



FortiGate NGFW to FortiSASE SPA Hub Conversion Deployment Guide

FortiSASE



DEFINE / DESIGN / **DEPLOY** / DEMO



Table of Contents

Change log	4
Deployment overview	5
Intended audience	7
About this guide	7
Design concept and considerations	7
FortiGate NGFW	7
FortiSASE SPA hub versus SD-WAN hub	7
Network restrictions	8
Product prerequisites	8
Deployment plan	8
Deployment procedures	9
Provisioning your FortiSASE instance	9
Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS CLI or GUI	9
IPsec VPN configuration using IPsec wizard and CLI	10
Tunnel interface configuration	12
Loopback interface configuration	13
Firewall policy configuration	14
BGP configuration	15
Converting FortiGate NGFW managed by FortiManager to a FortiSASE SPA hub	20
Configuring SPA to the FortiGate SPA hub in FortiSASE Private Access	20
Configuration workflow	21
Configuring network configuration	21
Configuring a new service connection	24
Viewing health and VPN tunnel status	28
Updating service connection priorities	29
Deleting a hub configuration	30
Monitoring private access hubs	30
Verifying private access policy configuration	30
Configuring a private access security profile	31
Configuring ZTNA tags in private access policies	31

Configuring DNS Settings	39
Split DNS Rules	40
Verifying IPsec VPN tunnels on the FortiGate hub	44
Verifying BGP routing on the FortiGate hub	45
Testing private access connectivity to FortiGate hub network from remote users	46
Verifying private access traffic in FortiSASE portal	46
Verifying private access hub status and location using the asset map	48
More information	49
Appendix A: Products used in this guide	49
Appendix B: Documentation references	49
Feature documentation	49
4-D resources: SASE	49
Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the IPsec wizard	50
IPsec VPN configuration	50
Tunnel interface configuration	55
Loopback interface configuration	56
Firewall policy configuration	57
BGP configuration	59

Change log

Date	Change description
2024-02-12	Initial release.
2024-02-13	Updated Deployment overview on page 5.
2024-03-07	Updated: <ul style="list-style-type: none">• Configuring DNS Settings on page 39• Split DNS Rules on page 40

Deployment overview

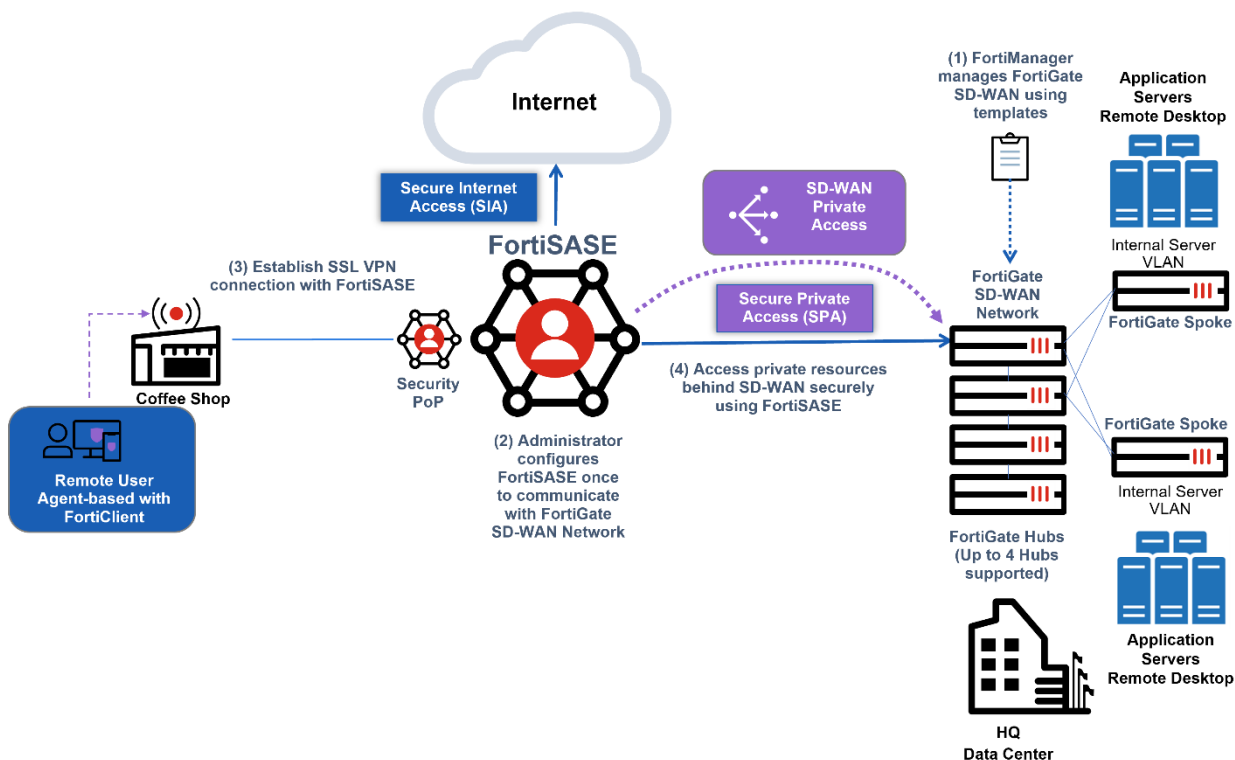
Organizations that have resources behind a newly deployed FortiGate next generation firewall (NGFW) standalone site or behind a newly deployed FortiGate NGFW in a data center and are not configured with SD-WAN enabled can provide their FortiSASE remote users with access to private resources.

Scenarios involving a FortiGate NGFW converted to a FortiSASE secure private access (SPA) hub or involving an existing FortiGate SD-WAN hub allow broader and seamless access to privately hosted TCP- and UDP-based applications.

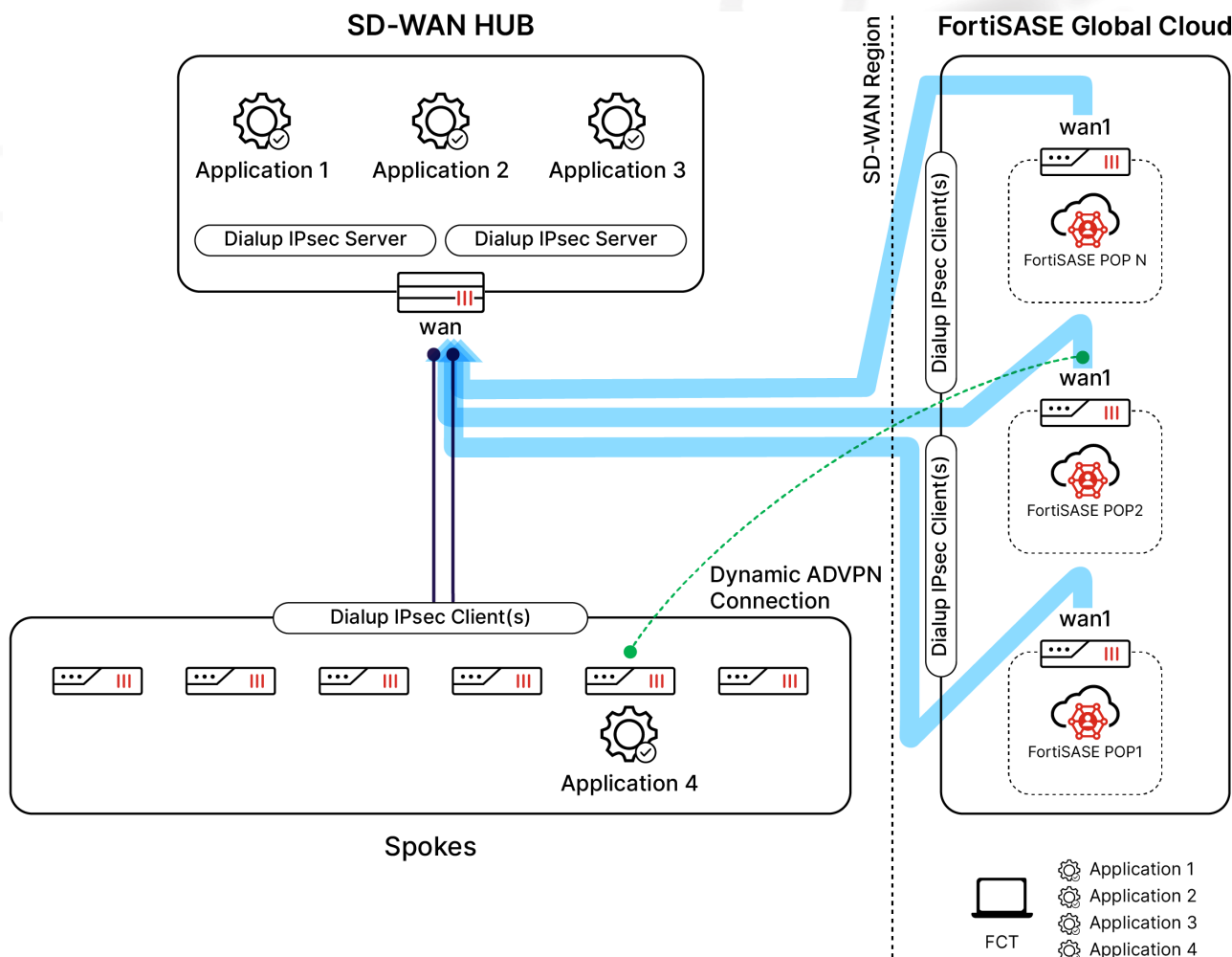
In the NGFW SPA use case, you must first convert the newly deployed NGFW to a FortiSASE SPA hub. After configuring FortiSASE to communicate with this hub, the FortiSASE security points of presence (PoPs) act as spokes to this hub, relying on IPsec VPN overlays and internal border gateway protocol to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

For a list of product prerequisites, see [SPA using a FortiSASE SPA hub](#).

