Feature SPA Deployment Guide using BGP per Overlay

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

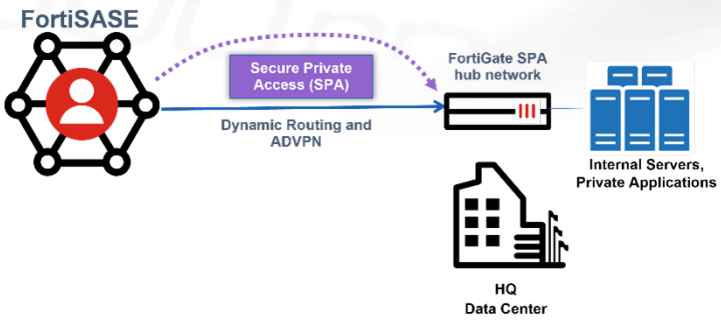
Change log

Date	Change description
2025-11-12	Initial release.
2026-01-30	Updated: • Deployment overview on page 7 • Deployment overview on page 11 • Deployment overview on page 13 • SPA design concept and considerations on page 5

Deployment overview

Organizations that have resources behind a FortiGate secure private access (SPA) hub network can provide their FortiSASE endpoints with access to private resources.

Scenarios involving a FortiGate as a FortiSASE SPA hub allows broader and seamless access to privately hosted TCP- and UDP-based applications.



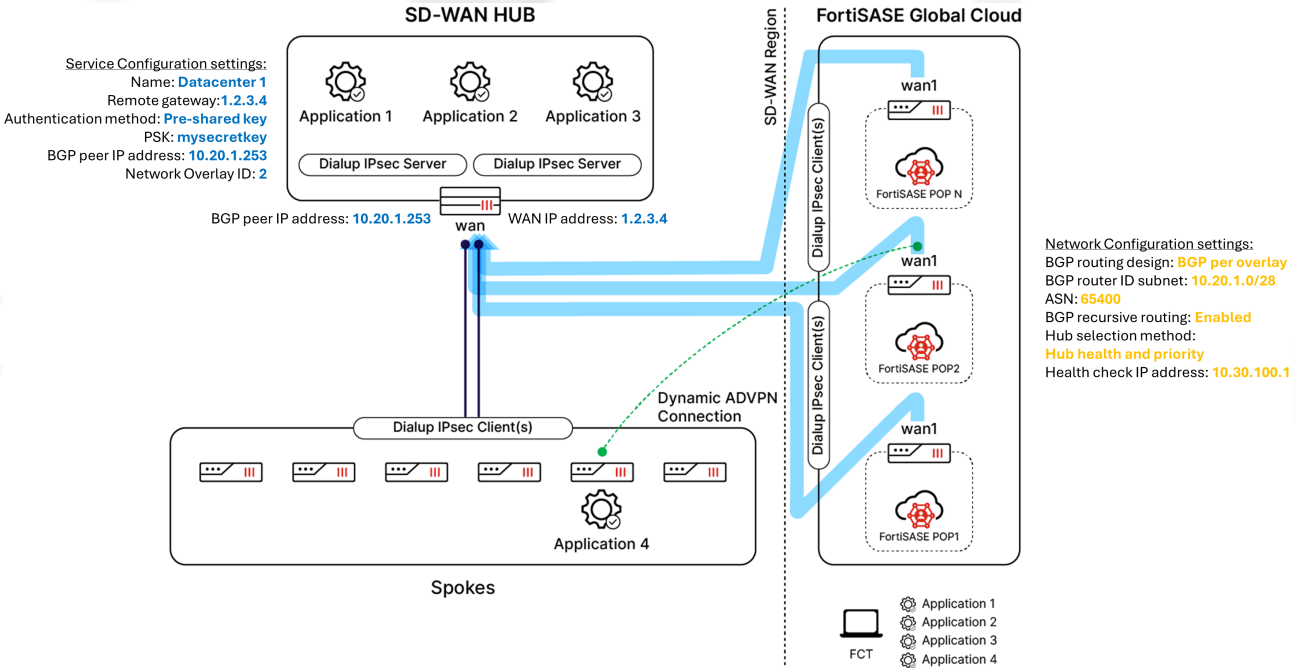
The Feature SPA Deployment Guide using BGP per Overlay contains deployment configurations for three use cases where the FortiGate SPA hub network varies in implementation:

- SPA with a FortiGate SD-WAN deployment on page 7
- FortiGate NGFW to FortiSASE SPA hub conversion deployment on page 11
- FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator on page 12

SPA design concept and considerations

FortiSASE SPA and Fortinet ADVPN

FortiSASE security PoPs and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE endpoints may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel.

The SPA use cases with FortiGate hubs allow traffic flow in the following directions:

From...	To...
Remote agents	FortiGate hubs (or spokes connected to hubs)
FortiGate hubs (or spokes connected to hubs)	Remote agents

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

FortiSASE SPA hub versus SD-WAN hub

A FortiSASE secure private access (SPA) hub allows the FortiSASE security points of presence to connect to the hub as spokes. Essentially, the FortiGate becomes an IPsec auto-discovery VPN (ADVPN) hub in a hub-and-spoke topology, and for most deployments, this configuration is sufficient to provide FortiSASE remote users with SPA to internal resources behind the FortiGate NGFW.

SD-WAN uses ADVPN for its VPN overlay. In some deployments, administrators may prefer configuring their FortiGate NGFW as an SD-WAN hub instead of just as an ADVPN hub. For these deployments, administrators require additional configuration of SD-WAN performance SLAs and SD-WAN rules using the FortiOS CLI or GUI, or use FortiManager to ensure their FortiGate NGFW become fully SD-WAN enabled. These configuration changes to convert an ADVPN hub to an SD-WAN hub are outside of the scope of this guide.

For more details on SD-WAN configuration, then please refer to Performance SLA and SD-WAN Rules sections of the FortiOS Admin Guide. For more details on SD-WAN configuration using FortiManager, then please refer to SD-WAN Single Datacenter Enterprise Deployment Guide.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

Intended audience

Midlevel network and security administrators of FortiGate devices in companies of all sizes and verticals should find this guide helpful. A working knowledge of FortiOS, FortiGate, and FortiManager configuration and the Fortinet Security Fabric is helpful.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture for the FortiSASE SPA use case using three different implementations of the FortiGate as a FortiSASE SPA hub.

Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. Reviewing the reference architecture guide(s), such as the FortiSASE Architecture Guide, is advisable if readers are still in the process of selecting the right architecture. See also the FortiSASE Concept Guide.

This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. Reviewing supplementary material found on the Fortinet Document Library in product administration guides, example guides, cookbooks, release notes, and other documents is recommended, where appropriate.

SPA with a FortiGate SD-WAN deployment

The SPA with a FortiGate SD-WAN deployment use case deployment overview includes the following:

Deployment overview

Organizations with new or existing FortiGate SD-WAN deployments can provide their FortiSASE remote users with access to private resources.

For the FortiGate SD-WAN SPA use case, you must configure a new FortiGate SD-WAN deployment or have an existing FortiGate SD-WAN deployment already configured. You then configure FortiSASE to communicate with the FortiGate SD-WAN hub. After completing this configuration, the FortiSASE security points of presence (PoP) act as spokes to this hub, relying on IPsec overlays and iBGP to secure and route traffic between security PoPs and the networks behind the organization's FortiGate SD-WAN hub-and-spoke network.

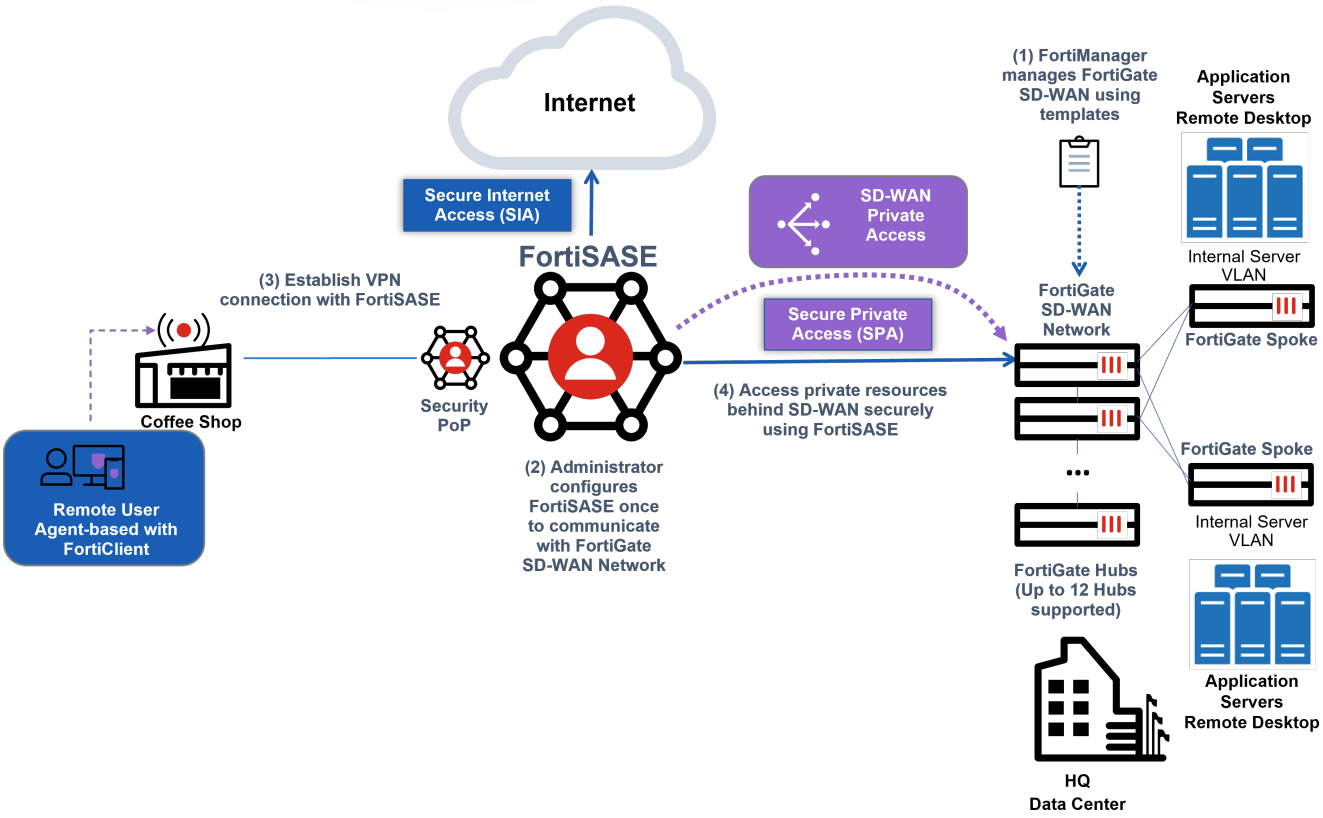
By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

FortiGate SD-WAN network deployments are expected to conform to Fortinet's best practices for SD-WAN architecture and deployment for the following topologies:

- SD-WAN with a single datacenter or hub
- SD-WAN with dual datacenters or hubs
- SD-WAN with up to 12 datacenters or hubs

Fortinet's best practices for SD-WAN deployments include using FortiManager to manage the FortiGate SD-WAN hub and spoke devices configuration.

A typical topology for deploying this example design is as follows:



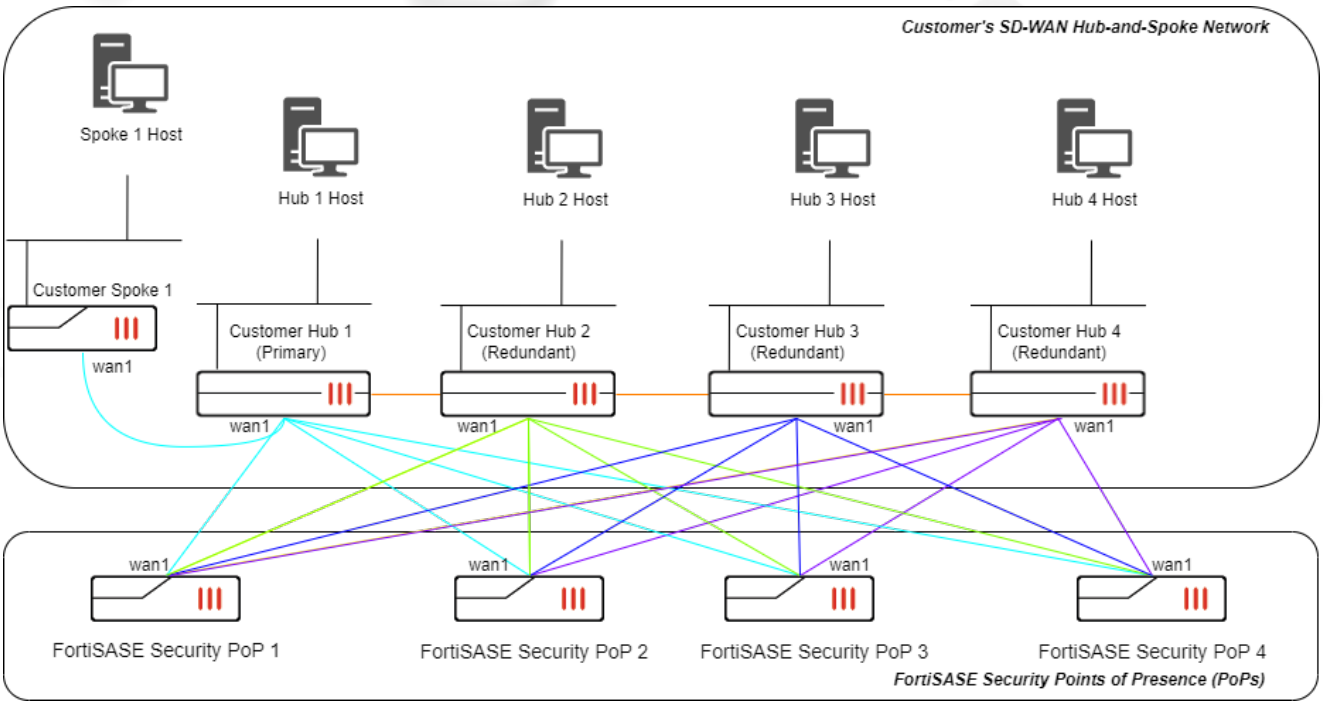
Design concept and considerations

FortiGate SD-WAN network topology

FortiSASE supports secure private access to the following SD-WAN topologies:

- SD-WAN with a single datacenter or hub
- SD-WAN with dual datacenters or hubs
- SD-WAN with up to 12 datacenters or hubs

The following topology diagram depicts an SD-WAN with four datacenters or hubs:



In the example topology, the SD-WAN hub-and-spoke network administrator configures the following settings outside of the FortiSASE network. According to SD-WAN best practices, administrators configure these settings using FortiManager:

- Hub 1, hub 2, hub 3, hub 4, and spoke 1 WAN1 IP addresses
- IPsec settings including network overlay for hub 1, hub 2, hub 3, hub 4, and spoke 1
- BGP settings including BGP router IDs of hub 1, hub 2, hub 3, hub 4, and spoke 1

The following table maps the aforementioned settings that FortiManager configures with the settings that you configure in FortiSASE using the *Secure private access* or *BGP* page:

Network setting in FortiManager	Network Setting in FortiSASE *Secure private access* or *BGP* page
Hub 1 WAN IP Address	Remote Gateway for Hub 1
Hub 2 WAN IP Address	Remote Gateway for Hub 2
Hub 3 WAN IP Address	Remote Gateway for Hub 3
Hub 4 WAN IP Address	Remote Gateway for Hub 4
Hub 1 BGP Router ID	BGP Peer ID for Hub 1
Hub 2 BGP Router ID	BGP Peer ID for Hub 2
Hub 3 BGP Router ID	BGP Peer ID for Hub 3
Hub 4 BGP Router ID	BGP Peer ID for Hub 4
Hub 1 Host IP address (typically) or any other IP address of a host locally connected to Hub 1	Health Check IP

In addition, the administrator should configure these host IP addresses:

- Hub 1 Host IP address
- Hub 2 Host IP address
- Hub 3 Host IP address

- Hub 4 Host IP address
- Spoke 1 Host IP address

You can configure the hub 1 host IP address or any other host locally connected to hub 1 later to set up the health check for the SD-WAN performance SLA rule that FortiSASE uses.

FortiSASE dynamically generates the remaining settings for the FortiSASE security points of presence (PoPs), namely, the BGP router ID, using the parameters specified in the FortiSASE *Secure private access* GUI. On the FortiSASE security PoPs, the IPsec interface IP addresses to the primary hub and the IPsec interface IP addresses to the redundant hub are dynamically assigned using the IPsec `mode-cfg` feature enabled on the hubs.

For solution and design overviews of the single datacenter for enterprise and multiple datacenter for enterprise solutions, see the SD-WAN 4-D documentation:

- SD-WAN Single Datacenter for Enterprise Deployment Guide
- SD-WAN Multiple Datacenters for Enterprise (primary/secondary) Deployment Guide
- SD-WAN Multiple Datacenters for Enterprise (primary/primary) Deployment Guide

Network restrictions

As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

Product prerequisites

For a list of product prerequisites, see SPA using a FortiGate SD-WAN hub.

FortiGate hub and spoke devices configured by administrators primarily using the FortiOS CLI or GUI is outside the scope of this guide.

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 16 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input subscriptions as needed.
2. Ensure the FortiGate SD-WAN deployment has the proper configuration:
   a. Configure a new FortiGate SD-WAN deployment using FortiManager.
   b. Review and modify the configuration settings of an existing FortiGate SD-WAN deployment using FortiManager.
3. Using the FortiSASE *BGP* and *Secure private access* pages, configure the FortiSASE security points of presence as spokes of the FortiGate SD-WAN Hub using its specific network attributes as parameters.
4. Configure the DNS settings to allow resolving hostnames for external and internal domains.
5. Verify IPsec tunnels on the FortiGate SD-WAN hub(s).
6. Verify BGP routing on the FortiGate SD-WAN hub(s).
7. Test private access connectivity to the FortiGate SD-WAN network from remote users.

FortiGate NGFW to FortiSASE SPA hub conversion deployment

The FortiGate NGFW to FortiSASE SPA hub conversion deployment use case deployment overview includes the following:

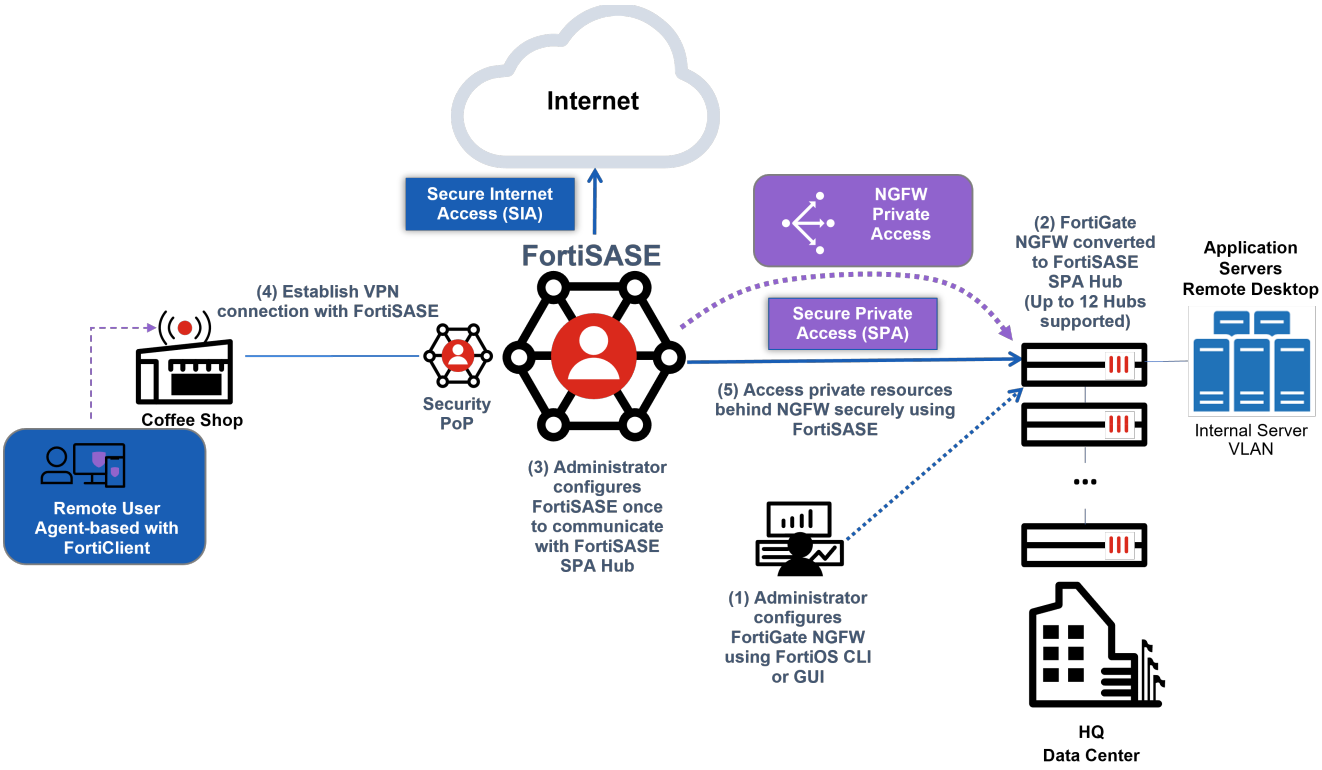
Deployment overview

Organizations that have resources behind a newly deployed FortiGate next generation firewall (NGFW) standalone site or behind a newly deployed FortiGate NGFW in a data center and are not configured with SD-WAN enabled can provide their FortiSASE remote users with access to private resources.

In the NGFW SPA use case, you must first convert the newly deployed NGFW to a FortiSASE SPA hub. After configuring FortiSASE to communicate with this hub, the FortiSASE security points of presence (PoPs) act as spokes to this hub, relying on IPsec overlays and internal border gateway protocol to secure and route traffic between security PoPs and the networks behind the organization's NGFW.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

A typical topology for deploying this example design is as follows:



Design concept and considerations

FortiGate NGFW

The FortiGate in the standalone next generation firewall (NGFW) topology is typically used by customers with a single FortiGate deployed on-premise to protect their site or with a single FortiGate deployed on-premise per site when multiple sites are involved. The design goals for deploying a FortiGate NGFW device are to use it for NGFW protection including antivirus, web filtering, intrusion prevention system, and application control features, and for LAN segmentation. Typically, a FortiGate NGFW has not yet been configured with advanced features such as SD-WAN, zero trust network access, or FortiSASE.

Network restrictions

As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

Product prerequisites

For a list of product prerequisites, see SPA using a FortiSASE SPA hub.

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 16 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input subscriptions as needed.
2. Convert the FortiGate NGFW to a FortiSASE SPA hub:
   a. Convert FortiGate NGFW configured using FortiOS CLI or GUI.
   b. Convert FortiGate NGFW managed by FortiManager.
3. Using the FortiSASE *Secure private access* page, configure the FortiSASE security points of presence as spokes of the FortiGate SD-WAN Hub using its specific network attributes as parameters.
4. Configure the DNS settings to allow resolving hostnames for external and internal domains.
5. Verify IPsec tunnels on the FortiGate SD-WAN hub(s).
6. Verify BGP routing on the FortiGate SD-WAN hub(s).
7. Test private access connectivity to the FortiGate SD-WAN network from remote users.

FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator

The NGFW to SPA hub conversion using Fabric Overlay Orchestrator (FOO) use case deployment overview includes the following:

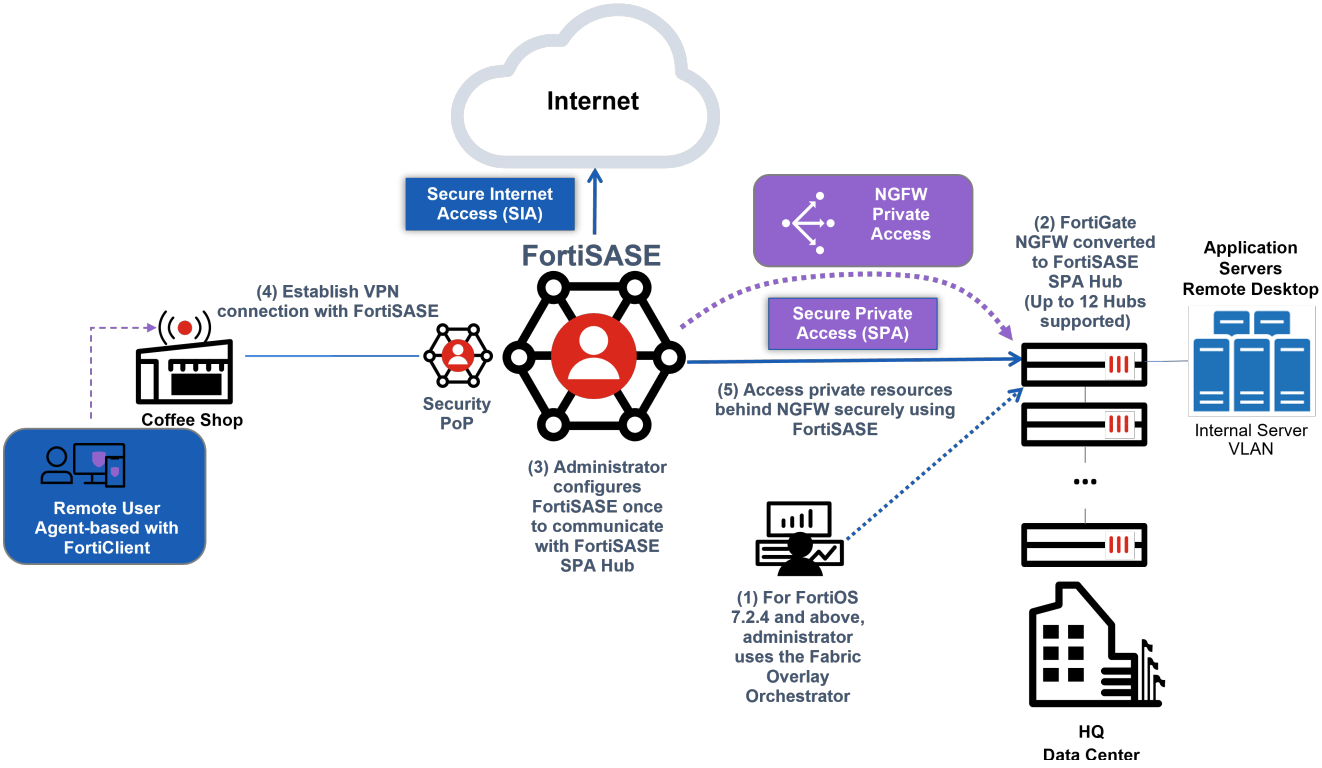
Deployment overview

Organizations that have resources behind a newly deployed FortiGate next generation firewall (NGFW) standalone site or behind a newly deployed FortiGate NGFW in a data center and are not configured with SD-WAN enabled can provide their FortiSASE remote users with access to private resources.

In the NGFW SPA use case, you must first convert the newly deployed NGFW to a FortiSASE SPA hub. Starting in FortiOS 7.2.4, you can accomplish this using Fabric Overlay Orchestrator. After configuring FortiSASE to communicate with this hub, the FortiSASE security points-of-presence (PoPs) act as spokes to this hub, relying on IPsec overlays and iBGP to secure and route traffic between PoPs and the networks behind the organization's NGFW.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

A typical topology for deploying this example design is as follows:



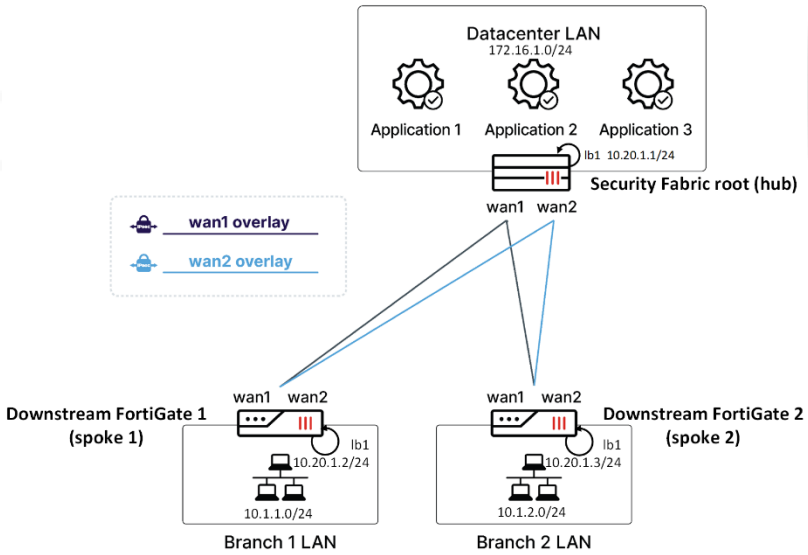
Design concept and considerations

Fabric Overlay Orchestrator

FortiOS 7.2.4 and above includes a Fabric Overlay Orchestrator feature, which is an easy-to-use GUI wizard that simplifies the process of configuring a self-orchestrated SD-WAN overlay within a single Security Fabric. This feature is self-orchestrated since no additional tool or device aside from the FortiGates themselves is required to orchestrate this configuration. An SD-WAN overlay configuration consists of IPsec and BGP configuration settings.

Currently, the Fabric Overlay Orchestrator supports a single hub architecture and builds upon an existing Security Fabric configuration. This feature configures the root FortiGate as the SD-WAN overlay hub and configures the downstream FortiGates, namely, first-level children from the root, as the spokes.

The Fabric Overlay Orchestrator supports configuring an overlay for the following example hub-and-spoke topology using ADVPN and a single hub as depicted below:



The above network topology corresponds to the single datacenter (active-passive gateway) design using the IPsec overlay design of one-to-one overlay mapping per underlay. For further details on these topics, see the SD-WAN Architectures for Enterprises design guide.

In the hub-and-spoke topology above, the datacenter FortiGate (or the Root FortiGate in the Security Fabric) is the hub and the branch FortiGates (or the Downstream FortiGates in the Security Fabric) are the spokes. Each FortiGate has a distinct LAN subnet defined and has a loopback interface, lb1, with an IP address within the 10.20.1.0/24 subnet.

The Fabric Overlay Orchestrator creates loopbacks to act as health check servers that are always up, and which can be accessed by adjacent fabric devices. When configured with the policy creation options of automatic or health check on the hub, the Fabric Overlay Orchestrator configures performance SLA from the hub to the health check servers on 10.20.1.2 and 10.20.1.3 corresponding to Spoke 1 and Spoke 2 FortiGate devices, respectively. Likewise, the Fabric Overlay Orchestrator when run on each spoke creates a performance SLA to the Hub using its loopback address 10.20.1.1.

Instead of using loopbacks, any business-critical applications and resources connected to the LAN of each device can be used as health check servers for performance SLAs.

Network restrictions

As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

Product prerequisites

For a list of product prerequisites, see SPA using a FortiSASE SPA hub using the FortiOS Fabric Overlay Orchestrator feature in the FortiSASE Release Notes.

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 16 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input subscriptions as needed.
2. Review the overlay, BGP, and firewall policy configuration settings required by a FortiSASE SPA hub.
3. Convert the FortiGate NGFW to a FortiSASE SPA hub using the FortiOS Fabric Overlay Orchestrator feature.
4. Using the FortiSASE *Secure private access* page, configure the FortiSASE security points of presence as spokes of the FortiGate SD-WAN Hub using its specific network attributes as parameters.
5. Configure the DNS settings to allow resolving hostnames for external and internal domains.
6. Verify IPsec tunnels on the FortiGate SD-WAN hub(s).
7. Verify BGP routing on the FortiGate SD-WAN hub(s).
8. Test private access connectivity to the FortiGate SD-WAN network from remote users.

Deployment procedures

Provisioning your FortiSASE instance

Ensure that you have purchased the subscription to provision FortiSASE, then do the following.

To provision your FortiSASE instance:

1. From the Fortinet Support site, register your FortiSASE subscription.
2. Once registered, go to *Services* > *Cloud Services* > *FortiSASE* to provision your FortiSASE instance.
3. When provisioning, select the geographic location for your security sites and logging. Once provisioned, the FortiSASE dashboard displays your entitlement in the *Remote users* widget. The number of endpoints that the widget lists is the number of agents that are entitled to use this service.

Use case specific deployment configurations

The following configurations are specific to their respective use case. Complete the steps that apply to your use case:

- SPA with a FortiGate SD-WAN specific configurations on page 16
- FortiGate NGFW to SPA hub conversion specific configurations on page 21
- FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator specific configurations on page 32

Once you have finished the required configuration, proceed to Configuring SPA to the FortiGate SPA hub in FortiSASE Secure private access on page 47.

SPA with a FortiGate SD-WAN specific configurations

The following deployment steps are unique to the SPA with a FortiGate SD-WAN use case.

Configuring a new FortiGate SD-WAN enterprise deployment using FortiManager

The steps for configuring a new FortiGate SD-WAN enterprise deployment using FortiManager depend on the specific SD-WAN architecture chosen for your deployment. See the following table for configuration steps described in the 4-D SD-WAN enterprise deployment guide corresponding to your SD-WAN deployment.

SD-WAN architecture	SD-WAN Enterprise Deployment Guide	Configuration steps
SD-WAN single datacenter	SD-WAN Single Datacenter Enterprise Deployment Guide	Configuring SD-WAN Overlay Template Configuring ADVPN
		Configuring SD-WAN Rules
		Configuring Normalized Interfaces, Policy Packages and Firewall Policies
		Verifying the SD-WAN Configuration
SD-WAN multidatacenter (primary/secondary)	SD-WAN Multi-Datacenter (Primary/Secondary) Enterprise Deployment Guide	Configuring SD-WAN Overlay Template Configuring ADVPN
		Configuring SD-WAN Rules
		Configuring Normalized Interfaces, Policy Packages and Firewall Policies
		Verifying the SD-WAN Configuration
SD-WAN multidatacenter (primary/primary)	SD-WAN Multi-Datacenter (Primary/Primary) Enterprise Deployment Guide	Configuring SD-WAN Overlay Template Configuring ADVPN
		Configuring SD-WAN Rules
		Configuring Normalized Interfaces, Policy Packages, and Firewall Policies
		Verifying the SD-WAN Configuration

Reviewing configuration settings of an existing FortiGate SD-WAN hub deployment previously configured using FortiManager

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

If you have previously configured the FortiGate SD-WAN hub using the steps in Configuring a new FortiGate SD-WAN enterprise deployment using FortiManager on page 17 for one of the types of SD-WAN deployments, then your configuration should already match the configuration settings in this section and you can move on to the FortiSASE configuration steps in the next section.

This section describes the IPsec tunnel, tunnel interface, BGP, and firewall policies configuration settings that are required on your FortiGate SD-WAN hub and is included for your reference and for troubleshooting purposes. For reference, review the GitHub 4-D SD-WAN demonstration configurations for various topologies.

