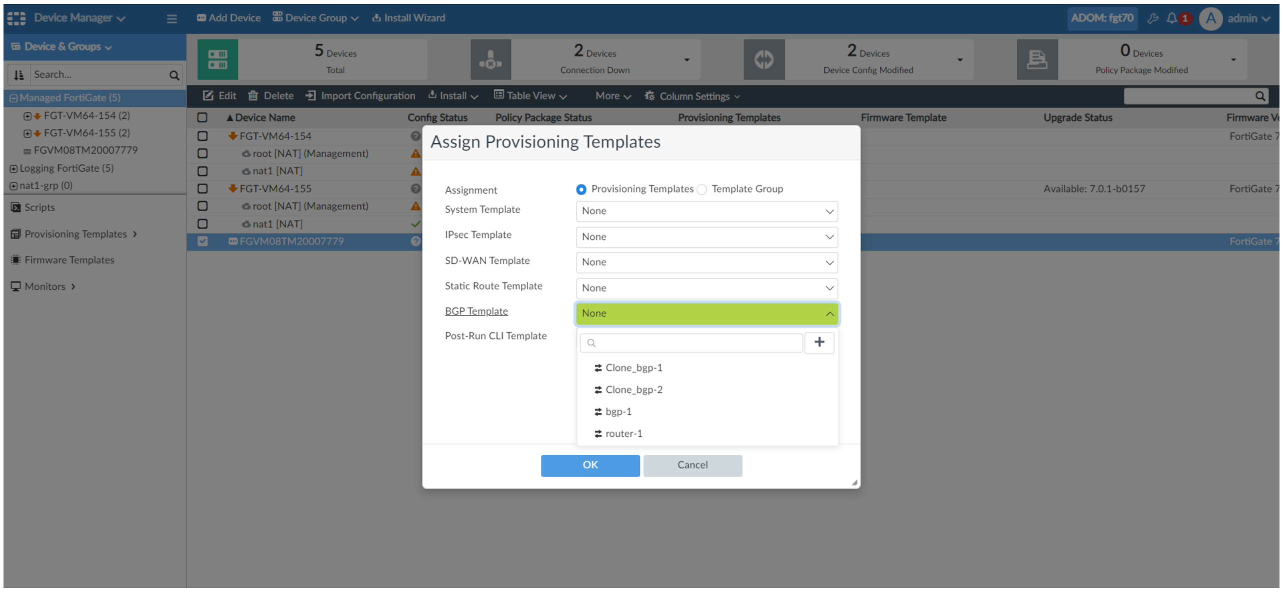


☐	Name	Assigned to Device
☐	bgp-1	1 Devices in Total View Details > FGT-VM64-154 (root)
☑	Clone_bgp-1	0 Device in Total
☐	router-1	0 Device in Total
☐	Clone_bgp-2	0 Device in Total

You can also right-click on the device in *Device Manager* and click *Assign Provisioning Templates* to assign the BGP template to that device.



☐	▲Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Template	Upgrade Status	Firmware Ve
☐	FGT-VM64-154	Unknown					FortiGate 7
☐	root [NAT] (Management)	Modified	Never installed	bgp-1			
☐	nat1 [NAT]	Modified	Never installed				
☐	FGT-VM64-155	Unknown				Available: 7.0.1-b0157	FortiGate 7
☐	root [NAT] (Management)	Modified	Never installed				
☐	nat1 [NAT]	✓Synchronized	Never installed				
☑	FGVM08TM20007779	Unknown	Never installed				FortiGate 7



Assign Provisioning Templates

Assignment ● Provisioning Templates ○ Template Group

System Template: None

IPsec Template: None

SD-WAN Template: None

Static Route Template: None

BGP Template: None

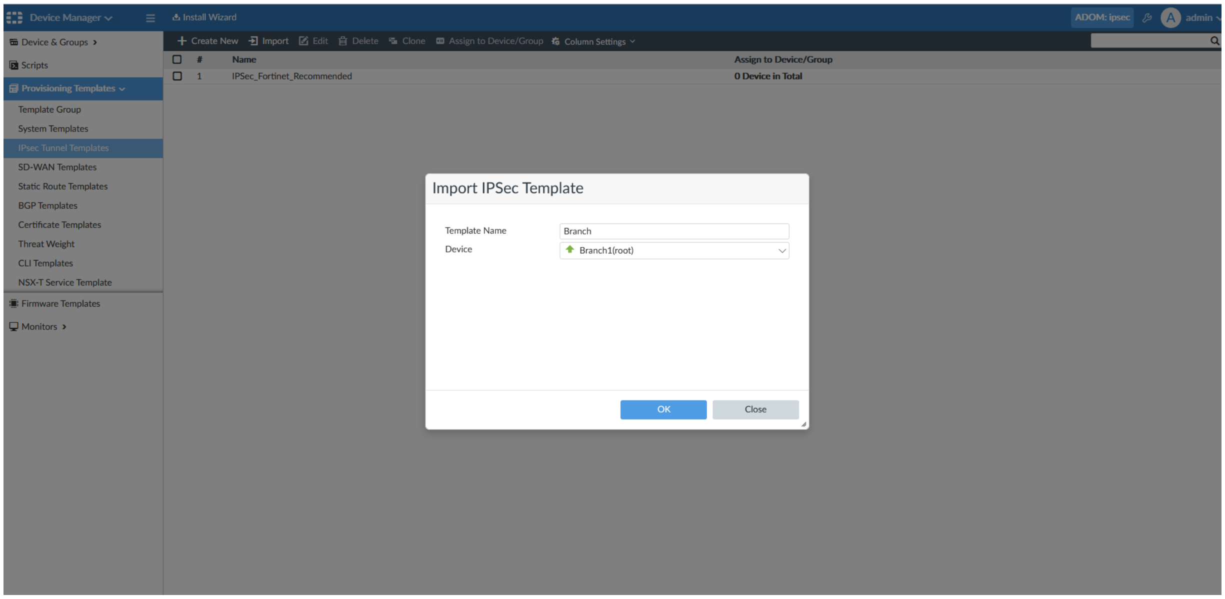
Post-Run CLI Template

Import IPSec VPN configuration from a managed FortiGate into a IPSec template - FMG 7.0.2

Import IPSec VPN configuration from a managed FortiGate into a IPSec Template.

To import an IPSec VPN config:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*, and click *Import* in the toolbar.
2. Enter a name for the template, and select a device from which to import the template.
3. Click *OK* to import.



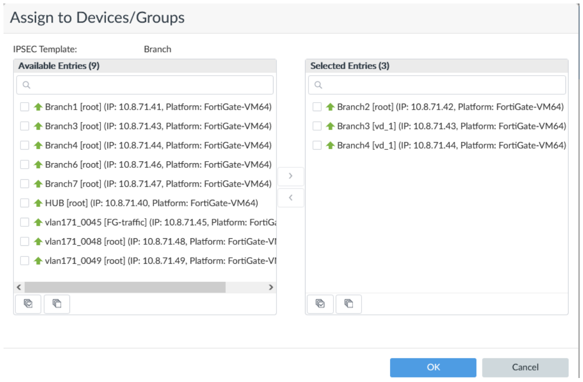
#	Name	Assign to Device/Group
1	IPSec_Fortinet_Recommended	0 Device in Total

Import IPSec Template

Template Name: Branch

Device: Branch1(root)

4. Assign the template to devices.
   In this example, the template is assigned to devices: *Branch2*, *Branch3*, and *Branch4*.



Assign to Devices/Groups

IPSEC Template: Branch

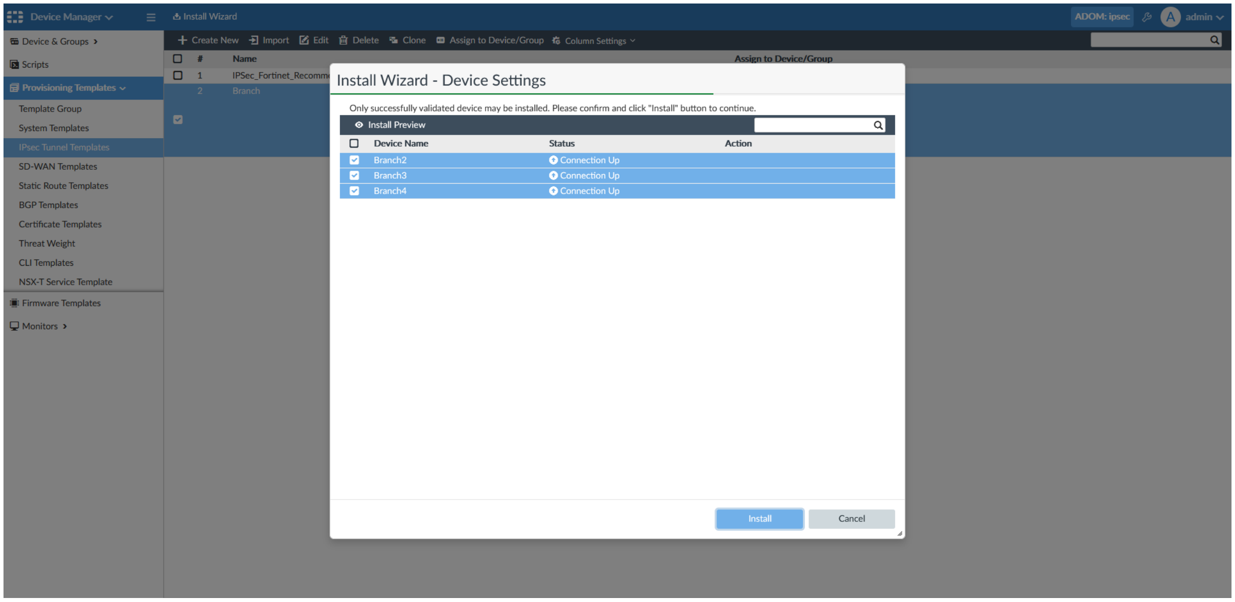
Available Entries (9)

- Branch1 [root] (IP: 10.8.71.41, Platform: FortiGate-VM64)
- Branch3 [root] (IP: 10.8.71.43, Platform: FortiGate-VM64)
- Branch4 [root] (IP: 10.8.71.44, Platform: FortiGate-VM64)
- Branch6 [root] (IP: 10.8.71.46, Platform: FortiGate-VM64)
- Branch7 [root] (IP: 10.8.71.47, Platform: FortiGate-VM64)
- HUB [root] (IP: 10.8.71.40, Platform: FortiGate-VM64)
- vlan171_0045 [FG-traffic] (IP: 10.8.71.45, Platform: FortiGa
- vlan171_0048 [root] (IP: 10.8.71.48, Platform: FortiGate-VI
- vlan171_0049 [root] (IP: 10.8.71.49, Platform: FortiGate-VI

Selected Entries (3)

- Branch2 [root] (IP: 10.8.71.42, Platform: FortiGate-VM64)
- Branch3 [vd_1] (IP: 10.8.71.43, Platform: FortiGate-VM64)
- Branch4 [vd_1] (IP: 10.8.71.44, Platform: FortiGate-VM64)

5. Execute device installation to push the IPSec VPN settings to devices.
   Click *Install Wizard* > *Device Settings* and follow the wizard to install the IPSec VPN settings.



Install Wizard - Device Settings

Only successfully validated device may be installed. Please confirm and click "Install" button to continue.

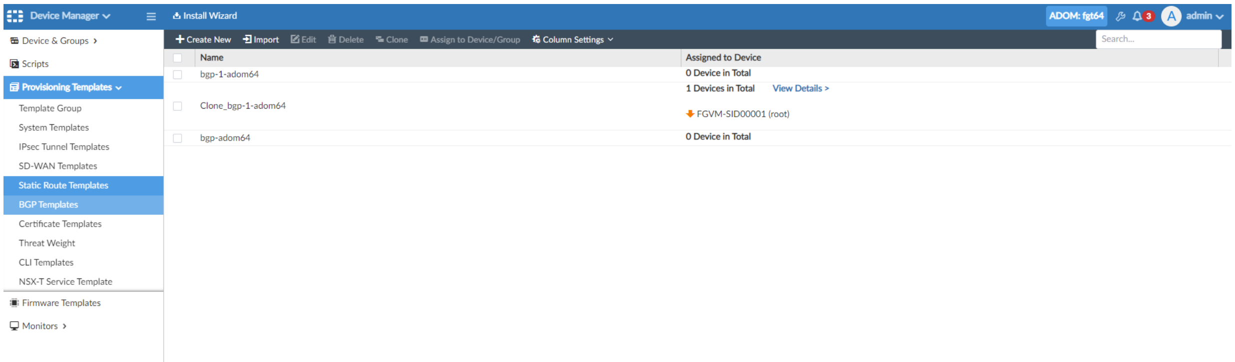
☐	Device Name	Status	Action
☑	Branch2	Connection Up	
☑	Branch3	Connection Up	
☑	Branch4	Connection Up	

Import BGP routing configuration from a managed FortiGate into a template - FMG 7.0.3

Import BGP routing configuration from a managed FortiGate into a template that can be used at the ADOM level.

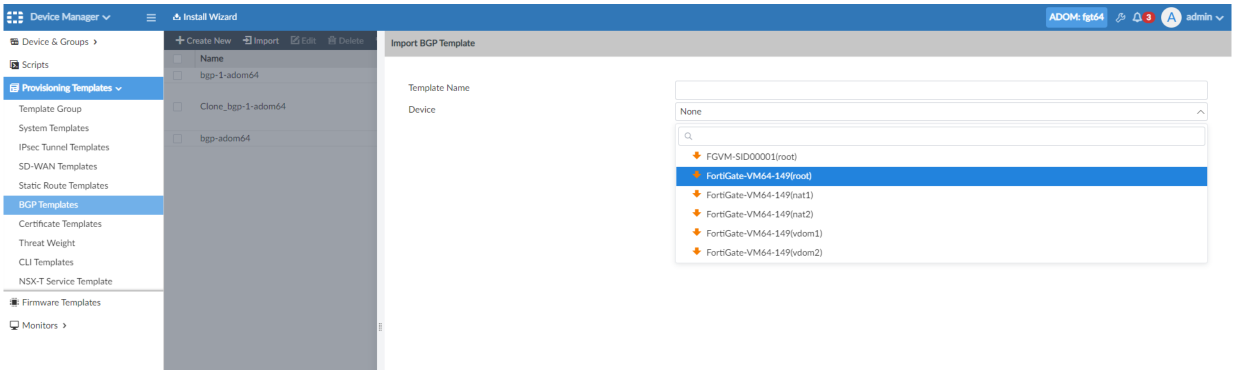
To import a BGP template:

1. Go to *Device Manager* > *Provisioning Templates* > *BGP Templates*.
2. Click *Import* in the toolbar.



☐	Name	Assigned to Device
☐	bgp-1-adom64	0 Device in Total
☐	Clone_bgp-1-adom64	1 Devices in Total View Details > FGVM-SID00001 (root)
☐	bgp-adom64	0 Device in Total

3. Enter a name for the template, and select a device VDOM from which to import the template.



4. Click *OK*.

BGP and IPsec recommended templates for SD-WAN overlays - FMG 7.0.3

FortiManager 7.0.3 introduces new default BGP and IPsec templates with recommendations that are designed to help you configure SD-WAN overlays in a hub and spoke topology. The templates are based on Fortinet's best practice recommendations.

Overlays generally consist of a VPN portion and a dynamic routing portion. IPsec templates configure the network connectivity, while BGP templates configure the dynamic routing between all locations. The hub acts as a dialup server that accepts connections from dialup clients (SD-WAN branch device). The hub uses the `mode-cfg` option to automatically assign IP addresses from the user defined network space to connecting branch devices. BGP neighbor configuration and neighbor range automatically accept BGP connections from the IP range configured with the `mode-cfg` option.

Each overlay network requires its unique network space and `network-id` defined in the IPsec template. The last two IP addresses of the network space should be reserved for the hub's IP address in the network and another for administrative use. For example, in a 10.10.10.0/24 overlay network:

- Spokes utilize 10.10.10.1 - 10.10.10.252
- Hub reserves 10.10.10.253
- Last usable is reserved for the *remote IP* section of the hub's interface: 10.10.10.254

Keep these guidelines in mind when configuring templates for SD-WAN overlays.

In the FortiManager GUI, you can access the new templates by going to *Device Manager* > *Provisioning Templates*. You must activate the templates before you can use them. Once activated, a popup pane is displayed, prompting you to enter details specific to your environment. Although the templates are designed for branch and hub devices, you can modify the templates as necessary after you create them.

This topic contains the following sections:

- Using recommended BGP templates on page 85
- Using recommended IPsec templates on page 89

Using recommended BGP templates

FortiManager includes the following BGP templates of recommendations to help you configure SD-WAN overlays:

Template Name	Description
BRANCH_BGP_Recommended	Fortinet's recommended BGP template for branch device configurations.
HUB_BGP_Recommended	Fortinet's recommended BGP template for hub device configurations.

You must activate the recommended templates to use them. After you created a BGP template for your environment, you can edit, delete, or clone the BGP template.

Meta fields can be used with a recommended template's required fields to ensure that fields are unique when the template is assigned to multiple devices.

This section describes how to:

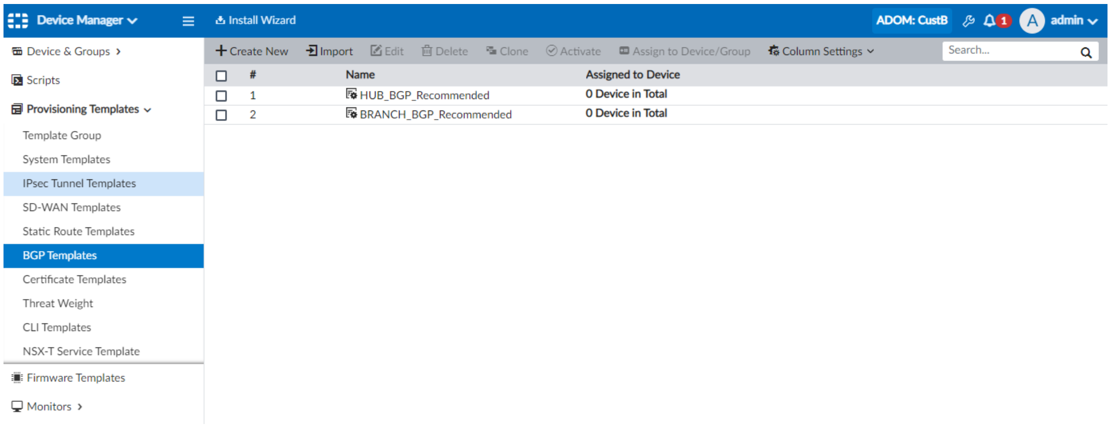
- Activate and create a BGP hub template by using the *HUB_BGP_Recommended* template. See Activating and creating a hub BGP template on page 85.
- Activate and create a BGP branch template by using the *BRANCH_BGP_Recommended* template. See Activating and creating a branch BGP template on page 87.

Activating and creating a hub BGP template

This section describes how to activate and create a BGP template for a hub device. The *HUB_BGP_Recommended* template guides you to complete the required settings for your environment.

