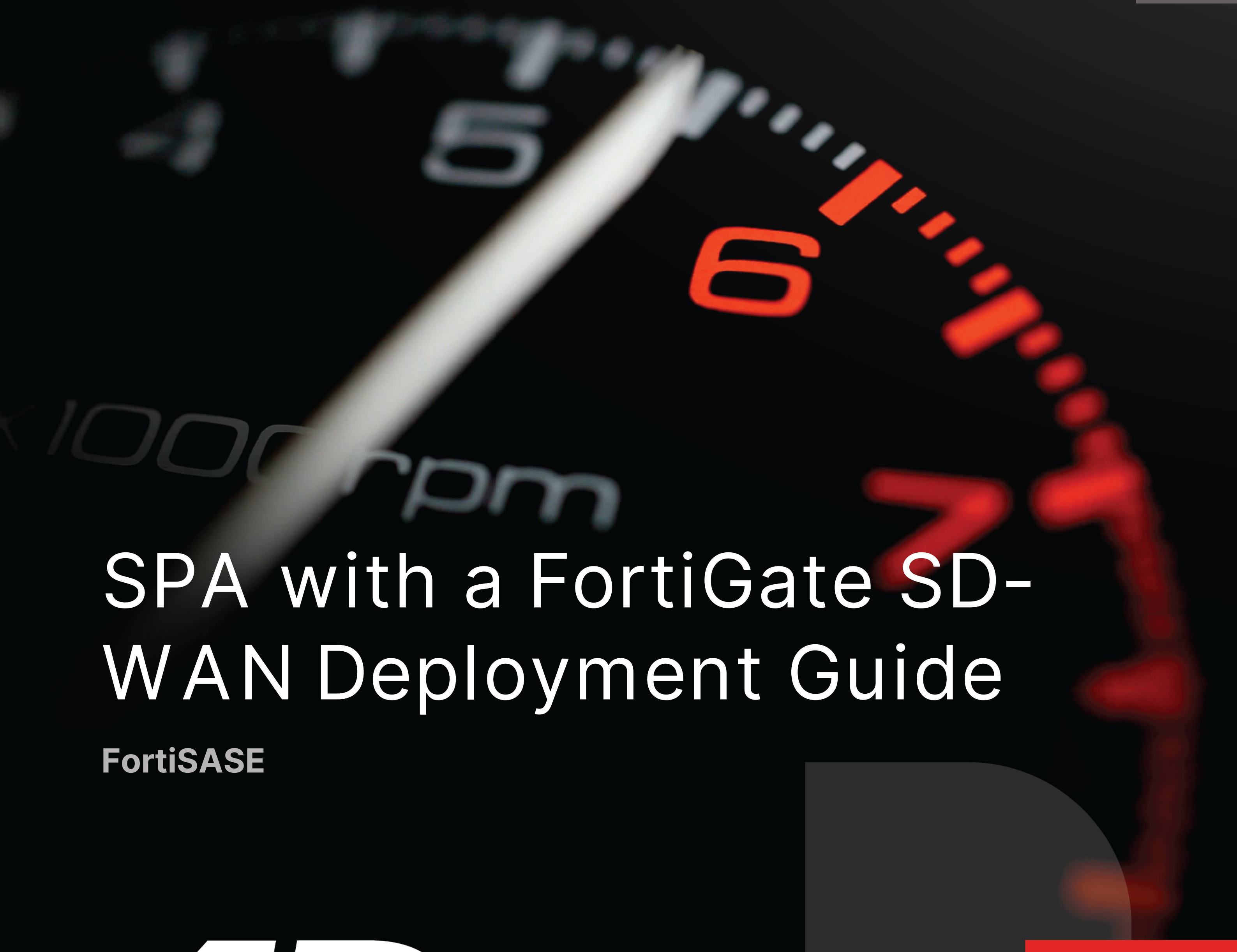


SPA with a FortiGate SD-WAN Deployment Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change log **4**

Deployment overview **5**

Intended audience **8**

About this guide **8**

Design concept and considerations **8**

FortiGate SD-WAN network topology **8**

Network restrictions **10**

Product prerequisites **10**

Deployment plan **10**

Deployment procedures **12**

Provisioning your FortiSASE instance **12**

Configuring a new FortiGate SD-WAN enterprise deployment using FortiManager **12**

Reviewing configuration settings of an existing FortiGate SD-WAN hub deployment previously configured using FortiManager **13**

IPsec VPN configuration **13**

Tunnel interface configuration **15**

BGP configuration **15**

Firewall policy configuration **16**

Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access **17**

Configuration workflow **17**

Configuring network configuration **17**

Configuring a new service connection **20**

Viewing health and VPN tunnel status **24**

Updating service connection priorities **25**

Deleting a hub configuration **26**

Monitoring private access hubs **26**

Verifying private access policy configuration **26**

Configuring a private access security profile **27**

Configuring ZTNA tags in private access policies **27**

Configuring DNS Settings **35**

Split DNS Rules **36**

Verifying IPsec VPN tunnels on the FortiGate hub 40
Verifying BGP routing on the FortiGate hub 41
Testing private access connectivity to FortiGate hub network from remote users 42
Verifying private access traffic in FortiSASE portal 42
Verifying private access hub status and location using the asset map 44
More information 45
Appendix A: Products used in this guide 45
Appendix B: Documentation references 45
Feature documentation 45
4-D resources: SASE 45

Change log

Date	Change description
2024-02-12	Initial release.
2024-02-13	Updated Deployment overview on page 5.
2024-03-07	Updated: • Configuring DNS Settings on page 35 • Split DNS Rules on page 36

Deployment overview

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

Scenarios involving a FortiGate next generation firewall (NGFW) converted to a FortiSASE secure private access (SPA) hub or involving a FortiGate SD-WAN hub are use cases that allow broader and seamless access to both privately hosted TCP- and UDP-based applications.

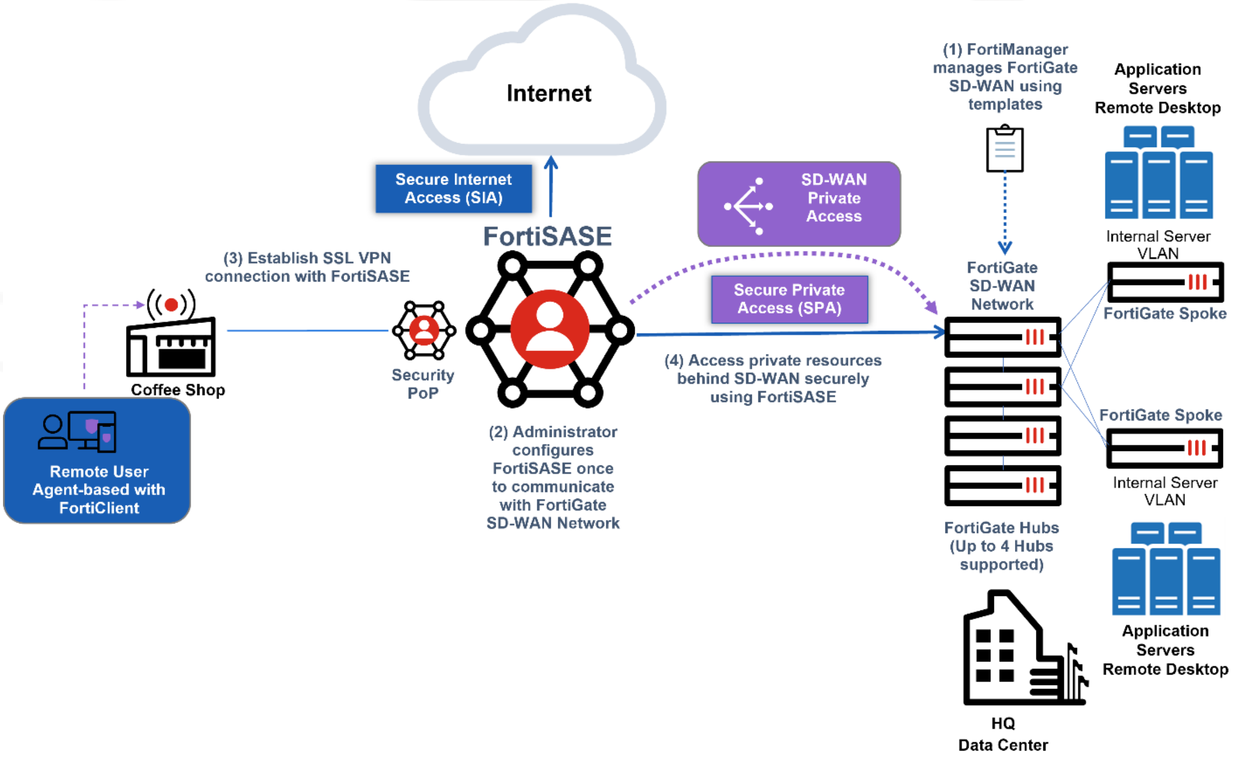
For the FortiGate SD-WAN SPA use case, you must configure a new FortiGate SD-WAN deployment or have an existing FortiGate SD-WAN deployment already configured. You then configure FortiSASE to communicate with the FortiGate SD-WAN hub. After completing this configuration, the FortiSASE security points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

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

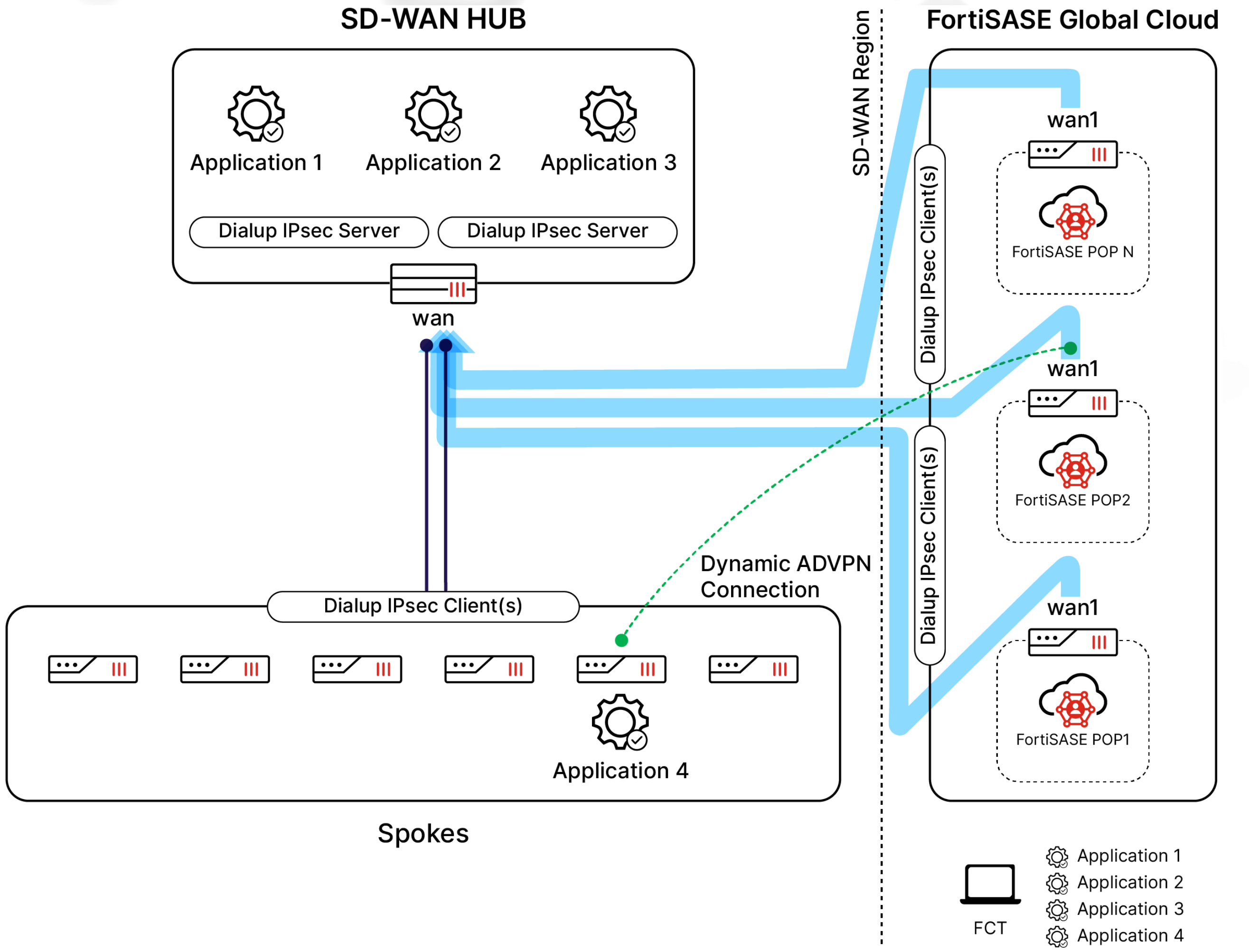
- SD-WAN with a single datacenter/hub
- SD-WAN with dual datacenters/hubs
- SD-WAN with up to four datacenters/hubs

