FORTINET

Deployment Guide

Overlay-as-a-Service

4D

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log 3
Introduction 4
About this guide 5
About the 4-D documentation series 5
Intended audience 5
Deployment objectives 6
Deployment assumptions 6
Solution overview 8
Design overview 9
Use cases and topologies 9
Product prerequisites 10
Deployment procedures 11
Deployment prerequisites 11
Planning 12
Firewall policies 12
Assumptions 12
Configuration steps 14
Registering FortiCloud Overlay-as-a-Service licenses 14
Preparing site FortiGate devices for OaaS 15
Accessing the OaaS portal 16
Defining the SD-WAN hub device 17
Deploying a new SD-WAN site for the hub 17
Monitoring link performance and quality across SD-WAN devices in OaaS 22
Centralized OaaS policy example 24
Testing and verifying connectivity between sites deployed using OaaS 28

Change Log

Date	Change Description
2025-01-03	Initial release.

Introduction

FortiCloud Overlay-as-a-Service (OaaS) is a service for FortiGate devices to easily provision new SD-WAN overlay networks from FortiCloud. OaaS is a subscription service providing an easy-to-use GUI wizard that simplifies the process of configuring an SD-WAN overlay within a single region. OaaS supports FortiGate devices running FortiOS 7.4.4 and later.

Currently, OaaS supports a geo-redundant, dual hub architecture where the SD-WAN overlay hub is powered by FortiOS and managed by FortiCloud, and your branch FortiGates and datacenter FortiGates are configured as spokes within this overlay.

- OaaS and the spokes rely on Fortinet Inc.'s Auto-Discovery VPN (ADVPN), which allows the central hub to dynamically inform spokes about a better path for traffic between two spokes.
- ADVPN shortcut tunnels, also known as shortcuts, are formed between spokes, such as between branches and the datacenter, or between branches themselves so that traffic does not need to pass through the hub.

For successful setup of ADVPN tunnels, the spokes' ISPs must allow traffic over UDP port 500 and UDP port 4500 for NAT traversal (NAT-T).

Essentially, the OaaS hub acts as a bridge to allow overlay shortcuts to be formed between your spokes.

OaaS requires a license for each spoke, either as a FortiGate VM or a hardware FortiGate device.

OaaS only supports FortiGate devices running FortiOS 7.4.4 and later.

OaaS is the official replacement for OCVPN. Migration of deployments from OCVPN to OaaS is beyond the scope of this deployment guide. See the SD-WAN Overlay Migration from OCVPN to OaaS Deployment Guide.

This document covers the step-by-step procedures required to use OaaS to deploy the Fortinet Secure SD-WAN solution to a single SD-WAN region and configure a geo-redundant, dual hub architecture.

The architecture, components, and technology referenced in this document are covered in the Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide.

For additional information and documentation about the topics covered in this document, please see the Fortinet Document Library at https://docs.fortinet.com.

About this guide

This guide provides the design and steps for deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture and design outlined in this guide suits them. It is advised to review the Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide if readers are still in the process of selecting the right architecture.

This guide is part of the 4-D documentation series.

About the 4-D documentation series

Fortinet Secure SD-WAN documentation is categorized into four distinct documents (called 4-D documents): Define, Design, Deploy, and Demo. Each document is designed for a specific purpose and builds on the other documents by providing you a complete path from beginning to end.

The 4-D documentation series includes the following components:

- **Define**: Conceptual guide meant to introduce the reader to common SD-WAN use cases and the Fortinet Secure SD-WAN solution
- **Design**: Reference architecture guide that provides an overview of the components and architectures to satisfy common uses
- **Deploy**: Deployment guides that provide step-by-step procedures for deploying the desired architecture
- **Demo**: Github repository of the configuration and examples provided by subsequent documents

The architecture, components, and technology referenced in this document are covered in the Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide.

For additional information and documentation about the topics covered in this document, please see the Fortinet Document Library at https://docs.fortinet.com.

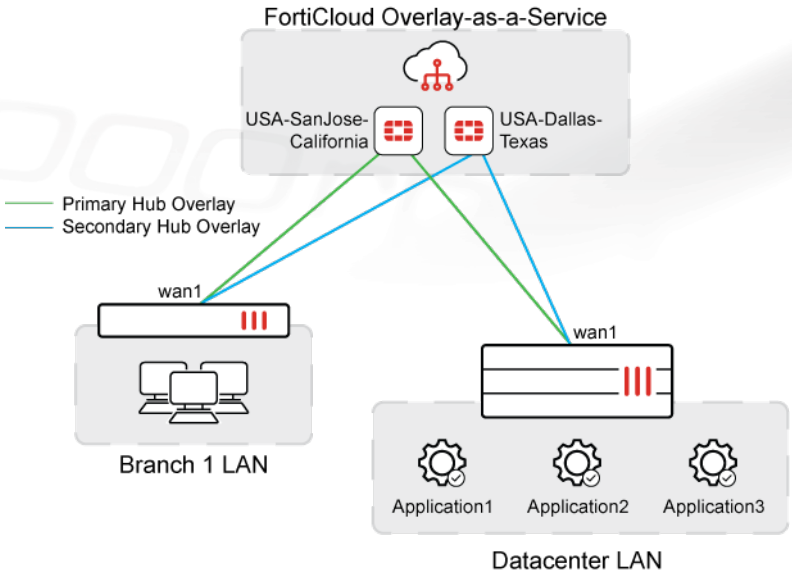
Intended audience

This guide is primarily created for a technical audience, including system architects and design engineers, who want to deploy Fortinet Secure SD-WAN in greenfield or new scenarios. It is assumed that you have read the SD-WAN Architecture for Enterprise guide and have identified the architecture that satisfies your use case and goals. This document does not provide an overview or description of the solution technologies and components.

For implementation, a working knowledge of FortiOS networking and policy configuration is ideal.

Deployment objectives

This deployment guide is the supporting document to the Single datacenter (active-passive gateway) section of the *SD-WAN Architecture for Enterprise* guide.



Deployment assumptions

- Greenfield deployment of new Fortinet Secure SD-WAN devices.
- Each remote site or spoke includes a FortiGate VM or hardware device with a valid OaaS license.
- Two geo-located hubs on OaaS are located in the FortiCloud platform.
- The two hubs will provide secure access between spoke sites (branch or datacenter sites) that require connectivity to local application and services.
- The two hubs each have a single WAN connection.
- The two hubs will be deployed in a primary and secondary FortiCloud location to provide active-passive redundancy.
- In this deployment, each remote site or spoke has a single WAN underlay. In general, OaaS supports multiple underlays; up to three underlays.
- WAN connections can reach all other devices in the region.
- All WAN interfaces have already been configured, have default gateways, and have valid internet connectivity configured across all links.
- The two hubs on OaaS have been configured to establish overlay connections with each spoke.

OaaS requires a license for each spoke, either as a FortiGate VM or a hardware FortiGate device.

OaaS only supports FortiGate devices running FortiOS 7.4.4 and later.

DEPLOYMENT OBJECTIVES

OaaS is the official replacement for OCVPN. Migration of deployments from OCVPN to OaaS is beyond the scope of this deployment guide. See the SD-WAN Overlay Migration from OCVPN to OaaS Deployment Guide.

Solution overview

This solution uses the FortiCloud Overlay-as-a-Service (OaaS) application to configure an SD-WAN overlay with the specified FortiGates.

OaaS supports a geo-redundant, dual hub architecture where the SD-WAN overlay hubs are powered by FortiOS and managed by FortiCloud, and your branch FortiGates and datacenter FortiGates are configured as spokes within this overlay.

When configuring the spoke FortiGates, OaaS configures the following settings in the background:

- IPsec overlay configuration (hub-and-spoke ADVPN tunnels)
- BGP configuration
- Policy routing
- SD-WAN zone
- SD-WAN performance SLAs
- SD-WAN rule
- Firewall addresses
- Firewall policies

OaaS configures SD-WAN rules on each of the spokes to provide a complete SD-WAN deployment.

In summary, this document describes how to:

1. Use OaaS to configure the overlay between the hub and spoke FortiGates as well as generate firewall policies.
2. Test and verify the SD-WAN configuration of the spoke FortiGates after using OaaS.

Design overview

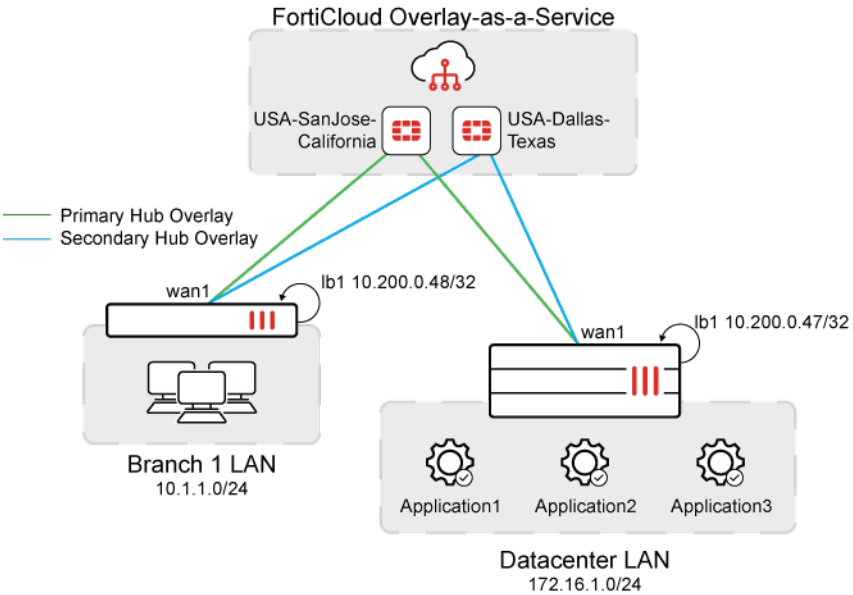
In this design, the SD-WAN gateway (sometimes called the hub) acts as a connector to provide connectivity between remote SD-WAN sites. The SD-WAN gateway is located in the FortiCloud infrastructure managed by Fortinet.

