SPA Deployment Guide using BGP on loopback

FortiSASE 7.2

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change log 4

Deployment overview 5

Intended audience 5

About this guide 5

SPA design concept and considerations 6

FortiSASE SPA and Fortinet ADVPN 6

FortiSASE SPA hub versus SD-WAN hub 7

BGP on loopback 7

Network restrictions 7

Supported features for each SPA BGP routing design 7

FortiGate NGFW to FortiSASE SPA hub conversion deployment 8

Deployment overview 8

Design concept and considerations 9

Product prerequisites 9

Deployment plan 9

Deployment procedures 11

Provisioning your FortiSASE instance 11

Use case specific deployment configurations 11

FortiGate NGFW to SPA hub conversion specific configurations 11

Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access 18

Configuration workflow 18

Configuring network configuration 18

Configuring a new service connection 22

Viewing health and VPN tunnel status 25

Editing SLA thresholds 26

Updating service connection priorities 28

Deleting a hub configuration 29

Monitoring private access hubs 30

Configuring a private access policy for client-to-server traffic 30

Configuring a private access policy for server-to-client traffic 33

Configuring a private access security profile 35

Configuring ZTNA tags in private access policies 35
Configuring DNS Settings 43
Split DNS Rules 45
Verifying IPsec VPN tunnels on the FortiGate hub 50
Verifying BGP routing on the FortiGate hub 51
Testing private access connectivity to FortiGate hub network from remote VPN users and edge devices 52
Testing private access connectivity to FortiGate hub network from remote SWG users 52
Testing private access connectivity from FortiGate hub network to remote VPN users 53
Verifying private access traffic in FortiSASE portal 53
Verifying private access traffic from hubs 55
Verifying private access hub status and location using the asset map 55
Restricting access using a FortiGate SPA hub/spoke policy 56
More information 59
Appendix A: Products used in this guide 59

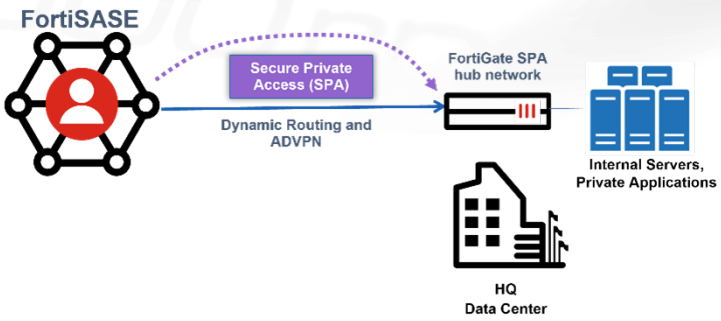
Change log

Date	Change description
2026-06-17	Initial release.

Deployment overview

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

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



This deployment document was tested with a particular FortiSASE version and particular firmware versions of associated Fortinet products. The features in this deployment guide may have been updated since this document was originally published. For the latest details about features included in this guide, please refer to the FortiSASE 7.2 Administration Guide.

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

- FortiGate NGFW to SPA hub conversion specific configurations on page 11

Intended audience

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

About this guide

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

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

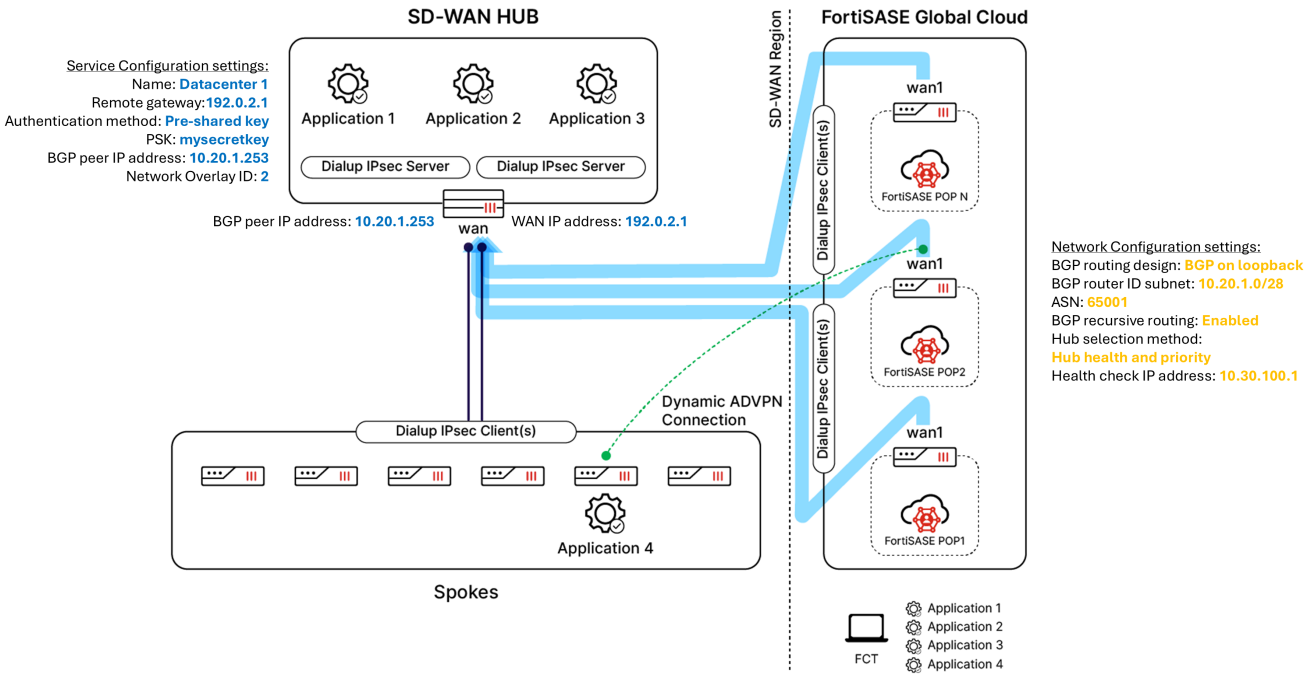
This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. Reviewing supplementary material

found on the Fortinet Document Library in product administration guides, example guides, cookbooks, release notes, and other documents is recommended, where appropriate.

SPA design concept and considerations

FortiSASE SPA and Fortinet ADVPN

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



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

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

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

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

> This deployment guide only covers the FortiGate configuration for the BGP on loopback routing design.

FortiSASE SPA hub versus SD-WAN hub

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

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

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

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

BGP on loopback

BGP on loopback is the newer BGP routing design supported by FortiSASE SPA hubs. It offers improved scalability since less routes are advertised in the network and offers simplified configuration since fewer BGP neighbors need to be configured.

For details on the BGP on loopback routing design, refer to BGP on loopback and BGP on loopback: advantages.

Network restrictions

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

Supported features for each SPA BGP routing design

The following is a summary of the features supported based on the BGP routing design:

Feature	BGP per overlay	BGP on loopback
Additional IPsec overlay	No	Yes
ADVPN Route Tag	No	Yes
Agentless ZTNA	Yes	
DNS redirection rules	Yes	
External feeds	Yes	No
Forwarding logs to on-premise private FortiAnalyzer	Yes	
FSSO with private FortiAuthenticator	Yes	No

Feature	BGP per overlay	BGP on loopback
Peering via eBGP		
Peering via iBGP		

FortiGate NGFW to FortiSASE SPA hub conversion deployment

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

- Deployment overview on page 8
- Design concept and considerations on page 9
- Product prerequisites on page 9
- Deployment plan on page 9

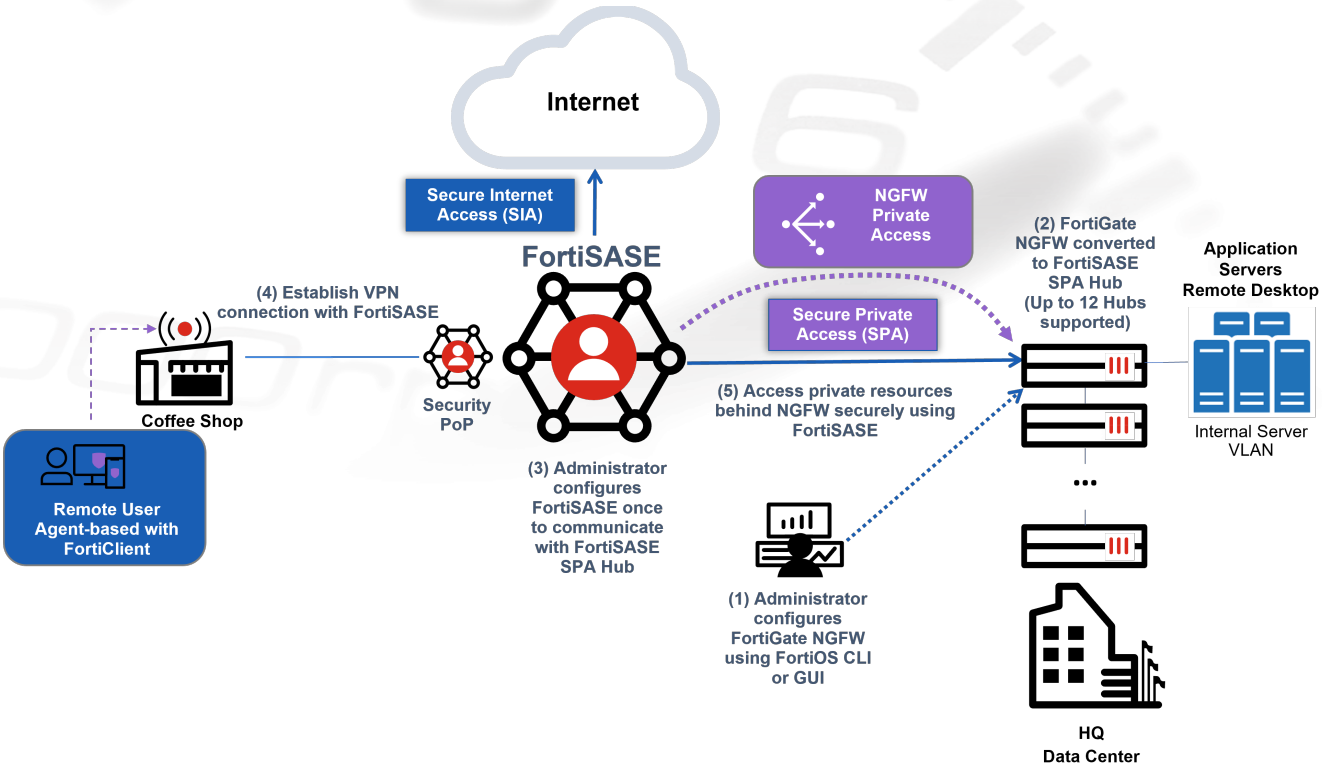
Deployment overview

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

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

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

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



Design concept and considerations

FortiGate NGFW

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

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 11 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input subscriptions as needed.
2. Convert the FortiGate NGFW to a FortiSASE SPA hub using FortiOS CLI.
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 subscription to provision FortiSASE, then do the following.

To provision your FortiSASE instance:

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

Use case specific deployment configurations

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

- FortiGate NGFW to SPA hub conversion specific configurations on page 11

Once you have finished the required configuration, proceed to Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access on page 18.

FortiGate NGFW to SPA hub conversion specific configurations

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

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

Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS CLI

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

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

- IPsec VPN configuration on page 12
- Loopback interface and static routing configuration on page 13
- Firewall policy configuration on page 14
- BGP configuration on page 15

This deployment guide only covers the FortiGate configuration for the BGP on loopback routing design.

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.
- 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
- Configure `set exchange-ip-addrv4 <BGP peer IP address>` to allow IKE to inject a custom /32 route on the dial-up IPsec tunnel interfaces towards the spokes. This route provides loopback reachability without the use of additional routing protocols.

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

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

- 10.1.2.253 is the hub BGP peer IP address, which is the IP address of the loopback interface used for BGP peering. See Loopback interface and static routing configuration on page 13.
- Unlike with BGP per overlay, in the BGP on loopback design there is no need to configure any tunnel IPs. Therefore, there is no need to plan tunnel subnets and IKE mode configuration is no longer used.