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

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


Internet
Secure Internet Access (SIA)
FortiSASE
SD-WAN Private Access
Secure Private Access (SPA)
(1) FortiManager manages FortiGate SD-WAN using templates
Application Servers Remote Desktop
Internal Server VLAN
FortiGate SD-WAN Network
FortiGate Spoke
(3) Establish SSL VPN connection with FortiSASE
Coffee Shop
Security PoP
(4) Access private resources behind SD-WAN securely using FortiSASE
Remote User Agent-based with FortiClient
(2) Administrator configures FortiSASE once to communicate with FortiGate SD-WAN Network
FortiGate Spoke
Internal Server VLAN
FortiGate Hubs (Up to 4 Hubs supported)
Application Servers Remote Desktop
HQ Data Center

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 remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel. Therefore, the SPA use cases with FortiGate hubs only allow traffic to be initiated from FortiSASE spokes to FortiGate spokes.

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

This deployment guide describes how to configure FortiSASE PoPs to act as spokes with a new or existing FortiGate SD-WAN hub-and-spoke network deployment. This guide covers the cases when the newly deployed or existing FortiGate SD-WAN network is managed using FortiManager according to Fortinet's SD-WAN best practices. After performing subsequent FortiSASE configuration steps, FortiSASE remote users can privately access internal networks behind these deployments.

For the FortiGate NGFW SPA use case, you must first convert the NGFW to a standalone IPsec VPN hub. For deployment details for this use case, see the 4-D FortiGate NGFW to FortiSASE SPA Hub Conversion Deployment Guide (FortiOS 7.0.7+) instead of this guide.

For the FortiGate NGFW SPA use case running FortiOS 7.2.4 and above, you can use the Fabric Overlay Orchestrator feature to convert the NGFW to a standalone IPsec VPN hub. For deployment details, see the 4-D FortiGate NGFW to FortiSASE SPA Hub Conversion using Fabric Overlay Orchestrator Deployment Guide (FortiOS 7.2.4+, 7.4.0+).

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

Intended audience

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

For comments and feedback about this document, visit the FortiSASE Integration with Existing SD-WAN Hub Deployment on community.fortinet.com.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture for the FortiSASE SPA use case using a new or existing FortiGate SD-WAN network.

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

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

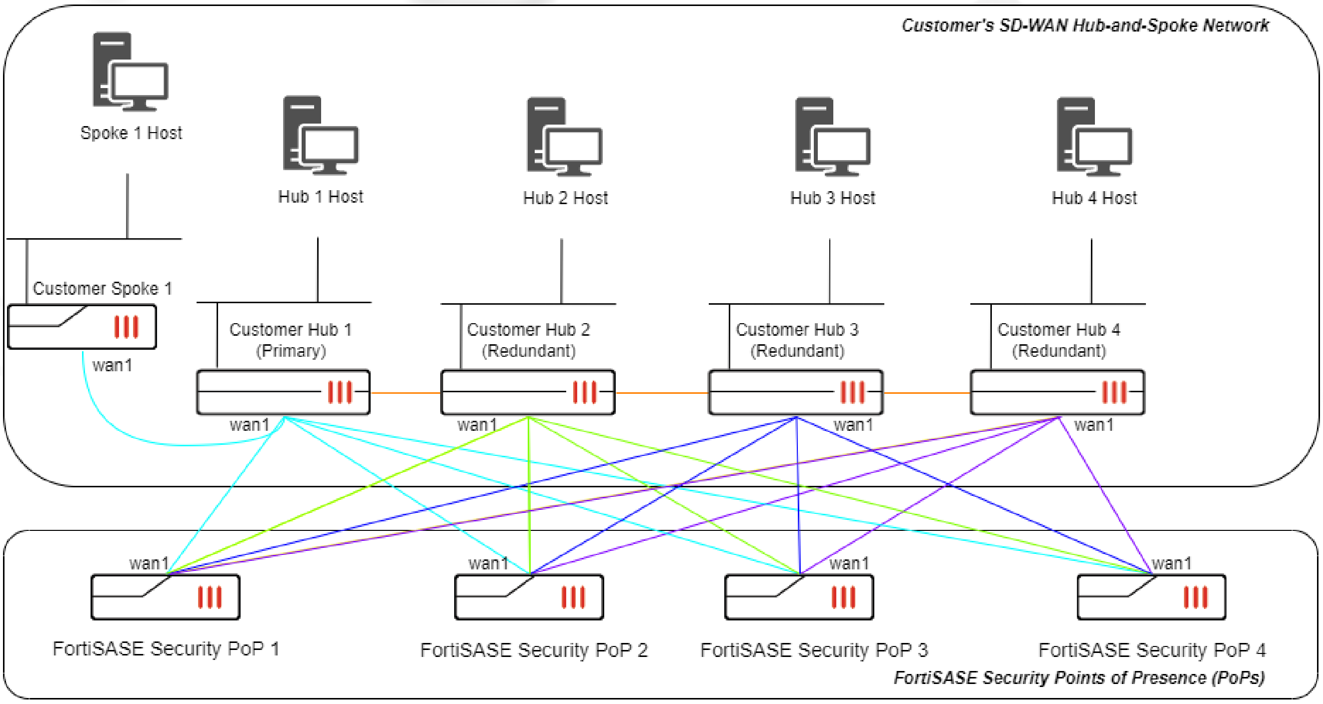
Design concept and considerations

FortiGate SD-WAN network topology

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

- SD-WAN with a single datacenter/hub
- SD-WAN with dual datacenters/hubs
- SD-WAN with up to four datacenters/hubs

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



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

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

The following table maps the aforementioned settings configured by FortiManager with the settings that you configure in FortiSASE using the *Secure Private Access* page:

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

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

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

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

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

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

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

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

Network restrictions

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

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

Product prerequisites

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

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

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 12 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Ensure the FortiGate SD-WAN deployment has the proper configuration:
   a. Configure a new FortiGate SD-WAN deployment using FortiManager.
   b. Review and modify the configuration settings of an existing FortiGate SD-WAN deployment using FortiManager.

3. Using the FortiSASE *Secure Private Access* page, configure the FortiSASE security points of presence as spokes of the FortiGate SD-WAN Hub using its specific network attributes as parameters.
4. Configure the DNS settings to allow resolving hostnames for external and internal domains.
5. Verify IPsec VPN tunnels on the FortiGate SD-WAN hub(s).
6. Verify BGP routing on the FortiGate SD-WAN hub(s).
7. Test private access connectivity to the FortiGate SD-WAN network from remote users.

Deployment procedures

Provisioning your FortiSASE instance

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

To provision your FortiSASE instance:

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

Configuring a new FortiGate SD-WAN enterprise deployment using FortiManager

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

SD-WAN architecture	SD-WAN Enterprise Deployment Guide	Configuration steps
SD-WAN single datacenter	SD-WAN Single Datacenter Enterprise Deployment Guide	Configuring SD-WAN Overlay Template Configuring ADVPN
		Configuring SD-WAN Rules

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

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

If you have previously configured the FortiGate SD-WAN hub using the steps in Configuring a new FortiGate SD-WAN enterprise deployment using FortiManager on page 12 for one of the types of SD-WAN deployments, then your configuration should already match the configuration settings in this section and you can move on to the FortiSASE configuration steps in the next section.

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

IPsec VPN configuration

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

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

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

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

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

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

Tunnel interface configuration

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

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

BGP configuration

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

The hub FortiGate requires the following BGP settings:

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

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

The following shows sample BGP CLI configuration:

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

Firewall policy configuration

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

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

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

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, especially those sections covering Design concept and considerations on page 8, Product prerequisites on page 10, and Reviewing configuration settings of an existing FortiGate SD-WAN hub deployment previously configured using FortiManager on page 13.

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

Configuration workflow

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

1. Click the *Network Configuration* tab at the top of the page and configure the common network configuration settings. See Configuring network configuration on page 17.
2. Click the *Service Connections* tab at the top of the page, click *Create*, and configure a new service connection (hub). See Configuring a new service connection on page 20.

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

Configuring network configuration

Before proceeding with configuring hubs or service connections, you must configure common SPA network configuration used by all service connections.

Only a single BGP routing design method can be used for all hubs and spokes. They cannot be mixed.