The following sections help describe the solution design:

- Use cases and topologies on page 9
- Product prerequisites on page 10

Use cases and topologies

OaaS can configure an overlay for the following example hub-and-spoke topology using ADVPN and a single hub:



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

In the example hub-and-spoke topology, the SD-WAN overlay hub is powered by FortiOS and deployed in FortiCloud where a primary hub (USA-SanJose-California DC) and a secondary hub (USA-Dallas-Texas DC) are configured for

overlay redundancy. The single datacenter FortiGate and branch FortiGate are configured as spokes within this overlay.

OaaS relies on the FortiCloud management tunnel to FortiGates to retrieve interface information and to install configuration settings orchestrated from OaaS.

By default, OaaS has reserved 10.200.0.0/16 for overlay IP addressing of all spokes, and you should not use this network in either the LAN subnets or WAN network. If you have a network conflict, you can modify the reserved subnet in the *Settings* view within the OaaS portal.

Each FortiGate has a distinct LAN subnet and a loopback interface with an IP address within the 10.200.0.0/24 subnet.

As part of the orchestration process on each spoke, OaaS creates a performance SLA from the spoke to the hub using a health check server within the reserved overlay subnet and then uses this performance SLA to configure a lowest cost (SLA) SD-WAN rule.

Product prerequisites

- FortiOS 7.4.4 and later on the FortiGates acting as spokes.
- FortiCloud Overlay-as-a-Service licenses for all spokes.
- FortiCloud SD-WAN Network Monitor licenses for Bandwidth feature.

Deployment procedures

FortiCloud Overlay-as-a-Service (OaaS) is used to configure SD-WAN for a topology that includes a single datacenter and multiple sites. The deployment instructions include the following topics:

- Deployment prerequisites on page 11
- Planning on page 12
- Firewall policies on page 12
- Assumptions on page 12
- Configuration steps on page 14

OaaS requires a license for each spoke, either as a FortiGate VM or a hardware FortiGate device.

OaaS only supports FortiGate devices running FortiOS 7.4.4 and later.

OaaS is the official replacement for OCVPN. Migration of deployments from OCVPN to OaaS is beyond the scope of this deployment guide. See the SD-WAN Overlay Migration from OCVPN to OaaS Deployment Guide.

Deployment prerequisites

This guide presumes the following prerequisites have been met:

- All FortiGate spokes sites (branches and datacenters) have an OaaS license.
- All FortiGates in the SD-WAN region are running FortiOS 7.4.4 and later.
- ISP links and other interfaces have been configured on all devices.
  - ISP routing is configured where branches have proper routes to reach the hub.
  - LAN and other directly connected networks have been assigned.
- The WAN and LAN interfaces for OaaS service are not used in any existing firewall policy.

- The WAN and LAN ports are not used in any existing network zone.
- The WAN port is not bound to any SD-WAN zone.

Planning

The deployment example in this guide uses the following settings, including IP networks, BGP AS number, performance SLA criteria, and so on:

1. Overlay network address space:
   a. This address space is reserved and used by OaaS for the IP addressing of all spoke devices.
   b. The default 10.200.0.0/16 is used. If you have a network conflict, you can modify this reserved subnet in the *Settings* view in the OaaS portal
2. Loopback IP address space:
   a. These addresses are used for Performance SLAs, Router IDs and other admin operations.
   b. The default 10.200.0.0/24 is used.
3. Autonomous System number for BGP:
   a. A private number is used and must remain exclusively for this SD-WAN BGP configuration.
   b. The AS of 65001 is used.
4. Performance SLA criteria:
   a. Lowest Cost (SLA) mode is used, where SD-WAN chooses the lowest latency link that satisfies SLA to forward traffic.
   b. Latency Threshold: 100 ms

Firewall policies

OaaS creates firewall policies to allow all traffic through the SD-WAN overlay.

OaaS creates firewall policies with wildcard address objects and services on the spoke FortiGates that allow all traffic. For some cases, these policies do not provide the necessary granularity to restrict overlay traffic to specific subnets or hosts.

Centralized OaaS policies can be configured and applied in the OaaS portal. See Centralized OaaS policy example on page 24 and OaaS Policy.

Assumptions

The deployment example in this guide uses the following ports and IP addresses:

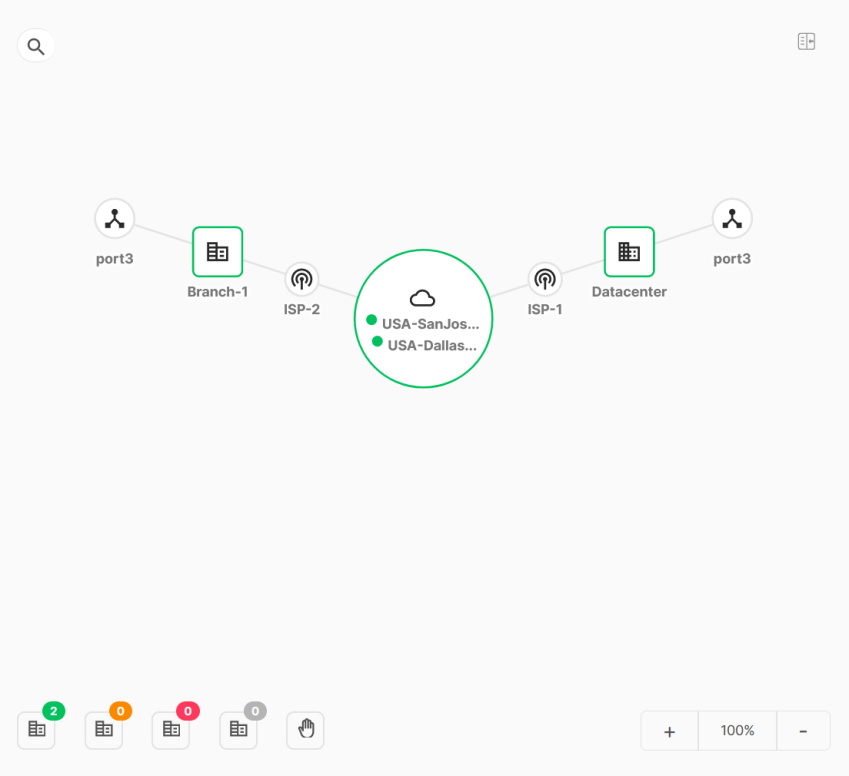
- ISP1 is connected to WAN1 on all FortiGates.
- All FortiGates are connected to the primary and secondary hub locations for overlay redundancy.
- LAN is connected to internal7 on the Branch 1 FortiGate.
- LAN is connected to internal6 on the datacenter FortiGate.

ASSUMPTIONS

- Datacenter LAN is 172.16.1.0/24.
- Branch 1 LAN is 10.1.1.0/24.

By default, OaaS has reserved 10.200.0.0/16 for overlay IP addressing of all spokes, and you should not use this network in either the LAN subnets or WAN network. If you have a network conflict, you can modify the reserved subnet in the *Settings* view within the OaaS portal.

When you finish deploying a configuration from OaaS to the sites, you can view the topology in OaaS:



The components of the topology in OaaS map to the following components in an SD-WAN topology:

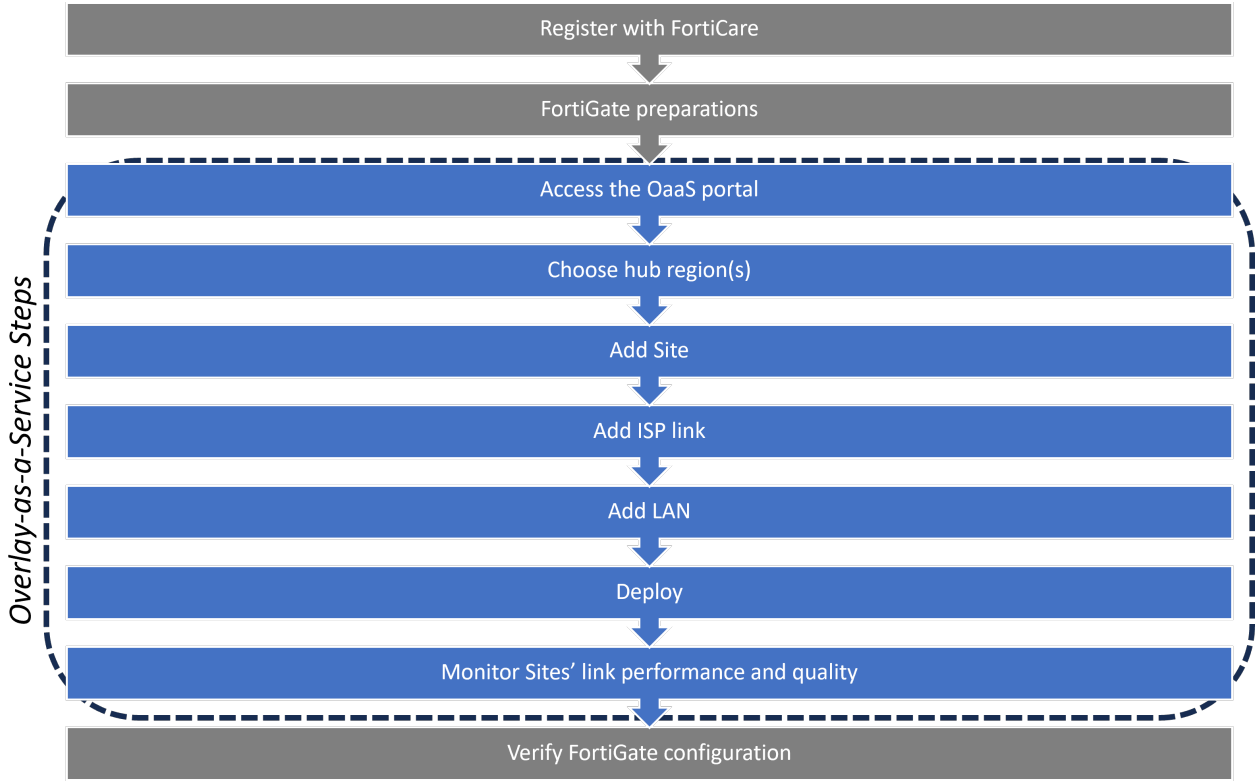
OaaS topology component	SD-WAN topology component
FortiCloud Hub on USA-SanJose-California	Primary Hub
FortiCloud Hub on USA-Dallas-Texas	Secondary Hub
Datacenter site (Data Center site type)	Spoke at Datacenter location
ISP-1	Underlay used by Datacenter spoke
port3	Datacenter LAN
Branch-1 (Branch site type)	Spoke at Branch-1 location
ISP-2	Underlay used by Branch-1 spoke
port3	Branch-1 LAN

Throughout this guide, a site is synonymous with a spoke. The terms are used interchangeably.