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



FortiSASE 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 remote users 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. Therefore, the SPA use cases with FortiGate hubs only allow traffic to be initiated from FortiSASE spokes to FortiGate spokes.

FortiSASE supports these main routing design methods:

- [BGP per overlay](#) (default)
- [BGP on loopback](#)

This deployment guide describes how to configure a new FortiGate NGFW deployment to convert it to become a FortiSASE SPA standalone hub with no spokes and covers the cases when you configure the newly deployed FortiGate NGFW using the FortiOS CLI or GUI, or FortiManager manages the FortiGate NGFW. After performing the conversion steps and subsequent FortiSASE configuration steps, FortiSASE remote users can privately access internal networks behind these deployments.

For deployment details for the existing SD-WAN SPA use case, see the [4-D FortiSASE SPA with a FortiGate SD-WAN Deployment Guide](#) instead of this guide.

For the FortiGate NGFW SPA use case running FortiOS 7.2.4 and above, you can use the Fabric Overlay Orchestrator feature to convert the NGFW to a standalone IPsec VPN hub. For deployment details, see the [4-](#)

D FortiGate NGFW to FortiSASE SPA Hub Conversion using Fabric Overlay Orchestrator Deployment Guide (FortiOS 7.2.4+, 7.4.0+).

Intended audience

Midlevel network and security administrators of FortiGate NGFW 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 a FortiGate NGFW converted to 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.

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 (IPS), and application control features, and for LAN segmentation. Typically, a FortiGate NGFW has not yet been configured with advanced features such as SD-WAN, ZTNA, or FortiSASE.

This guide covers the cases when the newly deployed FortiGate NGFW is either configured using the FortiOS CLI or GUI, or managed using FortiManager.

This guide assumes a newly deployed FortiGate NGFW, which means that the device does not contain any existing routing or firewall policies to reconfigured.

FortiSASE SPA hub versus SD-WAN hub

This guide describes steps required to configure the FortiGate NGFW as a FortiSASE SPA hub. A FortiSASE SPA hub allows the FortiSASE Security Points of Presence (PoPs) 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 will be sufficient to provide FortiSASE remote users with secure private access 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](#).

Network restrictions

Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16

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 9](#) for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses 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 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 VPN 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.

Deployment procedures

Provisioning your FortiSASE instance

Ensure that you have purchased the contract to provision FortiSASE, then do the following:

To provision your FortiSASE instance:

1. From the [Fortinet Support site](#), register your FortiSASE contract.
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.
4. Once provisioned, the FortiSASE dashboard displays your entitlement in the Remote User Management widget. The number of endpoints that the widget lists is the number of VPN users that are entitled to use this service.

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

FortiSASE 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 using IPsec wizard and CLI on page 10](#)
- [Tunnel interface configuration on page 12](#)
- [Loopback interface configuration on page 13](#)
- [Firewall policy configuration on page 14](#)
- [BGP configuration on page 15](#)

For details on configuring using the FortiOS GUI without using the IPsec wizard or FortiOS CLI, see [Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the IPsec wizard on page 50](#).

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

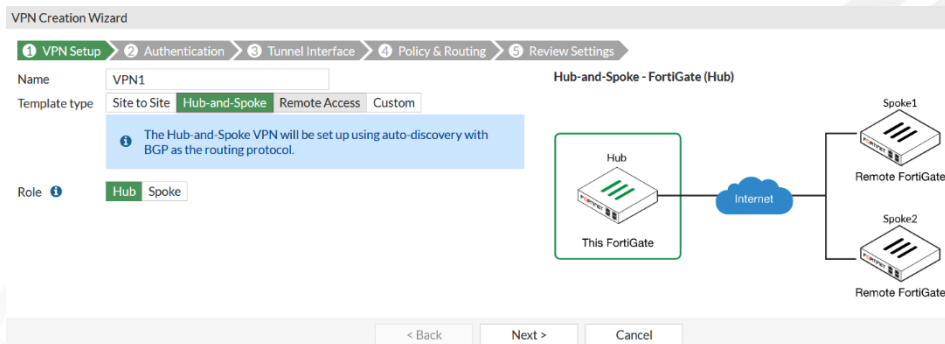


The following settings are only examples. Do not consider them as recommended settings.

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 10.251.1.254.
 - b. In the *Remote IP/netmask* field, enter 10.251.1.253/24. 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, 10.251.1.251, 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 10.251.1.251
    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.



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

Loopback interface configuration

You must create a loopback interface on the FortiGate hub. The configuration uses the loopback interface to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment and provide a health check target for the performance SLA on the FortiSASE security PoPs.



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

To configure the 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*.

Name	Lo-BGP-RID
Alias	<input type="text"/>
Type	Loopback Interface
VRF ID	<input type="text" value="0"/>
Role	<input type="text" value="LAN"/>

Address	
IP/Netmask	<input type="text" value="10.1.0.254/255.255.255.255"/>
Create address object matching subnet	<input checked="" type="checkbox"/>
Name	Lo-BGP-RID address
Destination	10.1.0.254/255.255.255.255
Secondary IP address	<input type="checkbox"/>

Administrative Access		
IPv4	<input type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP
	<input type="checkbox"/> FMG-Access	<input type="checkbox"/> SSH
	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting
	<input type="checkbox"/> Speed Test	<input checked="" type="checkbox"/> PING
		<input type="checkbox"/> SNMP
		<input type="checkbox"/> Security Fabric Connection

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.



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

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.

Name	vpn_VPN1_spoke2hub_0
Incoming Interface	VPN1
Outgoing Interface	LAN_HQ (port4)
Source	all
IP/MAC Based Access Control	
Destination	VPN1_local
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
Firewall/Network Options	
NAT	<input type="checkbox"/>
Protocol Options	<input checked="" type="checkbox"/> default

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.

Name	vpn_VPN1_spoke2spoke_0
Incoming Interface	VPN1
Outgoing Interface	VPN1
Source	all
IP/MAC Based Access Control	
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT DENY
Inspection Mode	Flow-based Proxy-based
Firewall/Network Options	
NAT	
Protocol Options	default

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

This policy allows 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 *Lo-HC*.
3. Set the following options:
 - a. For *Incoming interface*, select *VPN1*.
 - b. For *Outgoing interface*, select *Lo-BGP-RID*.
 - 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

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 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

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* section.
- The following are configured via the *Neighbor Ranges* section:
 - BGP neighbor IP address for each overlay is configured via *Neighbor Ranges* section.
 - BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs

The screenshot displays the 'Local BGP Options' configuration window in the FortiGate GUI. It is divided into three main sections: 'Neighbor Groups', 'Neighbor Ranges', and 'Networks'.

Neighbor Groups: This section contains a table with two columns: 'Name' and 'Remote AS'. A single entry is shown with 'VPN1' as the name and '65001' as the Remote AS. Above the table are buttons for '+ Create New', 'Edit', and 'Delete'.

Neighbor Ranges: This section contains a table with three columns: 'Prefix', 'Neighbor Group', and 'Maximum Neighbor Number'. A single entry is shown with the prefix '10.251.1.0/25', 'VPN1' as the Neighbor Group, and '0' as the Maximum Neighbor Number. Above the table are buttons for '+ Create New', 'Edit', and 'Delete'.

Networks: This section has a field for 'IP/Netmask' with the value '192.168.111.0/255.255.255.0'. Below this field is a '+' button to add more networks. There are also sections for 'IPv6 Networks' and 'IPv4 Redistribute' which are currently empty.

An 'Apply' button is located at the bottom right of the configuration window.

Best Path Selection

Always compare med	<input type="radio"/>
AS path ignore	<input type="radio"/>
Compare confederation AS path	<input type="radio"/>
Compare router ID	<input type="radio"/>
Med confederation	<input type="radio"/>
Med missing AS worst	<input type="radio"/>
Synchronization	<input type="radio"/>
Deterministic med	<input type="radio"/>
Client to client reflection	<input checked="" type="radio"/>
EBGP multi path	<input type="radio"/>
IBGP multi path	<input checked="" type="radio"/>
Additional path	<input checked="" type="radio"/>
Enforce first AS	<input checked="" type="radio"/>
Fast external failover	<input checked="" type="radio"/>
Log neighbor changes	<input checked="" type="radio"/>
Network import check	<input checked="" type="radio"/>
Ignore optional capability	<input checked="" type="radio"/>

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:



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



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.

Local BGP Options

Local AS

65001

Router ID

10.1.0.254

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

Neighbors

+ Create New

Edit

Delete

IP	Remote AS
10.10.1.3	65001

1

Confirm

⚠ Are you sure you want to delete the selected elements?

Neighbors

+ Create New

Edit

Delete

IP	Remote AS
No results	

0

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 VPN tunnel interface of the hub used to listen for spoke VPN connections. This example selects VPN1.

- b. Click *OK*.