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

To configure SPA network configuration:

1. Go to *Network > Secure Private Access* and click the *Network Configuration* tab.
2. For the *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select one of the following:
   - BGP per overlay (default selection)
   - BGP on loopback. FortiSASE automatically selects and grays out *BGP Recursive Routing* after you selecting this option.
3. Fill in the rest of the fields with values of the attributes of the FortiGate hub network connection. FortiSASE performs input validation and notifies you of any invalid values. See the following table:

Network attributes	Description	Example
BGP Routing Design	FortiSASE supports these main routing design methods: • 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.	BGP per overlay
BGP router ID subnet	For BGP per overlay, available/unused subnet that can be used to assign loopback interface IP addresses used for BGP router IDs parameter only on the FortiSASE security PoPs. /28 is the minimum subnet size. For *BGP on loopback*, you must configure this subnet as a neighbor range in the hub BGP settings.	10.20.1.0/24
Autonomous system number (ASN)	BGP autonomous system (AS) number of your hubs. Typically, this should be the same on both hubs.	65400
BGP recursive routing	Enabling the BGP recursive routing setting allows for interhub connectivity and redundancy to networks behind the active hub if each hub has a physical connection to the others for cases when connectivity between a FortiSASE security PoP and the active hub fails. For example, consider that this BGP configuration setting enabled and a FortiSASE security PoP's connectivity with hub 1 goes down. To ensure the security PoP can reach a network behind hub 1, it would route traffic to hub 2 first, then route it to hub 1 via its interhub connection, followed by routing the traffic to the desired destination network behind hub 1.	Enabled

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) requirements. A hub can be assigned a different priority level in different PoPs. • **BGP MED**: BGP multi-exit discriminator (MED) is an attribute that an autonomous system advertising routes to another peer sets. FortiSASE learns MED from the configured hubs. See BGP multi-exit discriminator.	Hub health and priority
Health check IP address	IP address of a server behind the hub that should be used to set up the SD-WAN performance SLA rule. 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.	10.30.100.1

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

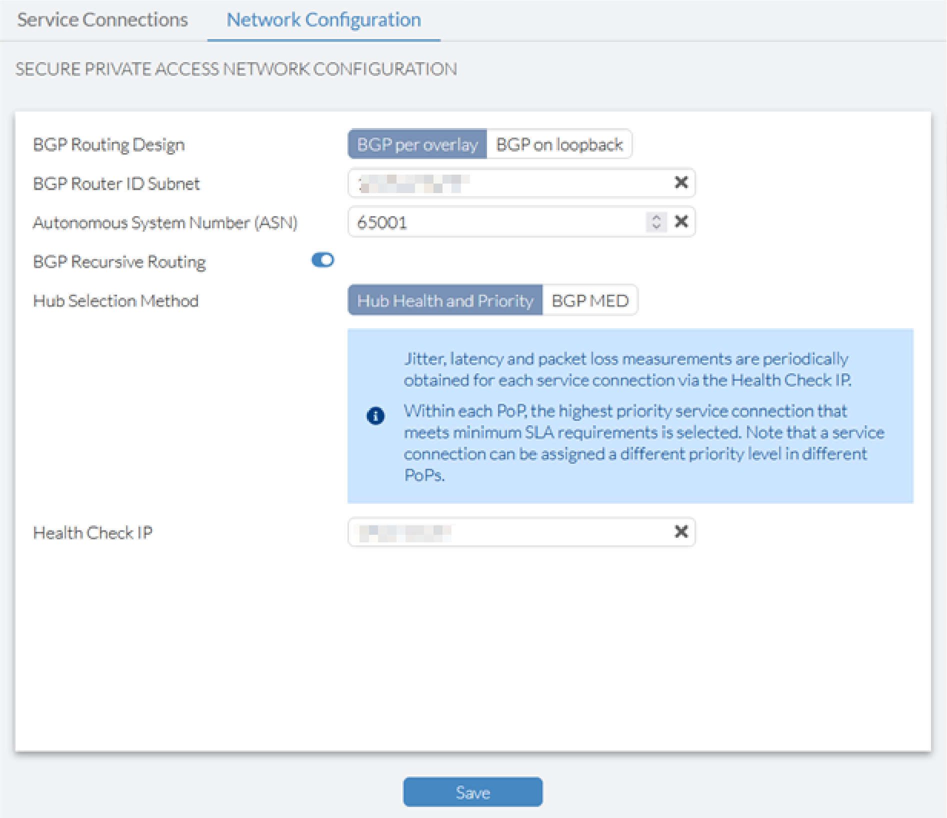
- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

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

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

4. Click *Save*.



BGP Routing Design: BGP per overlay | BGP on loopback

BGP Router ID Subnet:

Autonomous System Number (ASN): 65001

BGP Recursive Routing

Hub Selection Method: Hub Health and Priority | BGP MED

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

Health Check IP:

Configuring a new service connection

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

- BGP per overlay (default)
- BGP on loopback

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

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

To configure service connections or hubs for BGP per overlay:

1. Go to *Network > Secure Private Access*.
2. On the *Service Connection* tab, click *Create*.
3. Fill in the rest of the fields with the attributes of the FortiGate hub or service connection. FortiSASE validates the input and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Remote gateway	IPsec VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports *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.	mysecretkey
PKI User	When *Authentication Method* is configured as *Certificate*, select the PKI user with valid subject and CA certificate used by to validate the hub's 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 security PoP. You must import this certificate into via *System > Certificates* as a *Local Certificate*.	Fortinet_Factory
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	192.168.10.253
Network overlay ID	Define a unique network ID for each hub. If an active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2

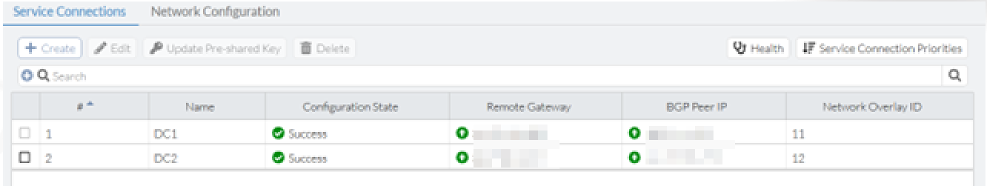
Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

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

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

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

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



	#	Name	Configuration State	Remote Gateway	BGP Peer IP	Network Overlay ID
□	1	DC1	✓ Success	[redacted]	[redacted]	11
□	2	DC2	✓ Success	[redacted]	[redacted]	12

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

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

Also, for 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 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 in the desired order of preference from the most preferred hub to the least preferred hub.

To configure service connections or hubs for BGP on loopback:

1. Go to *Network > Secure Private Access*.
2. On the *Service Connection* tab, click *Create*.
3. For the *Create a New Secure Private Access Service Connection* step, fill in the fields with the attributes of the FortiGate hub or service connection. performs input validation and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Remote gateway	IPsec VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports *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.	mysecretkey

Network attributes	Description	Example
PKI User	When *Authentication Method* is configured as *Certificate*, select the PKI user with valid subject and CA certificate used by to validate the hub's 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 security PoP. You must import this certificate into 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.	1
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.10.10.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2

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

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

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

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

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

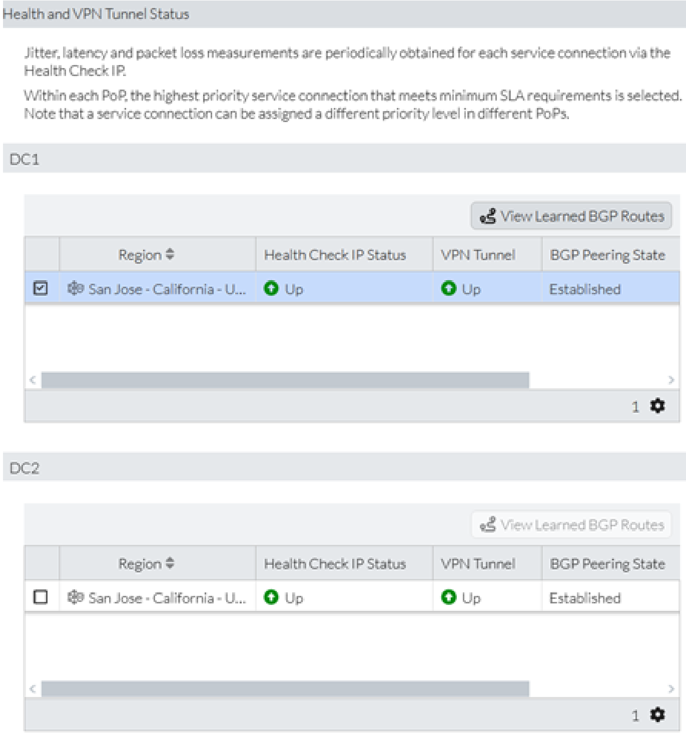
To update the authentication method settings for a service connection:

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

Viewing health and VPN tunnel status

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

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



Health and VPN Tunnel Status

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

DC1

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
☑	San Jose - California - U...	Up	Up	Established

1

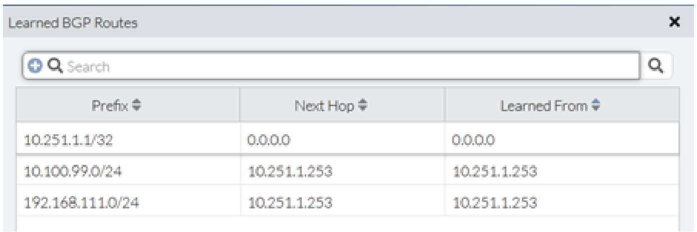
DC2

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
□	San Jose - California - U...	Up	Up	Established

1

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



Learned BGP Routes

Search

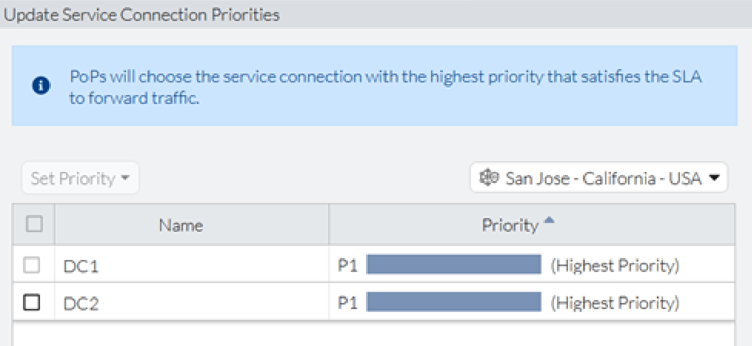
Prefix	Next Hop	Learned From
10.251.1.1/32	0.0.0.0	0.0.0.0
10.100.99.0/24	10.251.1.253	10.251.1.253
192.168.111.0/24	10.251.1.253	10.251.1.253

Updating service connection priorities

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

To update hub priorities:

1. Go to *Network > Secure Private Access*. On the *Service Connection*s tab, click the *Update Service Connection Priorities* button at the top of the page.
2. From the *Security PoP* dropdown list, select the desired PoP hub. The example selects the San Jose – California – USA security PoP.