Configuration steps

Following is a summary of the steps required to configure SD-WAN using FortiCloud Overlay-as-a-Service:

1. Register FortiCloud OaaS licenses in FortiCloud. See Registering FortiCloud Overlay-as-a-Service licenses on page 14.
2. Prepare your FortiGate devices to be used by OaaS as sites in the SD-WAN network. See Preparing site FortiGate devices for OaaS on page 15.
3. Access the OaaS portal. See Accessing the OaaS portal on page 16.
4. Define the hub region for the SD-WAN network. See Defining the SD-WAN hub device on page 17.
5. Define and deploy the sites for the hub in the SD-WAN network. See Deploying a new SD-WAN site for the hub on page 17.
   a. Add a site to the hub.
   b. Add ISP link.
   c. Add LAN.
   d. Deploy the SD-WAN configuration to the site.
6. Monitor link performance and quality across devices in the SD-WAN network. See Monitoring link performance and quality across SD-WAN devices in OaaS on page 22.
7. Configure centralized OaaS policies. See Centralized OaaS policy example on page 24.
8. Test and verify connectivity between sites deployed using OaaS. See Testing and verifying connectivity between sites deployed using OaaS on page 28.



Registering FortiCloud Overlay-as-a-Service licenses

In FortiCloud, register the following licenses:

- Overlay-as-a-Service:
  - The OaaS SKU is in the format FC-10-XXXXX-657-02-DD where XXXXX corresponds to the model code and DD corresponds to the validity period of the license in months.
- SD-WAN Network Monitor
  - The OaaS SKU is in the format FC-10-XXXXX-288-02-DD where XXXXX corresponds to the model code and DD corresponds to the validity period of the license in months.
  - This is a optional license for the Monitor SDWAN Bandwidth Service.
- License for each FortiGate device to be used as a site or spoke in the SD-WAN network:
  - Register an OaaS SKU to each FortiGate that will be used in a site or spoke. You must register each FortiGate device that will be used with OaaS to the same FortiCloud account that will be used to log in to OaaS.
  - You must also obtain a FortiCloud OaaS license, and apply it to each FortiGate device to be used as a site or spoke in the overlay.

For details on registering products, see Registering assets.

Preparing site FortiGate devices for OaaS

Complete the following tasks to prepare your FortiGate devices to be used by OaaS as site or spoke devices in the SD-WAN network:

1. Register the FortiGate devices with FortiCare, and activate the FortiGate devices with FortiGate FortiCloud. See Registering with FortiCare and activating with FortiGate Cloud on page 15.
2. Configure each FortiGate with a WAN IP address and a default gateway IP address for accessing the internet. See Configuring FortiGates for sites on page 16.

Registering with FortiCare and activating with FortiGate Cloud

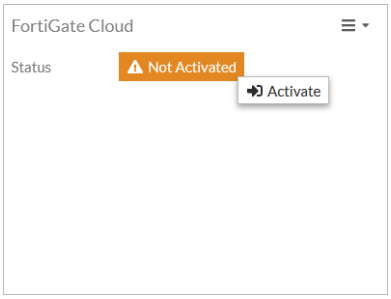
Your FortiGate devices must be registered with FortiCare and activated with FortiGate Cloud.

This step is required because OaaS uses the FortiCloud management tunnel to FortiGates to retrieve interface information and to install configuration settings orchestrated from OaaS.

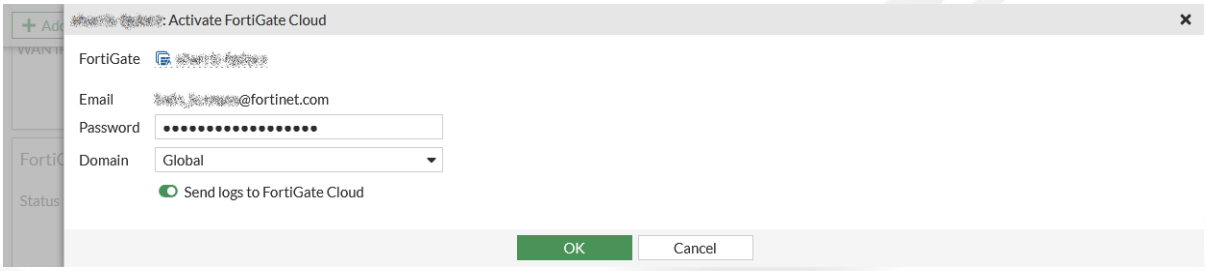
Typically, for FortiGate devices already registered with FortiCare, you can activate them using these steps on the FortiGate GUI:

To configure an additional incoming interface on a spoke:

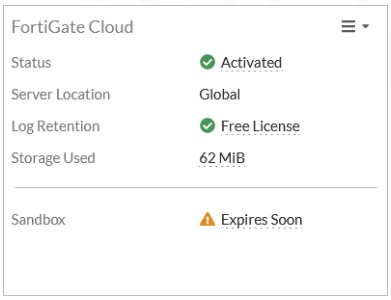
1. Go to *Dashboard* > *Status*.
2. In the *FortiGate Cloud* widget, click *Not Activated* > *Activate*.



3. Enter the password for the account that was used to register the FortiGate.



4. Click *OK*.
   The *FortiGate Cloud* widget now shows the activated FortiCloud account.



For details on registering products, see Registering assets.

For details on activating the FortiGate with FortiGate Cloud, see FortiCare and FortiGate Cloud login.

Configuring FortiGates for sites

Each FortiGate that will be used as a site in the SD-WAN network must be configured with a WAN IP address and default gateway IP address for accessing the internet. See Basic configuration.

The local interface IP address for the local subnet must be configured as well. See Interface settings.

Before OaaS can use your FortiGate as a site in the SD-WAN network, the following requirements must be met:

- WAN and LAN ports must not be in any predefined zone or must not be a member of any other SD-WAN zone. See Zone.
- WAN and LAN ports must not be bound to any existing firewall policies. See Firewall Policy.
- For the direct or indirect local subnet port configured in OaaS, do not use a switch or aggregate interface member port. See Software switch, Hardware switch, and Aggregation and redundancy.

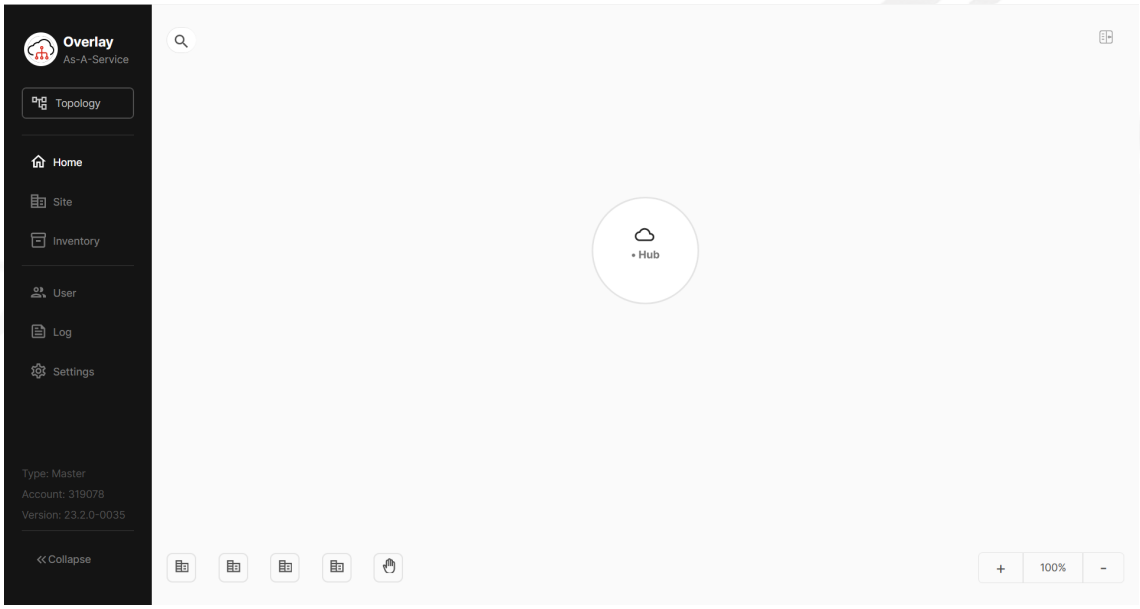
These steps are required because OaaS obtains the interface configuration from the FortiGate and displays it for overlay configuration in the OaaS portal.

Accessing the OaaS portal

To access the OaaS portal:

1. Go to https://overlay-as-a-service.forticloud.com.
2. Log in using your FortiCloud account.

After logging in, the *Home* view is displayed.

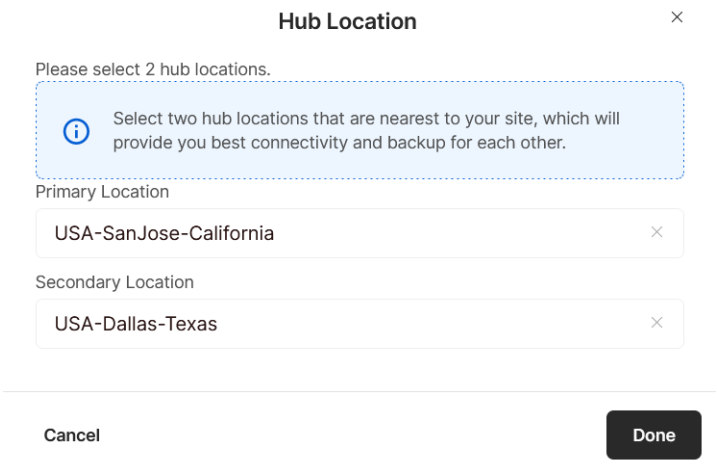


Defining the SD-WAN hub device

OaaS creates the hub device of the SD-WAN network for you, but you must specify the primary and secondary locations for the hub.