Edit BGP Neighbor Group

Name
VPN1

Remote AS
65001

Interface
VPN1

Activate IPv4

IPv4 Filtering

Filter list in

Filter list out

Distribute list in

Distribute list out

Prefix list in

Prefix list out

Route map in

Route map out

Allow AS in

Graceful restart time
0

Max prefix

Attribute unchanged

☒ Route reflector client
☐ Soft reconfiguration
☒ Capability: graceful restart

☒ Next hop self
☐ AS override
☒ Capability: route refresh

☐ Remove private AS
☐ Route Server Client
☐ Capability: default originate

OK

Cancel

6. Under *Advanced Options*, configure the following:

- In the *Keepalive* field, enter 60.
- Enable *Holdtime* and enter 180.
- Enable *Background scan* and enter 60.

Advanced Options

Cluster ID
10.1.0.254

Default Local Preference
100

Distance external
20

Distance internal
200

Distance local
200

Keepalive
60

Holdtime
☒ 180

Background scan
☒ 60

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
  config neighbor-group
    edit "VPN1"
      set link-down-failover enable
      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.

Configuring SPA to the FortiGate SPA hub in FortiSASE Private Access



Before configuring the *Secure Private Access* settings in the FortiSASE portal, 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, especially those sections covering [Design concept and considerations on page 7](#), [Product prerequisites on page 8](#), and [Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS CLI or GUI on page 9](#).

At this point, the FortiGate NGFW has been converted to a FortiSASE SPA Hub. Therefore, in the steps that follow, the FortiGate NGFW will now be referred to as the FortiSASE SPA Hub.

To allow FortiSASE remote users with secure private access (SPA) to resources behind your FortiGate SD-WAN hub network, you can configure FortiSASE security PoPs as spokes in your hub-and-spoke network using the *Secure Private Access* page.

Configuration workflow

To configure SPA service connections (hubs), you must follow this configuration workflow in *Network > Secure Private Access*:

1. Click the *Network Configuration* tab at the top of the page and configure the common network configuration settings. See [Configuring network configuration on page 21](#).
2. Click the *Service Connections* tab at the top of the page, click *Create*, and configure a new service connection (hub). See [Configuring a new service connection on page 24](#).



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

Configuring network configuration

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



You can use Only one BGP routing design method for all hubs and spokes. They cannot be mixed.

Also, the BGP routing design method cannot be changed once saved. You must delete the service connection(s) and network configuration and reconfigure with a different BGP routing design method.

To configure SPA network configuration:

1. Go to *Network > Secure Private Access* and click the *Network Configuration* tab.
2. For the *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select one of the following:
 - BGP per overlay (default selection)
 - BGP on loopback. FortiSASE automatically selects and grays out *BGP Recursive Routing* after you selecting this option.
3. Fill in the rest of the fields with values of the attributes of the FortiGate hub network connection. FortiSASE performs input validation 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: <ul style="list-style-type: none">• 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.	BGP per overlay

Network attributes	Description	Example
	See Routing design methods .	
BGP router ID subnet	For BGP per overlay, available/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. For <i>BGP on loopback</i> , you must configure this subnet as a neighbor range in the hub BGP settings.	10.20.1.0/24
Autonomous system number (ASN)	BGP autonomous system (AS) number of your hubs. Typically, this should be the same on both hubs.	65400
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
Hub selection method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: <ul style="list-style-type: none"> • 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 PoP that meets lowest cost (SLA) requirements. A hub can be assigned a different priority level in different 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 address	IP address of a server behind the hub that should be 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.	



Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16



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 *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.



When using the BGP MED option, user-defined hub priorities are not used because the SD-WAN SLA rule is disabled in this case.

4. Click *Save*.

Configuring a new service connection

You can create a new service connection (hub) using one of the following BGP routing design methods:

- BGP per overlay (default)
- BGP on loopback



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

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's settings, such as updating the PSK or updating the PKI user or certificate.

To configure service connections or hubs for BGP per overlay:

1. Go to *Network > Secure Private Access*.
2. On the *Service Connections* tab, click *Create*.
3. Fill in the rest of the fields with the attributes of the FortiGate hub or service connection. 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 VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports <i>Pre-shared key</i> (default) and <i>Certificate</i> .	Pre-shared key
Pre-shared key (PSK)	When <i>Authentication Method</i> is configured as <i>Pre-shared key</i> , define the hub PSK.	mysecretkey
PKI User	When <i>Authentication Method</i> is configured as <i>Certificate</i> , select the PKI user with valid subject and CA certificate that FortiSASE uses to validate the hub's certificate. You can directly create the PKI user from <i>+Create</i> or via <i>Configuration > PKI</i> , then select it here.	mypeer
Certificate	When <i>Authentication Method</i> is configured as <i>Certificate</i> , select the certificate for the FortiSASE security PoP to present. You must import this certificate into FortiSASE via <i>System > Certificates</i> as a <i>Local Certificate</i> .	Fortinet_Factory
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	192.168.10.253
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 the hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2



Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

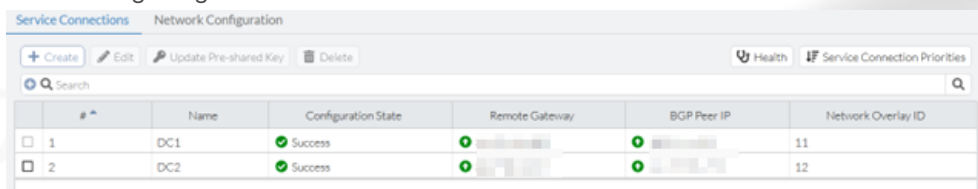
- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16



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 *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

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



	Name	Configuration State	Remote Gateway	BGP Peer IP	Network Overlay ID
1	DC1	Success			11
2	DC2	Success			12



For FortiSASE security points of presence (PoP), the SD-WAN performance SLA (health check) setting has the following parameters:

- **Latency threshold:** 120 ms
- **Jitter threshold:** 55 ms
- **Packet loss threshold:** 1%

Also, for FortiSASE 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 used by each FortiSASE security PoP, 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 FortiSASE in the desired order of preference from the most preferred hub to the least preferred hub.

To configure service connections or hubs for BGP on loopback:

- Go to *Network > Secure Private Access*.
- On the *Service Connections* tab, click *Create*.
- For the *Create a New Secure Private Access Service Connection* step, fill in the fields with the attributes of the FortiGate hub or service connection. FortiSASE performs input validation 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 VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports <i>Pre-shared key</i> (default) and <i>Certificate</i> .	Pre-shared key
Pre-shared key (PSK)	When <i>Authentication Method</i> is configured as <i>Pre-shared key</i> , define the hub PSK.	mysecretkey

Network attributes	Description	Example
PKI User	When <i>Authentication Method</i> is configured as <i>Certificate</i> , select the PKI user with valid subject and CA certificate used by FortiSASE to validate the hub's certificate. You can directly create the PKI user from <i>+Create</i> or via <i>Configuration > PKI</i> , then select it here.	mypeer
Certificate	When <i>Authentication Method</i> is configured as <i>Certificate</i> , select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via <i>System > Certificates</i> as a <i>Local Certificate</i> .	Fortinet_Factory
ADVPN Route Tag	For <i>BGP on loopback</i> only, ADVPN route tag number for spoke to tag incoming routes advertised from a hub. See Enhanced BGP next hop updates and ADVPN shortcut override .	1
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.10.10.253
Network overlay ID	Define a unique network ID for each hub. If a 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 VPN tunnels towards each hub have different network overlay IDs.	2



Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16



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 *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

4. Click *Save*.
5. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
6. (Optional) Repeat the steps to configure up to a total of four service connections as necessary to support your secure private access service connection network topology.

To update the authentication method settings for a service connection:

1. Go to *Network > Secure Private Access*.
2. On the *Service Connections* tab, click *Update Authentication Method*.
3. Select the *Authentication Method* and configure the corresponding parameter(s):
 - a. *New Pre-shared Key* when *Pre-shared Key* is selected.
 - b. *PKI User* and *Certificate* when *Certificate* is selected.
4. Click *OK*. Once FortiSASE successfully updates the authentication method for the service connection, it notifies you with the message *Authentication method updated successfully*.

Viewing health and VPN tunnel status

Click the *Health* button at the top of the page to view the *Health and VPN Tunnel Status* page, which shows all configured hubs' health and VPN tunnel status. This page provides advanced monitoring of the IPsec VPN 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 VPN tunnel status from this page:

Health and VPN Tunnel Status

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.
Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected.
Note that a service connection can be assigned a different priority level in different PoPs.

DC1

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
<input checked="" type="checkbox"/>	San Jose - California - U...	Up	Up	Established

1

DC2

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
<input type="checkbox"/>	San Jose - California - U...	Up	Up	Established

1

For any hub, selecting a 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:

Learned BGP Routes

Search

Prefix	Next Hop	Learned From
10.251.1.1/32	0.0.0.0	0.0.0.0
10.100.99.0/24	10.251.1.253	10.251.1.253
192.168.111.0/24	10.251.1.253	10.251.1.253

Updating service connection priorities

When you configure the hub selection method as hub health and priority within each 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 PoPs using the *Update 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 *Network > Secure Private Access*. On the *Service Connections* tab, click *Update Service Connection Priorities*.
2. From the *Security PoP* dropdown list, select the desired PoP hub. The example selects the San Jose – California – USA security PoP.