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 exchange-ip-addr4 10.1.2.253
        set proposal aes256-sha256 aes256-sha1 aes128-sha256 aes128-sha1
        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 11
        set psksecret <pre-shared key>
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit VPN1
        set phase1name VPN1
        set proposal aes256gcm aes256-sha256 aes128gcm aes128-sha256 aes128-sha1 aes256-sha1
chacha20poly1305
        set dhgrp 21 14 5
    next
end
```

Loopback interface and static routing configuration

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

- A loopback interface Lo_BGP-RID to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment.
- A loopback interface Lo-HC to provide a health check target for the performance SLA on the FortiSASE security PoPs. In FortiSASE, you will need to set the Health Check IP address to the IP address configured for this interface. See Configuring a new service connection on page 22.

In addition, a loopback summary must be advertised using BGP from the hub to the spokes to ensure that spoke-to-spoke traffic first comes to the hub before going to directly to the spoke to create spoke-to-spoke ADVPN shortcut tunnels.

- A loopback summary is a large subnet which contains all the possible loopback IP addresses
- For a loopback summary to be advertised, it must exist in the FortiGate routing table.
- Since only the hub loopback interface has an IP address within the loopback summary subnet, then the administrator must explicitly define the loopback summary in the FortiGate routing table. This is achieved by adding a blackhole static route (also known as a null static route) to the routing table.
- In this example, the FortiGate SPA hub has defined a loopback interface with IP address of 10.1.2.253/32. Therefore, the loopback summary is 10.1.2.0/23 and this is defined as a blackhole static route as demonstrated below.

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

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

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.1.2.253 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

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

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

To configure a blackhole static route in the FortiGate routing table:

```
config router static
    edit 100
        set dst 10.1.2.0 255.255.254.0
        set blackhole enable
    next
end
```

Firewall policy configuration

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

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

To configure firewall policies using the CLI:

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

BGP configuration

FortiSASE security points of presence (PoPs) connect to the hub FortiGate and establish iBGP peerings. FortiSASE security PoPs learn routes to your network and advertise the IPAM pool used for remote agents and edge devices.

- Routes learned by security PoPs from the SPA hubn network allow remote agents and edge devices to send traffic to private servers behind the SPA hub network.
- Routes advertised from security PoPs to SPA hub allow reply traffic from private servers to reach remote agents and edge devices initiating requests.

The hub FortiGate requires the following BGP settings:

- AS numbers
- Router ID

- Using iBGP for dynamic routing via overlays
- BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs
  - Route reflector (RR) functionality must be enabled on the neighbor-group for the correct ADVPN operation since dynamic BGP is currently not used for BGP on loopback design with FortiSASE security PoPs.
- One BGP session per overlay associated with the hub loopback interface between the hub and each FortiSASE security PoP, regardless of the number of IPsec overlays
- A route map is defined with the well-known “no-export” community which ensures that the loopback summary is not advertised to eBGP peers.
  - As mentioned previously, a loopback summary must be advertised using BGP from the hub to the spokes to ensure that spoke-to-spoke traffic first comes to the hub before going to directly to the spoke to create spoke-to-spoke ADVPN shortcut tunnels.

As demonstrated below, the BGP router ID subnet is 10.1.3.0/24 and the loopback summary is 10.1.2.0/23. Therefore, the BGP peer IP address for the hub is 10.1.2.253, chosen from within 10.1.2.0/23 but not overlapping with 10.1.3.0/24 which are assigned to Security PoPs.

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

To configure route map used by BGP using the CLI:

```
config router route-map
    edit "LOCAL_REGION"
        config rule
            edit 1
                set set-community "no-export"
                unset set-ip-prefsrc
            next
        end
    next
end
```

To configure BGP using the CLI:

To allow for dynamic scaling of customer environments, as-needed, it is necessary to use the BGP router ID subnet with a larger subnet (i.e. /24 or 255.255.255.0) instead of the minimum /28 subnet (255.255.255.240).

As demonstrated below, the BGP router ID subnet is 10.1.3.0/24 and the loopback summary is 10.1.2.0/23. Therefore, the BGP peer IP address for the hub is 10.1.2.253, chosen from within 10.1.2.0/23 but not overlapping with 10.1.3.0/24 which are assigned to Security PoPs.

```
config neighbor-range
        edit 1
            set prefix 10.1.3.0 255.255.255.0
            set neighbor-group "VPN1"
        next
    end
    config network
        edit 3
            set prefix 10.1.2.0 255.255.254.0
            set route-map "LOCAL_REGION"
        next
    end
end
```

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

```
config router bgp
    set as 65001
    set router-id 10.1.2.253
    set keepalive-timer 5
    set holdtime-timer 15
    set ebgp-multipath enable
    set ibgp-multipath enable
    set recursive-next-hop enable
    set cluster-id 10.1.2.253
    config neighbor-group
        edit "VPN1"
            set advertisement-interval 1
            set next-hop-self enable
            set next-hop-self-rr enable
            set soft-reconfiguration enable
            set interface "Lo-BGP-RID"
            set remote-as 65001
            set update-source "Lo-BGP-RID"
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.1.3.0 255.255.255.240
            set neighbor-group "VPN1"
        next
    end
    config network
        edit 1
            set prefix 192.168.111.0 255.255.255.0
```