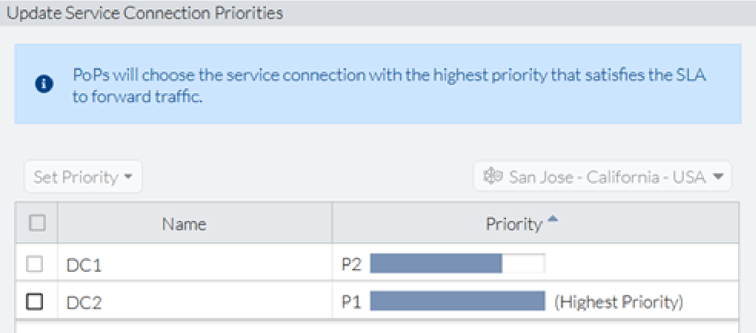
Update Service Connection Priorities

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

Set Priority ▾ | San Jose - California - USA ▾

☐	Name	Priority ▲
☐	DC1	P1 (Highest Priority)
☐	DC2	P1 (Highest Priority)

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



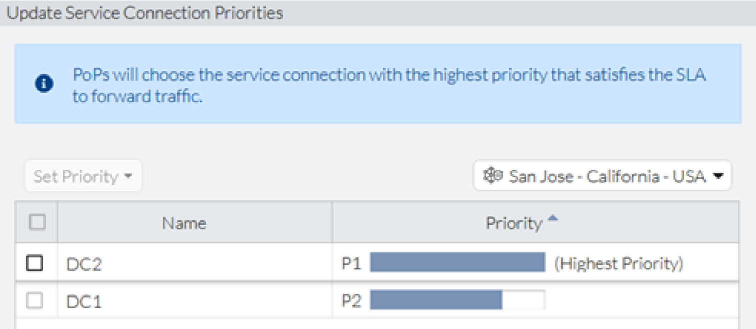
Update Service Connection Priorities

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

Set Priority ▾ | San Jose - California - USA ▾

☐	Name	Priority ▲
☐	DC1	P2
☐	DC2	P1 (Highest Priority)

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



Update Service Connection Priorities

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

Set Priority ▾ | San Jose - California - USA ▾

☐	Name	Priority ▲
☐	DC2	P1 (Highest Priority)
☐	DC1	P2

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:

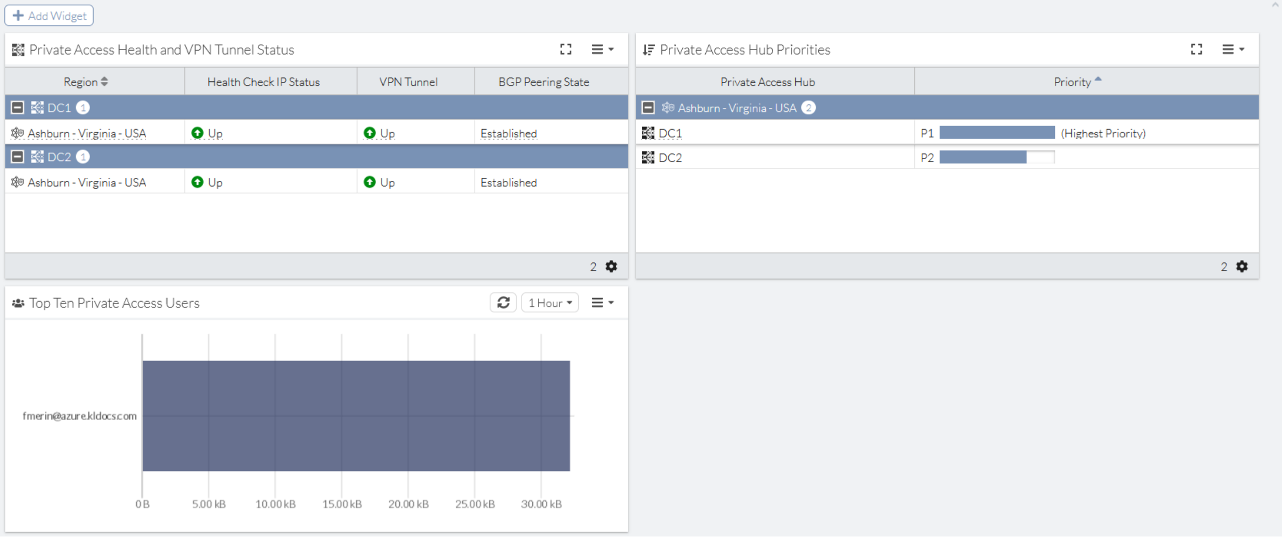
1. Go to *Network > Secure Private Access*.
2. Select the desired hub(s).
3. Click *Delete*.
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

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:



Private Access Health and VPN Tunnel Status

Region	Health Check IP Status	VPN Tunnel	BGP Peering State
⊟ DC1 1			
Ashburn - Virginia - USA	Up	Up	Established
⊟ DC2 1			
Ashburn - Virginia - USA	Up	Up	Established

2

Private Access Hub Priorities

Private Access Hub	Priority
⊟ Ashburn - Virginia - USA 2	
DC1	P1 (Highest Priority)
DC2	P2

2

Top Ten Private Access Users

Verifying private access policy configuration

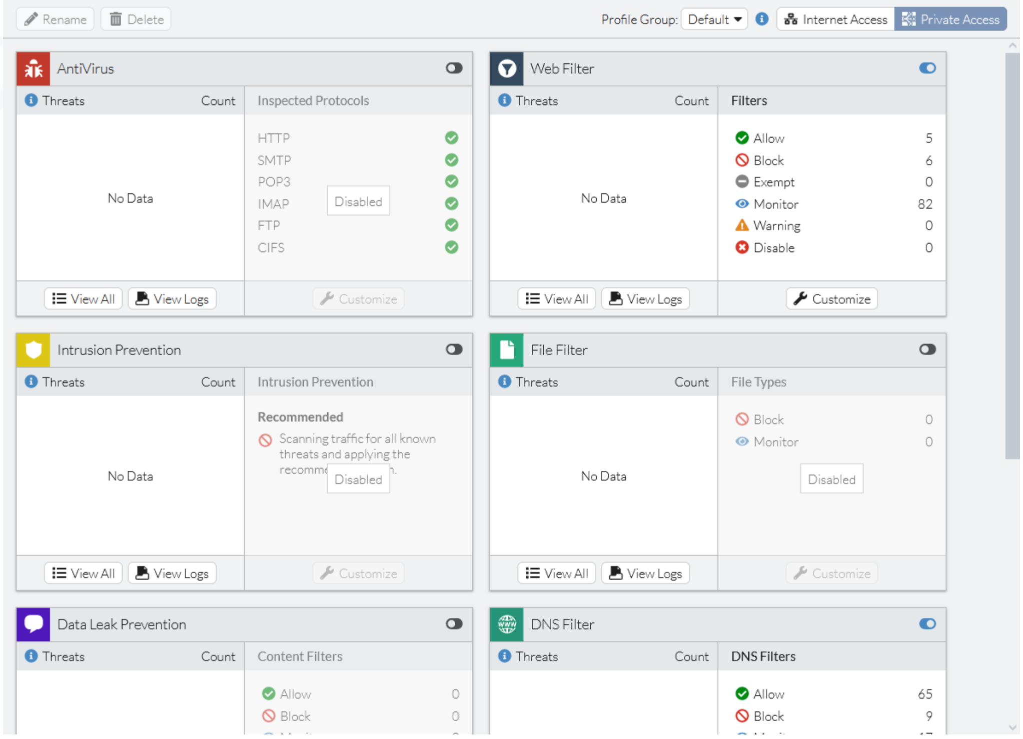
To verify private access policy configuration:

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

Configuring a private access security profile

To configure a private access security profile:

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



Rename | Delete | Profile Group: Default | Internet Access | Private Access

AntiVirus
Threats | Count | Inspected Protocols
No Data
HTTP ✓
SMTP ✓
POP3 ✓
IMAP ✓
FTP ✓
CIFS ✓
Disabled
View All | View Logs | Customize

Web Filter
Threats | Count | Filters
No Data

Filters	
Allow	5
Block	6
Exempt	0
Monitor	82
Warning	0
Disable	0

View All | View Logs | Customize

Intrusion Prevention
Threats | Count | Intrusion Prevention
No Data
Recommended
Scanning traffic for all known threats and applying the recomm... Disabled ...n.
View All | View Logs | Customize

File Filter
Threats | Count | File Types
No Data

File Types	
Block	0
Monitor	0

Disabled
View All | View Logs | Customize

Data Leak Prevention
Threats | Count | Content Filters

Content Filters	
Allow	0
Block	0

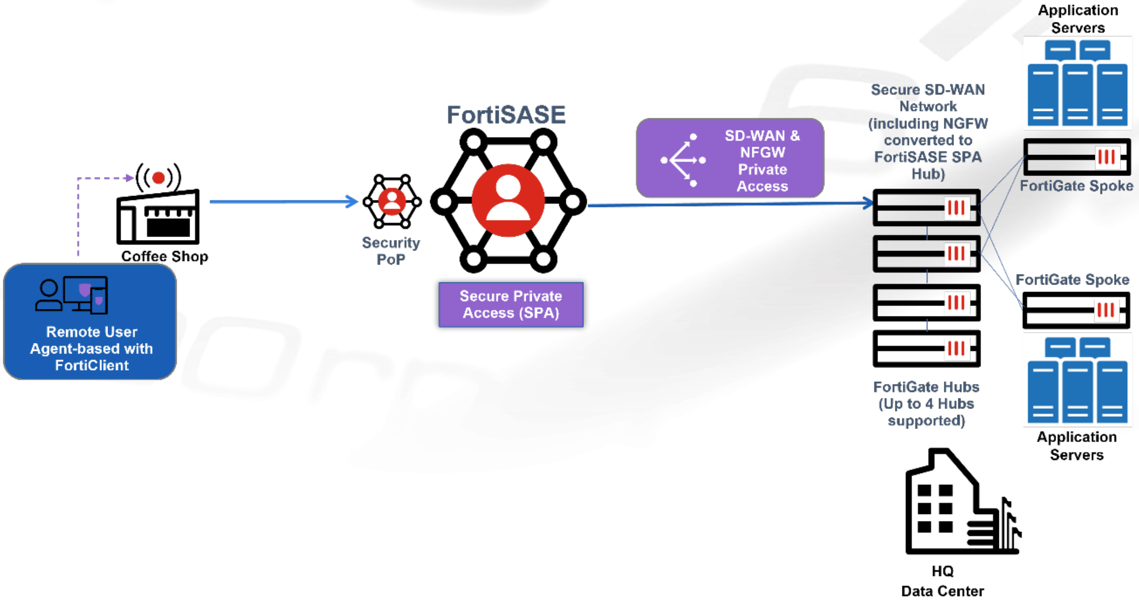
DNS Filter
Threats | Count | DNS Filters

DNS Filters	
Allow	65
Block	9

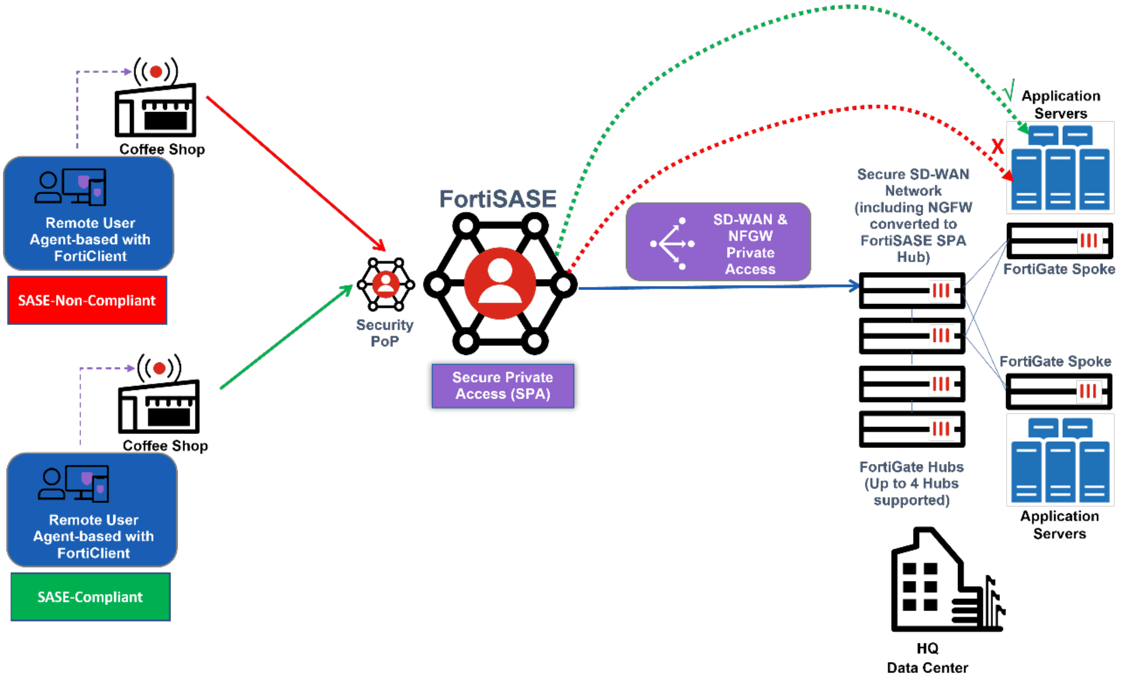
The security settings for Internet and private access are identical. For details on configuring security settings, see Security.