Update Service Connection Priorities

1 PoPs will choose the service connection with the highest priority that satisfies the SLA to forward traffic.

Set Priority ▼ San Jose - California - USA ▼

<input type="checkbox"/>	Name	Priority ▲
<input type="checkbox"/>	DC1	P1 <input type="text"/> (Highest Priority)
<input type="checkbox"/>	DC2	P1 <input type="text"/> (Highest Priority)

3. Select the desired hub and do one of the following to set the priority. P1 is the highest priority, and P2 is the lowest priority
 - a. From the *Set Priority* dropdown list, select the desired priority.
 - b. Right-click the hub, select *Set Priority*, and select the desired priority.
4. Set the priority for each hub that will influence hub selection. The example modifies the hub priorities so that the priority of DC1 is P2 and the priority of DC2 is P1:

Update Service Connection Priorities

1 PoPs will choose the service connection with the highest priority that satisfies the SLA to forward traffic.

Set Priority ▼ San Jose - California - USA ▼

<input type="checkbox"/>	Name	Priority ▲
<input type="checkbox"/>	DC1	P2 <input type="text"/>
<input type="checkbox"/>	DC2	P1 <input type="text"/> (Highest Priority)

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

Update Service Connection Priorities

1 PoPs will choose the service connection with the highest priority that satisfies the SLA to forward traffic.

Set Priority ▼ San Jose - California - USA ▼

<input type="checkbox"/>	Name	Priority ▲
<input type="checkbox"/>	DC2	P1 <input type="text"/> (Highest Priority)
<input type="checkbox"/>	DC1	P2 <input type="text"/>

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:

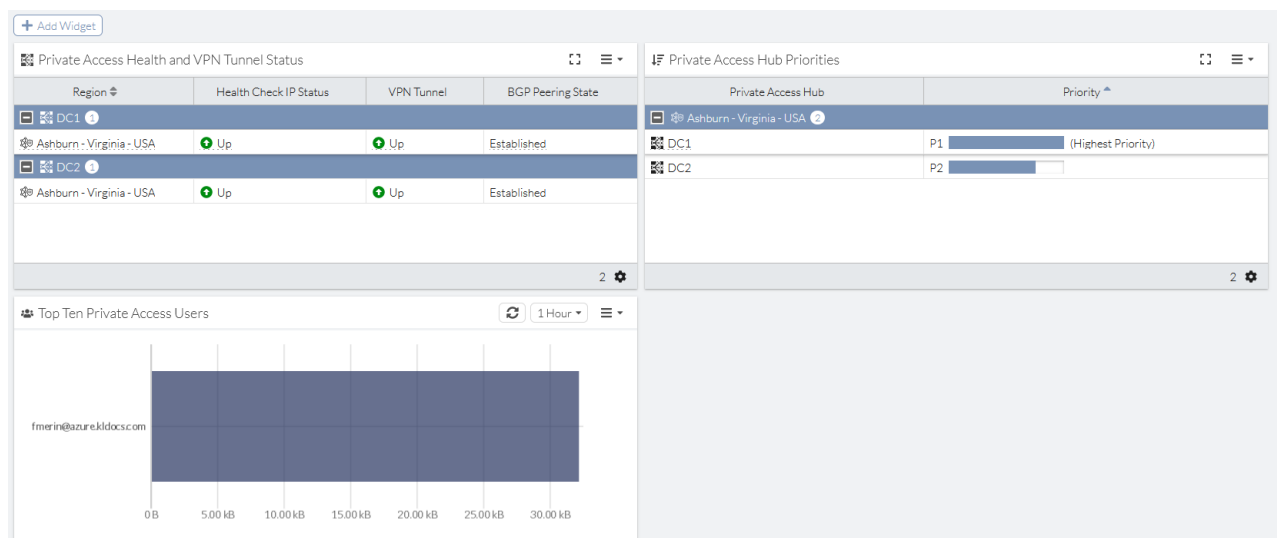
1. Go to *Network > Secure Private Access*.
2. Select the desired hub(s).
3. Click *Delete*.
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

Monitoring private access hubs

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

- Private Access Health and VPN 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:



Verifying private access policy configuration

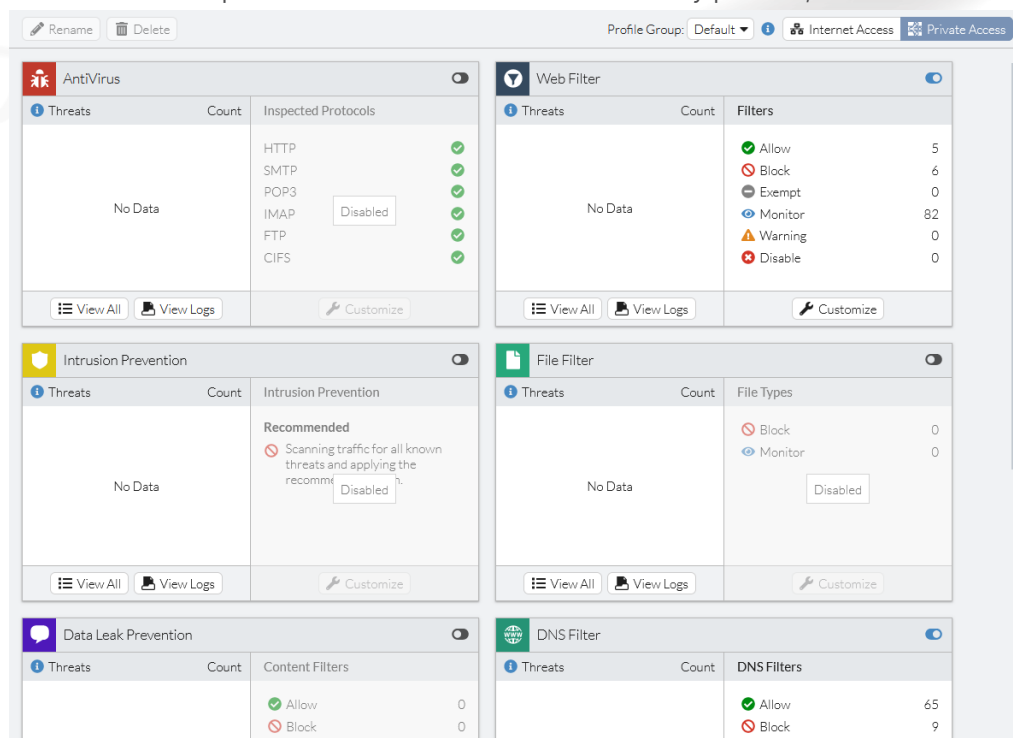
To verify private access policy configuration:

1. Go to *Configuration > Traffic > Policies*.
2. Click *Private Access*.
3. View the configured private access policy.

Configuring a private access security profile

To configure a private access security profile:

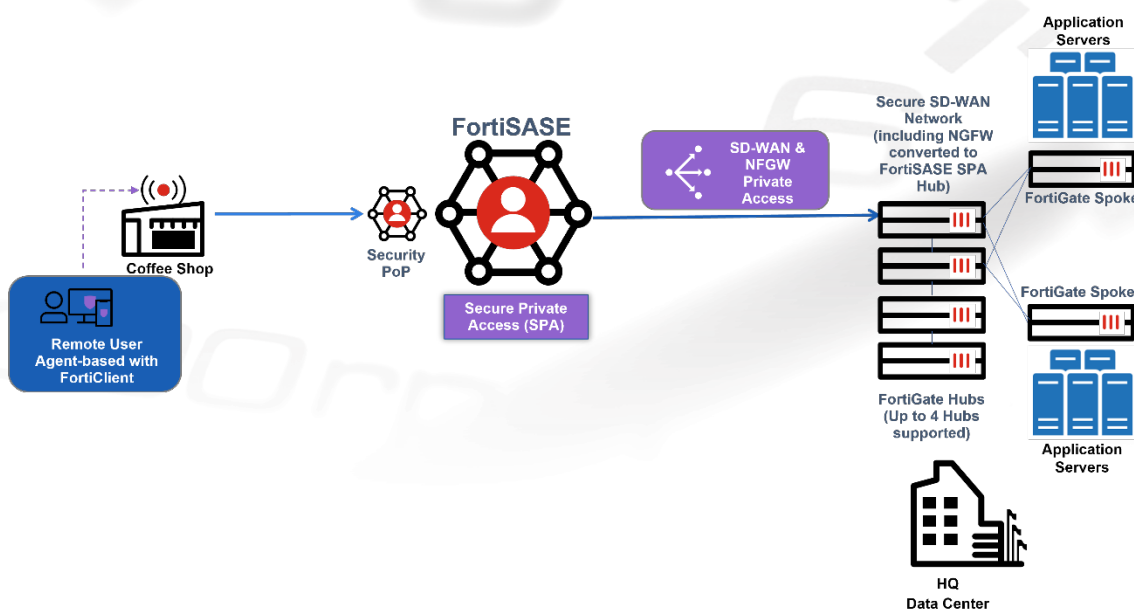
1. Go to *Configuration > Traffic > Security*.
2. In the top right corner, click *Private Access*.
3. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