```
        next
        edit 2
            set prefix 10.11.11.11 255.255.255.255
        next
        edit 3
            set prefix 10.1.2.0 255.255.254.0
            set route-map "LOCAL_REGION"
        next
    end
end
```

Configuring SPA to the FortiGate SPA hub in FortiSASE Secure 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.

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

To allow FortiSASE remote users with secure private access (SPA) to resources behind your FortiGate SPA 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:

1. Under *Network* > *Network Configuration*, configure the common network configuration settings. See Configuring network configuration on page 18.
2. Under *Network* > *Secure Private Access*, click *Create*, and configure a new service connection (hub). See Configuring a new service connection on page 22.

You cannot configure a service connection or hub without first configuring *Network* > *BGP* 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.

To configure SPA network configuration:

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

1. Go to *Network* > *Network Configuration*.
2. Under *Network* > *BGP*, under the *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select *BGP on loopback*.
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: • BGP per overlay (default) • BGP on loopback You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them. See Routing design methods. This deployment guide only covers the FortiGate configuration for the BGP on loopback routing design.	BGP on loopback
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.	10.1.3.0/24

Network attributes	Description	Example
	Typically, this BGP router ID subnet is a subnet within the overall BGP loopback summary range that is currently unused. For example, if the BGP loopback summary range is 10.20.1.0/24 then you can choose to configure 10.20.1.0/28 as the BGP router ID subnet if it is unused.	
Autonomous system number (ASN)	BGP autonomous system (AS) number of your hubs. Typically, this should be the same on both hubs.	65001
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

Network attributes	Description	Example
Hub selection method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: • **Hub health and priority**: periodically obtain jitter, latency, and packet loss measurements for each hub via the health check IP address. FortiSASE selects the highest priority hub within each PoP that meets lowest cost (SLA). 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.	10.11.11.11

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.	

4. Click *Save*.

Considerations

- As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.
- For BGP on loopback, the FortiSASE security PoPs use their loopback interface with IP address assigned from the BGP router ID subnet for BGP peering with the FortiGate hub(s). The BGP peer IP address defined in the service connection(s) should be a loopback interface on the FortiGate hub(s).
- The BGP peer IP address defined in each service connection should not fall within the BGP router ID subnet. A common strategy to avoid this is to pick a subnet, such as a /24, and allocate a portion of that subnet for the FortiSASE security PoPs, such as a /25, and the remaining portion of it for the FortiGate hub(s).
- When using the BGP MED option, user-defined hub priorities are not used because the SD-WAN SLA rule is disabled in this case.

Configuring a new service connection

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

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

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 on loopback:

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

1. Go to *Operations* > *Connectivity* > *Secure private access*.
2. Click *Create*.
3. For the *Create a 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 (-).	FGT-DC1
Autonomous System Number (ASN)	ASN number of the FortiGate hub. Only configurable if the support for multi-ASN configuration is enabled under *Network* > *BGP*.	65001
Remote Gateway	IPsec remote gateway (public IP address) for the hub.	192.0.2.1
Authentication Method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared Key* (default) and *Certificate*.	Pre-shared Key
Pre-shared Key	When *Authentication Method* is configured as *Pre-shared Key*, define the hub PSK.	mysecretkey
PKI User	If you configured *Authentication Method* as *Certificate*, select the PKI user with a valid subject and CA certificate that FortiSASE uses to validate the hub certificate. You can directly create the PKI user from *Create* or via *Configuration* > *PKI*, then select it here.	Mypeer
Certificate	When *Authentication Method* is configured as *Certificate*, select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via *System* > *Certificates* as a *Local Certificate*.	Fortinet_ Factory
ADVPN Route Tag	For BGP on loopback 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.	99
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.1.2.253
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 tunnels towards each hub have different network overlay IDs.	11

4. (Optional) If on the same hub you have a redundant WAN interface configured as the gateway, you can configure an additional IPsec tunnel from FortiSASE to redundant WAN interface. This additional IPsec overlay can be typically used as a redundant IPsec overlay. This configuration option is only available for *BGP on loopback* routing design. A maximum of one backup or redundant IPsec tunnel can be configured per Service Connection.

   To create additional IPsec overlay, click *Create* and fill in the attributes below.

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 (-).	FGT-DC2
Remote gateway	IPsec remote gateway (public IP address of redundant WAN interface) for the hub.	192.0.2.2
Authentication method	Method used to authenticate with the FortiGate hub. Supports Pre-shared key (default) and Certificate.	Pre-shared key
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK. This can be same or different than the Main IPsec overlay PSK.	mysecretkey
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 tunnels towards each hub have different network overlay IDs.	Mypeer