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.


Coffee Shop
Remote User Agent-based with FortiClient
Security PoP
FortiSASE
Secure Private Access (SPA)
SD-WAN & NFGW Private Access
Secure SD-WAN Network (including NGFW converted to FortiSASE SPA Hub)
Application Servers
FortiGate Spoke
FortiGate Spoke
Application Servers
FortiGate Hubs (Up to 4 Hubs supported)
HQ
Data Center

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.


Coffee Shop
Remote User Agent-based with FortiClient
SASE-Non-Compliant
Coffee Shop
Remote User Agent-based with FortiClient
SASE-Compliant
Security PoP
FortiSASE
Secure Private Access (SPA)
SD-WAN & NFGW Private Access
Secure SD-WAN Network (including NGFW converted to FortiSASE SPA Hub)
√
X
Application Servers
FortiGate Spoke
FortiGate Spoke
Application Servers
FortiGate Hubs (Up to 4 Hubs supported)
HQ
Data Center

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 that FortiClient detects as being without antivirus (AV) installed and running from accessing private applications behind the FortiGate hub. You would configure the following:

- Rule that applies a SASE-Compliant tag to Windows endpoints that FortiClient detects as having AV software installed and running

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

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

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

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

Configuration workflow

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

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

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

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

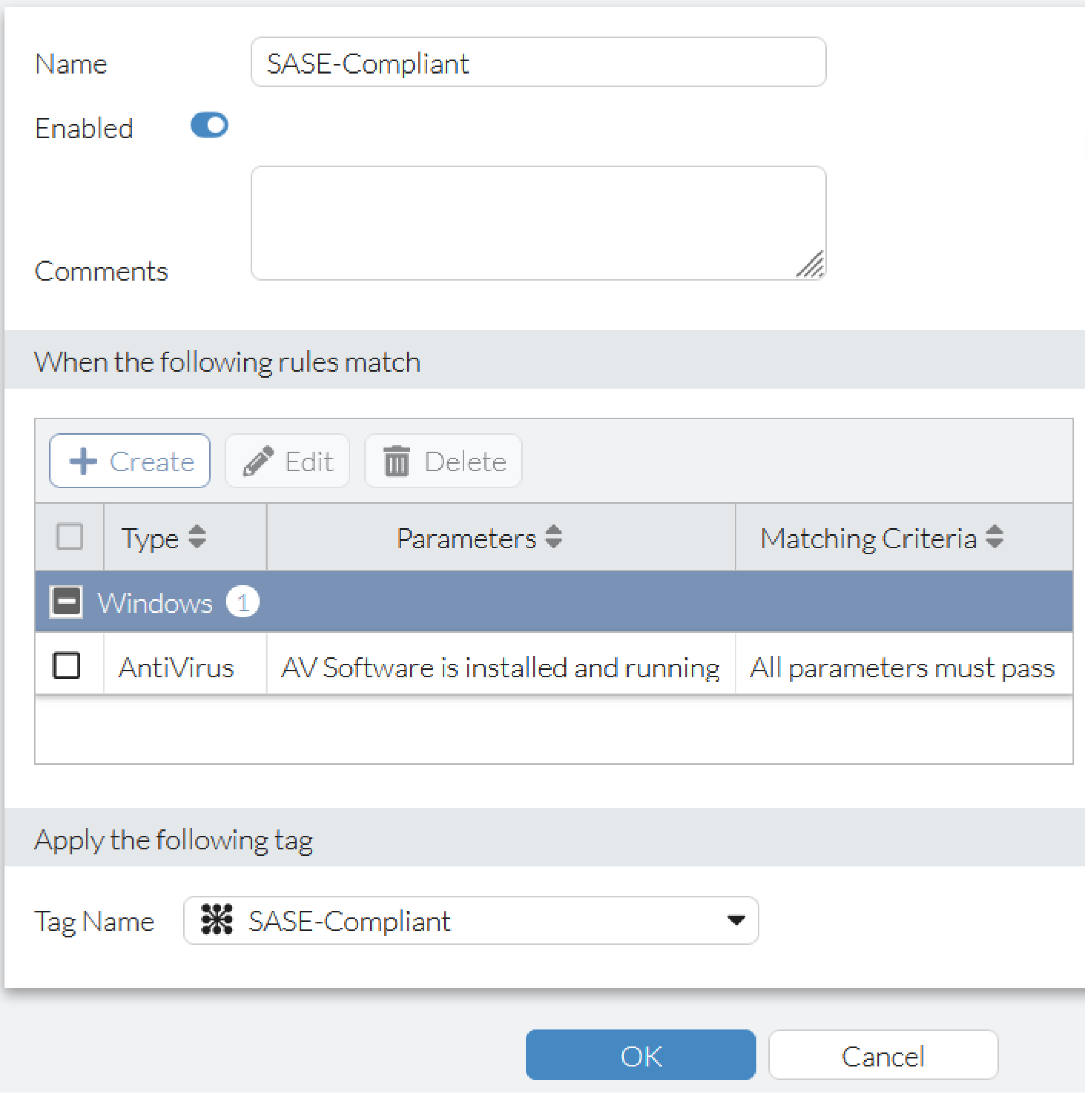
This example demonstrates how to configure zero trust network access (ZTNA) tag names and ZTNA tagging rule sets with the following posture checks:

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

To configure a ZTNA tagging rule set for compliant endpoints:

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

6. Configure the Severity Level rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   d. Click *OK*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.



Name: SASE-Compliant

Enabled: ●

Comments:

When the following rules match

☐	Type	Parameters	Matching Criteria
⊟	Windows 1		
☐	AntiVirus	AV Software is installed and running	All parameters must pass

Apply the following tag

Tag Name: SASE-Compliant

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

1. Go to *Configuration > ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.
5. Under *When the following rules match*, click *Create*.
6. Configure the Severity Level rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. Select *Negate*.

   d. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   e. Click *OK*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.

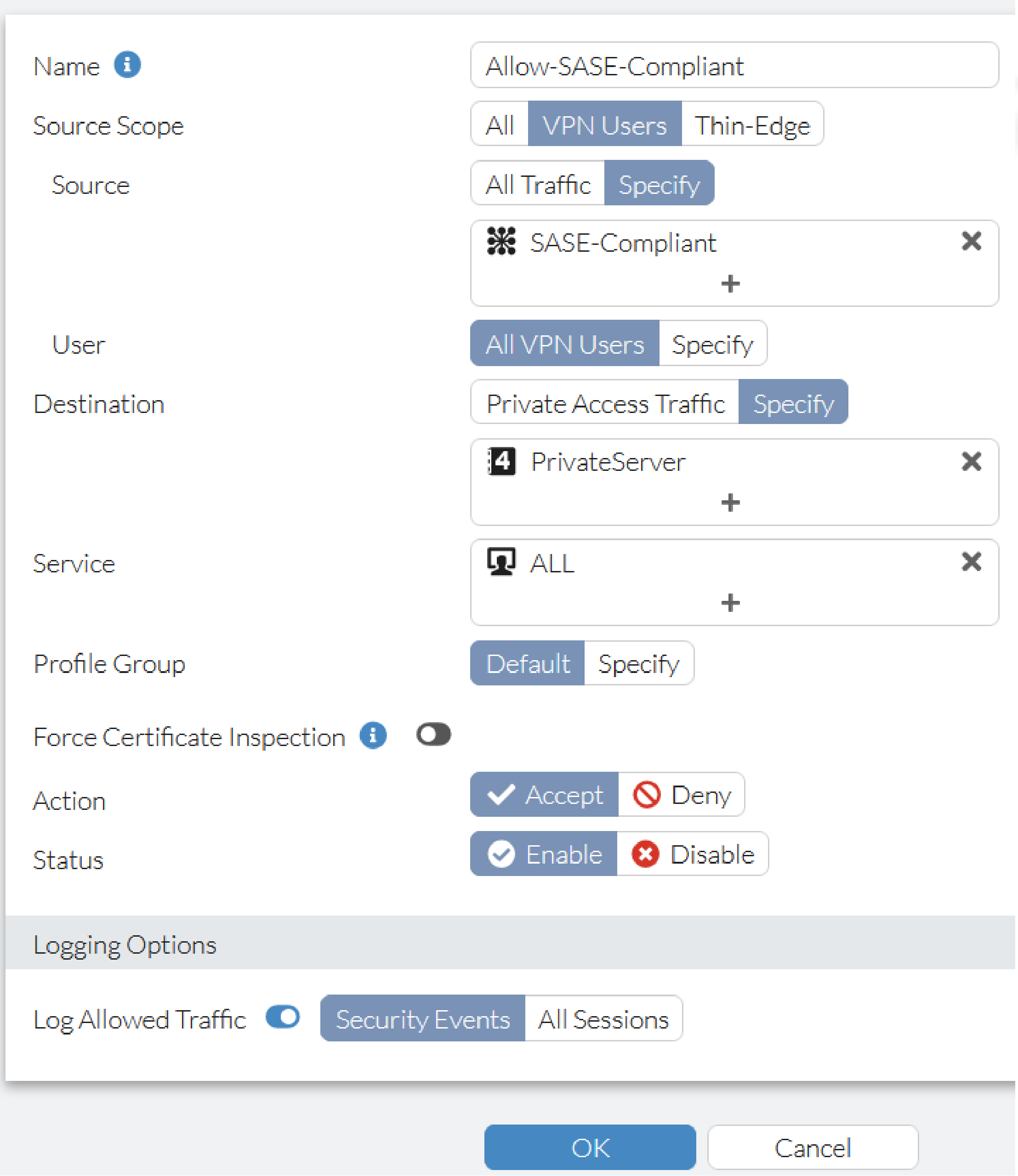
Configuring dynamic private access policies using ZTNA tags

This example demonstrates how to configure dynamic private access policies using the zero trust network access tags that you created in Configuring ZTNA rule sets to dynamically tag agent-based remote users on page 29 to allow endpoints tagged as SASE-Compliant with access to selected private resources and to deny access to selected private resources for endpoints tagged as SASE-Non-Compliant.

To configure a dynamic private access policy for compliant endpoints:

1. Go to *Configuration > Policies*.
2. Select *Private Access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Allow-SASE-Compliant.
   b. For *Source Scope*, select *VPN Users*.
   c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag > Private Access*, select the *SASE-Compliant* tag.
   d. For *Destination*, select *Specify*, click *+*, and in the *Select Entries* panel click *+Create* and click *IPv4 Host* to 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*.