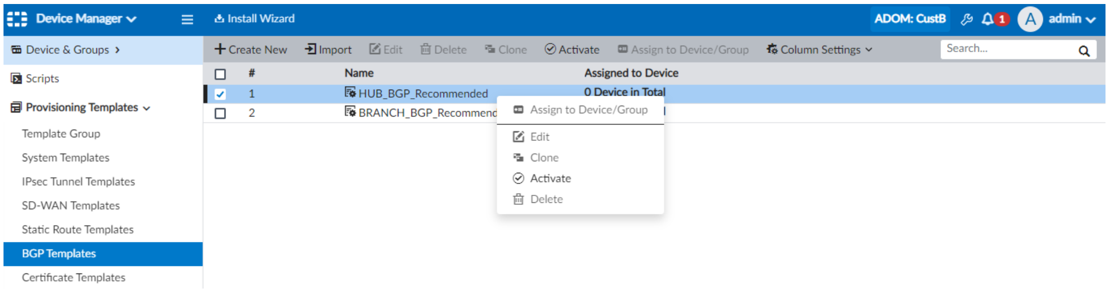
To activate and create a recommended BGP hub template:

1. Go to *Device Manager > Provisioning Templates > BGP Templates*.
   The following recommended BGP templates are available:
   - *HUB_BGP_Recommended*
   - *BRANCH_BGP_Recommended*

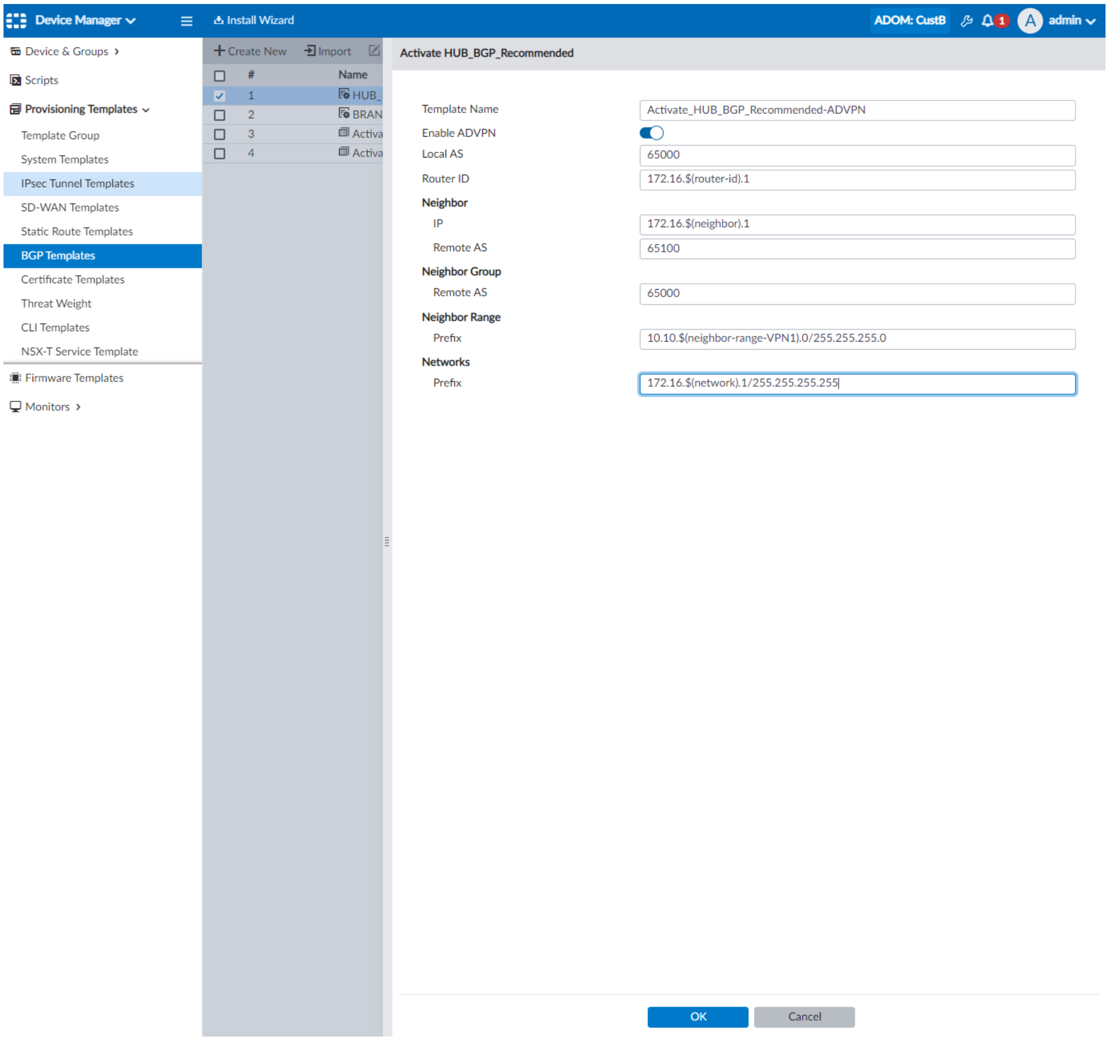


□	#	Name	Assigned to Device
□	1	HUB_BGP_Recommended	0 Device in Total
□	2	BRANCH_BGP_Recommended	0 Device in Total

2. Right-click the *HUB_BGP_Recommended* template, and select *Activate*.



The *Activate HUB_BGP_Recommended* pane is displayed.



Activate HUB_BGP_Recommended

Template Name: Activate_HUB_BGP_Recommended-ADVPN

Enable ADVPN: ●

Local AS: 65000

Router ID: 172.16.$(router-id).1

Neighbor

IP: 172.16.$(neighbor).1

Remote AS: 65100

Neighbor Group

Remote AS: 65000

Neighbor Range

Prefix: 10.10.$(neighbor-range-VPN1).0/255.255.255.0

Networks

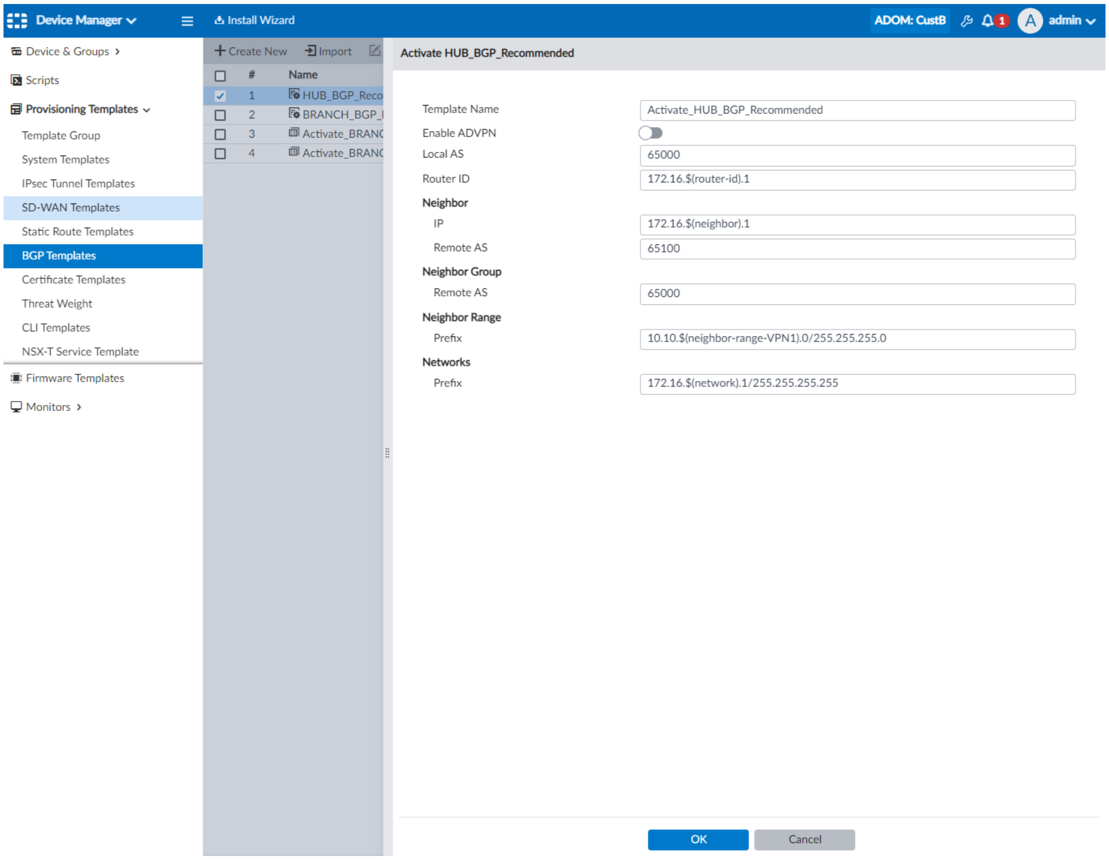
Prefix: 172.16.$(network).1/255.255.255.255

3. Complete the options, and click *OK* to create the template.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Local AS	Enter the local autonomous system (AS) number.

Router ID	Enter the router ID. The router ID is the unique IP address used to identify the hub device.
Neighbor	Enter the neighbor *IP* and *Remote AS*. The neighbor IP is the IP address used while peering as a neighbor.
Neighbor Group	Enter the neighbor group's *Remote AS*.
Neighbor Range	Enter the neighbor range *Prefix*. This is the network range that branch devices use to connect to the hub.
Networks	Enter the networks *Prefix*.

The following example uses meta fields in combination with the template.



Activate HUB_BGP_Recommended

Template Name	Activate_HUB_BGP_Recommended
Enable ADVPN	○
Local AS	65000
Router ID	172.16.$(router-id).1
Neighbor	
IP	172.16.$(neighbor).1
Remote AS	65100
Neighbor Group	
Remote AS	65000
Neighbor Range	
Prefix	10.10.$(neighbor-range-VPN1).0/255.255.255.0
Networks	
Prefix	172.16.$(network).1/255.255.255.255

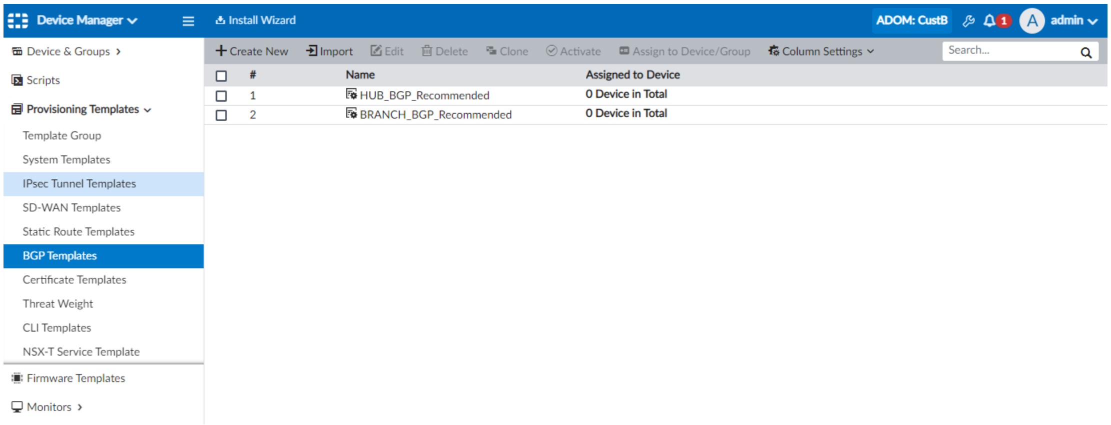
Activating and creating a branch BGP template

This section describes how to activate and create a BGP template for a branch device. The *BRANCH_BGP_Recommended* template guides you to complete the required settings for your environment.

To activate and create a branch BGP template:

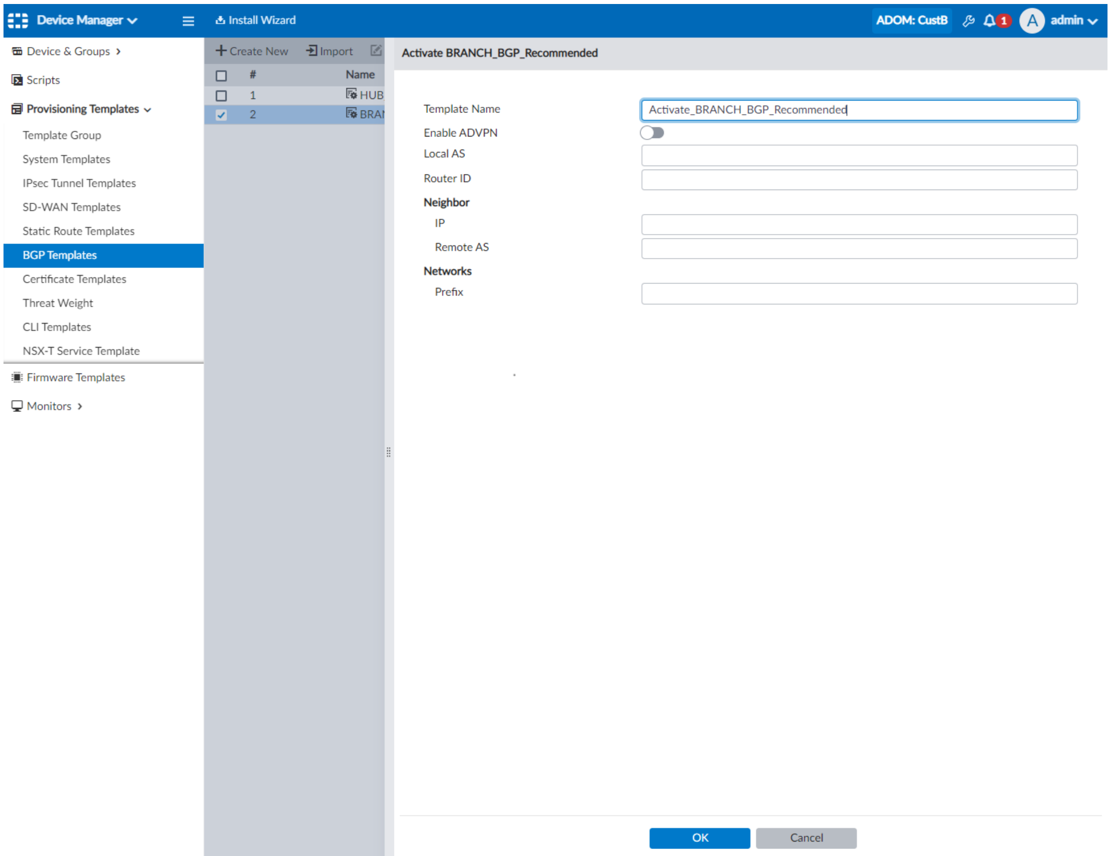
1. Go to *Device Manager* > *Provisioning Templates* > *BGP Templates*.
   The following recommended BGP templates are available:

- *HUB_BGP_Recommended*
- *BRANCH_BGP_Recommended*



#	Name	Assigned to Device
1	HUB_BGP_Recommended	0 Device in Total
2	BRANCH_BGP_Recommended	0 Device in Total

2. Right-click the *BRANCH_BGP_Recommended* template, and select *Activate*.



Activate BRANCH_BGP_Recommended

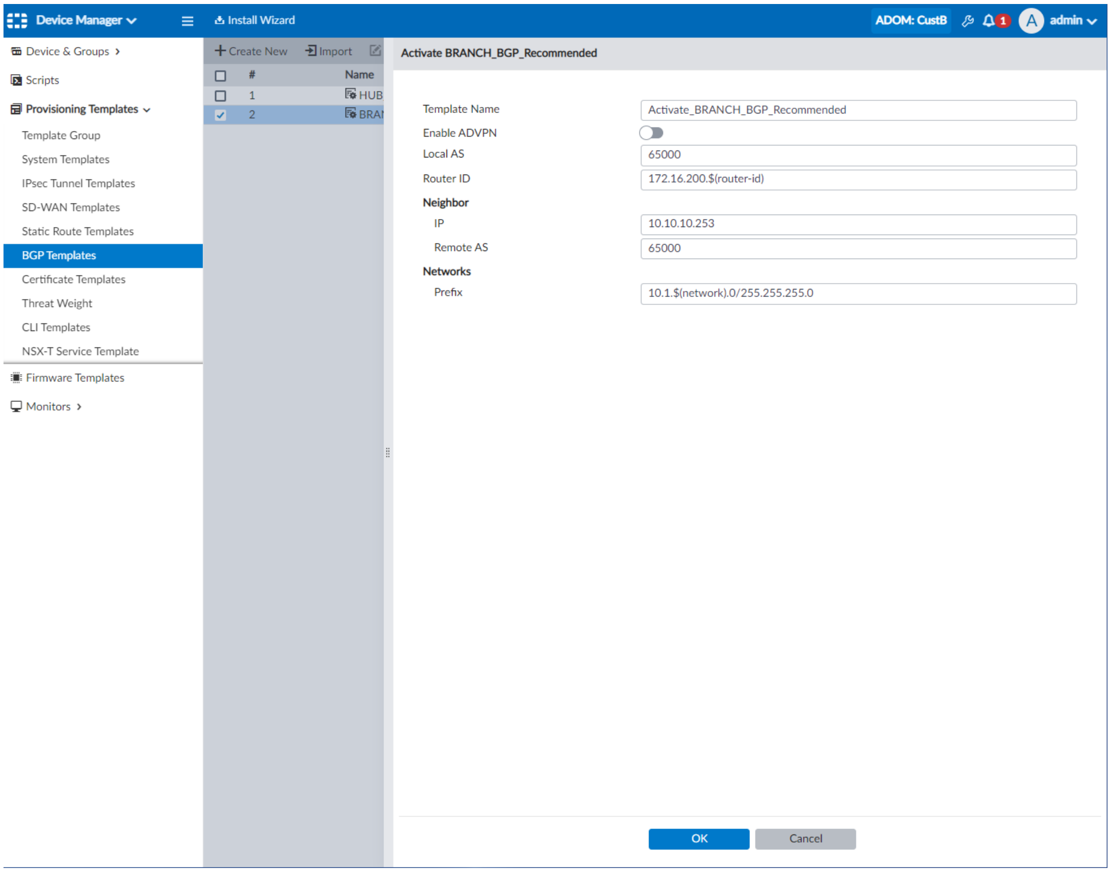
Template Name: Activate_BRANCH_BGP_Recommended
Enable ADVPN: ○
Local AS:
Router ID:
Neighbor
IP:
Remote AS:
Networks
Prefix:

3. Complete the options, and click *OK* to create the template.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Local AS	Enter the branch's local autonomous system (AS) number.

Router ID	Enter the router ID. The router ID is the unique IP address used to identify the branch device.
Neighbor	Enter the neighbor *IP* and *Remote AS*.
Networks	Enter the networks *Prefix*.

The following example uses meta fields in combination with the template.



Activate BRANCH_BGP_Recommended

Template Name	Activate_BRANCH_BGP_Recommended
Enable ADVPN	○
Local AS	65000
Router ID	172.16.200.$(router-id)
Neighbor	
IP	10.10.10.253
Remote AS	65000
Networks	
Prefix	10.1.$(network).0/255.255.255.0

Using recommended IPsec templates

FortiManager includes the following recommended IPsec templates to help you configure SD-WAN overlays:

Template Name	Description
HUB_IPSec_Recommended	Fortinet's recommended template for hub IPSec tunnels.
Branch_IPSec_Recommended	Fortinet's recommended template for IPSec branch device configurations.
IPSec_Fortinet_ Recommended	Fortinet's recommended template for IPSec configurations. This template is not used for SD-WAN configuration.

Recommended IPsec templates come preconfigured with best practice recommendations for use within your environment. These templates can be used to simplify deployment of SD-WAN interconnected sites.

You must activate the recommended templates to use them. After you create an IPsec template for your environment, you can edit, delete, or clone the template.

Meta fields can be used with a recommended template's required fields to ensure that fields are unique when the template is assigned to multiple devices.