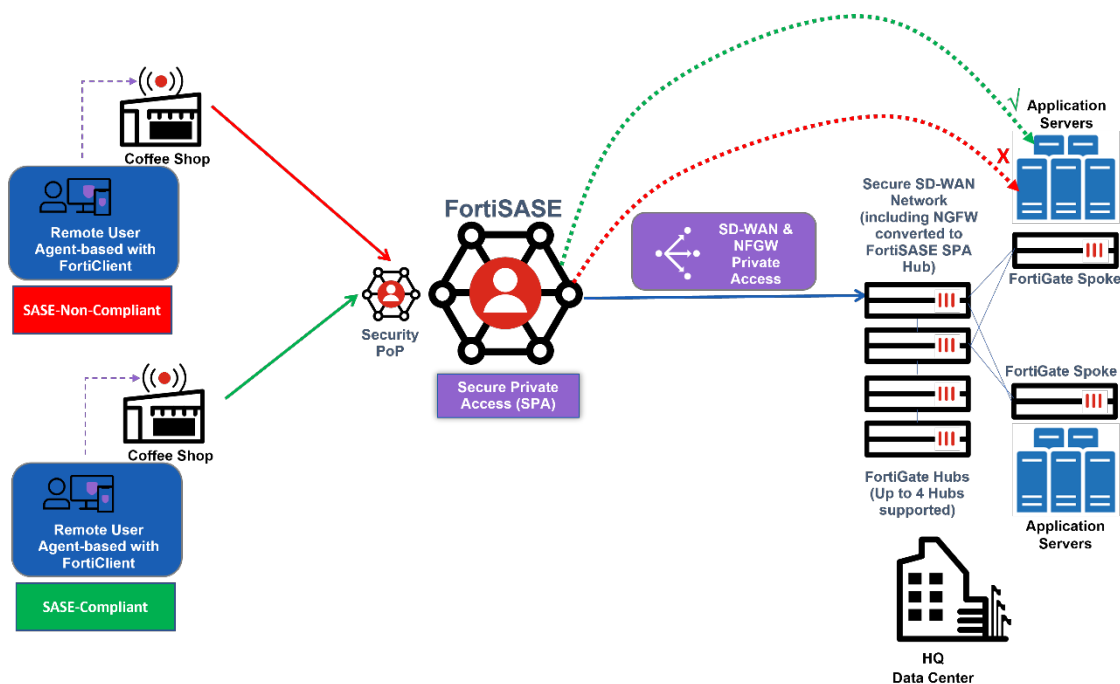
The security settings for Internet and private access are identical. For details on configuring security settings, see [Security](#).

Configuring ZTNA 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 zero trust network access (ZTNA) tagging rules that apply ZTNA 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 ZTNA 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 zero trust network access (ZTNA) tagging rule set for compliant endpoints.
2. Configure a ZTNA 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 ZTNA rule sets to dynamically tag agent-based remote users

This example demonstrates how to configure zero trust network access (ZTNA) tag names and ZTNA 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 ZTNA tagging rule set for compliant endpoints:

1. Go to *Configuration > ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.
5. Under *When the following rules match*, click *Create*.

6. Configure the Severity Level 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*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.

The screenshot shows the configuration interface for a SASE-Compliant tag. The 'Name' field is set to 'SASE-Compliant' and the 'Enabled' toggle is turned on. The 'Comments' field is empty. Below the 'When the following rules match' section, there is a table with two rules: 'Windows' and 'AntiVirus'. The 'Windows' rule is selected and has a count of 1. The 'AntiVirus' rule is also selected and has the matching criteria 'All parameters must pass'. Below the table, the 'Apply the following tag' section shows the 'Tag Name' dropdown set to 'SASE-Compliant'. At the bottom, there are 'OK' and 'Cancel' buttons.

Name: SASE-Compliant

Enabled: ☒

Comments:

When the following rules match

	Type	Parameters	Matching Criteria
<input checked="" type="checkbox"/>	Windows 1		
<input checked="" type="checkbox"/>	AntiVirus	AV Software is installed and running	All parameters must pass

Apply the following tag

Tag Name:

OK Cancel

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

1. Go to *Configuration > ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.
5. Under *When the following rules match*, click *Create*.
6. Configure the Severity Level 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*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.

Configuring dynamic private access policies using ZTNA tags

This example demonstrates how to configure dynamic private access policies using the zero trust network access tags that you created in [Configuring ZTNA rule sets to dynamically tag agent-based remote users on page 33](#) 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 *Configuration > Policies*.
2. Select *Private Access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
 - a. For *Name*, enter Allow-SASE-Compliant.
 - b. For *Source Scope*, select *VPN Users*.
 - c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag > Private Access*, select the *SASE-Compliant* tag.
 - d. For *Destination*, select *Specify*, click *+*, and in the *Select Entries* panel click *+Create* and click *IPv4 Host* to 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*.
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**.

The screenshot shows the 'Policy' configuration window in FortiGate. The policy is named 'Allow-SASE-Compliant'. The 'Source Scope' is set to 'VPN Users'. The 'Source' is set to 'All Traffic', and the 'Specify' button is active. The 'User' is set to 'All VPN Users', and the 'Specify' button is active. The 'Destination' is set to 'Private Access Traffic', and the 'Specify' button is active. The 'Service' is set to 'ALL'. The 'Profile Group' is set to 'Default'. The 'Force Certificate Inspection' is disabled. The 'Action' is set to 'Accept'. The 'Status' is set to 'Enable'. The 'Logging Options' section shows 'Log Allowed Traffic' is enabled, and 'Security Events' is selected. The 'OK' button is highlighted.

6. In *Configuration > Policies* with *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 *Configuration > Policies*.
2. Select *Private Access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
 - a. For *Name*, enter *Deny-SASE-Non-Compliant*.
 - b. For *Source Scope*, select *VPN Users*.
 - c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag > Private Access*, select the *SASE-Non-Compliant* tag.

- 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 *Configuration > Policies* with *Private Access* selected, ensure that you order the policies so that the *Deny-SASE-Non-Compliant* policy is before the *Allow-SASE-Compliant* policy. With this ordering of policies, FortiSASE denies endpoints that match the dynamic policy from accessing the specific private server.

<input type="checkbox"/>	Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
<input type="checkbox"/>	Deny-SASE-Non-Compliant		SASE-Non-Compliant	All VPN Users	PrivateServer	Deny	4	Enabled
<input type="checkbox"/>	Allow-SASE-Compliant	Default	SASE-Compliant	All VPN Users	PrivateServer	Accept	11	Enabled
<input type="checkbox"/>	Allow-All Private Traffic	Default	all	All VPN Users	All Private Access Traffic	Accept	0	Enabled
<input type="checkbox"/>	Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	Accept	0	Disabled
<input type="checkbox"/>	Implicit Deny		all	All VPN Users	All Private Access Traffic	Deny	14	Enabled

Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

1. In FortiSASE, go to *Configuration > Endpoints > Profile*.
2. Enable *Show tags on FortiClient*.
3. Click *Apply*. When this option is enabled, detected tags appear on the FortiClient avatar page.

fortinet

- ZERO TRUST TELEMETRY
- REMOTE ACCESS
- ZTNA DESTINATION
- VULNERABILITY SCAN
- Notifications
- Settings
- About

Add Full Name

Phone [Add Phone](#)

Email [Add Email](#)

Get personal info from

- User Input
- OS Updated 1/9/2023 10:21:05 AM
- LinkedIn
- Google
- Salesforce

Status Online/On-fabric

Hostname DESKTOP-BRQB09H

Domain

Zero Trust Tags

SASE-Non-Compliant

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 VPN user authentication defined on FortiSASE. Click *Connect*.

- In Windows Defender, set *Real-time protection* to *On* as [Stay protected with Windows Security](#) describes. This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.
- From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant Zero Trust tag applied.
- 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.
- 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
```

- In FortiSASE, in *Configuration > 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.

+ Create Edit Delete Search Internet Access Private Access								
<input type="checkbox"/>	Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
<input type="checkbox"/>	Deny-SASE-Non-Compliant		SASE-Non-Compliant	All VPN Users	PrivateServer	Deny	4	Enabled
<input type="checkbox"/>	Allow-SASE-Compliant	Default	SASE-Compliant	All VPN Users	PrivateServer	Accept	11	Enabled
<input type="checkbox"/>	Allow-All Private Traffic	Default	all	All VPN Users	All Private Access Traffic	Accept	0	Enabled
<input type="checkbox"/>	Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	Accept	0	Disabled
<input type="checkbox"/>	Implicit Deny		all	All VPN Users	All Private Access Traffic	Deny	14	Enabled

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

- In FortiClient, go to the *REMOTE ACCESS* tab.
- From the *VPN Name* dropdown list, select *Secure Internet Access*.
- Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.
- In Windows Defender, set *Real-time protection* to *Off* as [Stay protected with Windows Security](#) describes. This turns off AV and ensures that FortiSASE dynamically tags the endpoint as non-compliant.
- From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Non-Compliant Zero Trust tag applied.
- 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.
- 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),
```

8. In FortiSASE, in *Configuration > 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 increased.

Configuring DNS Settings

Remote users use *VPN Implicit DNS Rule* in FortiSASE under *Configuration > DNS* to resolve hostnames for internal and external domains.

By default, FortiSASE deployments use FortiGuard DNS as the default DNS server.