Name: Allow-SASE-Compliant

Source Scope: All | **VPN Users** | Thin-Edge

Source: All Traffic | **Specify**

SASE-Compliant ✕ +

User: **All VPN Users** | Specify

Destination: Private Access Traffic | **Specify**

PrivateServer ✕ +

Service: ALL ✕ +

Profile Group: **Default** | Specify

Force Certificate Inspection ○

Action: ✓ **Accept** | Deny

Status: **Enable** | Disable

Logging Options

Log Allowed Traffic ● **Security Events** | All Sessions

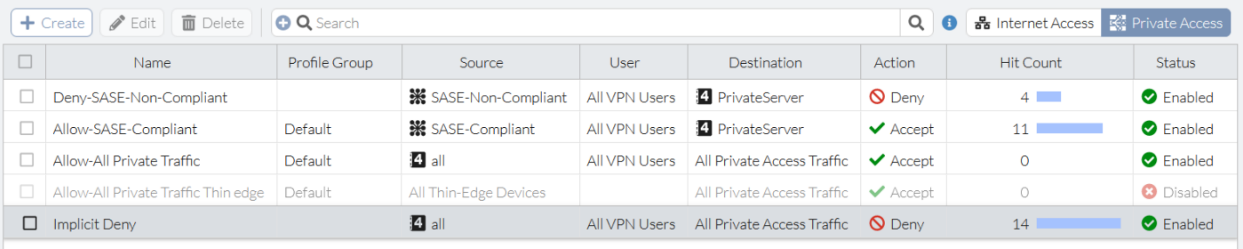
6. In *Configuration > Policies* with *Private Access* selected, ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private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

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

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

 d. For *Destination*, select *Private Access Traffic*.
 e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.
 f. For *Action*, select *Deny*.
 g. For *Status*, select *Enable*.

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

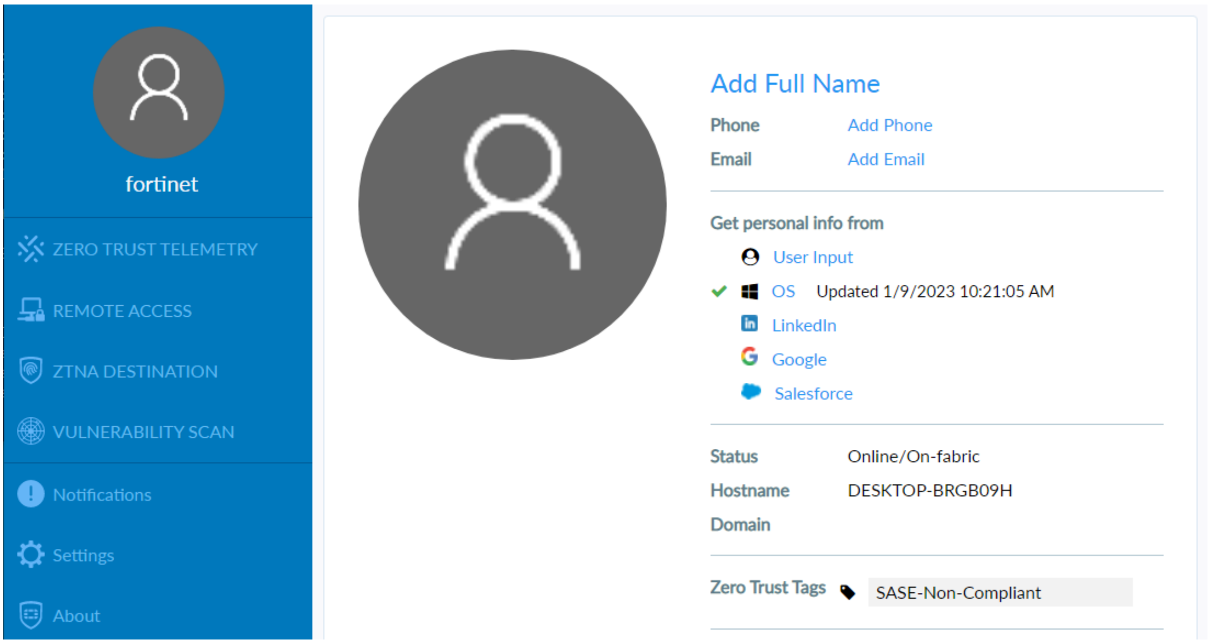


□	Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
□	Deny-SASE-Non-Compliant		SASE-Non-Compliant	All VPN Users	PrivateServer	⊘ Deny	4	✓ Enabled
□	Allow-SASE-Compliant	Default	SASE-Compliant	All VPN Users	PrivateServer	✓ Accept	11	✓ Enabled
□	Allow-All Private Traffic	Default	all	All VPN Users	All Private Access Traffic	✓ Accept	0	✓ Enabled
□	Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	✓ Accept	0	⊗ Disabled
□	Implicit Deny		all	All VPN Users	All Private Access Traffic	⊘ Deny	14	✓ Enabled

Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

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



Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

User Input

✓ OS Updated 1/9/2023 10:21:05 AM

LinkedIn

Google

Salesforce

Status Online/On-fabric

Hostname DESKTOP-BRGB09H

Domain

Zero Trust Tags SASE-Non-Compliant

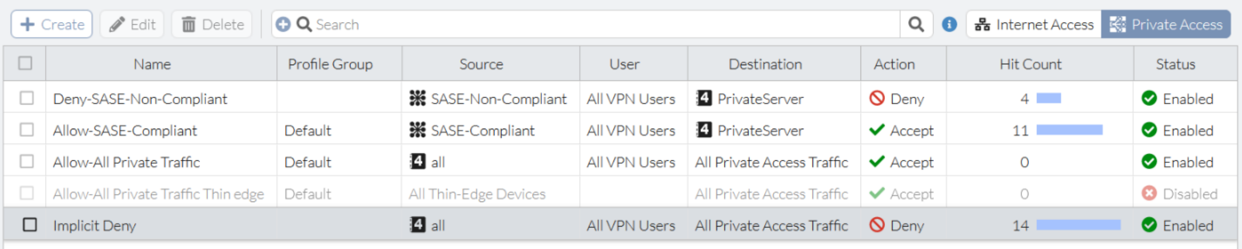
To test that FortiSASE allows a FortiClient endpoint tagged as SASE-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.

4. In Windows Defender, set *Real-time protection* to *On* as Stay protected with Windows Security describes. This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant Zero Trust tag applied.
6. 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.
7. 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
```

8. 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.



□	Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
□	Deny-SASE-Non-Compliant		SASE-Non-Compliant	All VPN Users	PrivateServer	Deny	4	Enabled
□	Allow-SASE-Compliant	Default	SASE-Compliant	All VPN Users	PrivateServer	✓ Accept	11	Enabled
□	Allow-All Private Traffic	Default	all	All VPN Users	All Private Access Traffic	✓ Accept	0	Enabled
□	Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	✓ Accept	0	Disabled
□	Implicit Deny		all	All VPN Users	All Private Access Traffic	Deny	14	Enabled

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

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 Windows Defender, set *Real-time protection* to *Off* as Stay protected with Windows Security describes. This turns off AV and ensures that FortiSASE dynamically tags the endpoint as non-compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Non-Compliant Zero Trust tag applied.
6. 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.
7. Observe the following output indicating the ICMP ping has timed out since FortiSASE denies access to the specific server:

```
C:\> ping 10.100.99.101

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

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

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

Configuring DNS Settings

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

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

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

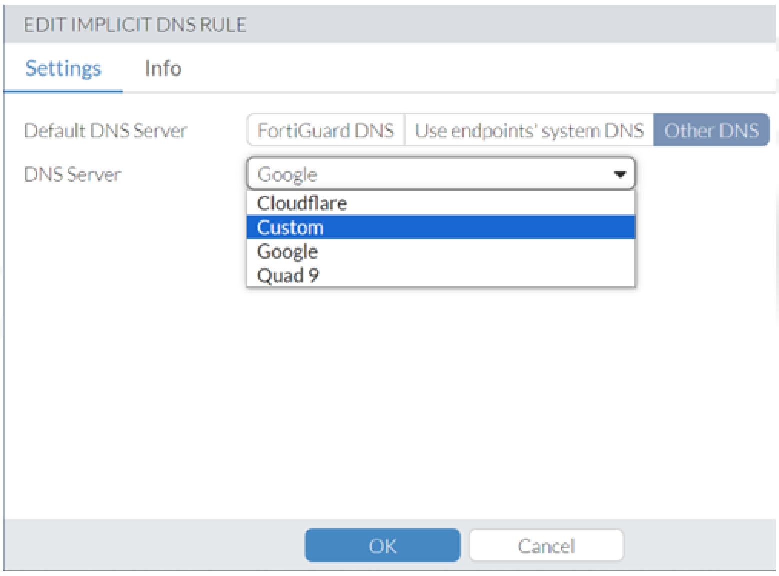
DNS server		Description	Primary and secondary DNS server IP address
FortiGuard DNS		Use FortiGuard DNS	208.91.112.53 208.91.112.52
Use endpoints' system DNS		Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS		Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
	CloudFlare	Use the CloudFlare public DNS server	1.1.1.1 1.0.0.1
	Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify IP address of primary and secondary DNS.
	Google	Use the Google public DNS server	8.8.8.8 8.8.4.4
	Quad 9	Use the Quad 9 public DNS server	9.9.9.9 149.112.112.112

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

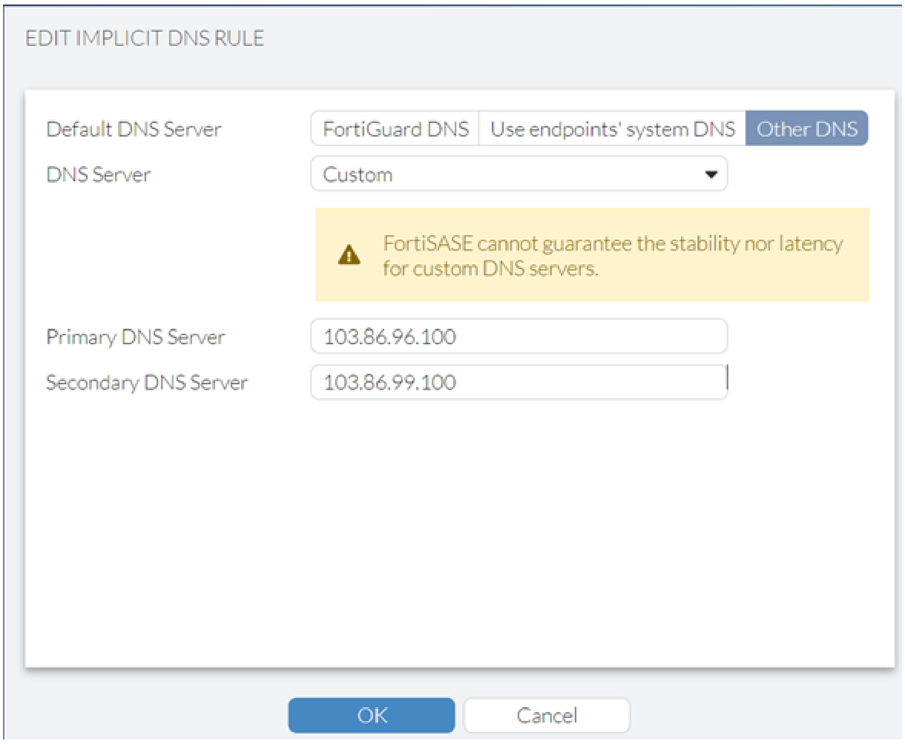
To configure a custom DNS server:

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

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.



DNS Server: Custom

FortiSASE cannot guarantee the stability nor latency for custom DNS servers.