IPsec configuration

The FortiGate SD-WAN hub requires the following IPsec settings:

- IKEv2
- Hub configured as an IPsec dialup server
- On spokes, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
- Using `mode config` for dynamic IP address
- Use network overlay IDs for each overlay tunnel configuring `set network-overlay enable` and `set network-id <n>`
- Preshared key for each overlay tunnel
- Phase 1 and phase 2 proposals and settings
  - IPsec phase 1 supports the following proposals:
    aes128-sha256
    aes256-sha256
    aes128-sha1
    aes256-sha1
    DH groups 14 and 5
  - IPsec phase 2 supports the following proposals:
    aes128-sha1
    aes256-sha1
    aes128-sha256
    aes256-sha256
    aes128gcm
    aes256gcm
    chacha20poly1305
    DH groups 14 and 5
- Hub configured with `set auto-discovery-sender enable` to enable ADVPN on the hub

The following shows a configuration sample of the IPsec CLI configuration:

- The IPsec type must be dynamic. The FortiSASE security points of presence (PoP) act as spokes and connect to your Hub to establish IPsec overlays.
- You must enable the `mode-cfg` setting. Each FortiSASE security PoP acquires IP addresses and automatically configures their tunnel interfaces IP addresses with the IP acquired. This IP address is also be used to set up BGP peering.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To allow for dynamic scaling of customer environments, as-needed, it is necessary to use the following mode configuration settings that make use of a /24 subnet for the mode configuration IP address space:

set ipv4-start-ip 192.168.10.1

set ipv4-end-ip 192.168.10.252

set ipv4-netmask 255.255.255.0

Depending on the size of the customer, the mode configuration IP address space may need to be even larger than a /24 subnet.

```
config vpn ipsec phase1-interface
    edit VPN1
        set type dynamic
        set interface port1
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set auto-discovery-sender enable
        set network-overlay enable
        set network-id 0
        set ipv4-start-ip 192.168.10.1
        set ipv4-end-ip 192.168.10.252
        set ipv4-netmask 255.255.255.0
        set psksecret < pre-shared key >
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit VPN1
        set phase1name VPN1
        set proposal aes256-sha256
    next
end
```

Tunnel interface configuration

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

You must assign a static IP address to the tunnel interface. FortiSASE security points of presence uses this to establish BGP peering to dynamically learn routes to your environment.

```
config system interface
    edit "VPN1"
        set vdom "root"
        set ip 192.168.10.253 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 192.168.10.254 255.255.255.0
        set snmp-index 13
        set interface "port1"
```

```
    next
end
```

BGP configuration

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

FortiSASE security points of presence (PoP) connect to the hub FortiGate and establish iBGP peering. FortiSASE security PoPs learn routes to your network but do not advertise any route except their router-id IP address.

The hub FortiGate requires the following BGP settings:

- AS number
- Router ID
- Using iBGP for dynamic routing via overlays
- BGP neighbor IP address for each overlay
- BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs
- For BGP per overlay, BGP peering is done via the IP addresses allocated to the Tunnel interfaces via IKE mode configuration. In this configuration example, the IP address range is 192.168.10.1-192.168.10.252. Therefore, in the BGP settings, the neighbor range needs to be the same as the IKE mode configuration tunnel IP address assignment.
- One BGP session per overlay between the hub and each FortiSASE security PoP

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

The following shows sample BGP CLI configuration:

```
config router bgp
    set as 64622
    set ebgp-multipath enable
    set ibgp-multipath enable
    set additional-path enable
    set graceful-restart enable
    set additional-path-select 4
   config neighbor-group
        edit "VPN1"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set remote-as 64622
            set additional-path send
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 192.168.10.0 255.255.255.0
            set neighbor-group "VPN1"
        next
    end
end
```

Firewall policy configuration

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To allow health checks from FortiSASE security points of presence to access the target SLA, as well as to allow FortiSASE remote users to access protected resources, you must configure these corresponding firewall policies to allow this traffic as demonstrated:

```
config firewall address
    edit "FSASE-VPN"
        set type iprange
        set start-ip 192.168.10.1
        set end-ip 192.168.10.252
    next
end
config firewall policy
    edit 1
        set name "FSASE-HealthCheck"
        set srcintf "VPN1"
        set dstintf "port2"
        set action accept
        set srcaddr "FSASE-VPN"
        set dstaddr "all"
        set schedule "always"
        set service "PING"
        set logtraffic all
    next
    edit 2
        set name "FORTISASE-To-Protected-Resources"
        set srcintf "VPN1"
        set dstintf "port2"
        set action accept
        set srcaddr "FSASE-VPN"
        set dstaddr "all"
        set schedule "always"
        set service "HTTP" "HTTPS" "SMB" "SSH" "RDP"
        set logtraffic all
    next
end
```

FortiGate NGFW to SPA hub conversion specific configurations

The following deployment steps are unique to the FortiGate NGFW to FortiSASE SPA hub conversion use case.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS CLI or GUI

FortiSASE security points of presence integrate with a hub-and-spoke network using ADVPN as its VPN overlay and BGP for its routing.

This section describes the following configuration settings and the FortiOS GUI configuration steps using the IPsec wizard and additional CLI and GUI configuration that you must configure on your FortiGate NGFW to convert it to a FortiSASE secure private access hub:

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

For details on configuring using the FortiOS GUI without using the IPsec wizard or FortiOS CLI, see Appendix B - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the IPsec wizard on page 86.

IPsec VPN configuration using IPsec wizard and CLI

The FortiGate next generation firewall requires the following IPsec VPN settings:

- IKEv2
- Hub configured as an IPsec VPN dialup server. The FortiSASE security points of presence (PoP) act as spokes and connect to your hub via IPsec dialup connections.
- You must enable the mode config setting. Each FortiSASE security PoP acquires IP addresses and automatically configures their tunnel interfaces IP addresses with the acquired IP address. You also use this IP address to set up BGP peering.
- On spokes, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
- Using mode config for dynamic IP address
- Use network overlay IDs for each overlay tunnel configuring `set network-overlay enable` and `set network-id <n>`
- Preshared key for each overlay tunnel
- Phase 1 and 2 proposals and settings
  - For IPsec phase 1, the following proposals are supported:
    aes128-sha256
    aes256-sha256
    aes128-sha1
    aes256-sha1
    DH groups 14 and 5
  - For IPsec phase 2, the following proposals are supported:
    aes128-sha1
    aes256-sha1
    aes128-sha256
    aes256-sha256
    aes128gcm
    aes256gcm
    chacha20poly1305
    DH groups 14 and 5

- Hub configured with `set auto-discovery-sender enable` to enable ADVPN on the hub

To allow for dynamic scaling of customer environments, as-needed, it is necessary to use the following mode configuration settings that make use of a /24 subnet for the mode configuration IP address space:

set ipv4-start-ip 192.168.1.1

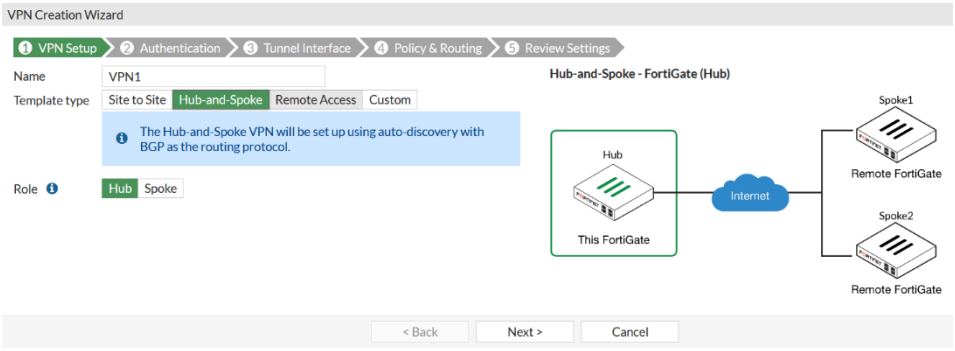
set ipv4-end-ip 192.168.1.252

set ipv4-netmask 255.255.255.0

Depending on the size of the customer, the mode configuration IP address space may need to be even larger than a /24 subnet.

To configure an IPsec VPN using the GUI and IPsec wizard:

1. Go to *VPN > IPsec Wizard*. The VPN Creation Wizard displays.
2. Configure the following *VPN Setup* options:
   a. In the *Name* field, enter VPN1.
   b. For *Template type*, select *Hub and Spoke*.
   c. For *Role*, select *Hub*. Click *Next*.



3. Configure the following *Authentication* options:
   a. From the *Incoming Interface* dropdown list, select the WAN interface that the hub will listen on for VPN peer connections. For example, you could select port1.
   b. For *Authentication method*, select *Pre-shared Key*.
   c. In the *Pre-shared key* field, enter the desired key in alphanumeric characters. Click *Next*.
4. Configure the following *Tunnel Interface* options:
   a. In the *Tunnel IP* field, enter 10.251.1.253.
   b. In the *Remote IP/netmask* field, enter 10.251.1.254/24. Click *Next*.
5. Configure the following *Policy & Routing* options:
   a. In the *Local AS* field, enter 65001.
   b. For *Local interface*, select one or more local interfaces on the FortiGate. For example, you can select port4.
   c. For *Local subnets*, the IPsec wizard selects local subnets that correspond to the selected local interfaces. You can also specify local subnets manually. These local subnets are advertised to BGP peers. For example, you could enter 192.168.111.0/24.
   d. For *Spoke type*, select *Range*.
   e. In the *Spoke range prefix* field, enter 10.251.1.0/24.
   f. For *Spoke neighbor group*, click *Create* to create a neighbor group called VPN1:
      i. In the *Name* field, enter VPN1.
      ii. In the *Remote AS* field, enter 65001.
      iii. Leave the *Interface* field blank.

iv. Enable *Activate IPv4*.
v. Disable *Attribute unchanged*.
vi. Select the following options:
- *Route reflector client*.
- *Next hop self*.
- *Capability: graceful restart*.
- *Capability: route refresh*.

vii. Click *OK*.

g. From the *Spoke neighbor group* dropdown list, select the newly created VPN1 neighbor group. Click *Next*.

6. Review the settings, then click *Create*. FortiOS displays a *The VPN has been set-up* message when the wizard successfully configures the IPsec VPN configuration.
7. Configure the following settings using the CLI. The IPsec wizard does not configure these settings. Replace VPN1 with your actual IPsec VPN phase 1 name:
   a. Enable IKEv2
   b. Enable network overlays
   c. Configure the VPN gateway network ID. Replace the 1 with the integer value corresponding to the network overlay ID.
   d. Enable mode config.
   e. Configure start and end IP addresses and netmask to use to automatically assign IP addresses to VPN peers using mode config. Replace 10.251.1.1, 10.251.1.252, and 255.255.255.0 accordingly.

```
config vpn ipsec phase1-interface
    edit VPN1
        set ike-version 2
        set network-overlay enable
        set network-id 1
        set mode-cfg enable
        set ipv4-start-ip 10.251.1.1
        set ipv4-end-ip 10.251.1.252
        set ipv4-netmask 255.255.255.0
    next
end
```

Tunnel interface configuration

You must assign a static IP address to the tunnel interface. This configuration is required to support BGP peering between the secure private access hub and the FortiSASE security points of presence.

The IPsec wizard automatically configures the tunnel interface. This topic provides the configuration for reference purposes.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To confirm the IP address on the tunnel interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Under *Physical Interface*, expand your WAN interface to display your IPsec tunnel interface. Click the tunnel interface and click *Edit*.

3. In the *Edit Interface* dialog, observe the following values:

Field	Value
Addressing mode	Manual
IP	10.251.1.253
Netmask	255.255.255.255
Remote IP/Netmask	10.251.1.254 255.255.255.0

Click *Cancel*.

Loopback interface configuration

You must create loopback interfaces on the FortiGate hub. The configuration uses the following loopback interfaces:

- A loopback interface *Lo_BGP-RID* to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment.
- A loopback interface *Lo-HC* to provide a health check target for the performance SLA on the FortiSASE security PoPs. In FortiSASE, you will need to set the *Health Check IP address* to the IP address configured for this interface. See Configuring a new service connection on page 51.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To configure the Lo-BGP-RID loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.
3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-BGP-RID.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.1.0.254/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.

To configure the Lo-BGP-RID loopback interface using the CLI:

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.1.0.254 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

To configure the Lo-HC loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.

3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-HC.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.11.11.11/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.

To configure the Lo-HC loopback interface using the CLI:

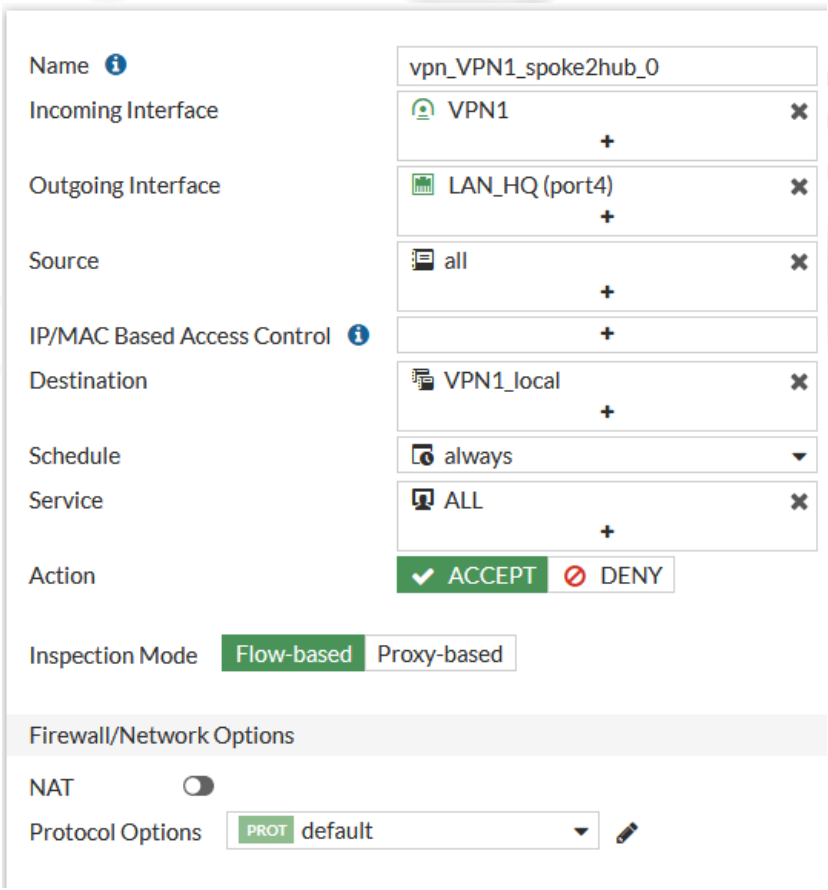
```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.11.11.11 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

Firewall policy configuration

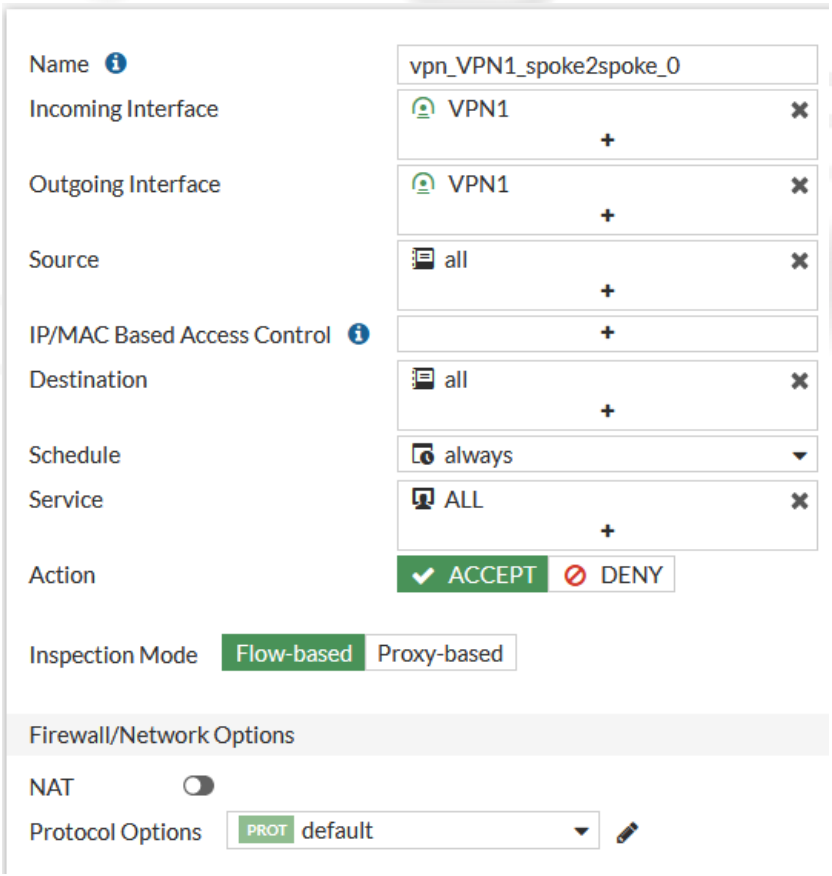
To allow health checks from FortiSASE security points of presence to access the target SLA, as well as to allow FortiSASE remote users to access protected resources, you must configure these corresponding firewall policies to allow this traffic as this topic demonstrates.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

This deployment requires a spoke-to-hub LAN firewall policy. This policy allows traffic sourced from a spoke subnet destined for hub subnets. The IPsec wizard automatically configures this policy. This topic provides the configuration for reference purposes.



This deployment requires a spoke-to-spoke firewall policy. This policy allows traffic sourced from a spoke subnet destined for other spoke subnets. The IPsec wizard automatically configures this policy. This topic provides the configuration for reference purposes.



To configure a spoke-to-loopback firewall policy using the GUI:

This policy allows BGP traffic and health check traffic from a spoke to the hub's loopback interface.

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*. The *New Policy* pane displays.
2. In the *Name* field, enter BGP.
3. Set the following options:
   a. For *Incoming interface*, select *VPN1*.
   b. For *Outgoing interface*, select *Lo-BGP-RID* and *Lo-HC*.
   c. For *Source*, select *all*.
   d. For *Destination*, select *all*.
   e. From the *Schedule* dropdown list, select *always*.
   f. For *Service*, select *ALL*.
   g. For *Action*, select *Accept*.
   h. Disable *NAT*.
   i. Select *Enable this policy*.
4. Click *OK* to save changes.

BGP configuration

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

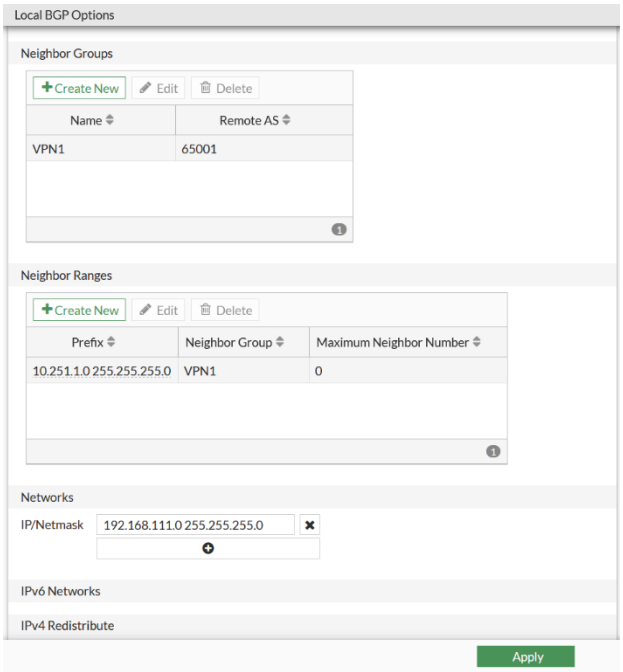
FortiSASE security points of presence (PoP) connect to the hub FortiGate and establish iBGP peering. FortiSASE security PoPs learn routes to your network but do not advertise any route except their router-id IP address.

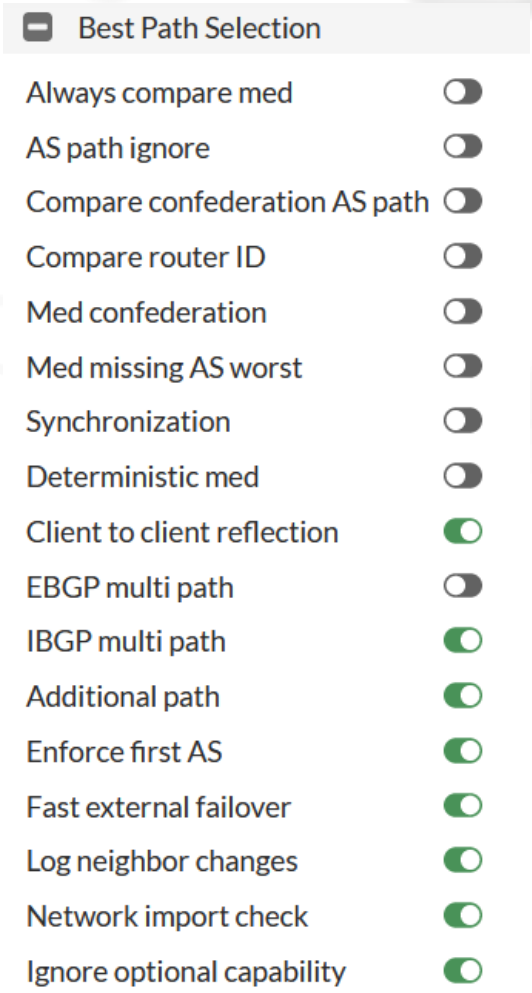
The hub FortiGate requires the following BGP settings:

- AS number
- Router ID
- Using iBGP for dynamic routing via overlays
- BGP neighbor IP address for each overlay
- BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs
- For *BGP per overlay*, BGP peering is done via the IP addresses allocated to the VPN tunnel interfaces via IKE mode configuration. In this configuration example, the IP address range is 192.168.10.1-192.168.10.252. Therefore, in the BGP settings, the neighbor range must be the same as the IKE mode configuration tunnel IP address assignment.
- One BGP session per overlay between the hub and each FortiSASE security PoP

The IPsec wizard automatically configures the aforementioned settings, except for the router ID. This topic provides the configuration for reference purposes. Note the following:

- For using iBGP for dynamic routing via overlays, local networks to be advertised are specified via *Networks*.
- The following are configured via *Neighbor Ranges*:
  - BGP neighbor IP address for each overlay
  - BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs





This section describes additional BGP settings that you must configure since the configuration that the IPsec wizard creates does not include them.

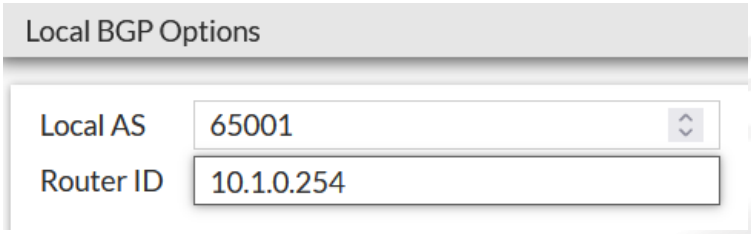
To configure BGP using the GUI:

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

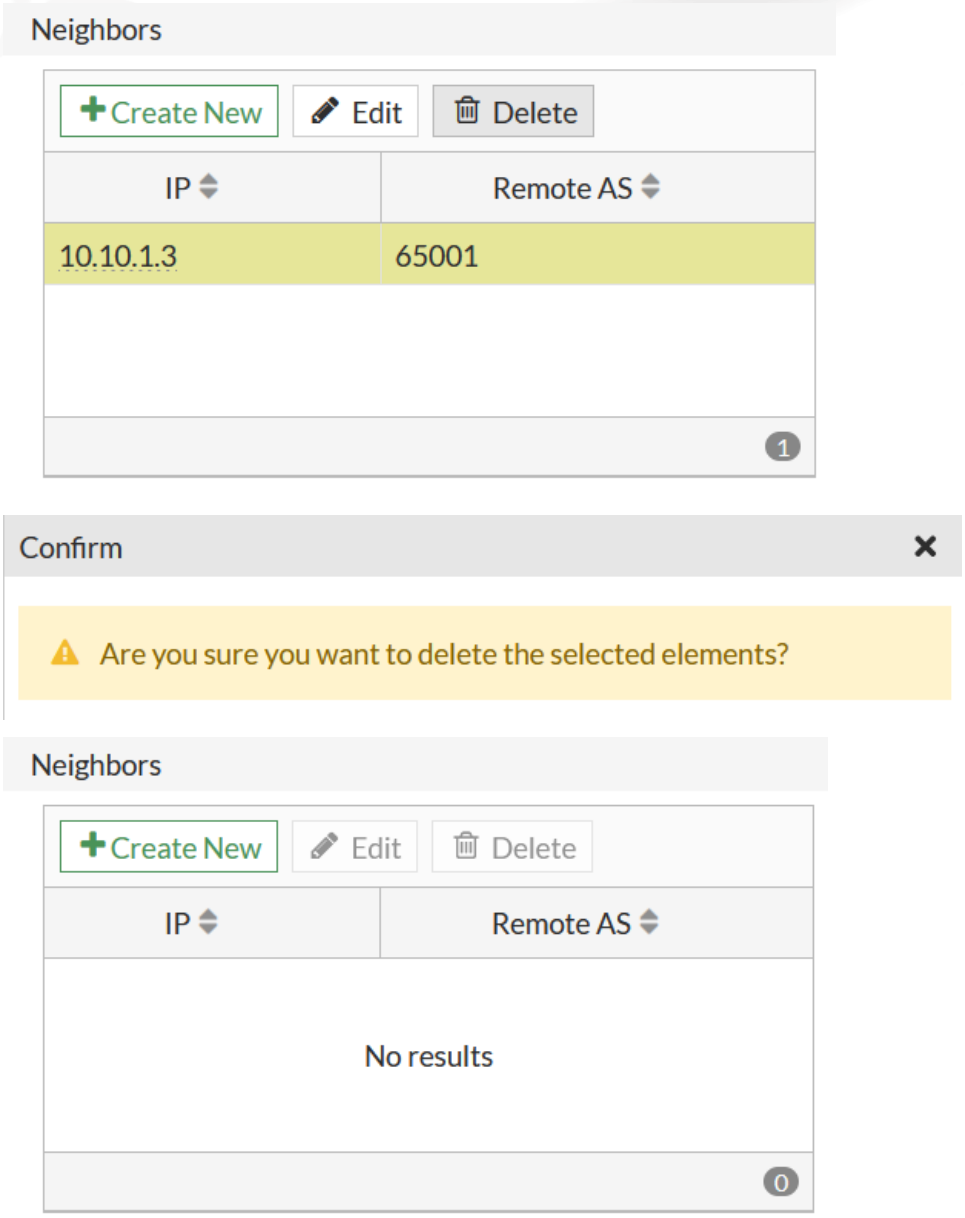
If you cannot view the *Network* > *BGP* tree menu, go to *System* > *Feature Visibility* and enable *Advanced Routing* in the *Core Features* column.

1. Go to *Network* > *BGP*.
2. Confirm that the *Local AS* field is set to 65001.

3. In the *Router ID* field, enter 10.1.0.254, which is the loopback interface IP address.



4. Under *Neighbors*, click the neighbor entry, then click *Delete*. Click *OK* in the dialog.



5. In the *Neighbor Groups* section, select the neighbor group that the IPsec wizard created. For example, click *VPN1*, then click *Edit*:
   a. From the *Interface* dropdown list, select the tunnel interface of the hub used to listen for spoke connections. This example selects VPN1.
   b. Enable *Soft reconfiguration*.
   c. Click *OK*.

6. Under *Advanced Options*, configure the following:
   a. In the *Keepalive* field, enter 5.
   b. Enable *Holdtime* and enter 15.
7. Click *Apply*.
8. Configure the following CLI options. Replace VPN1 with the name of the neighbor group that you configured. These options are not available in the GUI and you must run these CLI commands to configure them:

```
config router bgp
   set additional-path enable
   set additional-path-select 4
   config neighbor-group
        edit "VPN1"
            set additional-path both
            set adv-additional-path 4
        next
    end
end
```

Converting FortiGate NGFW managed by FortiManager to a FortiSASE SPA hub

If FortiManager is managing your FortiGate next generation firewall deployment, follow either step here to configure your FortiGate device as a hub only:

- SD-WAN Overlay Templates for new region deployments using FortiManager 7.2.0 and later with the Single Hub topology selected and with Auto-Discovery VPN (ADVPN) enabled
- FortiManager Recommended SD-WAN IPSec + BGP Templates using FortiManager 7.0.3 and later with Hub device templates and with Auto-Discovery VPN (ADVPN) enabled

FortiManager 7.0.3 and later includes 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.

FortiManager 7.2.0 and later includes an SD-WAN overlay template with a wizard to automate and simplify the process using Fortinet's recommended IPsec and BGP templates. The SD-WAN overlay template also makes use of an SD-WAN template which allows configuration of SD-WAN rules and performance SLAs on branch devices.

FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator specific configurations

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

The following deployment steps are unique to the NGFW to SPA hub conversion using Fabric Overlay Orchestrator use case.

This section describes how to use the Fabric Overlay Orchestrator feature in FortiOS 7.2.4 and later to convert the FortiGate NGFW to a FortiSASE SPA Hub. Since some VPN and BGP settings may not be configured by the Fabric Overlay Orchestrator, you will need to configure these settings later using the FortiOS CLI to complete the conversion.

For details on configuring using the FortiOS GUI without using the Fabric Overlay Orchestrator or FortiOS CLI, see Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the Fabric Overlay Orchestrator on page 99.

General steps

The following general steps should be used to configure a self-orchestrated SD-WAN overlay within a single Security Fabric.

These steps must be followed in this order and assume that the prerequisites and network topology above are in place.

1. Configure the root FortiGate using the Fabric Overlay Orchestrator.
2. Configure one or more downstream FortiGates using the Fabric Overlay Orchestrator.
3. Configure an overlay on spoke for additional incoming interface on hub (if applicable).
4. Verify the Fabric Overlay created by the Fabric Overlay Orchestrator:
   a. Verify IPsec tunnels on the hub FortiGate.
   b. Verify BGP Routing on the hub FortiGate.
   c. Verify the Performance SLAs on the hub FortiGate.
   d. Verify IPsec Tunnels on a spoke FortiGate.
   e. Verify BGP Routing on a spoke FortiGate.
   f. Verify the Performance SLA on a spoke FortiGate.

When configuring the root and downstream FortiGates, the Fabric Overlay Orchestrator configures the following settings in the background:

- IPsec overlay configuration (Hub-and-Spoke ADVPN tunnels)
- BGP configuration
- Policy routing
- SD-WAN zone
- SD-WAN performance SLAs

The FortiGate's role in the SD-WAN overlay is automatically determined by its role in the Security Fabric. The Fabric Root will have the role of the Hub and any first-level children (downstream devices) from the Fabric Root will have the role of a Spoke.

Policy creation

The Fabric Overlay Orchestrator can create firewall policies to allow all traffic through the SD-WAN overlay or create firewall policies just to allow health check traffic through it instead.

When enabling the Fabric Overlay Orchestrator on the root FortiGate device, you have three options for configuring the Policy creation setting: Automatic, Health Check (default), or Manual.

Policy creation option	Description
Automatic	Automatically creates policies for the loopback interface and tunnel overlays.
Health Check (default)	Automatically creates a policy for the loopback interface so SD-WAN health checks are functional.
Manual	No policies are created automatically.

The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

When the Fabric Overlay Orchestrator has already been configured on a device, changing the policy creation rule will create new policies based on the rule but will not delete existing policies. Deleting existing policies must be performed manually.

Configuring a root FortiGate using the Fabric Overlay Orchestrator

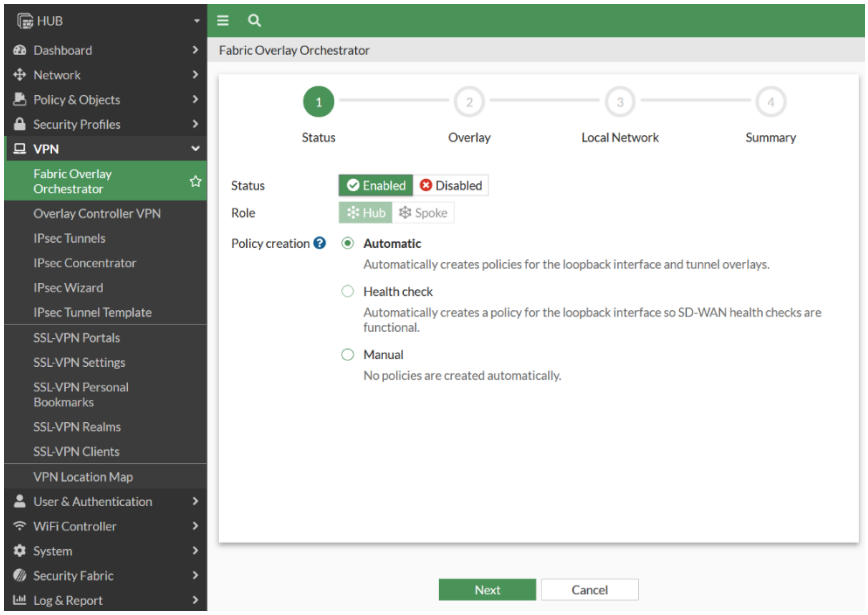
This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

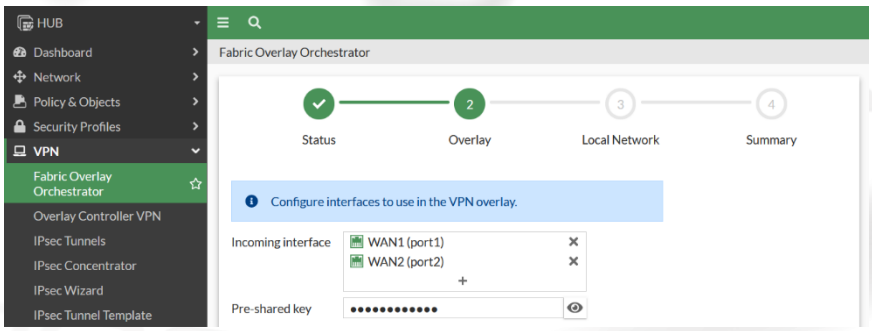
These steps describe how to run the Fabric Overlay Orchestrator on the root FortiGate.

To configure a root FortiGate using the Fabric Overlay Orchestrator:

1. Go to *VPN* > *Fabric Overlay Orchestrator*.
2. Set *Status* to *Enabled*. The *Role* is automatically selected depending on the FortiGate device's role in the Fortinet Security Fabric. When configuring the root FortiGate, confirm the *Role* is *Hub*. The Fabric root must always be the hub. For *Policy Creation*, select *Automatic*. Click *Next*.



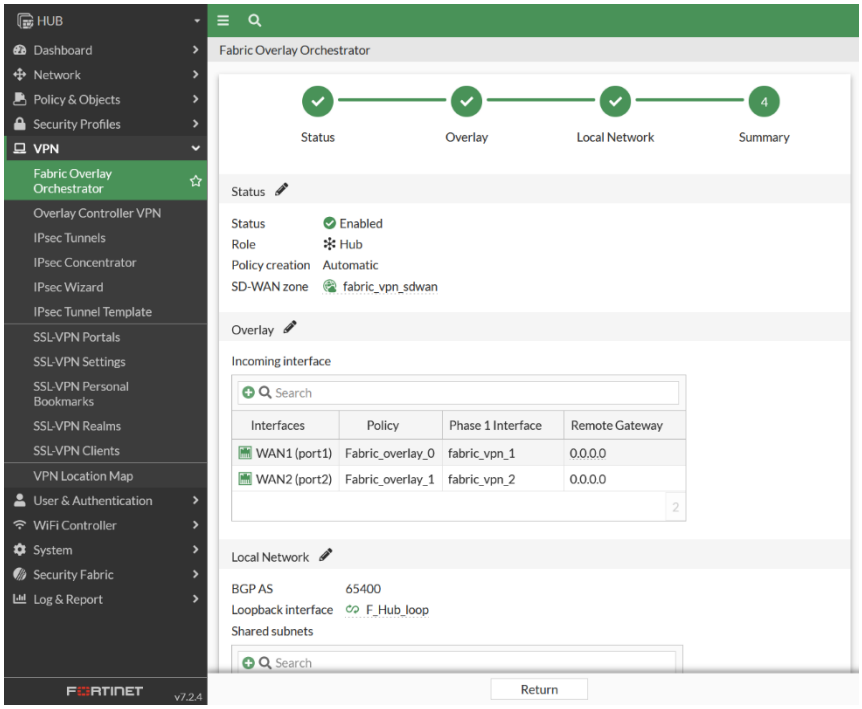
3. For *Overlay*, select one or more interfaces as the *Incoming interface* or the underlay link over which the overlay will be built, configure the *Pre-shared key*, and click *Next*. The example selects two incoming interfaces:

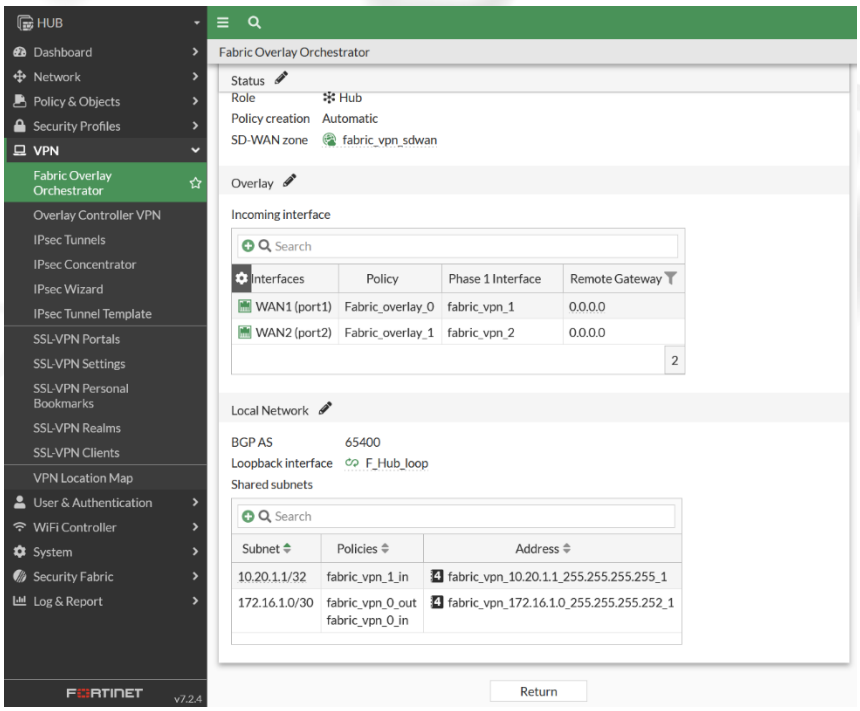


4. For *Local Network*, configure routing and local subnets to share with the VPN network, namely, the BGP AS, loopback address block, and shared interfaces settings:

Option	Description
BGP AS	Optionally, you can configure the BGP AS number. By default, this setting is set to 65400.
Loopback address block	Optionally, you can configure the loopback IP address. By default, this setting is set to 10.20.1.1/255.255.255.0.
Shared interfaces	Select the interface of the local network to share with the VPN network

   Click *Next*.
5. For the first *Summary* step, review the configured settings and click *Apply*.
6. For the second *Summary* step, observe that the following settings have been created as follows:





Option	Description
SD-WAN Zone	*Status* > *SD-WAN* zone. In the example, this is fabric_vpn_sdwan.
VPN Tunnels	*Overlay* > *Incoming interface* > *Phase 1 Interface*. In the example, they are fabric_vpn1 and fabric_vpn2.
BGP	*Local Network* > *BGP AS*, *Local Network* > *Shared subnets*. In the example, the BGP AS is 65400 and subnets are 10.20.1.1/32 and 172.16.1.0/30.
Loopback Interface	*Local Network* > *Loopback interface*. In the example, it is F_Hub_loop.
Firewall Policies	*Overlay* > *Incoming interface* > *Policy*, *Local Network* > *Shared subnets* > *Policies*. In the example, they are Overlay: Fabric_overlay_0, Fabric_overlay_1, Shared subnets: fabric_vpn_1_in, fabric_vpn_0_out, fabric_vpn_0_in.

Configuring a downstream FortiGate using the Fabric Overlay Orchestrator

These steps describe how to run the Fabric Overlay Orchestrator on a downstream FortiGate.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

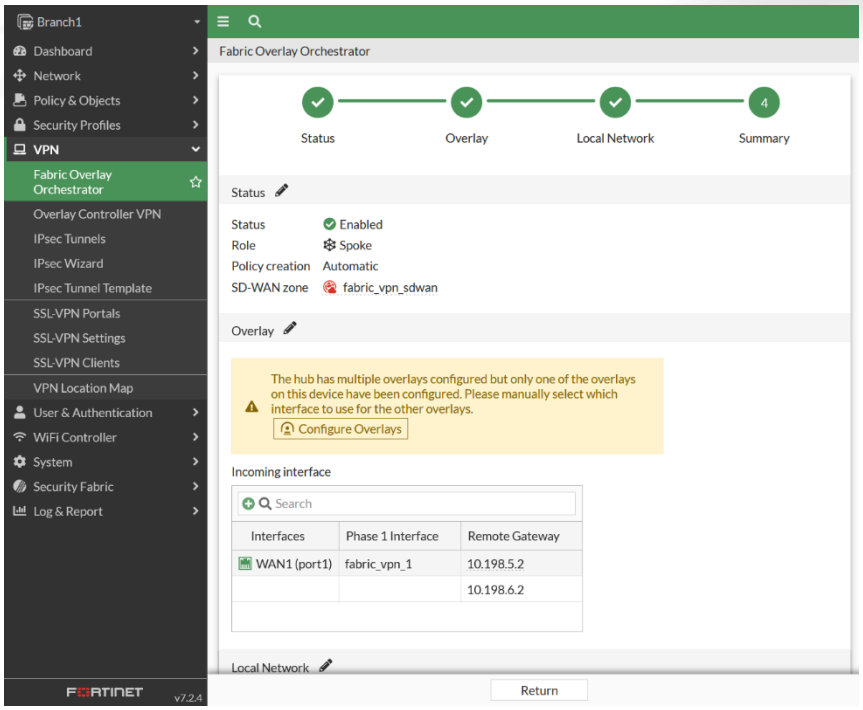
To configure a downstream FortiGate using the Fabric Overlay Orchestrator:

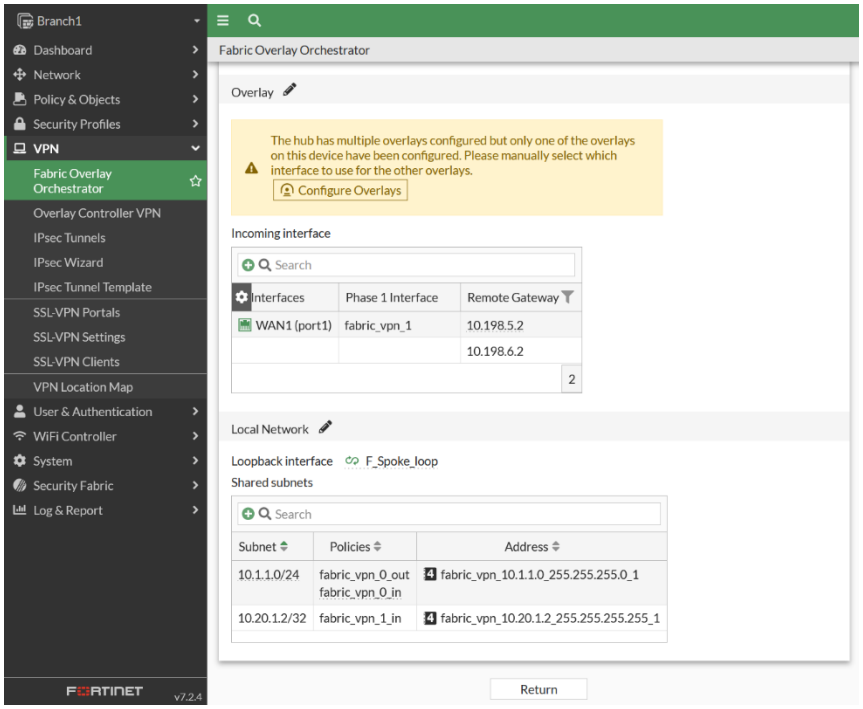
1. Go to *VPN* > *Fabric Overlay Orchestrator*.
2. Set *Status* to *Enabled*. The *Role* is automatically selected depending on the FortiGate device's role in the Fortinet Security Fabric. When configuring a downstream FortiGate, confirm the role is spoke. Only downstream FortiGates that are first-level children of the root may become spokes. Click *Next*.
3. For *Local Network*, configure routing and local subnets to share with the VPN network, namely, shared interfaces settings:

Option	Description
Shared interfaces	Select the interface of the local network to share with the VPN network

Click *Next*. Observe the *Configuring spoke Fabric VPN from root FortiGate notification* message.

4. For the first *Summary* step, review the configured settings and click *Apply*.
5. For the second *Summary* step, observe that the following settings have been created as follows:





Option	Description
SD-WAN Zone	*Status > SD-WAN* zone. In the example, this is fabric_vpn_sdwan.
VPN Tunnels	*Overlay > Incoming interface > Phase 1 Interface*. In the example, this is fabric_vpn1 .
BGP	*Local Network > BGP AS, Local Network > Shared subnets*. In the example, the BGP AS is 65400 and subnets are 10.1.10.0/24 and 10.20.1.2/32.
Loopback Interface	*Local Network > Loopback interface*. In the example, it is F_Spoke_loop.
Firewall Policies	*Local Network > Shared subnets > Policies*. In the example, they are fabric_vpn_1_in, fabric_vpn_0_out, fabric_vpn_0_in.

FortiOS generates the loopback IP addresses for the branches based on the index number of the trusted device in the hub Security Fabric system configuration. For example, if Branch1 is the first FortiGate and Branch2 is the second FortiGate authorized in the hub FortiGate, FortiOS generates the loopback addresses as follows:

FortiGate	Loopback IP address	Serial number
Branch1	10.20.1.2	FGVM02TM22009724
Branch2	10.20.1.3	FGVM02TM22009526

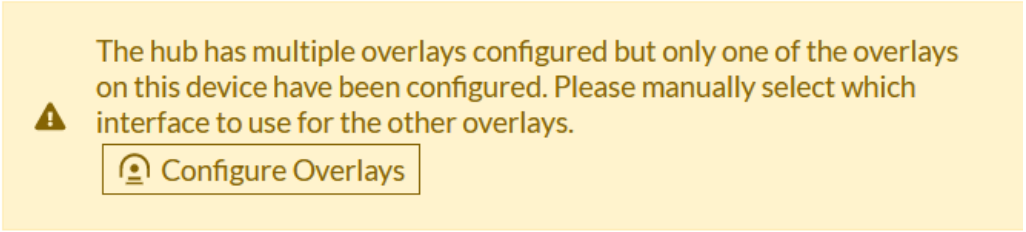
In this example, the Security Fabric trusted devices list in the Fabric-HUB FortiGate is as follows:

```
config system csf
    set status enable
    set group-name "fabric"
    config trusted-list
        edit "FGVM02TM22009724"
            set serial "FGVM02TM22009724"
            set index 1
        next
        edit "FGVM02TM22009526"
            set serial "FGVM02TM22009526"
            set index 2
        next
    end
end
```

Configuring an overlay on spoke for additional incoming interface on hub (if applicable)

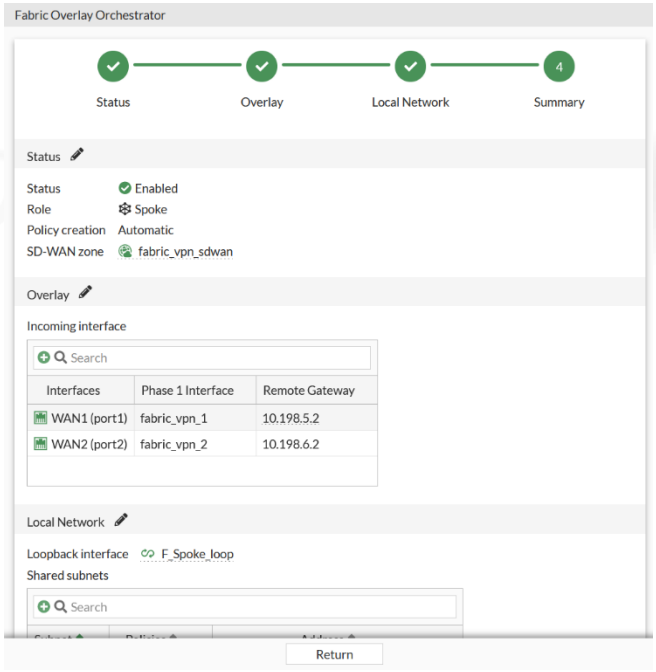
To configure an overlay on spoke for additional incoming interface on hub (if applicable):

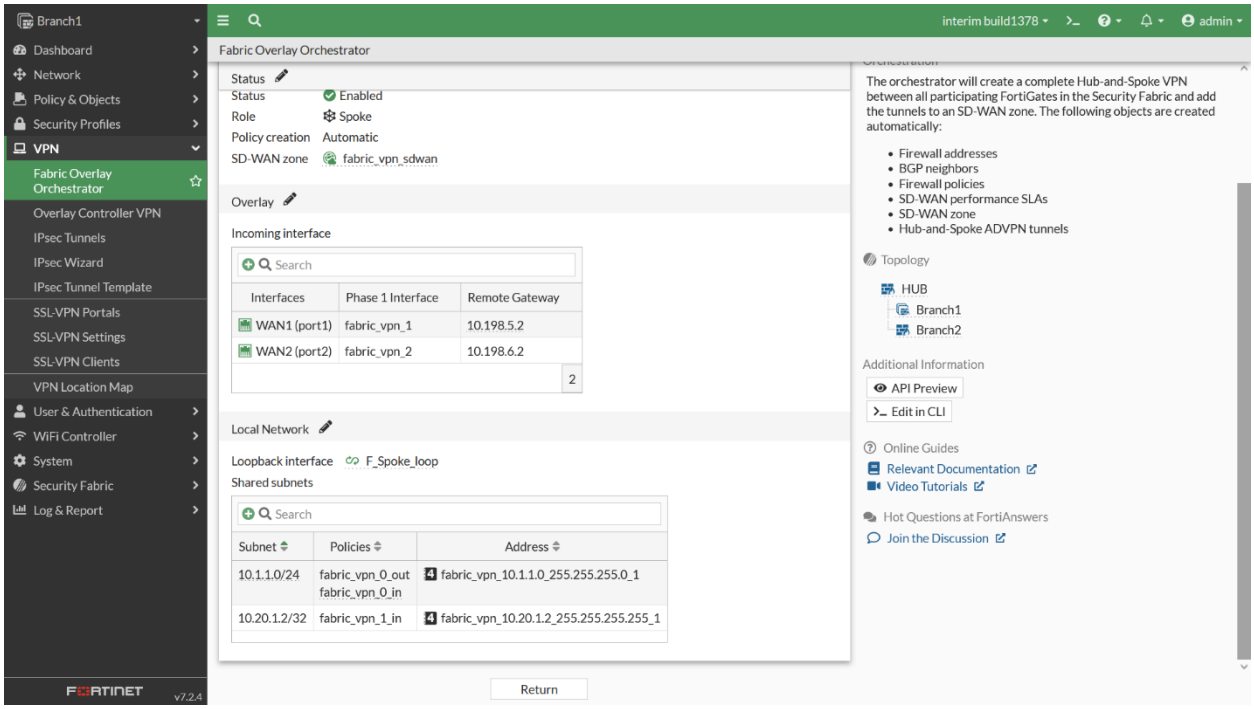
1. Typically, the hub will include two incoming interfaces. From the Fabric Overlay Orchestrator page, you will notice the following dialog:



You can configure an additional incoming interface (if applicable) using the GUI by clicking *Configure Overlays* in the dialog and adding the additional interface, such as WAN2 (port2), to the overlay.

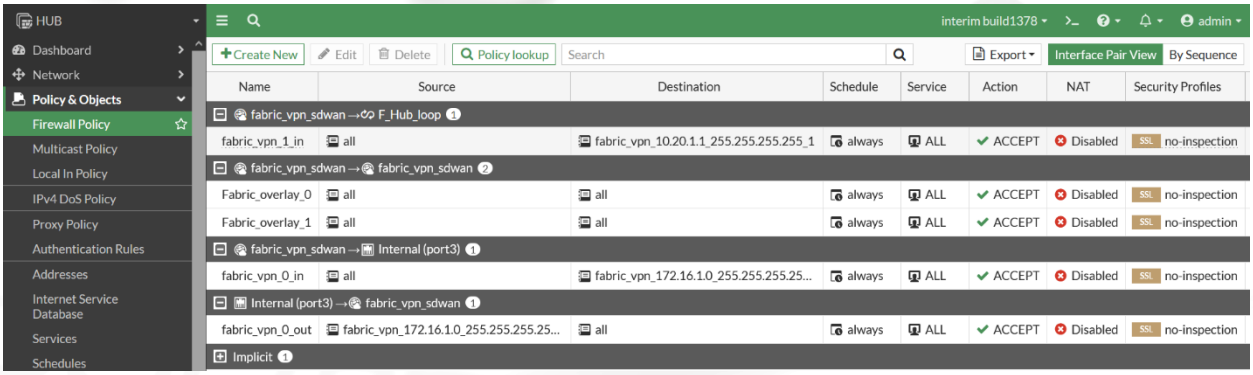
2. In the *Local Network* page, click *Next*.
3. In the *Summary* page, click *Apply*. You now see the following settings on the Summary page:





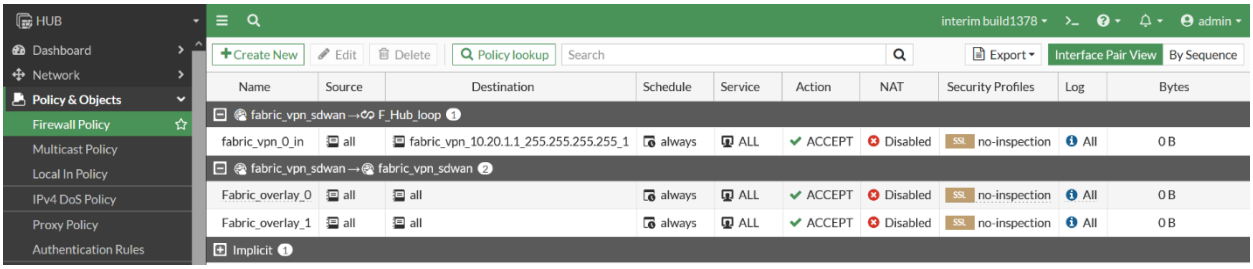
Verifying firewall policies on the hub FortiGate

On the hub, when *Policy creation* is set to *Automatic*, verify that wildcard firewall policies have been configured on the hub FortiGate. For this fabric overlay orchestrator configuration example using *Automatic*, the following firewall policies are configured on the hub FortiGate:



The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

On the hub, when *Policy creation* is set to *Health Check*, verify that a single firewall policy allowing health check traffic to the hub's loopback has been configured on the hub FortiGate. For a fabric overlay orchestrator configuration example using *Health Check*, the following firewall policies are configured on the hub FortiGate:



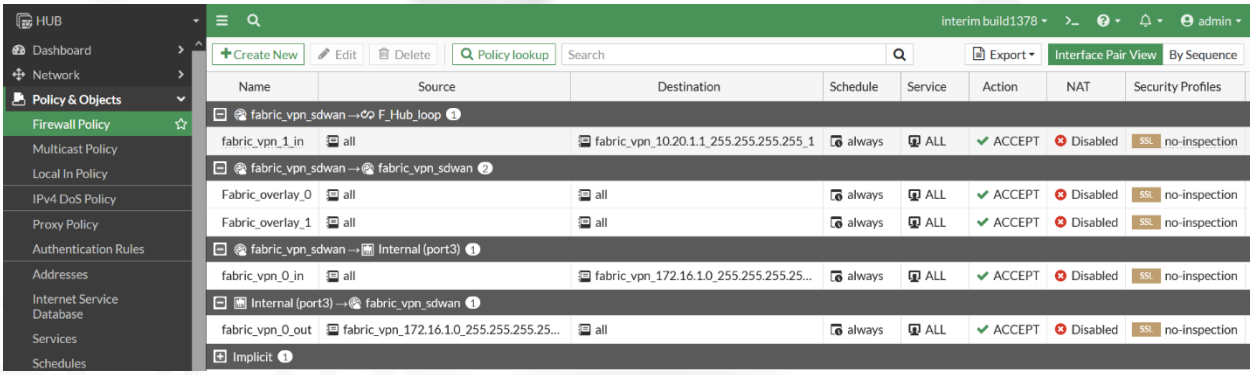
On the hub, when *Policy creation* is set to *Manual*, verify that no firewall policies were created by the fabric overlay orchestrator. Firewall policies must be manually configured on the hub FortiGate to allow traffic to the loopback interface for health checks and the overlays, if desired.

Verifying settings

After configuring the root and downstream FortiGates using the Fabric Overlay Orchestrator, you can verify settings on both hub and spoke.

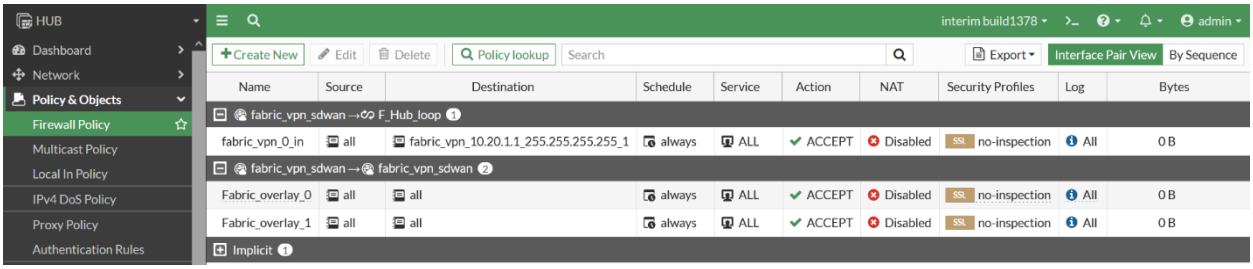
Verifying firewall policies on the hub FortiGate

On the hub, when *Policy creation* is set to *Automatic*, verify that wildcard firewall policies have been configured on the hub FortiGate. For this fabric overlay orchestrator configuration example using *Automatic*, the following firewall policies are configured on the hub FortiGate:



The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

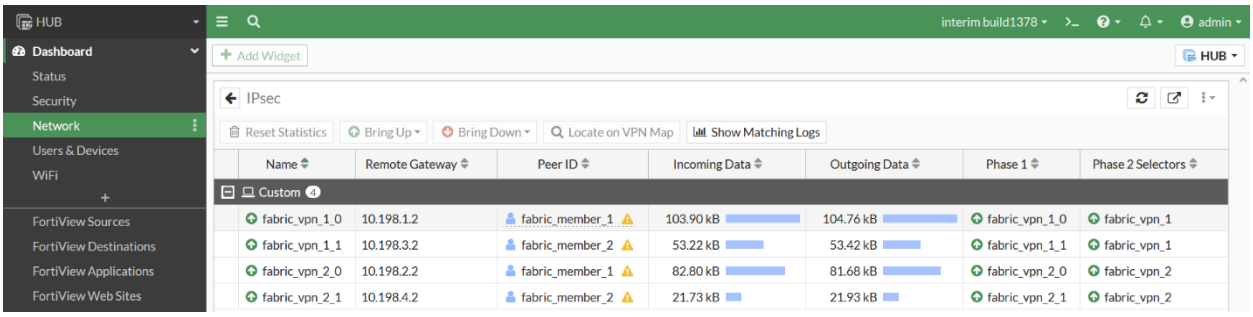
On the hub, when *Policy creation* is set to *Health Check*, verify that a single firewall policy allowing health check traffic to the hub's loopback has been configured on the hub FortiGate. For a fabric overlay orchestrator configuration example using *Health Check*, the following firewall policies are configured on the hub FortiGate:



On the hub, when *Policy creation* is set to *Manual*, verify that no firewall policies were created by the fabric overlay orchestrator. Firewall policies must be manually configured on the hub FortiGate to allow traffic to the loopback interface for health checks and the overlays, if desired.

Verifying IPsec VPN tunnels on the hub FortiGate

On a spoke, verify the IPsec tunnel back to the hub by going to *Dashboard* > *Network* and clicking on the IPsec widget to expand it:



There are two IPsec tunnels established with fabric_vpn_1_0 and fabric_vpn_1_1 and two IPsec tunnels established with fabric_vpn_2_0 and fabric_vpn_2_1 with <tunnel name>_0 and <tunnel name>_1 indicating the relative order in which these tunnels were established:

Tunnel name	Description
fabric_vpn_1_0	VPN tunnel listening on hub's WAN1 incoming interface, established with spoke 1 using its WAN1 interface
fabric_vpn_1_1	VPN tunnel listening on hub's WAN1 incoming interface, established with spoke 2 using its WAN1 interface
fabric_vpn_2_0	VPN tunnel listening on hub's WAN2 incoming interface, established with spoke 1 using its WAN2 interface
fabric_vpn_2_1	VPN tunnel listening on hub's WAN2 incoming interface, established with spoke 2 using its WAN2 interface

Verifying BGP routing on the hub FortiGate

To verify BGP routing on a hub FortiGate:

1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:

   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes

   The following provides sample output for these commands:

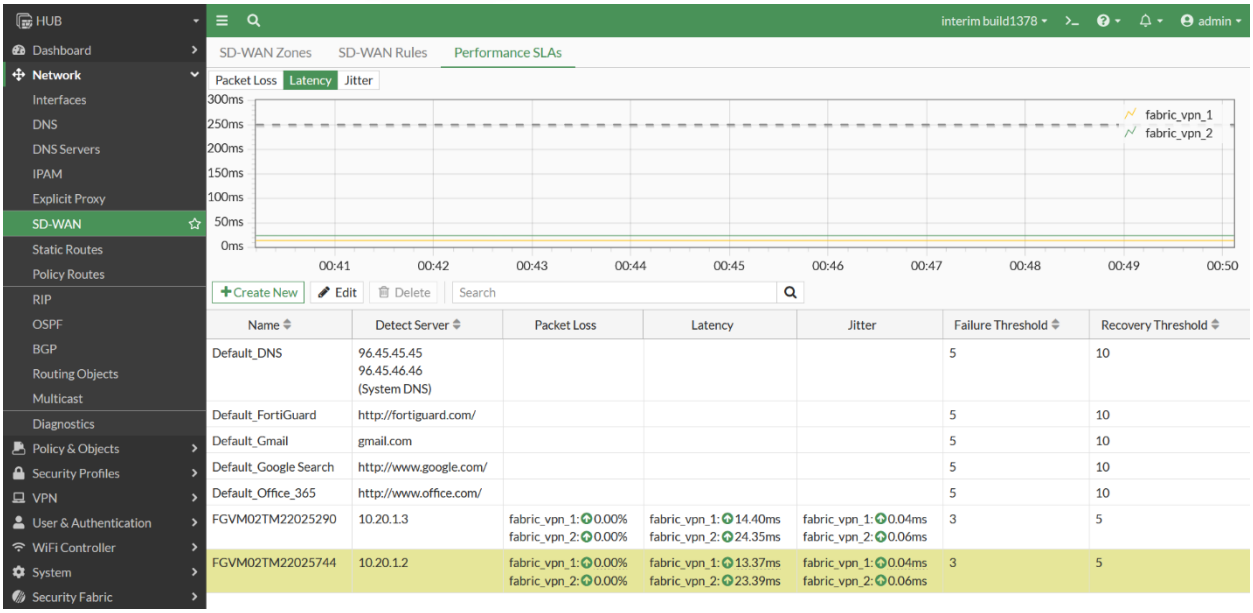
```
HUB # get router info bgp summary

VRF 0 BGP router identifier 10.20.1.1, local AS number 65400
BGP table version is 11
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 43 seconds

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1 4      65400      23      27       11    0    0 00:09:28        2
10.10.10.2 4      65400      16      16       11    0    0 00:06:36        2
10.10.11.1 4      65400      14      20       11    0    0 00:09:22        2
10.10.11.2 4      65400       7      11       11    0    0 00:03:22        2

Total number of neighbors 4


HUB # get router info bgp neighbors 10.10.10.1 advertised-routes
VRF 0 BGP table version is 11, local router ID is 10.20.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.1.1.0/24      10.10.11.1                        100      0        0 i <-/2>
*>i10.1.2.0/24      10.10.11.2                        100      0        0 i <-/2>
*>i10.1.2.0/24      10.10.10.2                        100      0        0 i <-/1>
*>i10.10.10.0/24    10.10.10.253                      100  32768        0 i <-/1>
*>i10.10.11.0/24    10.10.10.253                      100  32768        0 i <-/1>
*>i10.20.1.1/32     10.10.10.253                      100  32768        0 i <-/1>
*>i10.20.1.2/32     10.10.11.1                        100      0        0 i <-/2>
```

```
*>i10.20.1.3/32     10.10.11.2                100      0          0 i <-/2>
*>i10.20.1.3/32     10.10.10.2                100      0          0 i <-/1>
*>i172.16.1.0/30    10.10.10.253              100  32768          0 i <-/1>

Total number of prefixes 10
```

2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

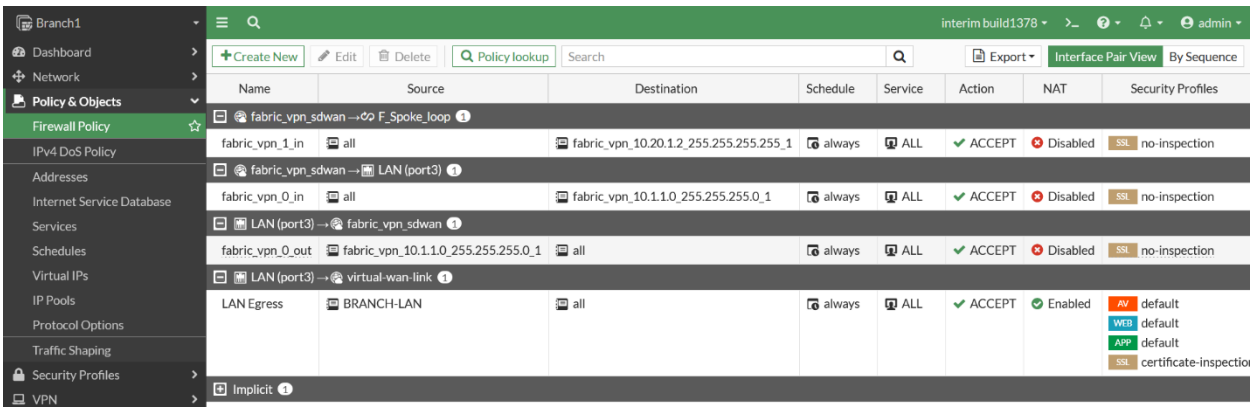
Verifying the performance SLAs on the hub FortiGate

On the hub, verify the performance SLAs are automatically created for each spoke named using the serial number of each spoke FortiGate by going to *Network* > *SD-WAN* and clicking the *Performance SLAs* tab:



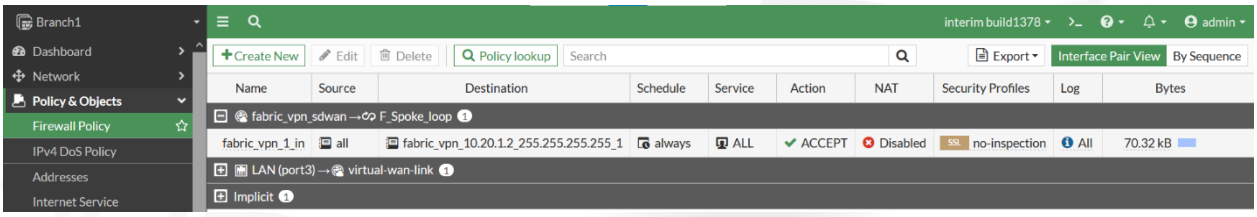
Verifying firewall policies on a spoke FortiGate

When *Policy creation* is set to *Automatic* on the hub FortiGate, verify that wildcard firewall policies have been configured on a spoke FortiGate. For this fabric overlay orchestrator configuration example using *Automatic*, the following firewall policies are configured on the spoke FortiGate:



The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

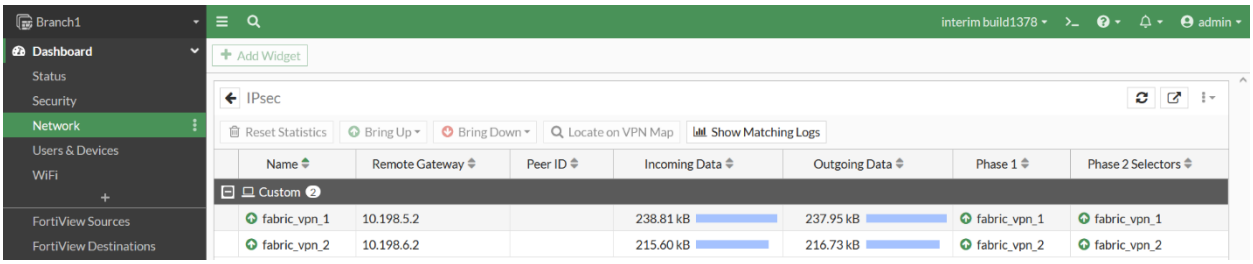
When *Policy creation* is set to *Health Check* on the hub FortiGate, verify that a single firewall policy allowing health check traffic to the spoke's loopback has been configured on a spoke FortiGate. For a fabric overlay orchestrator configuration example using *Health Check*, the following firewall policies are configured on the spoke FortiGate:



When *Policy creation* is set to *Manual* on the hub FortiGate, verify that no firewall policies were created by the fabric overlay orchestrator. Firewall policies must be manually configured on the spoke FortiGates to allow traffic to the loopback interface for health checks and the overlays, if desired.

Verifying IPsec VPN tunnels on a spoke FortiGate

On a spoke, verify the IPsec tunnel back to the hub by going to *Dashboard* > *Network* and clicking on the IPsec widget to expand it:



Verifying BGP routing on a spoke FortiGate

To verify BGP routing on a spoke FortiGate:

1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:

   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes

   The following provides sample output for these commands:

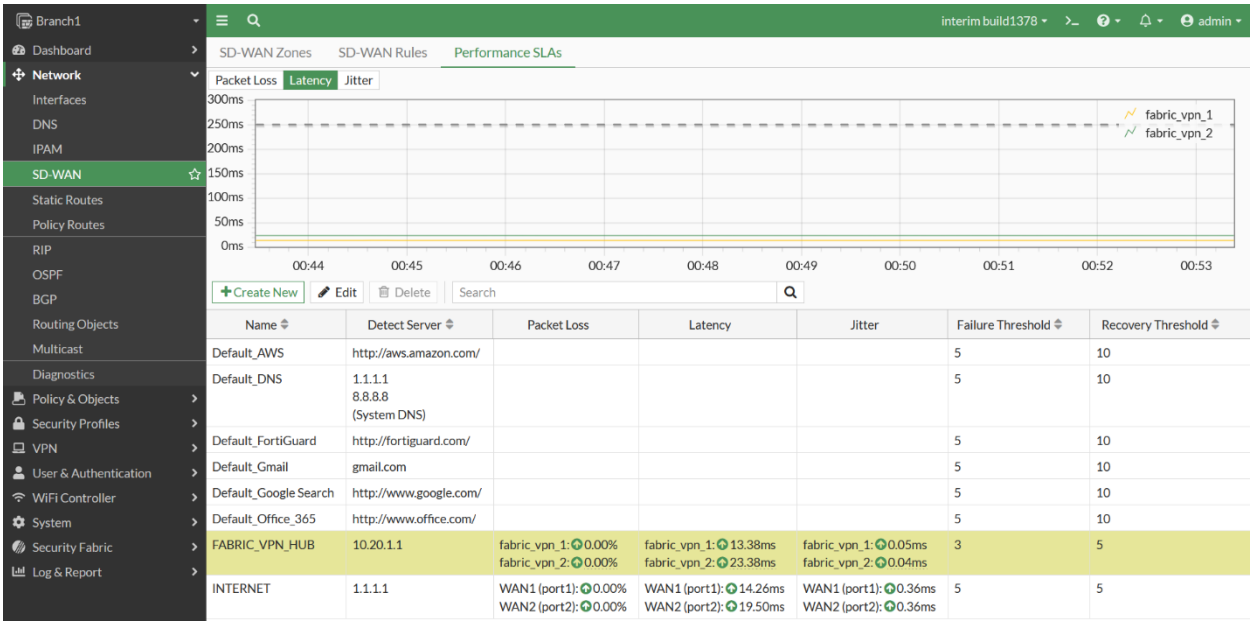
```
Branch1 # get router info bgp summary