5. Click *Save*.
6. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*. For *BGP on loopback*, *Configuration State* is based on the first overlay connection to the hub. If you have redundant IPsec overlays configured for your Service Connection, the backup IPsec overlay will always appear below the Main overlay.
7. (Optional) Repeat the steps to configure up to a total of twelve 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. 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*.

Considerations

- 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%

  You can edit these parameters in FortiSASE. See Editing SLA thresholds on page 26.

  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.
- Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following remaining network restrictions when network restrictions have been removed per Network restrictions removed, and ensure your network configuration does not overlap with them.

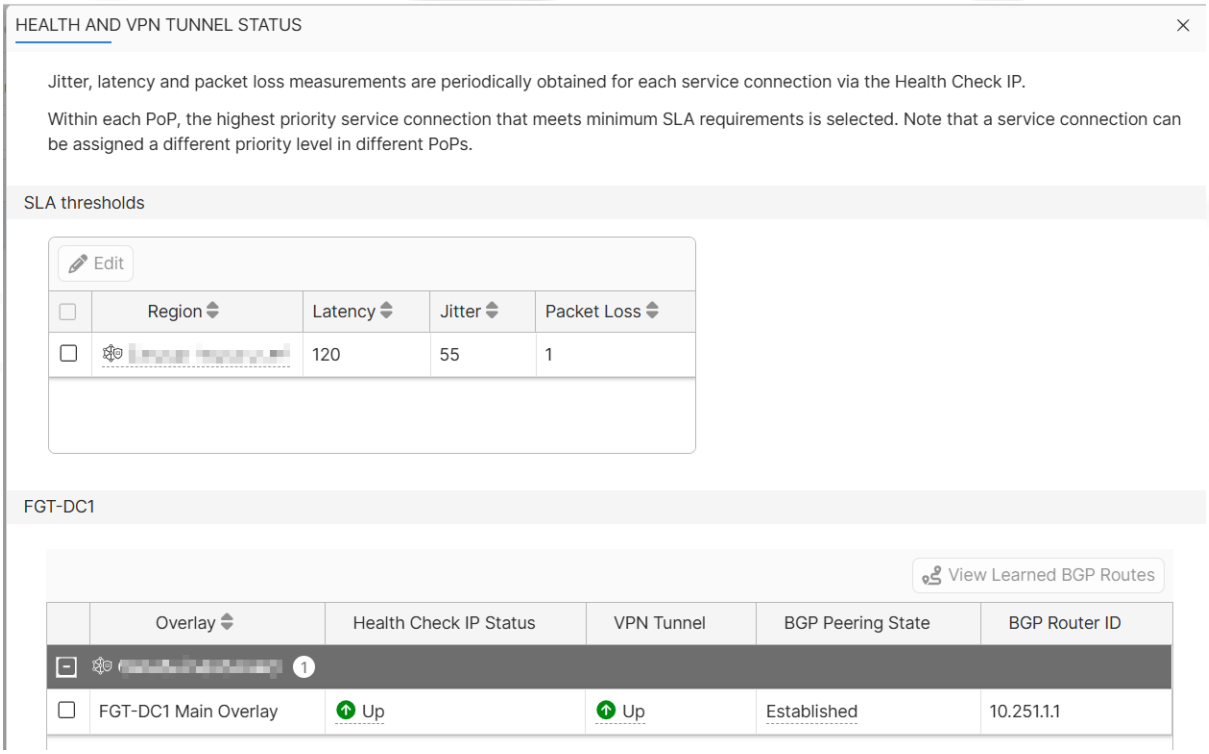
  The FortiExtender and LAN Extension control plane subnet are configurable (default subnet: 10.252.0.0/16). See IP management.
- For BGP on loopback, the FortiSASE security PoPs use their loopback interface with IP address assigned from the BGP router ID subnet for BGP peering with the FortiGate hub(s). The BGP peer IP address defined in the service connection(s) should be a loopback interface on the FortiGate hub(s).
- The BGP peer IP address defined in each service connection should not fall within the BGP router ID subnet. A common strategy to avoid this is to pick a subnet, such as a /24, and allocate a portion of that subnet for the FortiSASE security PoPs, such as a /25, and the remaining portion of it for the FortiGate hub(s).
- **Routing best practice for SPA hub**

  When advertising prefixes from SPA hubs, ensure that only the prefixes intended to be routed through SPA are advertised to FortiSASE security points of presence (PoPs). Avoid advertising the following prefixes, as they may unintentionally redirect traffic through SPA and disrupt FortiSASE routing behavior:
  - 0.0.0.0/0 (default route)
  - 0.0.0.0/1
  - 128.0.0.0/1
- FortiSASE security PoPs rely on their internal routing tables to handle internet-bound traffic from internal components. Advertising undesired prefixes to PoPs can result in traffic being misrouted through the SPA hub, resulting in connectivity issues.

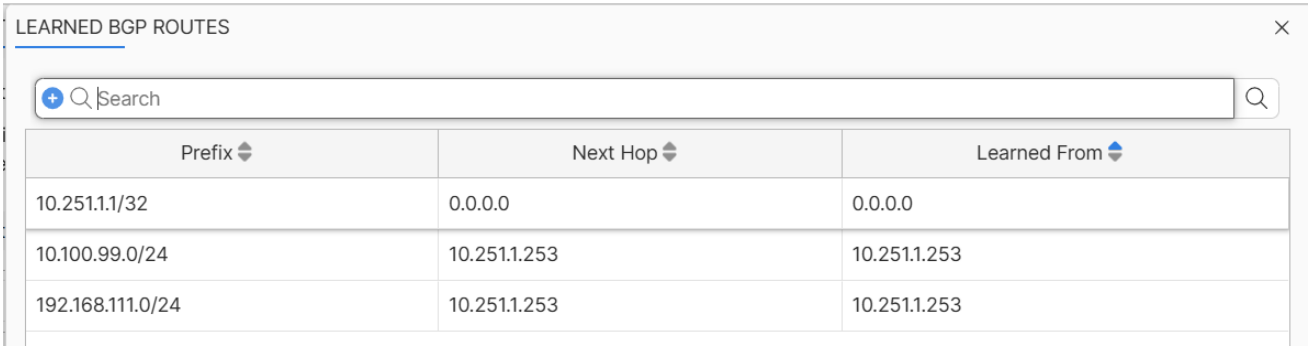
Viewing health and VPN tunnel status

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:



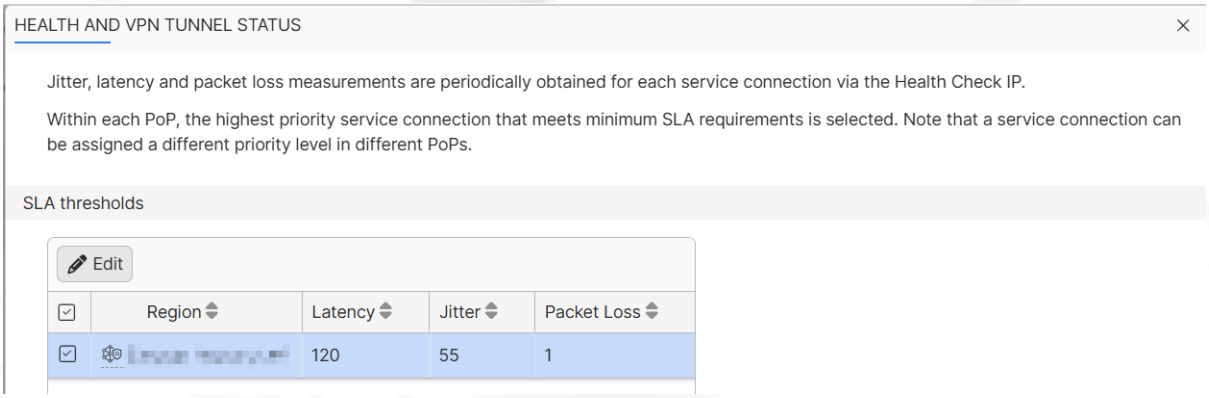
For any hub, selecting a point of presence and clicking *View Learned BGP Routes* displays the learned BGP routes for that hub. For example, the learned BGP routes for the example DC1 are as follows:



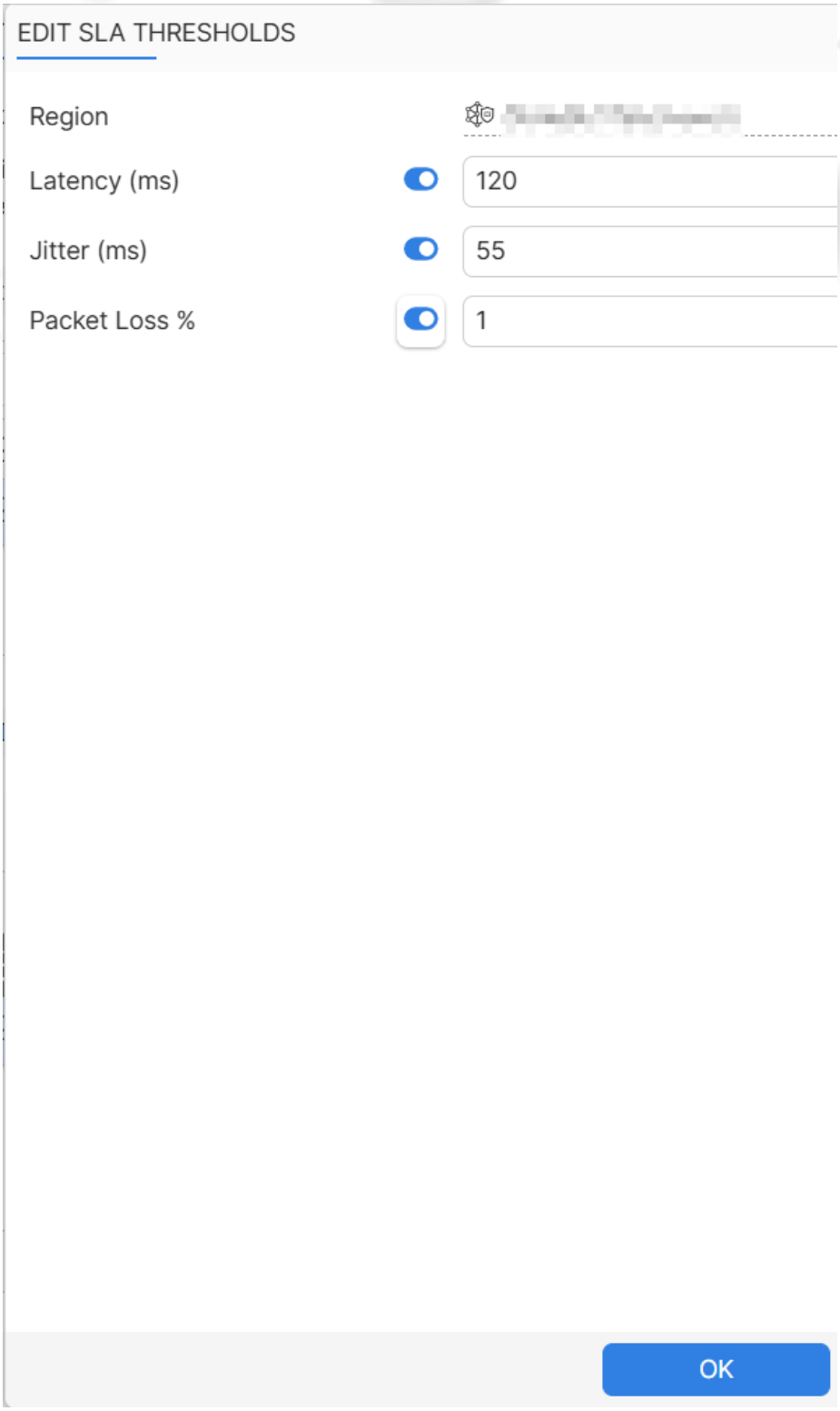
Editing SLA thresholds

You can customize latency, jitter, and packet loss SLA thresholds per security point of presence (PoP) used for secure private access hub SD-WAN health checks when *Hub Selection Method* is *Hub Health and Priority*. See Configuring network configuration on page 18.

SLA thresholds can be edited from *Network* > *Secure Private Access* by selecting a service connection and clicking *Health*, and then selecting a security PoP and clicking *Edit* to edit the SLA thresholds.



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

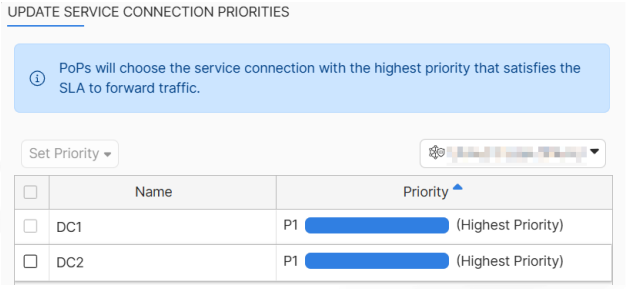


Updating service connection priorities

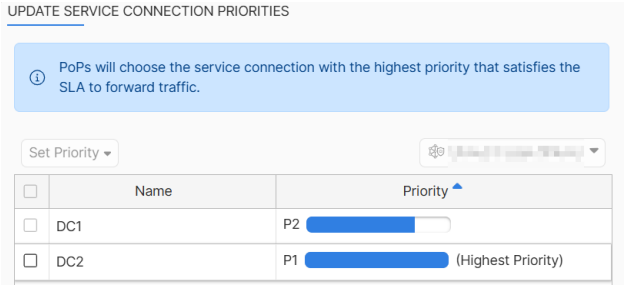
When you configure the hub selection method as hub health and priority within each point of presence (PoP), FortiSASE selects the highest priority hub that meets minimum SLA requirements. You can assign a hub a different priority level in different PoPs using the *Service Connection Priorities* page.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

To update hub priorities:

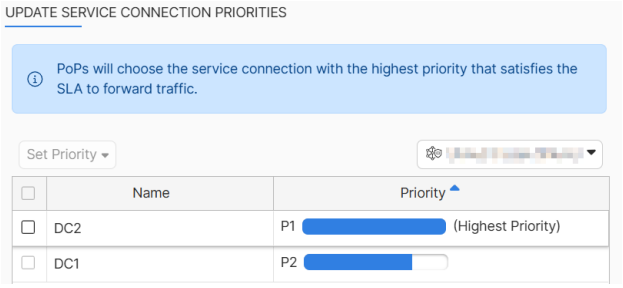
1. Go to *Network* > *Secure Private Access*. Click *Service Connection Priorities*.
2. From the *Security PoP* dropdown list, select the desired PoP hub.



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:



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



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

Deleting a hub configuration

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

To delete a hub configuration:

1. Go to *Network* > *Secure Private Access*.
2. Select the desired hub(s).
3. Click *Delete*.

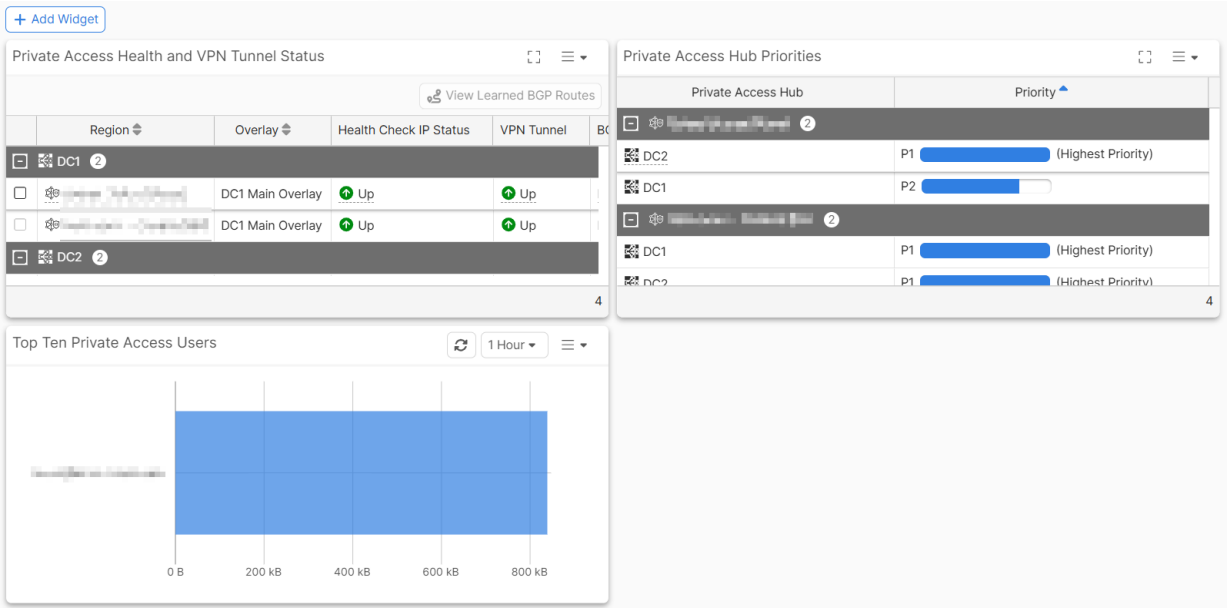
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

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:



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

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

For details on SPA server-to-client communication, see Configuring a private access policy for server-to-client traffic on page 33.

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

1. Go to *Configuration* > *Policies*.
2. Click the *Private Access* tab and then click the *To hubs* subtab.
3. Click *+Create* to create a new policy.

4. Configure these fields:

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

5. Click *OK*.

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

1. Go to *Configuration > SWG Policies*.
2. Click the *Private Access* tab and then click the *To hubs* subtab.
3. Click *+Create* to create a new policy.

4. Configure these fields:

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

5. Click *OK*.

Considerations

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

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

Secure private access (SPA) server-to-client communication allows traffic initiated from SPA hubs (or local networks behind SPA hubs) to remote users (currently VPN users only). This communication requires Remote VPN and edge device user identification and additional configuration steps on the FortiGate SPA hub itself. See Prerequisites and considerations on page 34.

For details on SPA client-to-server communication, see Configuring a private access policy for client-to-server traffic on page 30.

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

1. Go to *Configuration* > *Policies*.
2. Click the *Private Access* tab and then click the *From hubs* subtab.