Primary DNS Server: 103.86.96.100

Secondary DNS Server: 103.86.99.100

5. Click *OK*.

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

Split DNS Rules

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

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

To support these scenarios, 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 resolving hostnames for the specified internal domain (s) is necessary.
- Resolve all other hostnames for external domains using the implicit DNS rule.

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

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

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

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

Prerequisites

SSL Deep Inspection

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

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

See Certificate and deep inspection modes for further details on deep inspection.

Access to Internal DNS Server

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

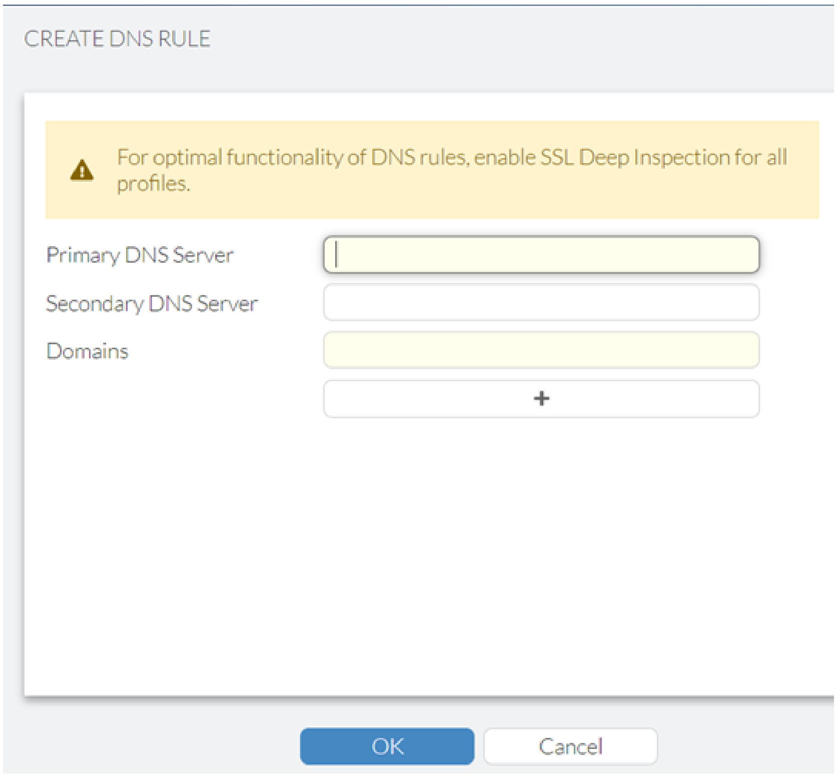
For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured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

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

Configuring Split DNS Rules

To configure Split DNS Rules:

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



CREATE DNS RULE

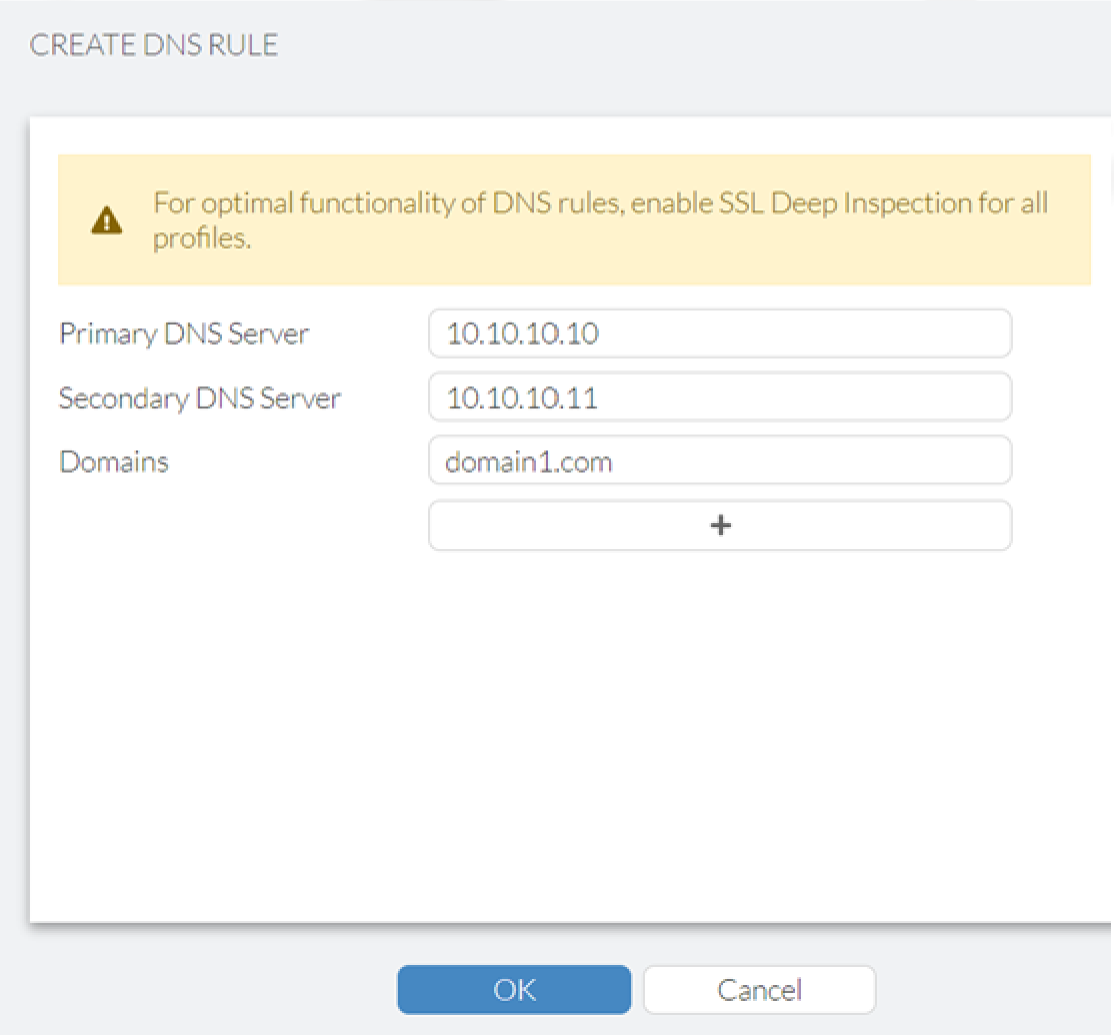
For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles.

Primary DNS Server

Secondary DNS Server

Domains

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



CREATE DNS RULE

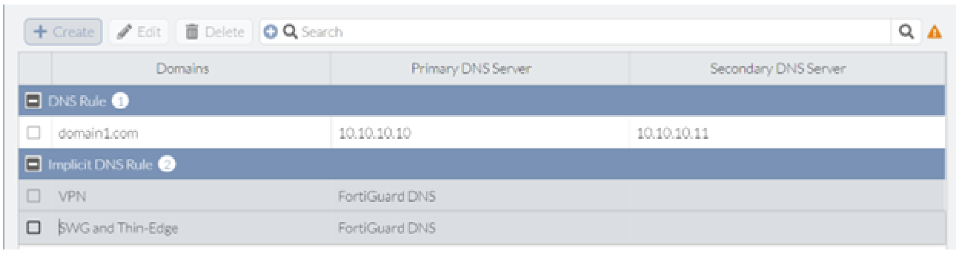
For optimal functionality of DNS rules, enable SSL Deep Inspection for all profiles.

Primary DNS Server: 10.10.10.10

Secondary DNS Server: 10.10.10.11

Domains: domain1.com

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



	Domains	Primary DNS Server	Secondary DNS Server
⊟	DNS Rule 1		
□	domain1.com	10.10.10.10	10.10.10.11
⊟	Implicit DNS Rule 2		
□	VPN	FortiGuard DNS	
□	SWG and Thin-Edge	FortiGuard DNS	

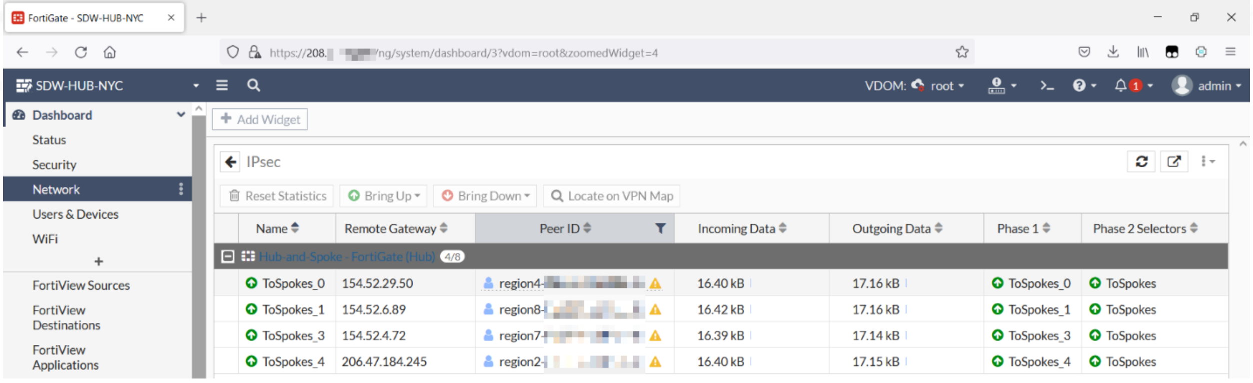
If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, then the Web Filter or DNS Filter blocks access to these local domains from FortiClient remote users if the Newly Observed Domain category is set to Block in the respective security component. In this case, you must create URL Filter entries for the Web Filter or Domain Filter entries for the DNS Filter to allow access to these local domains.

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

Verifying IPsec VPN tunnels on the FortiGate hub

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

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



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Hub-and-Spoke - FortiGate (Hub) 4/8						
ToSpokes_0	154.52.29.50	region4-[redacted]	16.40 kB	17.16 kB	ToSpokes_0	ToSpokes
ToSpokes_1	154.52.6.89	region8-[redacted]	16.42 kB	17.16 kB	ToSpokes_1	ToSpokes
ToSpokes_3	154.52.4.72	region7-[redacted]	16.39 kB	17.14 kB	ToSpokes_3	ToSpokes
ToSpokes_4	206.47.184.245	region2-[redacted]	16.40 kB	17.15 kB	ToSpokes_4	ToSpokes