This section describes how to:

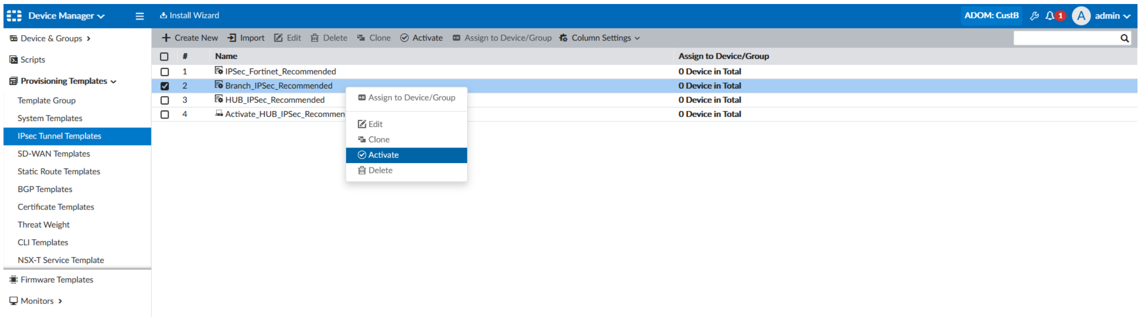
- Activate and create an IPsec branch template by using the *Branch_IPSec_Recommended* template. See Activating and creating a branch IPsec template on page 90.
- Activate and create an IPsec hub template by using the *HUB_IPSec_Recommended* template. See Activating and creating a hub IPsec template on page 91.

Activating and creating a branch IPsec template

This section describes how to activate and create an IPsec template for a branch device. The *Branch_IPSec_Recommended* template guides you to complete the required settings for your environment.

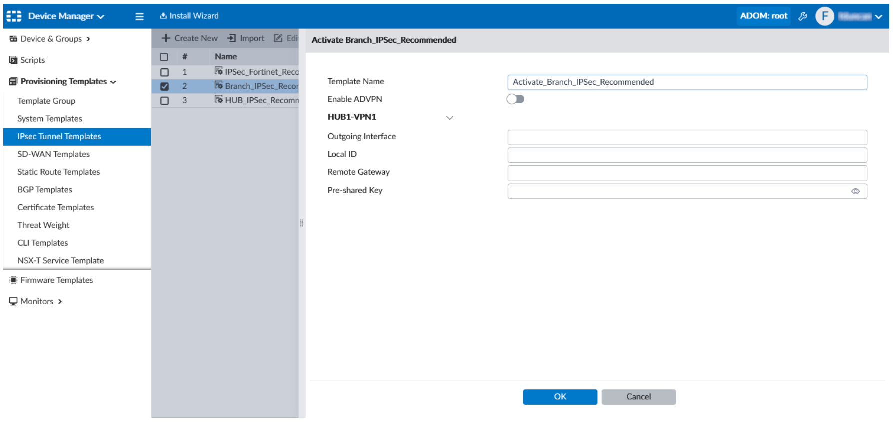
To activate and create a branch IPsec template:

1. Go to *Device Manager > Provisioning Templates > IPsec Tunnel Templates*.
   The following recommended IPsec templates are available:
   - *Branch_IPSec_Recommended*
   - *HUB_IPSec_Recommended*
   - *IPSec_Fortinet_Recommended*
2. Right-click the *Branch_IPSec_Recommended* template, and click *Activate*.



	#	Name	Assign to Device/Group
☐	1	IPSec_Fortinet_Recommended	0 Device in Total
☑	2	Branch_IPSec_Recommended	0 Device in Total
☐	3	HUB_IPSec_Recommended	0 Device in Total
☐	4	Activate_HUB_IPSec_Recommen	0 Device in Total

   A pane is displayed where you can enter details specific to your environment.



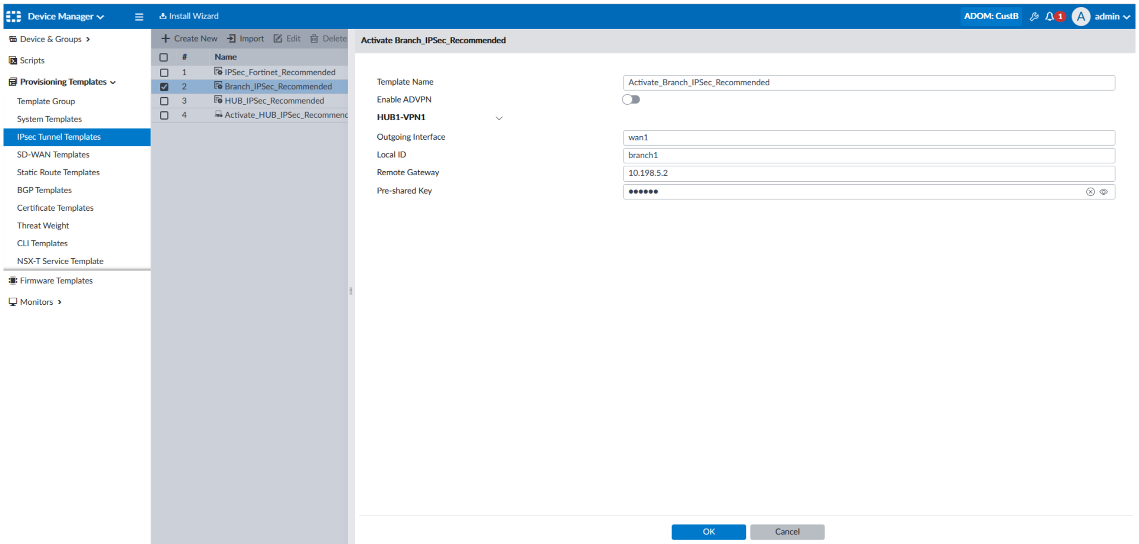
Activate Branch_IPSec_Recommended

Template Name: Activate_Branch_IPSec_Recommended
Enable ADVPN
HUB1-VPN1
Outgoing Interface
Local ID
Remote Gateway
Pre-shared Key

3. Complete the options, and click *OK* to create the template.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Outgoing Interface	Enter the outgoing interface. This is the physical port from which the tunnel connection is initiated.
Local ID	Enter a Local ID. This is used to identify devices connecting to the hub.
Remote Gateway	Enter the remote gateway.
Pre-shared Key	Enter the pre-shared key.

The following example uses meta fields in combination with the template.



	#	Name
□	1	IPSec_Fortinet_Recommended
☑	2	Branch_IPSec_Recommended
□	3	HUB_IPSec_Recommended
□	4	Activate_HUB_IPSec_Recommenc

Activate Branch_IPSec_Recommended

Template Name	Activate_Branch_IPSec_Recommended
Enable ADVPN	○
HUB1-VPN1	
Outgoing Interface	wan1
Local ID	branch1
Remote Gateway	10.198.5.2
Pre-shared Key	••••••

A new template is created based on the recommended template you selected and the configuration details provided.

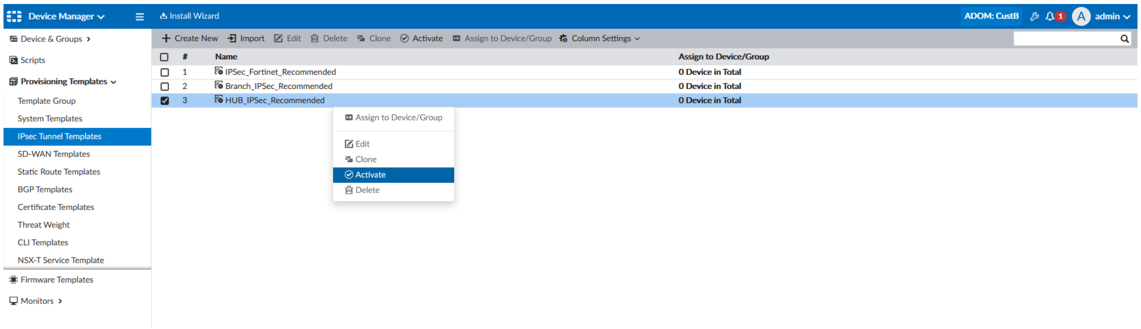
Activating and creating a hub IPsec template

This section describes how to activate and create an IPsec template for a hub device. The *HUB_IPSec_Recommended* template guides you to complete the required settings for your environment.

To activate and create a hub IPsec template:

1. Go to *Device Manager* > *Provisioning Templates* > *IPsec Tunnel Templates*.
   The following recommended IPsec templates are available:
   - *Branch_IPSec_Recommended*
   - *HUB_IPSec_Recommended*
   - *IPSec_Fortinet_Recommended*

2. Right-click the *HUB_IPSec_Recommended* template, and click *Activate*.



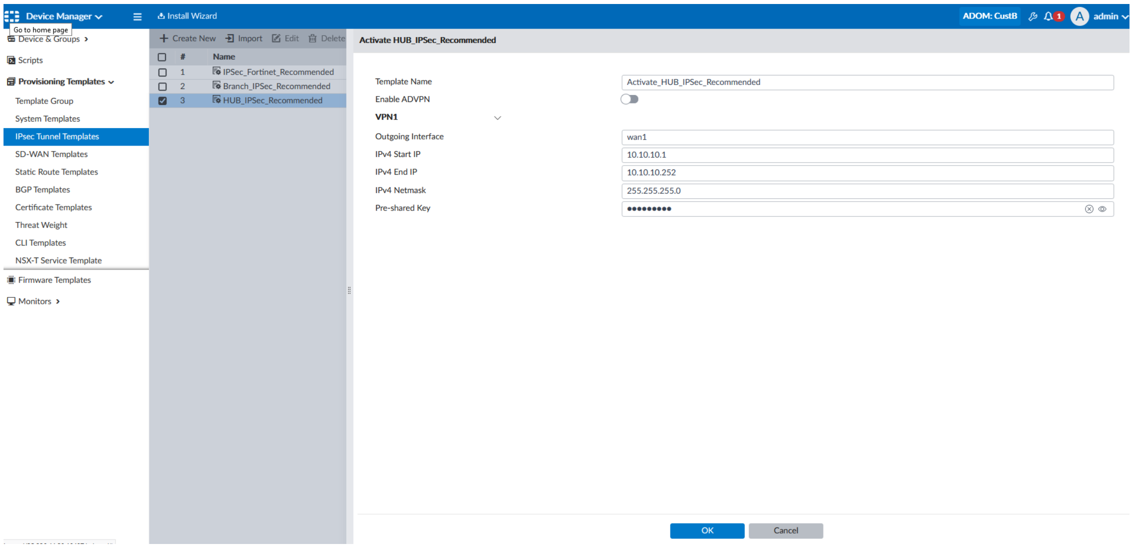
☐	#	Name	Assign to Device/Group
☐	1	IPSec_Fortinet_Recommended	0 Device in Total
☐	2	Branch_IPSec_Recommended	0 Device in Total
☑	3	HUB_IPSec_Recommended	0 Device in Total

A dialog will appear where you can enter configuration details specific to your environment.

3. Complete the options, and click *OK*.

Template Name	Enter a name for the template.
Enable ADVPN	Optionally, toggle this setting to enable Auto Discovery VPN (ADVPN).
Outgoing Interface	Enter the outgoing interface. This is the physical port that the branch devices are connecting in on.
IPv4 Start IP	Enter the first usable IP address in the range.
IPv4 End IP	Enter the last usable IP address in the range.
IPv4 Netmask	Enter the IPv4 netmask.
Pre-shared Key	Enter the pre-shared key.

The following example uses meta fields in combination with the template.



Activate HUB_IPSec_Recommended

Template Name	Activate_HUB_IPSec_Recommended
Enable ADVPN	○
VPN1	
Outgoing Interface	wan1
IPv4 Start IP	10.10.10.1
IPv4 End IP	10.10.10.252
IPv4 Netmask	255.255.255.0
Pre-shared Key	•••••••••

Reporting

7.0.1

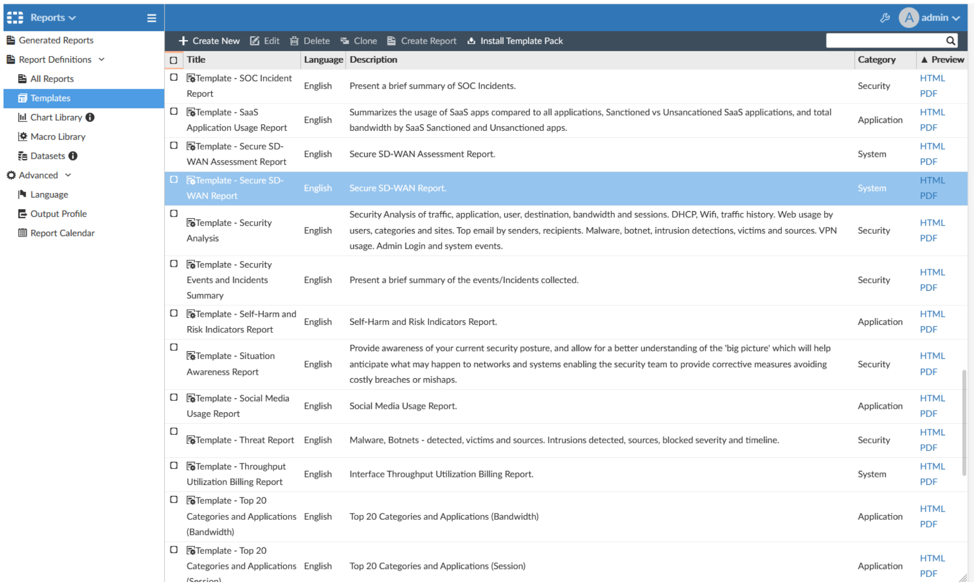
- Additional charts for SD-WAN reporting FAZ 7.0.1 on page 93

Additional charts for SD-WAN reporting - FAZ 7.0.1

The Secure SD-WAN Report now includes charts for SD-WAN Link Health Status and the Inbound/Outbound status per SD-WAN device interfaces.

To view additional charts in the SD-WAN Report:

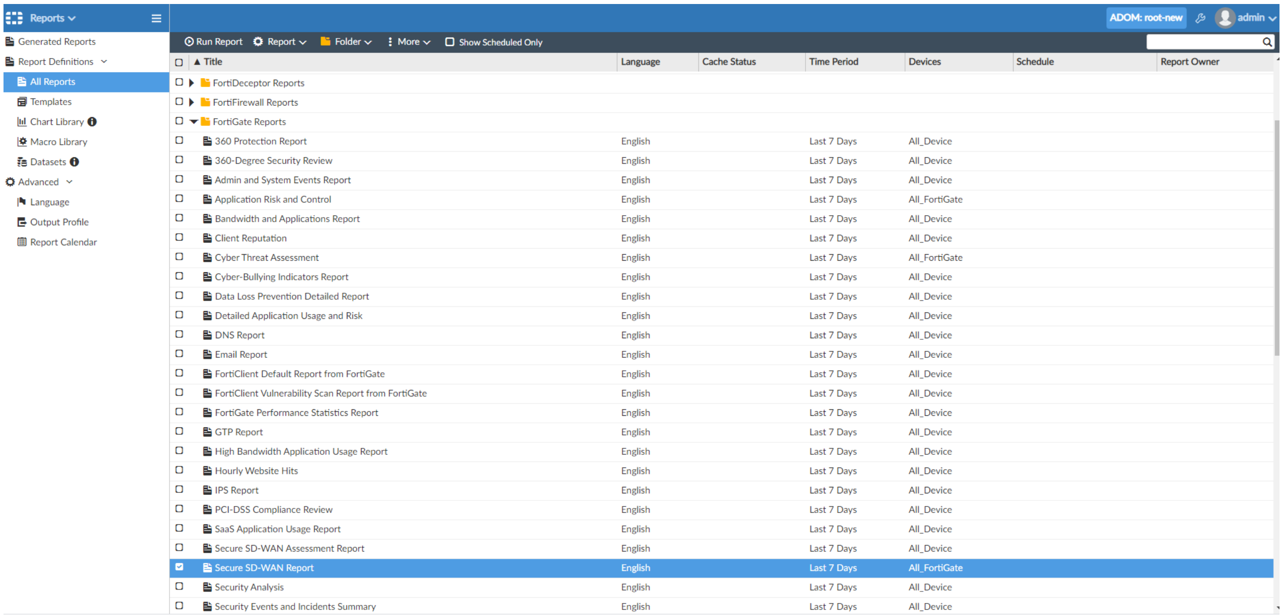
1. Go to *Reports* > *Templates*.
2. In the templates pane, right-click *Secure SD-WAN Report*, and click *Create Report*.



☐	Title	Language	Description	Category	▲ Preview
☐	Template - SOC Incident Report	English	Present a brief summary of SOC Incidents.	Security	HTML PDF
☐	Template - SaaS Application Usage Report	English	Summarizes the usage of SaaS apps compared to all applications, Sanctioned vs Unsancationed SaaS applications, and total bandwidth by SaaS Sanctioned and Unsanctioned apps.	Application	HTML PDF
☐	Template - Secure SD-WAN Assessment Report	English	Secure SD-WAN Assessment Report.	System	HTML PDF
☐	Template - Secure SD-WAN Report	English	Secure SD-WAN Report.	System	HTML PDF
☐	Template - Security Analysis	English	Security Analysis of traffic, application, user, destination, bandwidth and sessions. DHCP, Wifi, traffic history. Web usage by users, categories and sites. Top email by senders, recipients. Malware, botnet, intrusion detections, victims and sources. VPN usage. Admin Login and system events.	Security	HTML PDF
☐	Template - Security Events and Incidents Summary	English	Present a brief summary of the events/Incidents collected.	Security	HTML PDF
☐	Template - Self-Harm and Risk Indicators Report	English	Self-Harm and Risk Indicators Report.	Application	HTML PDF
☐	Template - Situation Awareness Report	English	Provide awareness of your current security posture, and allow for a better understanding of the 'big picture' which will help anticipate what may happen to networks and systems enabling the security team to provide corrective measures avoiding costly breaches or mishaps.	Security	HTML PDF
☐	Template - Social Media Usage Report	English	Social Media Usage Report.	Application	HTML PDF
☐	Template - Threat Report	English	Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and timeline.	Security	HTML PDF
☐	Template - Throughput Utilization Billing Report	English	Interface Throughput Utilization Billing Report.	System	HTML PDF
☐	Template - Top 20 Categories and Applications (Bandwidth)	English	Top 20 Categories and Applications (Bandwidth)	Application	HTML PDF
☐	Template - Top 20 Categories and Applications (Session)	English	Top 20 Categories and Applications (Session)	Application	HTML PDF

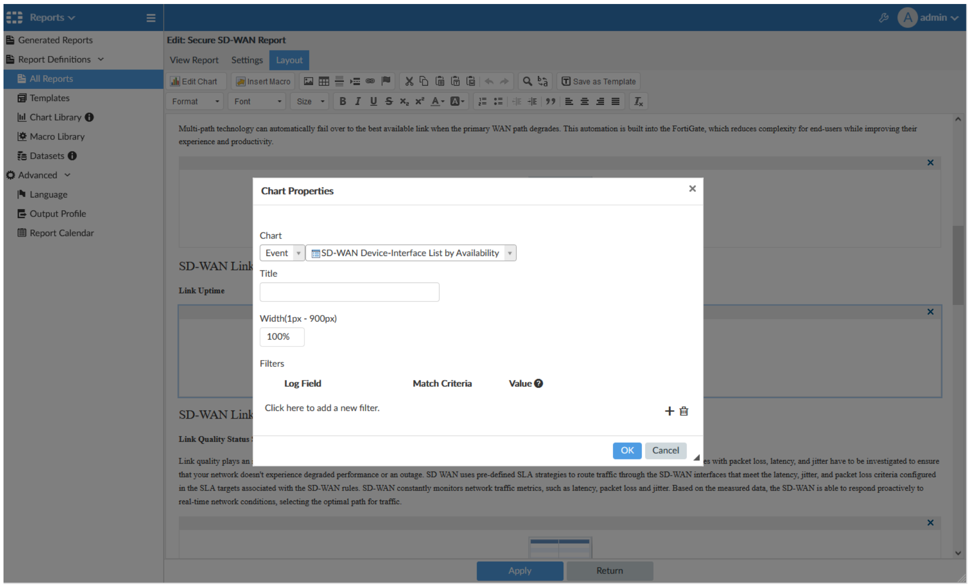
3. In the tree menu, click *Report Definitions* > *All Reports*.