3. Click *+Create* to create a new policy.
4. Configure these fields:

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

5. Click *OK*.

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

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

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

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

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

4. Click *OK*.

Prerequisites and considerations

Prerequisites

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

Considerations

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

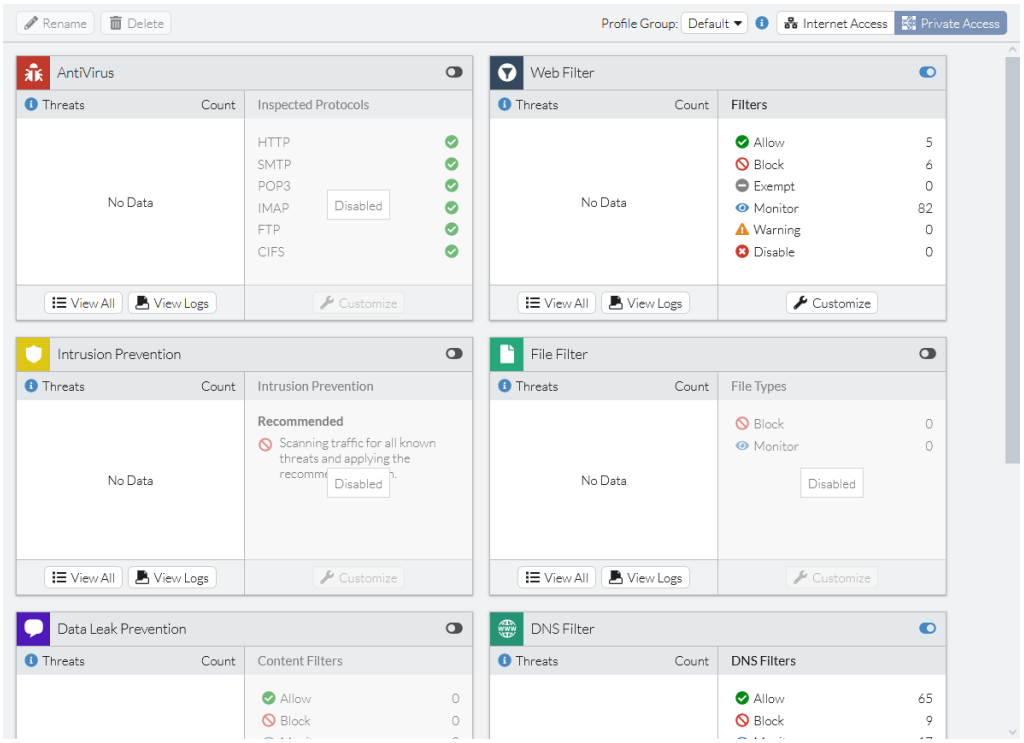
All allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device.

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

Configuring a private access security profile

To configure a private access security profile:

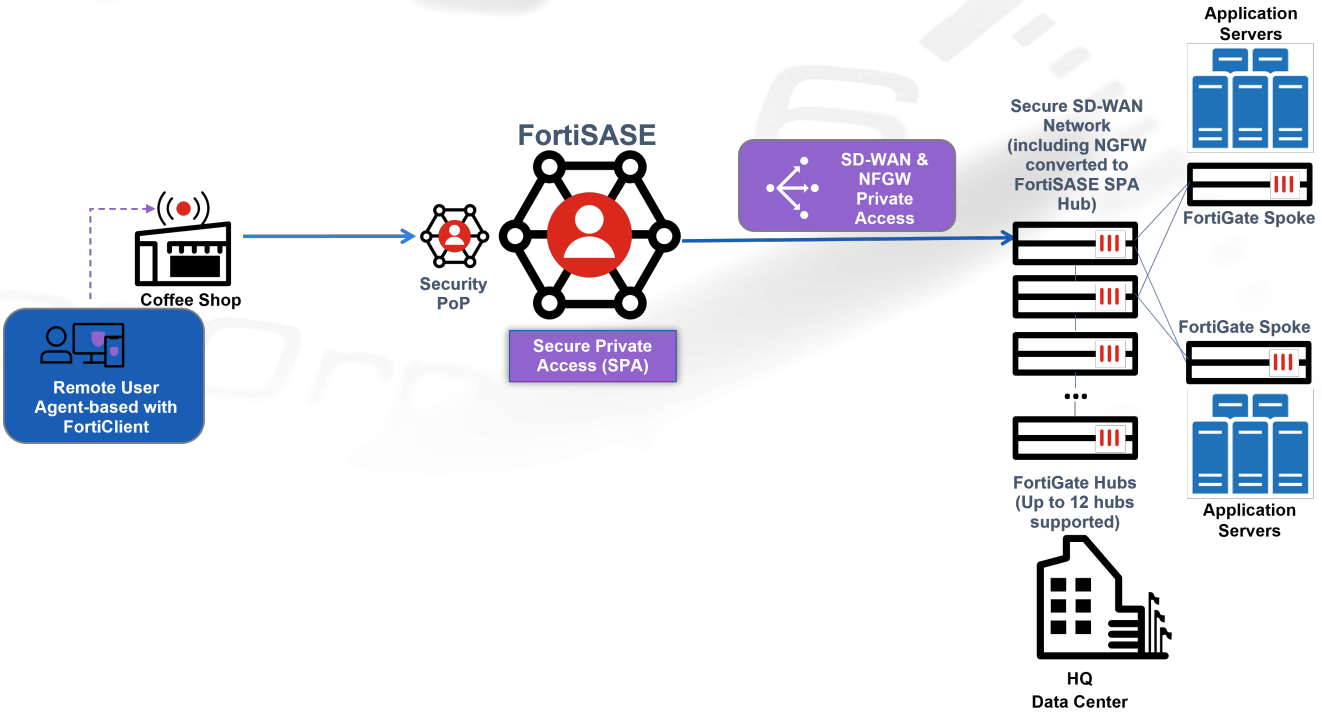
1. Go to *Configuration* > *Traffic* > *Security*.
2. In the top right corner, click *Private Access*.
3. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



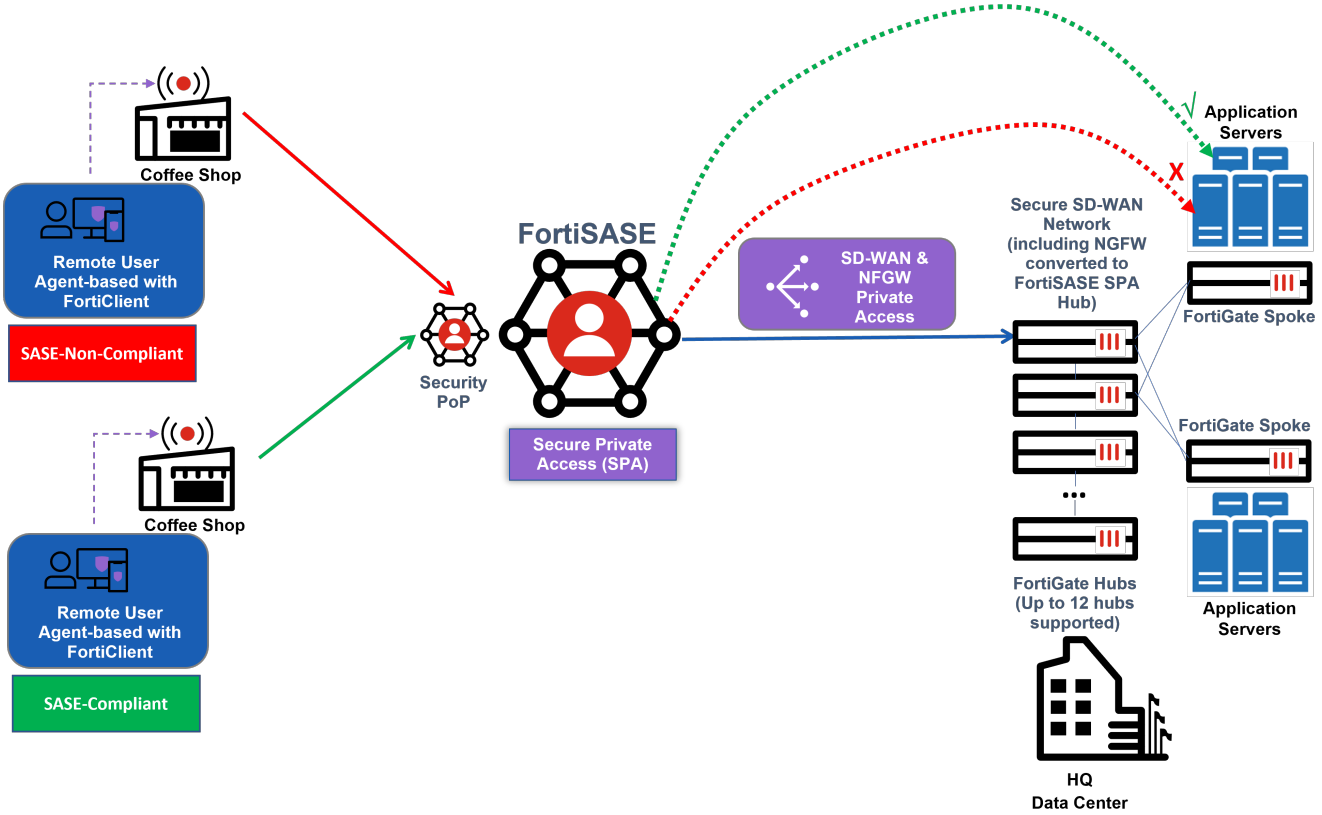
The security settings for Internet and private access are identical. For details on configuring security settings, see Security.

Configuring ZTNA tags in private access policies

By default, for the secure private access (SPA) use cases using a FortiGate hub configured through the *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.

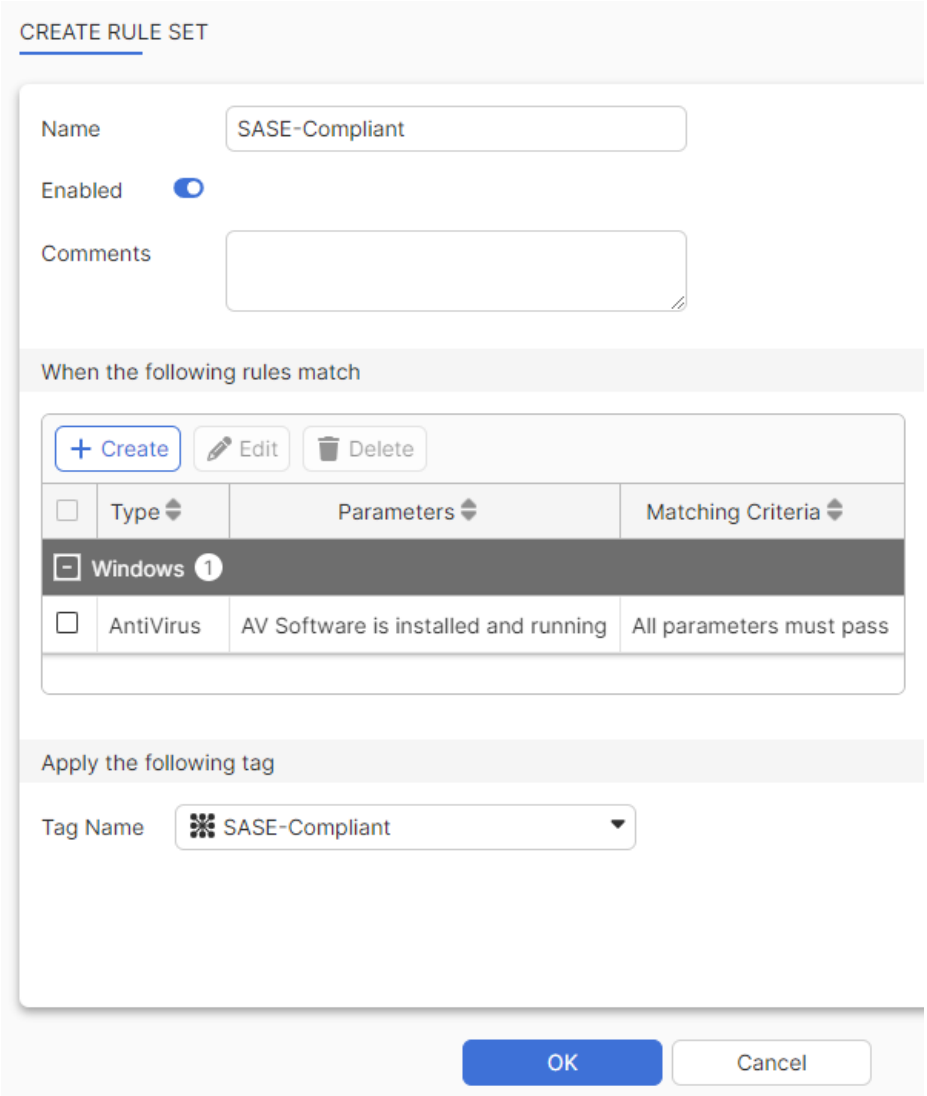
Configuring ZTNA rule sets to dynamically tag agent-based remote users

This example demonstrates how to configure zero trust network access (ZTNA) tag names and 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*.
2. In the *Tagging rules* tab, click *Create*.
3. In the *Name* field, enter the desired rule set name. For example, SASE-Compliant.
4. Toggle *Enabled* on or off to enable or disable the rule.
5. (Optional) In the *Comments* field, enter any desired comments.
6. Under *When the following rules match*, click *Create*.
7. Configure the rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   d. Click *OK*.
8. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
9. Click *OK* to select the new entry.
10. Click *OK*.



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

1. Go to *Configuration* > *ZTNA Tagging*.
2. In the *Tagging rules* tab, click *Create*.
3. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
4. Toggle *Enabled* on or off to enable or disable the rule.
5. (Optional) In the *Comments* field, enter any desired comments.
6. Under *When the following rules match*, click *Create*.
7. Configure the rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. Select *Negate*.
   d. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   e. Click *OK*.
8. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
9. Click *OK* to select the new entry.
10. Click *OK*.

Configuring dynamic private access policies using ZTNA tags

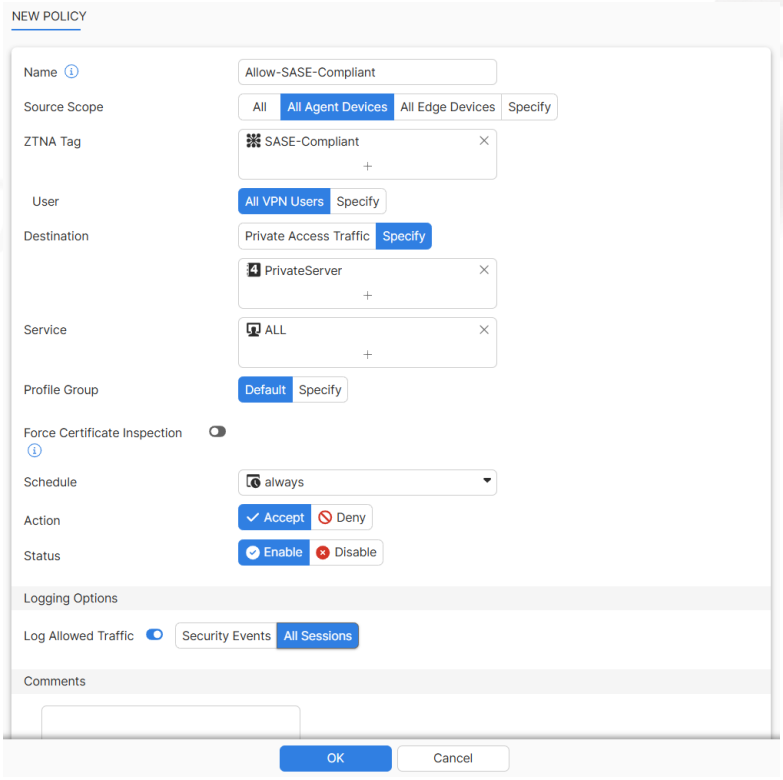
This example demonstrates how to configure dynamic private access policies using the zero trust network access (ZTNA) tags that you created in Configuring ZTNA rule sets to dynamically tag agent-based remote users on page 37 to allow endpoints tagged as SASE-Compliant with access to selected private 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. Click the *To hubs* subtab (selected by default).
3. Click *+Create*.
4. Configure the policy:
   a. For *Name*, enter Allow-SASE-Compliant.
   b. For *Source Scope*, select *All Agent Devices*.
   c. In the *ZTNA Tag* field, click *+*.
      i. From the *Select Entries* panel, under *ZTNA Tag* > *Private Access*, select the *SASE-Compliant* tag.
      ii. For *User*, select *All VPN Users*.
   d. For *Destination*, select *Specify*, click *+*, and in the *Select Entries* panel click *+Create* and click *IPv4 Host* to a create a new host for the specific server as follows:
      i. For *Location*, select *Private Access Hub*.
      ii. For *Category*, *IPv4 Host* is selected.
      iii. In the *Name* field, enter the desired name. In this example, the name is PrivateServer.
      iv. From the *Type* dropdown list, select *Subnet*.
      v. In the *IP/Netmask* field, enter 10.100.99.101/32.
      vi. Click *OK*.
      Select the newly created host to set it as the *Destination*.
   e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.

f. For *Action*, select *Accept*.
g. For *Status*, select *Enable*.

5. Click *OK*.

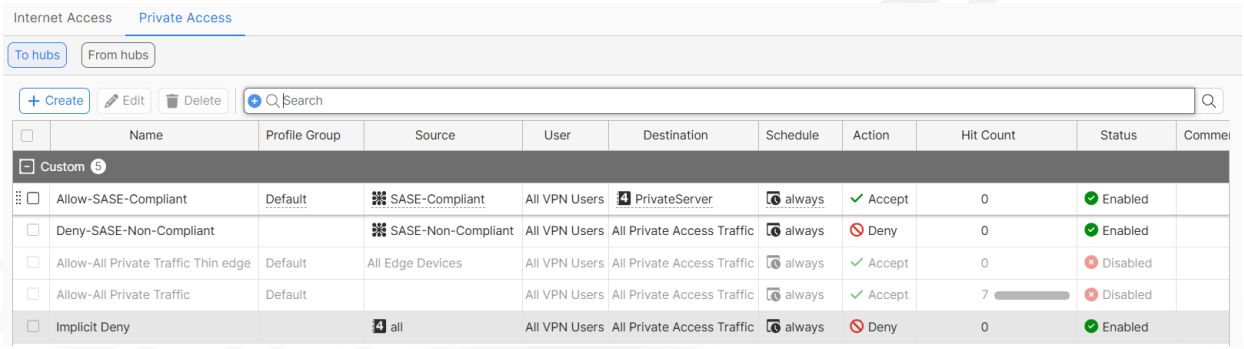


6. In *Configuration* > *Policies* with *Secure Private Access* selected, ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific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

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

1. Go to *Configuration* > *Policies*.
2. Select *Private Access* to display the list of private access policies. Click the *To hubs* subtab (selected by default).
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Deny-SASE-Non-Compliant.
   b. For *Source Scope*, select *All Agent Devices*.
   c. In the *ZTNA Tag* field, click *+*.
      i. 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 *Secure Private Access* selected, do the following:
   a. 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.

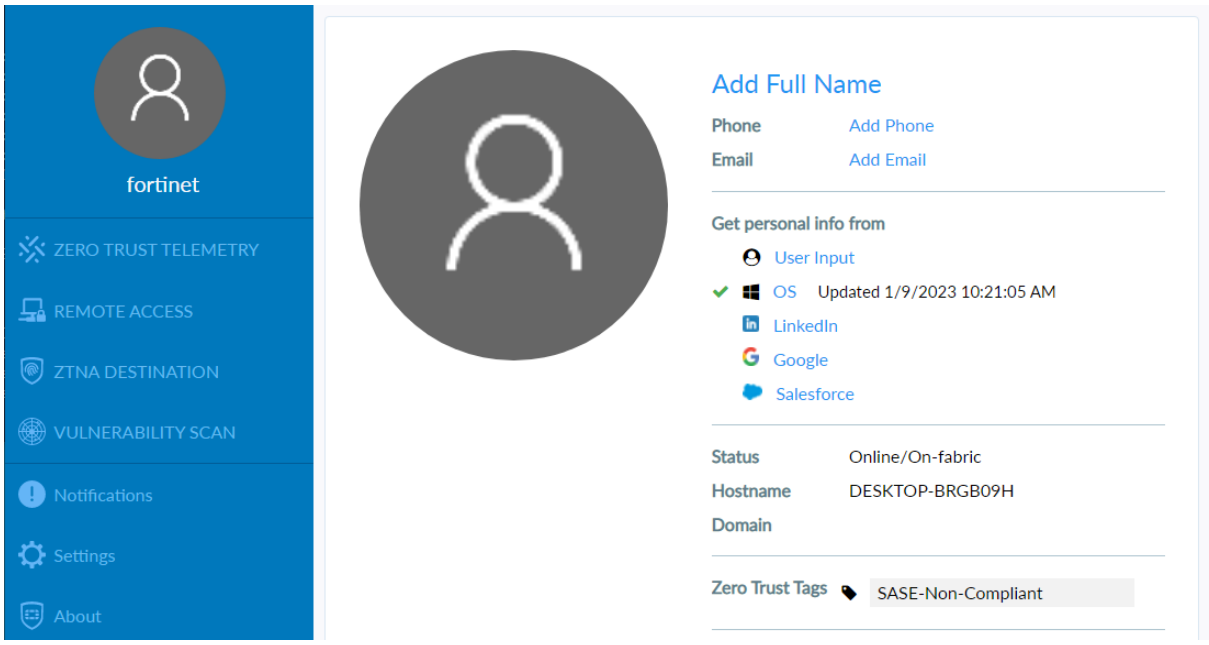
b. Disable the *Allow-All Private Traffic* and *Allow-All Private Traffic Thin edge* policies.



Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

1. In FortiSASE, go to *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.



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*.
4. In the Windows start menu, click the gear icon for *Settings*. Go to *Update & Security* > *Windows Security* > *Virus & threat protection*.
5. Ensure in *Virus & threat protection settings* > *Manage settings* that *Real-time protection* is enabled (by default). This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.
6. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant Zero Trust tag applied.
7. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.

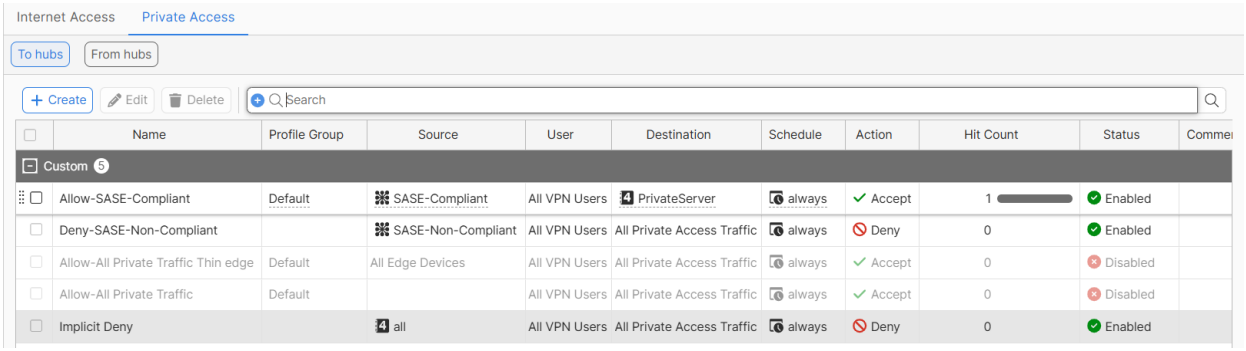
8. Observe the following output indicating the ping succeeded since FortiSASE allows access:

```
C:\> ping 10.100.99.101

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

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

9. In FortiSASE, in *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.



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

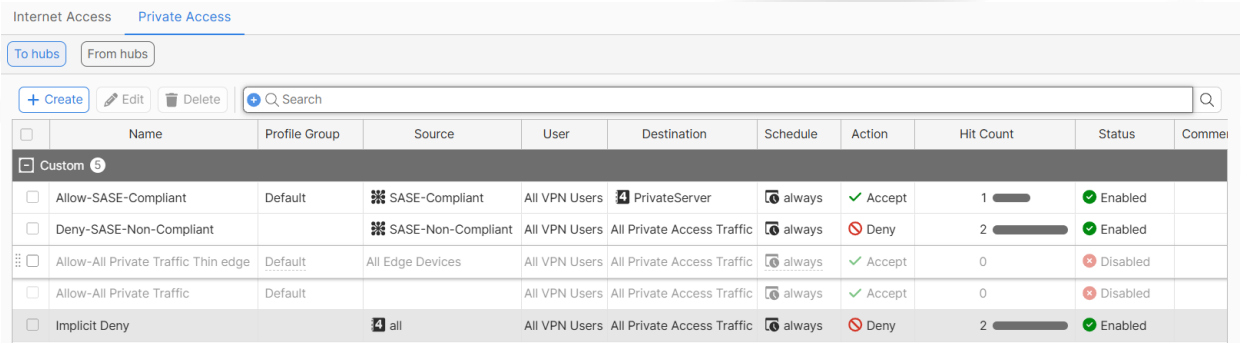
1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.
4. In the Windows start menu, click the gear icon for *Settings*. Go to *Update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

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

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

9. In FortiSASE, in *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 *DNS Server* in FortiSASE under *Configuration* > *DNS* to resolve hostnames for internal and external domains.

- Implicit DNS rules have been predefined for VPN users and for secure web gateway (SWG) and Thin-Edge users. These are used for resolving hostnames for external domains.
- You can create split DNS rules by clicking *Create*. These are used for resolving hostnames for internal domains. See Split DNS Rules on page 45.

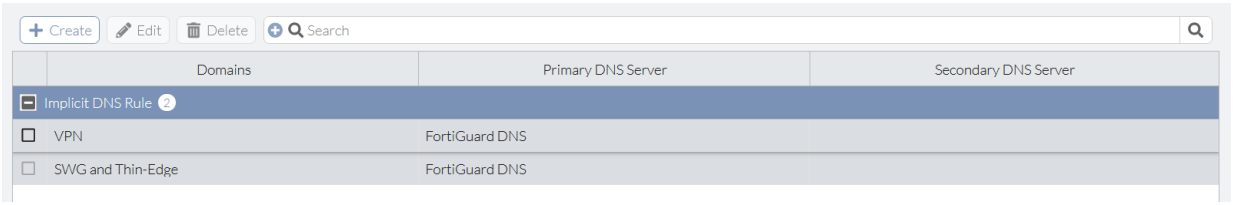
FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

Ensure that your FortiSASE remote users have access to the internal DNS server, internal RADIUS server, or internal LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy in the FortiSASE Administration Guide.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed in the FortiSASE Administration Guide.



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

FortiGuard DNS servers do not support DNS over TCP. If you require DNS over TCP, edit implicit DNS rules from the default FortiGuard DNS server to other DNS servers that support DNS over TCP.

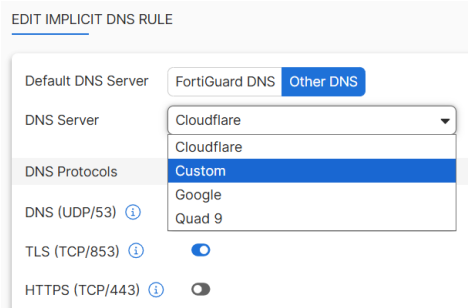
You can configure *Default DNS Server* with one of the following options, then click *OK* to save the change:

DNS Server		Description	Primary and secondary DNS server IP address
FortiGuard DNS		Use FortiGuard DNS	• 96.45.45.45 • 96.45.46.46
Use endpoints' system DNS		Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS		Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
	CloudFlare	Use the Cloudflare public DNS server	• 1.1.1.1 • 1.0.0.1
	Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify primary and secondary DNS IP address
	Google	Use the Google public DNS server	• 8.8.8.8 • 8.8.4.4
	Quad 9	Use the Quad 9 public DNS server	• 9.9.9.9 • 149.112.112.112

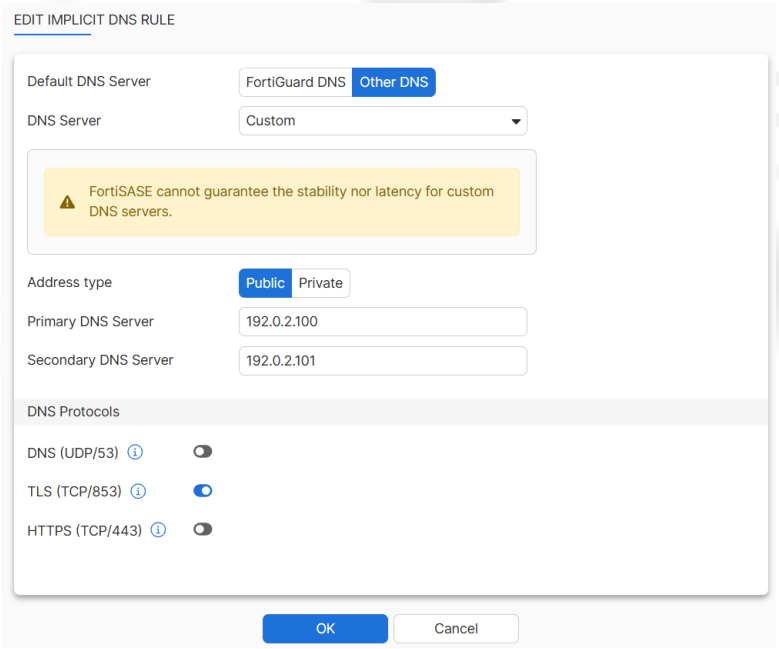
For example, you can edit the VPN implicit DNS rule to use a custom DNS server as follows:

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



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



5. Click *OK*.

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

Ensure that your FortiSASE remote users have access to the RADIUS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy in the FortiSASE Administration Guide.

Split DNS Rules

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

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

To support these scenarios, you can configure FortiSASE DNS settings for 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). If you have multiple internal DNS servers in different geographical locations, you can configure remote users to use the internal DNS server that is closest to their region using *PoP DNS override*, which enhances the DNS response time.
- Resolve all other hostnames for external domains using the implicit DNS rule.

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

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

Ensure that your FortiSASE remote users have access to the internal DNS server, internal RADIUS server, or internal LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy in the FortiSASE Administration Guide.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed in the FortiSASE Administration Guide.

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, you must enable SSL deep inspection for agent-based remote users on FortiSASE.

Prerequisites

SSL deep inspection

Split DNS requires enabling SSL deep inspection on FortiSASE so that FortiSASE can intercept the DNS traffic.

- To confirm that you enabled SSL deep inspection, go to *Configuration* > *Security* and at the top of the security profile group page, in the *SSL Inspection* section, confirm that it displays *SSL inspection: Deep inspection mode*.
- To enable SSL deep inspection, go to *Configuration* > *Security* and at the top of the security profile group page, in the *SSL Inspection* section, click *Configure SSL*. In the *SSL Inspection* pane, select *Deep inspection* and click *OK*.

See Certificate and deep inspection modes.

Install FortiSASE CA Certificate for Agentless and Site-based Edge Device Users

With deep inspection enabled, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing Certificate Authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

FortiSASE supports automatically installing the FortiSASE CA certificate for agent-based users with FortiClient installed on their endpoints.

The FortiSASE CA certificate must be manually installed on endpoints for agentless SWG users and site-based edge device users.

- For agentless SWG users, installing this CA certificate is already part of the SWG onboarding process.
- For endpoints using a site-based edge device, installing this CA certificate is an additional step that must be performed.

See Installing a certificate for deep inspection mode for installing the FortiSASE CA certificate.

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.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

Ensure that your FortiSASE remote users have access to the internal DNS server, internal RADIUS server, or internal LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy in the FortiSASE Administration Guide.