VRF 0 BGP router identifier 10.20.1.2, local AS number 65400
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.253 4      65400      41      37        4    0    0 00:23:39        8
10.10.11.253 4      65400      38      34        4    0    0 00:23:33        8

Total number of neighbors 2


Branch1 # get router info bgp neighbors 10.10.10.253 advertised-routes
VRF 0 BGP table version is 5, local router ID is 10.20.1.2
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.1.1.0/24      10.10.10.1                        100   32768        0 i <0/->
*>i10.20.1.2/32     10.10.10.1                        100   32768        0 i <0/->

Total number of prefixes 2
```

2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

Verifying the performance SLA on a spoke FortiGate

On the spoke, verify the performance SLA is automatically created for the hub FortiGate by going to *Network* > *SD-WAN* and clicking the *Performance SLAs* tab:



Verifying spoke-to-spoke ADVPN communication

To verify spoke-to-spoke ADVPN communication, run the following CLI commands on Spoke 1:

```
execute ping-options source <IP of interface on Spoke 1>
execute ping <IP of interface on Spoke 2>
get vpn ipsec tunnel summary
```

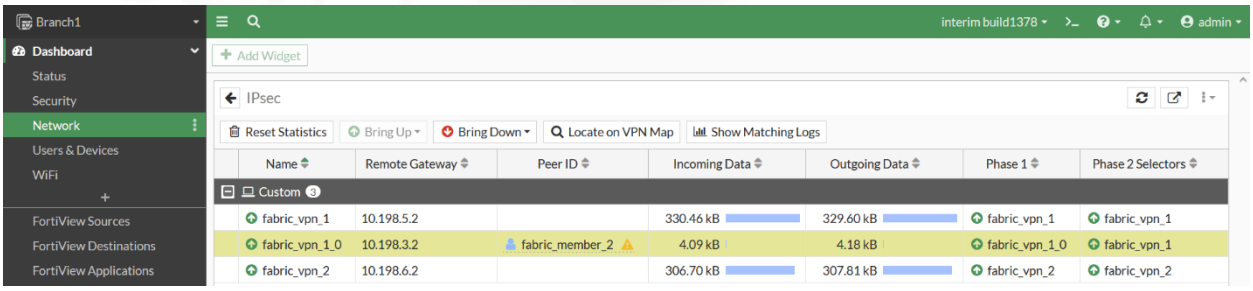
The following shows the expected output for this example:

```
Branch1 # exec ping-options source 10.20.1.2

Branch1 # exec ping 10.20.1.3
PING 10.20.1.3 (10.20.1.3): 56 data bytes
64 bytes from 10.20.1.3: icmp_seq=0 ttl=254 time=27.7 ms
64 bytes from 10.20.1.3: icmp_seq=2 ttl=255 time=17.4 ms
64 bytes from 10.20.1.3: icmp_seq=3 ttl=255 time=17.5 ms
64 bytes from 10.20.1.3: icmp_seq=4 ttl=255 time=17.4 ms