4. In the reports pane, expand *FortiGate Reports* and click *Secure SD-WAN Report*.



	Title	Language	Cache Status	Time Period	Devices	Schedule	Report Owner
□	▸ FortiDeceptor Reports						
□	▸ FortiFirewall Reports						
□	▾ FortiGate Reports						
□	360 Protection Report	English		Last 7 Days	All_Device		
□	360-Degree Security Review	English		Last 7 Days	All_Device		
□	Admin and System Events Report	English		Last 7 Days	All_Device		
□	Application Risk and Control	English		Last 7 Days	All_FortiGate		
□	Bandwidth and Applications Report	English		Last 7 Days	All_Device		
□	Client Reputation	English		Last 7 Days	All_Device		
□	Cyber Threat Assessment	English		Last 7 Days	All_FortiGate		
□	Cyber-Bullying Indicators Report	English		Last 7 Days	All_Device		
□	Data Loss Prevention Detailed Report	English		Last 7 Days	All_Device		
□	Detailed Application Usage and Risk	English		Last 7 Days	All_Device		
□	DNS Report	English		Last 7 Days	All_Device		
□	Email Report	English		Last 7 Days	All_Device		
□	FortiClient Default Report from FortiGate	English		Last 7 Days	All_Device		
□	FortiClient Vulnerability Scan Report from FortiGate	English		Last 7 Days	All_Device		
□	FortiGate Performance Statistics Report	English		Last 7 Days	All_Device		
□	GTP Report	English		Last 7 Days	All_Device		
□	High Bandwidth Application Usage Report	English		Last 7 Days	All_Device		
□	Hourly Website Hits	English		Last 7 Days	All_Device		
□	IPS Report	English		Last 7 Days	All_Device		
□	PCI-DSS Compliance Review	English		Last 7 Days	All_Device		
□	SaaS Application Usage Report	English		Last 7 Days	All_Device		
□	Secure SD-WAN Assessment Report	English		Last 7 Days	All_Device		
☑	Secure SD-WAN Report	English		Last 7 Days	All_FortiGate		
□	Security Analysis	English		Last 7 Days	All_Device		
□	Security Events and Incidents Summary	English		Last 7 Days	All_Device		

5. Click the *Layout* tab and scroll down to the *SD-WAN Link Health Status* chart, then click the *Chart Properties*. The *SD-WAN Device-Interface List by Activity* chart was added to the *Event* category.



Edit: Secure SD-WAN Report

Multi-path technology can automatically fail over to the best available link when the primary WAN path degrades. This automation is built into the FortiGate, which reduces complexity for end-users while improving their experience and productivity.

SD-WAN Link

Link Uptime

SD-WAN Link

Link Quality Status

Link quality plays an … s with packet loss, latency, and jitter have to be investigated to ensure that your network doesn't experience degraded performance or an outage. SD WAN uses pre-defined SLA strategies to route traffic through the SD-WAN interfaces that meet the latency, jitter, and packet loss criteria configured in the SLA targets associated with the SD-WAN rules. SD-WAN constantly monitors network traffic metrics, such as latency, packet loss and jitter. Based on the measured data, the SD-WAN is able to respond proactively to real-time network conditions, selecting the optimal path for traffic.

Chart Properties

Chart: Event | SD-WAN Device-Interface List by Availability

Title:

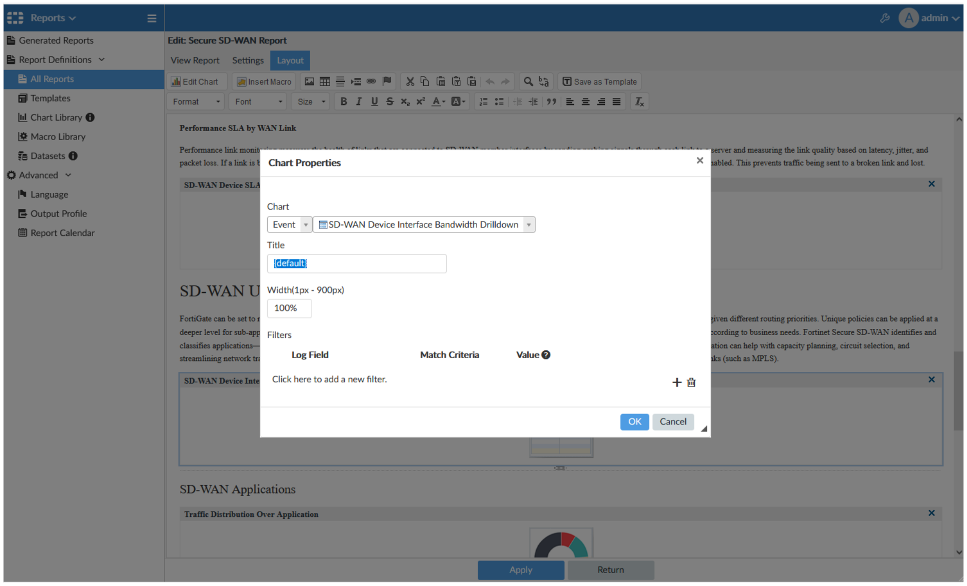
Width(1px - 900px): 100%

Filters

Log Field	Match Criteria	Value
Click here to add a new filter.		

OK Cancel

6. Scroll down to the *SD-WAN Utilization* section and click the *Chart Properties*. The *SD-WAN Device Interface Bandwidth Drilldown* chart was added to the *Event* category.



Edit: Secure SD-WAN Report

Performance SLA by WAN Link

SD-WAN Device SLA

SD-WAN U

SD-WAN Device Inte

SD-WAN Applications

Traffic Distribution Over Application

Chart Properties

Chart: Event | SD-WAN Device Interface Bandwidth Drilldown

Title: {default}

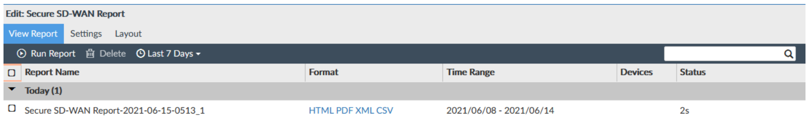
Width(1px - 900px): 100%

Filters

Log Field	Match Criteria	Value
Click here to add a new filter.		

OK Cancel

7. Click the *View Report* tab. In the *Format* column, click *PDF*.



Edit: Secure SD-WAN Report

□ Report Name	Format	Time Range	Devices	Status
Today (1)				
□ Secure SD-WAN Report-2021-06-15-0513_1	HTML PDF XML CSV	2021/06/08 - 2021/06/14		2s

The Table of Contents displays the *SD-WAN Link Health Status* report.

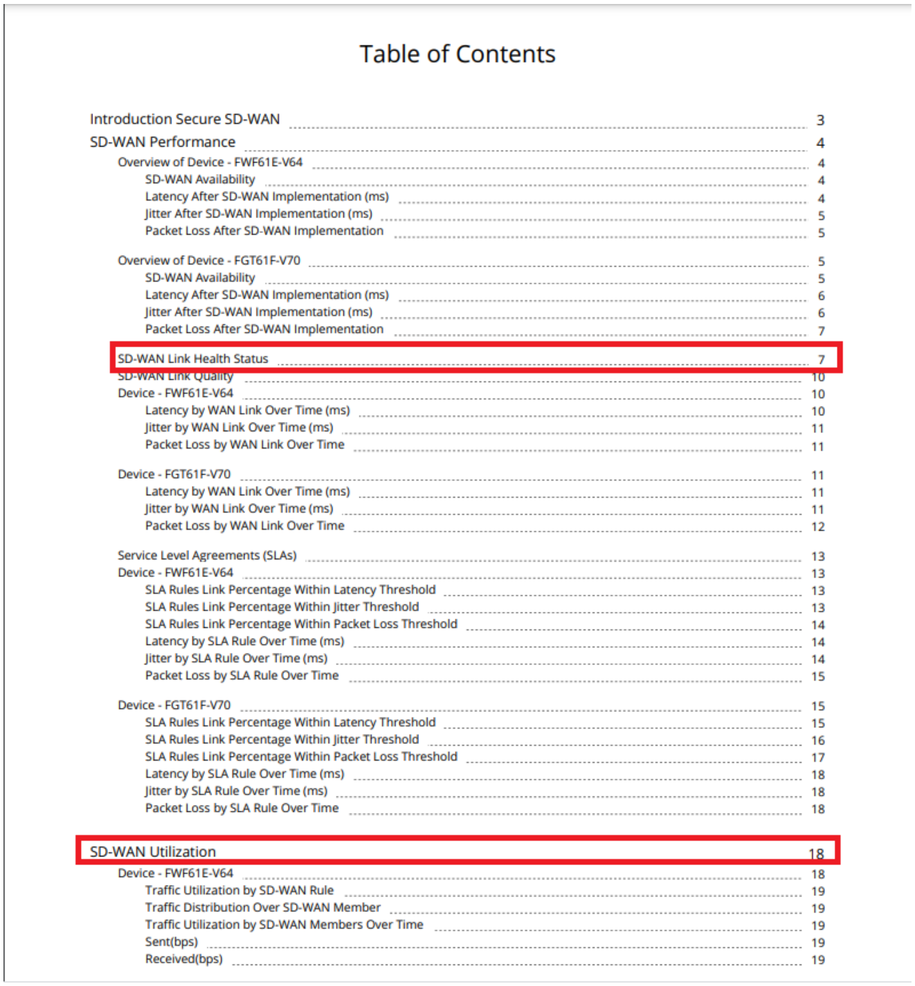
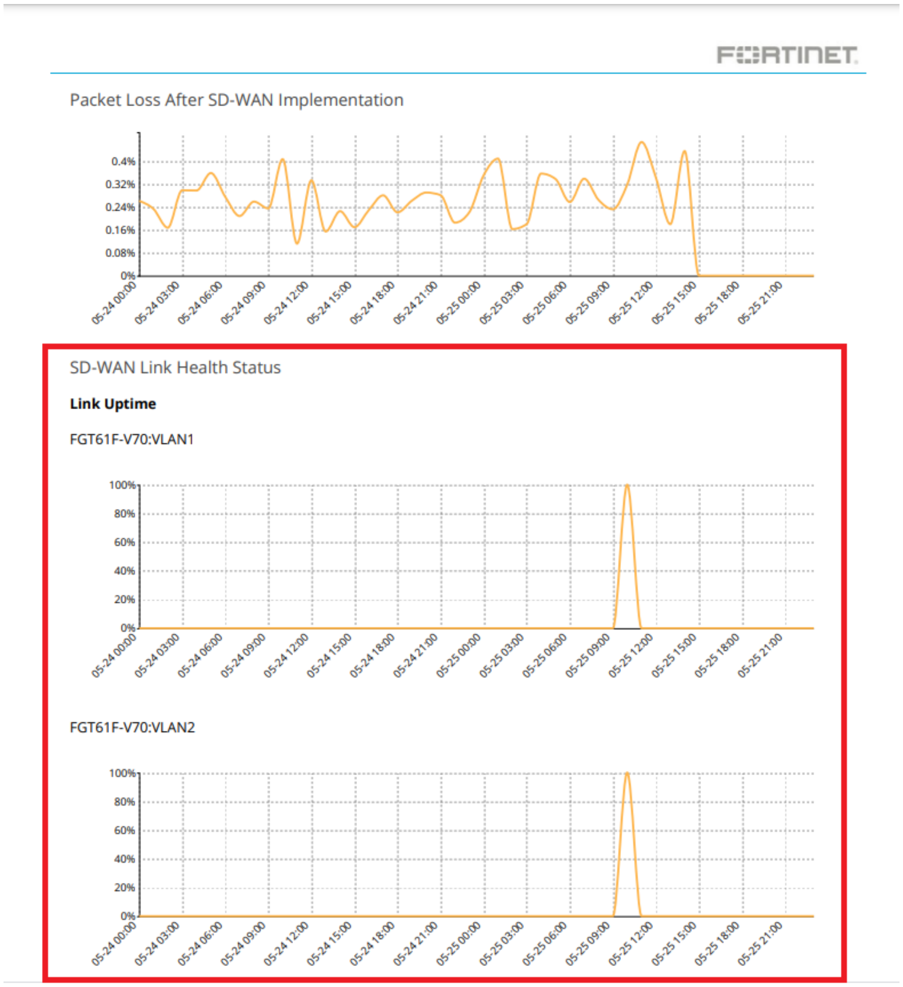


Table of Contents

The *SD-WAN Device-Interface List by Availability* drilldown charts are displayed.



Packet Loss After SD-WAN Implementation

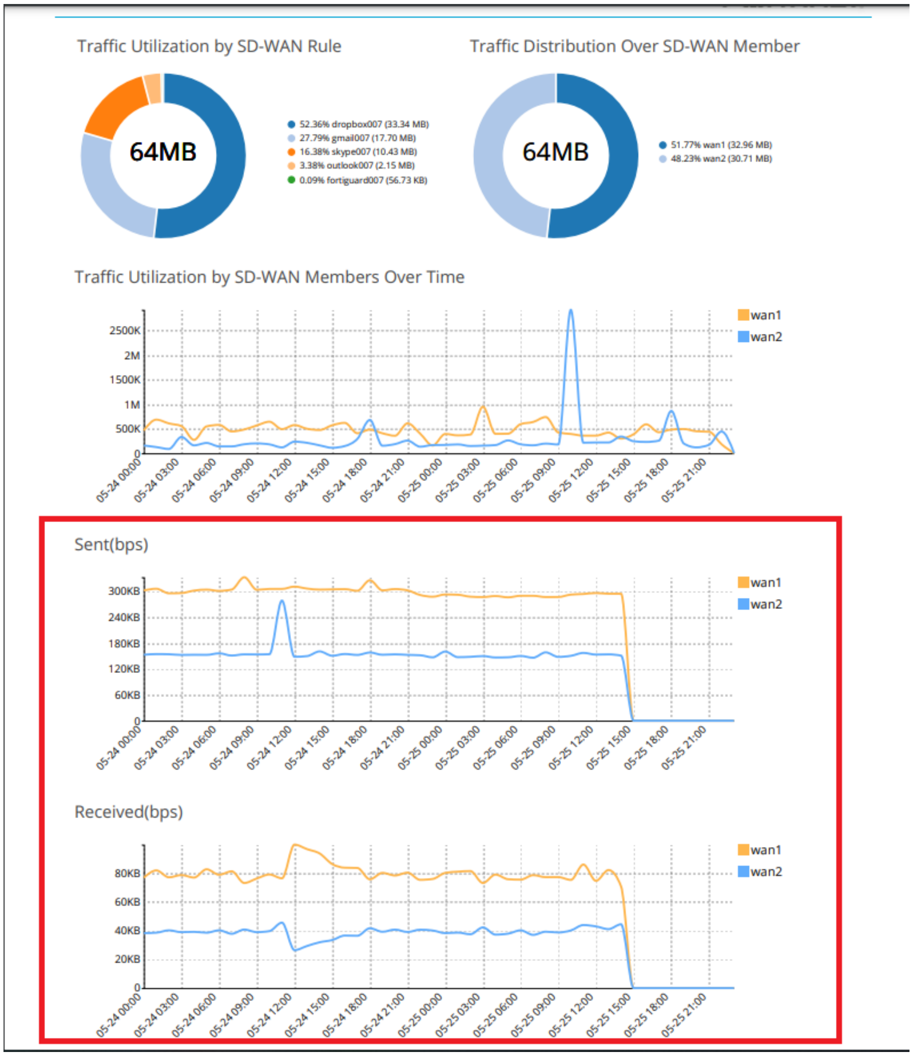
SD-WAN Link Health Status

Link Uptime

FGT61F-V70:VLAN1

FGT61F-V70:VLAN2

The *SD-Wan Device Interface Bandwidth Drilldown* charts are also displayed.


Traffic Utilization by SD-WAN Rule
64MB
52.36% dropbox007 (33.34 MB)
27.79% gmail007 (17.70 MB)
16.38% skype007 (10.43 MB)
3.38% outlook007 (2.15 MB)
0.09% fortiguard007 (56.73 KB)
Traffic Distribution Over SD-WAN Member
64MB
51.77% wan1 (32.96 MB)
48.23% wan2 (30.71 MB)
Traffic Utilization by SD-WAN Members Over Time
2500K
2M
1500K
1M
500K
0
wan1
wan2
05-24 00:00
05-24 03:00
05-24 06:00
05-24 09:00
05-24 12:00
05-24 15:00
05-24 18:00
05-24 21:00
05-25 00:00
05-25 03:00
05-25 06:00
05-25 09:00
05-25 12:00
05-25 15:00
05-25 18:00
05-25 21:00
Sent(bps)
300KB
240KB
180KB
120KB
60KB
0
wan1
wan2
05-24 00:00
05-24 03:00
05-24 06:00
05-24 09:00
05-24 12:00
05-24 15:00
05-24 18:00
05-24 21:00
05-25 00:00
05-25 03:00
05-25 06:00
05-25 09:00
05-25 12:00
05-25 15:00
05-25 18:00
05-25 21:00
Received(bps)
80KB
60KB
40KB
20KB
0
wan1
wan2
05-24 00:00
05-24 03:00
05-24 06:00
05-24 09:00
05-24 12:00
05-24 15:00
05-24 18:00
05-24 21:00
05-25 00:00
05-25 03:00
05-25 06:00
05-25 09:00
05-25 12:00
05-25 15:00
05-25 18:00
05-25 21:00

Routing

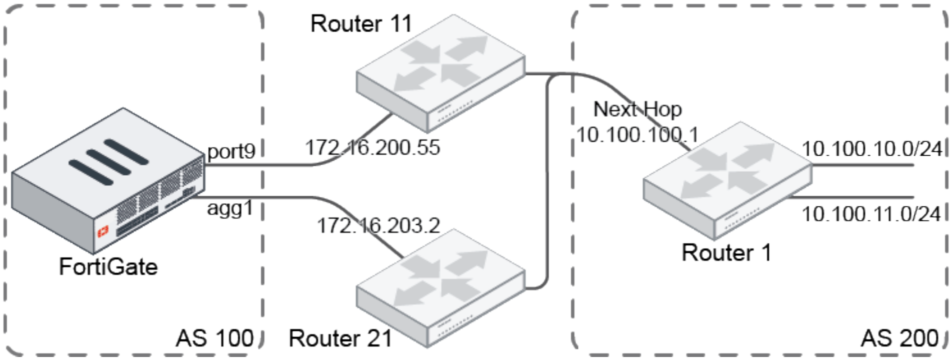
7.0.0

ECMP routes for recursive BGP next hop resolution

When there are multiple ECMP routes to a BGP next hop, all of them are considered for the next hop recursive resolution. This ensures that the outgoing traffic can be load balanced.

To support multipath, either EGBP or IGBP multipath must be enabled:

```
config router bgp
    set ebgp-multipath enable
    set ibgp-multipath enable
end
```



In this example, there are two static routes. The FortiGate has learned two BGP routes from Router 1 that have the same next hop at 10.100.100.1. The next hop is resolved by the two static routes.

To verify that the routes are added to the BGP routing table:

1. Check the two static routes:

```
# get router info routing-table static
Routing table for VRF=0
S       10.100.100.0/24 [10/0] via 172.16.200.55, port9
                        [10/0] via 172.16.203.2, agg1
```

2. Confirm that both routes are in the BGP routing table:

```
# get router info routing-table bgp
Routing table for VRF=0
B       10.100.10.0/24 [20/200] via 10.100.100.1 (recursive via 172.16.200.55, port9),
00:00:07
                                                 (recursive via 172.16.203.2, agg1),
00:00:07
B       10.100.11.0/24 [20/200] via 10.100.100.1 (recursive via 172.16.200.55, port9),
00:00:07
                                                 (recursive via 172.16.203.2, agg1),
00:00:07
```

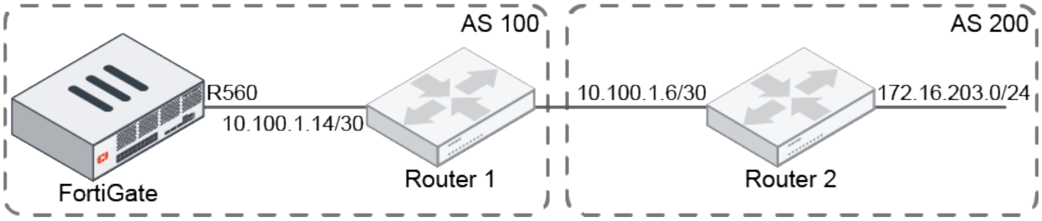
BGP next hop recursive resolution using other BGP routes

By default, BGP routes are not considered when a BGP next hop requires recursive resolution. They are considered when `recursive-next-hop` is enabled. Recursive resolution will resolve to one level.