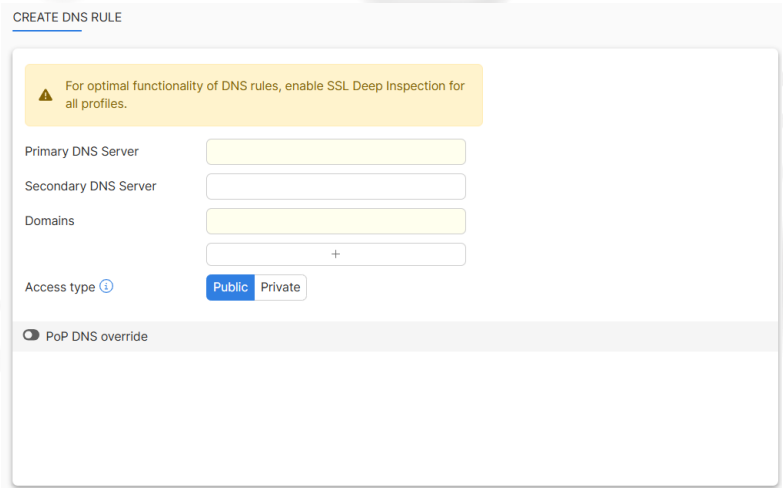
When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed in the FortiSASE Administration Guide.

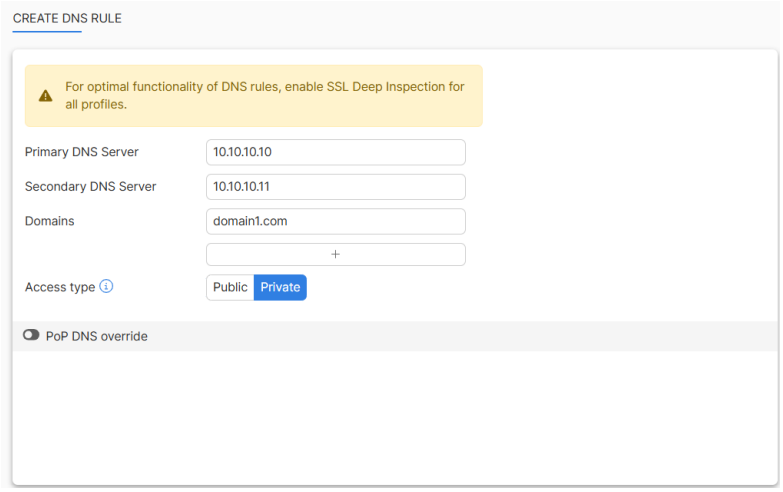
Configuring Split DNS Rules

To configure Split DNS Rules:

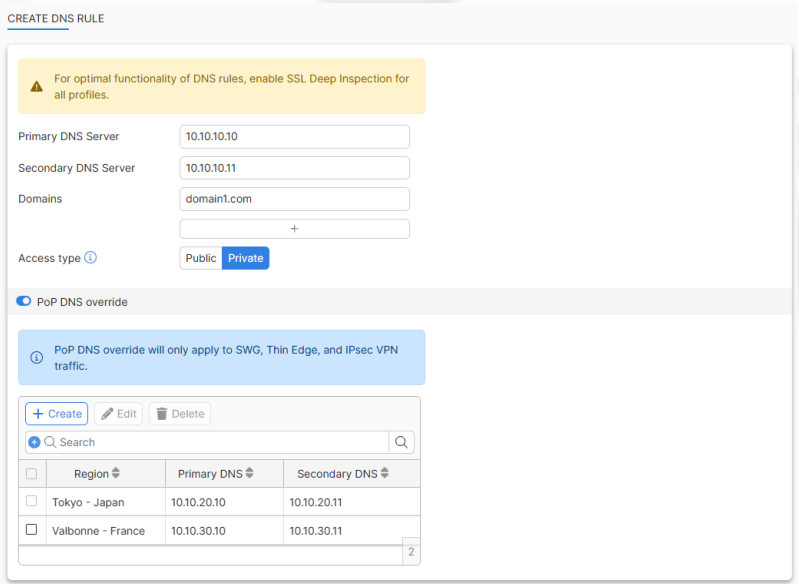
1. Go to *Configuration* > *DNS*.
2. Click *Create*.



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



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

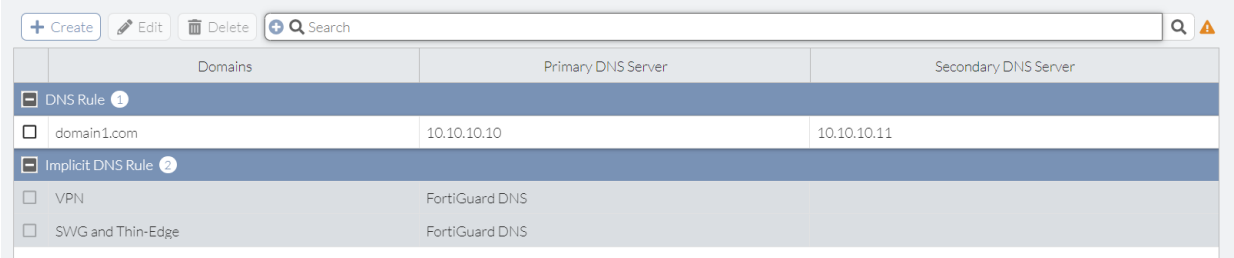


Only two internal DNS servers are configurable per-region for each domain. If the region does not appear in the list of PoP locations to use, the remote endpoint users uses the main *Primary* and/or *Secondary DNS Server* i.e. 10.10.10.10 and 10.10.10.11 to resolve the domain.

e. Click *OK* to save the split DNS rule.

> PoP DNS override will only apply to SWG, Thin Edge (edge device), and IPsec VPN traffic.

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



> 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.

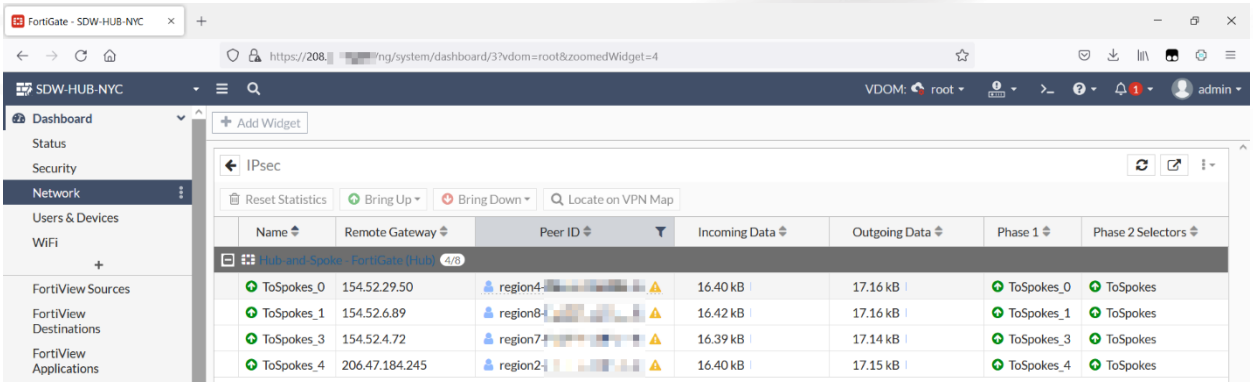
> If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.

> Ensure that your FortiSASE remote users have access to the RADIUS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy in the FortiSASE Administration Guide.

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/recv: 1/2
 lifetime/rekey: 86400/85206
 DPD sent/recv: 00000001/00000001
 peer-id: region8-fos001-tiui7pzu-1
```

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

3. 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:

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

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

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

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

C:\>ping 10.50.101.50

Pinging 10.50.101.50 with 32 bytes of data:

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

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

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

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

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

This example requires *System > SWG Configuration* and *Configuration > SWG User SSO* to be configured appropriately. See SWG client onboarding and Configuring FortiSASE with Entra ID SSO in SWG agentless mode.

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

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

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

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

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

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

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

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

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

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

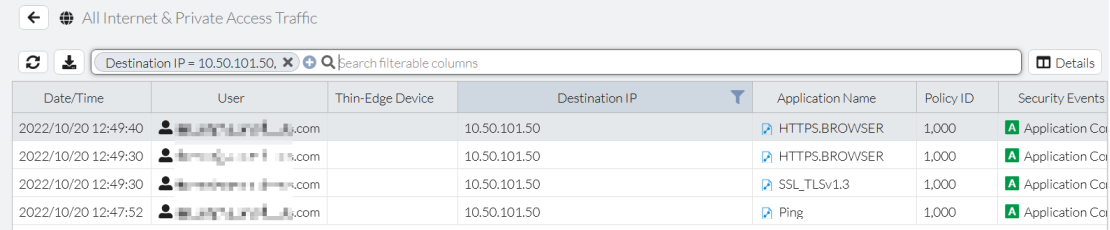
```
root@internal-server-01:~# ping 100.65.0.1
PING 100.65.0.1 (100.65.0.1) 56(84) bytes of data.
64 bytes from 100.65.0.1: icmp_seq=1 ttl=126 time=73.3 ms
64 bytes from 100.65.0.1: icmp_seq=2 ttl=126 time=72.5 ms
64 bytes from 100.65.0.1: icmp_seq=3 ttl=126 time=74.0 ms
64 bytes from 100.65.0.1: icmp_seq=4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

Verifying private access traffic in FortiSASE portal

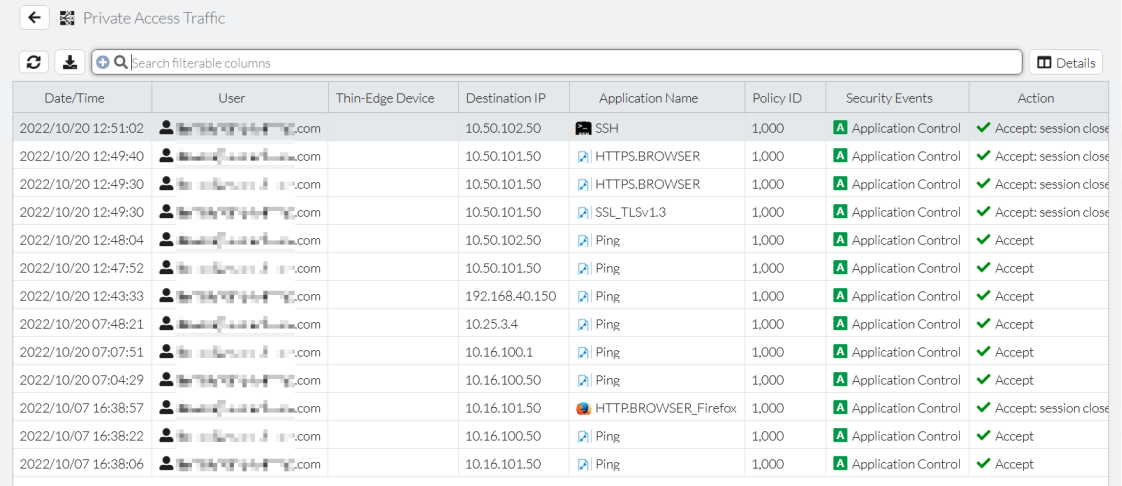
In the FortiSASE portal, you can verify traffic from FortiSASE remote users has reached private access destinations through these methods:

- 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

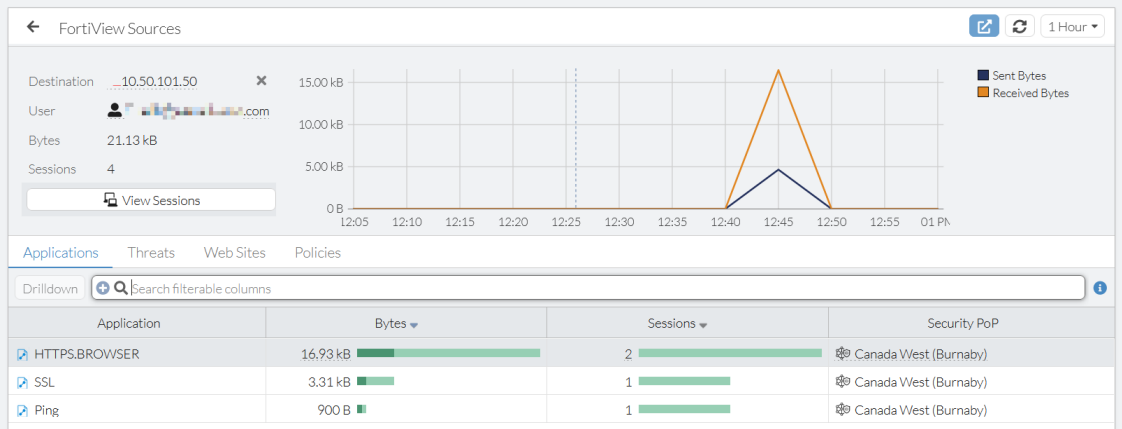
Following is an example of the *Analytics* > *Logs* > *Traffic* > *All Internet and Private Access Traffic* page, filtered for the private access destination IP address 10.50.101.50.