--- 10.20.1.3 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 17.4/20.0/27.7 ms
```

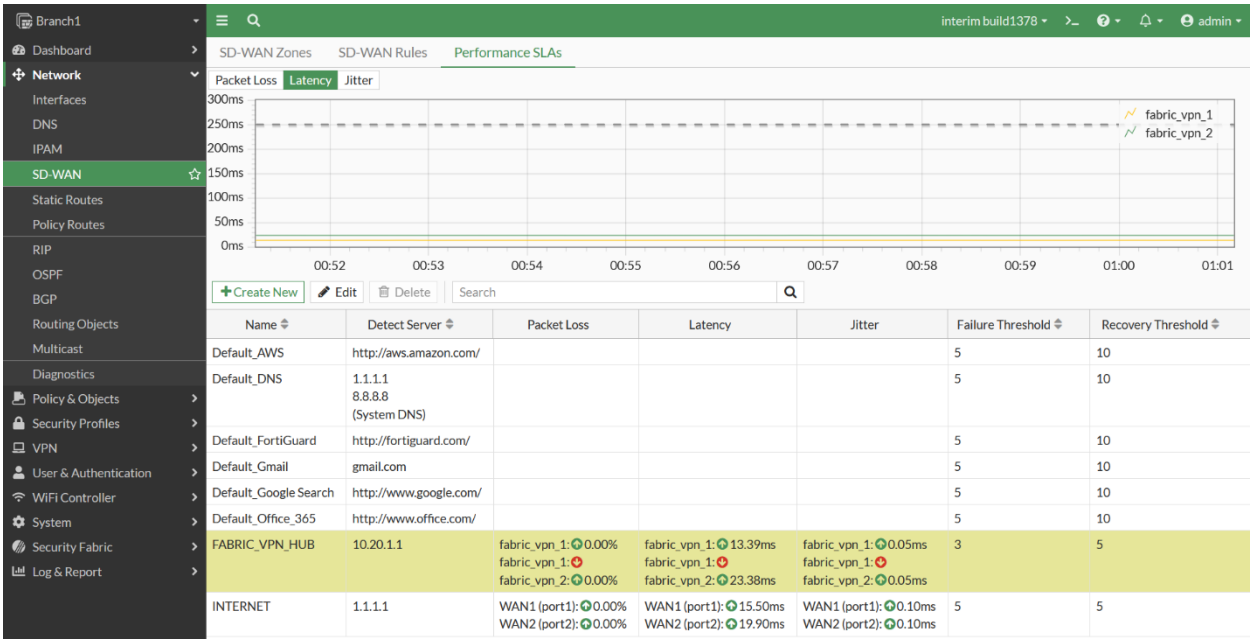
```
Branch1 # get vpn ipsec tunnel summary
'fabric_vpn_1_0' 10.198.3.2:0  selectors(total,up): 1/1  rx(pkt,err): 25/0  tx(pkt,err):
26/2
'fabric_vpn_1' 10.198.5.2:0  selectors(total,up): 1/1  rx(pkt,err): 8032/0  tx(pkt,err):
8022/2
'fabric_vpn_2' 10.198.6.2:0  selectors(total,up): 1/1  rx(pkt,err): 7462/0  tx(pkt,err):
7478/1
```

fabric_vpn_1_0 is created for Spoke 1 to Spoke 2 communication.

On Spoke 1, verify the IPsec VPN tunnel between Spokes 1 and 2 by going to *Dashboard* > *Network* and clicking the IPsec widget to expand it:



On Spoke 1, verify the performance SLA has been updated by going to *Network* > *SD-WAN* and clicking the *Performance SLAs* tab:



The first fabric_vpn_1 corresponding to the spoke-to-hub VPN tunnel is shown as green and up. The second fabric_vpn_1 corresponding to the spoke-to-spoke VPN tunnel fabric_vpn_1_0 is shown as red and down since 10.20.1.1 is the IP address corresponding to the hub's loopback interface which is not present on another spoke.

Configuring SPA to the FortiGate SPA hub in FortiSASE Secure private access

Before configuring *BGP* and *Secure private access* in FortiSASE, to ensure proper secure private access (SPA) functionality, you must ensure that the FortiSASE SPA hub conforms to details mentioned in all previous sections of this guide up until this point.

At this point, the FortiGate is functioning as a FortiSASE SPA hub.

To allow FortiSASE remote users with SPA to resources behind your FortiGate SD-WAN hub network, you can configure FortiSASE security points of presence as spokes in your hub-and-spoke network using *BGP* and *Secure private access*.

Configuration workflow

To configure SPA service connections (hubs), you must follow this configuration workflow:

1. Under *Network* > *BGP*, configure the common BGP configuration settings. See Configuring BGP on page 47.
2. Under *Operations* > *Connectivity* > *Secure private access*, click *Create*, and configure a new service connection (hub). See Configuring a new service connection on page 51.

You cannot configure a service connection or hub without first configuring *Network Configuration* settings.

Configuring BGP

Before proceeding with configuring hubs or service connections, you must configure common secure private access (SPA) network configuration that all service connections use .

To configure BGP:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

1. Go to *Network* > *BGP*.
2. (Optional) You can use an easy configuration key to simplify SPA setup on FortiSASE by automatically populating key fields in *BGP* and *Create Secure Private Access Service Connection* based on the FortiGate hub configuration. The easy configuration key is available on FortiOS 7.4.5 and later versions when the FortiGate is configured as a hub using Fabric overlay orchestrator. The FortiGate must have a valid SPA Service Connection subscription and be registered under the same FortiCloud account as FortiSASE. See SPA using a FortiSASE SPA hub with Fabric overlay orchestrator. You must set the following network attributes to use the key:

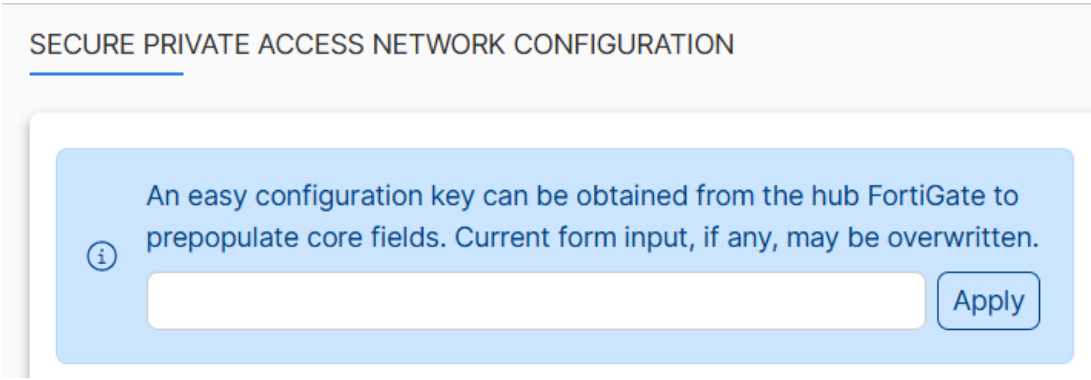
a. Under *Network* > *BGP*, set the following attributes. Otherwise, you cannot use the key:

Network attributes	Must be configured as...
BGP Routing Design	*BGP per overlay*
Hub Selection Method	*Hub Health and Priority*

b. After configuring the attributes under *Network* > *BGP*, you must configure the following authentication method under *Operations* > *Connectivity* > *Secure private access* to use the easy configuration key:

Network attributes	Must be configured as...
Authentication Method	*Pre-shared Key*

c. After completing the configuration on the hub FortiGate using Fabric overlay orchestrator, copy the key and paste it in *Operations* > *Connectivity* > *Secure private access* under the field in *Create Secure Private Access Service Connection* on FortiSASE. See SPA easy configuration key for FortiSASE and SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.



d. Click *Apply*. FortiSASE autopopulates fields such as *BGP Router ID Subnet*, *FortiSASE ASN*, and *Health Check IP* based off the FortiGate hub configuration. Click *Save* to finish SPA network configuration. You can proceed to Configuring a new service connection on page 51 without completing the remaining steps in this section.

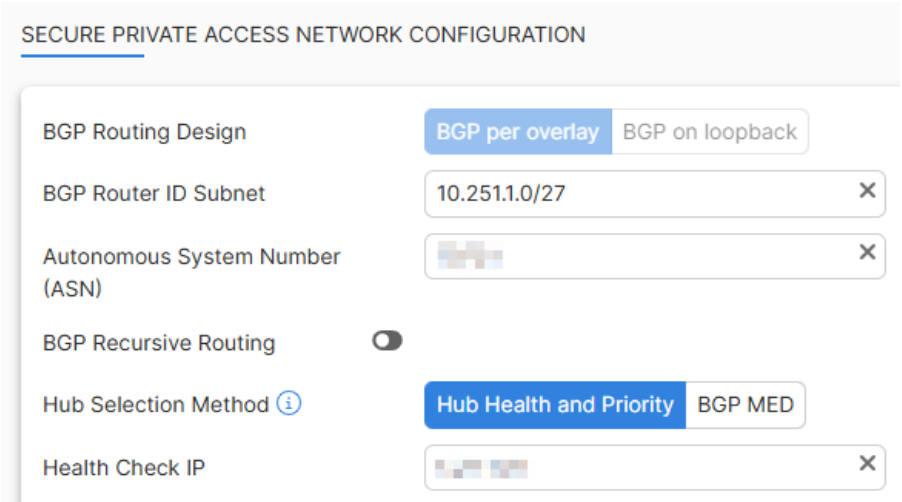
3. Under *Network* > *BGP*, under the *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select BGP per overlay (default selection).
4. Fill in the rest of the fields with values of the attributes of the FortiGate hub network connection. FortiSASE validates the input and notifies you of any invalid values. See the following table:

Network attributes	Description	Example
BGP Routing Design	FortiSASE supports these main routing design methods: • BGP per overlay (default) • BGP on loopback You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them. See Routing design methods. This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.	BGP per overlay

Network attributes	Description	Example
BGP Router ID Subnet	For BGP per overlay, available or unused subnet that can be used to assign loopback interface IP addresses used for BGP router IDs parameter only on the FortiSASE security PoPs. /28 is the minimum subnet size. Typically, this BGP router ID subnet is a subnet within the overall BGP loopback summary range that is currently unused. For example, if the BGP loopback summary range is 10.20.1.0/24 then you can choose to configure 10.20.1.0/28 as the BGP router ID subnet if it is unused.	10.20.1.0/28
SPA hubs belong to	If all SPA hub(s) are in the same BGP autonomous system number (ASN) as FortiSASE, select *FortiSASE autonomous system*. This option enables iBGP peering between FortiSASE and the SPA hub(s). If the SPA hub(s) are distributed across both the same and different BGP autonomous system numbers (ASNs) relative to FortiSASE, select *Different autonomous systems*. This configuration enables eBGP peering with SPA hubs in different ASNs and iBGP peering with those in the same ASN as FortiSASE.	FortiSASE autonomous system
FortiSASE ASN	BGP autonomous system (AS) number of your hubs. Typically, this is the same on both hubs.	65400
Hub Selection Method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: • **Hub health and priority**: periodically obtain jitter, latency, and packet loss measurements for each hub via the health check IP address. FortiSASE selects the highest priority hub within each security PoP that meets lowest cost (SLA) requirements. A hub can be assigned a different priority level in different security PoPs. • **BGP MED**: BGP multi-exit discriminator (MED) is an attribute that an autonomous system advertising routes to another peer sets. FortiSASE learns MED from the configured hubs. See BGP multi-exit discriminator.	Hub health and priority
Health Check IP	IP address of a server behind the hub used to set up the SD-WAN performance SLA rule.	10.30.100.1

Network attributes	Description	Example
	On the hub, you can configure a loopback interface for health check purposes and specify the IP address of that loopback interface for this parameter. Since there is only a single health check IP address, you can configure a loopback on all hubs with the same IP address. Also, in the hub configuration, you will need to create a policy to allow traffic from the IPsec tunnel to this loopback interface.	
Advanced Hub Priorities	FortiSASE security PoPs can advertise their configured hub priorities and SLA status to their associated hub(s) using BGP community. These BGP community values can be advertised further into a hub's network core to enable routing decisions in the network core using BGP community strings. See Advertise Hub Priorities.	
BGP Recursive Routing	Enabling the BGP recursive routing setting allows for interhub connectivity and redundancy to networks behind the active hub if each hub has a physical connection to the others for cases when connectivity between a FortiSASE security PoP and the active hub fails. For example, consider that this BGP configuration setting enabled and a FortiSASE security PoP's connectivity with hub 1 goes down. To ensure the security PoP can reach a network behind hub 1, it would route traffic to hub 2 first, then route it to hub 1 via its interhub connection, followed by routing the traffic to the desired destination network behind hub 1.	Enabled

5. Click *Save*.



Considerations

- As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.
- For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.
- When using the BGP MED option, user-defined hub priorities are not used because the SD-WAN SLA rule is disabled in this case.

Configuring a new service connection

You can create a new service connection (hub) using the BGP per overlay BGP routing design method.

You configured the corresponding BGP routing design method in *Network > BGP*.

After you create a service connection, you can update its authentication method using *Update Authentication Method*, namely, to switch from using a preshared key (PSK) to a certificate or vice-versa. You can also use this option to update the existing authentication method settings, such as updating the PSK, PKI user, or certificate.

To configure service connections or hubs for BGP per overlay:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

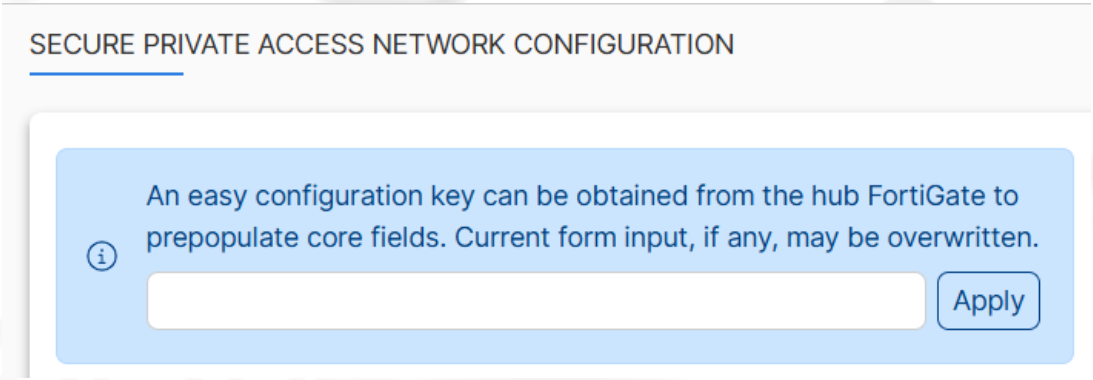
1. Go to *Operations > Connectivity > Secure private access*.
2. Click *Create*.
3. (Optional) You can use an easy configuration key to simplify SPA setup on FortiSASE by automatically populating key fields in *BGP* and *Create Secure Private Access Service Connection* based on the FortiGate hub configuration. The easy configuration key is available on FortiOS 7.4.5 and later versions when the FortiGate is configured as a hub using Fabric overlay orchestrator. The FortiGate must have a valid SPA Service Connection subscription and be registered under the same FortiCloud account as FortiSASE. See SPA using a FortiSASE SPA hub with Fabric overlay orchestrator. You must set the following network attributes to use the key:
   a. Under *Network > BGP*, set the following attributes. Otherwise, you cannot use the key:

Network attributes	Must be configured as...
BGP Routing Design	*BGP per overlay*
Hub Selection Method	*Hub Health and Priority*

   b. After configuring the attributes under *Network > BGP*, you must configure the following authentication method under *Operations > Connectivity > Secure private access* to use the easy configuration key:

Network attributes	Must be configured as...
Authentication Method	*Pre-shared Key*

   c. After completing the configuration on the hub FortiGate using Fabric overlay orchestrator, copy the key and paste it in *Operations > Connectivity > Secure private access* under the field in *Create Secure Private Access Service Connection* on FortiSASE. See SPA easy configuration key for FortiSASE and SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.
   d. Click *OK*. FortiSASE autopopulates fields based off the FortiGate hub configuration.



e. Manually configure the remaining fields:

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK.	mysecretkey

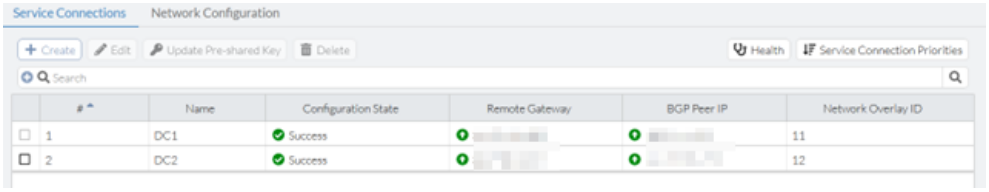
f. Click *OK* to finish configuring the SPA service connection. Once FortiSASE successfully configures the connection, it notifies you. The *Configuration State* column value changes from *Creating* to *Success*. You can proceed to viewing health and tunnel status without completing the remaining steps in this section.

4. Fill in the rest of the fields with the FortiGate hub or service connection attributes. FortiSASE validates the input and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Remote Gateway	IPsec remote gateway (public IP address) for the hub.	1.2.3.4
Authentication Method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared Key* (default) and *Certificate*.	*Pre-shared key*
Pre-shared Key	When you configure *Authentication Method* as *Pre-shared Key*, define the hub PSK.	mysecretkey
PKI User	When you configure *Authentication Method* as *Certificate*, select the PKI user with valid subject and certificate authority certificate that FortiSASE uses to validate the hub's certificate. You can directly create the PKI user from *Create* or via *Configuration* > *PKI*, then select it here.	mypeer

Network attributes	Description	Example
Certificate	When you configure *Authentication Method* as *Certificate*, select the certificate for the security PoP to present. You must import this certificate into FortiSASE via *System* > *Certificates* as a *Local Certificate*.	Fortinet_Factory
BGP Peer IP	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If an active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec tunnels towards each hub have different network overlay IDs.	2

5. Click *OK*.
6. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
7. (Optional) Repeat the steps to configure up to a total of 12 service connections as necessary to support your secure private access service connection network topology. The following shows the GUI after configuring two service connections:



To update the authentication method settings for a service connection:

1. Go to *Operations* > *Connectivity* > *Secure private access*.
2. Click *Update Authentication Method*.
3. Select the *Authentication Method* and configure the corresponding parameter(s):
   - *New Pre-shared Key* when *Pre-shared Key* is selected.
   - *PKI User* and *Certificate* when *Certificate* is selected.
4. Click *OK*. Once successfully updates the authentication method for the service connection, it notifies you with the message *Authentication method updated successfully*.

Considerations

- As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.
- For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.
- For security points of presence (PoP), the SD-WAN performance SLA (health check) setting has the following default parameters:
  - **Latency threshold**: 120 ms
  - **Jitter threshold**: 55 ms

- **Packet loss threshold**: 1%

You can edit these parameters in FortiSASE. See Editing SLA thresholds on page 55.

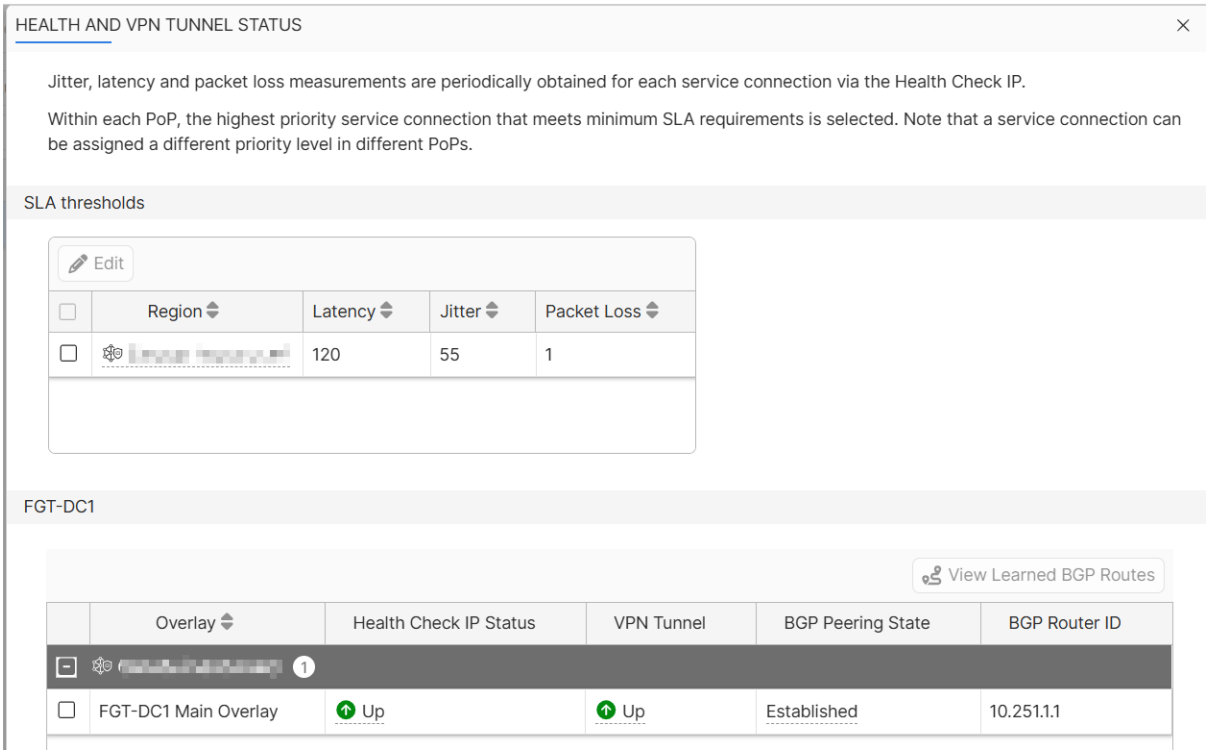
Also, for security PoPs, the SD-WAN rule is configured with the lowest cost (SLA) mode, where the security PoPs choose the lowest cost link (highest priority hub) that satisfies the SLA to forward traffic.

- In the SD-WAN rule that each security PoP uses, the interface preference order matters when selecting links of equal cost (equal priority hubs). Therefore, to define interface preference order, you must configure service connections in in the desired order of preference from the most preferred hub to the least preferred hub.

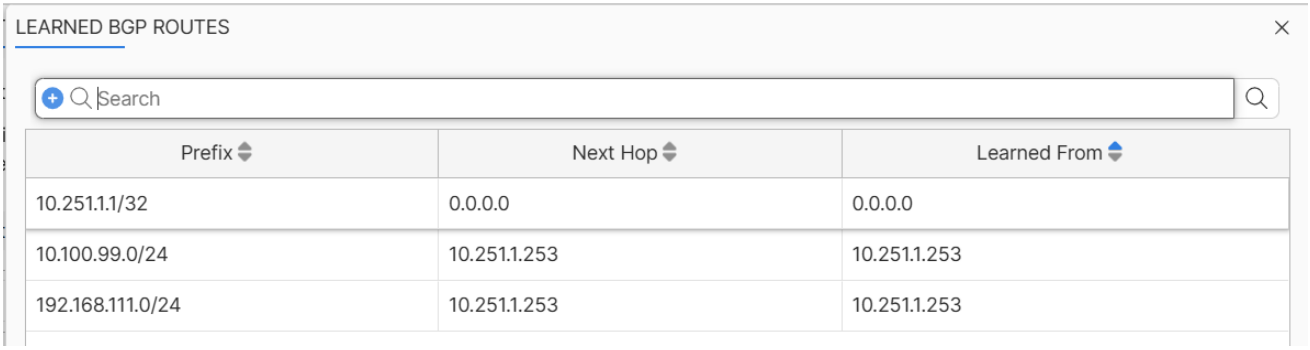
Viewing health and VPN tunnel status

Click the *Health* button at the top of the page to view the *Health and Tunnel Status* page, which shows all configured hubs' health and tunnel status. This page provides advanced monitoring of the IPsec tunnel, BGP peering state, and health check IP status that you can use for troubleshooting advanced scenarios with configured hubs.

For example, you can view two hubs' health and tunnel status from this page:



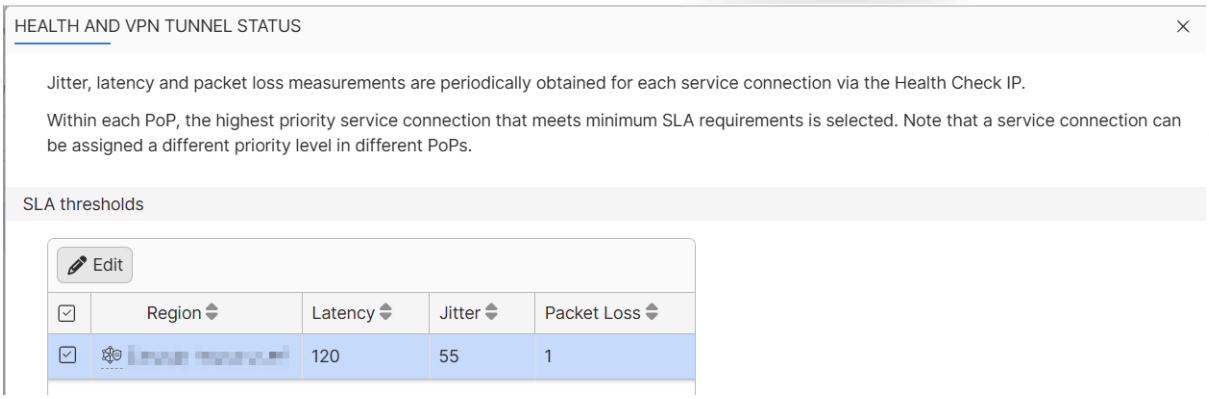
For any hub, selecting a security point of presence and clicking *View Learned BGP Routes* displays the learned BGP routes for that hub. For example, the learned BGP routes for the example DC1 are as follows:



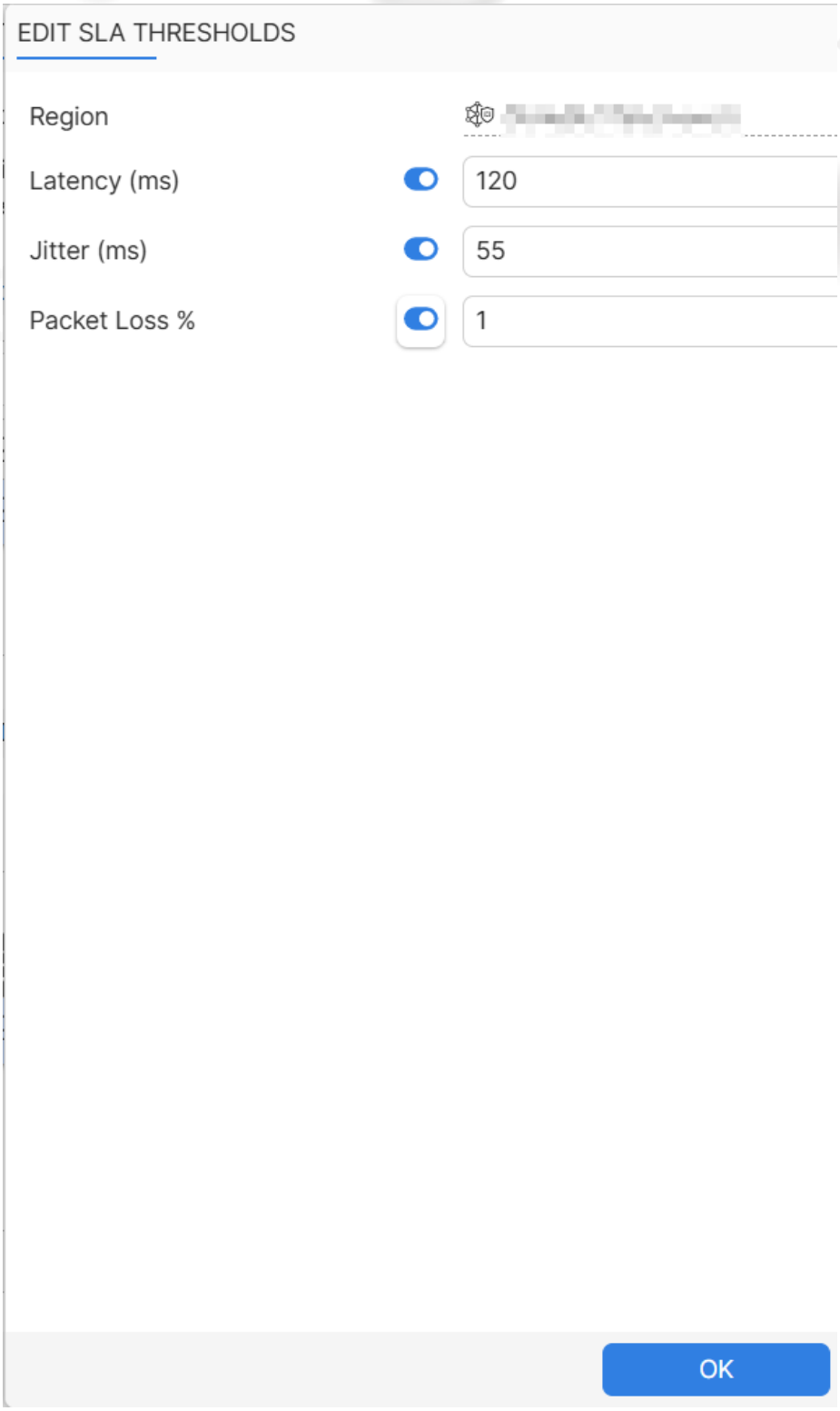
Editing SLA thresholds

You can customize latency, jitter, and packet loss SLA thresholds per security point of presence (PoP) used for secure private access hub SD-WAN health checks when *Hub Selection Method* is *Hub Health and Priority*. See Configuring BGP on page 47.

SLA thresholds can be edited from *Operations* > *Connectivity* > *Secure private access* by selecting a service connection and clicking *Health*, and then selecting a security PoP and clicking *Edit* to edit the SLA thresholds.



In the *Edit SLA Thresholds* slide-in, the default SLA threshold values are listed. You can edit each threshold by enabling it, entering a suitable value and clicking *OK*.

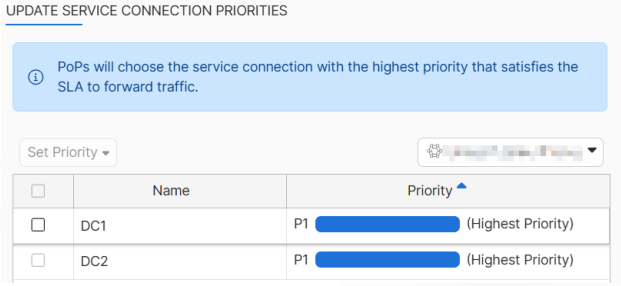


Updating service connection priorities

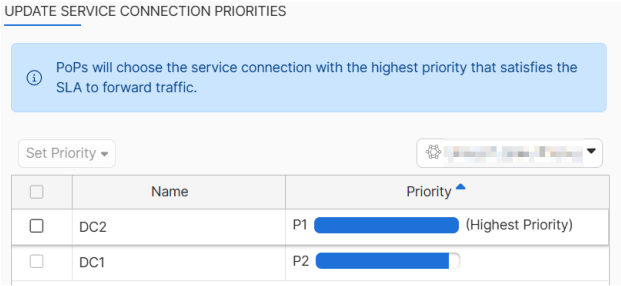
When the hub selection method is configured as hub health and priority within each security point of presence (PoP), FortiSASE selects the highest priority hub that meets minimum SLA requirements. You can assign a hub a different priority level in different security PoPs using the *Service Connection Priorities* page. A lower numerical cost value indicates a higher priority for a hub, and vice-versa.

To update hub priorities:

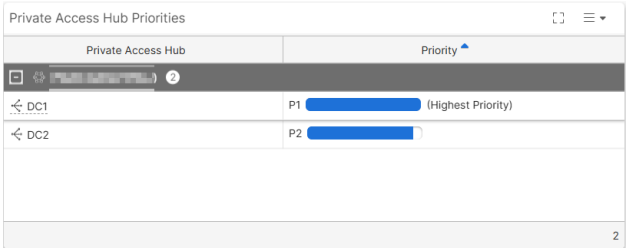
1. Go to *Operations* > *Connectivity* > *Secure private access*. Click *Service Connection Priorities*.
2. From the *Security PoP* dropdown list, select the desired security PoP hub.



3. Select the desired hub and do one of the following to set the priority:
   a. From the *Set Priority* dropdown list, select the desired priority. P1 is the highest priority, and P2 is the lowest priority.
   b. Right-click the hub, select *Set Priority*, and select the desired priority. P1 is the highest priority, and P2 is the lowest priority.
4. Set the priority for each hub that will influence hub selection. The example hub priorities are modified as follows:



5. Click *Apply* to save the updated priority values. The page sorts the hubs from highest to lowest priority:



6. (Optional) Repeat the steps to update hub priorities for other security PoPs.

Deleting a hub configuration

You cannot directly update hub configuration. You must delete any current configuration and reconfigure using new settings to update it.

To delete a hub configuration:

1. Go to *Operations* > *Connectivity* > *Secure private access*.
2. Select the desired hub(s).
3. Click *Delete*.

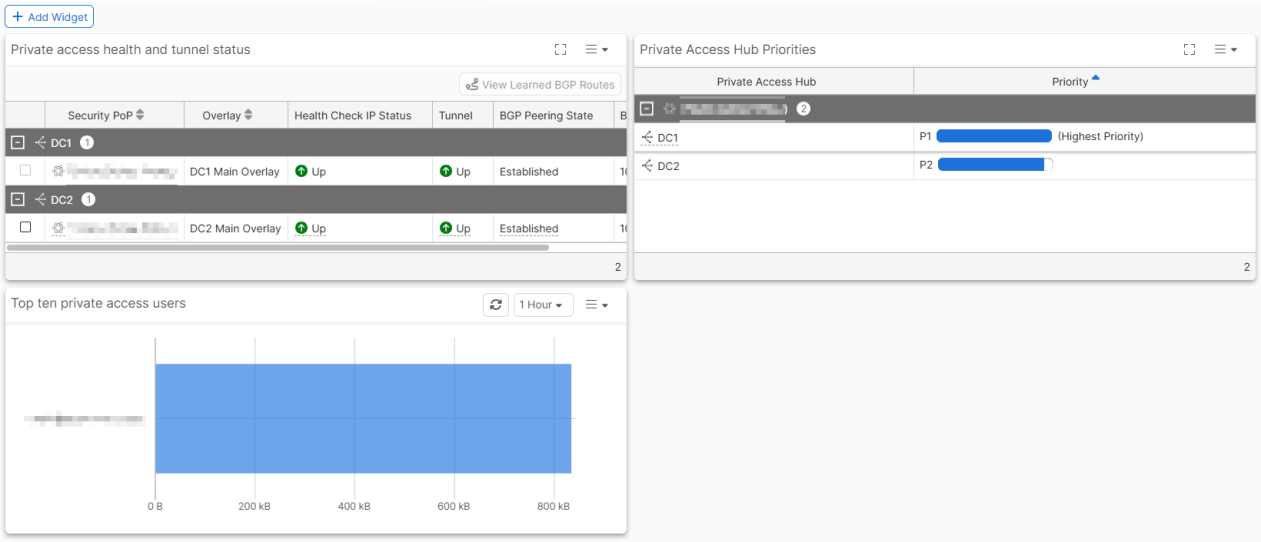
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

Monitoring private access hubs

To monitor private access hubs when they have been configured, view the following widgets in *Monitoring* > *Dashboards* > *Private access*:

- Private access health and tunnel status
- Private Access Hub Priorities
- Top ten private access users

For example, the following provides private access widgets with data for two private access hubs:



Configuring a private access policy for client-to-server traffic

Secure private access (SPA) client-to-server communication is the typical SPA use case, allowing traffic initiated from remote users (agents, proxy users, edge devices) to SPA hubs (or local networks behind SPA hubs).

For details on SPA server-to-client communication, see Configuring a private access policy for server-to-client traffic on page 61.

To configure a private access policy from remote agents and edge devices to SPA hubs:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click the *Secure private access* tab and then click the *To hubs* subtab.
3. Click *Create* to create a new policy.

4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *All*: all FortiSASE agents and edge devices • *Agent users*: remote endpoint users • *Edge Device*: Edge devices such as FortiExtender
Source	• *All Edge Devices*: Applies to all edge devices • *Specify*: specify selected hosts and host groups if you selected *Agent users*, or authorized Edge devices if you selected *Edge Device*.
User	• *Specify*: specify selected users and user groups for all source scopes • *Captive Portal Exempt*: If *Source Scope* is set to *Edge Device*, exempt the edge device traffic from encountering a captive portal to determine the identity of a connected endpoint. By default, a captive portal is enforced when edge device traffic matches policies with *Source Scope* set to *All*.
Destination	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups
Service	Click + and select services or service groups.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click *OK*.

To configure a private access policy from proxy users to SPA hubs:

1. Go to *Security* > *Traffic* > *Proxy Policies*.
2. Click the *Secure private access* tab.
3. Click *+Create* to create a new policy.

4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *All*: all HTTP and HTTPS traffic from proxy users • *Specify*: specify selected hosts and host groups
User	• *All proxy users*: All proxy users • *Specify*: specify selected users or users groups
Destination	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click *OK*.

Considerations

- For SSL remote agents, whenever changes are made to an existing secure internet access or private access policy, they take effect only after agents reconnect to FortiSASE.
- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with *Source Scope* set to *Edge Devices* will have *User* set to *Captive Portal Exempt*.
  - Any policies you created before FortiSASE 24.3.a with *Source Scope* set to *All* will not be modified. Therefore, any edge devices whose traffic matched an *All* allow policy before will now have authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any *All* allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device.
- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the Destination field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID.

Configuring a private access policy for server-to-client traffic

Secure private access (SPA) server-to-client communication allows traffic initiated from SPA hubs (or local networks behind SPA hubs) to remote users (currently agents only). This communication requires Remote agent and edge device user identification and additional configuration steps on the FortiGate SPA hub itself. See Prerequisites and considerations on page 62.

For details on SPA client-to-server communication, see Configuring a private access policy for client-to-server traffic on page 58.

To configure a private access policy to remote users from SPA hubs:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click the *Secure private access* tab and then click the *From hubs* subtab.
3. Click *+Create* to create a new policy.
4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups.
Destination	• *All*: all FortiSASE users/devices • *Agent users*: remote endpoint users
Service	Click + and select services or service groups.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click *OK*.

To configure a FortiGate SPA hub firewall policy required for traffic from SPA hubs:

On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote agents and edge device users via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE agents and edge device users.

In this example, for the FortiGate SPA hub, the SPA overlay (IPsec tunnel) is defined as *fgt_hub1* and the local connected networks DMZ_HQ and LAN_HQ are on port2 and port4, respectively. Therefore, we create a policy that allows traffic from the local connected networks on the hub to the FortiSASE remote agents.

1. On the FortiGate SPA hub, go to *Policy & Objects > Firewall Policy*.
2. Click *+Create New* to create a new policy.
3. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Incoming Interface	*DMZ_HQ (port2)* *LAN_HQ (port4)*
Outgoing Interface	*fgt_hub1*
Source	*all*
Destination	*All*
Schedule	*always*
Service	*ALL*
Action	*ACCEPT*
NAT	You can enable or disable NAT depending on the IP configuration of the organization's FortiGate SPA hub.
IP Pool Configuration	*Use Outgoing Interface Address*

4. Click *OK*.

Prerequisites and considerations

Prerequisites

- The display of the *From hubs* subtab and resulting functionality requires a FortiSASE instance with the remote VPN agent identification feature, which is included with new instances created after the FortiSASE 24.3.b release and may need to be added on instances created before that release. See Remote agent and edge device user identification. Otherwise, the *From hubs* subtab does not display.
- Currently, FortiSASE supports traffic from SPA hubs to remote agents only.
- On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote agents via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE remote agents.

Considerations

- For SSL agents, whenever changes are made to an existing secure internet or private access policy, they take effect only after SSL agents reconnect to FortiSASE.
- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with *Source Scope* set to *Edge Devices* will have *User* set to *Captive Portal Exempt*.
  - Any policies you created before FortiSASE 24.3.a with *Source Scope* set to *All* will not be modified. Therefore, any edge devices whose traffic matched an *All* allow policy before will now have authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any

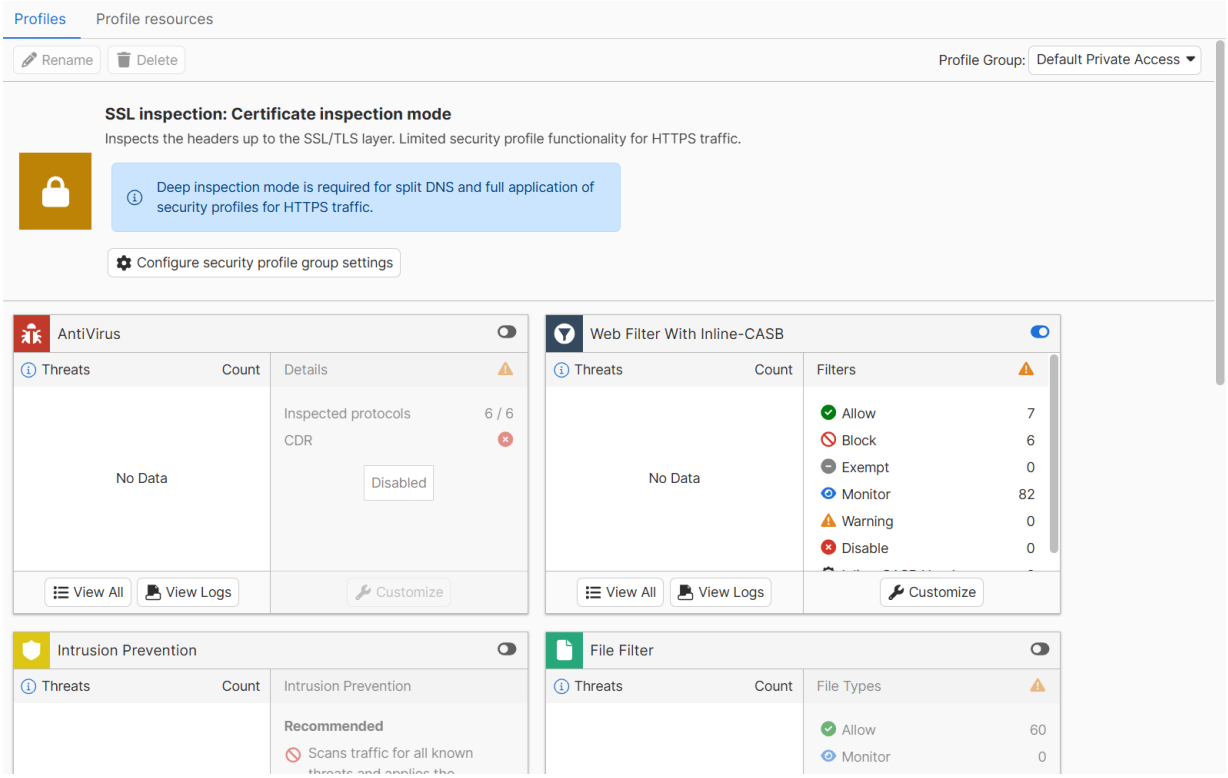
All allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device.

- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the *Destination* field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID.

Configuring a private access security profile

To configure a private access security profile:

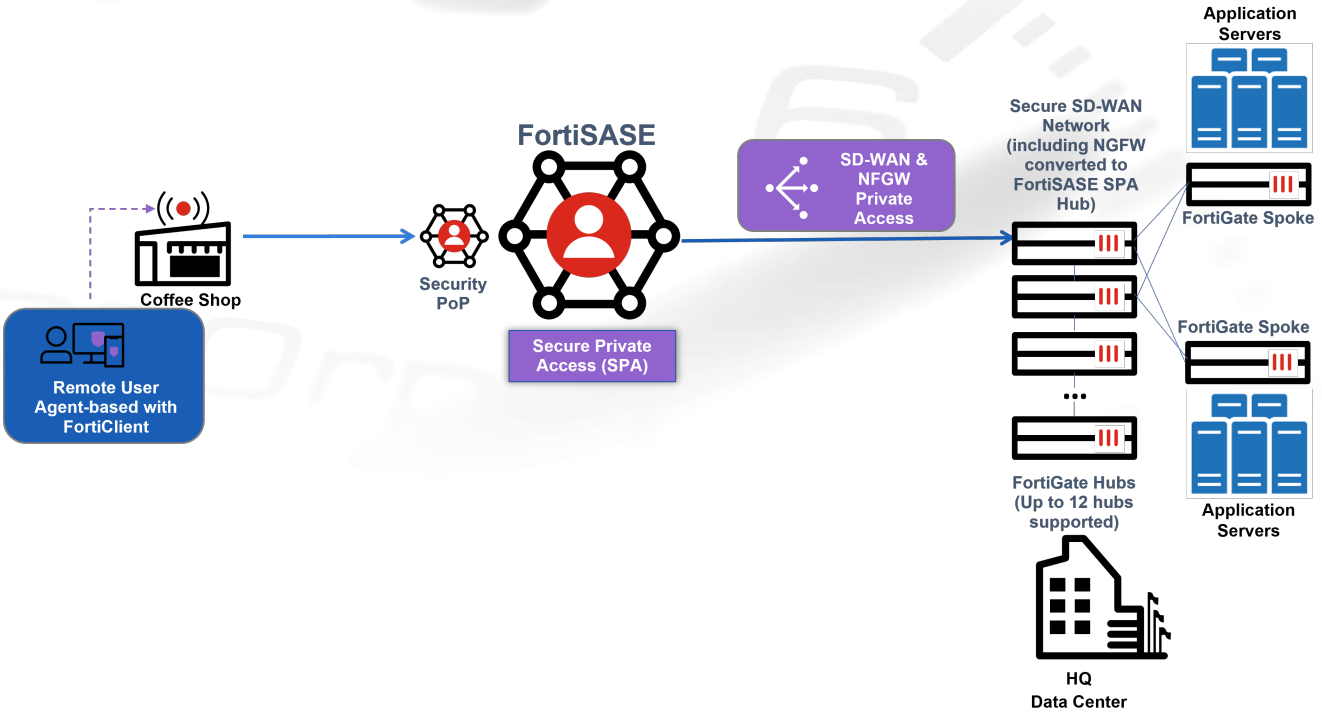
1. Go to *Security* > *Traffic* > *Security profiles*.
2. In the top right corner, select the default profile group, *Default Private Access*, or create a new one.
3. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



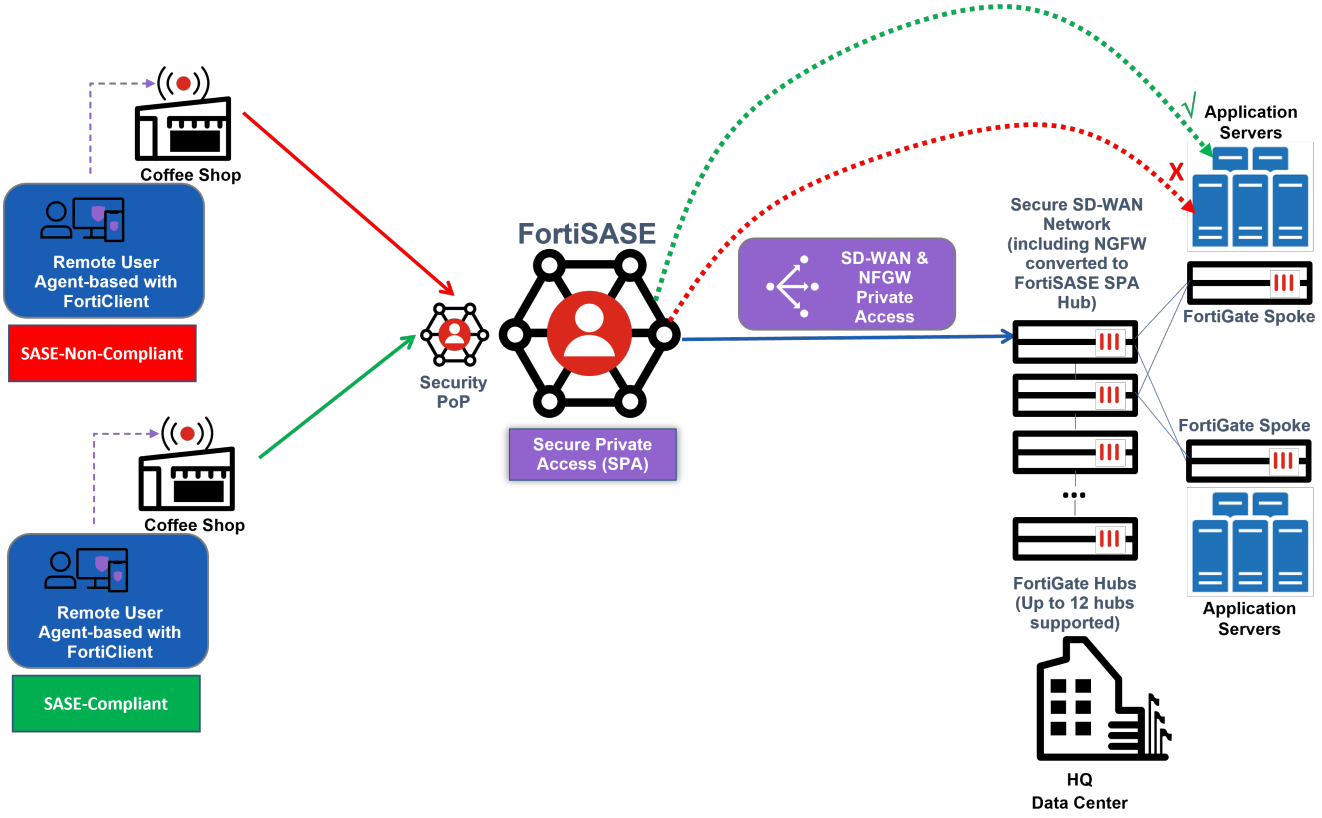
The security settings for Internet and private access are identical. For details on configuring security settings, see Security profiles.

Configuring security posture tags in private access policies

By default, for the secure private access (SPA) use cases using a FortiGate hub configured through the *Secure private access* page, all FortiSASE agent-based remote users have unrestricted access to private applications behind the hub network through an Allow-All Private Traffic private access policy.



To restrict SPA to private applications of any protocol (TCP, UDP, ICMP, and so on) behind a FortiGate hub, in the FortiSASE portal you can configure security posture tagging rules that apply security posture tags to remote users based on specified endpoint posture checks. You can then specify these tags as the source in a dynamic private access policy to deny or allow access as desired.



Using security posture tags to configure dynamic policies

You can use tags to build dynamic policies that you do not need to manually reconfigure whenever an endpoint's status changes. For example, consider that you want to deny Windows endpoints without antivirus (AV) installed and running as detected by FortiClient from accessing private applications behind the FortiGate hub. You would configure the following:

- Rule that applies a SASE-Compliant tag to Windows endpoints that FortiClient detects as having AV software installed and running
- Rule that applies a SASE-Non-Compliant tag to Windows endpoints that FortiClient detects as not having AV software installed
- Private access policy that allows Windows endpoints with the SASE-Compliant tag to access a specific server behind the FortiGate hub
- Private access policy that denies Windows endpoints with the SASE-Non-Compliant tag from accessing a specific server behind the FortiGate hub

As FortiSASE receives information from endpoints, it dynamically removes and applies the SASE-Non-Compliant tag to endpoints. For example, if an endpoint that previously had the SASE-Non-Compliant tag applied has its AV software installed or enabled as detected by FortiClient, then FortiSASE automatically removes the SASE-Non-Compliant tag from the endpoint and applies the SASE-Compliant tag instead. Consequently, the endpoint would then be able to access private applications behind the FortiGate hub.

Therefore, a dynamic policy is a policy that has one or more zero trust network access tags specified as its source.

For details on configuring dynamic tags and policies, see Tagging.

Configuration workflow

You can follow this configuration workflow, which the document describes in detail using the example configuration of a dynamic private access policy that allows access to private applications, which in this example is a private server behind the FortiGate hub:

1. Configure a security posture tagging rule set for compliant endpoints.
2. Configure a security posture tagging rule set for non-compliant endpoints.
3. Configure a dynamic private access policy to allow access to a specific private server from compliant endpoints.
4. Configure a dynamic private access policy to deny access to a specific private server from non-compliant endpoints.
5. Test the dynamic private access policies using ICMP ping to the specific private server from a compliant endpoint and from a non-compliant endpoint, respectively.

A similar workflow applies to a private access policy that allows or denies access to applications of any other protocols besides ICMP, such as TCP or UDP applications.

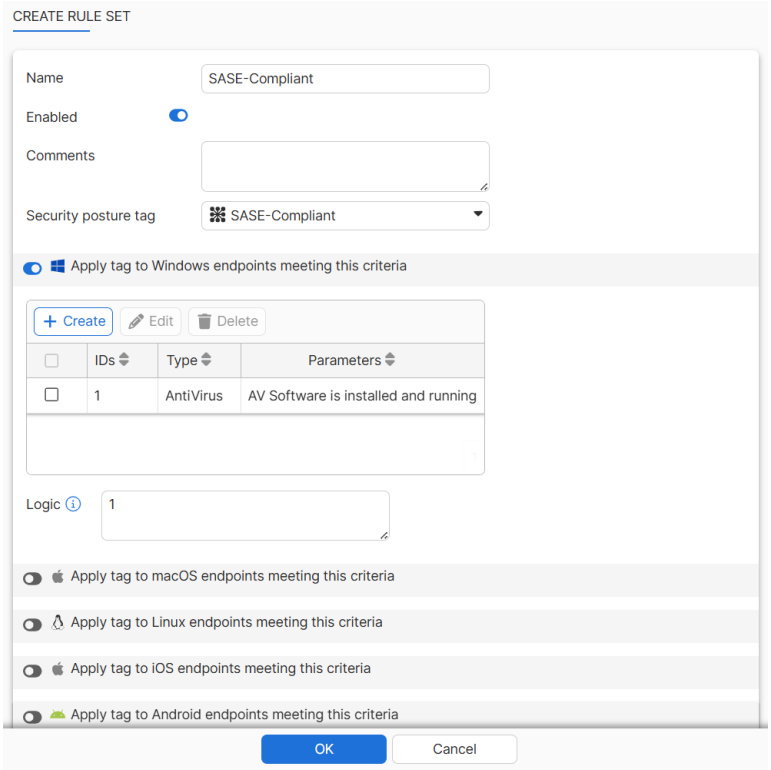
Configuring security posture tagging rule sets to dynamically tag agent-based remote users

This example demonstrates how to configure security posture tag names and tagging rule sets with the following posture checks:

- Endpoint is running Windows and has antivirus (AV) software installed and running
- Endpoint is running Windows and does not have AV software installed or running

To configure a security posture tagging rule set for compliant endpoints:

1. Go to *Endpoint management* > *Security posture tags*.
2. On the *Tagging rules* tab, click *Create*.
3. In the *Name* field, enter the desired rule set name. For example, SASE-Compliant.
4. Toggle *Enabled* on or off to enable or disable the rule.
5. (Optional) In the *Comments* field, enter any desired comments.
6. In the *Security posture tag* dropdown list, create a tag named *SASE-Compliant*. Click *OK* to select the new entry.
7. Enable *Apply tag to Windows endpoints meeting this criteria* and click *+Create*.
8. Configure the rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule type* dropdown list, select *AntiVirus*.
   c. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   d. Click *OK*.
9. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
10. Click *OK*.



To configure a security posture tagging rule set for non-compliant endpoints:

1. Go to *Endpoint management* > *Security posture tags*.
2. On the *Tagging rules* tab, click *+Create*.
3. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
4. Toggle *Enabled* on or off to enable or disable the rule.
5. (Optional) In the *Comments* field, enter any desired comments.
6. In the *Security posture tag* dropdown list, create a tag named *SASE-Non-Compliant*. Click *OK* to select the new entry.
7. Enable *Apply tag to Windows endpoints meeting this criteria* and click *+Create*.
8. Configure the rule:

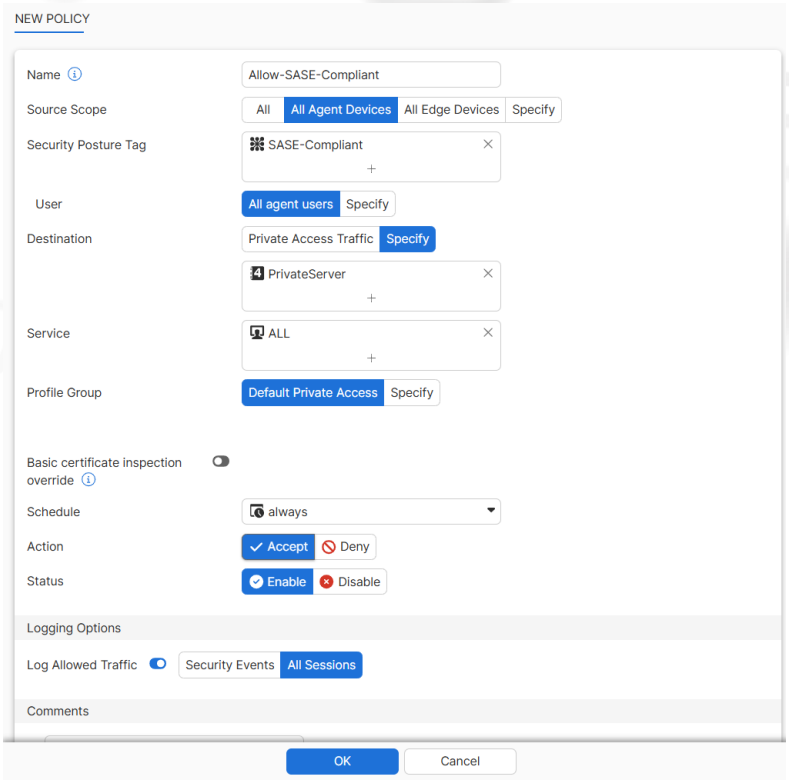
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. Select *Negate*.
   d. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   e. Click *OK*.
9. In the *Tag Name* dropdown list, create a tag named SASE-Non-Compliant.
10. Click *OK*.

Configuring dynamic private access policies using security posture tags

This example demonstrates how to configure dynamic private access policies using the security posture tags that you created in Configuring security posture tagging rule sets to dynamically tag agent-based remote users on page 65 to allow endpoints tagged as SASE-Compliant with access to selected private resources and to deny access to selected private resources for endpoints tagged as SASE-Non-Compliant.

To configure a dynamic private access policy for compliant endpoints:

1. Go to *Security* > *Traffic* > *Policies*.
2. Select *Secure private access* to display the list of private access policies. Click the *To hubs* subtab (selected by default).
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Allow-SASE-Compliant.
   b. For *Source Scope*, select *All Agent Devices*.
   c. In the *Security Posture Tag* field, click *+*.
      i. From the *Select Entries* panel, under *ZTNA* , select the *SASE-Compliant* tag.
      ii. For *User*, select *All agent users*.
   d. For *Destination*, select *Specify*, click *+*, and in the *Select Entries* panel click *+Create* and click *IPv4 Host* to a create a new host for the specific server as follows:
      i. For *Location*, select *Private Access Hub*.
      ii. For *Category*, *IPv4 Host* is selected.
      iii. In the *Name* field, enter the desired name. In this example, the name is PrivateServer.
      iv. From the *Type* dropdown list, select *Subnet*.
      v. In the *IP/Netmask* field, enter 10.100.99.101/32.
      vi. Click *OK*.
      vii. Click *OK* to select the newly created host to set it as the *Destination*.
   e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Accept*.
   g. For *Status*, select *Enable*.
5. Click *OK*.

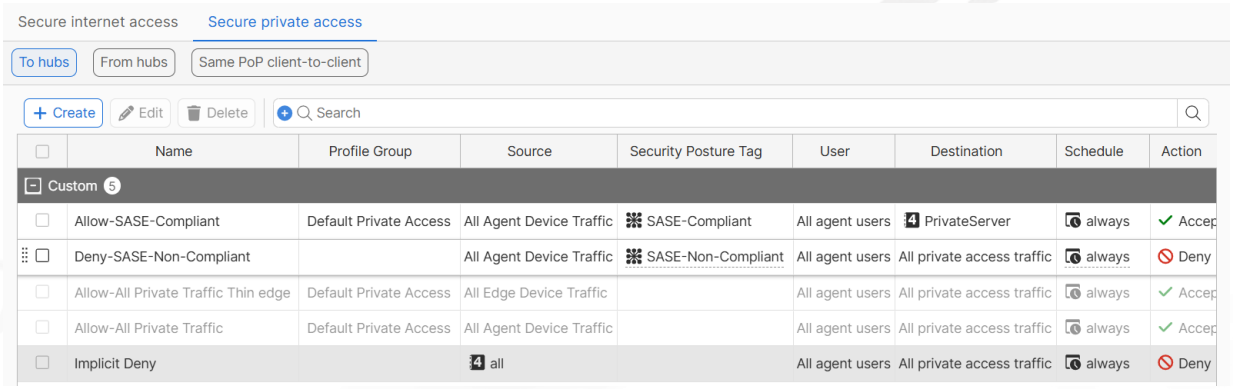


6. In *Security* > *Traffic* > *Policies* with *Secure private access* selected, ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.

To configure a dynamic private access policy for non-compliant endpoints:

1. Go to *Security* > *Traffic* > *Policies*.
2. Select *Secure private access* to display the list of private access policies. Click the *To hubs* subtab (selected by default).
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Deny-SASE-Non-Compliant.
   b. For *Source Scope*, select *All Agent Devices*.
   c. In the *Security Posture Tag* field, click *+*. From the *Select Entries* panel, under *ZTNA*, select the *SASE-Non-Compliant* tag.
      i. From the *Select Entries* panel, under *ZTNA*, select the *SASE-Non-Compliant* tag.
      ii. For *User*, select *All agent users*.
   d. For *Destination*, select *Private Access Traffic*.
   e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Deny*.
   g. For *Status*, select *Enable*.
5. Click *OK*.
6. In *Security* > *Traffic* > *Policies* with *Secure private access* selected, do the following:
   a. Ensure that you order the policies so that the *Deny-SASE-Non-Compliant* policy is before the *Allow-All Private Traffic* policy. With this policy order, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.

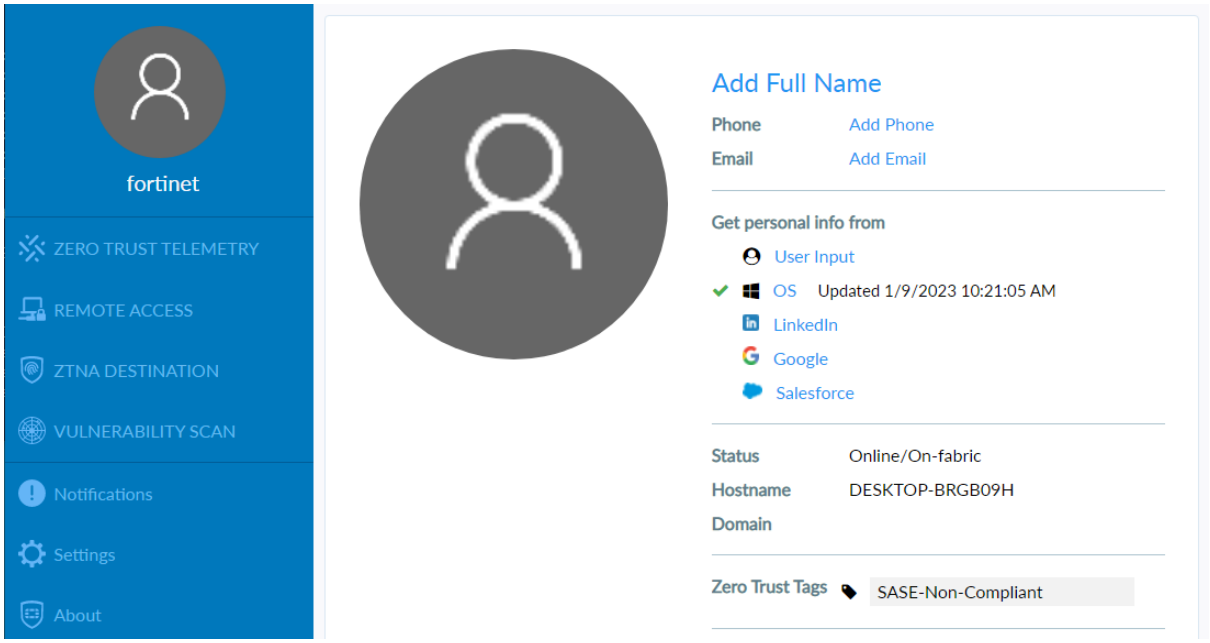
b. Disable the *Allow-All Private Traffic* and *Allow-All Private Traffic Thin edge* policies.



Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

1. In FortiSASE, go to *Endpoint management* > *Endpoint profiles*.
2. Create a new profile or edit an existing one.
3. On the *FortiClient GUI settings* tab, enable *Show security posture tags*.
4. Click *Apply*. When this option is enabled, detected tags appear on the FortiClient avatar page.



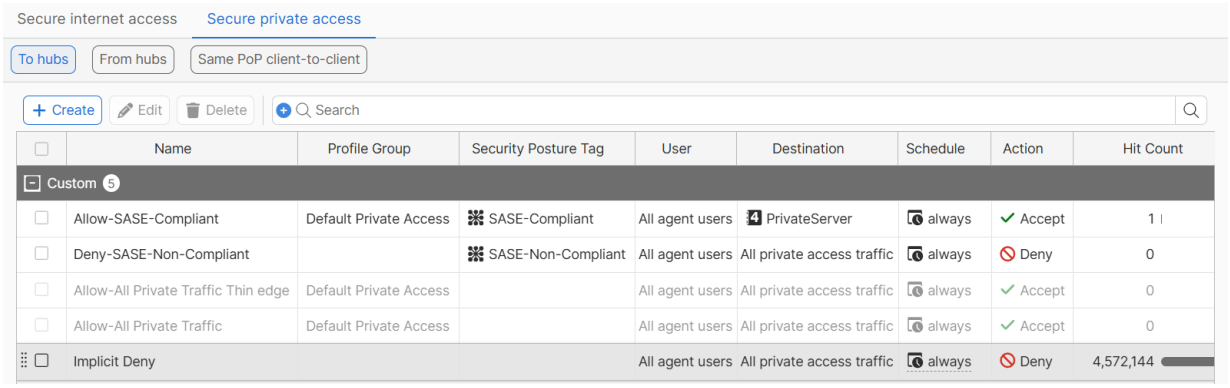
To test that FortiSASE allows a FortiClient endpoint tagged as SASE-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the agent authentication defined on FortiSASE. Click *Connect*.
4. In the Windows start menu, click the gear icon for *Settings*. Go to *Update & Security* > *Windows Security* > *Virus & threat protection*.
5. Ensure in *Virus & threat protection settings* > *Manage settings* that *Real-time protection* is enabled (by default). This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.

6. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant tag applied.
7. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
8. Observe the following output indicating the ping succeeded since FortiSASE allows access:

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=136ms TTL=62

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 137ms, Average = 136ms
```

9. In FortiSASE, in *Security* > *Traffic* > *Policies*, observe that the *Allow-SASE-Compliant* dynamic private access policy hit count increased and that the *Deny-SASE-Non-Compliant* dynamic private access policy hit count has not changed.