To consider BGP routes for recursive resolution of next hops:

```
config router bgp
    set recursive-next-hop enable
end
```

Example



To see the change in the routing table when the option is enabled:

1. Check the BGP routing table:

```
# get router info routing-table bgp
Routing table for VRF=0
B       10.100.1.4/30 [200/0] via 10.100.1.14 (recursive is directly connected, R560),
00:02:06
```

2. Enable BGP routes for recursive resolution of next hops:

```
config router bgp
    set recursive-next-hop enable
end
```

3. Check the BGP routing table again:

```
# get router info routing-table bgp
Routing table for VRF=0
B       10.100.1.4/30 [200/0] via 10.100.1.14 (recursive is directly connected, R560),
00:02:15
B       172.16.203.0/24 [200/0] via 10.100.1.6 (recursive via 10.100.1.14, R560),
00:00:06
```

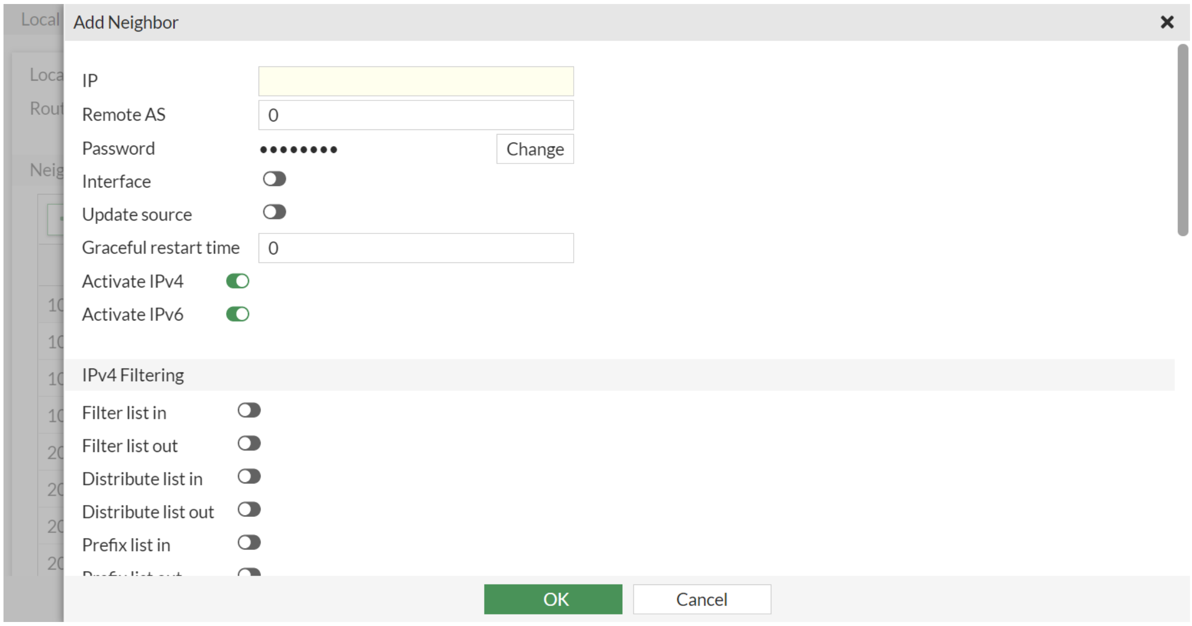
The second BGP route's next hop is now recursively resolved by another BGP route.

GUI advanced routing options for BGP

Users can configure advanced BGP routing options on the *Network* > *BGP* page. The *BGP* > *Routing Objects* page allows users to create new *Route Map*, *Access List*, *Prefix List*, *AS Path List*, and *Community List*.

BGP page enhancements

The *Password*, *Interface*, *Update source*, *Graceful restart time*, *Activate IPv4/IPv6*, and I*Pv4/IPv6 Filtering* options are available when creating a new neighbor.

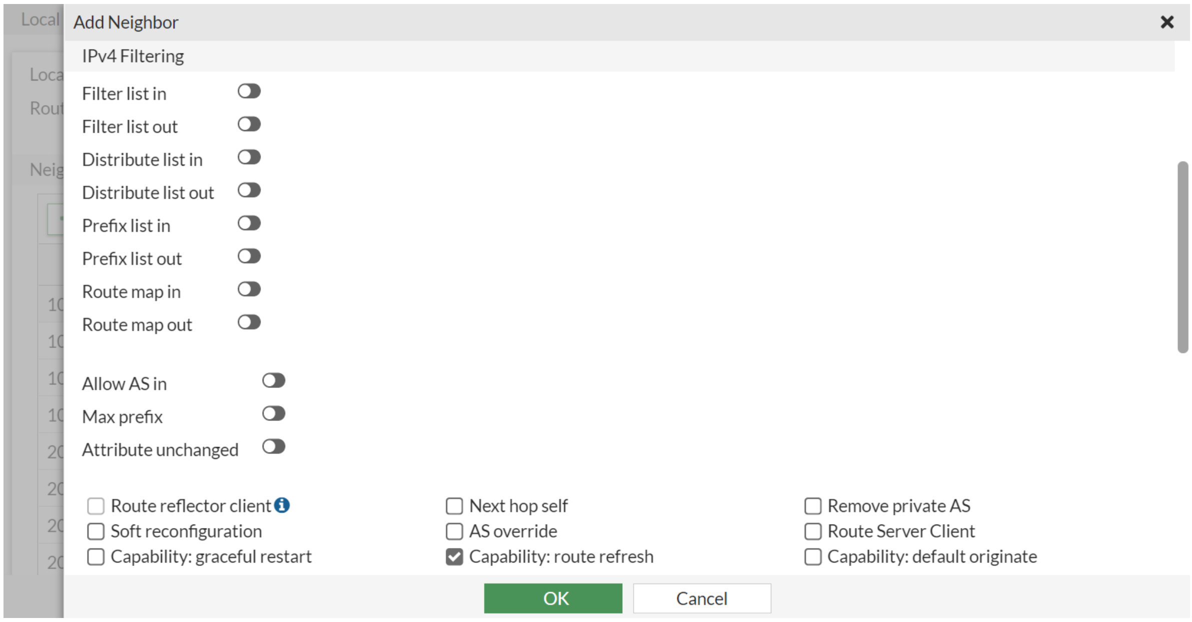


Add Neighbor

IP
Remote AS 0
Password •••••••• Change
Interface ○
Update source ○
Graceful restart time 0
Activate IPv4 ●
Activate IPv6 ●

IPv4 Filtering

Filter list in ○
Filter list out ○
Distribute list in ○
Distribute list out ○
Prefix list in ○
Prefix list out ○



Add Neighbor

IPv4 Filtering

Filter list in ○

Filter list out ○

Distribute list in ○

Distribute list out ○

Prefix list in ○

Prefix list out ○

Route map in ○

Route map out ○

Allow AS in ○

Max prefix ○

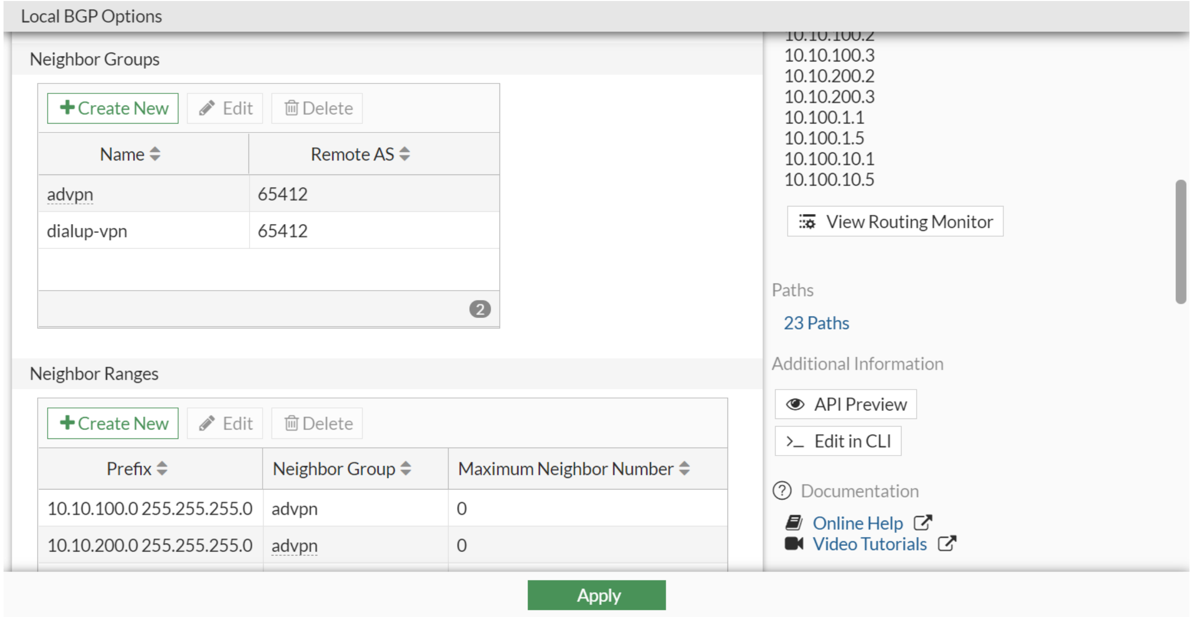
Attribute unchanged ○

☐ Route reflector client ☐ Next hop self ☐ Remove private AS

☐ Soft reconfiguration ☐ AS override ☐ Route Server Client

☐ Capability: graceful restart ☑ Capability: route refresh ☐ Capability: default originate

Tables are added to create new neighbor groups and neighbor ranges.



Local BGP Options

Neighbor Groups

Name	Remote AS
advpn	65412
dialup-vpn	65412

Neighbor Ranges

Prefix	Neighbor Group	Maximum Neighbor Number
10.10.100.0 255.255.255.0	advpn	0
10.10.200.0 255.255.255.0	advpn	0

10.10.100.2
10.10.100.3
10.10.200.2
10.10.200.3
10.100.1.1
10.100.1.5
10.100.10.1
10.100.10.5

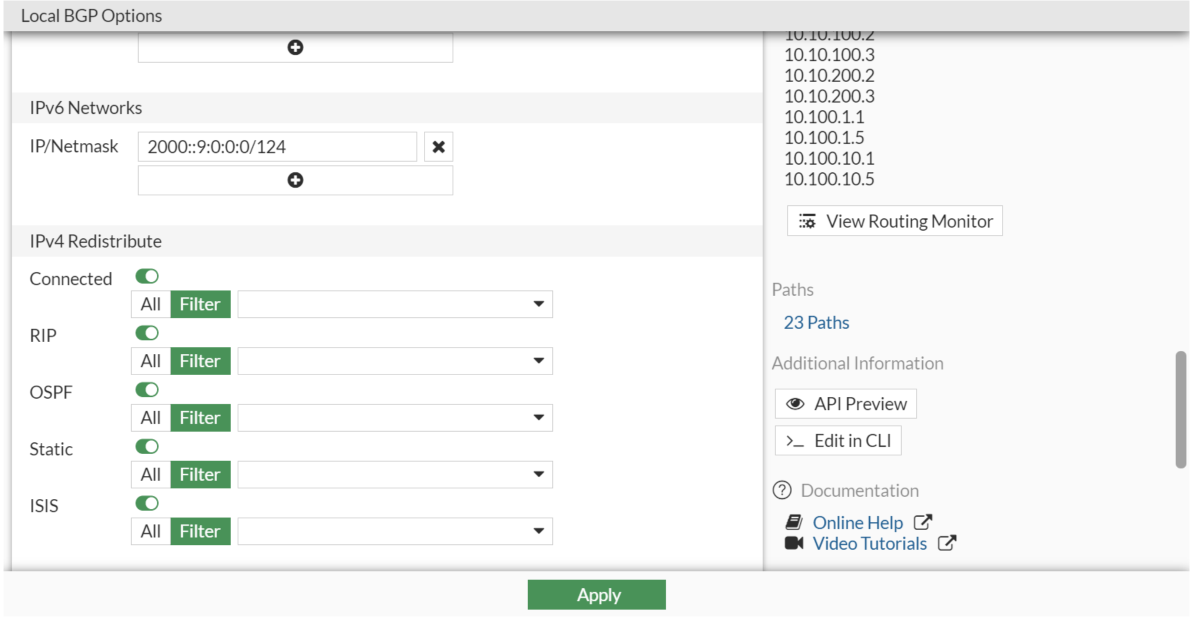
Paths

23 Paths

Additional Information

Documentation

There are settings for *IPv6 Networks* and *IPv4/IPv6 Redistribute* with filter options.



Local BGP Options

IPv6 Networks

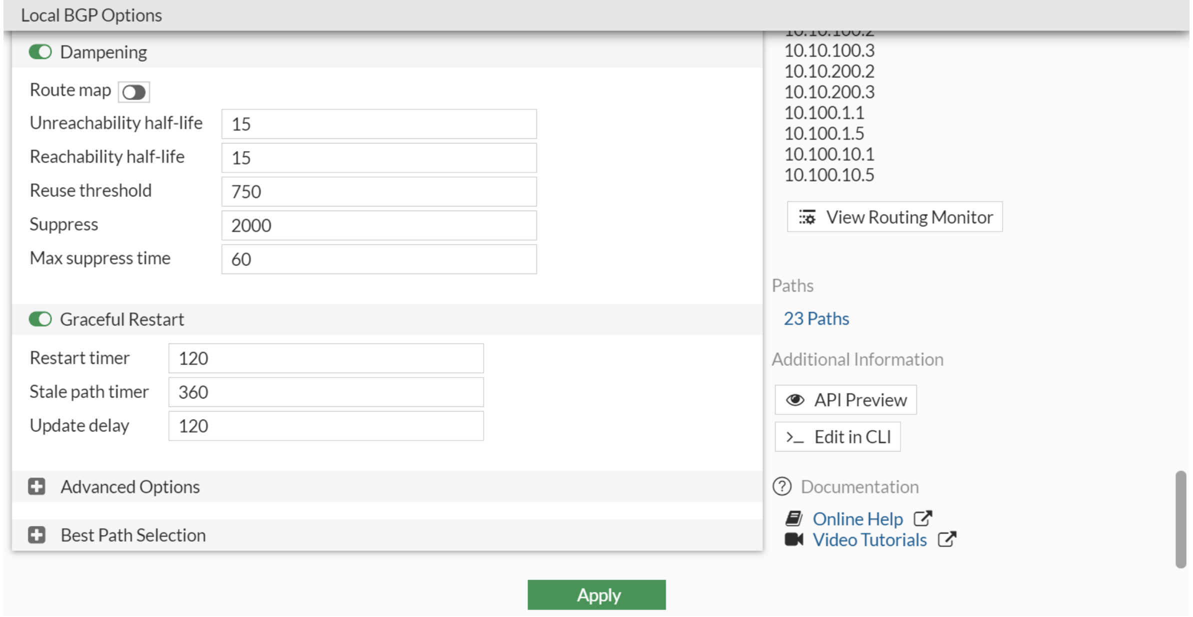
IP/Netmask: 2000::9:0:0:0/124

IPv4 Redistribute

Connected	●	All / Filter
RIP	●	All / Filter
OSPF	●	All / Filter
Static	●	All / Filter
ISIS	●	All / Filter

10.10.100.2
10.10.100.3
10.10.200.2
10.10.200.3
10.100.1.1
10.100.1.5
10.100.10.1
10.100.10.5

There are settings for *Dampening* and *Graceful restart*.



Local BGP Options

● Dampening

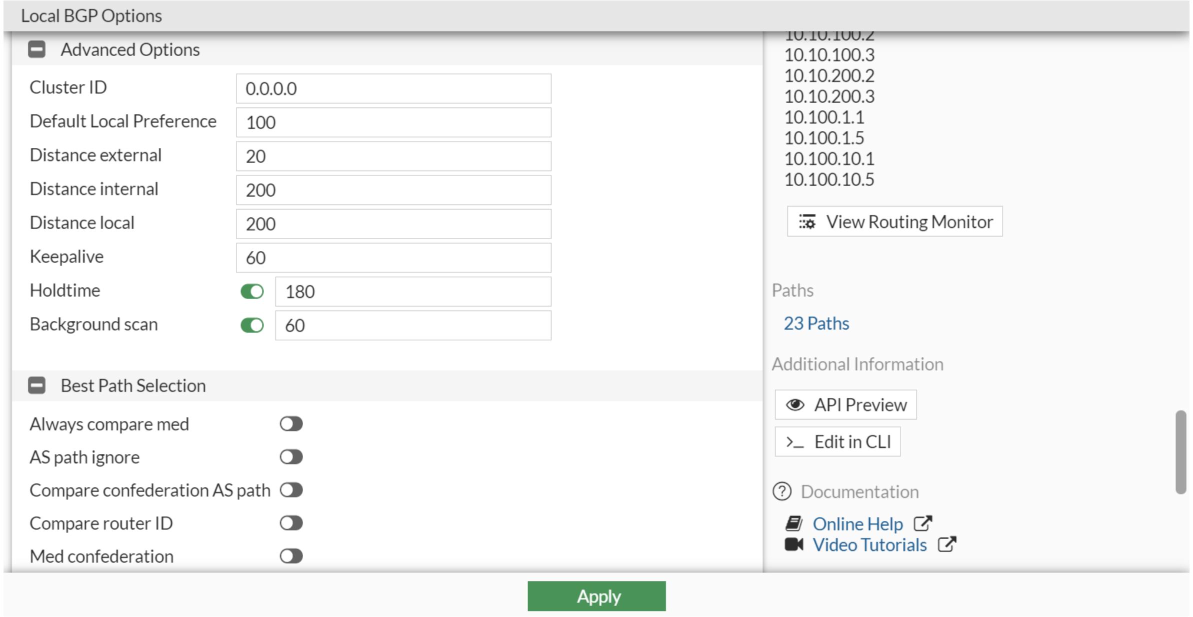
Route map	○
Unreachability half-life	15
Reachability half-life	15
Reuse threshold	750
Suppress	2000
Max suppress time	60

● Graceful Restart

Restart timer	120
Stale path timer	360
Update delay	120

10.10.100.2
10.10.100.3
10.10.200.2
10.10.200.3
10.100.1.1
10.100.1.5
10.100.10.1
10.100.10.5

Expand the *Advanced Options* and *Best Path Selection* sections to configure additional settings, such as *Default Local Preference*, *Distance external*, *Distance internal*, and *Distance local*.