To choose the hub locations:

1. Click *Topology* to enter the *Setup Topology* view.
2. Right-click *Hub* and select *Choose a location*.
3. In the *Hub Location* dialog box, select the *Primary Location* and the *Secondary Location*.



4. Click *Done*.

Deploying a new SD-WAN site for the hub

Complete the following steps to use your FortiGates with OaaS to configure and deploy a new site for the hub in the SD-WAN network:

1. Add a new site to the hub. See Adding a new site to a hub on page 18.
2. Add an ISP for your site. See Adding an ISP for the site on page 19.
3. Add a subnet for your site. See Adding a subnet for the site on page 20.
4. Deploy the SD-WAN configuration to your site and view task status. See Deploying the SD-WAN configuration to your sites and viewing Task Status on page 21.

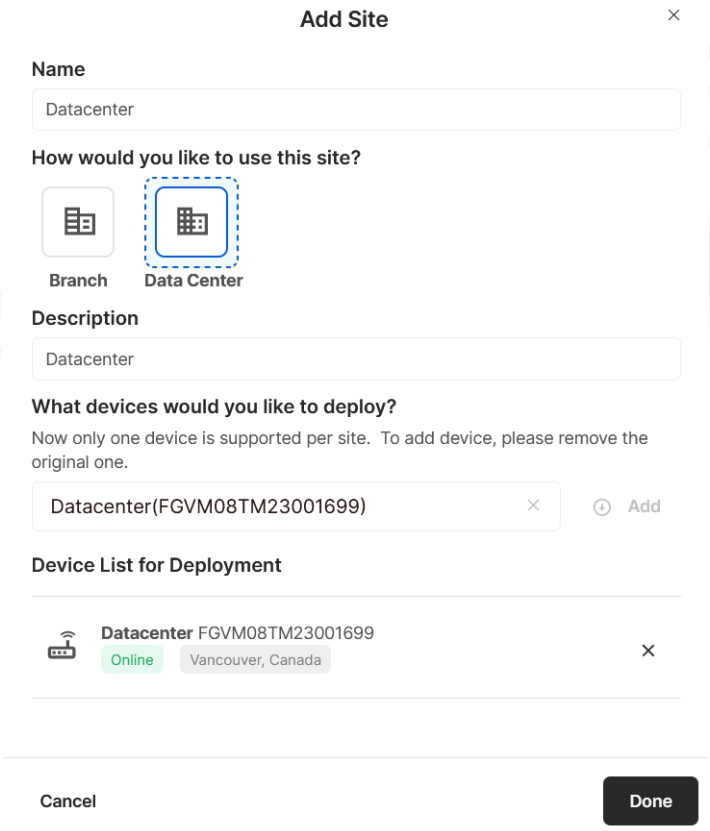
Adding a new site to a hub

SD-WAN sites are authorized FortiGate devices. Use OaaS to add your FortiGate devices to the site.

To add a new site:

1. From the *Topology* view, right-click the *Hub* and select *Add Site*.
2. In the *Add Site* dialog box, set the following options:
   - Enter a name for the site.
   - Set *How would you like to use this site?* to either *Branch* or *Data Center*.

     This option affects how the site is displayed in the *Home* and *Topology* views. It does not affect how OaaS configures or manages the site.
   - (Optional) In the *Description* box, enter a description.
3. Select the FortiGates to deploy:
   a. From the *What devices would you like to deploy* dropdown list, select a FortiGate, and click *Add*.
   b. Repeat this step to add all FortiGates.



It is critical for the added FortiGate device to appear with a status of *Online*. If the device lacks a status of *Online*, check whether the device is:

- Powered on
- Activated or logged in to FortiGate Cloud
- Configured and properly connected to its ISP's WAN link

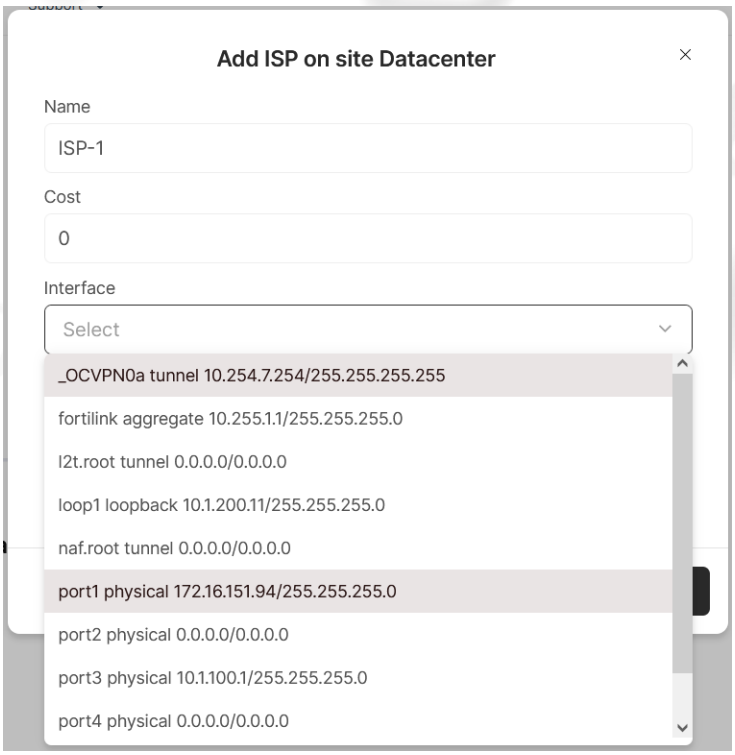
4. Click *Done*.

Adding an ISP for the site

Configure how the SD-WAN device connects to the region by selecting the ISP link for external access.

To add an ISP for your site:

1. From the *Topology* view, right-click the site and select *Add ISP*.
2. In the *Add ISP on site <site name>* dialog box, enter the *Name*, *Cost*, and *Description*, and select *Interface* in the dropdown list.



3. Click *Done*.

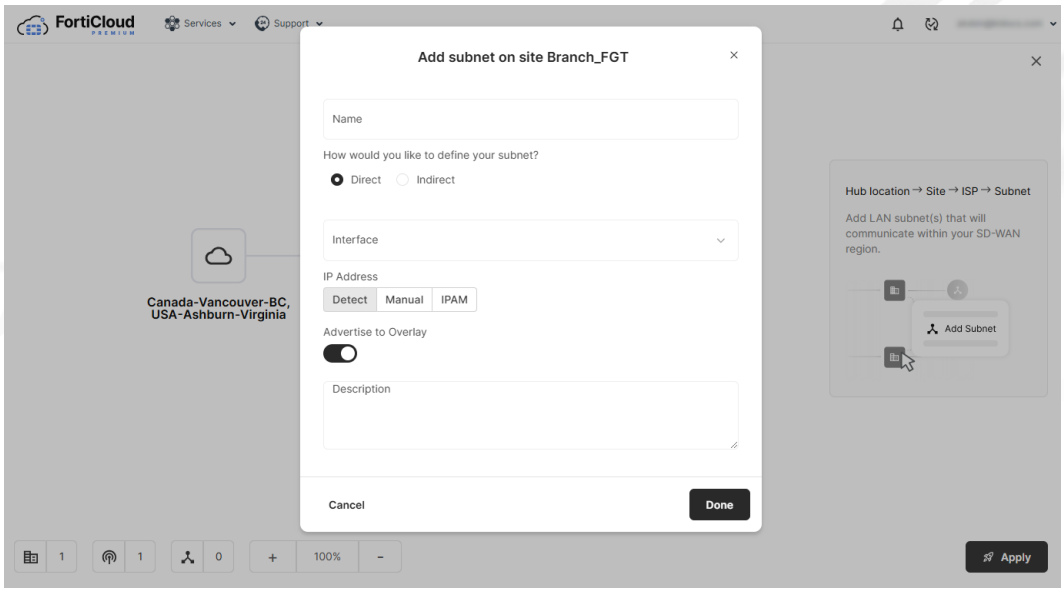
Adding a subnet for the site

Add LAN subnets(s) that will communicate within your SD-WAN region.

To add a subnet for your site:

1. From the *Topology* view, right-click the site, and select *Add Subnet* to add a LAN subnet behind the site.
2. In the *Add subnet on site <sitename>* dialog box:
   a. Enter a name for the subnet.
   b. For *How would you like to define your subnet?*, select either *Direct* or *Indirect*.
      - Direct means that you will directly select the subnet assigned to a FortiGate interface.
      - Indirect means that you will use a Classless Inter-Domain Routing (CIDR) prefix to select a subset of the interface's assigned subnet, which is typically a smaller subnet (192.168.2.0/30) within the interface's subnet (192.168.2.0/24). An indirect subnet usually means that there are multiple networks configured behind the interface.
   c. Select the *Interface* in the dropdown list.
   d. Select the *IP Address* method.
   e. Configure the IP address information, as needed. Fields will differ depending on the *IP Address* selected.
   f. Enable or disable *Advertise to Overlay*.
   g. (Optional) Enter a description.