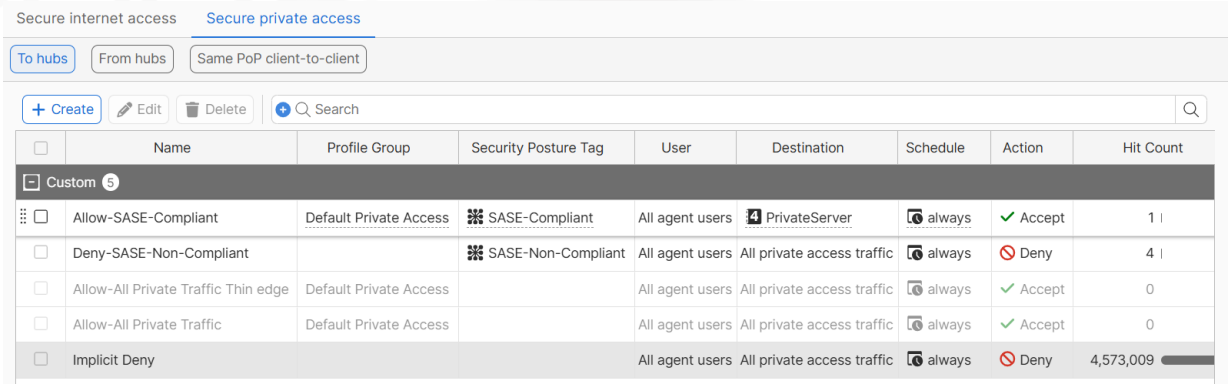
To test that FortiSASE denies a FortiClient endpoint tagged as SASE-Non-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the agent authentication defined on FortiSASE. Click *Connect*.
4. In the Windows start menu, click the gear icon for *Settings*. Go to *Update & Security* > *Windows Security* > *Virus & threat protection*.
5. Ensure in *Virus & threat protection settings* > *Manage settings* that *Real-time protection* is enabled (by default). This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.
6. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Non-Compliant tag applied.
7. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
8. Observe the following output indicating the ICMP ping has timed out since FortiSASE denies access to the specific server:

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

9. In FortiSASE, in *Security* > *Traffic* > *Policies*, observe that the *Allow-SASE-Compliant* dynamic private access policy hit count has not changed and that the *Deny-SASE-Non-Compliant* dynamic private access policy hit count has increased.

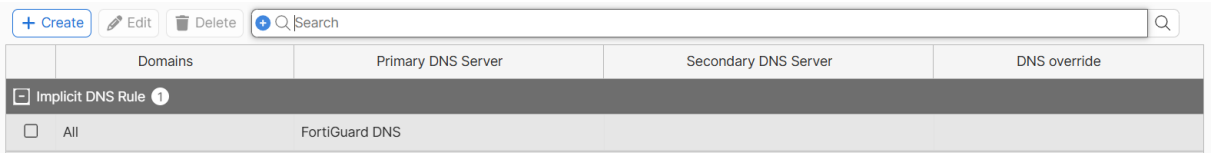


Configuring DNS Settings

Remote users use the DNS server in FortiSASE under *Network* > *DNS* to resolve hostnames for internal and external domains.

Agent and agentless endpoints and endpoints connected to authorized Edge devices forward their DNS traffic to FortiSASE. FortiSASE performs transparent DNS redirection to redirect DNS traffic conditionally as desired.

- Implicit DNS rules are predefined for agents and users connected to authorized Edge devices. FortiSASE uses these rules for resolving hostnames for external domains.
- You can create split DNS or DNS redirection rules by clicking *Create*. FortiSASE uses these rules for resolving hostnames for internal domains. See Split DNS Rules on page 74.



By default, FortiSASE deployments use FortiGuard DNS as the default DNS server for the *All* implicit DNS rule. You can select any implicit DNS rule and click *Edit* to change the default DNS server.

You can configure *Default DNS Server* with one of the following options, then click *OK* to save the change:

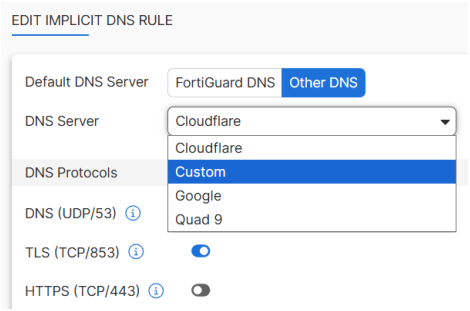
DNS Server	Description	Primary and secondary DNS server IP address
FortiGuard DNS	Use FortiGuard DNS	• 96.45.45.45 • 96.45.46.46

DNS Server		Description	Primary and secondary DNS server IP address
Use endpoints' system DNS		Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS		Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
	CloudFlare	Use the Cloudflare public DNS server	• 1.1.1.1 • 1.0.0.1
	Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify primary and secondary DNS IP address
	Google	Use the Google public DNS server	• 8.8.8.8 • 8.8.4.4
	Quad 9	Use the Quad 9 public DNS server	• 9.9.9.9 • 149.112.112.112

For example, you can edit the Tunnel implicit DNS rule to use a custom DNS server as follows:

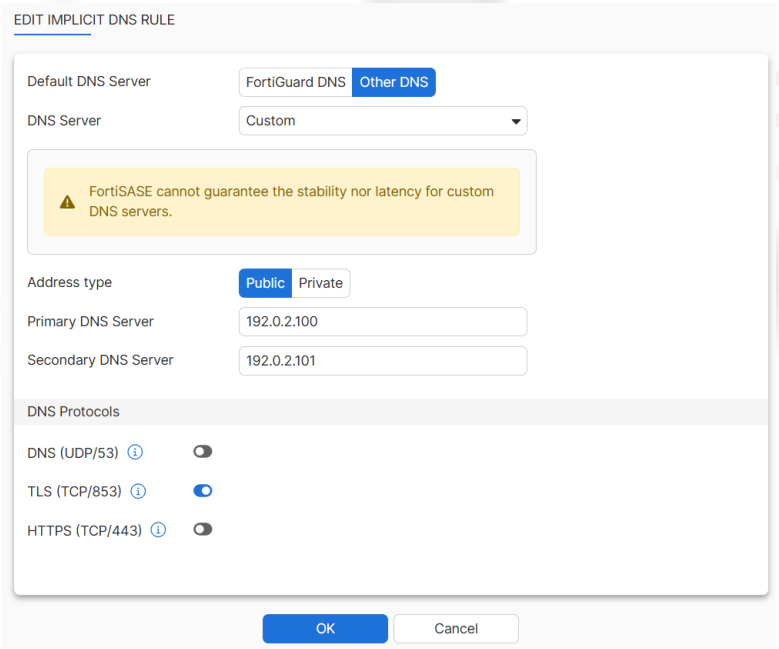
To configure a custom DNS server:

1. Go to *Network* > *DNS*, select the *All* implicit DNS rule, and click *Edit*.
2. In the *Edit Implicit DNS Rule* page, for *Default DNS Server*, select *Other DNS*.
3. From the *DNS Server* dropdown, select *Custom*.



4. In the *Primary DNS Server* and *Secondary DNS Server* fields, enter the respective IP addresses for the servers of your choice.

The screenshot uses IP addresses for documentation and should not be used in a production environment.



5. Click *OK*.

Using FortiGuard DNS or another public DNS service is sufficient for most secure internet access (SIA) use cases that simply require remote users to resolve hostnames for external domains.

Considerations

- The *All* Implicit DNS rule does not apply to Proxy users. Proxy users always use FortiGuard DNS servers.
- FortiGuard DNS servers do not support DNS over TCP. If you require DNS over TCP, edit implicit DNS rules from the default FortiGuard DNS server to other DNS servers that support DNS over TCP.
- FortiSASE cannot guarantee the stability nor latency for custom DNS servers. These factors must be considered by the customer or provider maintaining the custom DNS servers.
- FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs in the DNS, RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.
  - Implicit and DNS redirection rules for agent traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.
  - When the SPA hub has been configured with BGP on loopback, you will also need to set *Access Type* to *Private* in the DNS, RADIUS or LDAP server settings.
  - Ensure that your FortiSASE remote users have access to the internal DNS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 83.
- For edge devices, additional configuration is required to support DNS redirection rules and DNS filter functionality:
  a. Go to *Security* > *Traffic* > *Policies*.
  b. In the *Custom* section, edit the *Captive portal DNS traffic exemption (captive-dns-exempt)* policy.
  c. For *Profile Group*, select *Default* or select *Specify* and select a profile group with the DNS filter enabled.
  d. Click *OK* to save the policy changes.

Split DNS Rules

FortiSASE users often must resolve internal hostnames that public DNS servers cannot resolve in scenarios including but not limited to:

- Agent-based users are located within the organization's local network, also known as being on-net, and users must use an internal DNS server instead of a public DNS server.
- Agent-based, agentless, or Edge device users are located remotely, FortiSASE Private Access has been configured with secure private access (SPA) hubs, and users must use an internal DNS server behind the SPA hub.

To support these scenarios, you can configure FortiSASE DNS settings for DNS redirection using DNS redirection rules.

DNS redirection works as follows:

- Agent and agentless endpoints and endpoints connected to authorized edge devices forward all their DNS traffic to FortiSASE.
- FortiSASE performs transparent DNS redirection to redirect DNS traffic conditionally as desired.
- Selectively use an internal DNS server only when it is necessary to resolve hostnames for the specified internal domain(s). If you have multiple internal DNS servers in different geographical locations, you can configure remote users to use the internal DNS server that is closest to their region using *PoP DNS override*, which enhances the DNS response time.
- Resolve all other hostnames for external domains using the implicit DNS rule.

Some agent-based endpoints like mobile devices provide limited options for overriding the DNS server. Therefore, transparent DNS redirection also allows managed mobile agent-based users with iOS and Android devices to leverage DNS redirection.

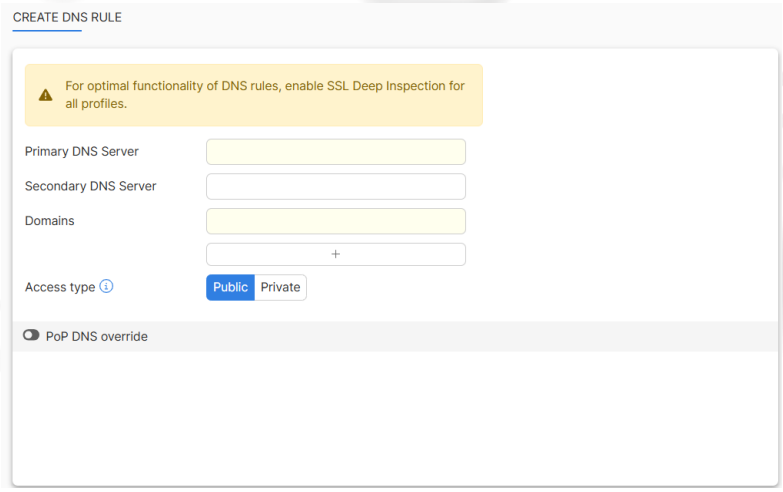
DNS redirection is more efficient than sending all DNS requests to DNS servers defined in the implicit DNS rules because it reduces any potential latency and downtime with using these DNS servers for resolving public hostnames if any issues arise with these limited availability and limited resource DNS server deployments. For resolving hostnames for external domains, DNS redirection can leverage the redundancy, extensive resources, and geographical coverage of public DNS servers with anycast capabilities.

To secure DNS requests, the DNS-over-HTTPS (DoH) protocol secures DNS requests and replies sent and received over HTTPS and works with public DNS servers that support this protocol. DoH is enabled by default on modern web browsers including Chrome, Edge, and Firefox and is supported by Google's public DNS servers, which is the default for upgraded FortiSASE deployments. Therefore, for DNS redirection rules to work with DNS servers that support DoH, you must enable SSL deep inspection for agent-based remote users on FortiSASE.

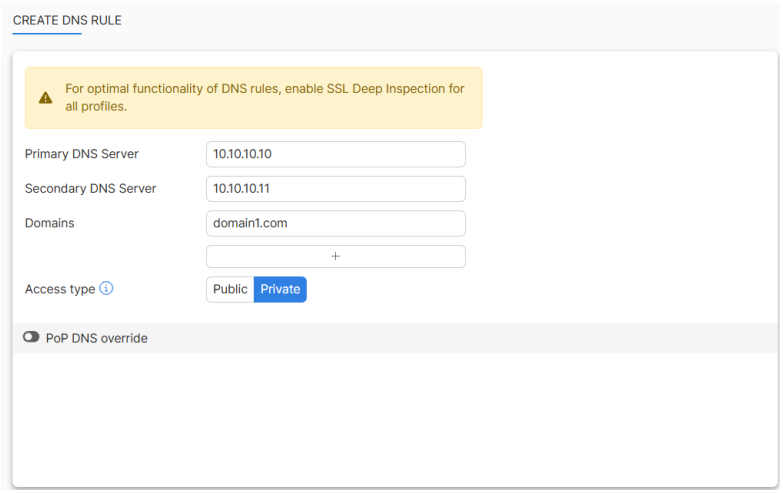
Configuring DNS redirection rules

To configure DNS redirection rules:

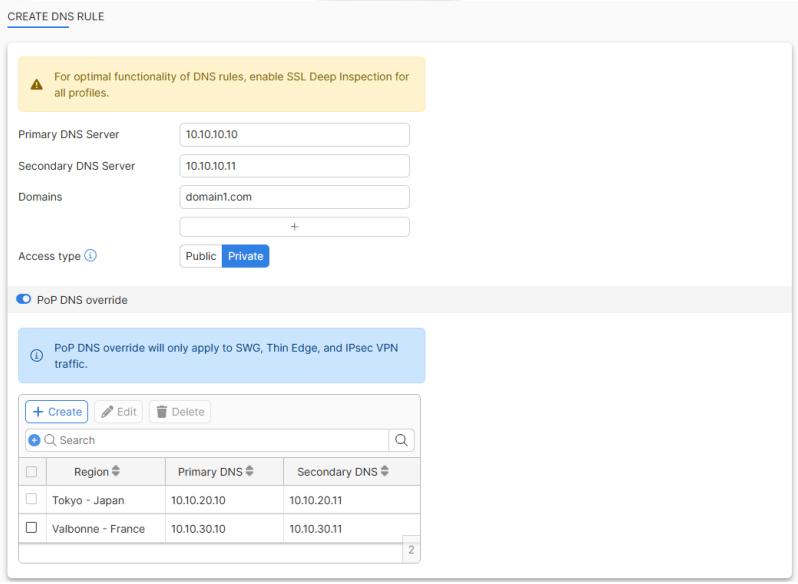
1. Go to *Network* > *DNS*.
2. Click *Create*.



3. In the *Create DNS Rule* pane, do the following:
   a. Enter the *Primary DNS Server*, (optional) *Secondary DNS Server*, and one or more *Domains*.
   b. (Optional) Click *+* to add more fields to enter in additional domains.
   c. The *Access type* field is only visible and required if you have SPA configured using *BGP on loopback* BGP routing design under *Network > BGP*. If the specified DNS server(s) are reachable via SPA, set *Access type* to *Private*. If the DNS servers are publicly accessible and not routed via SPA, set *Access type* to *Public*.



4. If you have multiple internal DNS servers spread geographically, enable *PoP DNS override* for remote endpoints to use geographically closest DNS server to them:
   a. Click *Create*.
   b. Select the *PoP* region using dropdown and specify the *Primary DNS Server* and (optional) *Secondary DNS Server*.
   c. Click *Submit*.
   d. Perform the same steps to configure different DNS server(s) per region. As shown, the remote endpoint closest to Tokyo-Japan region will use 10.10.20.10 and 10.10.20.11 as its DNS server, whereas remote endpoints closest to Valbonne-France region will use 10.10.30.10 and 10.10.30.11 as its DNS server, to resolve the domain domain1.com.



a. Only two internal DNS servers are configurable per region for each domain. If the region does not appear in the list of security PoPs to use, the remote endpoint users uses the main *Primary* and/or *Secondary DNS Server* i.e. 10.10.10.10 and 10.10.10.11 to resolve the domain.

b. Click *OK* to save the DNS redirection rule.

5. Observe that the DNS redirection rule has been created and displays in the table.

Prerequisites and considerations

Prerequisites

- DNS redirection requires enabling SSL deep inspection on FortiSASE so that FortiSASE can intercept the DNS traffic.
  - To confirm that you enabled SSL deep inspection, go to *Security* > *Security profiles* and at the top of the security profile group page, in the *SSL Inspection* section, confirm that it displays *SSL inspection: Deep inspection mode*.
  - To enable SSL deep inspection, go to *Security* > *Security profiles* and at the top of the security profile group page, in the *SSL Inspection* section, click *Configure SSL*. In the *SSL Inspection* pane, select *Deep inspection* and click *OK*.

  See Certificate and deep inspection modes.
- With deep inspection enabled, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing certificate authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.
  - FortiSASE supports automatically installing the FortiSASE CA certificate for agent-based users with FortiClient installed on their endpoints.
  - The FortiSASE CA certificate must be manually installed on endpoints for Proxy users and edge device users.
    - For Proxy users, installing this CA certificate is part of the Proxy onboarding process.
    - For endpoints using an edge device, installing this CA certificate is an additional step that they must perform.

  See Installing a certificate for deep inspection mode for installing the FortiSASE CA certificate.
- Ensure that your FortiSASE remote users have access to the internal DNS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 83.

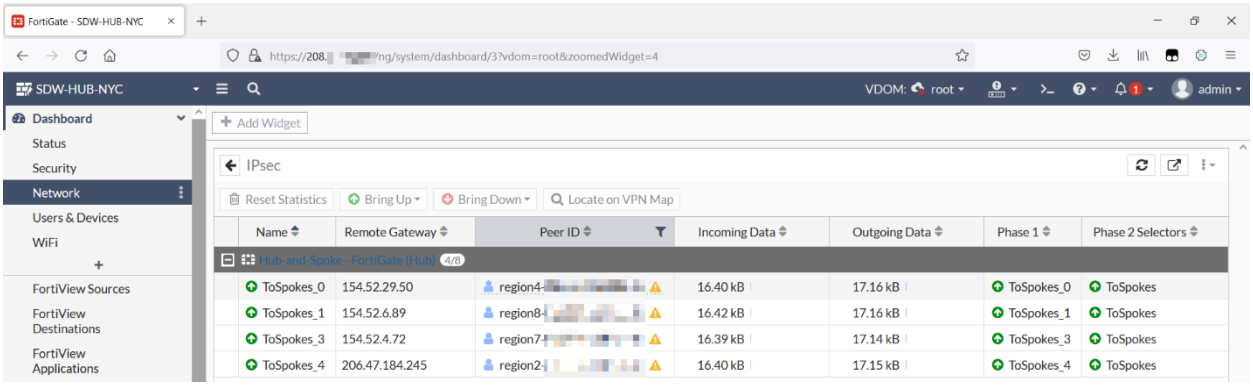
Considerations

- For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring DNS redirection using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE will yield inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that DNS redirection is configured using an internal DNS server with a public IP address.
- DNS redirection supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.
- FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.
- Implicit and DNS redirection rules for agent traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.
- If you are using DNS redirection to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.
- Security PoP DNS override will only apply to Proxy, Thin Edge (edge device), and IPsec traffic.
- If you are using DNS redirection to resolve local domains using an internal DNS server with an SPA hub configured, then the Web Filter or DNS Filter blocks access to these local domains from FortiClient remote users if the Newly Observed Domain category is set to Block in the respective security component. In this case, you must create URL Filter entries for the Web Filter or Domain Filter entries for the DNS Filter to allow access to these local domains.
- For edge devices, additional configuration is required to support DNS redirection rules and DNS filter functionality:
  a. Go to *Security* > *Traffic* > *Policies*.
  b. In the *Custom* section, edit the *Captive portal DNS traffic exemption (captive-dns-exempt)* policy.
  c. For *Profile Group*, select *Default* or select *Specify* and select a profile group with the DNS filter enabled.
  d. Click *OK* to save the policy changes.

Verifying IPsec tunnels on the FortiGate hub

Verify that the IPsec tunnels immediately appear on the FortiGate hub from all configured FortiSASE security points of presence(PoP).

On the FortiGate hub, verify that the IPsec tunnels from the FortiSASE PoPs acting as spokes by going to *Dashboard* > *Network* and clicking the *IPsec* widget to expand it.



To verify IPsec tunnels using the CLI:

1. Run at least one of the following commands. For a VDOM-enabled hub FortiGate, enter the proper VDOM before running the command(s):
   diagnose vpn ike gateway list
   diagnose vpn tunnel list
   get vpn ipsec tunnel summary
   a. For `diagnose vpn ike gateway list`, confirm that the phase 1 IKE security associations (SA) for the FortiSASE security PoPs with corresponding peer IDs are established. Confirm that the IKE SA and IPsec SA show created and established as 1/1. The following shows sample output for this command:

```
vd: root/0
name: ToSpokes_1
version: 2
...
created: 923s ago
peer-id: region8-fos001-tiui7pzu-1
...
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms


 ...
 direction: responder
 status: established 923-923s ago = 10ms
 proposal: aes128-sha256
 child: no
 ...
 PPK: no
 message-id sent/recv: 1/2
 lifetime/rekey: 86400/85206
 DPD sent/recv: 00000001/00000001
 peer-id: region8-fos001-tiui7pzu-1
```

2. For `diagnose vpn tunnel list`, confirm that the phase 2 IPsec SAs for the FortiSASE security PoPs are established. Confirm that the SA field exist and are populated. The following shows sample output for this command:

```
name=ToSpokes_1 ver=2 serial=3ba 208.85.68.228:4500->154.52.6.89:52270 tun_id=10.150.160.2 tun_
id6=::10.0.3.147 dst_mtu=1500 dpd-link=on
 weight=1
bound_if=25 lgwy=static/1 tun=intf/2 mode=dial_inst/3 encap=none/9096 options[2388]=npu rgwy-chg rport-
chg frag-rfc  run_state=0 accept_
traffic=1 overlay_id=0
parent=ToSpokes index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0 ad=s/1
stat: rxp=2689 txp=1042 rxb=16418 txb=18338
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=52270
proxyid=ToSpokes proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42258/0B replaywin=2048
       seqno=411 esn=0 replaywin_lastseq=00000a80 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
```

```
dec: spi=fd64b472 esp=aes key=16 0ab999cd40bc420cc78556f84b37747f
  ah=sha1 key=20 2e9f19e91d696d530adefb3d219ad1c74d08dcd8
enc: spi=14c9a05c esp=aes key=16 5446e233d666319b8f88fd1768f774b0
  ah=sha1 key=20 15989dc3ef5fd1d0b385df93241e0d6a0b373826
dec:pkts/bytes=2689/16346, enc:pkts/bytes=1042/21844
npu_flag=03 npu_rgwy=154.52.6.89 npu_lgwy=208.85.68.228 npu_selid=33d dec_npuid=1 enc_npuid=1
```

3. For `get vpn ipsec tunnel summary`, confirm that the phase 2 IPsec selectors for the FortiSASE security PoPs are sending and receiving traffic. Confirm that `selectors(total,up): 1/1`, `rx(pkt,err)`, and `tx(pkt,err)` are non-zero. The following shows sample output for this command:

```
'ToSpokes_0' 154.52.29.50:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err): 1043/0
'ToSpokes_1' 154.52.6.89:52270  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err): 1042/0
'ToSpokes_2' 50.208.126.11:0  selectors(total,up): 1/1  rx(pkt,err): 22149/0  tx(pkt,err): 55050/37
...
'ToSpokes_4' 206.47.184.245:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err): 1043/0
...
```

Verifying BGP routing on the FortiGate hub

To verify that all BGP peering is up on the FortiGate hub:

1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:
   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes
2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Static & Dynamic Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

Testing private access connectivity to FortiGate hub network from remote agents and edge devices

By using ping, you can verify access to the FortiGate hub network from FortiSASE remote users, namely, FortiClient users connected to FortiSASE in FortiClient agent-based mode and users behind FortiSASE edge devices.

For example, from a FortiClient user connected to FortiSASE, use ping within a Windows Command Prompt to verify access to a host behind the FortiGate hub internal network. The example pings 10.50.101.50, which is on an internal network. The following shows sample output:

```
C:\>ping 10.50.101.50

Pinging 10.50.101.50 with 32 bytes of data:

Reply from 10.50.101.50: bytes=32 time=80ms TTL=62

Reply from 10.50.101.50: bytes=32 time=80ms TTL=62

Reply from 10.50.101.50: bytes=32 time=80ms TTL=62

Reply from 10.50.101.50: bytes=32 time=84ms TTL=62
```

Testing private access connectivity to FortiGate hub network from remote proxy users

This example requires *System > Proxy configuration* and *Access & authentication > Authentication Sources > SSO > Proxy* to be configured appropriately. See Proxy client onboarding and Configuring FortiSASE with Entra ID SSO in proxy agentless mode.

By default, all proxy users can access all private access resources. You can limit proxy user access to private access resources by creating a private access policy for proxy users.

You can verify access to the FortiGate hub network from FortiSASE proxy users by using a web browser to access a host on the hub local network.

For example, consider the case when a host on the hub local network has an HTTP server running on 10.100.99.101 and only the default private access policy for proxy users is in place in FortiSASE.

To test private access connectivity to FortiGate hub network from remote proxy users:

1. From a web browser configured for proxy enter http://10.100.99.101.
2. If this is the first time going out to the internet, you will be prompted by SAML SSO to enter your credentials.
3. After entering your credentials, you should be able to access the web site at http://10.100.99.101 .

Testing private access connectivity from FortiGate hub network to remote agents

This test depends on a private access policy being defined in the *From Hub* direction on a FortiSASE instance with the remote agent identification selected availability feature. See Remote agent identification.

You can verify access from the FortiGate hub network to FortiSASE agents, namely FortiClient users connected to FortiSASE in FortiClient agent-based endpoint mode using ping.

From a host behind the FortiGate hub internal network, use ping to verify access to a FortiClient user connected to FortiSASE

The example pings the FortiClient user with 100.65.0.1 from 10.100.99.104, which is a host on an internal network. The following shows sample output:

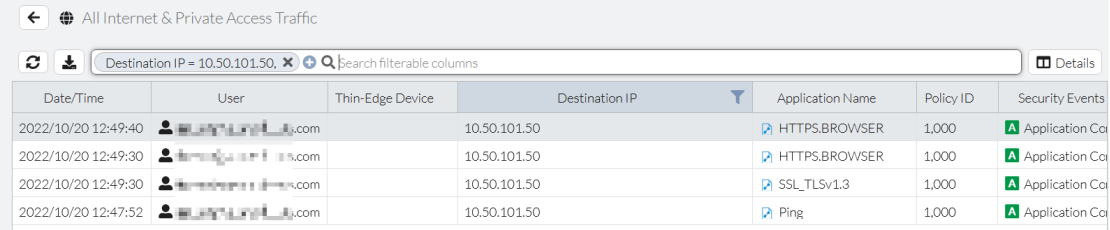
```
root@internal-server-01:~# ping 100.65.0.1
PING 100.65.0.1 (100.65.0.1) 56(84) bytes of data.
64 bytes from 100.65.0.1: icmp_seq=1 ttl=126 time=73.3 ms
64 bytes from 100.65.0.1: icmp_seq=2 ttl=126 time=72.5 ms
64 bytes from 100.65.0.1: icmp_seq=3 ttl=126 time=74.0 ms
64 bytes from 100.65.0.1: icmp_seq=4 ttl=126 time=72.1 ms
^C
--- 100.65.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 72.127/73.008/74.034/0.735 ms
```

Verifying private access traffic in FortiSASE portal

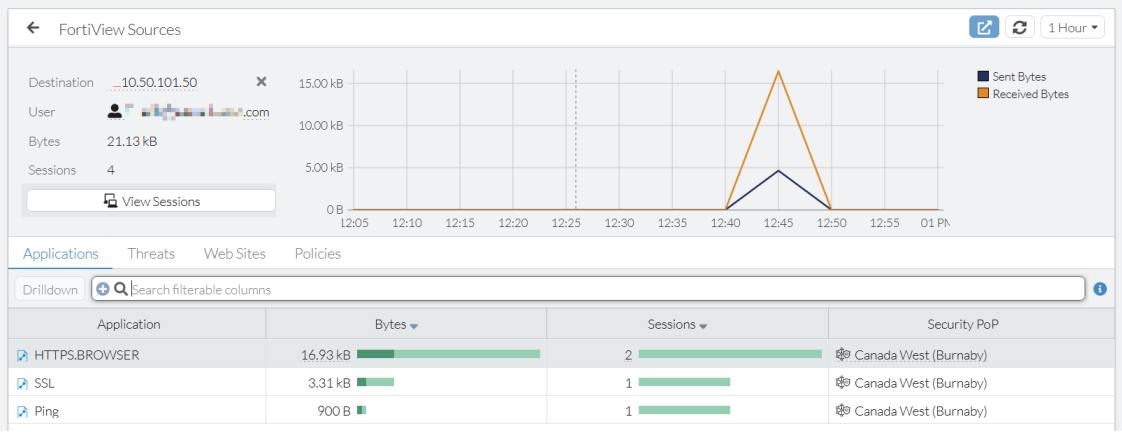
In FortiSASE, you can verify traffic from FortiSASE remote users has reached private access destinations through these methods:

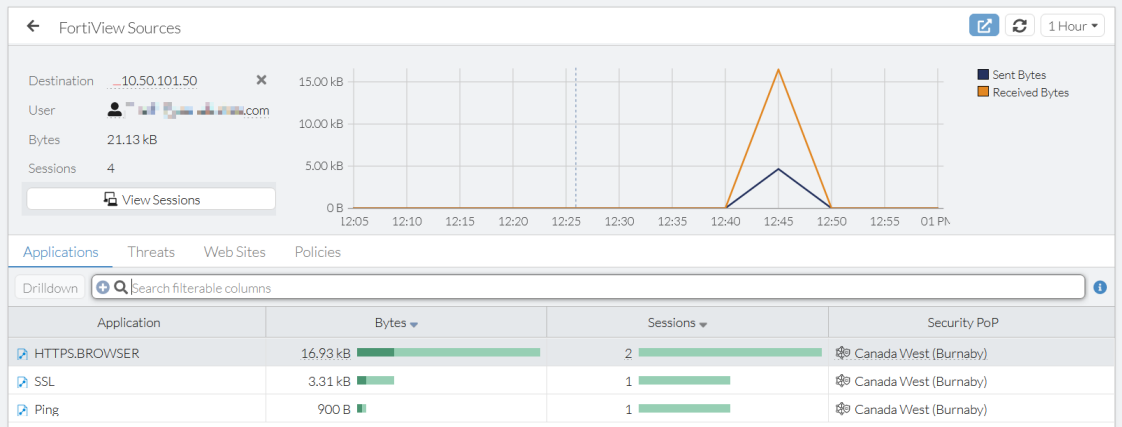
- From *Operations* > *Logs* > *Traffic* by viewing *All Internet* & *Private Access Traffic* , *Private Access Traffic (To Hubs)*, or *Private Access Traffic (From Hubs)*
- From *Monitoring* > *Monitors* > *FortiView Sources*, *Monitoring* > *Monitors* > *FortiView Destinations*, or *Monitoring* > *Monitors* > *FortiView Policies* and filtering on the private access destination IP address

Following is an example of the *Operations* > *Logs* > *Traffic* > *All Internet & Private Access Traffic* page, filtered for the private access destination IP address 10.50.101.50.



Following are examples of the *Monitoring* > *Monitors* > *FortiView Sources*, *Monitoring* > *Monitors* > *FortiView Destinations*, or *Monitoring* > *Monitors* > *FortiView Policies* pages, filtered on the private access destination IP address 10.50.101.50.





Verifying private access traffic from hubs

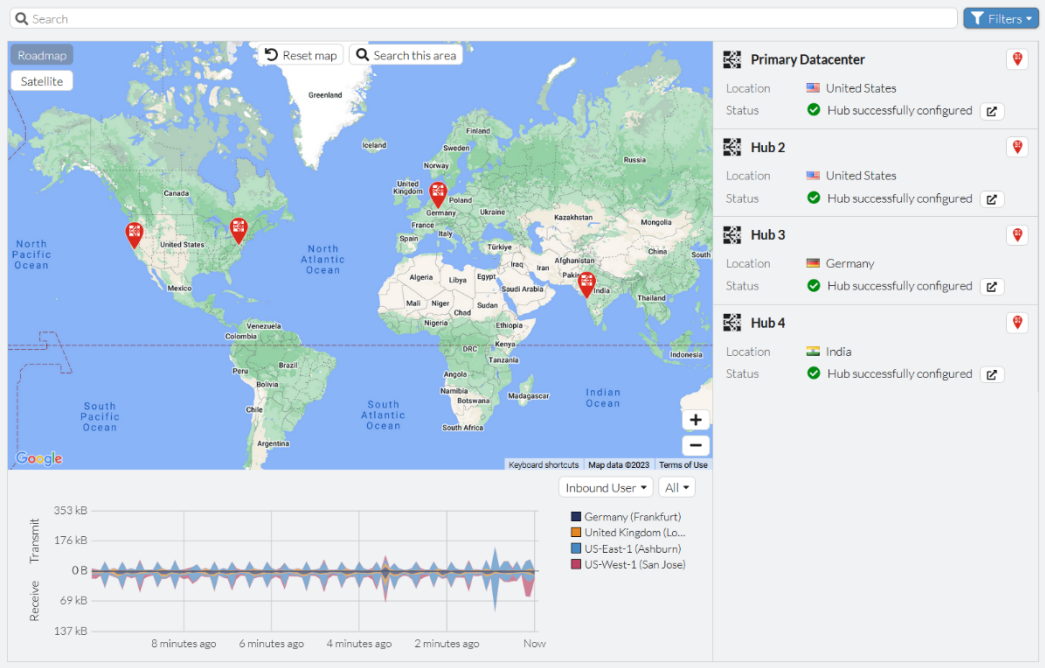
In FortiSASE, you can verify traffic from SPA hub sources (local networks or connected spokes) has reached FortiSASE remote user destinations through these methods:

- From *Operations* > *Logs* > *Traffic* by viewing *All Internet & Private Access Traffic* or *Private Access Traffic (From Hubs)*
- From *Monitoring* > *Monitors* > *FortiView Sources*, *Monitoring* > *Monitors* > *FortiView Destinations*, or *Monitoring* > *Monitors* > *FortiView Policies* and filtering on the remote agent destination IP address

Verifying private access hub status and location using the asset map

The *Operations* > *Connectivity* > *Asset Map* page in the FortiSASE portal supports filtering on *Private Access Hub* assets to display their status and geographical location.

Following is an example of the asset map filtered on *Private Access Hub* assets.



Restricting access using a FortiGate SPA hub/spoke policy

Depending on your network topology, the private HTTPS server you are providing access to through SPA may either be connected to the FortiGate SPA hub device directly or to a FortiGate spoke device that is connected to the hub device using an IPsec overlay, specifically, ADVPN.

If you have previously configured SPA, then you are already using a firewall policy on either your FortiGate SPA hub device or FortiGate spoke device (if applicable to your network topology) to the LAN interface that your private server is connected to. As a best practice, you may have restricted access to your private server from agents only by specifying the IPAM subnet as a source address. See IPAM configuration.

You can update this firewall policy to restrict access to your private server from agentless ZTNA users by adding the SPA BGP spoke IP range as a source address. This spoke IP range determines the private IP addresses that the SPA hub assigns after Security PoPs establish IPsec connections with it. This spoke IP range is configured on the FortiGate SPA hub as part of the IPsec Phase 1 configuration in the IKEv2 mode configuration address range settings.