Advanced Options

Cluster ID	0.0.0.0
Default Local Preference	100
Distance external	20
Distance internal	200
Distance local	200
Keepalive	60
Holdtime	180
Background scan	60

Best Path Selection

- Always compare med
- AS path ignore
- Compare confederation AS path
- Compare router ID
- Med confederation

10.10.100.2
10.10.100.3
10.10.200.2
10.10.200.3
10.100.1.1
10.100.1.5
10.100.10.1
10.100.10.5

Paths

23 Paths

Additional Information

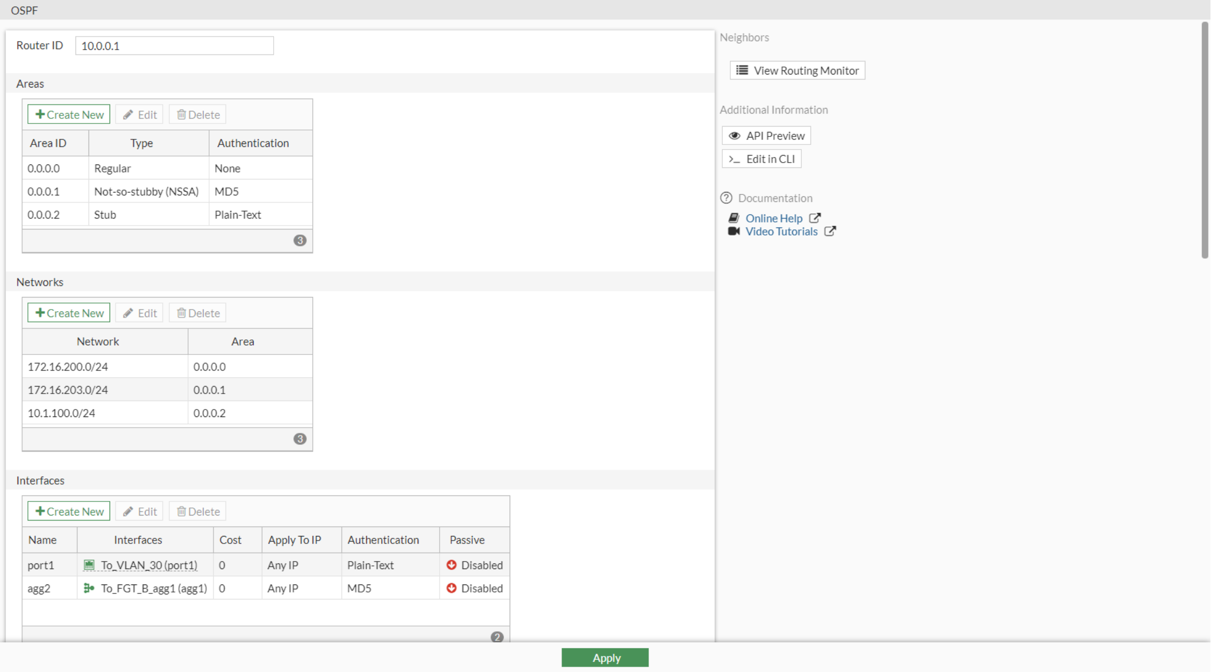
Documentation

GUI page for OSPF settings

Users can configure advanced OSPF routing options on the *Network* > *OSPF* page.

The OSPF page includes the following settings:

- Create new areas, networks, and interfaces.



Router ID 10.0.0.1

Areas

Area ID	Type	Authentication
0.0.0.0	Regular	None
0.0.0.1	Not-so-stubby (NSSA)	MD5
0.0.0.2	Stub	Plain-Text

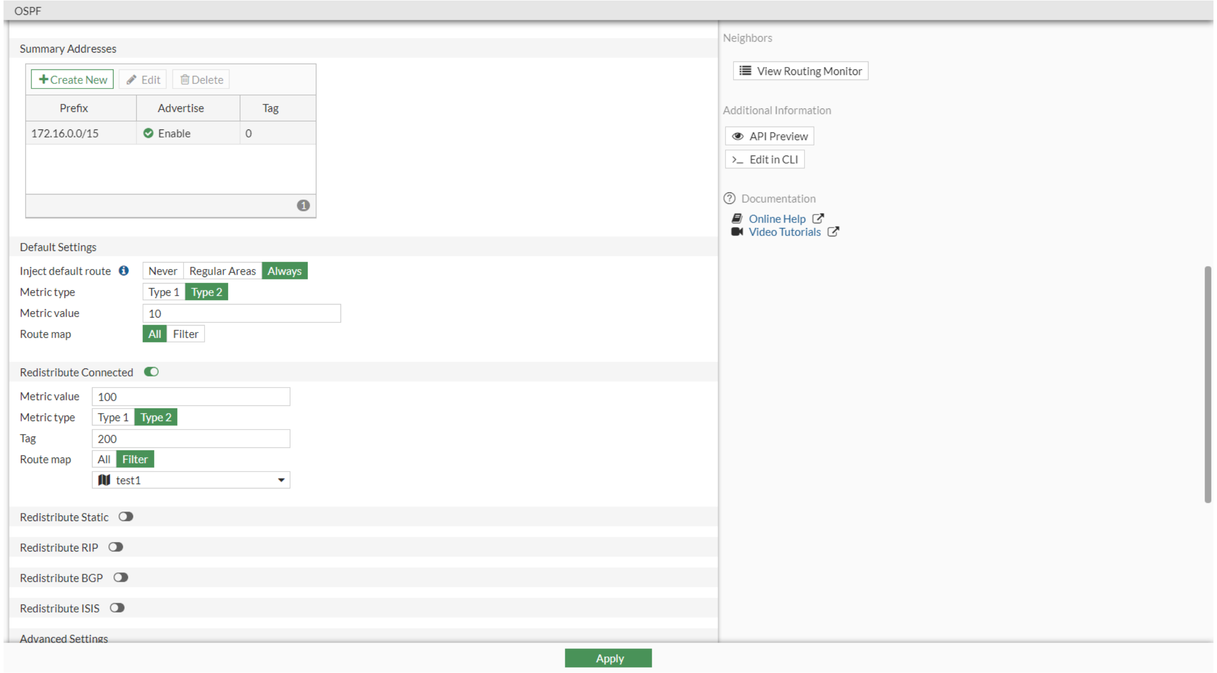
Networks

Network	Area
172.16.200.0/24	0.0.0.0
172.16.203.0/24	0.0.0.1
10.1.100.0/24	0.0.0.2

Interfaces

Name	Interfaces	Cost	Apply To IP	Authentication	Passive
port1	To_VLAN_30 (port1)	0	Any IP	Plain-Text	Disabled
agg2	To_FGT_B_agg1 (agg1)	0	Any IP	MD5	Disabled

- Create new IP address summary configurations.
- Edit the router default settings (metric type, metric value, and route map).
- Configure the redistribute attributes for each route type.



OSPF

Summary Addresses

Prefix	Advertise	Tag
172.16.0.0/15	Enable	0

Default Settings

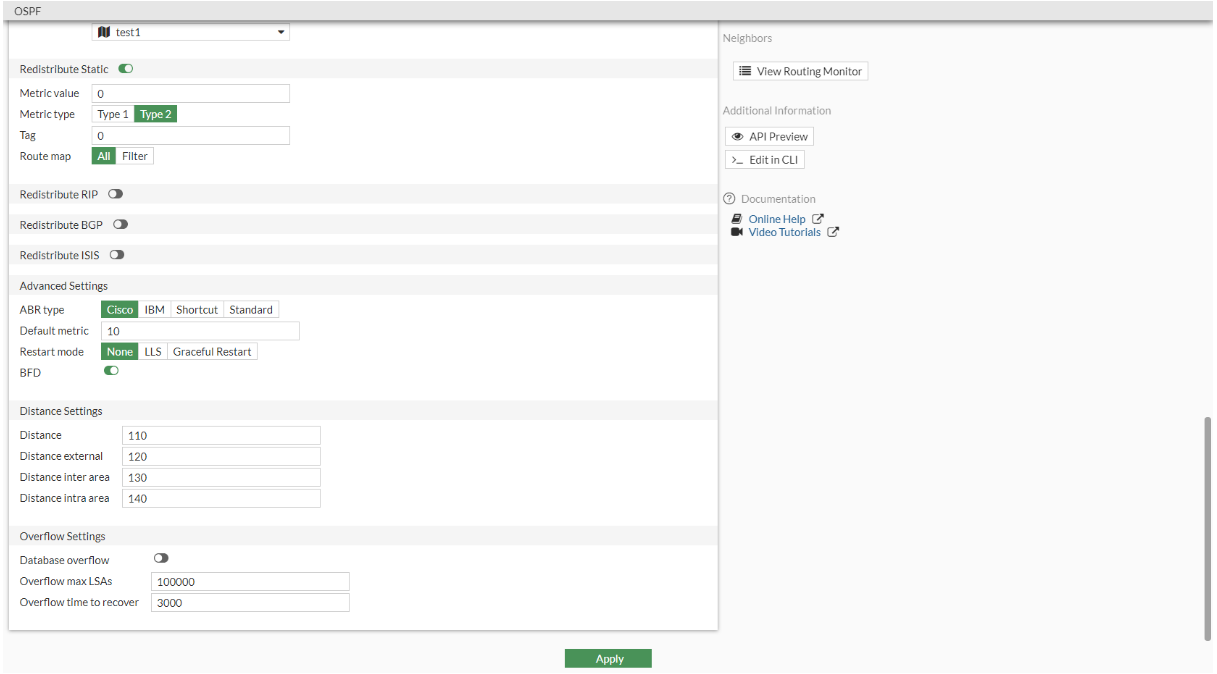
Inject default route: Always
Metric type: Type 2
Metric value: 10
Route map: All

Redistribute Connected (enabled)

Metric value: 100
Metric type: Type 2
Tag: 200
Route map: Filter
test1

Redistribute Static
Redistribute RIP
Redistribute BGP
Redistribute ISIS
Advanced Settings

- Configure advanced settings (ABR type, default metric, restart mode, and BFD).
- Configure distance and overflow settings.



OSPF

test1

Redistribute Static (enabled)

Metric value: 0
Metric type: Type 2
Tag: 0
Route map: All

Redistribute RIP
Redistribute BGP
Redistribute ISIS

Advanced Settings

ABR type: Cisco
Default metric: 10
Restart mode: None
BFD: enabled

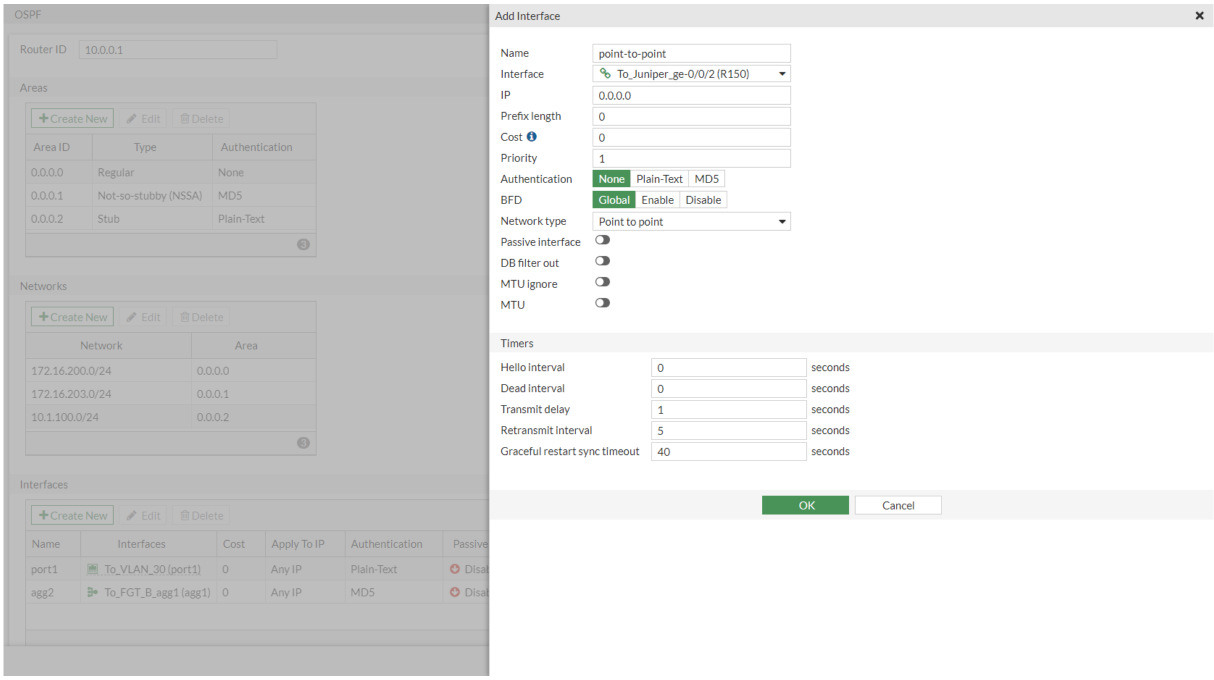
Distance Settings

Distance: 110
Distance external: 120
Distance inter area: 130
Distance intra area: 140

Overflow Settings

Database overflow: disabled
Overflow max LSAs: 100000
Overflow time to recover: 3000

- Configure advanced OSPF interface settings (prefix length, priority, BFD, network type, passive interface, DB filter out, MTU, MTU ignore, and so on).



OSPF

Router ID 10.0.0.1

Areas

Area ID	Type	Authentication
0.0.0.0	Regular	None
0.0.0.1	Not-so-stubby (NSSA)	MD5
0.0.0.2	Stub	Plain-Text

Networks

Network	Area
172.16.200.0/24	0.0.0.0
172.16.203.0/24	0.0.0.1
10.1.100.0/24	0.0.0.2

Interfaces

Name	Interfaces	Cost	Apply To IP	Authentication	Passive
port1	To_VLAN_30 (port1)	0	Any IP	Plain-Text	Disal
agg2	To_FGT_B_agg1 (agg1)	0	Any IP	MD5	Disal

Add Interface

Name	point-to-point
Interface	To_Juniper_ge-0/0/2 (R150)
IP	0.0.0.0
Prefix length	0
Cost	0
Priority	1
Authentication	[✓ None] Plain-Text MD5
BFD	[✓ Global] Enable Disable
Network type	Point to point
Passive interface	○
DB filter out	○
MTU ignore	○
MTU	○

Timers

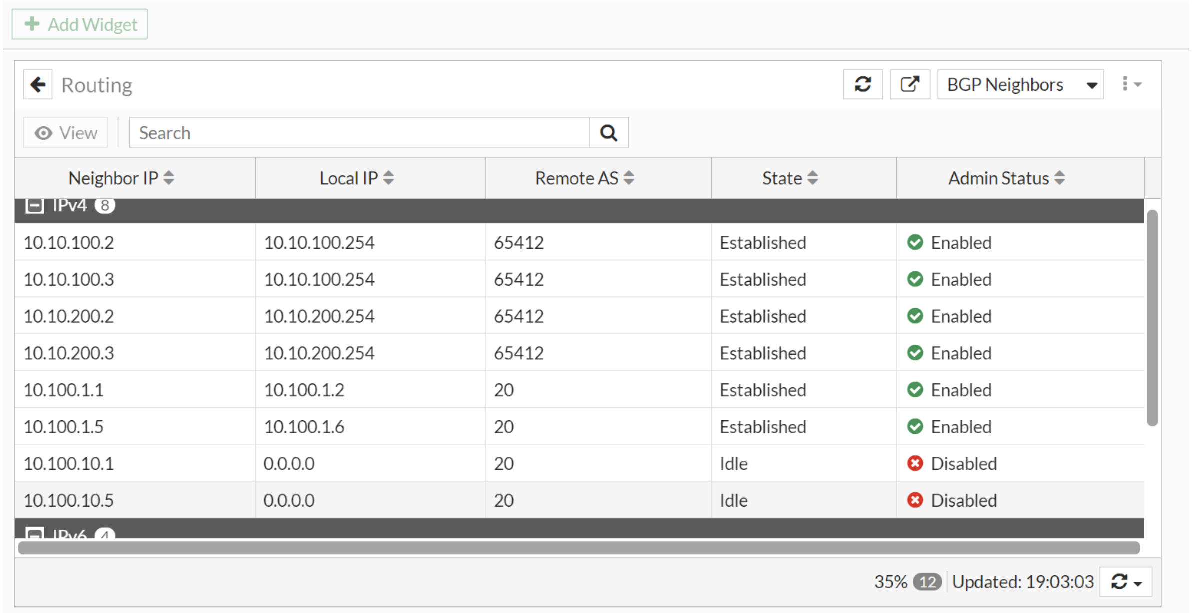
Hello interval	0	seconds
Dead interval	0	seconds
Transmit delay	1	seconds
Retransmit interval	5	seconds
Graceful restart sync timeout	40	seconds

GUI routing monitor for BGP and OSPF

BGP Neighbors, *BGP Paths*, and *OSPF Neighbors* data is visible in the *Routing* monitor widget.

To view the Routing widget:

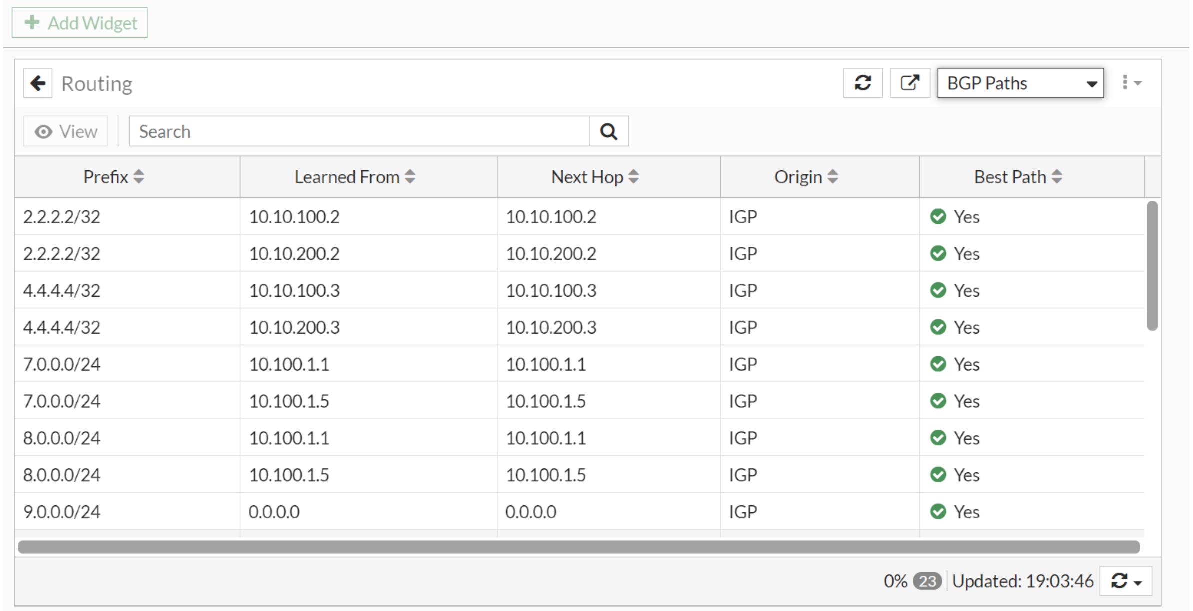
1. Go to *Dashboard* > *Network* and click the *Routing* widget.
2. Select one of the following options from the dropdown to view the data:
   a. *BGP Neighbors*



Neighbor IP	Local IP	Remote AS	State	Admin Status
IPv4 8				
10.10.100.2	10.10.100.254	65412	Established	✓ Enabled
10.10.100.3	10.10.100.254	65412	Established	✓ Enabled
10.10.200.2	10.10.200.254	65412	Established	✓ Enabled
10.10.200.3	10.10.200.254	65412	Established	✓ Enabled
10.100.1.1	10.100.1.2	20	Established	✓ Enabled
10.100.1.5	10.100.1.6	20	Established	✓ Enabled
10.100.10.1	0.0.0.0	20	Idle	✖ Disabled
10.100.10.5	0.0.0.0	20	Idle	✖ Disabled
IPv6 4				