3. Click *Done*.



Deploying the SD-WAN configuration to your sites and viewing Task Status

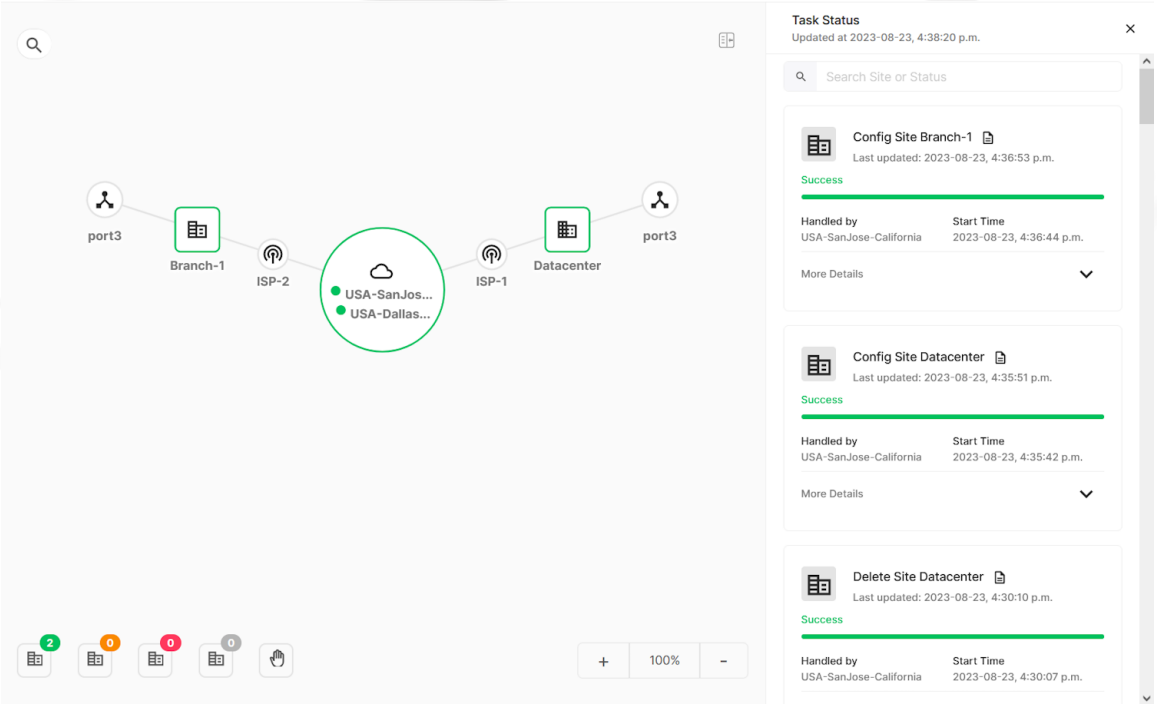
You may want to add several sites with their corresponding ISP and subnet(s) in the *Topology* view. For this deployment example, you will need to add the Branch-1 site to the topology.

When you apply the changes, the configuration is deployed to the FortiGates, and the SD-WAN network is configured.

To apply changes and view Task Status:

1. From the *Topology* view, finish adding sites and their corresponding configuration, and click *Apply* to save changes.

   After clicking *Apply*, the sync process runs in the background.
2. Click the *X* at top-right to close the *Setup Topology* view and view the deployment.
3. Next to the FortiCloud username at the top-right of the screen, click the *Task Status* icon to view the status of each configuration task.



4. Click the *View Config* file icon to the right of the task name to view the FortiGate configuration that was installed by the task.

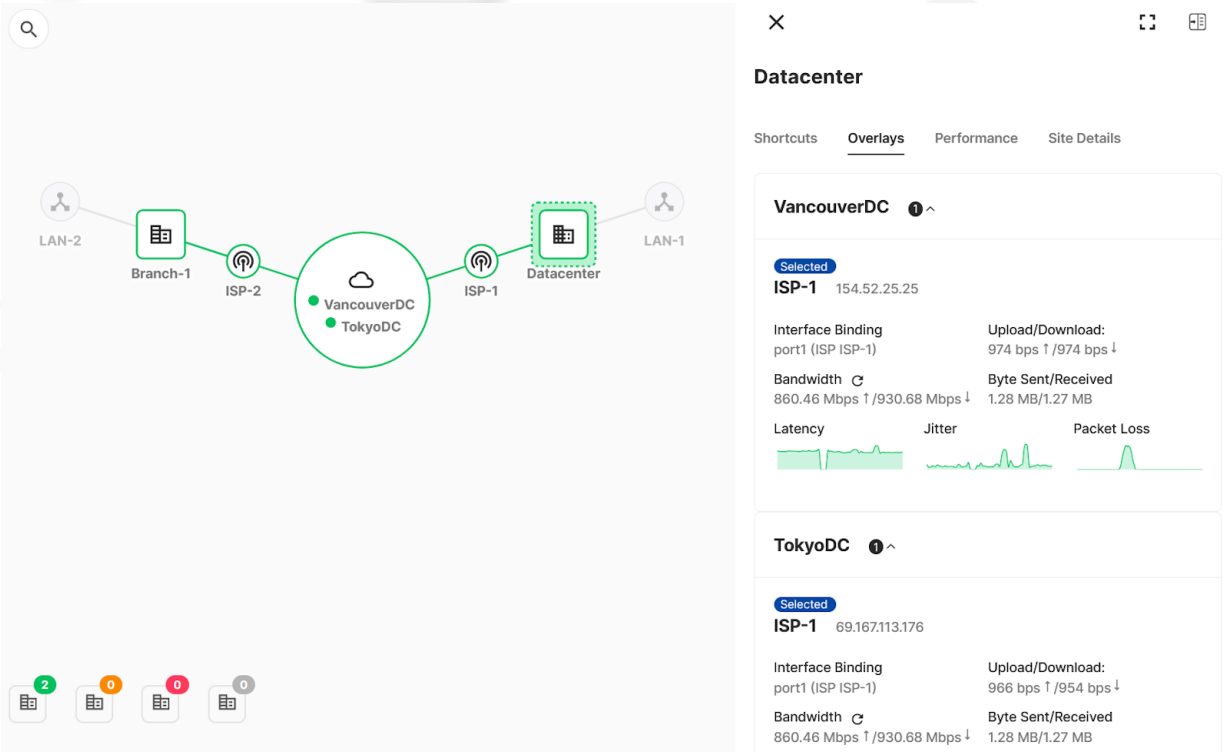
If a task has failed, then you can retry the task by clicking the *Retry* icon to the right of the *Failed* message.

Monitoring link performance and quality across SD-WAN devices in OaaS

To monitor Monitoring link performance and quality across SD-WAN devices in OaaS:

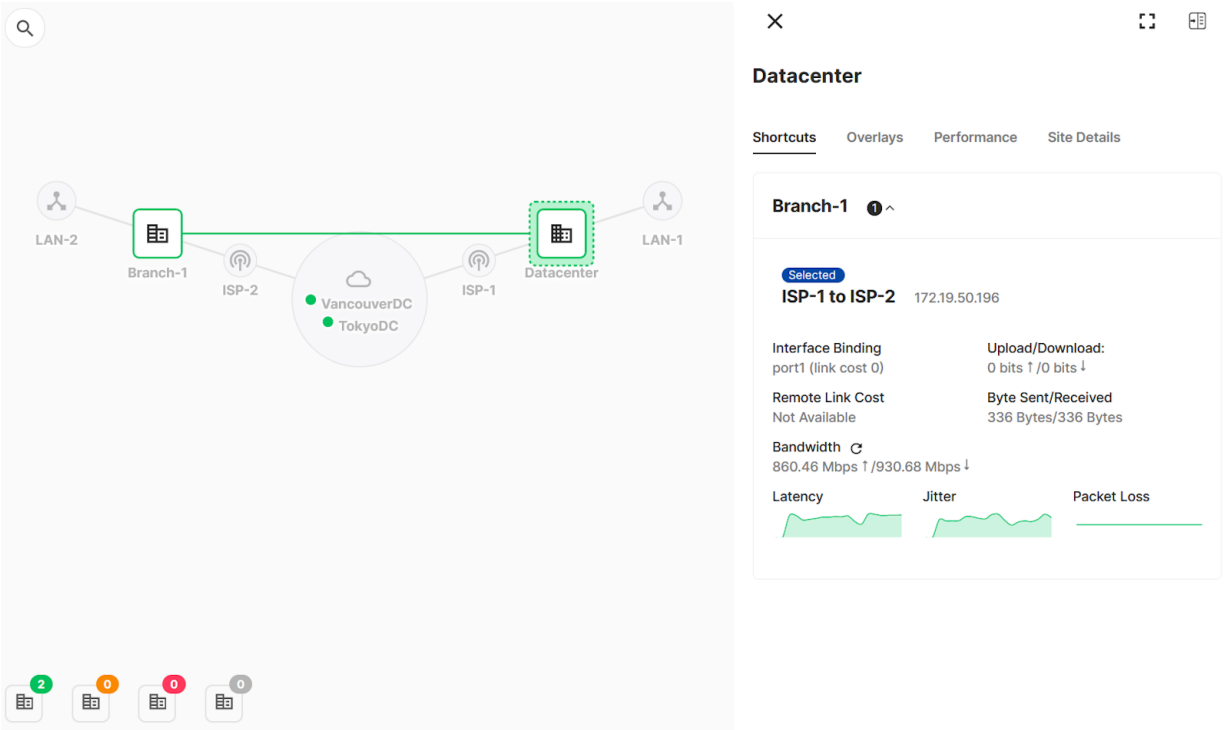
1. In the *Home* view, click any of the sites in the diagram to monitor the health of their overlays, monitor their performance, and view site details.