You can edit *VPN Implicit DNS Rule* and configure *Default DNS Server* with one of the following options and then click *OK* to save the change:

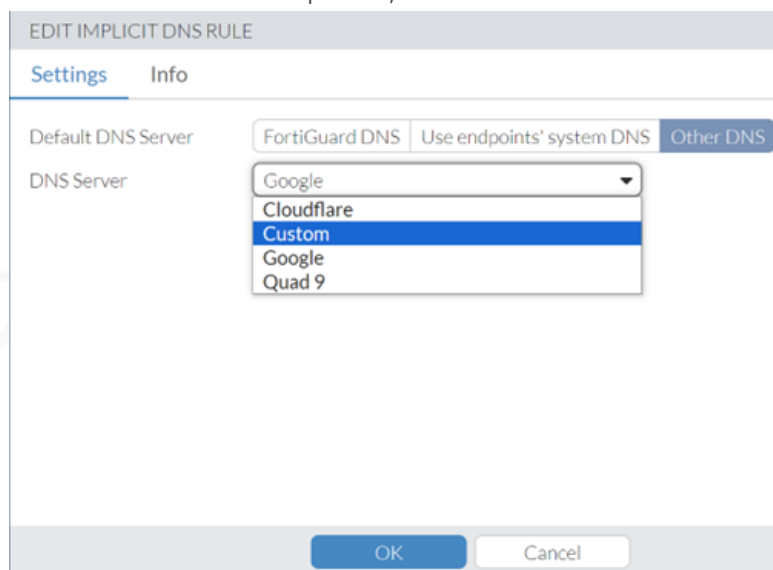
DNS Server		Description	Primary and secondary DNS server IP address
FortiGuard DNS		Use FortiGuard DNS	208.91.112.53 208.91.112.52
Use endpoints' system DNS		Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS		Use a public DNS server 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 IP address of primary and secondary DNS
	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 VPN implicit DNS rule to use a custom DNS server as follows:

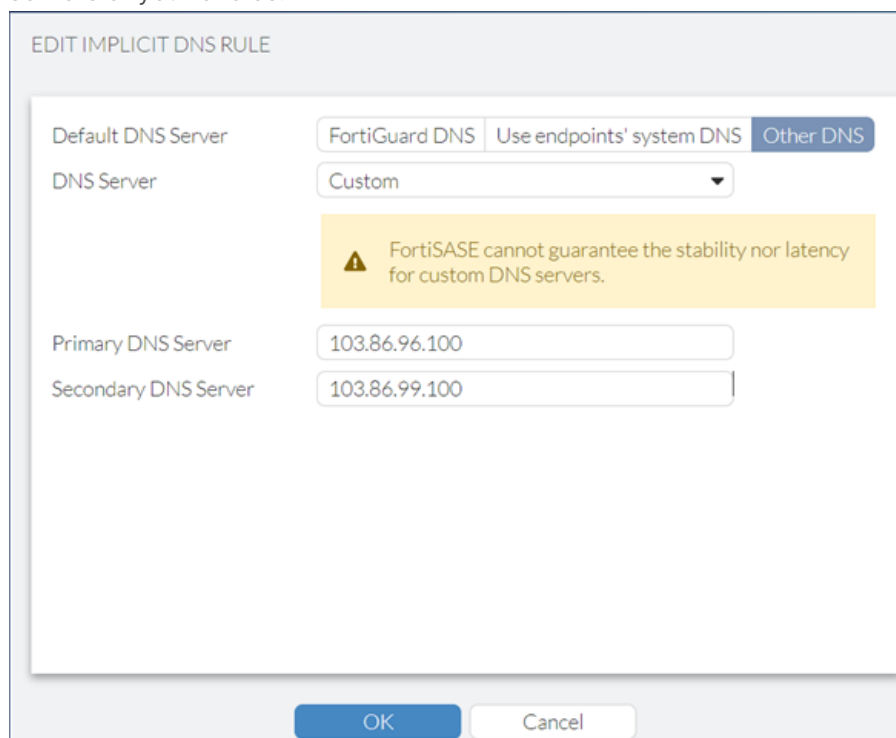
To configure a custom DNS server:

1. Go to *Configuration > DNS*, select *VPN Implicit DNS Rule*, and click *Edit*.
2. In the *Edit Implicit DNS Rule* page, for *Default DNS Server*, select *Other DNS*.

- From the *DNS Server* dropdown, select *Custom*.



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



- Click *OK*.

Using FortiGuard DNS or another public DNS service is sufficient for most agent-based Secure Internet Access (SIA) use cases that simply require agent-based remote users to resolve hostnames for external domains.

Split DNS Rules

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

- When 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.
- When 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, FortiSASE DNS settings can be configured for split DNS using *Split DNS Rules*.

Split DNS works as follows:

- Selectively use an internal DNS server only when it is necessary to resolve hostnames for the specified internal domain(s).
- Resolve all other hostnames for external domains using the implicit DNS rule.

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



For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

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 split DNS rules to work with DNS servers that support DoH, SSL deep inspection must be enabled for agent-based remote users on FortiSASE.

Prerequisites

SSL Deep Inspection

Split DNS requires SSL deep inspection to be enabled on FortiSASE so that FortiSASE can intercept the DNS traffic.

- To confirm SSL deep inspection is enabled, go to *Configuration > Security* and under the *SSL Inspection* widget ensure *Deep Inspection* is displayed.
- To enable SSL deep inspection, go to *Configuration > Security* and in the *SSL Inspection* widget click on *Customize*. In the *SSL Inspection* pane, select *Deep Inspection* and click *OK*.

See [Certificate and deep inspection modes](#) for further details on deep inspection.

Access to Internal DNS Server

Ensure that your FortiSASE remote users have access to the internal DNS server.



For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

Configuring Split DNS Rules

To configure Split DNS Rules:

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

CREATE DNS RULE

For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles.

Primary DNS Server

Secondary DNS Server

Domains


+

OK

Cancel

3. In the *Create DNS Rule* pane, enter the *Primary DNS Server*, (optional) *Secondary DNS Server*, and one or more *Domains*. Click *+* to add more fields to enter in additional domains. Click *OK*.

CREATE DNS RULE

 For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles.

Primary DNS Server

Secondary DNS Server

Domains

4. Observe that the split DNS rule has been created and is displayed in the table.

Domains	Primary DNS Server	Secondary DNS Server
DNS Rule 1		
<input type="checkbox"/> domain1.com	10.10.10.10	10.10.10.11
Implicit DNS Rule 2		
<input type="checkbox"/> VPN	FortiGuard DNS	
<input type="checkbox"/> SWG and Thin-Edge	FortiGuard DNS	



If you are using split DNS 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.

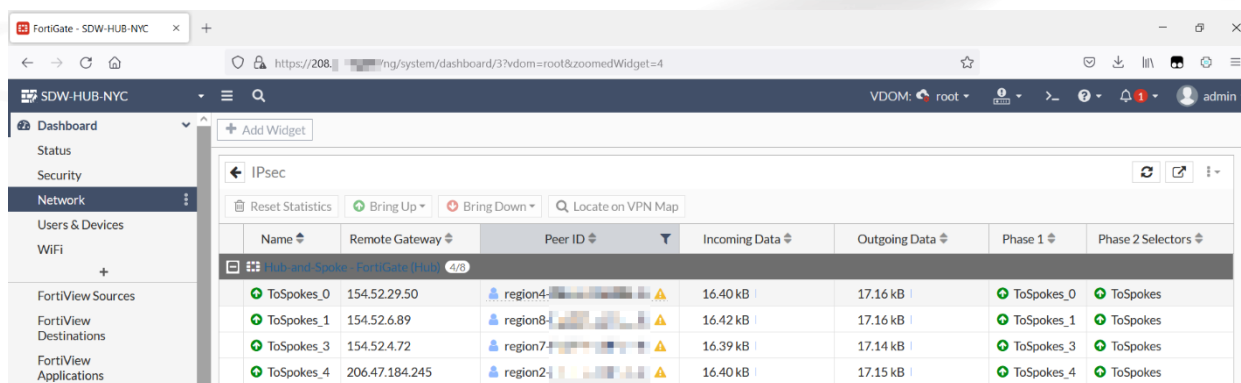


If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.

Verifying IPsec VPN tunnels on the FortiGate hub

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

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



To verify IPsec VPN 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 VPN 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/rcv: 1/2
lifetime/rekey: 86400/85206
DPD sent/rcv: 00000001/00000001
peer-id: region8-fos001-tiui7pzu-1
```

- For `diagnose vpn tunnel list`, confirm that the phase 2 IPsec VPN 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
```

- For `get vpn ipsec tunnel summary`, confirm that the phase 2 IPsec VPN 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:

- 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`
- 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 users