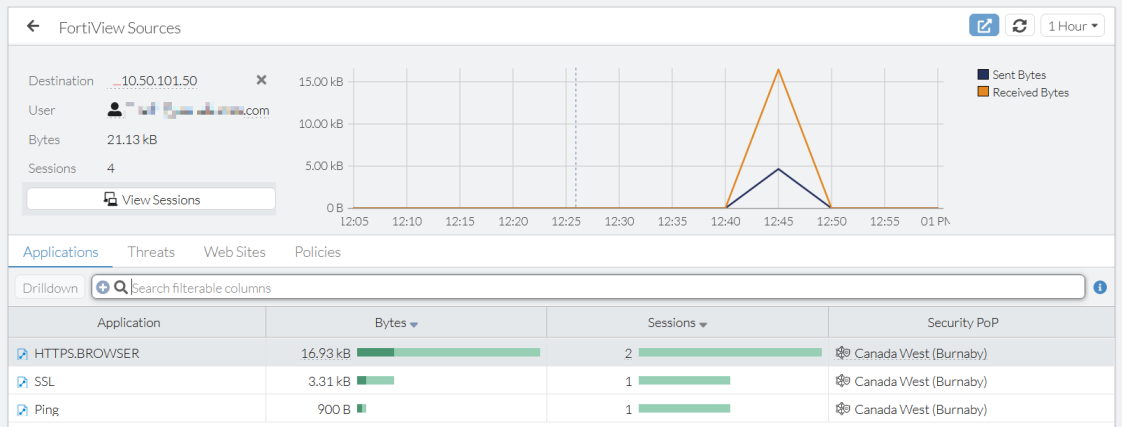


Following is an example of the *Analytics* > *Logs* > *Traffic* > *Private Access Traffic* page.



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 traffic from hubs

Verifying private access traffic from SPA hubs to FortiSASE remote users depends on a private access policy being defined in the *From Hub* direction on a FortiSASE instance with the remote VPN user identification selected availability feature. See Remote VPN user identification.

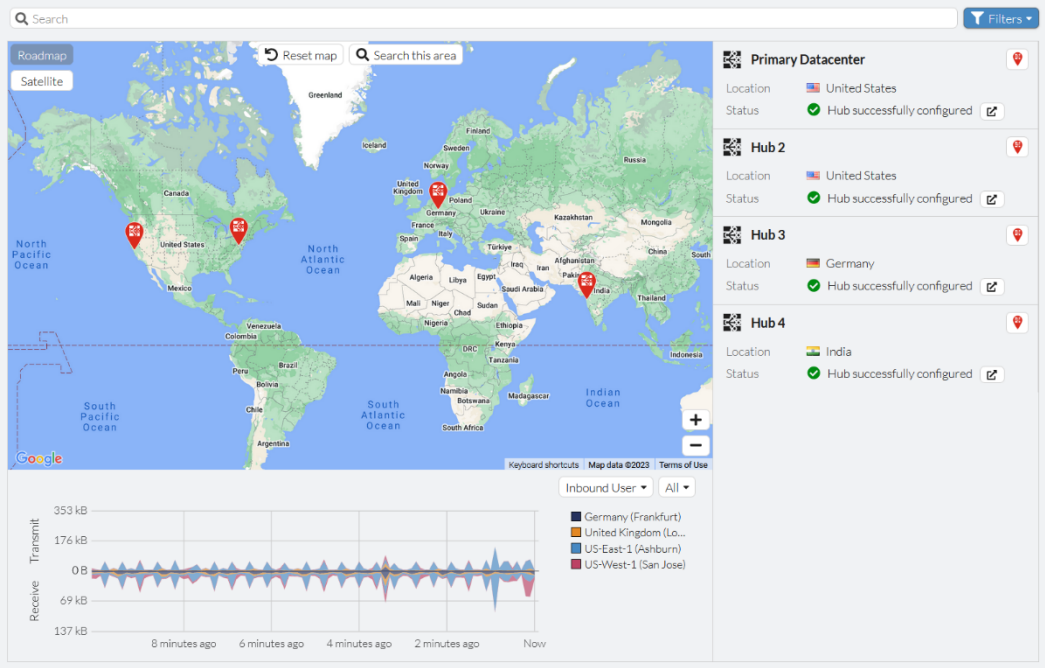
In the FortiSASE portal, you can verify traffic from SPA hub sources (local networks or connected spokes) has reached FortiSASE remote user destinations through these methods:

- From *Analytics* > *Logs* > *Traffic* by viewing *All Internet and Private Access Traffic* or *Private Access Traffic (From Hubs)*
- From *Dashboard* > *FortiView* > *Sources*, *Dashboard* > *FortiView* > *Destinations*, or *Dashboard* > *FortiView* > *Policies* and filtering on the remote VPN user destination IP address

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.



Restricting access using a FortiGate SPA hub/spoke policy

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

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

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

To restrict access using a FortiGate SPA device firewall policy:

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

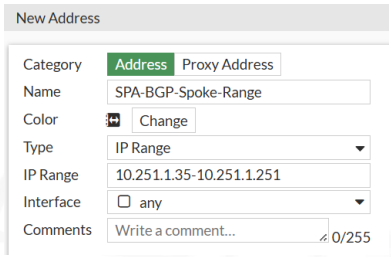
```
show vpn ipsec phase1-interface | grep ipv4-
```

Example output:

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

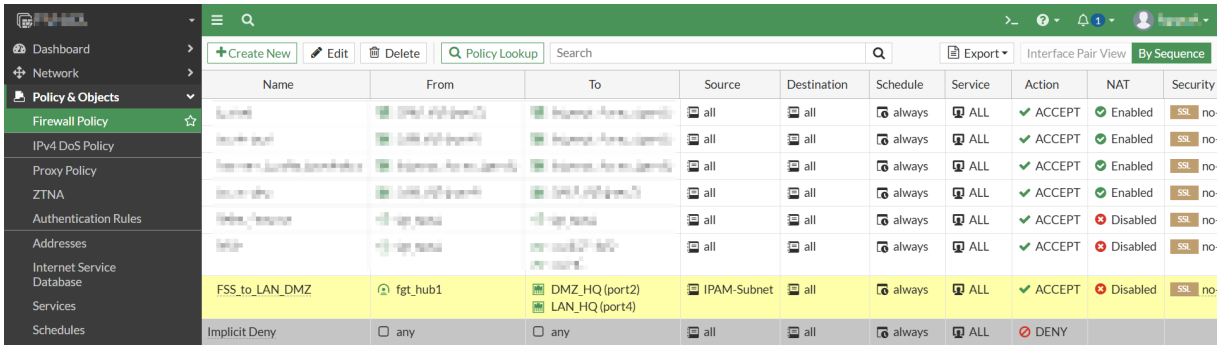
In the above example, the IKEv2 mode configuration address range is from 10.251.1.35-10.251.1.251.

2. On the FortiGate SPA hub or spoke device, configure a firewall address object for the BGP router ID subnet and use it in the firewall policy used to restrict access to the HTTPS private server:
   a. In *Policy & Objects* > *Addresses*, click *Create New* > *Address*. Create a new address object containing the IP range from the SPA hub.



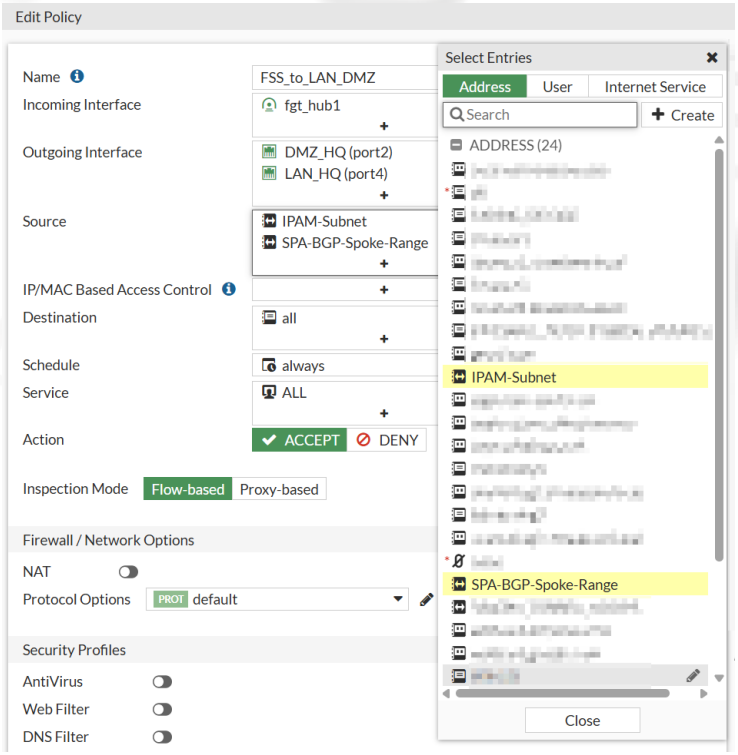
   In this example, an IP range address object named SPA-BGP-Spoke-Range is created for 10.251.1.35-10.251.1.251.

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

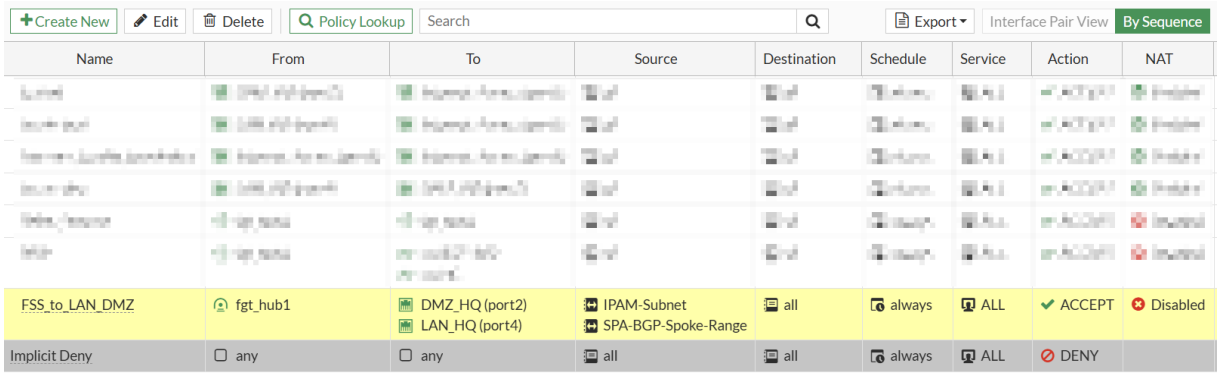


   In this example, the firewall policy of interest is the FSS_to_LAN_DMZ policy from IPsec overlay interface fgt_hub1 to DMZ_HQ (port2) and LAN_HQ (port4) LAN interfaces with source set to IPAM-Subnet to allow VPN users to access private resources.

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



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



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

More information

Appendix A: Products used in this guide

This deployment document was tested with a particular FortiSASE version and particular firmware versions of associated Fortinet products. The features in this deployment guide may have been updated since this document was originally published. For the latest details about features included in this guide, please refer to the FortiSASE 7.2 Administration Guide.

Product	Model	Firmware
FortiSASE	N/A	26.1.92 (26.1.2 v7.2)
FortiOS	N/A	v7.6.6

www.fortinet.com

72-261-1001698-20260617