CONFIGURATION STEPS

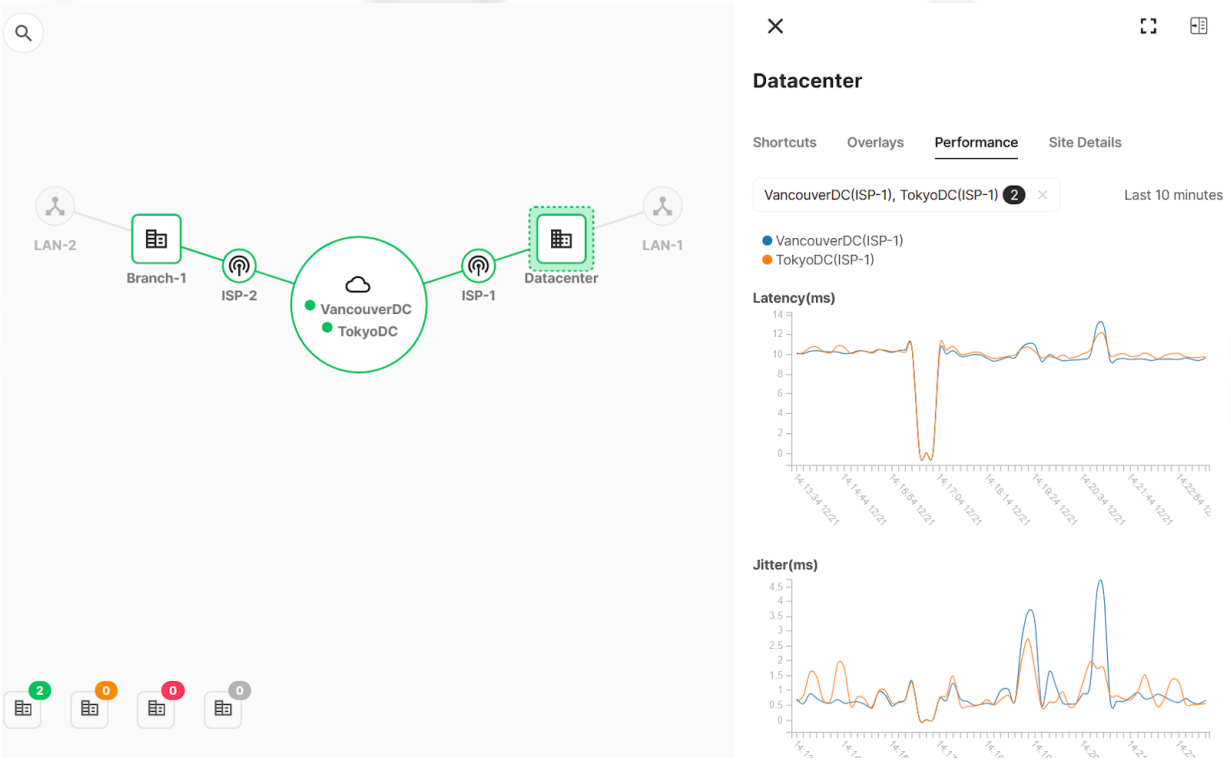


Bandwidth can be determined by performing a speed test. See Performing bandwidth speed tests in the OaaS Administration Guide.

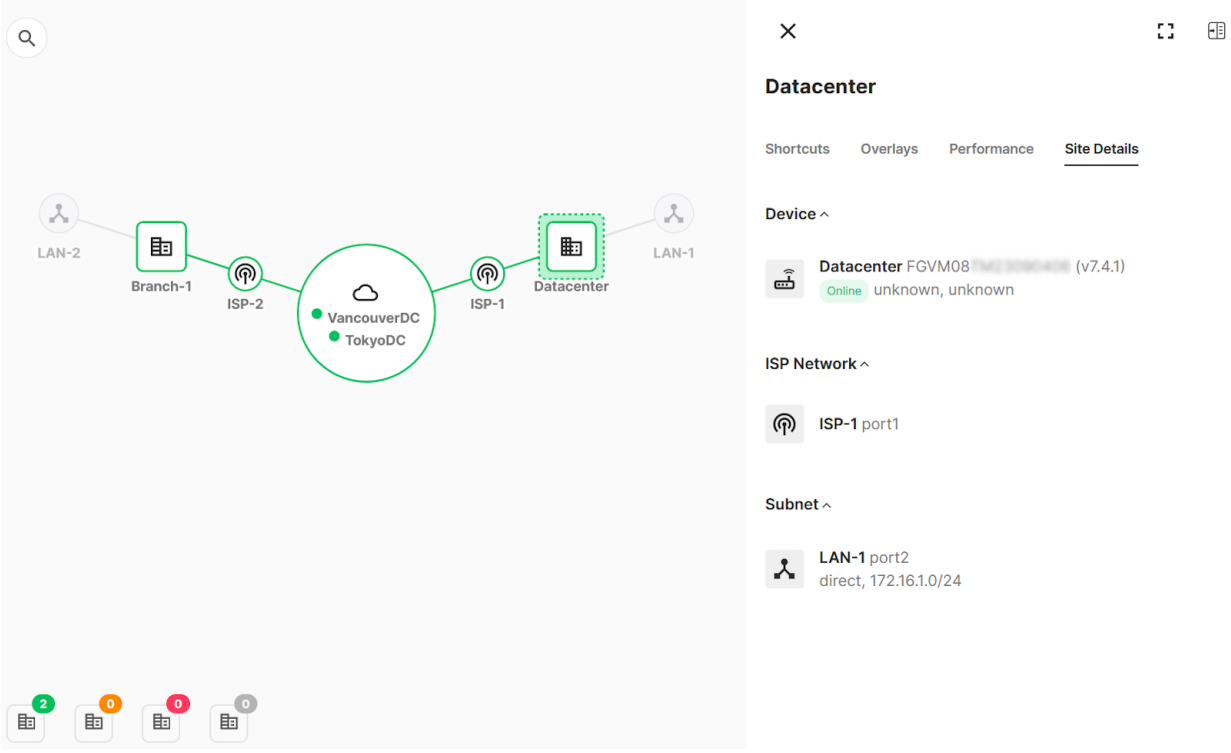
2. In the *Home* view with a site selected, select *Shortcuts* to monitor the health of the shortcut tunnels between sites.



3. In the *Home* view with a site selected, click *Performance*, and then use the graphs to monitor the latency, jitter, and packet loss. Select a time stamp to view the values for the hub locations and remote sites on the graphs.



4. In the *Home* view with a site selected, click *Site Details* to review details about the selected site.



Centralized OaaS policy example

Centralized OaaS policies can be configured and applied in the OaaS portal. See OaaS Policy for more information.

Given a topology that has already been previously orchestrated using the OaaS portal, the following example demonstrates how to create OaaS policies between two FortiGate sites in that topology using these steps:

CONFIGURATION STEPS

1. Configure an OaaS policy to allow traffic from the Datacenter LAN (10.1.100.0/24) to the Branch 1 LAN (10.1.1.0/24).
2. Test and verify connectivity from the Datacenter LAN to the Branch 1 LAN.
3. Test and verify connectivity from the Branch 1 LAN and the Datacenter LAN is not allowed by the OaaS policy configured in Step 1.
4. Configure an OaaS policy to allow traffic from the Branch 1 LAN (10.1.1.0/24) to the Datacenter LAN (10.1.100.0/24).
5. Test and verify connectivity from the Branch 1 LAN to the Datacenter LAN.

For granularity, OaaS policies are destined for the source and destination specified only. Therefore, an OaaS policy from site A crossing overlay networks to site B does not automatically allow traffic in the opposite direction from site B to site A. You must create a separate OaaS policy for traffic in the opposite direction between sites.

To configure an OaaS policy to allow traffic from the Datacenter LAN to the Branch 1 LAN:

1. Go to *Policy* > *OAAS Policy*.
2. Configure the policy as follows:

Name		DCport3-to-Br1port3
Source		Address
	Site	Datacenter
	Interface	port3 10.1.100.0/24
	Address	port3@Datacenter
Destination		Address
	Site	Branch-1
	Interface	port3 10.1.1.0/24
	Address	port3@Branch-1
Service		ALL
Service Group		
Schedule/Schedule Group		Schedule
Schedule		always
Action		Accept
Logging Options		
	Log Allowed Traffic	Enabled, All Sessions
	Generate Logs when Session Starts	Disabled
	Description	DC port3 to Br1 port3
Enable this policy		Enabled

3. Click *Save*.

4. In *Policy* > *OAAS Policy*:
   a. Status is *Unsaved*. Click *Save*.
   b. Status is *Unsynced*. Click *Apply*.
   c. Status is *Synced*. The policy has been applied to the FortiGate devices in the specified sites.

To test and verify connectivity from the Datacenter LAN to the Branch 1 LAN:

1. Run these CLI commands on the Datacenter FortiGate:

```
# execute ping-options source <IP address in Datacenter LAN>
# execute ping <IP address in Branch 1 LAN>
```

2. Observe the following output:

```
Datacenter# execute ping-options source 10.1.100.1

Datacenter# execute ping 10.1.1.99
PING 10.1.1.99 (10.1.1.99): 56 data bytes
64 bytes from 10.1.1.99: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 10.1.1.99: icmp_seq=1 ttl=255 time=2.7 ms
64 bytes from 10.1.1.99: icmp_seq=2 ttl=255 time=1.2 ms
64 bytes from 10.1.1.99: icmp_seq=3 ttl=255 time=1.9 ms
64 bytes from 10.1.1.99: icmp_seq=4 ttl=255 time=0.6 ms

--- 10.1.1.99 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.4/2.7 ms
```

To test and verify connectivity from the Branch 1 LAN and the Datacenter LAN is not allowed by the OaaS policy:

1. Run these CLI commands on the Branch 1 FortiGate:

```
# execute ping-options source <IP address in Branch 1 LAN>
# execute ping <IP address in Datacenter LAN>
```

2. Observe the following output:

```
Branch-1# execute ping-options source 10.1.1.99

Branch-1# execute ping 10.1.100.1
PING 10.1.100.1 (10.1.100.1): 56 data bytes

--- 10.1.100.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

To configure an OaaS policy to allow traffic from the Branch 1 LAN to the Datacenter LAN:

1. Go to *Policy* > *OAAS Policy*.
2. Configure the policy as follows:

Name		Br1port3-to-DCport3
Source		Address
	Site	Branch-1
	Interface	port3 10.1.1.0/24

	Address	port3@Branch-1
Destination		Address
	Site	Datacenter
	Interface	port3 10.1.100.0/24
	Address	port3@Datacenter
Service		ALL
Service Group		
Schedule/Schedule Group		Schedule
Schedule		always
Action		Accept
Logging Options		
	Log Allowed Traffic	Enabled, All Sessions
	Generate Logs when Session Starts	Disabled
	Description	
Enable this policy		Enabled

3. Click *Save*.
4. In *Policy* > *OAAS Policy*:
   a. Status is *Unsaved*. Click *Save*.
   b. Status is *Unsynced*. Click *Apply*.
   c. Status is *Synced*. The policy has been applied to the FortiGate devices in the specified sites.

To test and verify connectivity from the Branch 1 LAN to the Datacenter LAN:

1. Run these CLI commands on the Branch 1 FortiGate:

```
# execute ping-options source <IP address in Branch 1 LAN>
# execute ping <IP address in Datacenter LAN>
```

2. Observe the following output:

```
Branch-1# execute ping-options source 10.1.1.99

Branch-1# execute ping 10.1.100.1
PING 10.1.100.1 (10.1.100.1): 56 data bytes
64 bytes from 10.1.100.1: icmp_seq=0 ttl=254 time=50.6 ms
64 bytes from 10.1.100.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.1.100.1: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 10.1.100.1: icmp_seq=3 ttl=255 time=0.7 ms
64 bytes from 10.1.100.1: icmp_seq=4 ttl=255 time=0.4 ms

--- 10.1.100.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/10.5/50.6 ms
```

Testing and verifying connectivity between sites deployed using OaaS

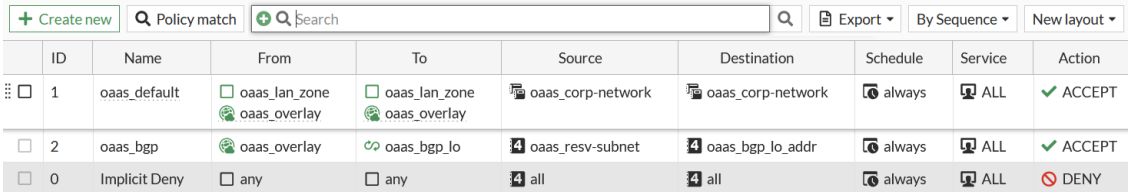
Following is a summary of the steps you can use to verify the configurations created by OaaS for the spoke FortiGates and to test connectivity between spoke devices:

- Firewall policies: Verifying firewall policies on a spoke on page 28
- IPsec VPN tunnels: Verifying IPsec VPN tunnels on a spoke on page 29
- BGP routing: Verify BGP routing on a spoke on page 29
- Performance SLAs: Verifying the performance SLAs on a spoke on page 30
- ADVPN communication: Verify spoke to spoke ADVPN communication on page 31
- SD-WAN rules on a spoke: Verifying SD-WAN rules on a spoke FortiGate on page 32
- OaaS agent status: Verifying the OaaS agent for uninterrupted spoke traffic on page 33

Verifying firewall policies on a spoke

To verify firewall policies on a spoke:

1. In FortiOS on a spoke FortiGate, go to *Policy & Objects* > *Firewall Policy*.
2. Verify that firewall policies have been configured.



OaaS creates firewall policies with wildcard address objects and services on the spoke FortiGates that allow all traffic. For some cases, these policies do not provide the necessary granularity to restrict overlay traffic to specific subnets or hosts.

OaaS will not affect any other FortiGate configuration settings and will only create and modify configuration settings that it generated. Therefore, the FortiGate spoke administrator is free to add firewall policies and other configuration settings as needed that only references these specific configuration settings created by OaaS:

- `oaas_lan_zone` and `oaas_wan_zone` defined in `config system zone`
- `oaas_overlay` defined in `config zone` within `config system sdwan`
- `oaas_corp_network` defined in `config firewall addrgrp`

However, to ensure proper operation of OaaS with regards to topology changes and updates, ensure that you do not reference any other OaaS configuration settings in firewall policies and other configuration settings that you have added after installing settings orchestrated from OaaS.

Verifying IPsec VPN tunnels on a spoke

To verify IPsec VPN tunnels on a spoke:

1. In FortiOS on a spoke FortiGate, go to *Dashboard* > *Network*, and click the IPsec widget to expand it.
2. Verify the IPsec tunnels that go back to the hub.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1
Custom 2					
oaas_overlay2	[redacted]	FGVHUBTM[redacted]-overlay-gateway	124.88 kB	124.91 kB	oaas_overlay2
oaas_overlay1	[redacted]	FGVHUBTM[redacted]-overlay-gateway	125.02 kB	125.01 kB	oaas_overlay1

For example, *oaas_overlay1* and *oaas_overlay2* are identified as the spoke's tunnels to the primary and secondary hubs, respectively.

When there is spoke-to-spoke communication, notice that a *_0* is added to the name of the shortcut tunnel to the hub.

For example, *oaas_overlay1_0* is identified as the spoke's tunnel that was created for traffic from spoke 1 to spoke 2.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1
Custom 3					
oaas_overlay2_0	[redacted]	Branch-1-port1	252 B	336 B	oaas_overlay2_0
oaas_overlay2	[redacted]	FGVHUBTM[redacted]-overlay-gateway	148.13 kB	148.16 kB	oaas_overlay2
oaas_overlay1	[redacted]	FGVHUBTM[redacted]-overlay-gateway	148.32 kB	148.31 kB	oaas_overlay1

Verify BGP routing on a spoke

To verify BGP routing on a spoke:

1. In the CLI on a spoke FortiGate, check the BGP peering status:

```
Datacenter # get router info bgp summary

VRF 0 BGP router identifier 10.200.0.54, local AS number 65001
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.200.0.1 4      65001     111     109        2    0    0 00:23:15        2
10.200.0.3 4      65001     108     108        2    0    0 00:23:15        2

Total number of neighbors 2
```

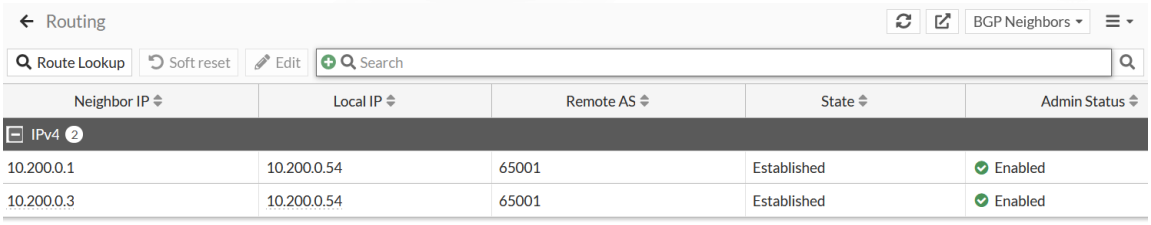
2. Check the BGP advertised routes:

```
Datacenter # get router info bgp neighbors 10.200.0.1 advertised-routes
VRF 0 BGP table version is 3, local router ID is 10.200.0.54
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i172.16.1.0/24    10.200.0.54                      100  32768        0 i <-/->

Total number of prefixes 1
```

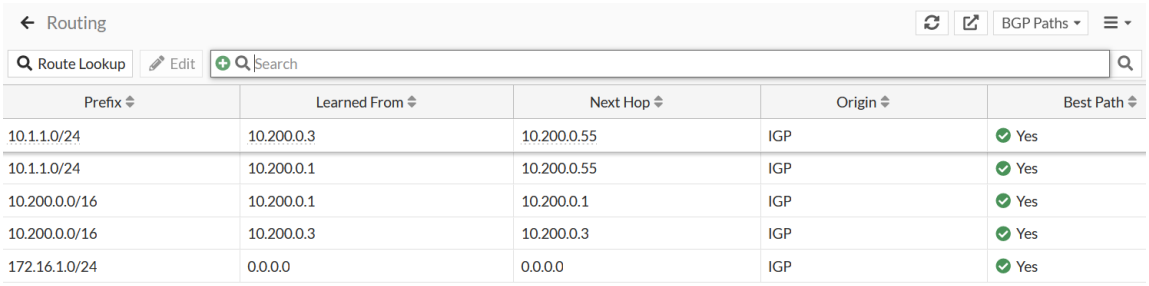
3. Check the BGP learned routes:

```
Datacenter # get router info bgp neighbors 10.200.0.1 received-routes
VRF 0 BGP table version is 3, local router ID is 10.200.0.54
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.1.1.0/24      10.200.0.55                      100      0         0 i <-/->
*>i10.200.0.0/16    10.200.0.1                       100      0         0 i <-/->

Total number of prefixes 2
```

4. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
5. In the dropdown, select *BGP Neighbors*.



6. In the dropdown, select *BGP Paths*.

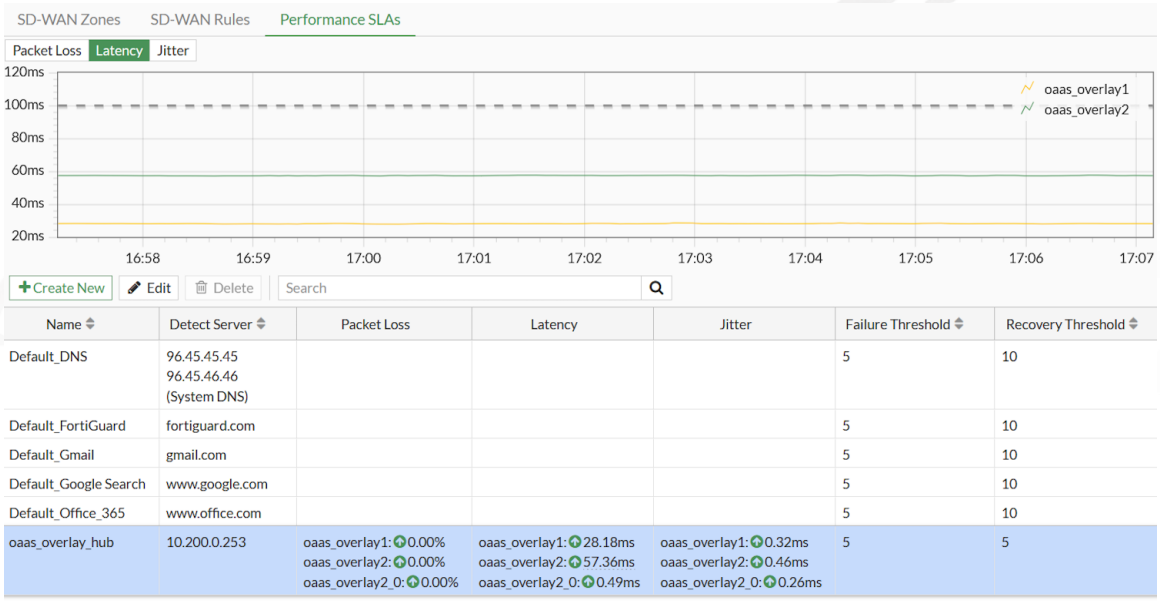


Verifying the performance SLAs on a spoke

To verify the performance SLAs on a spoke:

1. In FortiOS on a spoke FortiGate, go to *Network* > *SD-WAN*, and select the *Performance SLAs* tab.
2. Verify that the performance SLA is automatically created for the hub FortiGate. There is a new entry (*oaas_overlay_hub*).
   - The performance SLAs to the primary and secondary hubs are denoted by *oaas_overlay1* and *oaas_overlay2*, respectively.

- The performance SLA to the spoke is denoted by *oaas_overlay1_0*.



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_DNS	96.45.45.45 96.45.46.46 (System DNS)				5	10
Default_FortiGuard	fortiguard.com				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	www.google.com				5	10
Default_Office_365	www.office.com				5	10
oaas_overlay_hub	10.200.0.253	oaas_overlay1: 0.00% oaas_overlay2: 0.00% oaas_overlay2_0: 0.00%	oaas_overlay1: 28.18ms oaas_overlay2: 57.36ms oaas_overlay2_0: 0.49ms	oaas_overlay1: 0.32ms oaas_overlay2: 0.46ms oaas_overlay2_0: 0.26ms	5	5

Once a shortcut tunnel is established, it is also monitored using the performance SLA. If the performance SLA of the shortcut tunnel exceeds the specified thresholds during operation, then the shortcut tunnel will be removed as the best route learned using BGP in the routing table. Therefore, traffic for the destination spoke will be forwarded by the source spoke through the hub, which is not ideal.

This can be observed from `get router info routing-table all`:

```
Datacenter # get router info routing-table all
…
B       10.1.1.0/24 [200/0] via 10.200.0.57 tag 180879361 (recursive via oaas_overlay2_0
tunnel 172.16.151.95), 00:00:05
                                                          (recursive via oaas_overlay1
tunnel 38.21.192.175), 00:00:05, [1/0]
                    [200/0] via 10.200.0.57 tag 180879363 (recursive via oaas_overlay2_0
tunnel 172.16.151.95), 00:00:05, [1/0]
…
```

If the `oaas_overlay2_0` shortcut tunnel on the source spoke does not meet the performance SLA, the routes through `oaas_overlay2_0` will be removed, and then the `oaas_overlay1` tunnel to the hub becomes the best path to forward traffic. In that case, traffic will be forwarded to the hub on the way to the destination spoke.

Verify spoke to spoke ADVPN communication

To verify spoke-to-spoke ADVPN communication:

1. From Datacenter (172.16.1.99), ping Branch-1 (10.1.1.99):

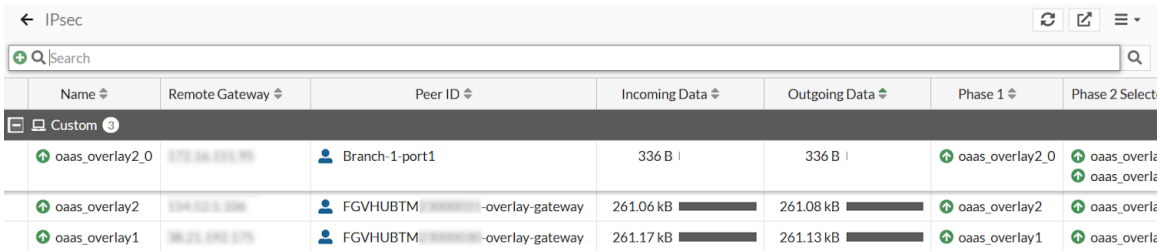
```
Datacenter # exec ping-options source 172.16.1.99

Datacenter # exec ping 10.1.1.99
PING 10.1.1.99 (10.1.1.99): 56 data bytes
64 bytes from 10.1.1.99: icmp_seq=0 ttl=254 time=114.7 ms
64 bytes from 10.1.1.99: icmp_seq=1 ttl=255 time=0.6 ms
64 bytes from 10.1.1.99: icmp_seq=2 ttl=255 time=0.6 ms
64 bytes from 10.1.1.99: icmp_seq=3 ttl=255 time=0.4 ms
64 bytes from 10.1.1.99: icmp_seq=4 ttl=255 time=0.3 ms
```

```
--- 10.1.1.99 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/23.3/114.7 ms
```

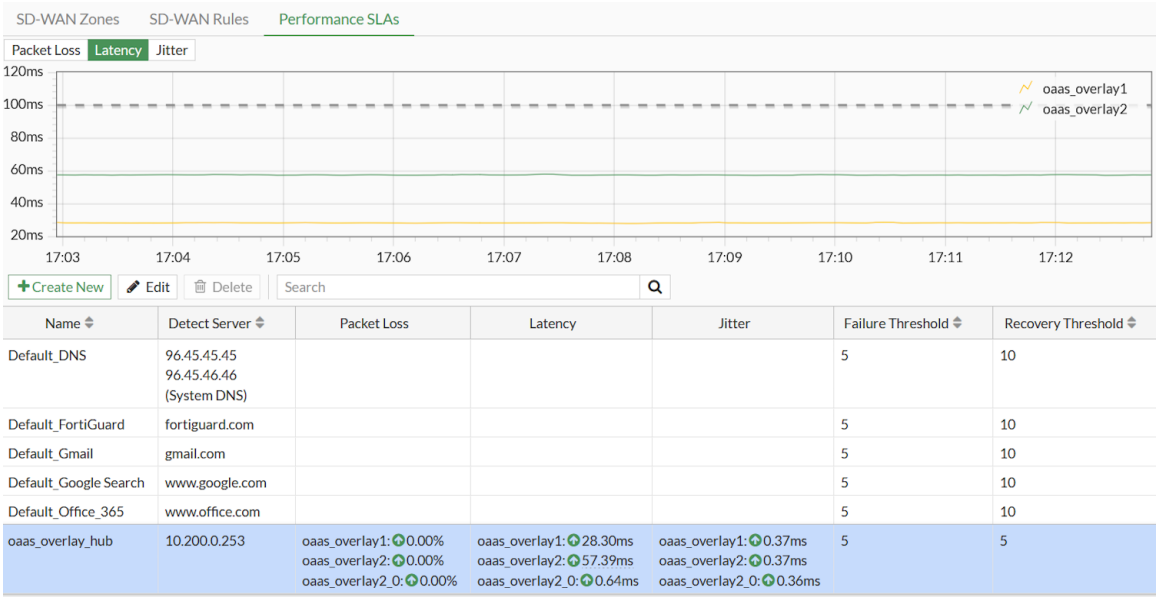
2. Verify the IPsec tunnel summary.
   - In the CLI, enter the following:

```
Datacenter # get vpn ipsec tunnel summary
'oaas_overlay2_0' 172.16.151.95:0  selectors(total,up): 2/2  rx(pkt,err): 4/0  tx
(pkt,err): 4/3
'oaas_overlay1' 38.21.192.175:4500  selectors(total,up): 1/1  rx(pkt,err): 4447/0
tx(pkt,err): 4448/14
'oaas_overlay2' 154.52.5.106:4500  selectors(total,up): 1/1  rx(pkt,err): 4444/0  tx
(pkt,err): 4445/14
```

   `oaas_overlay2_0` is identified as the spoke's tunnel that was created for traffic from the Datacenter spoke to the Branch-1 spoke.
   - In the GUI, go to *Dashboard* > *Network*, and click the *IPsec* widget to expand it.



3. Verify that the performance SLA was updated by going to *Network* > *SD-WAN*, and select the *Performance SLAs* tab.



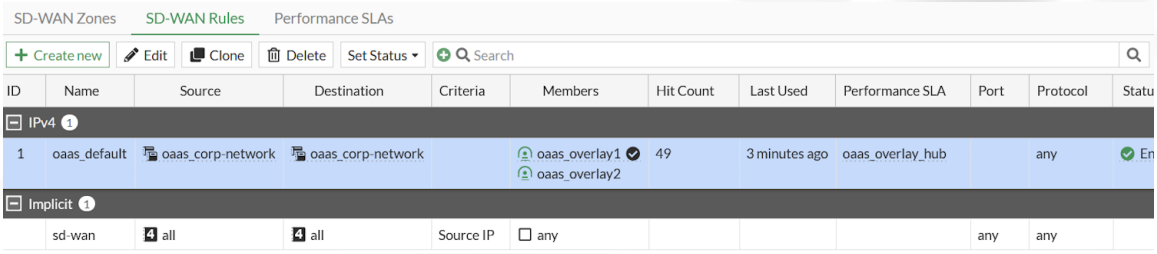
The first performance SLA, *oaas_overlay_hub*, corresponds to the spoke-to-hub VPN tunnel displays as *up*.

Verifying SD-WAN rules on a spoke FortiGate

On each spoke, OaaS automatically creates a performance SLA that corresponds to the hub FortiGate. An SD-WAN rule has been configured on the spoke FortiGates to direct traffic to the hub FortiGate using this performance SLA.

To verify SD-WAN rule on a spoke FortiGate:

1. On a spoke FortiGate, go to *Network* > *SD-WAN*, and select the *SD-WAN Rules* tab.
2. View the SD-WAN rule created by OaaS named *oaas_default* that corresponds to the performance SLA named *oaas_overlay_hub#1*.



You can create additional SD-WAN rules. Configure and place new rules below the *oaas_default* rule.

Verifying the OaaS agent for uninterrupted spoke traffic

To ensure FortiGate spoke traffic remains uninterrupted when configuration is orchestrated from OaaS, support for an OaaS agent on the FortiGate is available. The OaaS agent communicates with the OaaS controller in FortiCloud, validates and compares the FortiOS configuration, and applies the FortiOS configuration to the FortiGate as a transaction when it has been orchestrated from the OaaS portal. Secure communication between the OaaS agent and the OaaS controller is achieved using the FGFM management tunnel.

If any configuration change fails to be applied, then the OaaS agent rolls back all configuration changes that were orchestrated. The OaaS status on the spoke FortiGate can be acquired using `get oaas status`.

To determine the status of OaaS:

```
# get oaas status
Account ID: 78992
Account: admin@domain.com
Site: site1
Configuration version: 4
Configuration sync status: SUCCESS
    Target version: 4
    Task ID: xxxxxxxxx
    Error:
```

www.fortinet.com

85-244-1111713-20250103