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

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
```

Verifying private access traffic in FortiSASE portal

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

- From *Analytics > Logs > Traffic* by viewing either the *All Internet and Private Access Traffic* page or the *Private Access Traffic* page
- From *Dashboard > FortiView > Sources*, *Dashboard > FortiView > Destinations*, or *Dashboard > FortiView > Policies* and filtering on the private access destination IP address

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

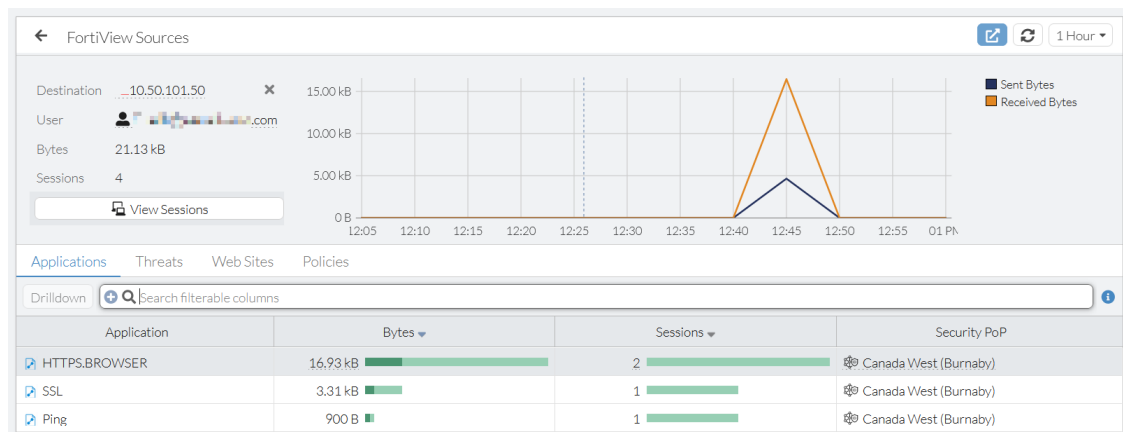
All Internet & Private Access Traffic						
Date/Time	User	Thin-Edge Device	Destination IP	Application Name	Policy ID	Security Events
2022/10/20 12:49:40	user@domain.com		10.50.101.50	HTTPS.BROWSER	1,000	Application Co
2022/10/20 12:49:30	user@domain.com		10.50.101.50	HTTPS.BROWSER	1,000	Application Co
2022/10/20 12:49:30	user@domain.com		10.50.101.50	SSL_TLsv1.3	1,000	Application Co
2022/10/20 12:47:52	user@domain.com		10.50.101.50	Ping	1,000	Application Co

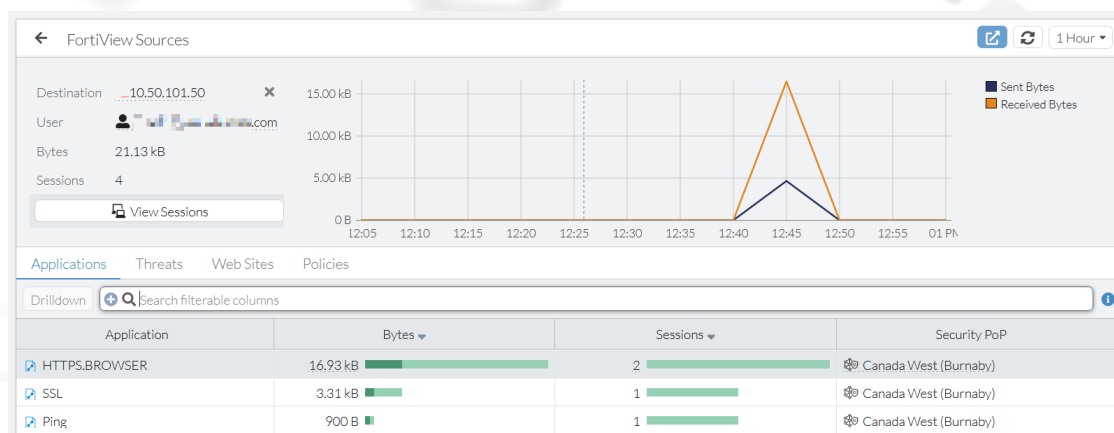
Following is an example of the *Analytics > Logs > Traffic > Private Access Traffic* page.

VERIFYING PRIVATE ACCESS TRAFFIC IN FORTISASE PORTAL

Private Access Traffic							
Date/Time	User	Thin-Edge Device	Destination IP	Application Name	Policy ID	Security Events	Action
2022/10/20 12:51:02	[redacted].com		10.50.102.50	SSH	1,000	Application Control	Accept: session close
2022/10/20 12:49:40	[redacted].com		10.50.101.50	HTTPS.BROWSER	1,000	Application Control	Accept: session close
2022/10/20 12:49:30	[redacted].com		10.50.101.50	HTTPS.BROWSER	1,000	Application Control	Accept: session close
2022/10/20 12:49:30	[redacted].com		10.50.101.50	SSL_TLSv1.3	1,000	Application Control	Accept: session close
2022/10/20 12:48:04	[redacted].com		10.50.102.50	Ping	1,000	Application Control	Accept
2022/10/20 12:47:52	[redacted].com		10.50.101.50	Ping	1,000	Application Control	Accept
2022/10/20 12:43:33	[redacted].com		192.168.40.150	Ping	1,000	Application Control	Accept
2022/10/20 07:48:21	[redacted].com		10.25.3.4	Ping	1,000	Application Control	Accept
2022/10/20 07:07:51	[redacted].com		10.16.100.1	Ping	1,000	Application Control	Accept
2022/10/20 07:04:29	[redacted].com		10.16.100.50	Ping	1,000	Application Control	Accept
2022/10/07 16:38:57	[redacted].com		10.16.101.50	HTTPBROWSER_Firefox	1,000	Application Control	Accept: session close
2022/10/07 16:38:22	[redacted].com		10.16.100.50	Ping	1,000	Application Control	Accept
2022/10/07 16:38:06	[redacted].com		10.16.101.50	Ping	1,000	Application Control	Accept

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

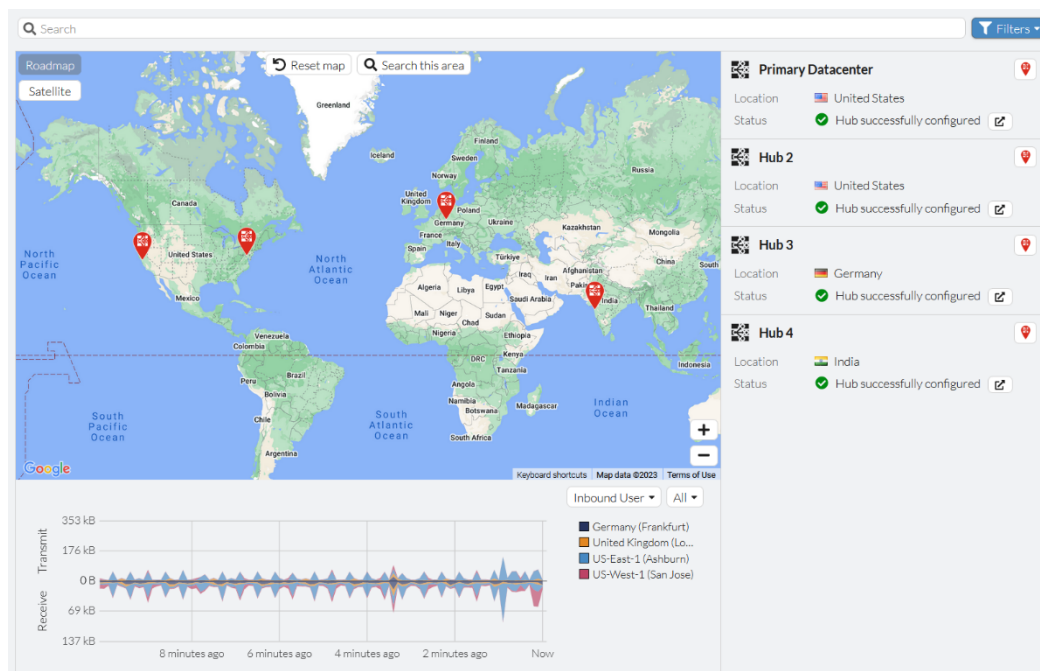




Verifying private access hub status and location using the asset map

The *Network > 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.



More information

Appendix A: Products used in this guide

For a list of product models and firmware that this guide uses, see [Product integration and support](#).

Appendix B: Documentation references

Feature documentation

Product document	Specific chapter if available
FortiOS 7.0.6 Admin Guide	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• SD-WAN Overlay Templates• IPsec tunnel templates• BGP templates

4-D resources: SASE

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

Appendix C - 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 9](#).

FortiSASE 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 on page 50](#)
- [Tunnel interface configuration on page 55](#)
- [Loopback interface configuration on page 56](#)
- [Firewall policy configuration on page 57](#)
- [BGP configuration on page 59](#)

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*.

The screenshot shows the 'New VPN Tunnel' configuration window in the FortiGate GUI. The 'Network' tab is active, displaying various configuration options. The 'Name' field is set to 'VPN1'. The 'Comments' field is empty. The 'Network' section includes options for 'IP Version' (IPv4 and IPv6), 'Remote Gateway' (Dialup User), 'Interface' (Internet_Access (port1)), 'Local Gateway' (disabled), 'Mode Config' (checked), 'Use system DNS in mode config' (unchecked), 'Assign IP From' (Range), 'IPv4 mode config' (Client Address Range: 10.251.1.1-10.251.1.251, Subnet Mask: 255.255.255.0, DNS Server: 0.0.0.0), 'IPv6 mode config' (Client Address Range: ::::, Prefix Length: 128, DNS Server: ::), 'Enable IPv4 Split Tunnel' (unchecked), 'Enable IPv6 Split Tunnel' (unchecked), 'NAT Traversal' (Enable), and 'Dead Peer Detection' (On Idle). The 'Additional Information' panel on the right contains links to 'API Preview', 'IPsec VPNs', 'Guides', 'IPsec VPN Cookbook Recipes', 'VPN Setup on FortiClient', 'Configuring an IPsec VPN Connection', 'Online Guides', 'Relevant Documentation', 'Video Tutorials', and 'Hot Questions at FortiAnswers'.

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*.

NAT Traversal	Enable Disable Forced
Dead Peer Detection	Disable On Idle On Demand
DPD retry count	3
DPD retry interval	60 s
Forward Error Correction	Egress <input type="checkbox"/> Ingress <input type="checkbox"/>
Advanced...	
Add route	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Disabled
Auto discovery sender	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Disabled
Auto discovery receiver	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Disabled
Exchange interface IP	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Disabled
Device creation	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Disabled

8. Set the *Authentication* options:

- From the *Method* dropdown list, select *Pre-shared Key*.
- In the *Pre-shared Key* field, enter an alphanumeric string.
- For *IKE > Version*, select *2*.
- From the *Accept Types* dropdown list, select *Any peer ID*.

Authentication		
Method	Pre-shared Key ▼	
Pre-shared Key	●●●●●●●●	
IKE		
Version	1 2	
Peer Options		
Accept Types	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).

Phase 1 Proposal
+ Add

☒ ☐

Encryption AES256 ▼

Authentication SHA256 ▼

	<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
Diffie-Hellman Groups	<input checked="" type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
	<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

Key Lifetime (seconds) 86400 ▼

Local ID

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.

- Advanced...

Phase 2 Proposal
+ Add

Encryption AES256 ▼

Authentication SHA256 ▼

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

	<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
Diffie-Hellman Group	<input checked="" type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
	<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

Local Port All ☒

Remote Port All ☒

Protocol All ☒

Autokey Keep Alive ☐

Key Lifetime Seconds ▼

Seconds 43200 ▼

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* and *Remote IP/Netmask*.
 - b. For *Administrative Access*, select *PING*.
4. Click *OK* to save the changes.

The screenshot shows the 'Edit Interface' dialog in the FortiGate GUI. The interface is named 'VPN1' and is a 'Tunnel Interface' connected to 'Internet_Access (port1)'. The VRF ID is 0 and the role is 'Undefined'. The addressing mode is 'Manual' with IP 10.251.1.254 and netmask 255.255.255.255. The remote IP/netmask is 10.251.1.253 255.255.255.0. Under 'Administrative Access', 'PING' is selected. The interface status is 'Up'.

To create the tunnel interface using the CLI:

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

Loopback interface configuration

You must create a loopback interface on the FortiGate hub. The configuration uses the loopback interface to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment and provide a health check target for the performance SLA on the FortiSASE security PoPs.



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

To configure the 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*.

Name

Lo-BGP-RID

Alias

Type

Loopback Interface

VRF ID ⓘ

0

Role ⓘ

LAN

Address

IP/Netmask

10.1.0.254/255.255.255.255

Create address object matching subnet

☒

Name

Lo-BGP-RID address

Destination

10.1.0.254/255.255.255.255

Secondary IP address

☐

Administrative Access

IPv4

☐ HTTPS

☐ HTTP ⓘ

☒ PING

☐ FMG-Access

☐ SSH

☐ SNMP

☐ FTM

☐ RADIUS Accounting

☐ Security Fabric Connection ⓘ

☐ Speed Test

To configure the 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