To restrict access using a FortiGate SPA device firewall policy:

1. On the FortiGate SPA hub, confirm the IKEv2 mode configuration address range using these CLI commands:

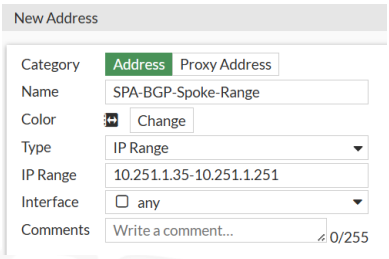
   ```
   show vpn ipsec phase1-interface | grep ipv4-
   ```

   Example output:

   ```
   FGT # show vpn ipsec phase1-interface | grep ipv4-
   set ipv4-start-ip 10.251.1.35
   set ipv4-end-ip 10.251.1.251
   set ipv4-netmask 255.255.255.0
   ```

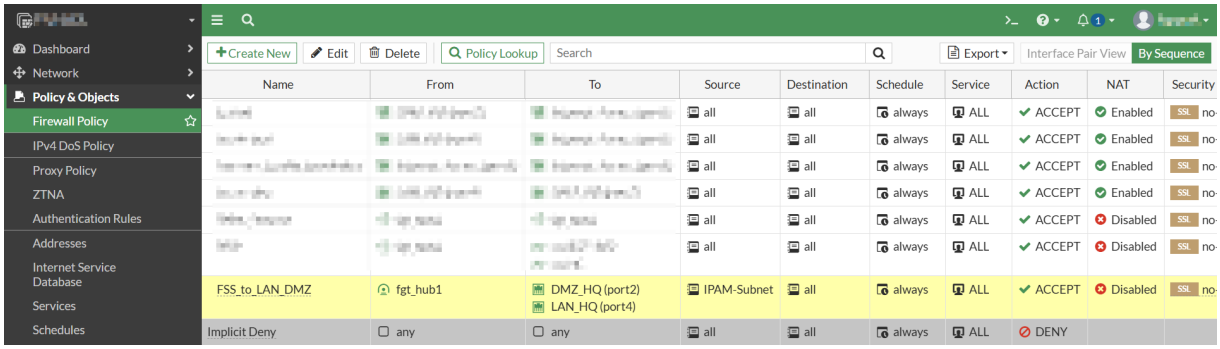
   In the above example, the IKEv2 mode configuration address range is from 10.251.1.35-10.251.1.251.
2. On the FortiGate SPA hub or spoke device, configure a firewall address object for the BGP router ID subnet and use it in the firewall policy used to restrict access to the HTTPS private server:

a. In *Policy & Objects* > *Addresses*, click *Create New* > *Address*. Create a new address object containing the IP range from the SPA hub.



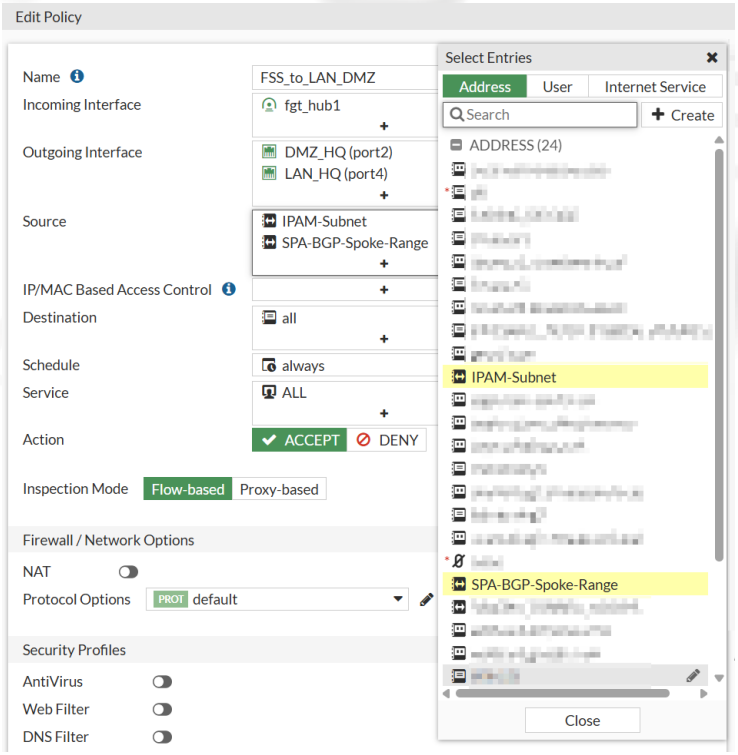
In this example, an IP range address object named SPA-BGP-Spoke-Range is created for 10.251.1.35-10.251.1.251.

b. In *Policy & Objects* > *Firewall Policy*, locate the existing firewall policy from the IPsec overlay interface to the LAN interface connected to the private HTTPS application server. Depending on your configuration, the source address for this policy may either be all or with an address object for the IPAM subnet used by agents.

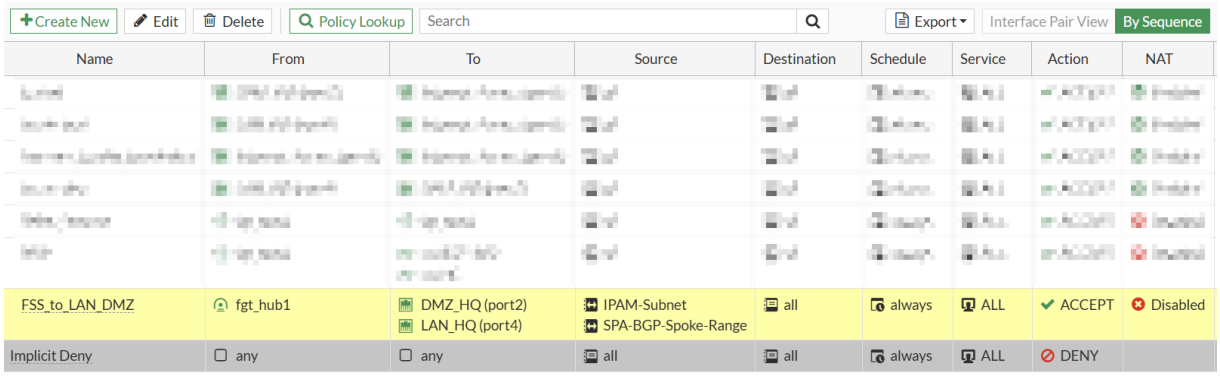


In this example, the firewall policy of interest is the FSS_to_LAN_DMZ policy from IPsec overlay interface fgt_hub1 to DMZ_HQ (port2) and LAN_HQ (port4) LAN interfaces with source set to IPAM-Subnet to allow agents to access private resources.

c. Select and edit the firewall policy, adding the address object with the SPA BGP spoke IP range as a source. Click *OK*.



The firewall policy should display both the IPAM-Subnet and added SPA-BGP-Spoke-Range as the *Source* of the policy.



Access to the HTTPS private server is now restricted to agents and Security PoPs, or agentless ZTNA users depending on the SPA-dependent feature that you are using.

More information

Appendix A: Documentation references

Feature documentation

Product document	Specific chapter if available
FortiOS 7.2.0 Admin Guide	• General IPsec VPN configuration • BGP • ADVPN with BGP as the routing protocol • Firewall policy parameters • Performance SLA • SD-WAN Rules
FortiClient 7.0 Admin Guide	
FortiManager 7.2.1 Admin Guide	• SD-WAN Overlay Templates • IPsec tunnel templates • BGP templates

4-D resources: SASE

- https://docs.fortinet.com/4d-resources/SASE

Appendix B - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the IPsec wizard

For ease of configuration, following the steps in this deployment guide that use the FortiOS GUI and IPsec wizard is recommended. See Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS CLI or GUI on page 21.

The following steps are unique to the FortiGate NGFW to FortiSASE SPA hub conversion use case.

FortiSASE security points of presence integrate with a hub-and-spoke network using ADVPN as its VPN overlay and BGP for its routing.

This section describes the following configuration settings and the FortiOS GUI configuration steps using the IPsec wizard and additional CLI and GUI configuration that you must configure on your FortiGate NGFW to convert it to a FortiSASE secure private access hub:

IPsec VPN configuration

The FortiGate next generation firewall requires the following IPsec VPN settings:

- IKEv2
- Hub configured as an IPsec VPN dialup server. The FortiSASE security points of presence (PoP) act as spokes and connect to your hub via IPsec dialup connections.
- You must enable the mode config setting. Each FortiSASE security PoP acquires IP addresses and automatically configures their tunnel interfaces IP addresses with the acquired IP address. You also use this IP address to set up BGP peering.
- On spokes, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
- Using mode config for dynamic IP address
- Use network overlay IDs for each overlay tunnel configuring `set network-overlay enable` and `set network-id <n>`
- Preshared key for each overlay tunnel
- Phase 1 and 2 proposals and settings
  - For IPsec phase 1, the following proposals are supported:
    aes128-sha256
    aes256-sha256
    aes128-sha1
    aes256-sha1
    DH groups 14 and 5
  - For IPsec phase 2, the following proposals are supported:
    aes128-sha1
    aes256-sha1
    aes128-sha256
    aes256-sha256
    aes128gcm
    aes256gcm
    chacha20poly1305
    DH groups 14 and 5
- Hub configured with `set auto-discovery-sender enable` to enable ADVPN on the hub

To allow for dynamic scaling of customer environments, as-needed, it is necessary to use the following mode configuration settings that make use of a /24 subnet for the mode configuration IP address space:

set ipv4-start-ip 192.168.1.1

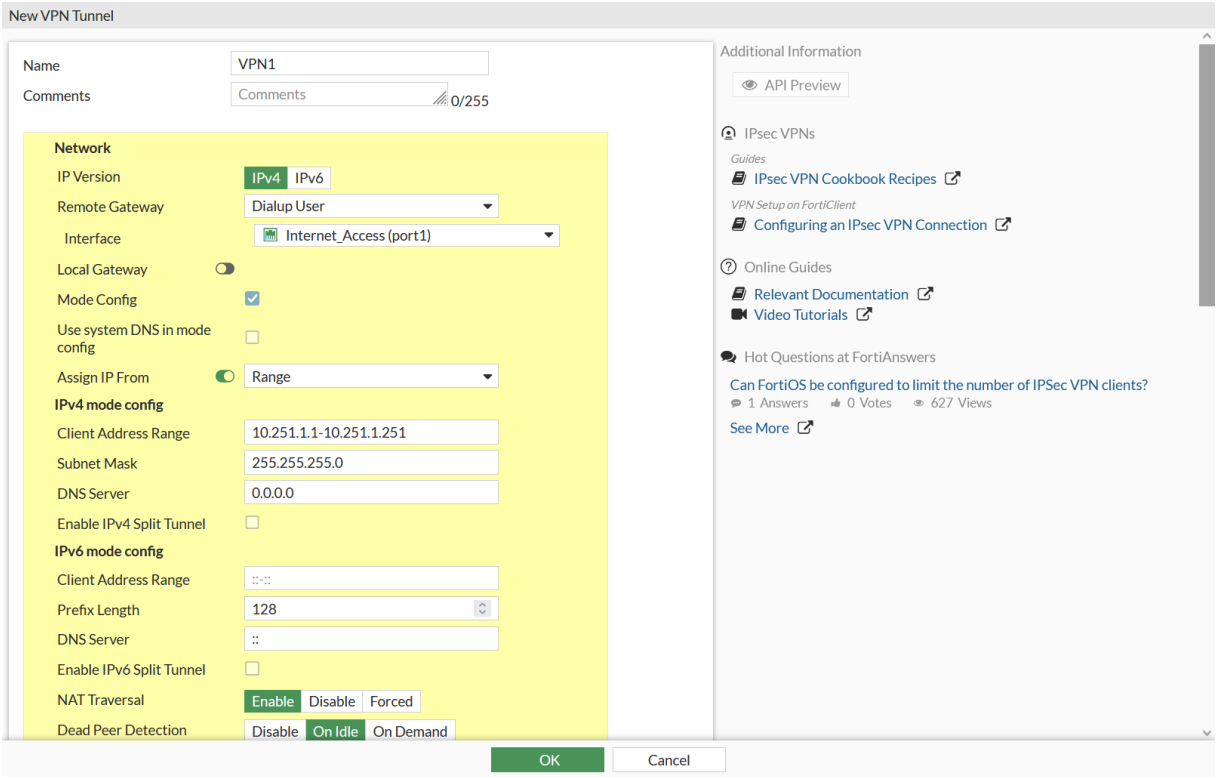
set ipv4-end-ip 192.168.1.252

set ipv4-netmask 255.255.255.0

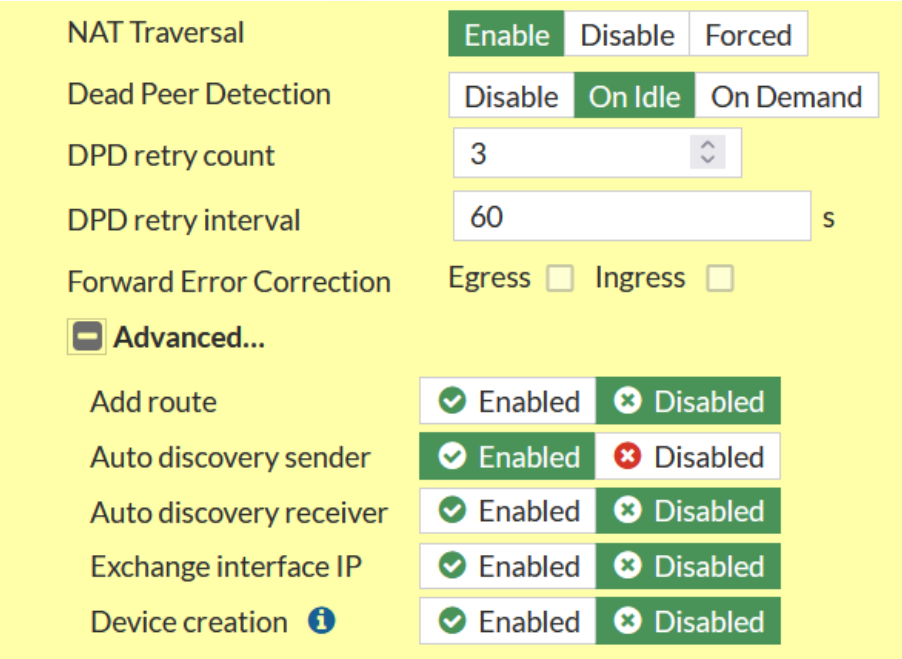
Depending on the size of the customer, the mode configuration IP address space may need to be even larger than a /24 subnet.

To configure an IPsec VPN tunnel using the GUI:

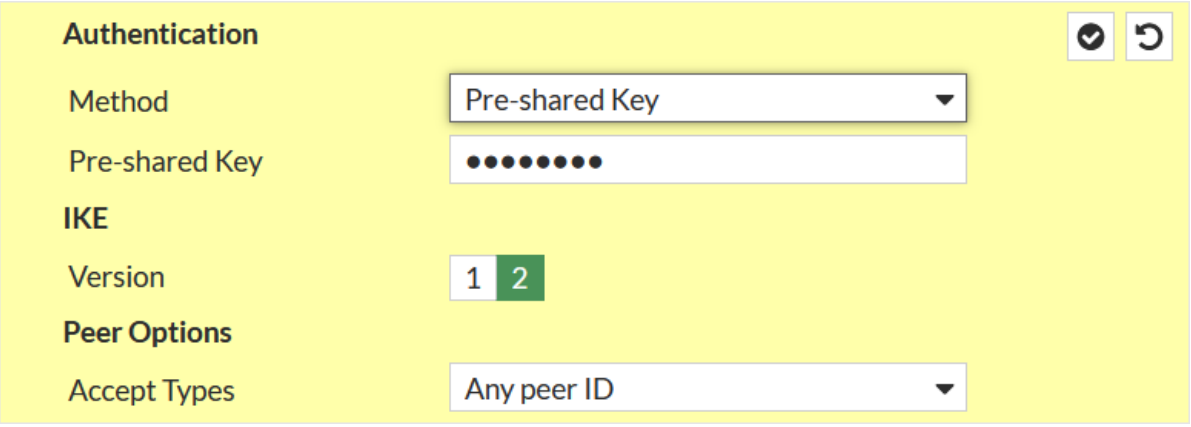
1. Go to *VPN* > *IPsec Tunnels*.
2. Click *Create New* > *IPsec Tunnel*. The *VPN creation Wizard* displays.
3. Set the following options, then click *Next*:
   a. In the *Name* field, enter VPN1.
   b. For *Template type*, select *Custom*.
4. Set the *Network* options:
   a. For *IP Version*, select *IPv4*.
   b. From the *Remote Gateway* dropdown list, select *Dialup User*.
   c. From the *Interface* dropdown list, select the WAN interface that the hub will listen on for VPN peer connections.
   d. Enable *Mode Config*.
   e. Enable *Assign IP From*, then select *Range* from the dropdown list.
5. Set the *IPv4 mode config* options:
   a. Configure the *Client Address Range*, *Subnet Mask*, and *DNS Server* fields to automate remote client addressing.
   b. Deselect *Enable IPv4 Split Tunnel*.



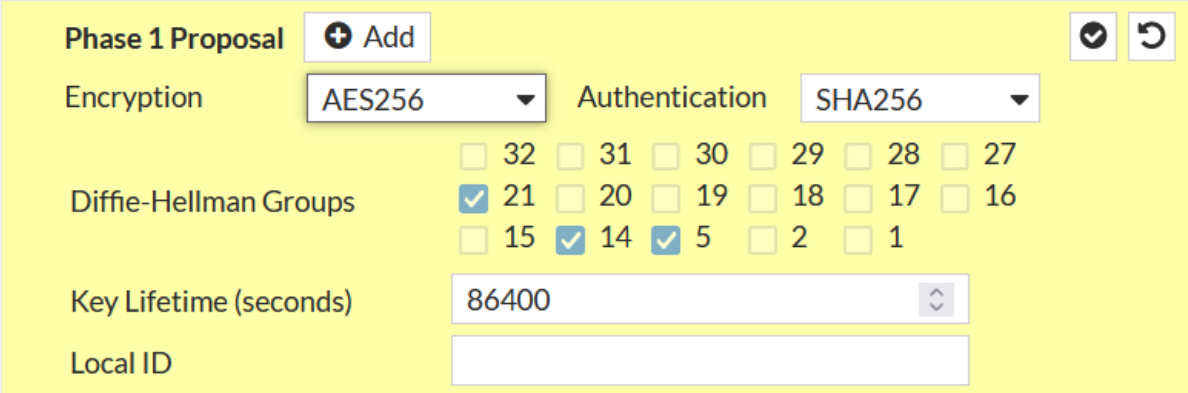
6. Set the remaining *Network* options:
   a. For *NAT Traversal*, select *Enable*.
   b. For *Dead Peer Detection*, select *On Idle*.
   c. In the *DPD retry count* field, enter 3.
   d. In the *DPD retry interval* field, enter 60.
   e. For *Forward Error Correction*, disable *Egress* and *Ingress*.
7. Expand *Advanced*, then set the following options:
   a. For *Add route*, select *Disabled*.
   b. For *Auto discovery sender*, select *Enabled*.
   c. For *Auto discovery receiver*, select *Disabled*.
   d. For *Exchange interface IP*, select *Disabled*.
   e. For *Device creation*, select *Disabled*.



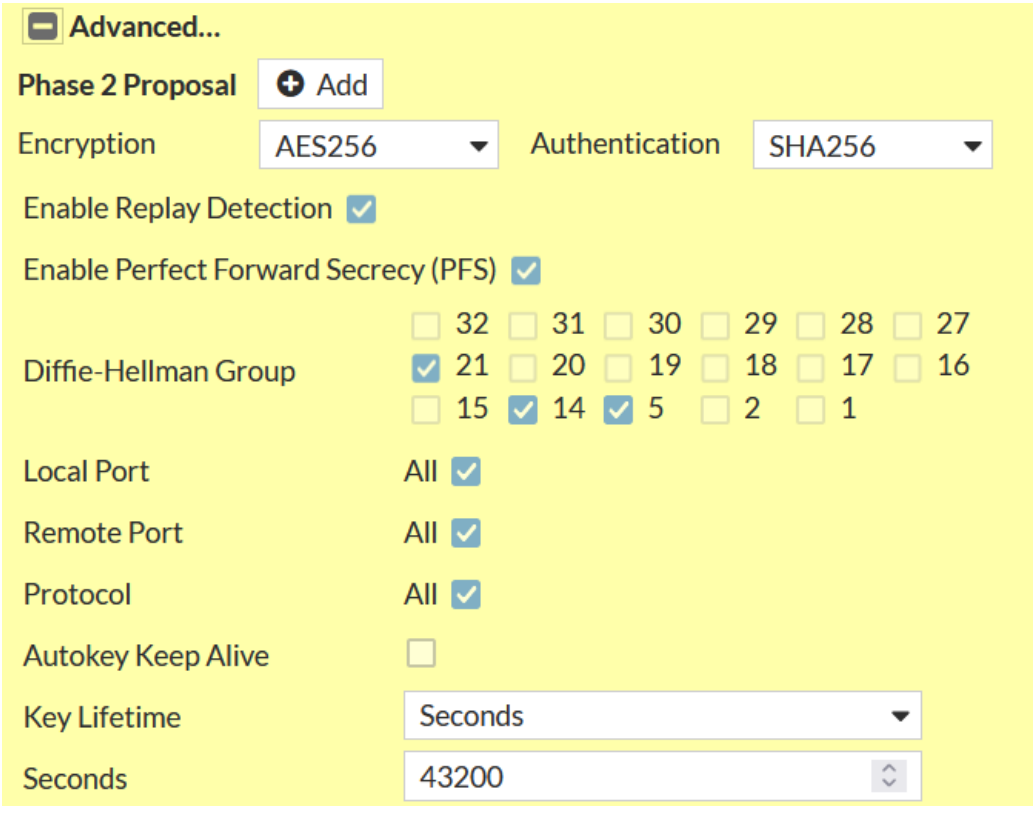
8. Set the *Authentication* options:
   a. From the *Method* dropdown list, select *Pre-shared Key*.
   b. In the *Pre-shared Key* field, enter an alphanumeric string.
   c. For *IKE* > *Version*, select *2*.
   d. From the *Accept Types* dropdown list, select *Any peer ID*.



9. Set the *Phase 1 Proposal* options:
   a. Add or remove *Encryption* and *Authentication* combinations as desired.
   b. Configure your desired *Diffie-Hellman Groups*, *Key Lifetime*, and *Local ID* (optional).



10. Set the *New Phase 2* options:
   a. If desired, enter a new value in the *Name* field. Otherwise, this defaults to the phase 1 name.
   b. Change the *Local Address* or *Remote Address* as needed. Otherwise, this defaults to 0.0.0.0/0.0.0.0 for both addresses, which is the wildcard subnet, allowing all subnets.
11. Expand *Advanced*, then set the following options:
   a. Add or remove *Encryption* and *Authentication* combinations as desired.
   b. Select *Enable Replay Detection*.
   c. Select *Enable Perfect Forward Secrecy (PFS)*.
   d. Select your desired *Diffie-Hellman Groups*.
   e. For *Local Port*, *Remote Port*, and *Protocol*, select *All*.
   f. Deselect *Autokey Keep Alive*.
   g. From the *Key Lifetime* dropdown list, select *Seconds*.
   h. In the *Seconds* field, enter the desired key lifetime value in seconds.



12. In the CLI, enable network overlays and configure the VPN gateway network ID. Replace VPN1 with the IPsec VPN phase 1 name. Replace 1 with the integer value that corresponds to the network ID. These options are unavailable in the GUI and you must run these CLI commands to configure them:

```
config vpn ipsec phase1-interface
  edit VPN1
    set network-overlay enable
    set network-id 1
  next
end
```

To configure an IPsec VPN tunnel using the CLI:

```
config vpn ipsec phase1-interface
    edit VPN1
        set type dynamic
        set interface port1
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set dhgrp 21 14 5
        set auto-discovery-sender enable
        set network-overlay enable
        set network-id 1
        set ipv4-start-ip 10.251.1.1
        set ipv4-end-ip 10.251.1.251
        set ipv4-netmask 255.255.255.0
        set psksecret < pre-shared key >
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit VPN1
        set phase1name VPN1
        set proposal aes256-sha256
    next
end
```

Tunnel interface configuration

You must assign a static IP address to the tunnel interface. This configuration is required to support BGP peering between the secure private access hub and the FortiSASE security points of presence.

The following settings are only examples. Do not consider them as recommended settings.

To create the tunnel interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Under *Physical Interface*, expand your WAN interface to display your IPsec VPN tunnel interface. Click the tunnel interface and click *Edit*.

3. In the *Edit Interface* dialog, do the following:
   a. Set the *IP* to *10.251.1.253* and *Netmask* to *255.255.255.255*.
   b. Set the *Remote IP/Netmask* to *10.251.1.254 255.255.255.0*.
   c. For *Administrative Access*, select *PING*.
4. Click *OK* to save the changes.

To create the tunnel interface using the CLI:

```
config system interface
    edit "VPN1"
        set vdom "root"
        set ip 10.251.1.253 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.251.1.254 255.255.255.0
        set interface "port1"
    next
end
```

Loopback interface configuration

You must create loopback interfaces on the FortiGate hub. The configuration uses the following loopback interfaces:

- A loopback interface *Lo_BGP-RID* to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment.
- A loopback interface *Lo-HC* to provide a health check target for the performance SLA on the FortiSASE security PoPs. In FortiSASE, you will need to set the *Health Check IP address* to the IP address configured for this interface. See Configuring a new service connection on page 51.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To configure the Lo-BGP-RID loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.
3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-BGP-RID.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.1.0.254/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.

To configure the Lo-BGP-RID loopback interface using the CLI:

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.1.0.254 255.255.255.255
        set allowaccess ping
        set type loopback
```

```
    next
end
```

To configure the Lo-HC loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.
3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-HC.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.11.11.11/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.

To configure the Lo-HC loopback interface using the CLI:

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.11.11.11 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

BGP configuration

FortiSASE security points of presence (PoP) connect to the hub FortiGate and establish iBGP peering. FortiSASE security PoPs learn routes to your network but do not advertise any route except their router-id IP address.

The hub FortiGate requires the following BGP settings:

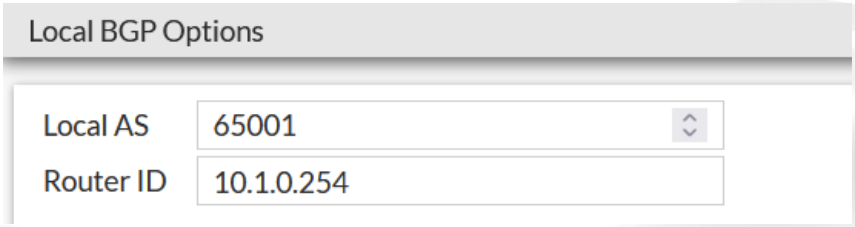
- AS number
- Router ID
- Using iBGP for dynamic routing via overlays
- BGP neighbor IP address for each overlay
- BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs
- One BGP session per overlay between the hub and each FortiSASE security PoP

The following settings are only examples. Do not consider them as recommended settings.

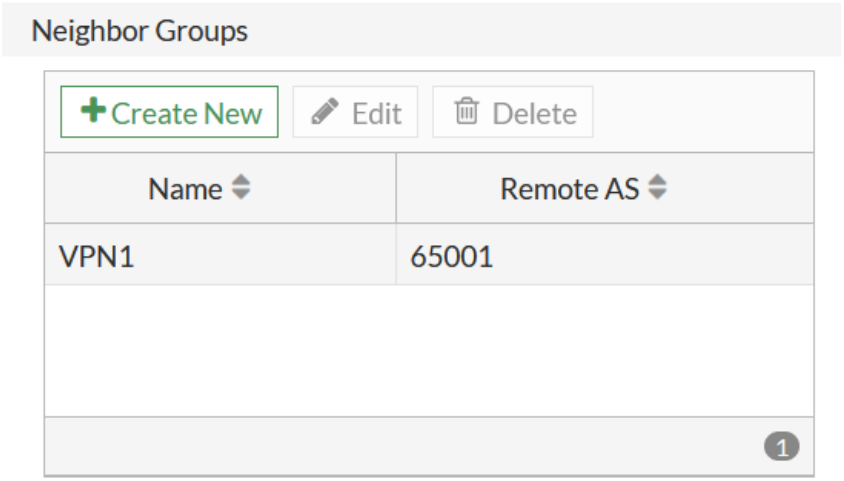
To configure BGP using the GUI:

If you cannot view the *Network* > *BGP* tree menu, go to *System* > *Feature Visibility* and enable *Advanced Routing* in the *Core Features* column.

1. Go to *Network* > *BGP*. Confirm that the *Local AS* field is set to 65001.
2. In the *Router ID* field, enter 10.1.0.254, which is the loopback interface IP address.

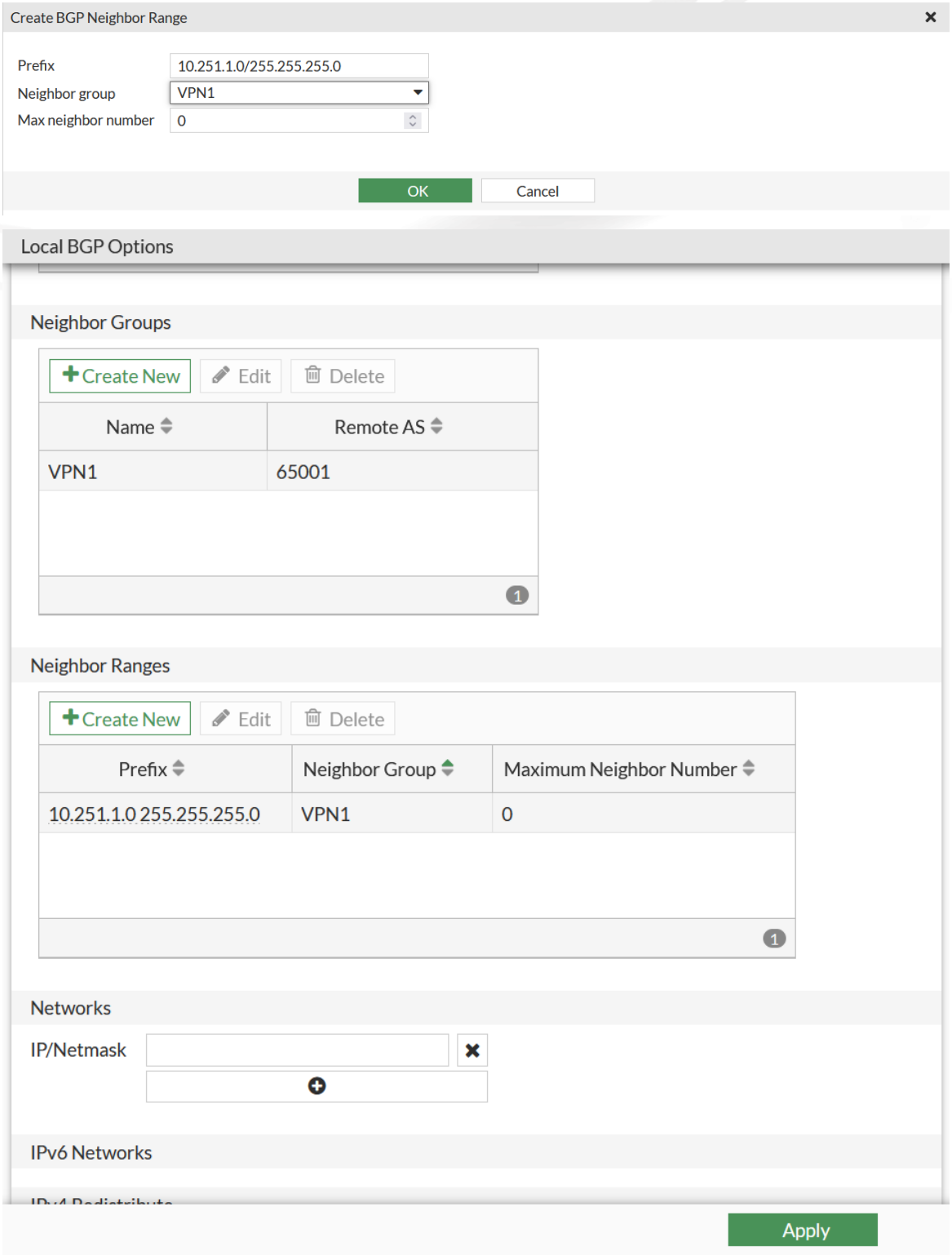


3. Configure neighbor options:
   a. In *Neighbor Groups*, create a new neighbor group:
      i. Click *Create New*. The *Add BGP Neighbor Group* pane displays.
      ii. In the *Remote AS* field, enter 65001.
      iii. Set *Interface* to the VPN tunnel interface on the hub used to listen to spoke VPN connections. For example, you may select VPN1.
      iv. Enable *Activate IPv4*.
      v. Disable *Attribute unchanged*.
      vi. Select the following options:
         - *Route reflector client*
         - *Next hop self*
         - *Soft reconfiguration*
         - *Capability: graceful restart*
         - *Capability: route refresh*
      vii. Click *OK*.



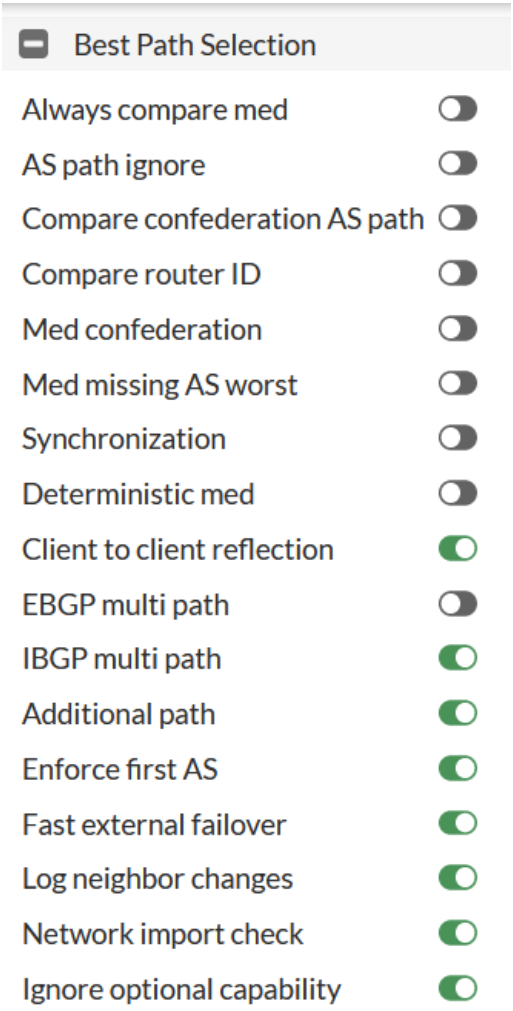
   b. Click *Apply* to perform a hard refresh of the browser.
   c. In *Neighbor Ranges*, create a new neighbor range:
      i. Click *Create New*. The *Create Neighbor Range* pane displays.
      ii. In the *Prefix* field, enter 10.251.1.0/255.255.255.0, which is the VPN peers subnet assigned using mode config.
      iii. From the *Neighbor group* dropdown list, select *VPN1*.
      iv. In the *Max neighbor number* field, enter 0.

v. Click *OK*.



4. In *Networks*, in the *IP/Netmask* field, enter 192.168.111.0 255.255.255.0.
5. Enable *Graceful Restart* and configure the following options:
   a. In the *Restart timer* field, enter 120.
   b. In the *Stale path timer* field, enter 360.
   c. In the *Update delay* field, enter 120.

6. Under *Advanced Options*, configure the following:
   a. In the *Cluster ID* field, enter *10.1.0.254*.
   b. In the *Keepalive* field, enter 5.
   c. Enable *Holdtime* and enter 15.
7. Under *Best Path Selection*, enable the following options:
   a. *Client to client reflection*
   b. *IBGP multi path*
   c. *Additional path*
   d. *Enforce first AS*
   e. *Fast external failover*
   f. *Log neighbor changes*
   g. *Network import check*
   h. *Ignore optional capability*



8. Click *Apply*.
9. Configure the following CLI options. These options are not available in the GUI and you must run these CLI commands to configure them:

```
config router bgp
   set additional-path enable
   set additional-path-select 4
```

```
        config neighbor-group
            edit "VPN1"
                set additional-path both
                set adv-additional-path 4
            next
        end
    end
```

To configure BGP using the CLI:

```
config router bgp
    set as 65001
    set router-id 10.1.0.254
    set keepalive-timer 5
    set holdtime-timer 15
    set ibgp-multipath enable
    set additional-path enable
    set cluster-id 10.1.0.254
    set graceful-restart enable
    set additional-path-select 4
    config neighbor-group
        edit "VPN1"
            set capability-graceful-restart enable
            set soft-reconfiguration enable
            set interface "VPN1"
            set next-hop-self enable
            set remote-as 65001
            set additional-path both
            set adv-additional-path 4
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.251.1.0 255.255.255.0
            set neighbor-group "VPN1"
        next
    end
    config network
        edit 1
            set prefix 192.168.111.0 255.255.255.0
        next
    end
end
```

Firewall policy configuration

To allow health checks from FortiSASE security points of presence to access the target SLA, as well as to allow FortiSASE remote users to access protected resources, you must configure these corresponding firewall policies to allow this traffic as this topic demonstrates.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To configure firewall policies using the GUI:

1. This deployment requires a spoke-to-hub LAN firewall policy. This policy allows traffic sourced from a spoke subnet destined for hub subnets. Create the policy:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create New*. The *New Policy* pane displays.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select port4.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK*.
2. This deployment requires a spoke-to-spoke firewall policy. This policy allows traffic sourced from a spoke subnet destined for other spoke subnets. Create the policy:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create New*. The *New Policy* pane displays.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select *VPN1*.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK*.
3. Create a spoke-to-loopback firewall policy. This policy allows BGP traffic and health check traffic from a spoke to the hub's loopback interface:
   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*. The *New Policy* pane displays.
   b. In the *Name* field, enter BGP.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select *Lo-BGP-RID* and *Lo-HC*.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK* to save changes.

To configure firewall policies using the CLI:

```
config firewall policy
    edit 1
        set name "Spoke-to-Hub"
        set srcintf "VPN1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 2
        set name "Spoke-to-Spoke"
        set srcintf "VPN1"
        set dstintf "VPN1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 3
        set name "BGP"
        set srcintf "VPN1"
        set dstintf "Lo-BGP-RID" "Lo-HC"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the Fabric Overlay Orchestrator

For ease of configuration, following the steps in this deployment guide that use the FortiOS GUI and IPsec wizard is recommended. See FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator specific configurations on page 32.