35% 12 Updated: 19:03:03

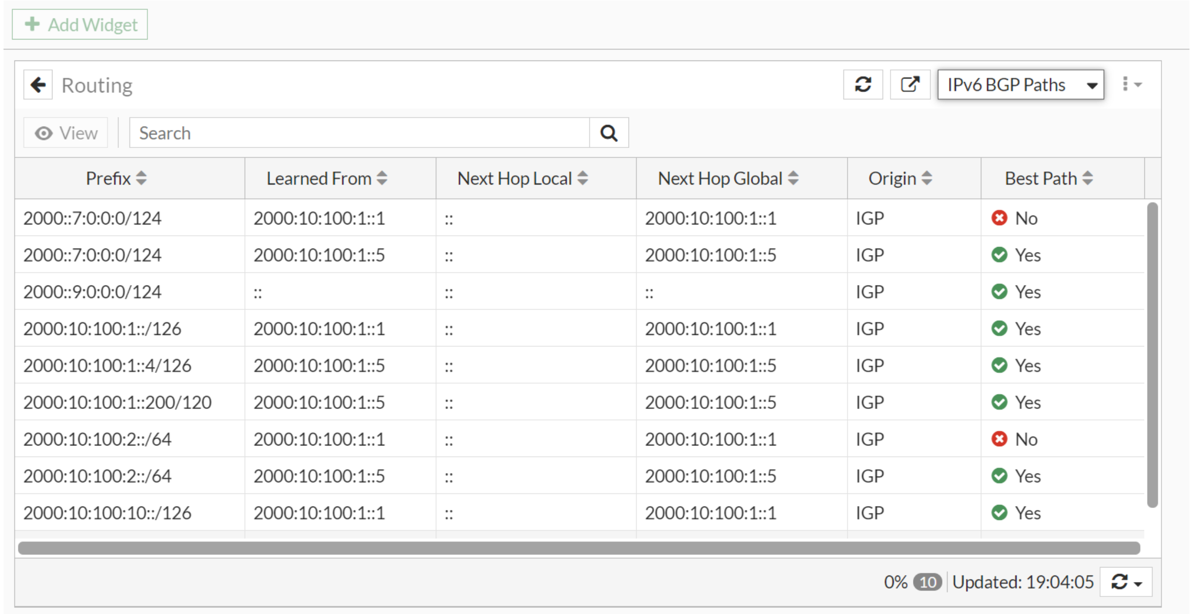
   b. *BGP Paths*



Prefix	Learned From	Next Hop	Origin	Best Path
2.2.2.2/32	10.10.100.2	10.10.100.2	IGP	✓ Yes
2.2.2.2/32	10.10.200.2	10.10.200.2	IGP	✓ Yes
4.4.4.4/32	10.10.100.3	10.10.100.3	IGP	✓ Yes
4.4.4.4/32	10.10.200.3	10.10.200.3	IGP	✓ Yes
7.0.0.0/24	10.100.1.1	10.100.1.1	IGP	✓ Yes
7.0.0.0/24	10.100.1.5	10.100.1.5	IGP	✓ Yes
8.0.0.0/24	10.100.1.1	10.100.1.1	IGP	✓ Yes
8.0.0.0/24	10.100.1.5	10.100.1.5	IGP	✓ Yes
9.0.0.0/24	0.0.0.0	0.0.0.0	IGP	✓ Yes

0% 23 Updated: 19:03:46

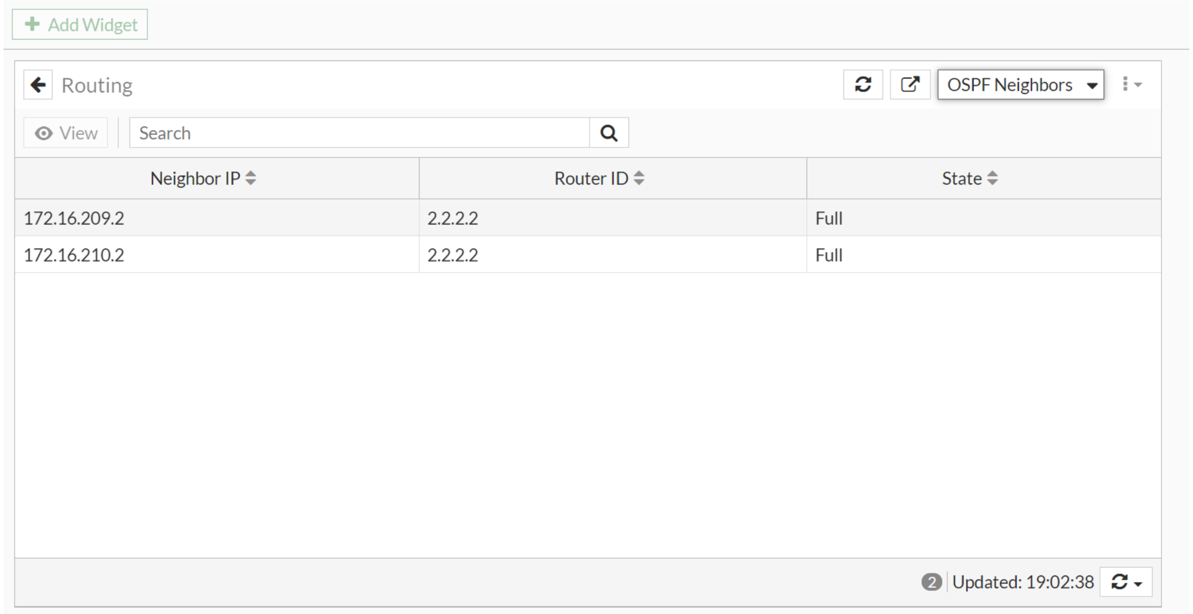
c. *IPv6 BGP Paths*



Prefix	Learned From	Next Hop Local	Next Hop Global	Origin	Best Path
2000::7:0:0:0/124	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✗ No
2000::7:0:0:0/124	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✓ Yes
2000::9:0:0:0/124	::	::	::	IGP	✓ Yes
2000:10:100:1::/126	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✓ Yes
2000:10:100:1::4/126	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✓ Yes
2000:10:100:1::200/120	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✓ Yes
2000:10:100:2::/64	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✗ No
2000:10:100:2::/64	2000:10:100:1::5	::	2000:10:100:1::5	IGP	✓ Yes
2000:10:100:10::/126	2000:10:100:1::1	::	2000:10:100:1::1	IGP	✓ Yes

0% 10 Updated: 19:04:05

d. *OSPF Neighbors*



Neighbor IP	Router ID	State
172.16.209.2	2.2.2.2	Full
172.16.210.2	2.2.2.2	Full

2 Updated: 19:02:38

SD-WAN steering

7.0.1

ECMP support for the longest match in SD-WAN rule matching - 7.0.1

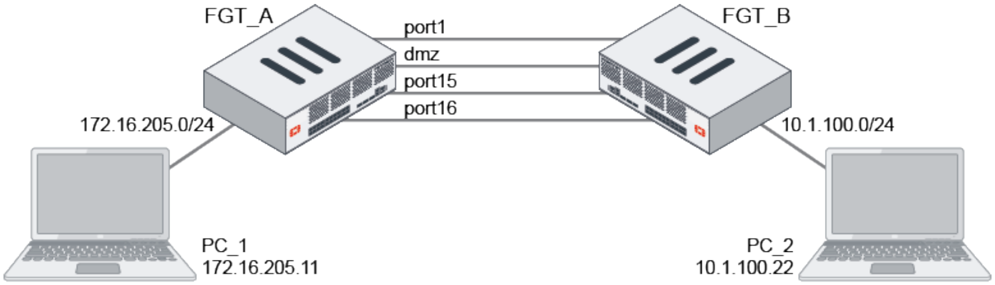
The longest match SD-WAN rule can match ECMP best routes. The rule will select the egress ports on ECMP specific routes, and not the less specific routes, to transport traffic.

The service mode determines which egress port on the ECMP specific routes is selected to forward traffic:

- Manual (`manual`): The first configured alive port is selected.
- Best Quality (`priority`): The best quality port is selected.
- Lowest Cost (`sla`): The first configured or lower cost port in SLA is selected.

Example

By default, SD-WAN selects the outgoing interface from all of the links that have valid routes to the destination. In some cases, it is required that only the links that have the best (or longest match) routes (single or ECMP) to the destination are considered.



In this example, four SD-WAN members in two zones are configured. The remote PC (PC_2 - 10.1.100.22) is accessible on port15 and port16, even though there are valid routes for all of the SD-WAN members. A single SD-WAN service rule is configured that allows traffic to balanced between all four of the members, but only chooses between port15 and port16 for the specific 10.1.100.22 address.

A performance SLA health check is configured to monitor 10.1.100.2. An SD-WAN service rule in Lowest Cost (SLA) mode is configured to select the best interface to steer the traffic. In the rule, the method of selecting a member if more than one meets the SLA (`tie-break`) is configured to select members that meet the SLA and match the longest prefix in the routing table (`fib-best-match`). If there are multiple ECMP routes with the same destination, the FortiGate will take the longest (or best) match in the routing table, and choose from those interface members.

To configure the SD-WAN:

```
config system sdwan
    config zone
        edit "virtual-wan-link"
        next
        edit "z1"
        next
    end
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.200.2
        next
        edit 2
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 3
            set interface "port15"
            set zone "z1"
            set gateway 172.16.209.2
        next
        edit 4
            set interface "port16"
            set zone "z1"
            set gateway 172.16.210.2
        next
    end
    config health-check
        edit "1"
            set server "10.1.100.2"
            set members 0
            config sla
                edit 1
                next
            end
        next
    end
    config service
        edit 1
            set name "1"
            set mode sla
            set dst "all"
            set src "172.16.205.0"
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2 3 4
            set tie-break fib-best-match
        next
    end
end
```

To check the results:

1. The debug shows the SD-WAN service rule. All of the members meet SLA, and because no specific costs are attached to the members, the egress interface is selected based on the interface priority order that is configured in the rule:

   ```
   FGT_A (root) # diagnose sys sdwan service

   Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
     Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
     Members(4):
       1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
       2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
       3: Seq_num(3 port15), alive, sla(0x1), gid(0), cfg_order(2), cost(0), selected
       4: Seq_num(4 port16), alive, sla(0x1), gid(0), cfg_order(3), cost(0), selected
     Src address(1):
           172.16.205.0-172.16.205.255
     Dst address(1):
           0.0.0.0-255.255.255.255
   ```

2. The routing table shows that there are ECMP default routes on all of the members, and ECMP specific (or best) routes only on port15 and port16:

   ```
   FGT_A (root) # get router info routing-table static
   Routing table for VRF=0
   S*      0.0.0.0/0 [1/0] via 172.16.200.2, port1
                            [1/0] via 172.16.208.2, dmz
                            [1/0] via 172.16.209.2, port15
                            [1/0] via 172.16.210.2, port16
   S       10.1.100.22/32 [10/0] via 172.16.209.2, port15
                                     [10/0] via 172.16.210.2, port16
   ```

   Because `tie-break` is set to `fib-best-match`, the first configured member from port15 and port16 is selected to forward traffic to PC_2. For all other traffic, the first configured member from all four of the interfaces is selected to forward traffic.

3. On PC-1, generate traffic to PC-2:

   ```
   ping 10.1.100.22
   ```

4. On FGT_A, sniff for traffic sent to PC_2:

   ```
   # diagnose sniffer packet any 'host 10.1.100.22' 4
   interfaces=[any]
   filters=[host 10.1.100.22]
   2.831299 port5 in 172.16.205.11 -> 10.1.100.22: icmp: echo request
   2.831400 port15 out 172.16.205.11 -> 10.1.100.22: icmp: echo request
   ```

   Traffic is leaving on port15, the first configured member from port15 and port16.

Override quality comparisons in SD-WAN longest match rule matching - 7.0.1

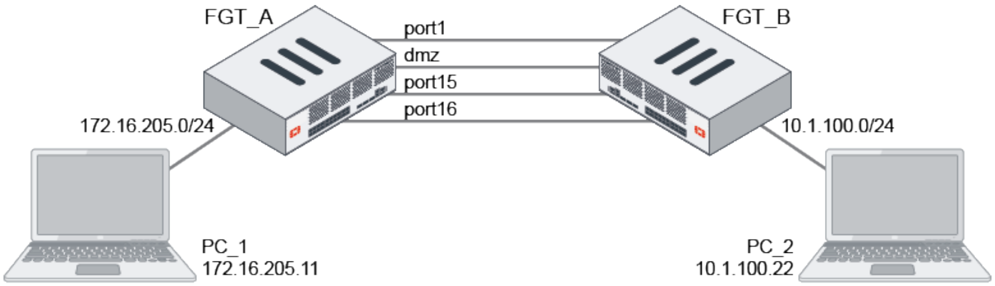
In SD-WAN rules, the longest match routes will override the quality comparisons when all of the specific routes are out of SLA.

With this feature in an SD-WAN rule:

- Lowest Cost (`sla`): Even though all of the egress ports on specific routes (longest matched routes) are out of SLA, the SD-WAN rule still selects the first configured or lower-cost port from the egress ports to forward traffic.
- Best Quality (`priority`): Even though the egress ports on specific routes (longest matched routes) have worse quality that all other ports on less specific routes, the SD-WAN rule still selects the best quality port from the ports on specific routes to forward traffic.

This features avoids a situation where, if the members on specific routes (longest matched routes) are out of SLA or have worse quality, the traffic might be forwarded to the wrong members in SLA (higher quality) on the default or aggregate routes.

Example



In this example, four SD-WAN members in two zones are configured. The remote PC (PC_2 - 10.1.100.22) is accessible on port15 and port16, even though there are valid routes for all of the SD-WAN members. A single SD-WAN service rule is configured that allows traffic to balanced between all four of the members, but only chooses between port15 and port16 for the specific 10.1.100.22 address. If neither port15 nor port16 meet the SLAs, traffic will be forwarded on one of these interfaces, instead of on port1 or dmz.

A performance SLA health check is configured to monitor 10.1.100.2. An SD-WAN service rule in Lowest Cost (SLA) mode is configured to select the best interface to steer the traffic. In the rule, the method of selecting a member if more than one meets the SLA (`tie-break`) is configured to select members that meet the SLA and match the longest prefix in the routing table (`fib-best-match`). If there are multiple ECMP routes with the same destination, the FortiGate will take the longest (or best) match in the routing table, and choose from those interface members.

To configure the SD-WAN:

```
config system sdwan
    config zone
        edit "virtual-wan-link"
        next
        edit "z1"
        next
    end
    config members
        edit 1
            set interface "port1"
            set gateway 172.16.200.2
        next
        edit 2
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 3
            set interface "port15"
            set zone "z1"
            set gateway 172.16.209.2
        next
        edit 4
            set interface "port16"
            set zone "z1"
            set gateway 172.16.210.2
        next
    end
    config health-check
        edit "1"
            set server "10.1.100.2"
            set members 0
            config sla
                edit 1
                next
            end
        next
    end
    config service
        edit 1
            set name "1"
            set mode sla
            set dst "all"
            set src "172.16.205.0"
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2 3 4
            set tie-break fib-best-match
        next
    end
end
```

To check the results:

1. The debug shows the SD-WAN service rule. Both port15 and port16 are up, but out of SLA:

```
FGT_A (root) # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(4):
    1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
    2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 port15), alive, sla(0x0), gid(0), cfg_order(2), cost(0), selected
    4: Seq_num(4 port16), alive, sla(0x0), gid(0), cfg_order(3), cost(0), selected
  Src address(1):
        172.16.205.0-172.16.205.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

2. The routing table shows that there are ECMP default routes on all of the members, and ECMP specific (or best) routes only on port15 and port16:

   ```
   FGT_A (root) # get router info routing-table static
   Routing table for VRF=0
   S*      0.0.0.0/0 [1/0] via 172.16.200.2, port1
                         [1/0] via 172.16.208.2, dmz
                         [1/0] via 172.16.209.2, port15
                         [1/0] via 172.16.210.2, port16
   S       10.1.100.22/32 [10/0] via 172.16.209.2, port15
                                  [10/0] via 172.16.210.2, port16
   ```

   Because `tie-break` is set to `fib-best-match`, even though both port15 and port16 are out of SLA, the first configured member of the two (port15) is selected to forward traffic to PC_2. For all other traffic, the first configured member from all of the interfaces that are in SLA is selected to forward traffic (port1).
3. On PC-1, generate traffic to PC-2:

   ```
   ping 10.1.100.22
   ```
4. On FGT_A, sniff for traffic sent to PC_2:

   ```
   # diagnose sniffer packet any 'host 10.1.100.22' 4
   interfaces=[any]
   filters=[host 10.1.100.22]
   2.831299 port5 in 172.16.205.11 -> 10.1.100.22: icmp: echo request
   2.831400 port15 out 172.16.205.11 -> 10.1.100.22: icmp: echo request
   ```

   Traffic is leaving on port15, the first configured member from port15 and port16, even though both are out of SLA.

Specify an SD-WAN zone in static routes and SD-WAN rules - 7.0.1

SD-WAN zones can be used in IPv4 and IPv6 static routes, and in SD-WAN service rules. This makes route configuration more flexible, and simplifies SD-WAN rule configuration. The `sdwan-zone` command replaces the `sdwan {enable | disable}` command.

A new predefined SD-WAN zone called *SASE* is also available.

To configure an SD-WAN zone in a static route:

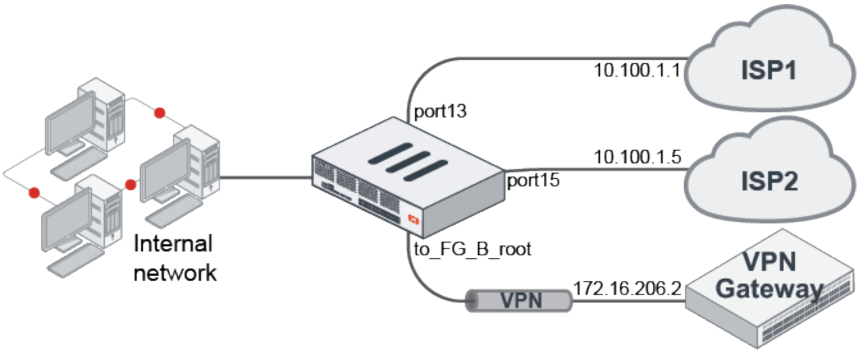
```
config router {static | static6}
    edit 1
        set sdwan-zone <zone> <zone> ...
    next
end
```

To configure an SD-WAN zone in an SD-WAN rule:

```
config system sdwan
    config service
        edit 1
            set priority-zone <zone>
        next
    end
end
```

Examples

In these two examples, three SD-WAN members are created. Two members, port13 and port15, are in the default zone (*virtual-wan-link*), and the third member, to_FG_B_root, is in the *SASE* zone.



Example 1

In this example:

- Two service rules are created. Rule 1 uses the *virtual-wan-link* zone, and rule 2 uses the *SASE* zone.
- Two IPv4 static routes are created. The first route uses the *virtual-wan-link* zone, and the second route uses the *SASE* zone.

To configure the SD-WAN:

1. Assign port13 and port15 to the *virtual-wan-link* zone and to_FG_B_root to the *SASE* zone:

```
config system sdwan
    set status enable
    config members
        edit 1
            set interface "port13"
            set zone "virtual-wan-link"
            set gateway 10.100.1.1
        next
        edit 2
            set interface "port15"
            set zone "virtual-wan-link"
            set gateway 10.100.1.5
        next
        edit 3
            set interface "to_FG_B_root"
            set zone "SASE"
        next
    end
end
```

2. Create two service rules, one for each SD-WAN zone:

```
config system sdwan
    config service
        edit 1
```

```
            set dst "10.100.20.0"
            set priority-zone "virtual-wan-link"
        next
        edit 2
            set internet-service enable
            set internet-service-name "Fortinet-FortiGuard"
            set priority-zone "SASE"
        next
    end
end
```

3. Configure static routes for each of the SD-WAN zones:

```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
    edit 2
        set dst 172.16.109.0 255.255.255.0
        set distance 1
        set sdwan-zone "SASE"
    next
end
```

To verify the results:

1. Check the service rule 1 diagnostics:

```
# diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port13), alive, selected
    2: Seq_num(2 port15), alive, selected
  Dst address(1):
        10.100.20.0-10.100.20.255
```

Both members of the *virtual-wan-link* zone are selected. In manual mode, the interface members are selected based on the member configuration order. In SLA and priority mode, the order depends on the link status. If all of the link statuses pass, then the members are selected based on the member configuration order.

2. Check the service rule 2 diagnostics:

```
# diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(1):
    1: Seq_num(3 to_FG_B_root), alive, selected
  Internet Service(1): Fortinet-FortiGuard(1245324,0,0,0)
```

The member of the *SASE* zone is selected.

3. Review the routing table:

```
# get router info routing-table static
Routing table for VRF=0
```

```
S*      0.0.0.0/0 [1/0] via 10.100.1.1, port13
                  [1/0] via 10.100.1.5, port15
S       172.16.109.0/24 [1/0] via 172.16.206.2, to_FG_B_root
```

The default gateway has the members from the *virtual-wan-link* zone, and the route to 172.16.10.9.0/24 has the single member from the *SASE* zone.

Example 2

In this example, two IPv6 static routes are created. The first route uses the *virtual-wan-link* zone, and the second route uses the *SASE* zone.

To configure the SD-WAN:

1. Configure port13 and port15 with IPv6 addresses and assign them to the *virtual-wan-link* zone, and assign to_FG_B_root to the *SASE* zone:

```
config system sdwan
    set status enable
    config members
        edit 1
            set interface "port13"
            set zone "virtual-wan-link"
            set gateway6 2004:10:100:1::1
            set source6 2004:10:100:1::2
        next
        edit 2
            set interface "port15"
            set zone "virtual-wan-link"
            set gateway6 2004:10:100:1::5
            set source6 2004:10:100:1::6
        next
        edit 3
            set interface "to_FG_B_root"
            set zone "SASE"
        next
    end
end
```

2. Configure IPv6 static routes for each of the SD-WAN zones:

```
config router static6
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
    edit 2
        set dst 2003:172:16:109::/64
        set distance 1
        set sdwan-zone "SASE"
    next
end
```

To verify the results:

1. Review the routing table:

```
# get router info6 routing-table static
Routing table for VRF=0
S*      ::/0 [1/0] via 2004:10:100:1::1, port13, 00:20:51, [1024/0]
             [1/0] via 2004:10:100:1::5, port15, 00:20:51, [1024/0]
S       2003:172:16:109::/64 [1/0] via ::ac10:ce02, to_FG_B_root, 00:20:51, [1024/0]
S       2003:172:16:209::/64 [5/0] via ::ac10:ce02, to_FG_B_root, 14:40:14, [1024/0]
```

The IPv6 default route includes the members from the *virtual-wan-link* zone, and the route to 2003:172:16:109::/64 has the single member from the *SASE* zone.

WAN remediation

7.0.0

- Packet duplication for dial-up IPsec tunnels on page 119

7.0.2

- Adaptive Forward Error Correction 7.0.2 on page 123

Packet duplication for dial-up IPsec tunnels

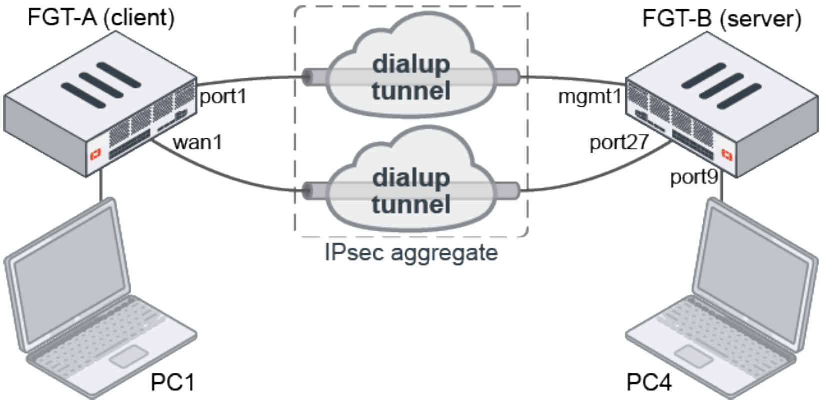
To support packet duplication on dial-up IPsec tunnels between sites, each spoke must be configured with a location ID. On the hub, packet duplication is performed on the tunnels in the IPsec aggregate that have the same location ID.

Multiple dial-up VPN tunnels from the same location can be aggregated on the VPN hub and load balanced based on the configured load balance algorithm.

IPsec traffic cannot be offloaded to the NPU.

Example

In this example, an IPsec aggregate tunnel is formed between two dial-up IPsec tunnels in order to support packet duplication.



To configure the client FortiGate (FGT-A):

1. Configure the IPsec tunnels:

```
config vpn ipsec phase1-interface
    edit "client1"
        set interface "port1"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.200.4
        set psksecret **********
    next
    edit "client2"
        set interface "wan1"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 173.1.1.1
        set psksecret **********
    next
end
```

2. Configure an aggregate of the IPsec tunnels:

```
config system ipsec-aggregate
    edit "agg1"
        set member "client1" "client2"
    next
end
```

3. Configure the location ID:

```
config system settings
    set location-id 1.1.1.1
end
```

To configure the server FortiGate (FGT-B):

1. Configure the IPsec tunnels:

```
config vpn ipsec phase1-interface
    edit "server1"
        set type dynamic
        set interface "mgmt1"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set psksecret ***********
        set dpd-retryinterval 60
    next
    edit "server2"
        set type dynamic
        set interface "port27"
        set peertype any
        set net-device disable
        set aggregate-member enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set psksecret **********
        set dpd-retryinterval 60
    next
end
```

```
config vpn ipsec phase2-interface
    edit "server1"
        set phase1name "server1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm 
aes256gcm chacha20poly1305
    next
    edit "server2"
        set phase1name "server2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm 
aes256gcm chacha20poly1305
    next
end
```

2. Configure an aggregate of the IPsec tunnels:

```
config system ipsec-aggregate
    edit "server"
        set member "server1" "server2"
    next
end
```

3. Configure a firewall policy:

```
config firewall policy
    edit 1
        set srcintf "server"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

To check the IPsec tunnel and aggregate state:

1. List all of the VPN tunnels:

```
FGDocs # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=server1 ver=1 serial=1 172.16.200.4:500->0.0.0.0:500 tun_id=1.0.0.0 dst_mtu=0 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=4 lgwy=static/1 tun=tunnel/15 mode=dialup/2 encap=none/4616 options[1208]=npu 
frag-rfc  accept_traffic=1 overlay_id=0

proxyid_num=0 child_num=2 refcnt=4 ilast=14210 olast=14210 ad=/0
stat: rxp=798921 txp=819074 rxb=121435992 txb=68802216
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=server2 ver=1 serial=2 173.1.1.1:500->0.0.0.0:500 tun_id=2.0.0.0 dst_mtu=0 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=17 lgwy=static/1 tun=tunnel/15 mode=dialup/2 encap=none/4616 options[1208]=npu 
frag-rfc  accept_traffic=1 overlay_id=0
```

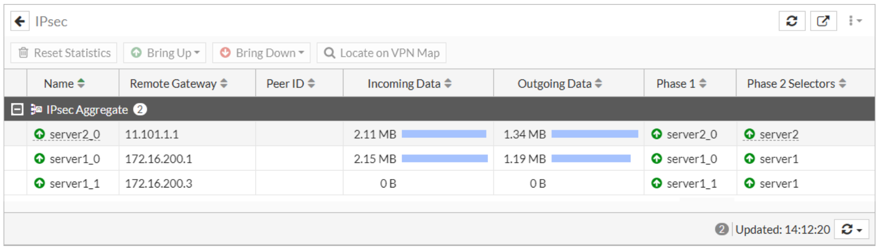
```
proxyid_num=0 child_num=1 refcnt=3 ilast=14177 olast=14177 ad=/0
stat: rxp=836484 txp=819111 rxb=137429352 txb=80046050
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=server1_0 ver=1 serial=8 172.16.200.4:500->172.16.200.1:500 tun_id=172.16.200.1
dst_mtu=1500 dpd-link=on remote_location=1.1.1.1 weight=1
bound_if=4 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/4744 options
[1288]=npu rgwy-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0

parent=server1 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=45 olast=45 ad=/0
stat: rxp=17176 txp=17176 rxb=2610752 txb=1442784
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=12
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=server1 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.1.100.0-10.1.100.255:0
  SA:  ref=3 options=2a6 type=00 soft=0 mtu=1438 expire=42342/0B replaywin=2048
       seqno=4319 esn=0 replaywin_lastseq=00004319 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43186/43200
  dec: spi=0aef2a07 esp=aes key=16 12738c8a1db02c23bfed73eb3615a5a1
       ah=sha1 key=20 0f3edd28e3165d184292b4cd397a6edeef9d20dc
  enc: spi=2cb75665 esp=aes key=16 982b418e40f0bb18b89916d8c92270c0
       ah=sha1 key=20 08cbf9bf78a968af5cd7647dfa2a0db066389929
  dec:pkts/bytes=17176/1442784, enc:pkts/bytes=17176/2610752
  npu_flag=00 npu_rgwy=172.16.200.1 npu_lgwy=172.16.200.4 npu_selid=6 dec_npuid=0 enc_
npuid=0
------------------------------------------------------
name=server1_1 ver=1 serial=a 172.16.200.4:500->172.16.200.3:500 tun_id=172.16.200.3
dst_mtu=0 dpd-link=on remote_location=2.2.2.2 weight=1
bound_if=4 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/4744 options
[1288]=npu rgwy-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0

parent=server1 index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=27 olast=27 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=server1 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=2a6 type=00 soft=0 mtu=1280 expire=43167/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=0aef2a0a esp=aes key=16 4b7a17ba9d239e4ae5fe95ec100fca8b
       ah=sha1 key=20 7d3e058088f21e0c4f1c13c297293f06c8b592e7
  enc: spi=7e961809 esp=aes key=16 ecd1aa8657c5a509662aed45002d3990
       ah=sha1 key=20 d159e06c1cf0ded18a4e4ac86cbe5aa0315c21c9
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=172.16.200.3 npu_lgwy=172.16.200.4 npu_selid=9 dec_npuid=0 enc_
npuid=0
------------------------------------------------------
name=server2_0 ver=1 serial=7 173.1.1.1:500->11.101.1.1:500 tun_id=11.101.1.1 dst_
mtu=1500 dpd-link=on remote_location=1.1.1.1 weight=1
```

```
bound_if=17 lgwy=static/1 tun=tunnel/15 mode=dial_inst/3 encap=none/4744 options
[1288]=npu rgwy-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0

parent=server2 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=45 olast=45 ad=/0
stat: rxp=16001 txp=17179 rxb=2113664 txb=1594824
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=12
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=server2 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.1.100.0-10.1.100.255:0
  SA:  ref=6 options=2a6 type=00 soft=0 mtu=1438 expire=42342/0B replaywin=2048
       seqno=431a esn=0 replaywin_lastseq=00003e80 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43185/43200
  dec: spi=0aef2a08 esp=aes key=16 394d4e444e90ccb5184e744d49aabe3c
       ah=sha1 key=20 faabea35c2b9b847461cbd263c4856cfb679f342
  enc: spi=2cb75666 esp=aes key=16 0b3a2fbac4d5610670843fa1925d1207
       ah=sha1 key=20 97e99beff3d8f61a8638f6ef887006a9c323acd4
  dec:pkts/bytes=16001/2113596, enc:pkts/bytes=17179/2762792
  npu_flag=03 npu_rgwy=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=7 dec_npuid=1 enc_npuid=1
```

2. List the IPsec aggregate members:

```
# diagnose sys ipsec-aggregate list
server
members(3):
        server1_1
        server1_0
        server2_0
```

3. In the GUI, go to *Dashboard* > *Network* and expand the *IPsec* widget to review the traffic distributed over the aggregate members:



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
IPsec Aggregate 2						
server2_0	11.101.1.1		2.11 MB	1.34 MB	server2_0	server2
server1_0	172.16.200.1		2.15 MB	1.19 MB	server1_0	server1
server1_1	172.16.200.3		0 B	0 B	server1_1	server1

Adaptive Forward Error Correction - 7.0.2

Forward Error Correction (FEC) is used to control and correct errors in data transmission by sending redundant data across the VPN in anticipation of dropped packets occurring during transit. The mechanism sends out *x* number of redundant packets for every *y* number of base packets.

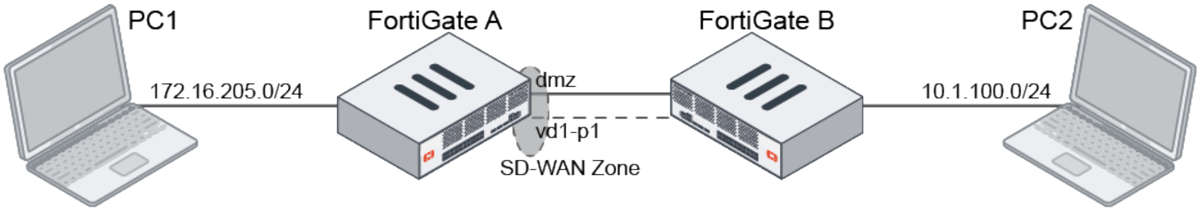
Adaptive FEC considers link conditions and dynamically adjusts the FEC packet ratio:

- The FEC base and redundant packet relationship is dynamically adjusted based on changes to the network SLA metrics defined in the SD-WAN SLA health checks. For example, when there is no or low packet loss in the network, FEC can work on a low redundant level sending only one redundant packet for every 10 base packets. As packet loss increases, the number of redundant packets sent can rise accordingly.

- FEC can be applied only to streams that are sensitive to packet loss. For Example, policies that allow the UDP based VoIP protocol can enable FEC, while TCP based traffic policies do not. This reduces unnecessary bandwidth consumption by FEC.
- Because FEC does not support NPU offloading, the ability to specify streams and policies that do not require FEC allows those traffic to be offloaded. This means that all traffic suffers a performance impact.

In this example, an IPsec tunnel is configured between two FortiGates that both have FEC enabled. The tunnel is an SD-WAN zone, and an SLA health-check is used to monitor the quality of the VPN overlay. The intention is to apply FEC to UDP traffic that is passing through the VPN overlay, while allowing all other traffic to pass through without FEC. An FEC profile is configured to adaptively increase redundant levels if the link quality exceeds a 10% packet loss threshold, or the bandwidth exceeds 950 Mbps.

The DMZ interface and IPsec tunnel vd1-p1 are SD-WAN members. FEC is enabled on vd1-p1, and health-check works on vd1-p1.



To configure the FortiGates:

1. On both FortiGates, enable FEC and NPU offloading on the IPsec tunnel vd1-p1:

```
config vpn ipsec phase1-interface
    edit "vd1-p1"
        set npu-offload enable
        set fec-egress enable
        set fec-ingress enable
    next
end
```

2. On FortiGate A, configure SD-WAN:

   The VPN overlay member (vd1-p1) must be included in the health-check and configured as the higher priority member in the SD-WAN rule.

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "dmz"
            set gateway 172.16.208.2
        next
        edit 2
            set interface "vd1-p1"
        next
    end
```

```
        config health-check
            edit "1"
                set server "2.2.2.2"
                set members 2
                config sla
                    edit 1
                    next
                end
            next
        end
        config service
            edit 1
                set name "1"
                set dst "all"
                set src "172.16.205.0"
                set priority-members 2 1
            next
        end
    end
```

3. On FortiGate A, create a policy to specify performing FEC on UDP traffic, and a policy for other traffic:

```
config firewall policy
    edit 1
        set srcintf "port5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "172.16.205.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL_UDP"
        set fec enable
    next
    edit 2
        set srcintf "any"
        set dstintf "any"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

4. On FortiGate A, configure FEC mapping to bind network SLA metrics and FEC base and redundant packets:

```
config vpn ipsec fec
    edit "m1"
        config mappings
            edit 1
                set base 8
                set redundant 2
                set packet-loss-threshold 10
            next
            edit 2
                set base 9
                set redundant 3
                set bandwidth-up-threshold 950000
            next
        end
    next
end
```

The mappings are matched from top to bottom: packet loss greater than 10% with eight base and two redundant packets, and then uploading bandwidth greater than 950 Mbps with nine base and three redundant packets.

5. On FortiGate A, apply the FEC mappings on vd1-p1:

```
config vpn ipsec phase1-interface
    edit "vd1-p1"
        set fec-health-check "1"
        set fec-mapping-profile "m1"
        set fec-base 10
        set fec-redundant 1
    next
end
```

The FEC base and redundant values are used when the link quality has not exceeded the limits specified in the FEC profile mapping. If `fec-codec` is set to `xor` the base and redundant packet values will not be updated.

To verify the results:

1. Send TCP and UDP traffic from PC1 to PC2, then check the sessions on FortiGate A:

```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=12 expire=3587 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=112/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=15->102/102->15
gwy=172.16.209.2/172.16.205.11
hook=pre dir=org act=noop 172.16.205.11:39176->10.1.100.22:5001(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.22:5001->172.16.205.11:39176(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=719 auth_info=0 chk_client_info=0 vd=0
serial=00020f7a tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x5000c00
npu info: flag=0x82/0x81, offload=8/8, ips_offload=0/0, epid=249/74, ipid=74/86,
vlan=0x0000/0x0000
vlifid=74/249, vtag_in=0x0000/0x0001 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=5/5

session info: proto=17 proto_state=00 duration=0 expire=180 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty fec
statistic(bytes/packets/allow_err): org=100366/67/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=15->102/102->15 gwy=172.16.209.2/0.0.0.0
hook=pre dir=org act=noop 172.16.205.11:49052->10.1.100.22:5001(0.0.0.0:0)
hook=post dir=reply act=noop 10.1.100.22:5001->172.16.205.11:49052(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=593 auth_info=0 chk_client_info=0 vd=0
serial=000210fa tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x5040000
no_ofld_reason:  non-npu-intf
```

Non-FEC protected TCP traffic is offloaded, while FEC protected UDP traffic is not offloaded

2. On FortiGate A, check the health-check result and the corresponding FEC base and redundant packets:

```
# diagnose sys sdwan health-check
Health Check(1):
Seq(2 vd1-p1): state(alive), packet-loss(0.000%) latency(0.168), jitter(0.021),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x1
```

Because bandwidth-up is more than 950000kbps, base and redundant are set to 9 and 3:

```
# diagnose vpn tunnel fec vd1-p1
egress:
    enabled=1 base=9 redundant=3 codec=0 timeout=10(ms)
    encode=6621 encode_timeout=6621 encode_fail=0
    tx_data=6880 tx_parity=18601
ingress:
    enabled=1 timeout=50(ms)
    fasm_cnt=0 fasm_full=0
    ipsec_fec_chk_fail=0 complete=0
    rx_data=0 rx_parity=0
    recover=0 recover_timeout=0 recover_fail=0
    rx=0 rx_fail=0
```

3. Make packet loss more than 10%, then check the health-check result and the corresponding FEC base and redundant packets again:

```
# diagnose sys sdwan  health-check
Health Check(1):
Seq(2 vd1-p1): state(alive), packet-loss(15.000%) latency(0.168), jitter(0.017),
bandwidth-up(999999), bandwidth-dw(999998), bandwidth-bi(1999997) sla_map=0x0
```

Because packet loss is more than 10%, entry one in FEC mapping is first matched, and base and redundant are set to 8 and 2:

```
# diagnose vpn tunnel fec  vd1-p1
egress:
    enabled=1 base=8 redundant=2 codec=0 timeout=10(ms)
    encode=6670 encode_timeout=6670 encode_fail=0
    tx_data=6976 tx_parity=18748
ingress:
    enabled=1 timeout=50(ms)
    fasm_cnt=0 fasm_full=0
    ipsec_fec_chk_fail=0 complete=0
    rx_data=0 rx_parity=0
```

```
        recover=0 recover_timeout=0 recover_fail=0
        rx=0 rx_fail=0
```

www.fortinet.com