```

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.



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

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 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 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 *Lo-HC*.
 - c. Set the following options:
 - i. For *Incoming interface*, select *VPN1*.
 - ii. For *Outgoing interface*, select *Lo-BGP-RID*.
 - 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 "Lo-BGP-HC"
set srcintf "VPN1"
set dstintf "Lo-BGP-RID"
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

- 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 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



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.

Local BGP Options

Local AS

65001

Router ID

10.1.0.254

Neighbors

+ Create New

Edit

Delete

IP	Remote AS
No results	

0

- 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*
 - *Capability: graceful restart*
 - *Capability: route refresh*
- vii. Click *OK*.

Edit BGP Neighbor Group

Name
VPN1

Remote AS
65001

Interface
VPN1

Activate IPv4

IPv4 Filtering

Filter list in

Filter list out

Distribute list in

Distribute list out

Prefix list in

Prefix list out

Route map in

Route map out

Allow AS in

Graceful restart time
0

Max prefix

Attribute unchanged

☒ Route reflector client
☐ Soft reconfiguration
☒ Capability: graceful restart

☒ Next hop self
☐ AS override
☒ Capability: route refresh

☐ Remove private AS
☐ Route Server Client
☐ Capability: default originate

OK

Cancel

Neighbor Groups

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> </div>	
Name	Remote AS
VPN1	65001
<div>1</div>	

- 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*.

Create BGP Neighbor Range
✕

Prefix

Neighbor group

VPN1
▼

Max neighbor number

OK
Cancel

Local BGP Options

Neighbor Groups

+ Create New
✎ Edit
🗑 Delete

Name	Remote AS
VPN1	65001

1

Neighbor Ranges

+ Create New
✎ Edit
🗑 Delete

Prefix	Neighbor Group	Maximum Neighbor Number
10.251.1.0 255.255.255.0	VPN1	0

1

Networks

IP/Netmask

✕

+

IPv6 Networks

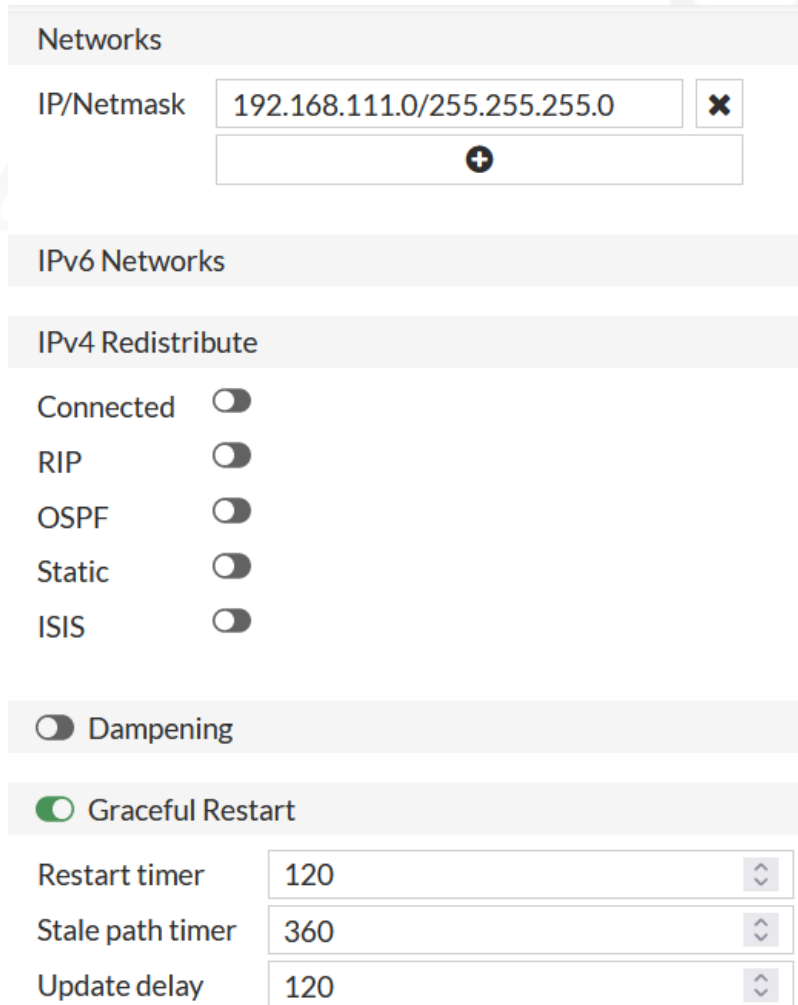
IPv4 Redistribute

Apply

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.



Networks

IP/Netmask

IPv6 Networks

IPv4 Redistribute

Connected ☐

RIP ☐

OSPF ☐

Static ☐

ISIS ☐

☐ Dampening

☒ Graceful Restart

Restart timer

Stale path timer

Update delay

6. Under *Advanced Options*, configure the following:

- a. In the *Keepalive* field, enter 60.
- b. Enable *Holdtime* and enter 180.

- c. Enable *Background scan* and enter 60.

Advanced Options

Cluster ID	10.1.0.254
Default Local Preference	100
Distance external	20
Distance internal	200
Distance local	200
Keepalive	60
Holdtime	<input checked="" type="checkbox"/> 180
Background scan	<input checked="" type="checkbox"/> 60

7. Under *Best Path Selection*, enable the following options:
- Client to client reflection*
 - EBGP multi path*
 - IBGP multi path*
 - Additional path*
 - Enforce first AS*
 - Fast external failover*
 - Log neighbor changes*
 - Network import check*

i. Ignore optional capability

Best Path Selection	
Always compare med	<input type="checkbox"/>
AS path ignore	<input type="checkbox"/>
Compare confederation AS path	<input type="checkbox"/>
Compare router ID	<input type="checkbox"/>
Med confederation	<input type="checkbox"/>
Med missing AS worst	<input type="checkbox"/>
Synchronization	<input type="checkbox"/>
Deterministic med	<input type="checkbox"/>
Client to client reflection	<input checked="" type="checkbox"/>
EBGP multi path	<input checked="" type="checkbox"/>
IBGP multi path	<input checked="" type="checkbox"/>
Additional path	<input checked="" type="checkbox"/>
Enforce first AS	<input checked="" type="checkbox"/>
Fast external failover	<input checked="" type="checkbox"/>
Log neighbor changes	<input checked="" type="checkbox"/>
Network import check	<input checked="" type="checkbox"/>
Ignore optional capability	<input checked="" type="checkbox"/>

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
  config neighbor-group
    edit "VPN1"
      set link-down-failover enable
      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 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 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
end
```



www.fortinet.com



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.