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 users

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

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

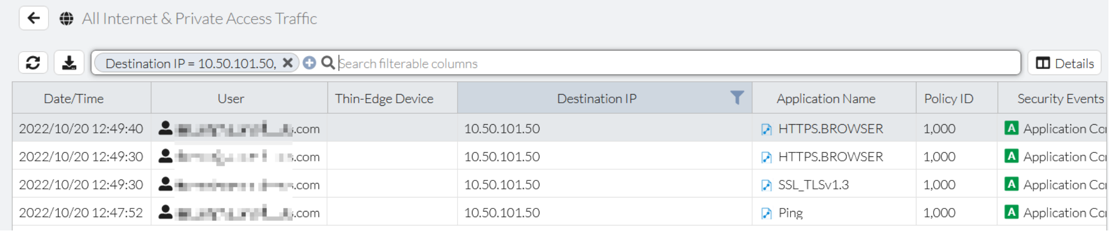
```
C:\>ping 10.50.101.50

Pinging 10.50.101.50 with 32 bytes of data:

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

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

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

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

Verifying private access traffic in FortiSASE portal

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

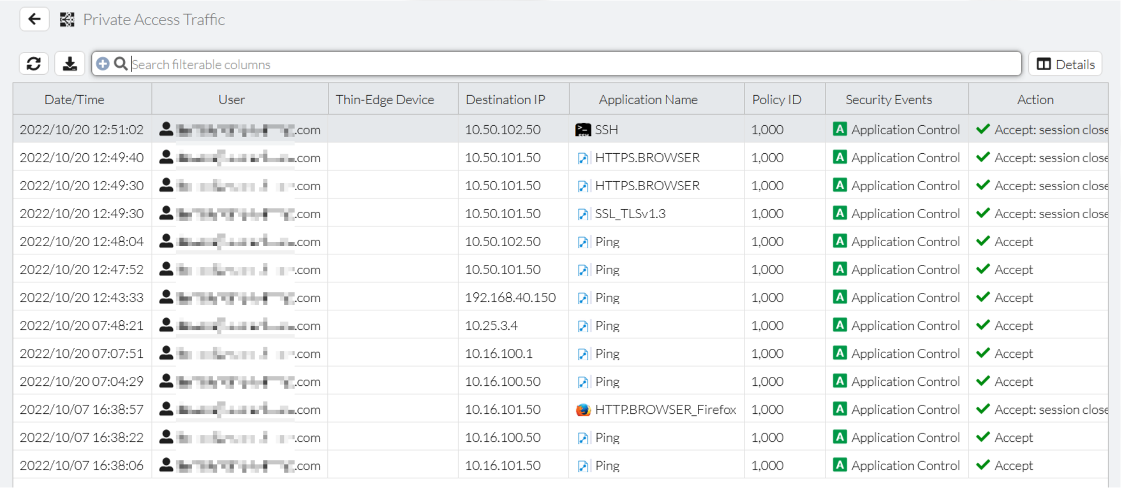
- From *Analytics > Logs > Traffic* by viewing either the *All Internet and Private Access Traffic* page or the *Private Access Traffic* page
- From *Dashboard > FortiView > Sources*, *Dashboard > FortiView > Destinations*, or *Dashboard > FortiView > Policies* and filtering on the private access destination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

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


All Internet & Private Access Traffic
Destination IP = 10.50.101.50,
Search filterable columns
Details

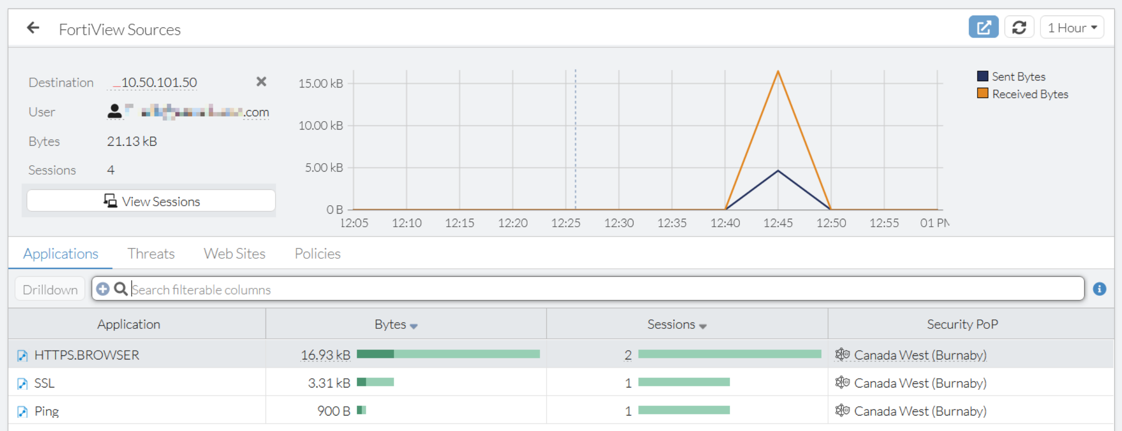
Date/Time	User	Thin-Edge Device	Destination IP	Application Name	Policy ID	Security Events
2022/10/20 12:49:40	[redacted].com		10.50.101.50	HTTPS.BROWSER	1,000	A Application Co
2022/10/20 12:49:30	[redacted].com		10.50.101.50	HTTPS.BROWSER	1,000	A Application Co
2022/10/20 12:49:30	[redacted].com		10.50.101.50	SSL_TLSv1.3	1,000	A Application Co
2022/10/20 12:47:52	[redacted].com		10.50.101.50	Ping	1,000	A Application Co

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



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

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



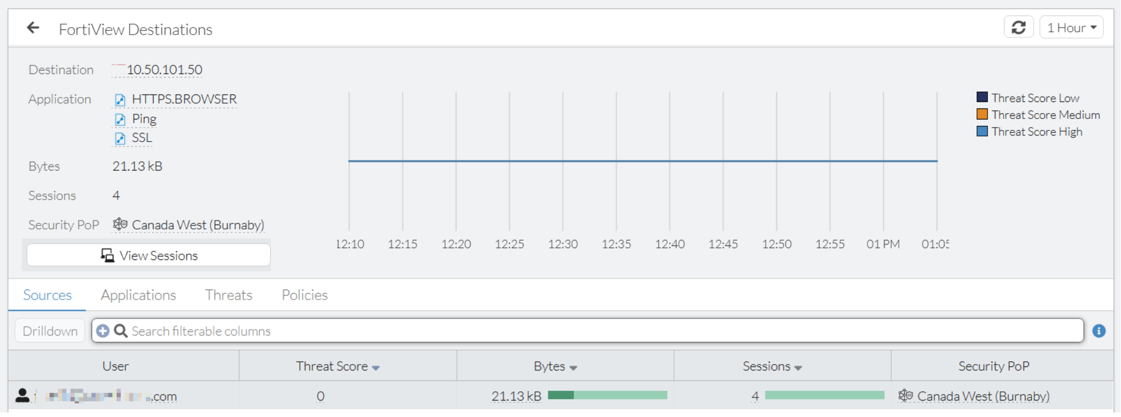
Destination 10.50.101.50

User [redacted].com

Bytes 21.13 kB

Sessions 4

Application	Bytes	Sessions	Security PoP
HTTPS.BROWSER	16.93 kB	2	Canada West (Burnaby)
SSL	3.31 kB	1	Canada West (Burnaby)
Ping	900 B	1	Canada West (Burnaby)



Destination 10.50.101.50

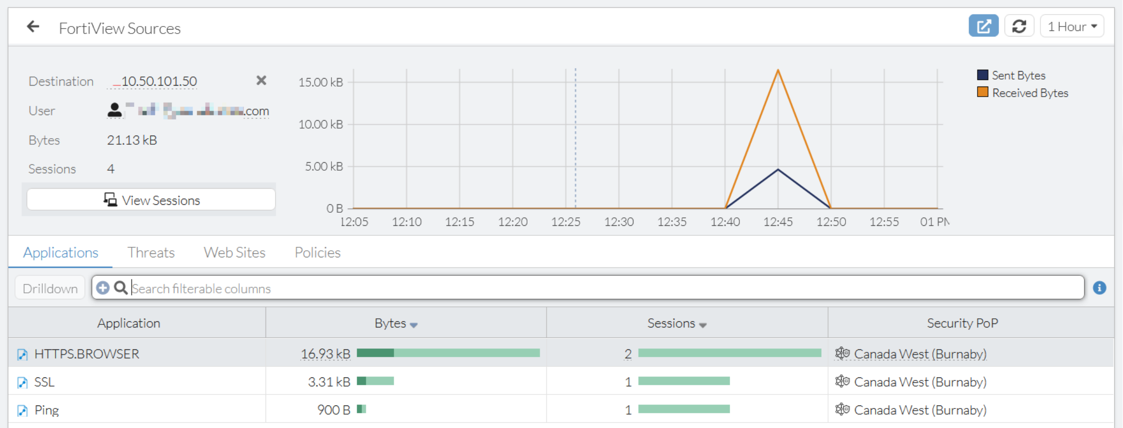
Application HTTPS.BROWSER
Ping
SSL

Bytes 21.13 kB

Sessions 4

Security PoP Canada West (Burnaby)

User	Threat Score	Bytes	Sessions	Security PoP
[redacted].com	0	21.13 kB	4	Canada West (Burnaby)



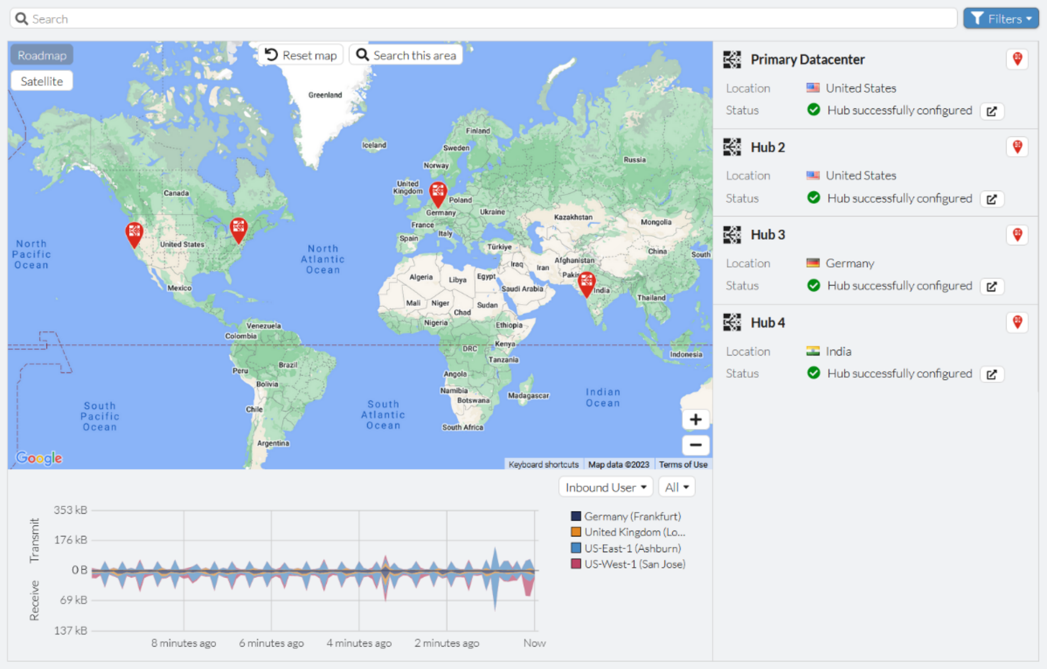
Destination 10.50.101.50
User [redacted].com
Bytes 21.13 kB
Sessions 4

Application	Bytes	Sessions	Security PoP
HTTPS.BROWSER	16.93 kB	2	Canada West (Burnaby)
SSL	3.31 kB	1	Canada West (Burnaby)
Ping	900 B	1	Canada West (Burnaby)

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.



Primary Datacenter
Location: United States
Status: Hub successfully configured

Hub 2
Location: United States
Status: Hub successfully configured

Hub 3
Location: Germany
Status: Hub successfully configured

Hub 4
Location: India
Status: Hub successfully configured

More information

Appendix A: Products used in this guide

For a list of product models and firmware that this guide uses, see Product integration and support.

Appendix B: Documentation references

Feature documentation

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

4-D resources: SASE

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

www.fortinet.com