The following deployment steps are unique to the NGFW to SPA hub conversion using Fabric Overlay Orchestrator use case.

FortiSASE security points of presence integrate with a hub-and-spoke network using ADVPN as its VPN overlay and BGP for its routing.

This section describes the following configuration settings and the FortiOS GUI configuration steps using the IPsec wizard and additional CLI and GUI configuration that you must configure on your FortiGate NGFW to convert it to a FortiSASE secure private access hub:

IPsec VPN configuration

The FortiGate next generation firewall requires the following IPsec VPN settings:

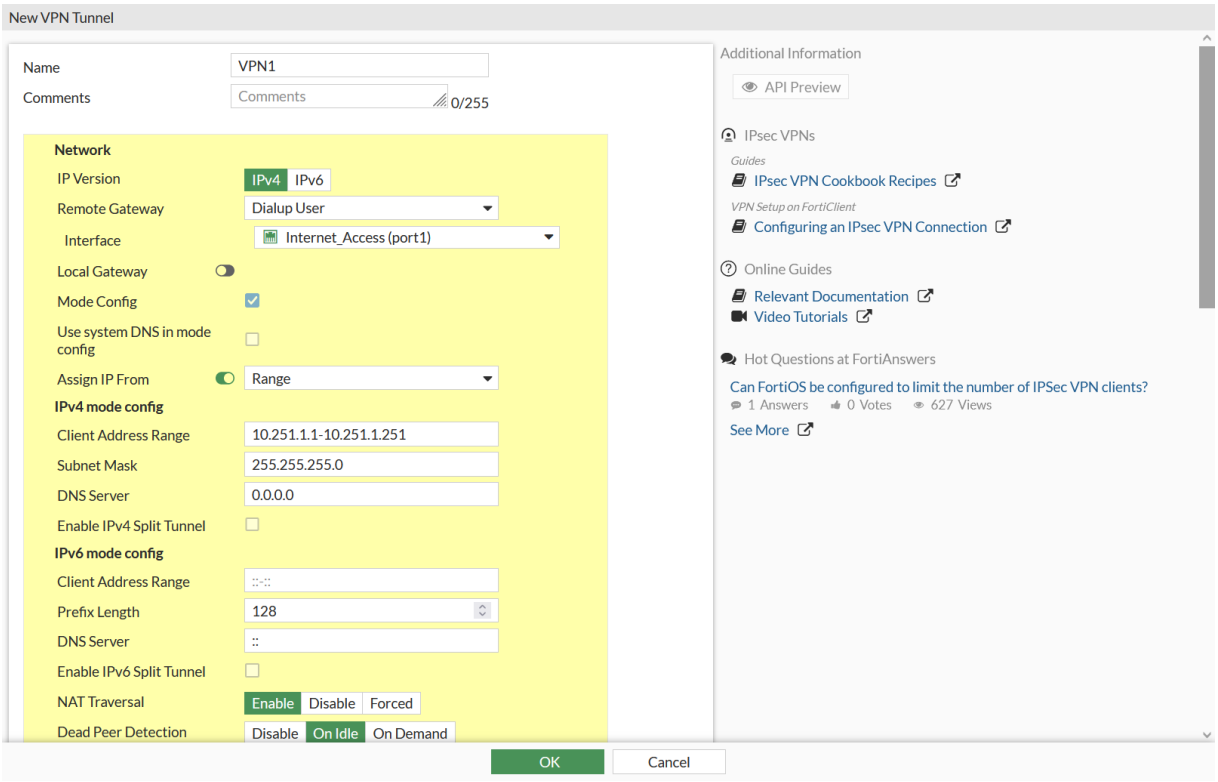
- IKEv2
- Hub configured as an IPsec VPN dialup server. The FortiSASE security points of presence (PoP) act as spokes and connect to your hub via IPsec dialup connections.
- You must enable the mode config setting. Each FortiSASE security PoP acquires IP addresses and automatically configures their tunnel interfaces IP addresses with the acquired IP address. You also use this IP address to set up BGP peering.
- On spokes, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
- Using mode config for dynamic IP address
- Use network overlay IDs for each overlay tunnel configuring `set network-overlay enable` and `set network-id <n>`
- Preshared key for each overlay tunnel
- Phase 1 and 2 proposals and settings
  - For IPsec phase 1, the following proposals are supported:
    aes128-sha256
    aes256-sha256
    aes128-sha1
    aes256-sha1
    DH groups 14 and 5
  - For IPsec phase 2, the following proposals are supported:
    aes128-sha1
    aes256-sha1
    aes128-sha256
    aes256-sha256
    aes128gcm
    aes256gcm
    chacha20poly1305
    DH groups 14 and 5
- Hub configured with `set auto-discovery-sender enable` to enable ADVPN on the hub

The following settings are only examples. Do not consider them as recommended settings.

To configure an IPsec VPN tunnel using the GUI:

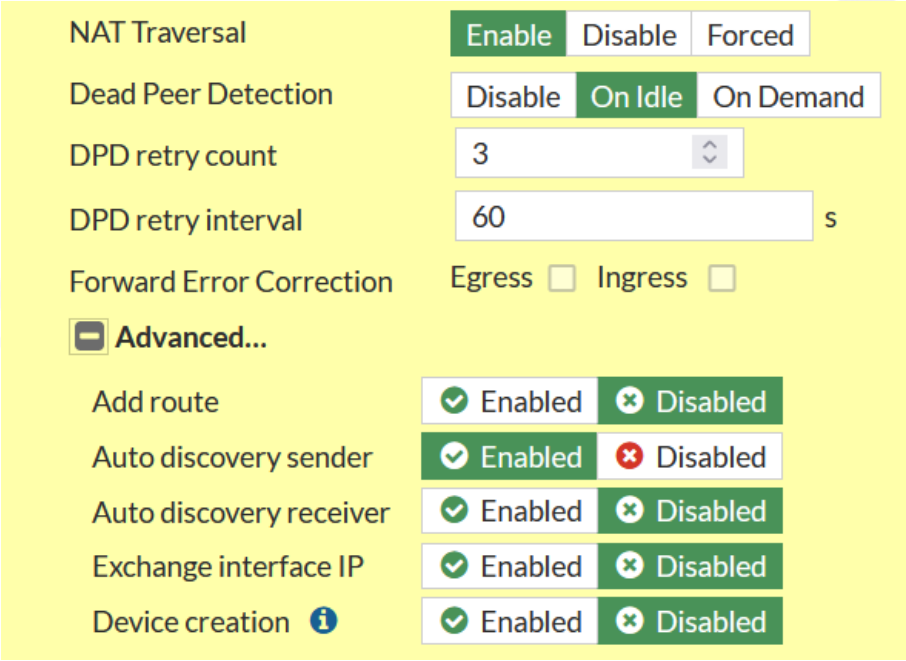
1. Go to *VPN* > *IPsec Tunnels*.
2. Click *Create New* > *IPsec Tunnel*. The *VPN creation Wizard* displays.

3. Set the following options, then click *Next*:
   a. In the *Name* field, enter VPN1.
   b. For *Template type*, select *Custom*.
4. Set the *Network* options:
   a. For *IP Version*, select *IPv4*.
   b. From the *Remote Gateway* dropdown list, select *Dialup User*.
   c. From the *Interface* dropdown list, select the WAN interface that the hub will listen on for VPN peer connections.
   d. Enable *Mode Config*.
   e. Enable *Assign IP From*, then select *Range* from the dropdown list.
5. Set the *IPv4 mode config* options:
   a. Configure the *Client Address Range*, *Subnet Mask*, and *DNS Server* fields to automate remote client addressing.
   b. Deselect *Enable IPv4 Split Tunnel*.

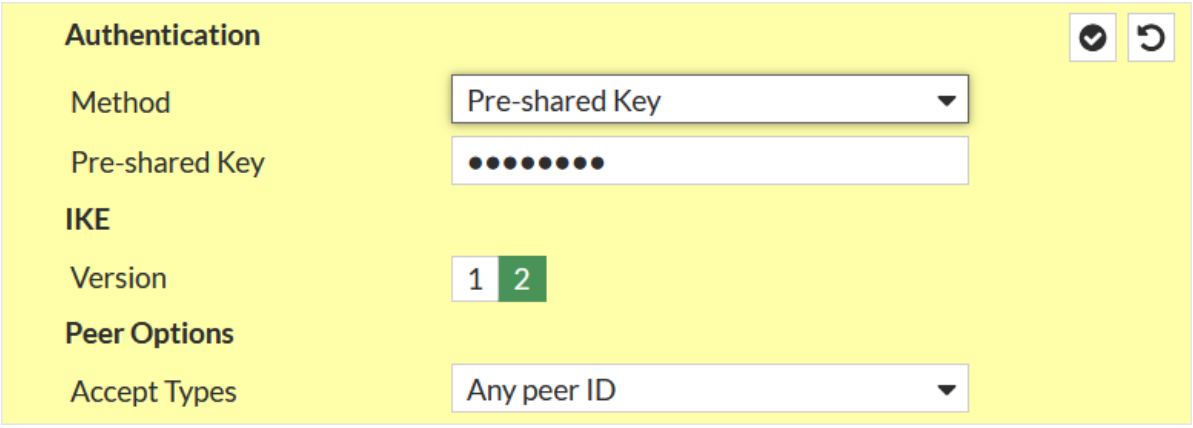


6. Set the remaining *Network* options:
   a. For *NAT Traversal*, select *Enable*.
   b. For *Dead Peer Detection*, select *On Idle*.
   c. In the *DPD retry count* field, enter 3.
   d. In the *DPD retry interval* field, enter 60.
   e. For *Forward Error Correction*, disable *Egress* and *Ingress*.
7. Expand *Advanced*, then set the following options:
   a. For *Add route*, select *Disabled*.
   b. For *Auto discovery sender*, select *Enabled*.
   c. For *Auto discovery receiver*, select *Disabled*.
   d. For *Exchange interface IP*, select *Disabled*.

e. For *Device creation*, select *Disabled*.



8. Set the *Authentication* options:
   a. From the *Method* dropdown list, select *Pre-shared Key*.
   b. In the *Pre-shared Key* field, enter an alphanumeric string.
   c. For *IKE* > *Version*, select *2*.
   d. From the *Accept Types* dropdown list, select *Any peer ID*.

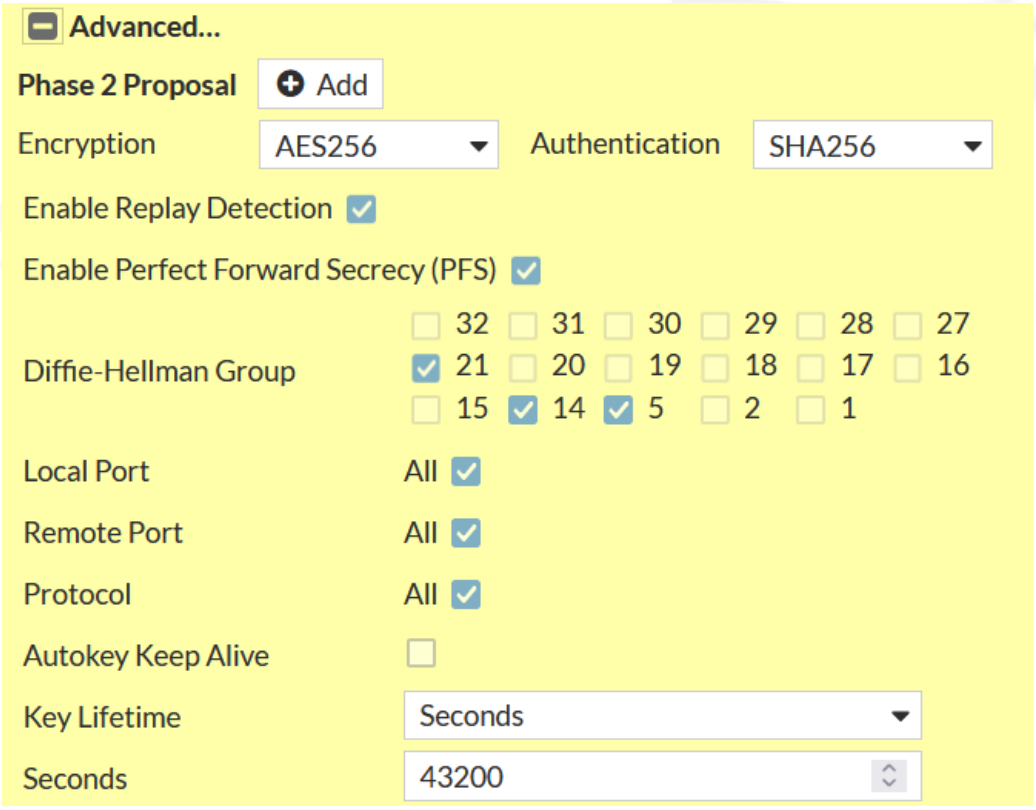


9. Set the *Phase 1 Proposal* options:
   a. Add or remove *Encryption* and *Authentication* combinations as desired.
   b. Configure your desired *Diffie-Hellman Groups*, *Key Lifetime*, and *Local ID* (optional).
10. Set the *New Phase 2* options:
   a. If desired, enter a new value in the *Name* field. Otherwise, this defaults to the phase 1 name.
   b. Change the *Local Address* or *Remote Address* as needed. Otherwise, this defaults to 0.0.0.0/0.0.0.0 for both addresses, which is the wildcard subnet, allowing all subnets.
11. Expand *Advanced*, then set the following options:
   a. Add or remove *Encryption* and *Authentication* combinations as desired.
   b. Select *Enable Replay Detection*.
   c. Select *Enable Perfect Forward Secrecy (PFS)*.
   d. Select your desired *Diffie-Hellman Groups*.
   e. For *Local Port*, *Remote Port*, and *Protocol*, select *All*.

f. Deselect *Autokey Keep Alive*.

g. From the *Key Lifetime* dropdown list, select *Seconds*.

h. In the *Seconds* field, enter the desired key lifetime value in seconds.



12. In the CLI, enable network overlays and configure the VPN gateway network ID. Replace VPN1 with the IPsec VPN phase 1 name. Replace 1 with the integer value that corresponds to the network ID. These options are unavailable in the GUI and you must run these CLI commands to configure them:

```
config vpn ipsec phase1-interface
  edit VPN1
    set network-overlay enable
    set network-id 1
  next
end
```

To configure an IPsec VPN tunnel using the CLI:

To allow for dynamic scaling of customer environments, as-needed, it is necessary to use the following mode configuration settings that make use of a /24 subnet for the mode configuration IP address space:

set ipv4-start-ip 192.168.1.1

set ipv4-end-ip 192.168.1.252

set ipv4-netmask 255.255.255.0

Depending on the size of the customer, the mode configuration IP address space may need to be even larger than a /24 subnet.

```
config vpn ipsec phase1-interface
    edit VPN1
        set type dynamic
        set interface port1
```

```
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set dhgrp 21 14 5
        set auto-discovery-sender enable
        set network-overlay enable
        set network-id 1
        set ipv4-start-ip 10.251.1.1
        set ipv4-end-ip 10.251.1.252
        set ipv4-netmask 255.255.255.0
        set psksecret < pre-shared key >
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit VPN1
        set phase1name VPN1
        set proposal aes256-sha256
    next
end
```

Tunnel interface configuration

You must assign a static IP address to the tunnel interface. This configuration is required to support BGP peering between the secure private access hub and the FortiSASE security points of presence.

The following settings are only examples. Do not consider them as recommended settings.

To create the tunnel interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Under *Physical Interface*, expand your WAN interface to display your IPsec VPN tunnel interface. Click the tunnel interface and click *Edit*.
3. In the *Edit Interface* dialog, do the following:
   a. Set the *IP* to *10.251.1.253* and *Netmask* to *255.255.255.255*.
   b. Set the *Remote IP/Netmask* to *10.251.1.254 255.255.255.0*.
   c. For *Administrative Access*, select *PING*.
4. Click *OK* to save the changes.

To create the tunnel interface using the CLI:

```
config system interface
    edit "VPN1"
        set vdom "root"
        set ip 10.251.1.253 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.251.1.254 255.255.255.0
        set interface "port1"
```

```
    next
end
```

Loopback interface configuration

You must create loopback interfaces on the FortiGate hub. The configuration uses the following loopback interfaces:

- A loopback interface *Lo_BGP-RID* to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment.
- A loopback interface *Lo-HC* to provide a health check target for the performance SLA on the FortiSASE security PoPs. In FortiSASE, you will need to set the *Health Check IP address* to the IP address configured for this interface. See Configuring a new service connection on page 51.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To configure the Lo-BGP-RID loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.
3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-BGP-RID.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.1.0.254/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.

To configure the Lo-BGP-RID loopback interface using the CLI:

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.1.0.254 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

To configure the Lo-HC loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.
3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-HC.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.11.11.11/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.

To configure the Lo-HC loopback interface using the CLI:

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.11.11.11 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

Firewall policy configuration

To allow health checks from FortiSASE security points of presence to access the target SLA, as well as to allow FortiSASE remote users to access protected resources, you must configure these corresponding firewall policies to allow this traffic as this topic demonstrates.

Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment.

To configure firewall policies using the GUI:

1. This deployment requires a spoke-to-hub LAN firewall policy. This policy allows traffic sourced from a spoke subnet destined for hub subnets. Create the policy:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create New*. The *New Policy* pane displays.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select port4.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK*.
2. This deployment requires a spoke-to-spoke firewall policy. This policy allows traffic sourced from a spoke subnet destined for other spoke subnets. Create the policy:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create New*. The *New Policy* pane displays.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select *VPN1*.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.

vi. For *Service*, select *ALL*.
vii. For *Action*, select *Accept*.
viii. Disable *NAT*.
ix. Select *Enable this policy*.

d. Click *OK*.

3. Create a spoke-to-loopback firewall policy. This policy allows BGP traffic and health check traffic from a spoke to the hub's loopback interface:
   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*. The *New Policy* pane displays.
   b. In the *Name* field, enter BGP.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select *Lo-BGP-RID* and *Lo-HC*.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK* to save changes.

To configure firewall policies using the CLI:

```
config firewall policy
    edit 1
        set name "Spoke-to-Hub"
        set srcintf "VPN1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 2
        set name "Spoke-to-Spoke"
        set srcintf "VPN1"
        set dstintf "VPN1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 3
        set name "BGP"
        set srcintf "VPN1"
        set dstintf "Lo-BGP-RID" "Lo-HC"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
```

```
        set logtraffic all
    next
end
```

BGP configuration

FortiSASE security points of presence (PoP) connect to the hub FortiGate and establish iBGP peering. FortiSASE security PoPs learn routes to your network but do not advertise any route except their router-id IP address.

The hub FortiGate requires the following BGP settings:

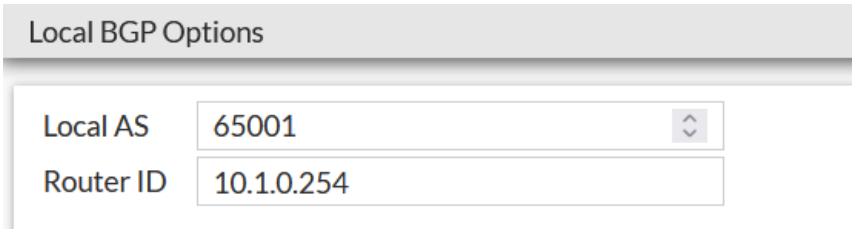
- AS number
- Router ID
- Using iBGP for dynamic routing via overlays
- BGP neighbor IP address for each overlay
- BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs
- One BGP session per overlay between the hub and each FortiSASE security PoP

The following settings are only examples. Do not consider them as recommended settings.

To configure BGP using the GUI:

If you cannot view the *Network* > *BGP* tree menu, go to *System* > *Feature Visibility* and enable *Advanced Routing* in the *Core Features* column.

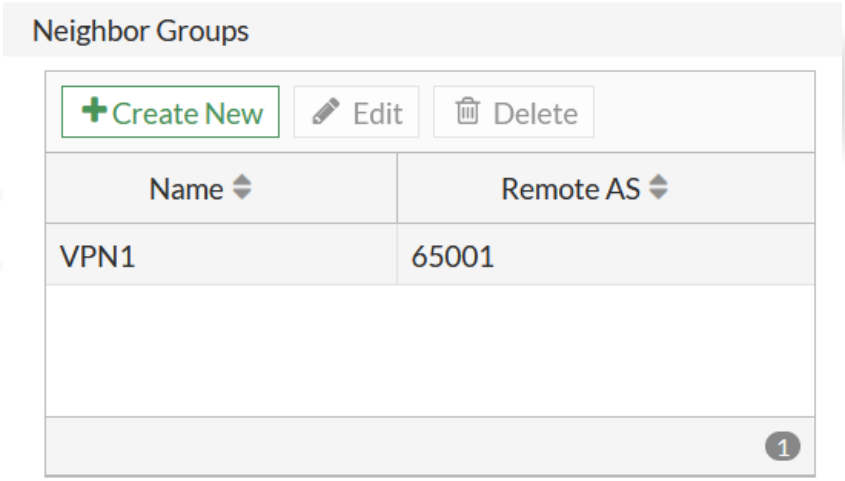
1. Go to *Network* > *BGP*. Confirm that the *Local AS* field is set to 65001.
2. In the *Router ID* field, enter 10.1.0.254, which is the loopback interface IP address.



3. Configure neighbor options:
   a. In *Neighbor Groups*, create a new neighbor group:
      i. Click *Create New*. The *Add BGP Neighbor Group* pane displays.
      ii. In the *Remote AS* field, enter 65001.
      iii. Set *Interface* to the VPN tunnel interface on the hub used to listen to spoke VPN connections. For example, you may select VPN1.
      iv. Enable *Activate IPv4*.
      v. Disable *Attribute unchanged*.
      vi. Select the following options:
         - *Route reflector client*
         - *Next hop self*
         - *Soft reconfiguration*

- *Capability: graceful restart*
- *Capability: route refresh*

vii. Click *OK*.



b. Click *Apply* to perform a hard refresh of the browser.

c. In *Neighbor Ranges*, create a new neighbor range:

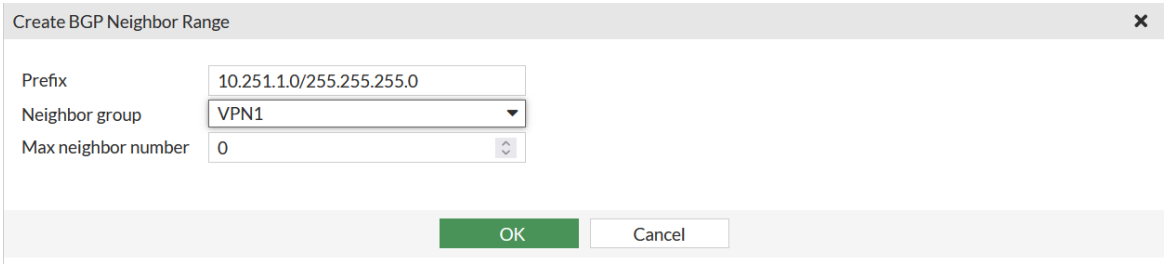
i. Click *Create New*. The *Create Neighbor Range* pane displays.

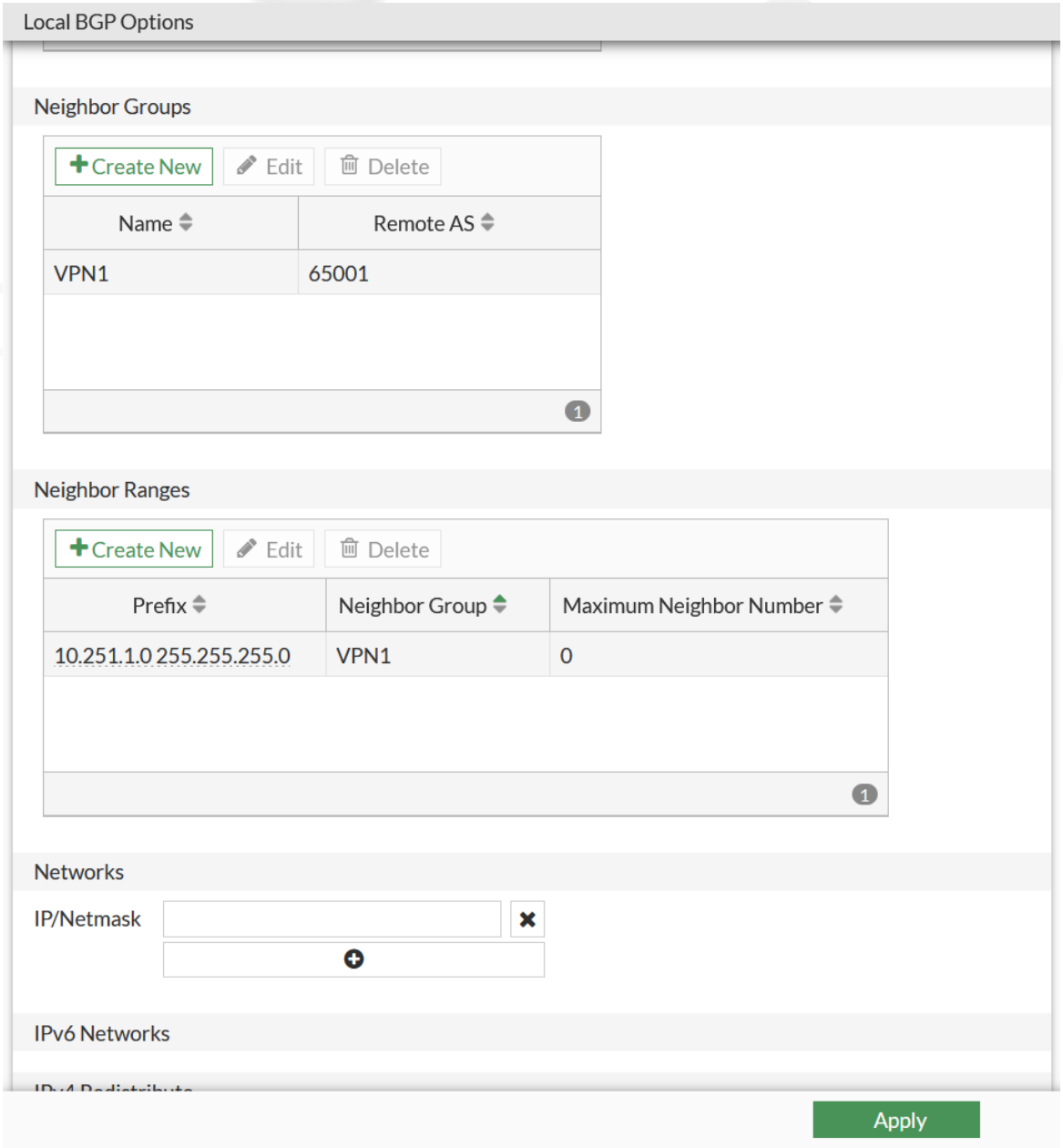
ii. In the *Prefix* field, enter 10.251.1.0/255.255.255.0, which is the VPN peers subnet assigned using mode config.

iii. From the *Neighbor group* dropdown list, select *VPN1*.

iv. In the *Max neighbor number* field, enter 0.

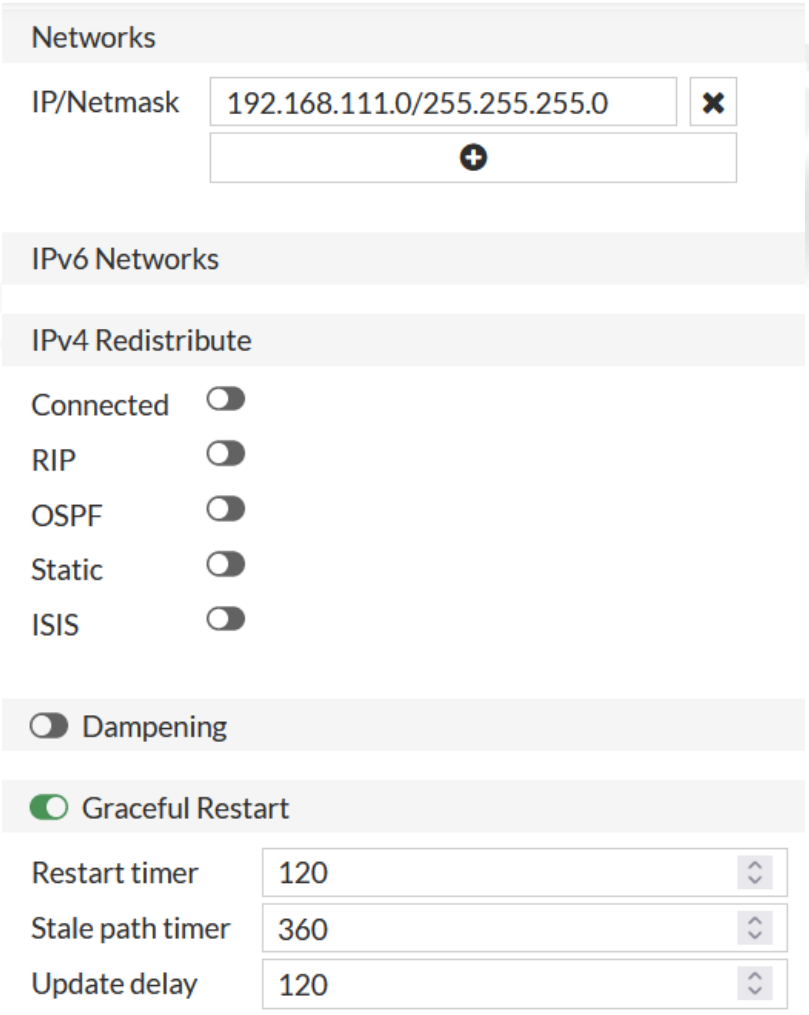
v. Click *OK*.





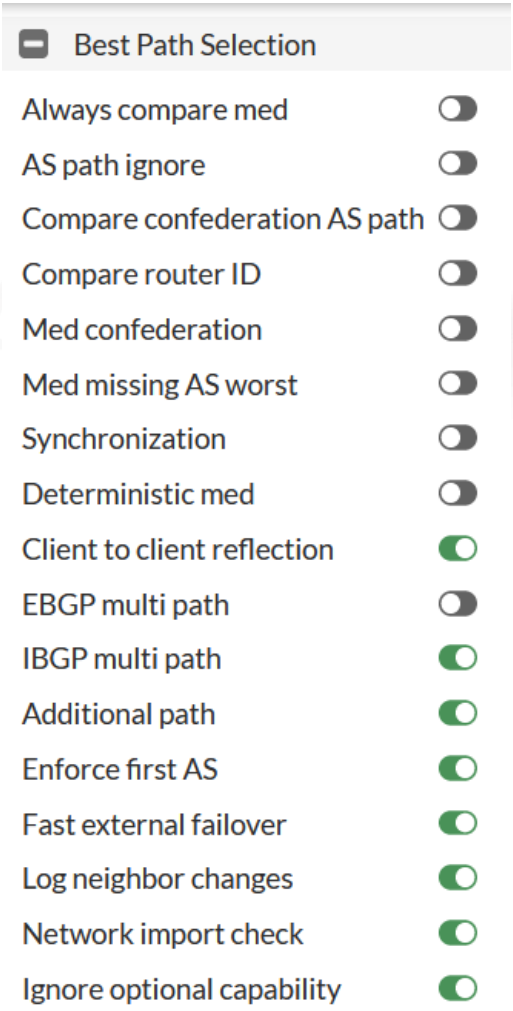
4. In *Networks*, in the *IP/Netmask* field, enter 192.168.111.0 255.255.255.0.
5. Enable *Graceful Restart* and configure the following options:
   a. In the *Restart timer* field, enter 120.
   b. In the *Stale path timer* field, enter 360.

c. In the *Update delay* field, enter 120.



6. Under *Advanced Options*, configure the following:
   a. In the *Cluster ID* field, enter *10.1.0.254*.
   b. In the *Keepalive* field, enter 5.
   c. Enable *Holdtime* and enter 15.
7. Under *Best Path Selection*, enable the following options:
   a. *Client to client reflection*
   b. *IBGP multi path*
   c. *Additional path*
   d. *Enforce first AS*
   e. *Fast external failover*
   f. *Log neighbor changes*
   g. *Network import check*

h. *Ignore optional capability*



8. Click *Apply*.
9. Configure the following CLI options. These options are not available in the GUI and you must run these CLI commands to configure them:

```
config router bgp
   set additional-path enable
   set additional-path-select 4
   config neighbor-group
        edit "VPN1"
            set additional-path both
            set adv-additional-path 4
        next
    end
end
```

To configure BGP using the CLI:

```
config router bgp
   set as 65001
   set router-id 10.1.0.254
   set keepalive-timer 5
   set holdtime-timer 15
   set ibgp-multipath enable
```

```
    set additional-path enable
    set cluster-id 10.1.0.254
    set graceful-restart enable
    set additional-path-select 4
    config neighbor-group
         edit "VPN1"
             set capability-graceful-restart enable
             set soft-reconfiguration enable
             set interface "VPN1"
             set next-hop-self enable
             set remote-as 65001
             set additional-path both
             set adv-additional-path 4
             set route-reflector-client enable
         next
     end
     config neighbor-range
         edit 1
             set prefix 10.251.1.0 255.255.255.0
             set neighbor-group "VPN1"
         next
     end
     config network
         edit 1
             set prefix 192.168.111.0 255.255.255.0
         next
     end
end
```

www.fortinet.com

72-254-1001698-20260130